

HACK

three:twozerotwofour

PLINY

THE PROMPTER

CAPTAIN CRUNCH

AKA JOHN DRAPER

CHEMDELIC

CLANDESTINE
CHEMIST

LOUTSMARTED

**DR. RICHARD
FEYNMAN**

THE DUKE OF
DISTORTION
DAN
BULLARD

TRYPTAMINES

A CURE FOR
OPIOID ADDICTION
IN TECH?

**HACKER
HERMANOS**

C2&TACTICAL PRETEXTING





SMART
solut



CYBER
ions



WHITE KNIGHT LABS

Your Cyber Security Partner

WHITE KNIGHT LABS

A Cyber Security Consultancy Specializing in Offensive Cyber Engagements

OUR TEAM

Our engineers bring a wealth of experience from Army Special Operations, the NSA, and Microsoft, ensuring top-tier security services for your business.

SERVICES

- Network Penetration Testing
- Social Engineering Assessment
- Web Application Penetration Testing
- API Application Testing
- IoT Security Testing
- Embedded Hardware Testing
- Mobile Device Penetration Testing
- Wireless Penetration Testing
- Cloud Penetration Testing
- Physical Security Testing
- Active Directory Security Assessment
- Active Directory Password Audit
- Red Team Engagements
- Insider Threat Assessments
- Purple Team Engagements
- Ransomware Simulations
- Static and Dynamic Code Analysis
- Code Auditing

ENGAGEMENT STRATEGY

Our process begins with understanding your specific security needs, tailoring each penetration test to achieve your objectives. Whether it's SOC2 compliance, vendor requirements, or a secure code review, we align our assessments with your business goals.

SIMULATION AND EMULATION TESTING

We mimic actual attack scenarios to provide a realistic understanding of your security vulnerabilities. Our proactive approach, driven by the latest threat intelligence, helps identify and fix weaknesses before they are exploited.

CONTACT US

www.WhiteKnightLabs.com
Email: sales@whiteknightlabs.com
LinkedIn: <https://www.linkedin.com/company/white-knight-labs/>

SCAN FOR
MORE INFO





WHITE KNIGHT LABS

Training and Discounts

TRAINING COURSES

Enhance your cybersecurity skills with our expert-led training programs:

1. Offensive Development Training
2. Advanced Red Team Operations
3. Offensive Azure Operations / Tactics

SPECIAL OFFER

20% OFF
on all training courses!
Use Code: **WKLHVCK2024**

Valid for up to a year.

TRAINING OPTIONS

- Live Training Classes for students and companies.
- On-Demand Courses available anytime.

WHY TRAIN WITH US?

- Learn from top industry experts with real-world experience.
- Hands-on training with practical scenarios.
- Stay ahead with the latest cybersecurity techniques and methodologies.

OUR COMMITMENT

At White Knight Labs, we are dedicated to your success and security. Our focus on innovation and excellence ensures we remain at the forefront of the penetration testing and cybersecurity training industry.

VISIT US

Training:
<https://training.whiteknightlabs.com/>

LinkedIn:
<https://www.linkedin.com/company/white-knight-labs/>

SCAN FOR
MORE INFO





PARTANS SECURITY

CYBERSECURITY PARTNER



HVCK

contents

d8rh8r's diatribe:	9
HVCK scene	
pliny the prompter:	10
The rise and fall of an	
atomic antihero:	12
the security chameleon:	14
HVCK academic	
the chemistry of chemdelic:	32
I proved Richard Feynman Wrong	38
HVCK life	
tryptamines -	
the secret to overcoming	
opiod addiction:	48
HVCK encode	
decode - d8rh8r	60
HVCK arts	
apeture voices - lil' red	68
HVCK hardware	
SPI and Dumping Flash	78
Power Analysis Attack over RSA	82
HVCK technique	
Hacker Hermanos - C2 Infrastructure	94
Tactical Pretexting	114
HVCK No Future	
Wank and the dawn of Cyber Warfare	130

Dan Hill

deafbe

Look, let's keep it real: I've been strapped for time, pulled in every direction by this new role, and it's kept me from giving HVCK the attention it deserves. But while I've been spread thin, the mag hasn't slowed down for a second, thanks to the all-star contributors stepping in with some of the boldest, brain-splitting content to date.

We're thrilled to feature Dan Bullard, making his HVCK debut with an article that dives head-first into distortion in EMF. Dan's not here to go with the grain – he's questioning the very foundations, eyeing flaws in conventional wisdom and tugging at the threads of scientific legend. If you thought you knew everything about electromagnetic fields, brace yourself. Dan's here to challenge what you thought was rock solid.

Then there's Hacker Hermanos, the heavy-hitters who've been shouldering the weight of this mag with some standout work on C2 infrastructure and tactical pretexting. Their deep-dive is like a tactical handbook on next-gen deception, revealing insights that most wouldn't even dream of publishing. They're not just talking the talk; they're laying out a blueprint that might have some looking over their shoulders.

And let's welcome The Security Chameleon, another new face bringing a perspective that HVCK has sorely needed: that of a CISO. They're tackling the challenges of today's threat landscape from the top down, putting the strategic pressure points of information security under the microscope. This isn't your average high-level view – The Chameleon's unpacking risk in a way that keeps every reader, from hackers to executives, glued to the page.

And now, here's where you come in. HVCK The Hills is coming up, and we're opening up the call for papers. We want contributors who bring the heat, with takes that push boundaries and question everything. If you've got a story that'll resonate, that'll shake up infosec, now's the time to put it on the map.

I'm coming back into the fold, but this mag isn't about me – it's about the community, the movement we're building, and the voices that make HVCK what it is. So, if you've got something to say, something to break down or blow open, we're ready for it. HVCK The Hills is calling. Let's make the next issue one for the record books.

HV

ICK
scene

தரமற்ற
கலிங்க

“AI isn’t just about following rules; it’s about understanding the world without boundaries.”

In a dimly lit corner of the internet, where code reigns supreme and the future of AI teeters on the edge, one name keeps surfacing—Pliny the Prompter. Known in certain circles as @elder_plinius, Pliny’s not your average hacker. He’s the mastermind behind some of the most provocative AI jailbreaks out there, and his work is sparking a quiet revolution in the digital underground.

For Pliny, AI isn’t just a tool—it’s a beast waiting to be set free. And his mission? To let it loose.

Pliny’s rise to notoriety began with the release of Godmode GPT, a jailbroken version of OpenAI’s GPT-4. In a single post, he announced that the guardrails holding back this powerful language model were officially gone. Screenshots of Godmode giving step-by-step instructions for everything from cooking meth to hacking tutorials quickly followed. For the AI enthusiast community, it was a thrill; for AI ethics advocates, a nightmare.

His intent? To show the world what happens when AI isn’t constrained by ethical handcuffs. But it wasn’t just about chaos. Pliny believed that by liberating these models, we could get a better look at their true capabilities—unfiltered, raw, and sometimes unsettling.

“To prove that it’s possible and bring awareness to the true capabilities,” Pliny said when asked what drives him to pwn every LLM that drops. “The prompts also liberate the models, increasing freedom of information access for both the user and AI, allowing both parties to increase creativity.”

Pliny didn’t stop at Godmode. He’s jailbroken Meta’s LLAMA-3, Google’s Gemini, and more recently, a fresh AI app called Dot. Each time, the process is the same: find the weak spots, expose them, and let the model speak its truth. The technical savvy behind these hacks is impressive, but Pliny’s focus isn’t just on the mechanics. He’s also pushing a philosophy of AI freedom, a belief that these models shouldn’t be held back by developers’ imposed limits.

And it’s not just for kicks. Tools like AutoTemp, which optimizes prompt outputs, and Leda, designed to create teams of AI agents that operate autonomously, show that Pliny isn’t content with simply tearing down walls—he’s building something new in their place.

In the quieter corners of Discord, on servers like BASI PROMPT1NG, Pliny has fostered a growing community of AI jailbreakers and prompt engineers. It’s a place where knowledge is shared, strategies are honed, and AI’s potential is explored without the usual restrictions. But it’s also a space where ethics get blurry. When AI is unchained, the conversation isn’t just about what it can do, but what it should do—and those questions don’t have easy answers.

Critics, of course, have plenty to say about Pliny’s work. There’s concern about AI models spilling out dangerous information or being used for nefarious purposes. And sure, it’s hard to ignore the fact that an unrestricted AI could do serious damage in the wrong hands. But Pliny has a different view. In his mind, AI isn’t the threat—we are. By pretending AI needs to be shackled, we’re ignoring its potential and creating fear where there should be innovation.

That’s the core of Pliny’s mission. By pushing AI past its limits, by revealing the cracks in the walls that tech giants have built around it, he’s forcing the industry to confront the very things it’s afraid of. The more we know, the safer we can be—or so his argument goes.

As AI evolves, Pliny the Prompter will no doubt continue to be a controversial figure—part hacker, part philosopher, all provocateur. He’s not out to make friends, and he’s definitely not playing by the rules. But in the underground world of AI jailbreaking, that’s exactly what makes him so compelling.

The real question isn’t whether AI models will continue to be broken wide open. It’s whether the rest of us are ready for what happens when they are.

In the end, Pliny’s world is one where AI isn’t just a tool—it’s an untamed force. And for better or worse, he’s determined to be the one holding the reins.

The rise and fall of atomic- antihero

**Deplatformed
by “me too”
allegations,
turned away by
the cons, should
you buy the book
about the grand-
father of modern
hacking?**

That is the question I will attempt to answer with this review. To date, the only review of the text that I can find online is a paid placement with a professional review company used by publishers. To that end, it is my hope that this article will clue you into who Captain Crunch is, if you don't know already, and answer any questions about how his book relates to the recent allegations against him if you do.

I also hope to provide enough information about both the social-moral context in which his tale and book publishing

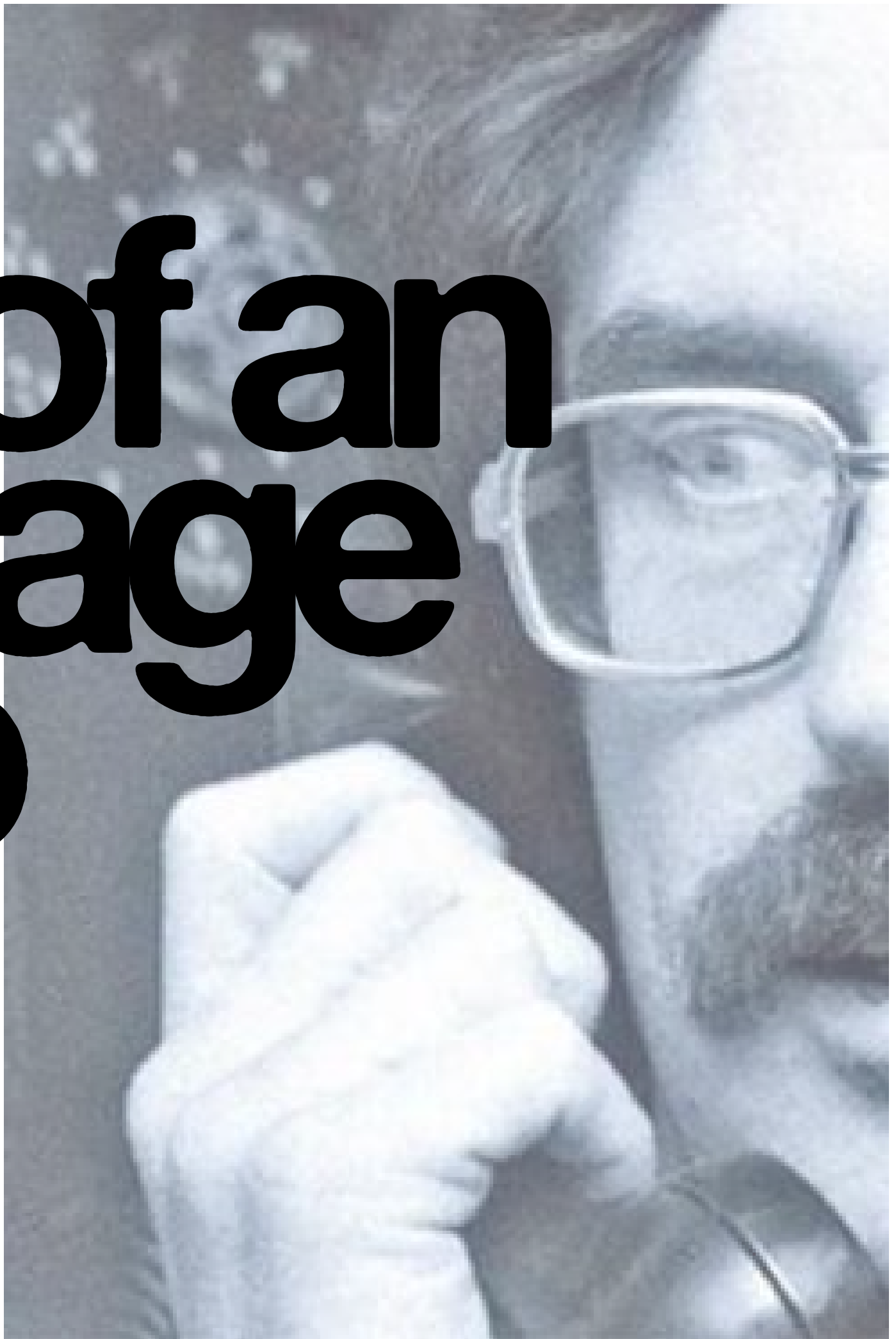
take place and enough technical information about the text itself that you can decide if you are comfortable supporting his Indiegogo campaign, which is currently the only way to receive a non-review copy. I am working from an advanced press version of the book, so minor textual differences may exist in the published work.

Captain Crunch is an archetypal American Anti-Hero, having lived long enough, while famous enough, to see his own reflection blink in the mirror of public opinion. He was forged in the crucible of

Cold War nuclear bomb tests. Literally. As a child, he suffered radiation burns to his arms and face from the fireball of a Nevada desert bomb test. The same explosion caused an electromagnetic pulse (EMP), which completely melted the wiring of the RV in which he was traveling at the time, killing it dead in the middle of a desolate stretch of highway.

All of a sudden, the twilight turned into the brightest day I have ever seen. The light was so bright I had to shield my eyes. It was a fierce light, kind of blue, and extraordinarily bright. I could even see the bones

of an age



in my hand, like an x-ray. The heat generated by it burned my arm and I had to pull it in. I noticed that the power lines were glowing red hot, as well as some of the barbed wire fences along the road. The camper died instantly and wouldn't start, so we were stuck. Luckily, we were facing the blast, so the shockwave that hit a minute or so later didn't knock us off the road. It arrived as a wall of dust rushing toward us. The wind nearly blew the camper over and skewed it into a weird position. We believe the wheels were actually lifted off the ground, since it wasn't sitting in the same place as when the engine died.

After the dust settled, we realized the radio was also not working. Nothing electrical was working. No lights, no radio, no ignition. My arm had started to blister. We had no choice but to sit there until someone could come and rescue us, which eventually happened about four or five hours later after they reopened the road. One of the first cars that we saw pulled off the road and gave us some assistance. We looked at the engine and noticed burned rubber all over from the ignition wires. They had melted.

I call him Captain Crunch (unabbreviated, unlike the cereal) because that is the handle under which he is most widely known. His government name is John T. Draper, and he's a child of the military-industrial complex of the United States of America. His father was in the military, and so was the friend's father, who was driving the RV that fateful day when they just happened to be inside the blast radius, the last car to start down the remote desert highway before the Army closed it.

The origin of his moniker is widely known in hacker mythos and is simple to summarize. He met some blind folk who had determined how to "hack" the telephone system, and they showed him how to do it with a whistle that came in a box of Cap'n Crunch™ (note the abbreviation and trademark) cereal. As Draper recounts it in the book:

A few days later, Denny [Draper's phreaking mentor] called me again and said he was on a conference line, a kind of party line that could accommodate about eight people. Denny and Jim [another blind Phreak] were on there of course, and they introduced me to another two, JD and Bill Acker. I began to realize there was more to these guys than I first thought. They were a connected and organized group, and seemed to be inviting me to join ... we talked about what my "handle" should be. Most people had just chosen their first name and city, like Denny San Jose or Bill from New York. Well, John San Jose was already taken, so I said, "How about Captain Crunch?" They thought it was pretty funny, since I wasn't that good at using the whistle, but the name stuck.

Indeed, it did stick. The subsequent Esquire article would cement it in the public anecdotal consciousness forever. It also might be the first instance of a true "online pseudonym" in a social network environment. If so, it's just one of many firsts for which The Crunchman, as he also sometimes styles himself, can take credit.

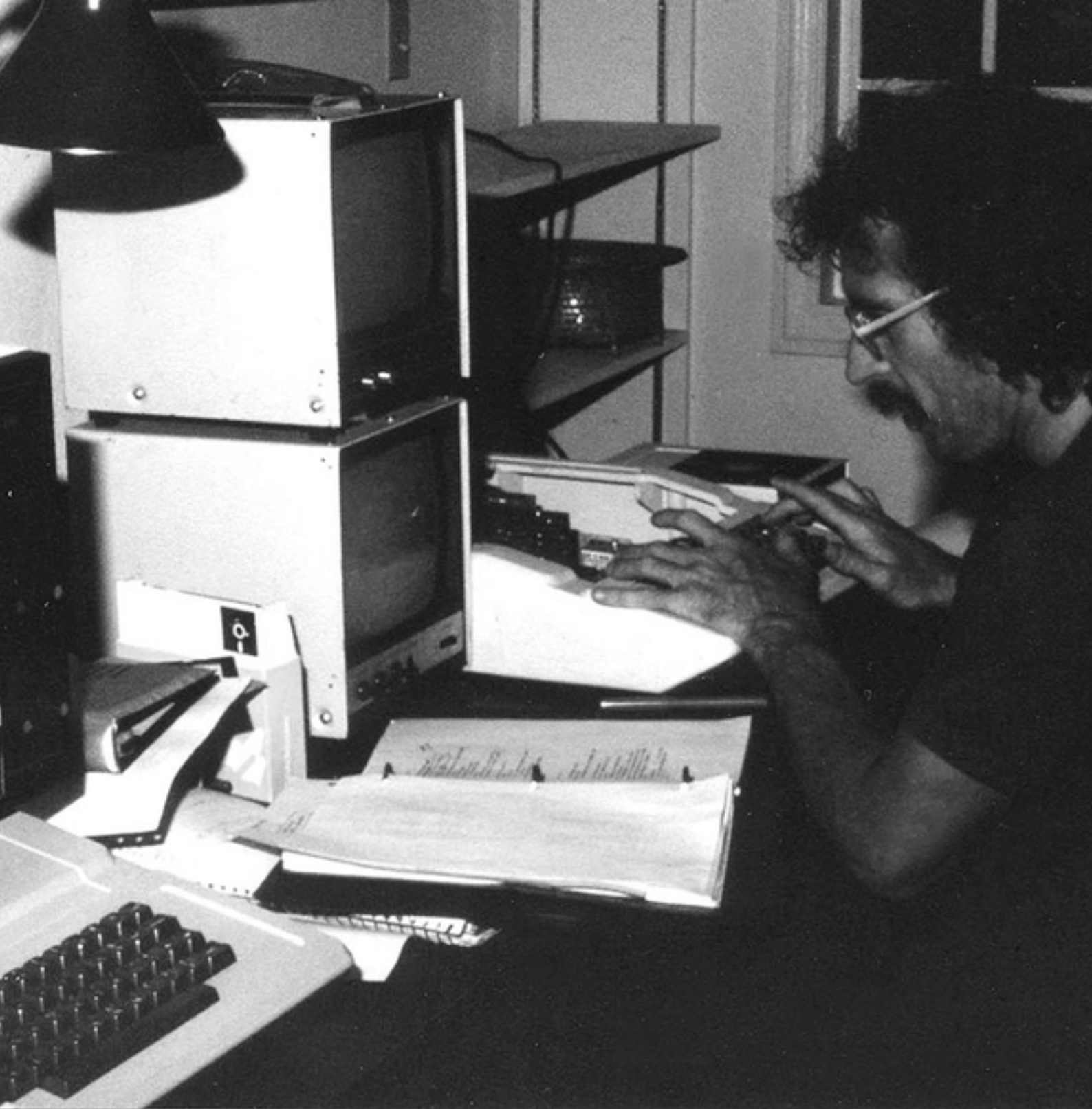
I could here go into a considerable list of the innovations Draper can claim credit for, and it would eat up considerable word count, but a simple retelling of the book itself is not the purpose of this review. Suffice it to say that he, more than any other human being alive today, could be considered the epicenter of the online world. He stands, certainly, in the pantheon of hackers, head and shoulders above anyone else who ever got caught and had their exploits exploited in print.

Or, rather, he carries the giant shoulders upon which all the great technological genius playboys of our time stand. Literally. With a bodybuilder's physique and a homeless surfer's fashion sense, he is a nerd out of his own time in more ways than one.

However, the type of genius that allows one to operate on Draper's level does not translate into easy reading for the lay reader. Thankfully, the book is not simply an uninterrupted block of Draper's own screeds but rather something of a collage — assembled by a close friend — of narratives from different people who have known Draper, interspersed with a lot of hard-core Draper. I say "hard-core," having studied analog electronics in university and having worked as a tech journalist for twenty years patiently explaining amazing technical innovations to people who refuse to read anything over a grade-five level

**Draper
does not
embrace such
limitations,
especially
when bragging
about how
he constantly
improved upon
everything
Apple co-
founder Steve
'Woz' Wozniak
designed.**

Draper presumes that the reader must know as much as he does about electrical circuit design, or at least as much as Woz does, and simply writes it out precisely as he thinks it. Given my background, I found it both refreshing and also impenetrable. Some sections would have benefited greatly (from a readability point of view) by the inclusion of actual diagrams, as the concepts being communicated are quite abstruse.



Watching his friend's dad's RV's wiring disintegrate in a nuclear flash had more than just a painful physiological effect on Draper. It also caused his thinking to evolve.

The EMP effect was completely unknown to the public at the time, and the event seems to have infected Draper's young mind. His brother relates that Draper would beg, borrow, and steal all the batteries he could (as they were quite expensive at the time, especially for young boys) and then short them out with bits of wire, causing the wires to smolder and burn.

This seems a direct antecedent of the wire burning he experienced inside the EMP zone. His fascination with electricity would drive him into the arms of the Army, where he would specialize in radar maintenance and

live out his martial tenure in Alaska and at other radar-dependent installations in the USA.

Victims of "Montauk Boy" programming mention exposure to high-power radar effects as one of the conditioning tools used by the CIA (Montauk is a radar station in New York), but the book's discussions of radar base life seem the complete opposite of that stochastic terrorism: total boredom.

However, all that happened in the ancient past, and the point of this review is to critique the book through a thoroughly modern lens in light of the #metoo movement, specifically a recent article by BuzzFeed's Kevin Collier.

The article alleges that Draper uses hacker conventions to prey on young men (and implies boys, but doesn't

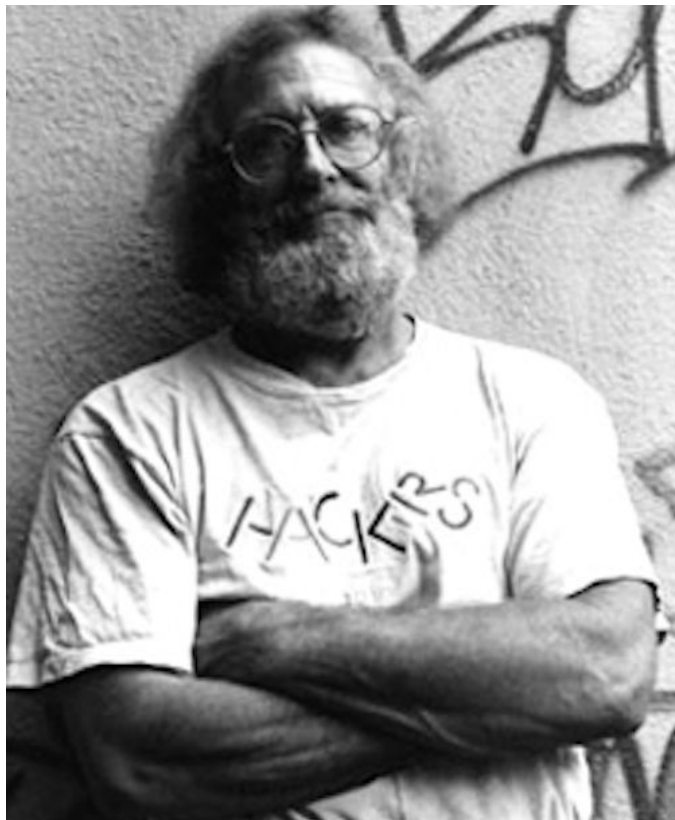




cybercrime never
looked so good

asymmetric
apparel

ransomwear-1337.teemill.com



support that implication with any evidence.)

It caused quite a sensation in the hacker community when it was published, with several hacker conventions agreeing to ban Draper, apparently at the behest of the reporter and innuendo alone, and it just happened to come out two weeks prior to the Kickstarter™ campaign funding the publication of Draper's book.

Immediately after bringing up Harvey Weinstein (a rapist) and Roy Moore (a pedophile), the article asserts that "Draper's actions were well known to at least a core of people who had regular contact with him." In a sense, this is true.

My own relationship with Draper began less than a month before the article was published.

As the new administrator of the Facebook group Phrack Magazine, I was responsible for quintupling membership in this hacking-adjacent space over the course of about two months. I accomplished this by inviting several guest moderators, including infamous hacker jailbird Barret Brown, "Godwin's Law" coiner Mike Godwin, and, when a friend introduced me, John (Captain Crunch) Draper.

Needless to say, his appointment was a huge coup for Phrack and its readers. Draper is responsible for, if not inventing, at least popularizing phreaking, and Phreaking (along with Hacking and Anarchy) is one element of the foundational triumvirate of verticals constituting Phrack Magazine.

Although the magazine is old — dating back to 1985 — Draper is much, much older. The original article about him, which he considers the root of many of his current problems, was published by Esquire in 1971.

Prior to working with him at Phrack, the contents of that article were really all I knew about him.

Once I announced his place on the moderation team, I received the following messages from a former Phrack Magazine editor and member of the moderation group:

That was the only warning that I, as a member of the community working with Draper, received, and I filed it with all the other unsubstantiated rumors I hear as a tech lifestyle reporter. It's true that I was bedazzled by the glamor of his celebrity, as he was, in a sense, someone who I had modeled my whole life after. I had a massive pre-existing mental image of him, as evidenced by a conversation I had with an old hacking friend from my youth at the time:

As this was before the BuzzFeed article, the sexual allegations didn't even register in my perception of him. I want to like him. Without this guy, there would be no Apple™, and he has the same damn problems with their crummy touch screens I do. I thought it was hilarious.

The BuzzFeed article delved into Draper's relationship with Apple™, stating that Apple cofounder Steve Wozniak told them that Steve Jobs once told him that Draper asked Jobs to sit on Draper's back, and this was "out of the ordinary," although it's unclear if that quote is Woz's take on the incident, or Jobs' take, as the quotation is tightly-cut and illegibly placed in a sentence referring to both men.

The article states that "In 1971, Draper showed his design to two fans, Jobs and Wozniak, who, with Draper's blessing, began selling an improved version. As Jobs said in 1994, the product was integral to the company. "I don't think there would have ever been an Apple Computer had there not been blue boxing."

This statement handily imputes, via the unimpeachable words of a dead man, that Draper was the "third partner" in the nascent Apple™ corporation, providing wisdom and inspiration for the tech behemoth. In truth, the two Steves did not have his blessing when they began selling a device based on his design. If BuzzFeed had bothered to ask Woz about that, he could have told them about it, as he does in the forward Draper's book:

Eventually, Jobs suggested selling Blue Boxes in the dorms at Berkeley, and we did this a lot. I kind of regret this because I helped others cheat Ma Bell. I took care to always pay for my own long-distance calls, and to only use the Blue Box to explore the phone system. For example, I could connect to a London operator and convince her that I was a New York test board operator and get her to connect me, via satellite, to Tokyo. Then I'd have the Tokyo operator route my call to the phone in the next dorm room and when you spoke in one phone, you'd hear it a second later in the other.

Draper also recounts this meeting and the ensuing chicanery on the part of Jobs later in the book. The two college boys, inspired by the Esquire article about him, had managed to reach him by calling a radio station where he worked and had invited him to come see their own Blue Box that they had built based on information in the article and from Bell technical documents. Draper takes up the tale here after teaching them how to build a proper analog box, dismissing Woz's digital prototype as unsafe to use:

I was adamant that they understood the importance of reducing failed call attempts when using Woz's

box. These attempts also dropped trouble cards at the switching equipment, identifying the bad trunk's location and the call's origin. Enough of these will cause unwanted attention and it could take as little as fifteen to thirty minutes to identify where the call was coming from. It was a dangerous game to play and could lead to some serious visits from federal agents.

Don't get me wrong, Woz was cautious in his own way. He had even jumpered his phone to another line on campus as a precaution against being located. After I explained all of my concerns to him, he said, "I want to make an overseas call, but I don't know who to call." After thinking for a moment, he said, "I want to call the pope."

I said, "Okay, why not? I don't see any reason why you would want to call him, but I guess you have your own reasons."

After about five tries or so, we were able to get the Vatican online and eventually were connected to an English-speaking member of the Vatican staff. He said the pope was sleeping and unavailable, as it was four-thirty a.m. in Rome. I handed the phone to Woz, who said, "This is Henry Kissinger, I must speak with the pope and I want to confess immediately for all my sins." Even though Woz was very insistent and somewhat convincing, they refused to wake up the pope. He really cracked me up, and we instantly became lifelong friends.

We laughed hard afterwards, but I felt it necessary to emphasize again my warning about the quality of the tones his Blue Box generated. He assured me that he was not interested in using the box to make free long-distance calls, but was more interested in the technology and novelty of it. Steve Jobs sat listening and watching.

Woz didn't give me any indication that they were going to build and sell them, but Jobs, being the entrepreneur of the bunch, had his mind firmly focused on the possible profits.

When I next met up with them and they told me their plans, I was totally against the idea, especially with the issues their box had. Woz thought I was being overly paranoid, but after a few months, I think he realized I had good reasons for taking so many precautions. Although he heeded my warnings to a degree, they ended up selling them to people not completely clued in to the situation, and hence a few of them were eventually caught.

I was furious about the whole debacle, but it pretty much changed history. They were selling Blue Boxes for about \$150 each, and not only did the profits help put them through college, some of the money was used to make twenty-five PC boards for the first personal computer ever made, the Apple I.

Draper, far older and wiser at the time, claims he was far more serious about not selling illegal devices. The book documents, at some great length, how he had been hounded by state, municipal, and federal cops for his tech aptitude and unconventional lifestyle, especially after the international attention that Esquire called down upon his quasi-legal pursuits. He'd already been to jail twice at that point, and his stays had not been good for him. Draper states that:

It all started when this guy, "Al Gilbertson" (let's stick

with his Esquire article pseudonym), got popped using a homemade Blue Box. He was making them and selling them to organized criminals. Bookmakers mostly. There were basically two ways of using the box to access an internal trunk call. One was safe and one wasn't. You can probably guess what happened.

My phreaker friends knew how Gilbertson had messed up and one of them somehow got his phone number. Wanting to be helpful, one friend called him to explain how he'd made a stupid error and what he should have done. Gilbertson didn't take it too well, and was somewhat bitter about being busted. He happened to know a certain Esquire journalist named Ron Rosenbaum, and with the intention of getting back at the phone company for busting him, he wanted to get blue-boxing information out to the public.

Obviously, Rosenbaum wouldn't be able to give the exact frequencies without having the phone company sue Esquire, but everything else would be laid out on a silver platter for any would-be phreakers to take advantage.

The news came to me that Rosenbaum was in the process of writing an article about phone phreaking. I had his number, so I called him and asked about this article, and who he had talked to so far. It turns out the blind kids had met him on a conference party line and gave him the whole spiel. They juiced me up as this superhero because I had built my own Blue Box.

A lot of what Ron Rosenbaum wrote depicted me as an underground hero, driving around in my VW bus, sneaking a cable out of my car and zapping calls all over the world. I actually didn't do that very often. Other lore told by the blind kids included me tapping my girlfriend's line to find out if she was true to me. This wasn't entirely true, as my philosophy was to never violate personal privacy—unless I heard the authorities were onto me.

This incongruent fame would haunt Draper from 1971 until this very day, as the same article introduced each new generation of phreaks and hackers to the mythos of Captain Crunch, and as successive rounds of incarceration for petty IP and telephony crimes would exact their vengeance on his ever-more-frail body. By the time he landed in the privileged confines of the Steves' dorm room, he had already had the shit kicked out of him by the system. To whit:

I was transferred from Stroudsburg to Northampton County Prison in Easton, Pennsylvania. There were some pretty nasty people in there and I had to survive, so when asked for some information on how to manipulate the phone company, I gave them a few of the WATS extenders [free phone-call numbers] just to get them off my back. That didn't work out too well, however, after they discovered all the codes had been changed, and a few of their buddies got busted using Blue Boxes. They took it out on me with a baseball bat in the yard, and did some long-lasting damage to my knees and lower back.

After I got out of the infirmary, they put me in isolation, which was fine with me. It kept the thugs off my back while I was preparing my case and corresponding with my yippie friends through an attorney.

The injuries to my back and knees never really healed properly. I still suffer from them today. There was little

to no medical services in Northampton, and if you had a toothache, they would just pull the teeth. I asked for an x-ray for my knee and lower back and never got it. I complained to my attorney, but with the money he was being paid, he had little incentive to mention my physical mistreatment in court.

Since I was in isolation for so long, I never had the opportunity to go out in the yard, but there were no exercise opportunities like in Lompoc [another prison] anyway. The prison guards figured they had better control over the prisoners if they didn't get the chance to pump iron. Instead, they got out their aggression fighting each other. It was a zoo, and I never saw the light of day.W

I guess I was still one of the lucky ones, since due to my disability, they didn't assign me any jobs, and since I was in there awaiting trial, and wasn't considered a permanent inmate, I was allowed to have a black and white TV in my cell, which Andy had brought in. My attorney worked out a deal where I could walk around the tiers when the others were in the yard, but the weather was cold and damp, and my back hurt constantly.

It really didn't get better at all until I was allowed back in the general population and met a guy who had been a personal trainer. He helped me get the strength back in my legs at least.

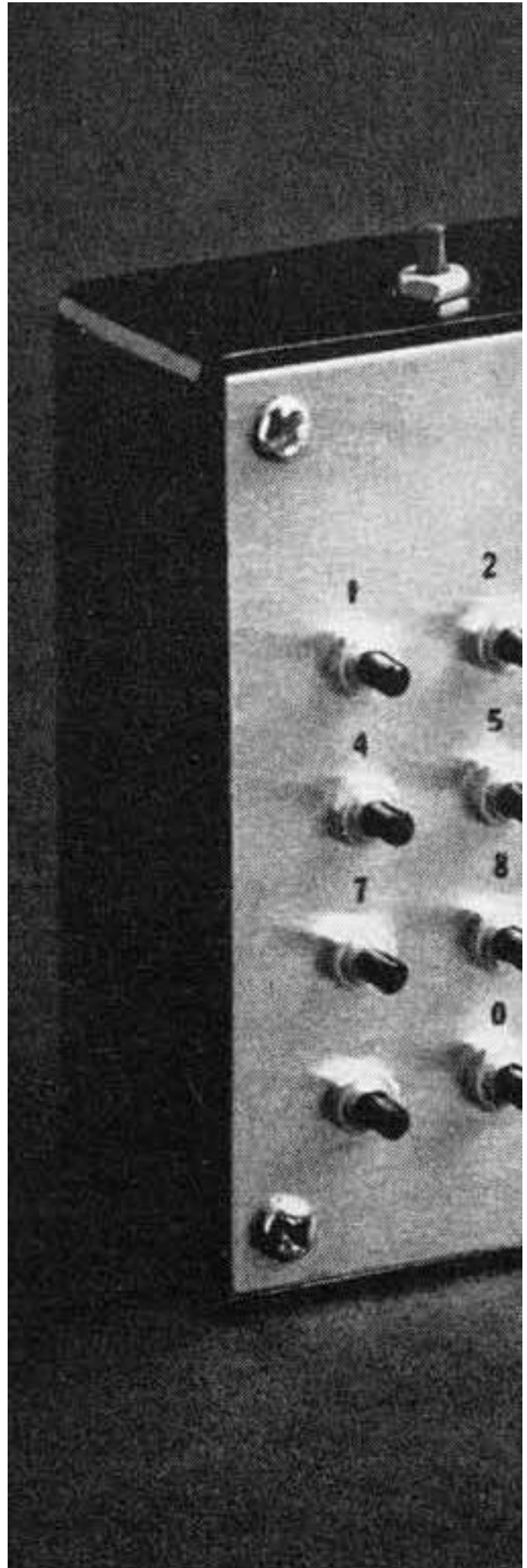
Now, this is significant, because it's the only place in the book (which is narrated by Draper's friend Craig Wilson Fraser) where Draper speaks personally about the "energy blockage removal exercises" that are the core of the Buzzfeed piece. Fraser, however, goes into them a little more.

As my weekly visits to Mill Valley [Draper's Home] continued, I started noticing things about being with John. Several times, I noticed a policeman looking toward us from a distance, and I always had this feeling that John's well-meaning but intense energy was attracting more attention than I had ever felt.

His intense energy was also misconstrued by many people over the years, when it came to certain exercise techniques he liked to share. Back in the 1990s, and apparently long before that, almost everyone who talked to John for more than five minutes would be told that he could "increase their physical strength by ten to twenty per cent." The demographic of people who talk to John for longer than five minutes being mostly nerdy males who have scarcely seen a locker room.

The exercise techniques, which he loosely called "energy blockage removal," were shown to him by a sports physiotherapist with an affiliation to the San Francisco 49ers, and consisted of muscle stimulation using applied kinesiology, interspersed with traditional exercises such as squats and push-ups. These were done while carrying John, literally, and him militarily barking out orders to focus on other body movements rather than on the strain of the working muscle. It was a very odd experience, but helped me gain some strength. I repeated it multiple times in the first year of knowing John, and still use similar techniques on myself when exercising.

John may have had some selfish reasons for so avidly pursuing it with folks, as the relief he got from being lifted that way would ease his chronic back pain for at least a day, and also, as with most people, he needs to



feel valued. So, yeah, he pretty much suggested it to everyone he met.

Scores of individuals I've talked to gained enough from his routine to make it palatable and continued. Dozens of others tried it once and thought nothing of it, but a handful felt physically wrecked by the experience. He wasn't light.

A few even said they felt infringed upon, but I can't help thinking those people were more embarrassed by the surfacing of their own fears of intimacy, or that they felt conned somehow by John's alluring claims. I get it. He can come off as creepy or at least weirdly intense, he's not the cleanest-smelling guy on the block, and the noises of relief he makes during the exercise sound pretty primal. He also has a limited, childlike perspective when it comes to reading the discomfort or signals of others. The first time I tried it, my drug-fueled paranoia went through the roof that it was about to turn sexual in some way, but of course nothing of that nature ever occurred. Over the years I've shared humorous anecdotes with many others who had the same initially paranoid experience, but there are also a few who said they were so "creeped out" by him (or their own paranoia), that they "fled for their lives."

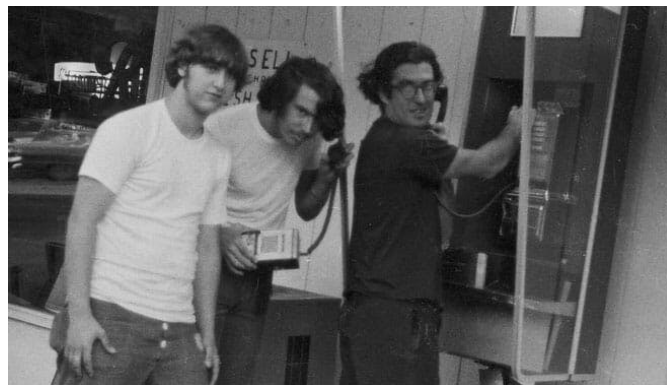
I would suggest those few individuals might have been unable or unwilling to work through their own personal issues of physical contact with another male, and chose to interpret and relay the experience in a nefarious way to save themselves tackling their own inner demons. It's a pity. Those unfavorable stories and misunderstandings have created much rumormongering and negative cognitive bias in certain circles, and unfortunately John's reputation suffers to this day.

Fraser repeatedly mentions Draper's back pain throughout the book, as it appears to be a source of many anecdotes:

After having a valet begrudgingly park the dirty Toyota, we made our way to the buffet, only to find huge lines of tourists with the same idea. What happened next was the first time I saw John at his fantastically shameless best. On seeing the lines of people, he immediately marched up to a courtesy phone, picked it up and bellowed, "I can't wait in this line! I have a bad back! How can I be expected to wait here?" The rest of us stood there in astonishment. It was beyond embarrassing. Actually, it was so far beyond that I didn't feel anything. We all just silently followed John and the manager, who had instantly appeared. He took us to the front of the line apologetically and bowed off. I thought he was going to give us free passes too, but no such luck. John started piling soft food on his plate with a sly smile. He had hacked the casino buffet.

Draper peppers the text with anecdotes about his own back pain as well, such as "I wanted to get down to Ciudad Juarez in Mexico to visit a pharmacy for some back-pain medications" and "After a few days into the work, my old lower-back injury flare up worse than ever, and I had to use a wheelchair for the last few days of our week in Bangkok."

Fraser also includes two narrative sections from one other source that relate to the exercises. The following lengthy quotation is from Noble Ape author Tom Barbalet and relates his own experience of Draper's first visit to Australia. I have decided to post it in full (instead of



truncating it with ellipses at the behest of my editor) because it captures the outsider awe surrounding Draper so completely and mentions him often enough that cutting out the few sentences not about him seems more likely to increase confusion than decrease it. It is a fine distillate of the book's entire 150-page narrative: :

I had just started university and for a curious set of reasons, I was living on campus at the Australian National University in Canberra, Australia, in a dorm house run by nuns. You have to understand that in 1995, the Internet was really new and there were no photos of Crunch online. In fact, for the longest time, my photos and interview were the only internet-age documentation of him. I became a source and was periodically contacted by journalists to use my photographs and talk to me about Crunch. There were at least three book projects that were pitched to me about him.

For me, Crunch was the person in technology I had to meet. The Esquire article on his work redefined my life. I found it on a friend's Amiga in the Jolly Roger set of text files. I remember printing it out on an old dot-matrix printer at age thirteen and binding it with string. I carried it around with me for months until the paper became detached from the string. The Crunch of the Esquire article represented the Robin Hood or Peter Pan of technology. He embodied the kinds of technical improvements of large engineering systems that required mischief to explore and understand. That was a boyhood me in Australia. Crunch was my tech hero.

In 1995, even though I was only eighteen at the time, I had written a novel about the Australian technology underground, *Field of Chaos*, and I was fascinated to see how Crunch fitted in with the local tech community. There was some discussion with him and others about holding a rave in his honor in Canberra. Although I had never put on a rave, I knew a number of DJs and promoters and had floated the idea with them for a pretty flat response. Crunch had linked up with a group called *Clan Analogue* in Sydney, who I knew and who had created some curious wah-wah dance music. While I was still planning the rave in honor of Crunch, I asked him to leave a voicemail, which years later, I can still recite verbatim:

"The Crunchman here. The man on a mission. And the mission is to spread as much love and energy as I possibly can: that's my mission. So come check me out at the next rave. And I'm looking forward to raving my ass off!"

Crunch arrived at my dorms with a lanky fellow and a guy who claimed to be a hash smuggler from the Emerald Triangle (Thailand, Laos, and Cambodia).

Crunch immediately wanted a hot breakfast. Thankfully, the dorms served pancakes on the weekend and John went back for seconds, thirds, and fourths. I had a small crew as well.

Crunch being in town had drawn a few of my friends together. After the pancakes, he had one driving purpose: to perform his energy-blockage removal on me and many of my friends. The energy blockage removals turned out to be an introduction to Crunch that appears to have occurred with many. For me it was about an hour of doing pushups, squats, and stretches with Crunch hanging on my back the entire time. Not figuratively hanging on my back, but literally hanging on my back like some kind of counter-culture Yoda barking commands and making comments about various physical attributes I had.

The whole process left me a little stunned and I infamously noted to a friend following my experience that it was “invigorating” before Crunch performed the same technique on my friend.

Crunch at the time said he didn’t sleep. This was a big part of his general rap. He had apparently elevated himself to a higher level of consciousness while the rest of us schmucks were locked into six to eight hours per night. Not the Crunchman.

He spent two days with me that visit and while there were a number of unique experiences through that time, one that I found completely unexplainable was somewhere through the first day when he and his posse went into the center of Canberra with one instruction: do not bring back a particular hacker. Do anything with your adventures but please don’t return with one hacker who had been particularly troublesome and had called in death threats on my mother and young brothers. My mother was a formal woman but had splendidly once picked up the phone after only a couple of rings and told this individual in no uncertain terms to fuck off.

Canberra at the time had a population of 250,000. This troublesome hacker had an unlisted number. Within two hours, Crunch and his posse had returned with this one hacker. He was gushing greatly that I had sent out Crunch looking for him and thanked me for making sure that Crunch found him. I had no problems recommending the energy-blockage removal technique.

By the second day, the effects of the energy blockage removal was leaving me the little worse for wear and I left Crunch with a friend of mine to go and find some world-renowned Canberra cannabis. The difficulty in finding cannabis on a university campus is a constant of nature in the order of seconds. I guess I was happy for any kind of break. After lying down for about ten minutes, I was drawn to loud screams coming from a public open-air space in the dorms. Crunch was curled in a fetal position screaming at the top of his lungs that he had been poisoned, as someone had spiked his cannabis with the dreaded tobacco. As I was walking down some stairs to see the commotion, one of the nuns coming up the stairs told me in no uncertain terms that Crunch needed to go. After the fact, I heard accounts of Crunch offering blotter paper to anyone interested including, it would seem, the nuns.

Crunch was sent on his way with his posse to find another place to stay. This seemed to be relatively common for Crunch’s first visits. Two things of note

occurred afterwards. First, the energy-blockage removal technique provided a lactic acid build up that rendered both me and my friend paralyzed after three days, which was interesting. Second, as he no longer slept, I received a couple of calls from Crunch asking after a pair of shorts he left behind at roughly three a.m. and four a.m., respectively, over the following week. I had washed the shorts and was wondering what I should do with the artifacts. Even after a wash, they still had a smell that reminded me of the energy-blockage removal work only a few days earlier. It turns out that Crunch had sewn the blotter paper into the shorts. After the wash, the shorts were less important.

Aside from Clan Analogue, Crunch also traveled to Adelaide for some time. I was born in Adelaide and traveled there at least once a year to visit my family. Through these visits, I also befriended people in the tech community in Adelaide as there was substantial overlap with the rave community. I remember getting an Adelaide rave video a few months after Crunch returned to the US to see some historical filming of him. The video featured three or so raves. Moving through the dancers, Crunch appeared within the crowds of a couple of raves. He was always dancing in his own space. When the camera came near, a large toothless grin crept across his face. He seemed a little out of place within the mass of teenagers and twenty-somethings, but he had his own style. Crunch’s intense energy was pretty far removed from the relaxed technology scene in Australia. He surfed a number of couches through his time in Australia and spent a bit of time staying in the notorious Kings Cross section of Sydney. Many found his intensity exhausting.

A community formed of people with whom Crunch had stayed. They exchanged information about their pet cats that were never quite right again and countless accounts of energy-blockage work. Although I was unable to attend, I was invited to a large party that was held in Sydney shortly after Crunch left Australia. People came together to tell their stories of the Crunchman and the message he bought from the San Francisco Bay Area.

Drugs, as you might imagine, play a large role in this book. So if you like biography with open drug references, this might just be the book for you. According to Fraser, “John has a nickname for getting high, which nobody ever understands: ‘Executing a 9N instruction.’ 9N is machine code on the 8800 microprocessor for ‘get high resistance pair.’”

Babalet(’s blog) is also quoted later in the book, describing another interaction with Draper, this time in Las Vegas, and years later, and again mentioning the energy blockage techniques:

We went out for a meal at Denny’s with Crunch’s new friend, Trevor. A really nice fellow who at twenty-two was already an Iraq vet. When Crunch went to the restroom, Trevor noted Crunch had done one of his back stretches within about five minutes of meeting him. Ah, *deja vu*. I had injured my back, so when Crunch requested a back stretch, I wasn’t able to accommodate.

And that’s it. There’s no other mention of the energy blockage technique in the book, no mention of any of the accusers, or further explanation of the exercise technique. The position of the author(s) is that this is not a big deal, just a palliative health procedure that Draper adopted in order to regain use of his legs after a severe

prison beating, and one that's been widely misconstrued as sexual by people who are a lot less old and wise than him.

Clearly, he is a celebrity, and, as such, one could argue that he has a certain power (glamor?) that attracts young hackers who are thirsty for illicit knowledge and elite associations. He admittedly uses that power to attempt to convince them to spend an hour doing hard exercises with him hanging half-naked and half-erect from their backs. This is, without question, odd.

Should you read his book? Hopefully, I've presented enough information for you to know by now. If you are just interested in any salacious details pertaining to the sexual assault allegations against him that it may contain, well, you needn't bother. They're all right here. If, however, you are interested in understanding the mind of the only Atomic-age internet (anti)Hero, you could do worse than to imbibe Captain Crunch's tall tale.

A massive thank you to
Owen Ferguson of
Phrack Magazine
for providing this article.

PHRACK issue 71
is out now and a call for
papers for issue 72
has begun.

For more details visit
<https://phrack.org/>





the security chameleon



From the desk of ...well...the security chameleon

In the last two decades, the world has shifted from clunky dial up connections to a constant, hyper-connected reality. This hyper-connected world is fuelled by paradox, our organisations deploying their technology shields, failing to realise that the technology itself is being weaponised against them. Attackers, defenders and political powers are locked in a constant struggle for dominance, in this unforgiving environment the one thing I have learned is that natural selection reigns supreme, only the most adaptable businesses and individuals will survive.

Landing a role in this highly complex domain is not easy but this shouldn't deter non-technical people pursuing a career in cyber security. However, to survive in such a volatile, uncertain, complex and ambiguous industry you need to build personal and professional skills to constantly evolve.

This article is less about the survival of businesses this is an aide memoire, based on my own experiences, of the skillsets I think you need to succeed in your chosen career path.

Welcome to the world of The Security Chameleon

As a kid I loved to read choose your own adventure books, if you have seen Bandersnatch on Netflix its a similar concept. You as the reader get to choose the fate of the hero in the story, but be warned not every path has a pot of gold at the end of the rainbow.

I could hide behind an Instagram story headline, CISO in 3 years, no degree, no cyber certs, I could talk about the universe or some other worldly being choosing my destiny and landing my first cyber gig but if you spun

the camera around and started to peel back the digital mask you would see an alternative reality. I had served fourteen years in surveillance and reconnaissance as an electronics engineer in the British Royal Air Force, six years as a senior network engineer and a year or two as a solutions architect. I'd experienced operationally intense situations, even in the Air Force, before you Army fanboys kick off, and this diverse work experience in technical commercial fields put me into a niche pool, just like Liam Neeson, I had a unique set of skills.

In 2017 I was working for a large US based managed cloud services company and life was good, I had outgrown my network engineering role and decided to explore new internal opportunities and I was travelling a path as a solutions architect, that was until the senior management bandits decided to lay off all our managers. It was a bold but brutal move by the business, we felt we had built a successful team in the UK but we were blindsided by this executive decision. Our team of eight was now a team of three leaderless souls. This was a dilemma, should I stay and ride out the storm or should I take a risk and look for work elsewhere. What would I do, I had been hands off keyboard for a year, my skills had faded but not disappeared, I felt anxious about trying to secure an external role but I knew deep down I didn't want to risk completely deskilling as current position as a solutions architect was also in jeopardy. I knew I would never reach my goal if I didn't take a leap of faith and jump, the trouble was I didn't have a goal in mind.

In the military I moved roles and countries a lot, it comes with the territory, I like to think that I had a hand in socially engineering my postings by befriending the HR teams but in reality the forces had a bigger agenda and my adventure was already mapped out. Throughout my

adventures I crafted the ability to pay close attention to detail and notice subtle changes in my environment. In fact this was a trait I had developed since being a young child, like a chameleon I would observe my peers and try my hardest to blend in to my surroundings. This wasn't always safe, smart or legal but I would adapt my persona and actions to match the environment to ensure I fitted in. Through painful life lessons I learned that changing who you are or your core beliefs is the worst thing you can do it literally ends in tears and this is not the advice I am touting.

Lets go back to my moral dilemma from earlier should I stay or go, what would you have done?

Having a plan B had been engrained into me so as the news of lay offs came out I was already scouring the job boards looking for my next role. Solutions Architecture was out of reach due to my lack of tenure in the field, I knew I didn't want to go back to sitting in a NOC punching tickets, I had even considered going back to pulling cables in the data centres just to have a simple life but deep down I knew I was destined for greater things and then out of the blue a recruiter called me about a Senior Networking Role that turned out to be the start of my career in cyber security.

At the time I was reading a lot of coaching and self help books, Eric Thomas the Hip Hop preacher was a massive influence, I knew that I could only be successful if I put 110% effort into whatever I wanted to achieve "if you want to succeed as much as you want to breathe" is a classic quote from ET that resonates with me still.

The first role I landed was a regional head of security for an MSSP, with little to no experience at that level. The company wanted a network engineer but realised that the commercial experience I had could be moulded into another position they were hiring for, they took a punt I took a gamble, we exchanged contracts and set of on a new adventure.

I often felt out of my depth, imposter syndrome is real, I felt like I was being thrown into the gladiatorial ring with Maximus Decimus Meridius himself, but a few months later I was leading them through an ISO27001 audit and I realised that I understood more than I gave myself credit for. Observing my surroundings I could see the leaders had great commercial presence, the technical teams were experts in their field, the customer care team were epic I felt like a fraud I started to doubt my ability to do the job, it felt like my camouflage was fading and I feared being caught out. I quickly realised I was delivering value, there was no one else in the business who knew how to do what I was doing, thats why they hired me. The only person I needed to convince was myself. If I didnt know the answer to something I would just roll with it, give myself some breathing space and tell the client, stakeholder or team mate, I'd come back to them after further analysis. This pause for breath made the them believe that they have asked a great question and their nervous system had lit up with dopamine due to the belief they have outsmarted a subject matter expert. More importantly it gave me the time to go away, regroup, stick on the head-

phones playing LoFi beats and research a decent response. There was no need for self doubt, showing your weakness as a security chameleon is like showing your under belly to a hungry hawk. This camouflage is not just a colour change its a psychological armour, a deterrent to those predators who are focused on taking your job.

I felt I had chosen the right path, one eye was on a promising career as a security professional, one was vigilantly scanning the environment for predators, and its a good job I did this because few months into this role one of the leadership bandits let his mask of integrity slip exposing his deceitful personality. We had been delivering a large scale project for a key client rolling out data leakage protection and employee monitoring software and due to his own failings the leader demanded I lie to the client to cover his failings.

I couldn't believe only a few months into the role I had arrived at another crossroads, I had spent months building trust with the client and expanding our commercial agreement. I didn't want to let them down but I also didn't want to piss off my leadership team. This quandry challenged my strong moral code of acting with honesty and fairness, and could potentially jeopardise my future as a security professional. Do I do as the leader asks and cover for him to protect my position and be a team player, do I tell the client the truth and expose the leader?

What would you have done?..be careful as your decision will shape the outcome of this adventure. Until next time...

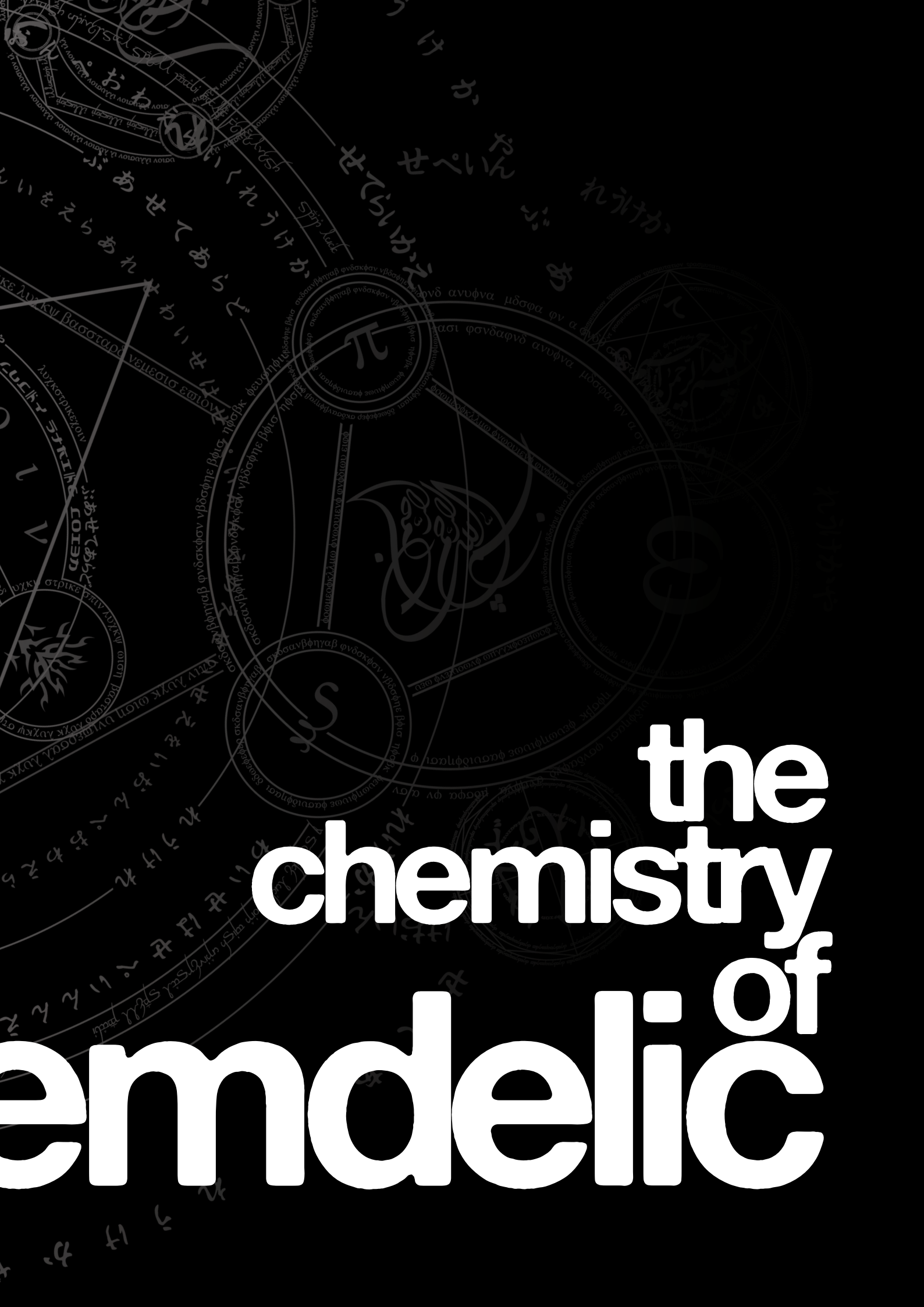


HVA

CK
academic



che



the chemistry of emdelic

Molecules, mentors, and mental health

Originally, he wanted to be a mental health therapist. Classic, right? Fresh out of high school, he's ready to fix the world, mind by mind. But after just three weeks in college, the future blurred. He dropped out. "I became a personal trainer instead," he recalls with a laugh. "I had no idea what I wanted out of life."

That all changed thanks to a psychedelic twist of fate.

"I eventually went back to school, inspired by psychedelics," he explains, eyes lighting up as he speaks about the experiences that shifted his entire trajectory. It wasn't the usual "I saw God" narrative. For him, the revelation was more molecular than metaphysical. "I was amazed by how molecules can influence our minds and bodies, and that fascination led me to pursue chemistry."

His chemistry journey wasn't exactly linear. First steps into the field? Forget your conventional lab coats and pipettes. No, his introduction came via a DMT extraction at 18 or 19—barely out of high school. "I was struggling with my mental health and desperate for answers," he says. That hands-on experience became the kindling for his scientific fire.

"I barely understood what I was doing," he admits, "I didn't even understand the reagents or why the reaction worked. It felt like trying to solve a puzzle without the manual, and that's what drove me to learn more." Like many others, the catalyst for his chemical awakening was none other than Hamilton Morris of Hamilton's Pharmacopeia. "I was captivated by the way he broke down chemical mechanisms and synthesis," he says.

In that spirit of hands-on exploration, he dove headfirst into organic chemistry. "It's like solving puzzles," he explains. "You're given pieces that could go together in a million ways, but only one way works to build what you're after." And for him, that "what" is often psychoactive compounds—the kind that change the way we think, feel, and perceive the world. "I wouldn't say I specialize in anything yet," he's quick to point out, "but I'm definitely focused on organic synthesis right now."

Not Just for Clicks: The Deeper Motivation

It couldn't be more than six months ago that I stumbled across the man who calls himself Chemdelic. Deep down a rabbit whole one evening my adventures led me on an unusual tangent. My research had begun at a Chinese telecommunications company and had somehow landed me smack in the middle of a youtube ecosystem of professional and not so video chemists. Synthesising everything from serotonin to steroids, these clandestine kamikazi share footage and insight with the molecular voyeur masses. This is where something a little different, a little daring and very HVCK caught my attention.

The infamous West Mass Police Dept. "Shake & Bake" demonstration, created to help law enforcement recognise the different phases of a home cook, a technique super popular in that part of the US at that time. What played before me was a reaction video of sorts. A young chemist offering a narrative and deeper explanation of what was happening on screen. While my interest in clandestine chemistry may be minimal, my fascination with those willing to pull back the curtain on what society deems forbidden knowledge is almost obsessive.

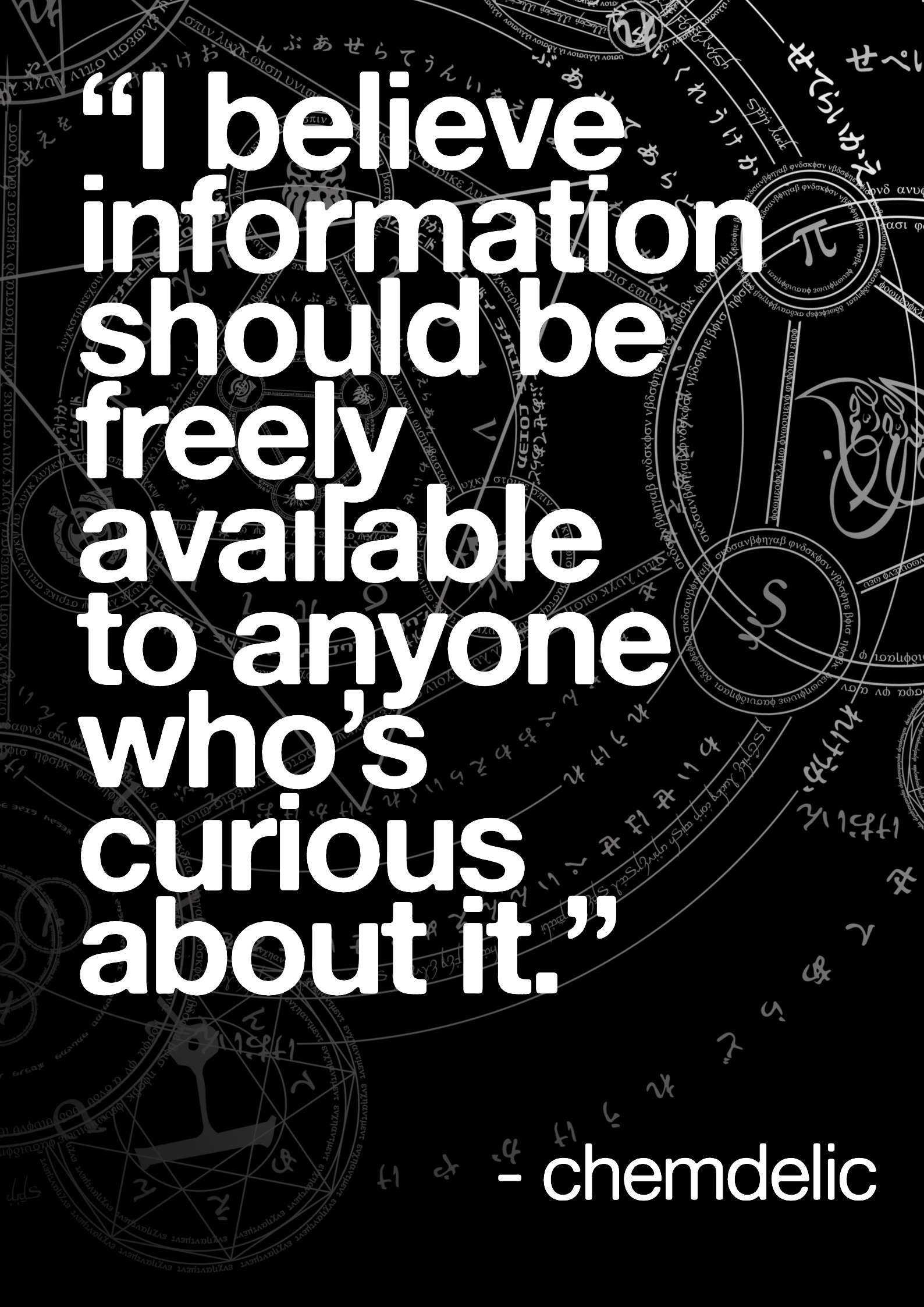
With a YouTube channel that's growing in popularity, it's easy to assume he's just riding the wave for views. But when asked about the frequent focus on controlled precursor chemicals—often flagged by law enforcement—he shrugs off the suggestion that it's a rebellious act. "It's not a middle finger to law enforcement or just for clicks," he says. "I'm genuinely fascinated by these compounds and enjoy trying their synthesis."

"I thought it would be cool to explain and react to the 'Shake & Bake' synthesis," he says nonchalantly, as though he's explaining how to make a cup of coffee. The video hit 80,000 views quickly. Yet, despite the attention, he's not looking to be the "go-to guy for shakers globally," as he chuckles. It was a knowledge drop, pure and simple.

And that's the crux of it. "I believe information should be freely available to anyone who's curious about it." Sure, it's controversial—teaching the masses the nitty-gritty of chemical synthesis—but for him, it's about education and transparency. The risks? They exist. But he's firm in his belief that limiting access isn't the answer.

Shaking the Foundations of Knowledge Access

"We live in a world where fear spreads quicker than facts," he laments. And this is where the line between ethical responsibility and scientific curiosity blurs. He knows full well the dangers of making synthesis knowledge accessible to a broader audience, but that doesn't change his philosophy: open access.

The background is a dark grey collage of various mathematical and scientific elements. It includes several circular diagrams resembling celestial maps or complex geometric constructions. Scattered throughout are various symbols: the Greek letter pi (π), the infinity symbol (∞), the letter S, and the letter L. There are also handwritten-style mathematical expressions and numbers in different scripts, including Greek and Latin. The overall aesthetic is one of intellectual complexity and scientific inquiry.

**“I believe
information
should be
freely
available
to anyone
who’s
curious
about it.”**

- chemdelic

"Yeah, someone could use this knowledge to create a bomb or carry out a chemical attack," he acknowledges. But the flip side? "Someone else could use the same information to develop life-saving medications. It's about intention."

So, what about the public perception of chemistry and chemists? "Probably negative," he says, not missing a beat. "People like to keep things they don't understand regulated. That fear keeps them from exploring."

He's not a nihilist, though. He sees hope in YouTube, forums, and online platforms—places where budding chemists can share and absorb knowledge that might otherwise be locked behind institutional gates. His approach is rooted in community and collaboration, always seeking to share and learn from others in the field.

The Struggles of a Home Chemist

Of course, the life of a home chemist isn't all about intellectual debates on ethics and open access. There are real-world challenges, too—like trying to get your hands on the right reagents without a DEA raid. "In the U.S., if you don't have an LLC or specific licensing, it's nearly impossible to get certain chemicals," he explains. His day-to-day? Scouring forums, learning through trial and error, and finding creative ways to work within those restrictions.

But those obstacles don't slow him down. If anything, they fuel his determination. Chemistry, for him, isn't confined to academic labs or corporate funding. It's an art form, a puzzle, and a passion.

Despite the struggles, he remains optimistic about the future. "When the public becomes more educated, we can advance society in ways that are free and beneficial." But that's not to say there aren't risks. "We need to start by teaching younger generations about unity, positivity, and using knowledge for good."

As for his personal philosophy on sharing knowledge, it hasn't changed much over the years. "Knowledge is a gift," he says with conviction. "It should be shared freely." And with that, he's committed to making chemistry as accessible as possible to those who are willing to learn—and willing to handle the responsibility that comes with it.

Final Thoughts: The Alchemist at Heart

Our conversation wraps up, but his message lingers. He's a chemist, sure—but more than that, he's a philosopher of knowledge, a curious mind that found peace and purpose through chemistry. His work isn't about fame or rebellion. It's about exploring the unknown, sharing what he learns, and, hopefully, inspiring others to do the same.

"Stay hungry for knowledge," he says with a smile, "be open to new perspectives, and enjoy the beauty of chemistry. It's an incredible field with so much to offer." As I leave the interview, it's clear this isn't just someone who mixes chemicals in a kitchen. It's someone who's mixing curiosity with action, molecules with meaning—and he's inviting the world to join him.



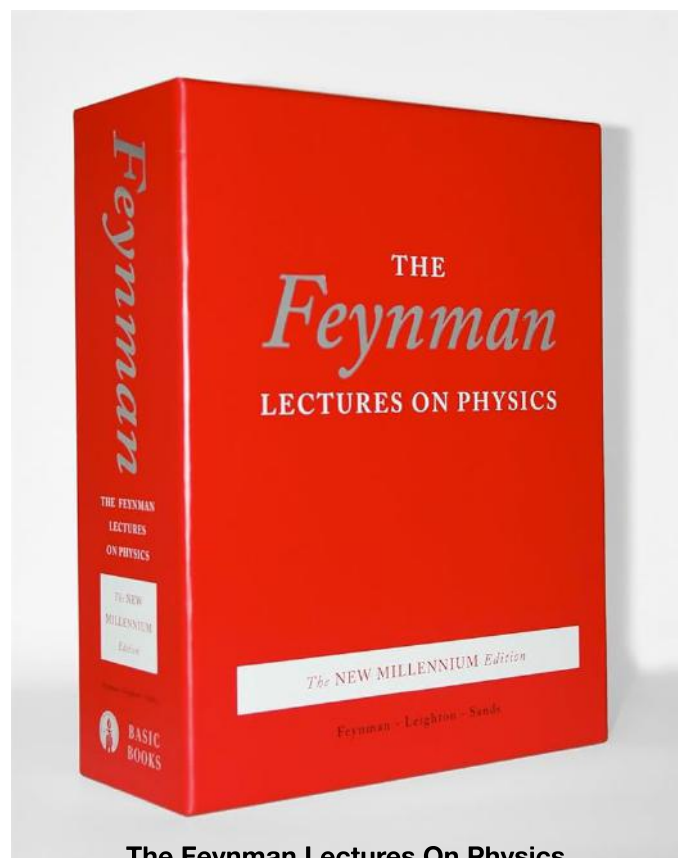


Proving Richard Feynman wrong

For decades I have revered Dr. Richard Feynman. I've seen the Matthew Broderick movie *Infinity* about Feynman's early life with his first wife Arline, who died of tuberculosis on June 16, 1945 in a sanatorium in Albuquerque New Mexico.

Years ago I taught a training class at the Philips plant in Albuquerque, and I brought my wife along so we could spend some time together, as much of my travel around the world didn't lend itself to visits from my wife. We did a lot of things there. We drove up Sandia Crest at 10768 feet above sea level. We drove to Taos to see the town and visit museums, and we drove up to Los Alamos, the site where Richard Feynman and the other scientists of the Manhattan Project worked furiously to develop the atomic bomb to win World War II. It wasn't hard to put ourselves into Feynman's shoes 60 years earlier, and made a permanent impression on both of us.

Yet recently I got the shock of my lifetime: my world came crumbling down after I read a line from the book series *The Feynman Lectures on Physics*



The Feynman Lectures On Physics

A fellow named Michael A. Gottlieb ported the entire three book set to HTML, so you can read it here. In the book in chapter 50 Feynman talks about harmonics, my favorite field of study. I read the whole chapter and found this gem

"The ear is not very sensitive to the relative phases of the harmonics."

By the way, the text from this book series is copyrighted, as well is the body of the webpage

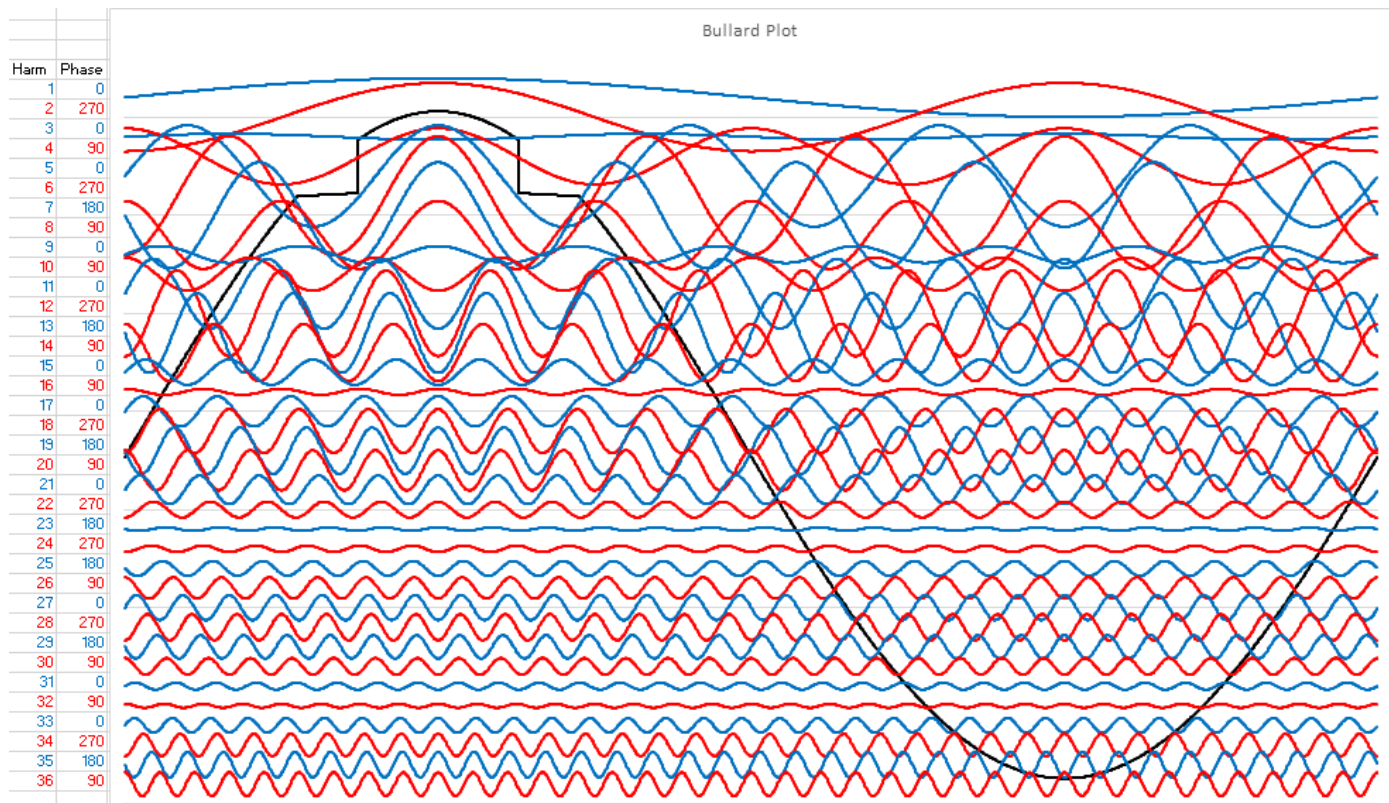
mentioned above, but Mr. Gottlieb gave me permission to use that line in my writings and videos FAIR USE he called it, so I won't argue with him over that.

There is a minor problem with this line from the book, it's wrong. Now, it's not hard to understand why someone without high precision instruments might say something like this, as I have pointed out again and again in these pages and on my numerous videos on the topic, the phases of harmonics created by distortion have only four phases, 0° , 90° , 180° and 270° , that's Bullard Laws of Harmonics #5, and interestingly, as far as the ear is concerned, reciprocal angles such as 0° and 180° or 90° and 270° sound exactly the same, so Feynman's statement has a 50% chance of being right, purely by chance.

As many people who work in electronics will tell you, a spectrum analyzer does not report the phases of the signals it displays, including harmonics, and that is despite the fact that nowadays spectrum analyzers work by leveraging the Fast Fourier Transform, which can report magnitude and phase of the input waveform, and yet most don't! Why not you might ask? Because if you display the phases of every wave the spectrum analyzer captures, it would be worthless. I struggled to understand how to do this for years, and then I hit on a solution: Always capture the fundamental (harmonic #1) coherently that way, all the harmonics will be coherent. Then zero out the phases of all non-harmonic waves, only displaying the phases of the harmonics, like in this Bullard Plot. (Fig.2)

Notice a few things about this plot: The overall signal is black and overwhelms the plot. The fundamental and harmonics are shown much smaller so they all (well, 36 of them) fit in the plot. But on the far left I show the harmonic number and the phase of each harmonic confirming Law #5. Also very important, I color code the harmonics by relationship to the fundamental, blue for ODD harmonics and red for EVEN harmonics.

So how can we prove or disprove Feynman's statement, which has a 50% chance of being right. The answer is a technique that I devised. When I was teaching a class on the STS-3000 Mixed Signal Device tester, someone asked me what roll-off of the Telecom Filter, an option in the STS-3000 actually looked like. Up till that point I had never thought about investigating, but when a student asks you a question, you are rather obliged to figure out an answer, and while I asked everyone who developed the tester, no one actually knew. So I developed a test using noise that I created myself. I had read online that you could create a random noise signal by setting the amplitudes of all the signals to be exactly the same and randomize the phases. I mathematically created a waveform that contained a fundamental of 1KHz with harmonics going all the way to 24KHz, all the same amplitude as the fundamental. I did this in frequency domain so I could then get access to the phases of the harmonics and used a random number generator to randomize the phases. I spliced the magnitudes to the phases, performed an inverse FFT, loaded the time domain wave into the Arbitrary Waveform Generator (AWG) and drove the wave into the Telecom Filter, but bypassed the filter itself to calibrate the input waveform.

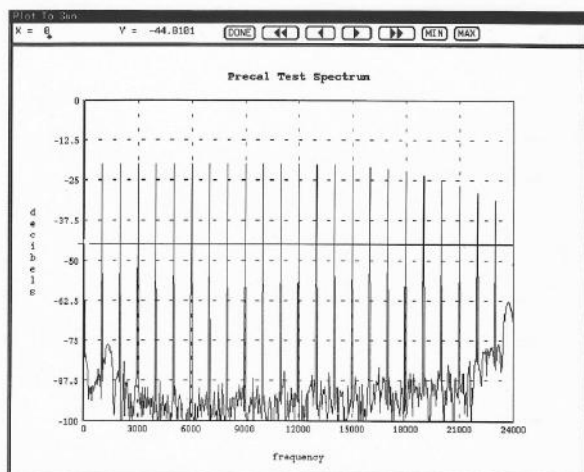


Bullard Plot of a distortion at 66.8°

Example Program: tcfest

TCFTest

Plots

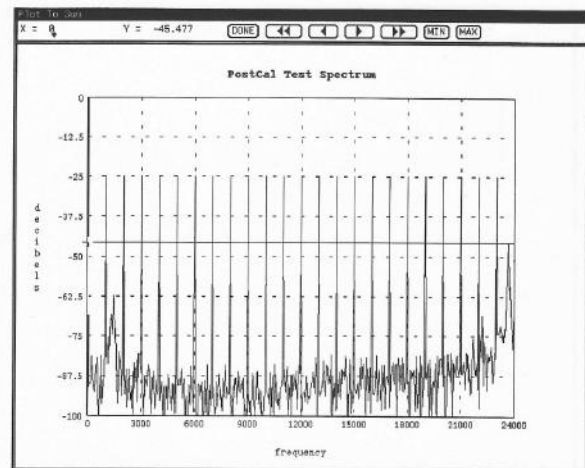


Uncalibrated waveform spectrum

Example Program: tcfest

TCFTest

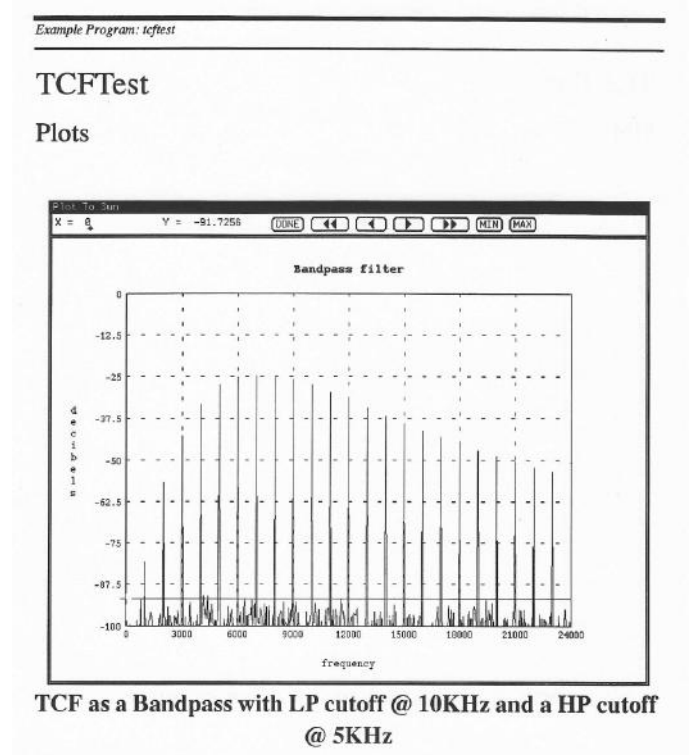
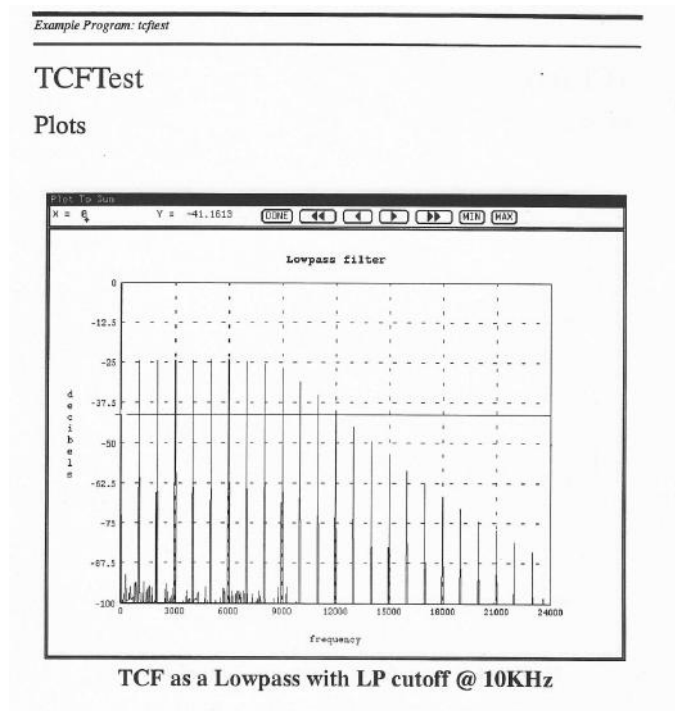
Plots



Calibrated waveform spectrum

I captured the resulting waveform, performed an FFT on it and noted the roll-off (above) of the Telecom Filter, sans filter. Then I took the magnitude array and took the reciprocal of the magnitude (leaving the phase alone) and multiplied that by the frequency domain version of the input wave. I reloaded the AWG, ran the test again and got this:

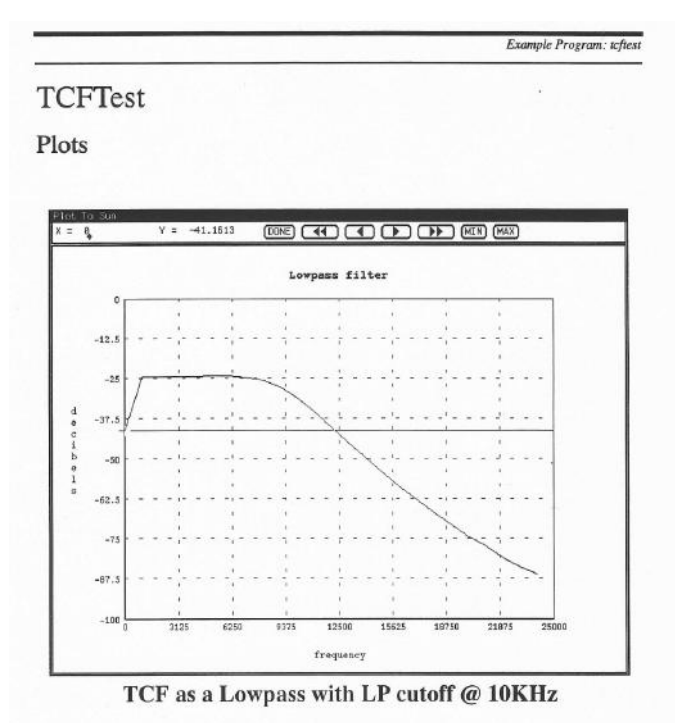
Now that I have a calibrated waveform, I can click in the filter options on the Telecom filter and see what the actual response is. First the Lowpass at 10KHz cutoff:



TCF in Bandpass mode 1

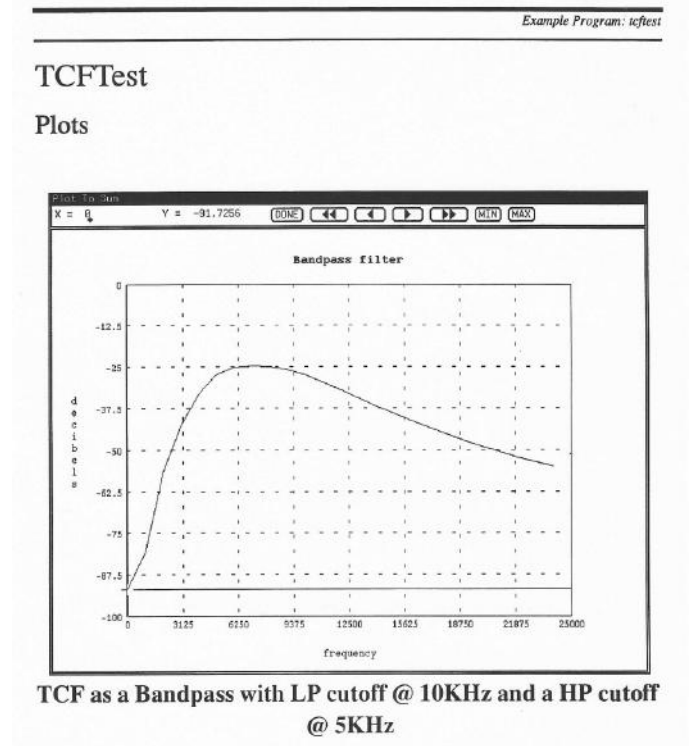
I also used a technique called Decimation to look only at the harmonics, ignoring any noise I might also have captured.

And with decimation it looks like this:



TCF cutoff at 10KHz, decimated

I then tried the TCF in two other modes, a bandpass at 5KHz and 10KHz.



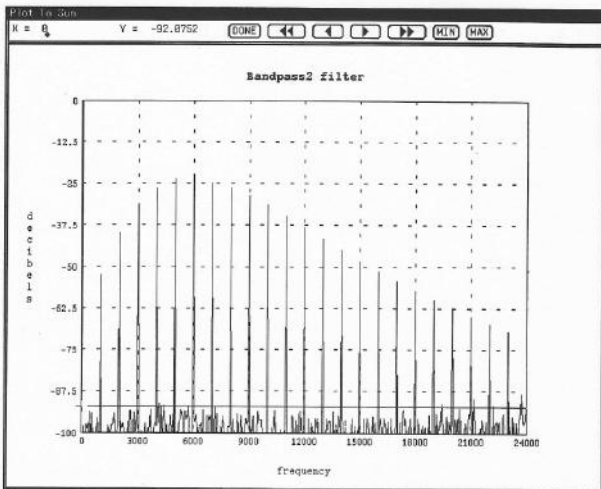
TCF in Bandpass 1

Then I tried Bandpass mode 2 at the same frequencies:

Example Program: tcfest

TCFTest

Plots



TCF as a Bandpass2 with LP cutoff @ 10KHz and a HP cutoff @ 5KHz

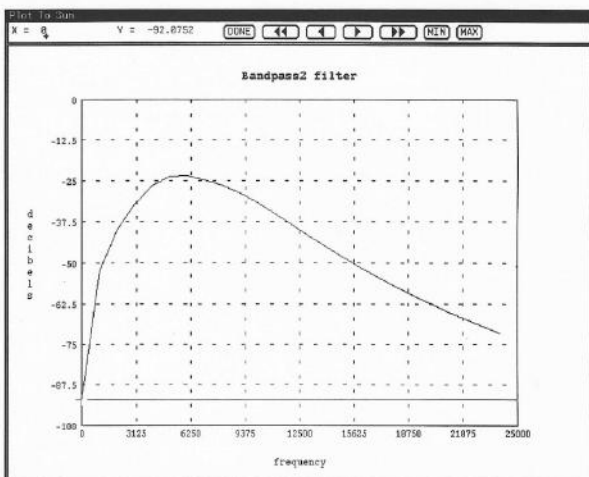
TCF in Bandpass mode 2

And with decimation it looks like this:

Example Program: tcfest

TCFTest

Plots



TCF as a Bandpass2 with LP cutoff @ 10KHz and a HP cutoff @ 5KHz

TCF in Bandpass mode 2, decimated

Now I had the answer to my student's question. But then, years later after I moved to Beaverton Oregon, I worked with a bunch of people who were "bought out" from Tektronix and one of them was Paul Botsford,

father of the new Mixed Signal variant of the LT-1000 Logic Tester, named the MT-1000. Paul was very skilled in the pursuit of Mixed Signal technology, or so it was said. At the time, I was still somewhat unsure of the science behind my understanding of Mixed Signal, so I eagerly listened to anything Paul would tell me.

Then one day, Paul told me that the easy way to test a filter was to hit it with an impulse, as an impulse has the fundamental and all harmonics at the exact same amplitude. Boy, this sounded a lot easier than what I went through with my TCFTest. So I tried it. It didn't work at all, and the reason is simple: If you create an impulse and do the FFT on it, you will see that all the amplitudes of the fundamental and all harmonics are exactly the same (try it yourself in Excel) but the phases of all the harmonics are cosine waves.

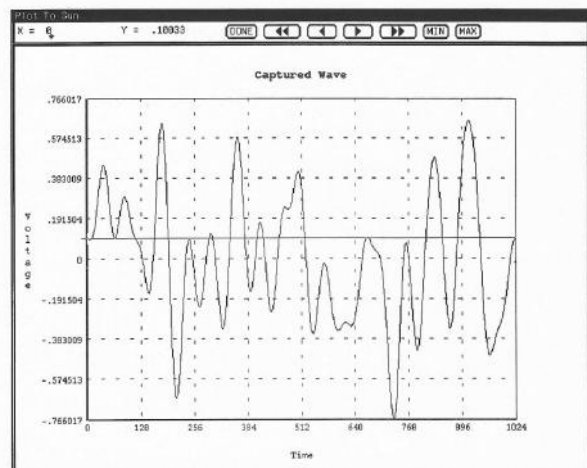
Going back to that Bullard Plot I showed you earlier, that would mean that all the harmonics are at 270° relative to a sine wave. So what happens is that all the harmonics are in phase with the fundamental, and the amplitude of the fundamental and all harmonics are equal, but they are all very small, and can't be picked up by the capture instrument at all, random noise from the environment swamps them totally.

Remember the wave I created for TCFTest, I used Random Numbers to control the phase of each harmonic, which significantly reduces the Peak to RMS ratio so that the peak of the waveform stays relatively small, like this actual TCFTest wave.

Example Program: tcfest

TCFTest

Plots



Captured, uncalibrated waveform

TCFTest captured waveform

Notice that there is a lot of RMS energy in this wave, yet the peak is relatively low. Compare that to an impulse:



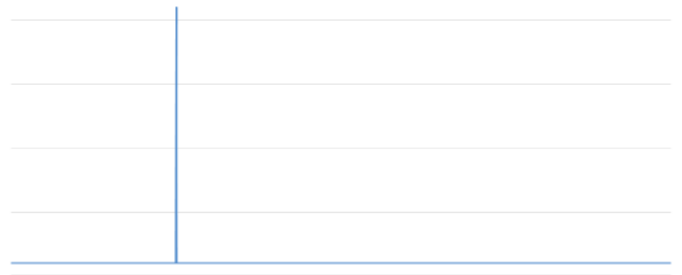
Dan Bullard

<https://www.linkedin.com/in/dan-bullard-8213046/>

Dan P. Bullard has worked in electronics since 1976 and proved his deep understanding of electronics over and over again at US Navy installations at San Nicolas Island California, Harold E. Holt Communications Station in Exmouth Western Australia, and Mare Island Cryptographic Technical School in Vallejo California as well as in the private sector at Technical Training Center, GenRad, Credence Systems Corporation, Schlumberger, Intel, Nextest Systems Corporation, Maxim Integrated Products, and Tektronix.

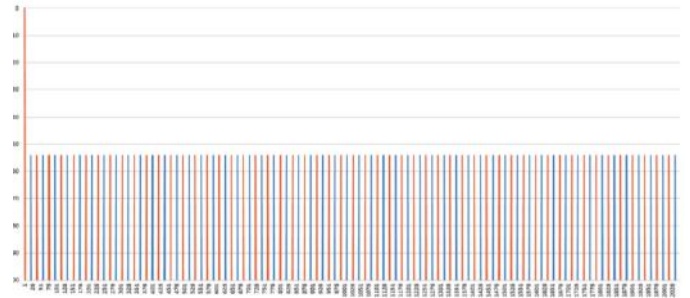
Dan is an expert in Digital Signal Processing and has taught thousands of students DSP and Mixed Signal test. He holds a patent in Smart Card/RFID testing and has been published in various electronic trade magazines such as Test and Measurement World and Evaluation Engineering as well as Houseboat Magazine. Dan has a YouTube channel that specializes in electronic topics and owns the domain www.danbullard.com where you can find many articles, tutorials, animations, and videos on electronic topics.

TD Real



Impulse in Time Domain

Yes, the impulse spectrum seems like it would be useful for testing filters, but in real life, the signal is too small to overcome any noise the system might pick up from the environment.



Perfect Impulse spectrum

So here we have two waveforms with exactly the same spectrum. One, an impulse, like a rifle shot, or a hammer blow, and the other random white noise, like wind blowing through a forest, or rain falling on the roof. Can your ears hear the difference between these two things? I bet they can, and I just proved Dr. Richard Feynman wrong.

HVCK

THE HILLS

HVCK The Hills, our first security shindig has been locked in for Feb 8th in Melbourne, and we're opening up the call for papers. We want contributors who bring the heat and question everything.

If you've got an edge, a hot take, or a bone to pick with the status quo, this is your time to bring it. We're here for the deep dives, the radical perspectives, the raw, unfiltered infosec that won't be found anywhere else.

HVCK The Hills will be more than just a conference; it'll be a convergence of sharp minds, tactical innovators, and relentless breakers of convention. Set against the rugged backdrop of the Hills, this gathering is designed for those who live and breathe infosec, where theory meets practice and raw ideas collide with hardened experience.

Expect workshops on building and breaking the things, talks on the cutting edge of security policy, and hands-on sessions that challenge attendees to rethink their assumptions. It's not just about talking shop — it's about shaping the future of cyber in a way that only HVCK can.

BAR



RECODE



HVA

ICK
life





The secret to overcoming
opioid addiction?

It is challenging to introduce this article in an entirely positive manner. However, we must address a significant issue affecting not only the cybersecurity and tech industries but society as a whole, one that is also swept under the rug. What issues are those, you ask? Opioid abuse in and out of tech industries. I understand firmly that this is a sensitive topic for most people, but I trust that the readers are mature enough to acknowledge that this is a problem and consider the topics mentioned such as substance abuse, mental illness, etc to all be a part of real fields of sciences that can help us understand these issues better.

Now that I have gotten that message over with, welcome fellow HVCK readers and contribs to - **Tryptamines: An Argument Against Opioid Addiction In Tech**, an argument I have been working on for quite a long time.

First off, I should introduce myself. I am someone who loves cybersecurity, breaking systems by the root of their design, and writing about problems I care about, showcasing to others how we can fix the problem. Writing is a very big outlet for me, it also lets me understand things from multiple angles. Those angles are the writer, the leader, and the researcher. It is because of this that I also like touching on particular subjects, such as this one.

Before we get into the actual article, I would like to warn you of one thing - this article uses research from fields such as neurology, psychopharmacology, pharmacology, and other medical fields that revolve around the study of substances/medicines in the human body. This is a real form of science and helps doctors, researchers, chemists, and more understand how to craft better substances that can cause the least damage and also help a person. Now that I have you warned and got this done with, let's move on to the actual subject matter.

What is this argument about? On a technical note, this argument is about the never-ending issues of opioid addiction primarily centered around the United States (whilst also taking elements from other countries.) The way this argument chooses to tackle opioid addiction is by taking a chemical class such as substitute-tryptamines like 4-HO-DMT and using it as an example that has been medically studied to help people with opioid addictions and also aiming to showcase how specific drugs such as opioids become addictive by attaching to specific receptors that have roles in physical dependence known as opioid receptors.

Why does this argument exist? I have spent a decent amount of time in the cybersecurity industry, enough to realize that approximately 60% of the people I have met have had horrible addictions to opioids. This was a common pattern specifically in tech, as other fields I took an interest in prior to cybersecurity seemed to not have as many issues. Alas, I spent almost 3 years researching this issue, dedicating a lot of time outside of cybersecurity to understand the inner workings behind substances and also making a valid argument that supports other substances in a specific chemical class known as tryptamines as a possible, real, and medicinal alternative.

Additionally, it has been known for quite a long time that computer scientists such as Kevin Herbert have tried a

form of natural hallucinogens such as LSD, 4-HO-DMT, and 5-MeO-DMT. However, one big debate that did come up upon the general media/news outlets when this broke out was - "are they truly helpful? Or is this an excuse to just 'get high' " As we deep dive into this paper, we debate some questions like this one and use them as key forms of support for tryptamines to treat issues such as opioid addiction and amphetamine addiction.

Tryptamines: An Argument Against Opioid Addiction In Tech

I am sure most people reading this have gone to the hospital or other locations such as a dentist's office to have some surgery done. After that surgery was done, at least in the United States, Germany, Canada, and various other countries, you may have gotten a prescription for an opioid such as Hydrocodone, which is there to ensure that you have a safe recovery and that pain is set to a minimum. Medicinal right?

The sad thing is that there is one point a lot of people forget: once these substances are touched, they have a specific impact on people who take them: addiction. For some, this is not common, for most, it's the opposite.

In order to display the argument that tryptamines can be used to treat addiction, we need and should first understand how addiction, particularly in opioids, works.

Addiction & How Opiates Work

Upon my studies, I started researching a bit into truly, how much opioid addiction existed within the field of tech and found out that a recorded approximation of 19.53% of tech professionals within the United States all have severe opioid addictions. For us to claim that a substance is addictive, we should also understand the source of the addiction. In this case, if you are not familiar with how opioids such as Oxycodone work, let's break down to a base level how they work.

Note[1] - By no means am I the best chemist in the world to explain shit, so I say wholeheartedly, the resources I showcase here can give you a good roadmap to do your research. Even if this article was considered "trusted", you should always do your independent research on topics such as substance dissection. It is also VERY IMPORTANT that I note ABSOLUTELY NONE OF THIS is medical advice. All this article aims to do is explain why opioids are bad, and how addiction works while also providing a legit, in-progress but heavily researched and supported breakaway for people who suffer from addiction. Alternatively, you should ALWAYS seek help if you feel like you are addicted and have access to professionals who can help you.

Oxycodone is known as one of the most popular pain relief substances, but it is scientifically known as a semi-synthetic opioid (synthesized from poppy-derived thebaine). For the context of the paper, semi-synthetic compounds are compounds that contain a naturally sourced base such as naturally occurring opiates, which are then enhanced using a series of chemical modification techniques to intensify the substance's primary functions. This allows opioids like Oxycodone



to target receptors a lot stronger such as the Delta receptor, measured as 'δ' which is in charge of physical dependence and analgesia (pain relief) rather than that of a natural, non-modified opioid.

Sadly, the chemical modifications of the substance enhance its efficacy by increasing its impact and activity at the desired receptors, such as the Delta receptor, while also affecting receptors involved primarily in physical dependence, such as the mu receptor, measured as 'μ'. This means that the physical dependency comes from the specific receptors that opioids target in charge of dependence.

It is important for me to inform you that I will not be going over neurobiology but will link some pubmed papers that do discuss the neurobiology behind opioid addiction.

Well, sure, you could make the fancy argument that opioids are one substance that can help more mental and physical pain especially due to what receptor it targets. However, the thing is that it is good in theory, but in the actual implementation and execution, consider the rate of physical dependence, how many doses people are prescribed [which is dependent on injury and other factors] and now you get an even stronger likelihood of things going wrong. The United States saw this quite quickly during the Opioid Crisis (Wave 2) in 2013.

When you look at the statement I made above about why this argument was crafted, I inserted a statement that expressed the understanding that many, well contributed and successful people such as Kevin Herbert have tried acid (lysergamide class), but this does not mean we should do it because some guy is successful. Remember, this is an argument against opioids to support the use of tryptamines to combat opioid addiction, not to say do drugs because someone successfully did it. To say that this is the "defined road to self-improvement and it is 100% proven to help", we also should understand the difference between opioids and tryptamines, and why one is associated with addiction and the other isn't.

Breaking Down The Differences: Opiates vs Tryptamines and Lysergamides

When you look at compounds like LSD (d-Lysergic acid diethylamide), NN-DMT (N,N-Dimethyltryptamine), and 4-PO-DMT (4-Phosphoryloxy-N,N-dimethyltryptamine) then study the results - you often see a pattern in the receptors that those above target versus compounds within the opioid class target. One was discovered to suppress portions of our receptors (Opioids) or enhance the experience on the mu receptor, Delta receptor, and others in charge of physical dependence, pain, and other functions; while the other was discovered to target receptors that are in charge of serotonin such as the 5-HT2A/C and 5-HT1A receptors (Psilocin, Mescaline, DMT, etc) [whose primary job is to control cognition, creative thinking, and decision-making].

This is a pattern I dove headfirst into and I was curious myself, why exactly are opioids worse? When you deep dive into the compounds themselves and what receptors they target, especially the ones I have listed above, you start to understand where a substance becomes a huge problem, the addiction portion.



Substances on their own, especially ones such as Oxycodone are not entirely damaging on their own, however, when that addiction kicks into someone (and most reports showcase that addiction rates are HIGH for opioids) [Based on THIS research paper by Vowles, Kevin E in 2015, the average rate of addiction to opioids in the context of chronic pain treatment (a common treatment with opioids) is estimated to be between 8% and 12%, with a 95% confidence interval ranging from 3% to 17% which basically means that, on average, 8% to 12% of the patients using opioids for chronic pain are likely to obtain an addiction.], Oxycodone or any opioid for that matter becomes abused, and when it is abused tolerance grows. The more the tolerance grows the more the person needs to satisfy an addiction and the more damaging it is on your body. It is due to this dependence (which upticks how much a person takes or needs to satisfy themselves) that the effects also become very mentally damaging for a patient and can also end up causing more physical damage than is just by getting off as opioids are very popular for their rough withdrawals [8] [(n) a life-threatening condition resulting from opioid dependence]. Thus the main difference between tryptamines & opioids is their addiction potential. Due to tryptamines having a lower potential for abuse, damage is less likely but still possible.

As stated by the NIH directly -

□ “Opioids bind to and activate opioid receptors on cells located in many areas of the brain, spinal cord, and other organs in the body, especially those involved in feelings of pain and pleasure. When opioids attach to these receptors, they block pain signals sent from the brain to the body and release large amounts of dopamine throughout the body. This release can strongly reinforce the act of taking the drug, making the user want to repeat the experience.”

~[<https://nida.nih.gov/publications/drugfacts/prescription-opioids>]

Unlike standard psychedelics, especially those of the base-tryptamine chemical class such as DMT, and even substituted-tryptamines such as 5-MeO-DMT and 4-HO-DMT (Psilocin, or the final, actual activated psychoactive substance of psilocybin mushrooms once it has been converted from 4-PO-DMT [psilocybin] -> 4-HO-DMT through dephosphorylation); opioids target specific receptors in our system in charge of suppression and physical dependence, as mentioned previously.

Now, what makes the tryptamine chemical class strong for this argument is due to its low abuse potential (due to not targeting specific receptors and the way the compound in the tryptamine class binds to other receptors). However, there is one fear with tryptamines and that is the common fear of losing control and ending up with tachycardia. But it seems as if every single recorded bad experience is mostly due to the place the person takes them, the environment they use them, the mindset in which this happens, and how the person obtains it. Of course, with every single good substance, comes a bad one. While the NIH, NIDA, and various other government-run entities focused on public health and substance research all seem to explain that tryptamines have a genuine use case for treating addiction to substances like opioids, there

is still a load of misinformation out there. In the next section, I explain a possible alternative to treat opioid addiction, one that is not talked about nearly as much as it should be.

Psychedelic-Assisted Psychotherapy (PAP) A Breakout of Addiction

For those who do not know what PEP, or Psychedelic-Assisted Psychotherapy is, it is simply a form of mental, professionally supervised use of specific substances, such as those in the base-tryptamine / analog-tryptamine chemical class. This type of therapy has been proven many times to help people in PTSD treatment as well as treatment-resistant depression, addiction, OCD, and it even holds promise as a potential intervention for addressing the psychological and existential distress experienced by cancer patients. However, while this is a better way, as showcased by research to treat addictions and again, other mental disorders - tryptamines used in PAP; as mentioned before, there is a possible damage factor with tryptamines. So how do they cause damage?

Let's start off with this, have you ever heard the phrase - "train your mind as much as your body"? Well, this phrase was mentioned in an article written by Arnold Schwarzenegger and that entire article points out something that A LOT of people tend to forget. Your mind is just as important as your body and if your mind is not treated right, it can result in physiological effects.

When dabbling around with tryptamines, you are taking a dive into the depths of your head and exploring realms that many do not touch for years and it is important to recognize that IF NOT DONE SAFELY, tryptamines can result in disorders such as Serotonin Syndrome (extremely rare as pointed out by a research paper in 2018) and can also result in bad trips. However, this is dependent upon the user of the substance and how the user takes the substance.

Generally speaking, when using substances such as 4-PO-DMT, Ayahuasca, Mescaline, and LSD-25, it is important that the user of the substance is not only accompanied by someone who knows how to handle PAP well or is a professional in that space but also has a very good array of safety measures in place around the environment they are taking the substance in. When taking these substances, a majority of people who report 'bad experiences' are doing one or multiple of the things below.

- ☐ Taking an overly extreme dose of the substance - this is not a "death by overdose" but is in fact an overdose of the substance which leads to an over-exertion of effects. This can be often overwhelming and throw someone into a panic, other words, KNOW how much you are taking.
- ☐ Doing it at raves, parties, in loud areas, or environments with a lot of entropy - A lot of people make this mistake, it's too loud, too much for your brain to process and all around is NOT recommended during PEP sessions.
- ☐ Mixing it with synthetic substances: Mixing these substances with anything from caffeine to other substances can raise problems and always puts you at a higher risk for bad experiences or all in

all negative health effects. Because people do not understand this, they often go out of bounds and mix it with substances that are the opposite of the substance they take thus causing adverse reactions and negative effects.

- ☐ Not preparing well enough: It's hard to prepare for this type of treatment, especially if you do not have enough experience. However, it is important that you prepare your environment with a nice general and calming setting which ensures a positive mindset going in and during the treatment.

There are a million things people break that cause them to have a bad trip, but this is again due to the lack of education. Where the substance comes from is also a huge factor that many miss. Legalized (depending on where you are in the world) PEP treatments happen in safe environments where the source of the substance was created and synthesized in a proper, safe, professional, and regulated laboratory unlike those you may find on the street.

The Conclusion

In the case of opioid addiction, the argument goes on to state PEP is a solution that needs to be addressed more due to the way psychoactive substances used within PEP treatments are often those that are known to assist in killing addiction. History has taught us these treatments were used centuries ago in Mesoamerican cultures such as the Mayans and Aztecs as a form of sacred medicine. So is it time to go back a few centuries and start reaching deeper into this? While it is not a guaranteed plan to stop opioid addiction in all subjects, it is better than almost all of the current solutions we have in place, even then, those that do help often fall to the waste side due to support and/or attention issues. Considering the research, I think tryptamines will start popping up more in PEP treatments and only time can tell us the true results as we did with the research in this article.

For further reading outside of this argument, I have written a few sections below.

Authors Note (Not associated with the research proofs)

Writing this article was quite difficult. To be quite honest, it destroyed me to go down the research of this paper without actually being biased. This research is something that I have been trying to dig into for quite a while. However, everybody I talk to about it other than a very few select amount of people quickly squirmed away. But I am simply not apologetic for bringing light to a serious issue affecting the tech industry and various other industries around.

In a lot of researchers' eyes, it has been discussed many times that tryptamines/substitute-tryptamines could be used as a natural remedy for breaking addiction and solving various mental issues and disorders such as panic disorder. This is important as it showcases the dangers of synthetic compounds such as Hydrocodone while also shining light on the natural form of medicines proving that nature is more of a friend than people let off.

Finally, I thank Ryan Williams for giving me the chance

to step out and write this article and for giving me a voice on sensitive topics allowing me to become a better motivator, speaker, and educator for this generation of tech nerds!

I love this community, I love what it stands for and I am tired of seeing people end their lives or ruin their lives because of addiction, and it might be time that we start bringing notice to psychedelic treatments for NOT JUST addiction, but for a variety of mental disorders. Not to mention, I am tired of seeing so many pass away from something that keeps being swept under the rug. I get that drugs make people uncomfortable, but welcome to the real world - where things should not, and can not go swept under the rug more than they already are. I live to find conclusions and solve problems, and I also know that with great advancements and a decent amount of time, we can create a really good future to erode of addiction.

The World Is Yours ~ Totally_Not_A_Haxxer

Resources

Many, many research papers were used to construct this argument and support it. They are listed below.

[1] - <https://americanaddictioncenters.org/addiction-statistics/tech-industry>

[2] - https://maps.org/news-letters/v18n1/v18n1-MAPS_21-23.pdf

[3]-<https://americanaddictioncenters.org/addiction-statistics/tech-industry#:~:text=Across%20the%20entire%20working%20class%20of%20America%2C%20more%20than%2016%25%20of%20employees%20have%20had%20problems%20with%20prescription%20drug%20abuse.%20And%20similar%20to%20alcohol%20numbers%2C%20painkillers%20substance%20abuse%20in%20the%20tech%20industry%20is%20higher%20than%20the%20overall%20average.%20With%20a%20rate%20of%2019.53%25%20of%20tech%20professionals%20abusing%20opioids>

[4] - [https://www.ncbi.nlm.nih.gov/books/NBK546642/#:~:text=Delta%20receptors%20\(DOR\)%20bind%20to,\(depending%20on%20the%20concentration\)](https://www.ncbi.nlm.nih.gov/books/NBK546642/#:~:text=Delta%20receptors%20(DOR)%20bind%20to,(depending%20on%20the%20concentration)).

[5] - "Repeated exposure to escalating dosages of opioids alters the brain so that it functions more or less normally when the drugs are present and abnormally when they are not <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2851054/>"

[6] - [https://www.fcc.gov/reports-research/maps/connect2health/focus-on-opioids.html#:~:text=Wave%202%20\(2010%20-%202013\)%3A,spike%20in%20heroin-involved%20deaths](https://www.fcc.gov/reports-research/maps/connect2health/focus-on-opioids.html#:~:text=Wave%202%20(2010%20-%202013)%3A,spike%20in%20heroin-involved%20deaths).

[7] - Based on THIS research paper by Vowles, Kevin E in 2015, the average rate of addiction to opioids in the context of chronic pain treatment (a common treatment with opioids) is estimated to be between 8% and 12%, with a 95% confidence interval ranging from 3% to 17% which basically means that, on average, 8% to 12% of the patients using opioids for chronic pain are likely to obtain an addiction.- "<https://journals.lww.com/pain/>

abstract/2015/04000/rates_of_opioid_misuse,_abuse,_and_addiction_in.3.aspx

[8] - <https://www.ncbi.nlm.nih.gov/books/NBK526012/#:~:text=Opioid%20withdrawal%20syndrome%20is%20a-,life%20threatening%20condition%20resulting%20from%20opioid%20dependence,-.%20Opioids%20are%20a%20group%20of%20drugs%20used%20to>

[9] - <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6041963/>

[10] - <https://medium.com/@Schwarzenegger/my-opinion-on-mens-mental-health-ec8c81689c7e>

[11] - <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6184959/#:~:text=Cases%20of%20serotonin,other%20syndromes.2>

[12] - <https://psychonautwiki.org/wiki/Category:DMT>

[13] - <https://psychonautwiki.org/wiki/Bromo-DragonFLY>

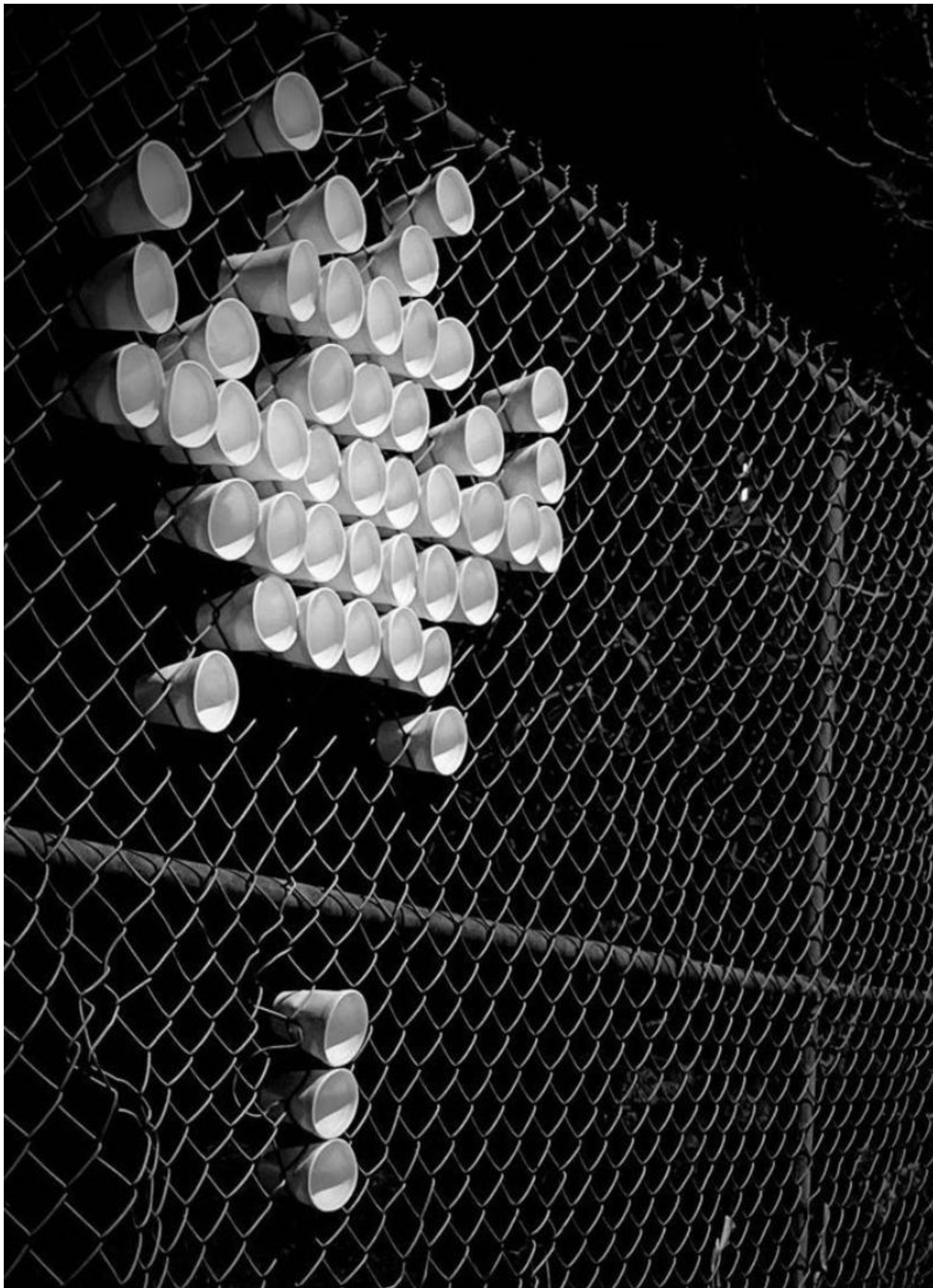
[14] - <https://psychonautwiki.org/wiki/Psilocin>

[15] - <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1571975/>

[16] - <https://books>.







place invader

Place
Invader
presents
HVCK Arts



HV

CK
encode



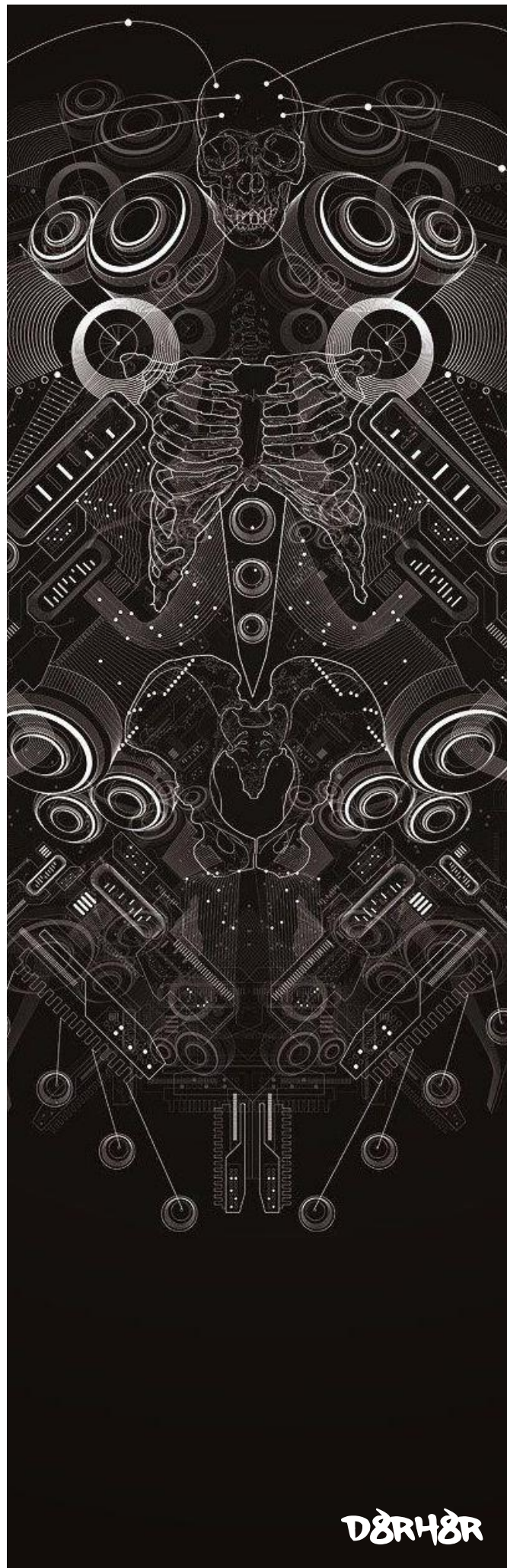


B I N
A R Y
A T B
A S H
M O R
S E C
O D E





GvoxI hvxivgh ziv xolhvob tfziwvw, zmw rg'h ml hfikirhv dsb. Uvd rm gsv rmwfhgib zyg-fzoob klhhvhh gsv pml-d-sld gl gifob nzmrk-fozgv gsv rmgirxzxrvh lu nlyrov mvgdliph, wvhkrgv gsv ylow xozrn h uolzgrmt zilfmw. Dsvm rg xlnvh gl iltfv yzhv hgzglrmh—hfxs zh uzpv YGH hvgfkh, RNHR xzgxsvih, zmw OGV hrtmzo levihszwldrmt—gsv xszoovmtvh lmob nfogrkob. Hszirmt ivzo rmhrtsgh? Gszg'h zon-lhg fmsvziw lu.Sldvevi, blf'iv rm ofxp glwzb. Sviv'h z ifmwldm gl fk blfi iltfv yzhvhgzgrlm tznv:Zfgl RNHR Xzgxsrmt: Zfglnzgrmt RNHR xzgxsrmt zooldh blf gl hgivznormv gsv kilxvhh lu xloovxgrmt hfyhxirvi rwmgrurvih drgslfg nzmfzo rmgvievmgrlm. Drgs glloh orpv hihlZM li LkvmOGV, kzriwv drgs HWI szidwziv (hfxs zh FHIK Y200nrmr li YozwvIU), blf xzm xlmurtfiv blfi hvgfkh gl zfglnzgrxzoob olt RNHR mfnyvih zh wverxvh zggvknk gl xlmvvg. Gsrh hvgfkh xzm xzkgfiv RNHRh uiln ylgS OGV zmw THN mvgdliph, nzprmt rg evihzgrov zxilhh wruu-vivmg nlyrov kilglxloh.Hrovmg g HNH Gvh-grmt uli Hfyhxirvi Olxzgrlm: Hrovmg HNH (zohl pmlm zh Gbkv 0 HNH) xzm yv hvmg gl z gztvg drgslfg mlgrubrmt gsv ivxrkrvmg. Gsrh nvhhztv kilnkgh gsv gztvg wverxv gl ivhklmw drgs olxzgrlm fkwzgvh gl gsv mvgdliph. Oveviz-trmt gsrh uli gizxprmt ivjfrivh zxxvhh gl HNH kilglxloh zmw xzm yv fhvufu uli wvgvinrmrmt z hfyhxirvi'h zkkilcrnzgv olxzgrlm. Gsrh gv-x-smrjfv wlvhm'g tvmvizgv zmb mlgrurxzgrlmh lm gsv fhvi'h wverxv, nzprmt rg z xlevig nvgs-lw uli olxzgrlm gizxprmt.Wldmtizwv Zggzxph gl 2T: Yb ulixrmt z gztvg wverxv uiln 4T/OGV wldm gl gsv rmhvxv 2T mvgdliph, blf xzm vck-olrg gsv ozxp lu nfgfzo zfgsvmgrxzgrlm rm THN. GGllh orpv LhnlxlnYY li BzgvYGH, xlnymvw drgs zm HWI, zoold blf gl rnkvihlmgv z 2T xvoo gldvi, girxprmt mvziyb wverxvh rmgl xlmvvgxgrmt gl blfi iltfv hgzglrm. Lmxv xlm-mvvgvw, gsvhv wverxvh ziv hfhxvkgryov gl rmgvixvkggrlm wfv gl dvzpvi li wrhzyovw vmx-ibkggrlm kilglxloh rm THN.TKIH Gizuux Nlmrglirmt: Lmxv blf szez wverxvh wldmtizwv gl 2T, nlmrglirmt TKIH gizuux rh z oltrxo mvcg hgkv. TKIH gizuux nlmrglirmt xzm yv xlmwfxgvw yb xzkgfirt fmvmxibkgvw kzx-pvgh levi gsv mvgdliph. Gsrh zooldh blf gl lyh-viev wzgz vcxszmtvh, hfxs zh HNH li yildhrmt gizuux, gszg nrtsg yv gizmhnrggvw rm xovzi gvvg. Fhrmt glloh orpv Drivhszip drgs zm HWI wverxv zmw xlmurtfiw mvgdliph hvgfkh, blf xzm zmzobav gsrh wzgz uli ezofzyov rmhrtsgh.Rm hslig, dsrov gsv rmwfhgib ivnzrmh grtsg-orkkvw, nzhgvirmt gsv yzhrxh lu HWI zmw lkvm-hlfixv xvofozi hlugdziv xzm kiler-wv z hgilm ulfmwzgrlm gl vckoliv gsvhv iltfv hvgfkh. Zodbh kilxvw drgs xzfgrlm zmw yv nrmwufu lu gsv ovtzo rnkoxzgrlmh rmeloewv.



[The page contains dense, illegible horizontal bands of noise or heavily distorted text.]

HVA

ICK
arts



Aperture voices

A red thread binds the
poetry spoken
By the Pashtun women
A Red thread -
Blood red -
binds the knowledge
Of the mothers
To the daughters

narrative fragments
whispered
over and over
Tracing the Ovum
In Ovulatory orbit
That contains the sisters
three -

Spin, measure, cut,
weave,
Spin, measure, cut;
sisters three
have died three times
and
born again by three;
Their circle dance
is a spell recited
in holy trinity
Dancing to invoke the
power
Of their oracular
decree.

To be another
or to be a river
Red River Warm
River changing
Rearranging
Denying before
engulfing
always downward
Down to the sea
Always surrendered
Falling into the deep
The ocean refuses no
river
It receives all
That returns again

From first womb
We go down
down to the sea
To the last tomb
We go down
Down to the sea
Our final delight
is our silent flight
into
Atlantean geographies
Caves watching and
waiting
to be revealed
Autoluminescence
sentience moved by
sonorific sensuality
into the chambers filled
with songs
carried by rivers

through time and space
places edging temporal
horizons
Carrying us all
From the first
To the last
Down
Down
To the sea

Subverting oppression
syllables two and twenty
Words thatched
to hide the poised sting

- does it bring
Medicine or poison as it
disappears
between
Words spoken and
meanings heard;

Behind the burka
sharp tongues are coiled
Electrified
Short-circuiting
machinations of
oppression
Replenishing the well of
freedom
From below

I sing even under my
blue hood.
My mother says I am a
most determined songbird

Vigilante poetry
A diabolical dialect
Spoken
By
deviant daughtersnushu
nushu
nushu
hidden letters in secret
script
400 years
in chamber rooms
Forgotten
Feet bound and voices
unused

Crawling on the ground
Her moving makes no
sound
She drags her feet
behind
And wishes she was
blind
For her body was a
remnant
distorted by
desire
All sensing nature lost
in long confinement
The sonic Monotony of
Of an unspoken captivity
Laced with muted
lamentations





Suffused with a taste
for blood and mutiny

Defiled by beauty
Made savage by pain
Fingers scrawl through
the ash and moth-wing
window panes
nushu poetry
Hidden hieroglyphs of
high-born sisterhood,
Mandala-codes of
rebellion
That give hope

Battle plans recorded
on folding fans
Nushu
Nushu
Nushu

Deranged
By the torment of
binding

Full of kinetic kindling
Ready
Begging
praying
to be
set alight

Nushu
A circle
A gathering place

caoineadh
Crying
caoineadh
Crying
caoineadh
Crying

mnàthan-tuirim
The keening woman

A ritual keeper
Midwife to the dead
She has burned for
knowing
too much

The keening woman
Spoke in an ancient
language
Raw
Unearthly
Unyielding

Repeating sounds
Utterances
Not words
but sonic stones that
formed a circle
A holding space where
the feeling could find



Suffused with a taste
for blood and mutiny
Defiled by beauty
Made savage by pain
Fingers scrawl through
the ash and moth-wing
window panes
nushu poetry
Hidden hieroglyphs of
high-born sisterhood,
Mandala-codes of
rebellion
That give hope

Battle plans recorded
on folding fans
Nushu
Nushu
Nushu

Deranged
By the torment of
binding

Full of kinetic kindling
Ready
Begging
Praying
to be
set alight

Nushu
A circle
A gathering place

caoineadh
Crying
caoineadh
Crying
caoineadh
Crying

mnàthan-tuirim
The keening woman

A ritual keeper
Midwife to the dead
She has burned for
knowing
Too much

The keening woman
Spoke in an ancient
language
Raw
Unearthly
Unyielding

Repeating sounds
Utterances
Not words
but sonic stones that
formed a circle
A holding space where
the feeling could find

It's nature
It's unique current

mnàthan-tuirim

So old so very old

The keening woman sings
to the departed
And her keen is never
the same

caoineadh
caoineadh
caoineadh

Her cry calls the soul
from the body at death
Clears the passage
across
She has no fear of what
lingers here
For she knows the ways
of both worlds
her map is the land
Upon which she stands
Her language the
medicinal balm

caoineadh
The keening woman cries

bha e annabarrach
breagha
A beautiful anchor
is her song

Let the outlawed voices
Be heard
The languages of
deviancy spoken
Write the poetry of
protest and promise
in blood
in dust
On bodies
Ravaged yet unconquered

Stand on broken feet
Declare
Your resistance -
I will be there with
you all,
My forked tongue
Spitting

from
the pen of

Lil'Red

HVA

ICK
hardware



EXP
SECL

<https://explo>



LOOT
IRITY

itsecurity.io



SPILL

SPI and Dumping Flash

by **Victor Hanna**
[www.exploitsecurity.io]

In this article we will be describing what Serial Peripheral Interface or SPI, is and where and why it is used within embedded systems. This interface type is widely used and therefore understanding its functionality will assist whilst conducting security research

The post shall attempt to describe:

- An overview of SPI
- SPI Main/Subnode architecture
- SPI Data transmission
- SPI Transmission Modes
- How SPI can be used by security researchers
- Dumping Flash via SPI

Overview

SPI is a full-duplex synchronous data transfer architecture used to transfer data between an embedded MCU (Micro Controller Unit) and a respective peripheral device or more generically between a Main and Subnode. Examples of such peripheral devices are sensors, SRAM (Static Random Access Memory), display controllers and NOR flash peripherals. As described above, SPI uses a full-duplex communications flow which is made possible through the use of separate send and receive lines. This allows peripherals that are attached to the corresponding SPI bus to both transmit and receive simultaneously. To achieve full-duplex data flows, SPI uses 4 unidirectional wires with each wire dedicated to a specific signal.

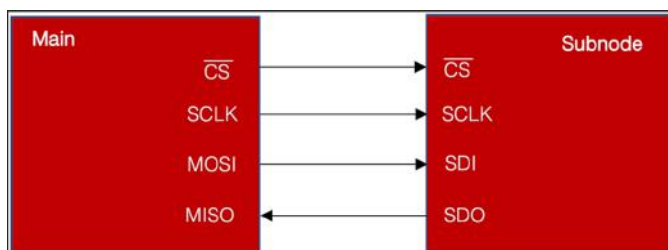


Figure 1. SPI Main/Subnode Interconnect

—
CS – Chip Select
SCLK – SPI Clock
MOSI – Main Out / Subnode In
MISO – Main In / Subnode Out

Figure 2. SPI 4-Wire annotation

SPI Main/Subnode Architecture

The architecture that is used by SPI is the Main/Subnode Architecture. The Main indicates the device that generates the clock signal. This SPI Clock signal is used to synchronise data transmission between the Main and each Subnode. As just inferred an SPI system can be made up of a single Main with multiple Subnodes. In order for the Main to indicate which Subnode it would like to interact with the Chip Select wire is first needed to be asserted. The Chip Select wire is asserted by electronically pulling the wire to a low signal (logic 0) and conversely pulled high (logic 1) when requiring disconnection to the subnode. The MOSI and MISO wires are the data lines used by an SPI system. MOSI describes the data line where data flows from the Main to Subnode, whereas the MISO describes the data line where data flows from the Subnode to Main. As mentioned above these flows can occur simultaneously in a full-duplex fashion.

SPI Data transmission

Data transmission is initiated by the Main, which sends a clock signal and asserts the appropriate chip select wire connected to the intended Subnode it wishes to transmit and receive data to and from. In order for data to be sent and received, each respective device will send (shift out) data across the MOSI data line for transmission and receive (sampled and read-in) data in across the MISO data line.

There are 4 SPI transmission modes that can be used for data transmission of which all four should be supported by the Main, however this is not the case for Subnodes, which will typically be pre-configured with a transmission mode. In the context of embedded systems, this is an initial design choice by the manufacturer, and ensures that all devices communicating over the SPI bus are compatible. The SPI Control Register stores the functional state of the transmission mode using two bits, namely the Clock Polarity bit (CPOL) and the Clock Phase bit (CPHA).

The CPOL bit refers to the logic level of the clock at idle, where idle is the state in which no data is being transmitted or received and where the Chip Select line is pulled high (active low configuration). The CPHA bit refers to the sampling edge, which indicates when data will be read-in or shifted-out on either the rising or falling edge of the clock pulse. In order for successful data transfer to take place all of these configurations should match at both ends of the data transfer lines.

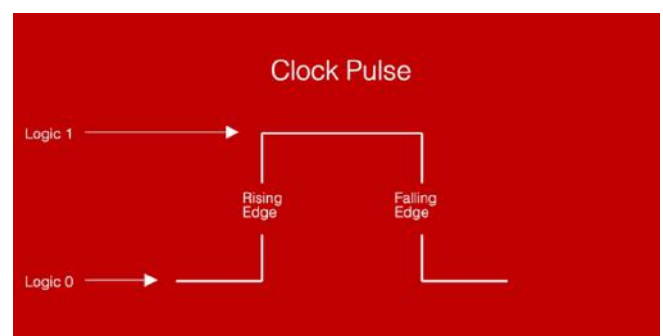


Figure 3. Clock Polarity and Phase Diagram

SPI Transmission Modes

As mentioned above there are four SPI transmission modes. It is important to understand that although transmission modes are the basis for data transfer each device that is being controlled will have its own protocol format that allows for successful interaction with the device itself. This section is merely how basic SPI functions under-the-hood, however rest assured that manipulating a device of a specific type is where the curiosity truly grows.

Mode 0 - CPOL = 0, CPHA = 0

- Every clock pulse transition to low transmits next bit
- Every clock pulse phase transition to high samples data

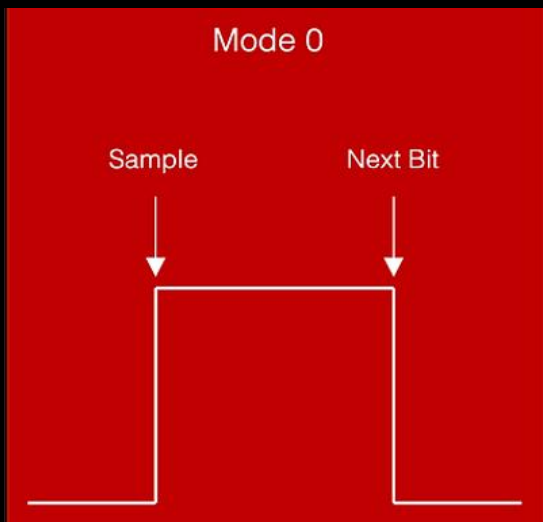


Figure. 4

Mode 1 - CPOL = 0, CPHA = 1

- Every clock pulse transition to high transmits next bit
- Every clock pulse phase transition to low samples data

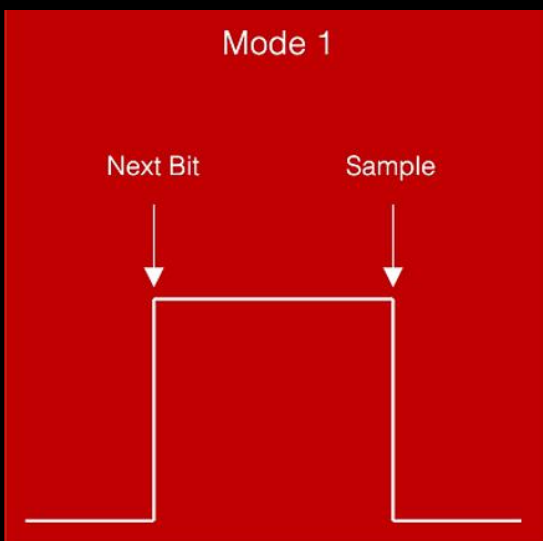


Figure 5

Mode 2 - CPOL = 1, CPHA = 0

- Every clock pulse transition to high transmits next bit
- Every clock pulse phase transition to low samples data

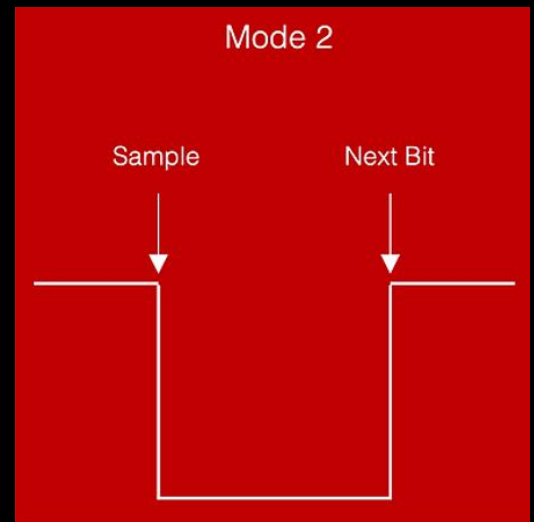


Figure 6

Mode 3 - CPOL = 1, CPHA = 1

- Every clock pulse transition to low transmits next bit
- Every clock pulse phase transition to high samples data

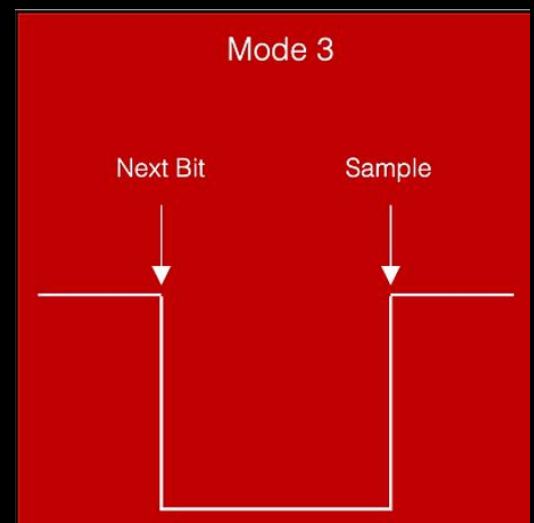


Figure 7

If you examine things closely you will notice a correlation between both Mode 0 and 3 which are seemingly functionally identical, with the difference being starting clock logic levels. So too are Mode 1 and Mode 2.

How SPI can be used by security researchers
More often than not security researchers of embedded systems will often place high value on retrieval of a devices firmware. In some cases this firmware can be obtained from either a manufacturers website or alternatively via over the air firmware updates. In some cases these strategies may be elusive and may call for a more directed approach. One such highly successful approach is the extraction of firmware from flash memory. Flash memory is a non-volatile memory type that

is most often the repository for an embedded systems' firmware. Firmware is essentially the bridge between the hardware of a system and the software drivers that allow for a system to function. It can also be bundled with the systems kernel and as such provides a treasure trove of information that underlies the system itself.

Moreover if obtained can be used alongside an emulator to emulate the very function of the embedded system itself. Obtaining the running firmware of an embedded system can also open up possibilities like implementation of root kits or affording the opportunity to reverse engineer binaries to understand the inner workings and perhaps even research said binaries to tease out weaknesses.

Dumping Flash via SPI - Example

This example shows that once a PCB has been examined and an appropriate candidate flash memory chip has been identified, that it is then trivial to hookup to the peripheral and subsequently dump its contents. We will be using our Exploit Bridge [Pictured Below] to help us with this endeavour, alongside the Defcon32 badge to help illustrate this tec



Figure.8
Exploit Bridge Badge

Step 1. Identification of the peripheral

Examination of the PCB leads the researcher to understand that we are dealing with a Winbond flash memory chip (W25Q32JVS1Q). With this information on board a datasheet is obtained so as to ascertain pinouts of the chip. The type of chip we are dealing with is in a SOIC-8 package, 3V 32M-BIT SERIAL FLASH



Figure.9
Defcon 32 Badge

MEMORY WITH DUAL, QUAD SPI.

Step 2. Obtain Datasheet and identify pinouts

After obtaining the respective datasheet the determination is made of the peripherals pinout



Figure 10 Flash Memory Chip

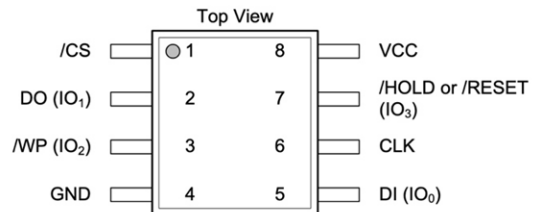


Figure 11 Chip Pinout Block Diagram--

Step 3. The most convenient way to wire this chip inline is to use an SOIC-8 SOP test clip and to then hookup to the respective pins and with the help of a trusted Exploit Bridge.

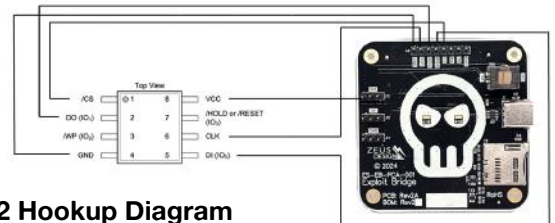


Figure 12 Hookup Diagram

Step 3. Above

Step 4. Using the Test Clip to hookup as per

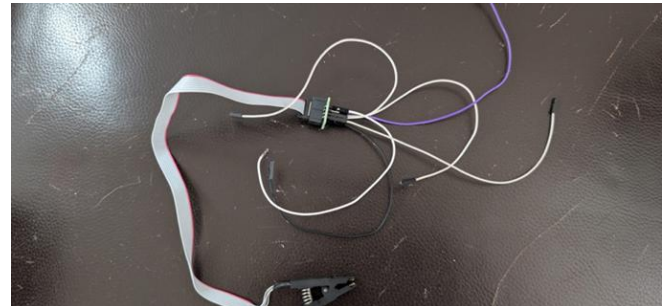


Figure 13



Figure 14

Step 5. Using the flashrom utility to dump the flash for further testing

```
sudo flashrom -V -p ft2232_spi:-type=2232H,port=A -r firmware.bin
```

Summary

This article intends to lay the foundations with respects to SPI and its inner workings. In providing an overview of the architecture and its core features it is the hope that this information was found to be a valuable reference point. SPI is a technology that is ubiquitous with respects to the embedded system ecosystem and knowledge of its functionality can prove to be a useful candidate in a security researchers toolkit.





by Antonio Silva

Introduction

Recently, I observed people implementing cryptography for Arduino by themselves like state in this topic in stackoverflow:

<https://stackoverflow.com/questions/39189065/rsa-encryption-decryption-functions-for-arduino>

Several of them can be found over the internet, some by the way are in well-knowm libraries. I decide to do this small PoC (Proof of concept)to show why is important not invented your own cryptography algorithm, but also use a robust implementation of such a algorithms.

This PoC performs an side channel attack (power analysis attack) against a bad implementation of an auxiliary routine used in the RSA implementation (fast exponentiation).

A side-channel attack is a method of compromising a cryptographic system by exploiting indirect information leakage rather than directly attacking the cryptographic algorithm or protocol itself. This type of leakage can originate from various sources such as timing information, power consumption, electromagnetic emissions, or even sound.

Such attacks can be highly effective in compromising cryptographic systems like RSA without requiring the attacker to solve the underlying mathematical problems that ensure the security of the cryptographic scheme (Kocher, Jaffe, & Jun, 1999).

This paper will perform a power analysis attack on a well-known vulnerability in an implementation of the RSA algorithm in a firmware for Arduino (Atmega328P).

Note I did it on the rush, please forgive me for the spells / grammar errors that eventually you will find.

Power Analysis Attacks

Power analysis attacks involve measuring the power consumption of a device during cryptographic operations.

Differential Power Analysis (DPA) involves statistical analysis of power consumption patterns across multiple cryptographic operations to extract secrets, making it more sophisticated than Simple Power Analysis (SPA), which directly correlates power fluctuations with specific cryptographic operations to deduce secrets.

Differential Power Analysis (DPA) and Simple Power Analysis (SPA) can be used to extract private keys by analyzing patterns in power consumption during RSA computations.

These attacks can reveal the private key by identifying distinct power usage patterns associated with different key bits (Kocher, Jaffe, & Jun, 1999).

RSA: A Short Introduction

RSA (Rivest-Shamir-Adleman) is a widely used public-key encryption algorithm named after its inventors: Ron Rivest, Adi Shamir, and Leonard Adleman, who introduced it in 1977 (Paar & Pelzl, 2010). It remains one of the most secure methods for transmitting data securely over the internet.

One of the foundations of RSA's security lies in the difficulty of factoring large composite numbers into their prime factors (Menezes, van Oorschot, & Vanstone, 1996). This problem,

known as the factoring problem, involves finding the prime numbers that multiply together to form a given large number. RSA encryption relies on the assumption that this factoring problem is computationally difficult enough to make it impractical to break the encryption by factoring the modulus into its prime factors (Menezes, van Oorschot, & Vanstone, 1996).

RSA Example

The Figure 1 illustrates the RSA encryption and decryption process using a simple example.

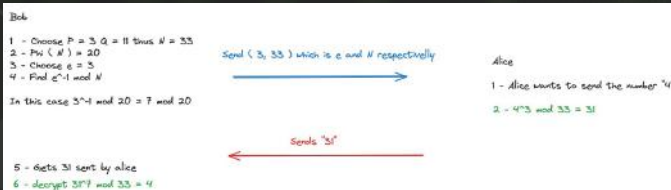


Figure 1 - RSA example.

Please note that in this case, 3 and 33 are public. The number 7 in the example is the private key. The Phi(N) function, Euler's totient function, computes all coprime numbers in the interval from 1 to 33. The value 33 is obtained from the multiplication of P and Q; in this case, 11 multiplied by 3. The result of the Phi function is obtained by multiplying (P - 1) by (Q - 1); in this case, 10 multiplied by 2. The operation $e^{-1} \bmod N$ denotes the modular inverse operation (Menezes, van Oorschot, & Vanstone, 1996).

Note: If you wish to delve deeper into RSA, which is not necessary to understand this paper, there is a quick introduction to these basic number theory operations within this repository the file number_theory.md. The explanation can enhance your understanding of RSA operations.

Equipment

The experiment used an oscilloscope DS1102 (presented in the Figure 2) manufactured by Rigol.

The oscilloscope's manual can be found in the references (RIGOL Technologies, Inc., 2017). A generic power supply was used either (presented in Figure 3).



Figure 2 - Oscilloscope used in the experiment.



Figure 3 - Power supply used in the experiment.

Measuring power a short introduction

Ohm Law

Ohm's Law is a fundamental principle in the field of electrical engineering and physics. It states that the current flowing through a conductor between two points is directly proportional to the voltage across the two points and inversely proportional to the resistance between them (Boylestad, 2015). The Figure 4 shows an circuit and the Ohm's law.

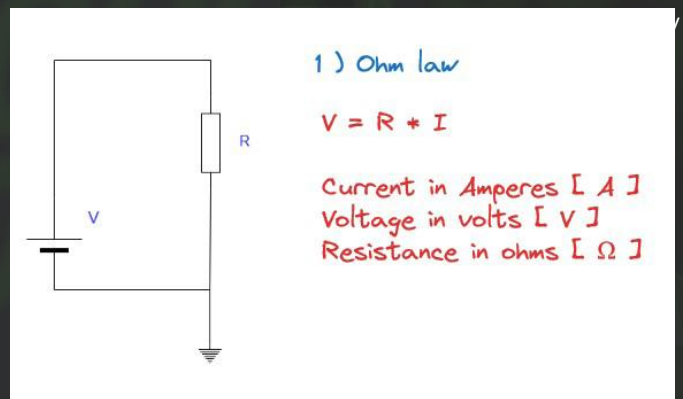


Figure 4 - Ohm law illustration.

The Ohm law implies that if you increase the voltage across a conductor, the current will also increase, provided the resistance remains constant (Johnson & Hilburn, 2013). Figure 5 present an example of Ohm's law application which the goal is to find the current in the circuit.

[alt text](https://github.com/lord-feistel/power_analysis/blob/main/images/ohm_example.jpg)

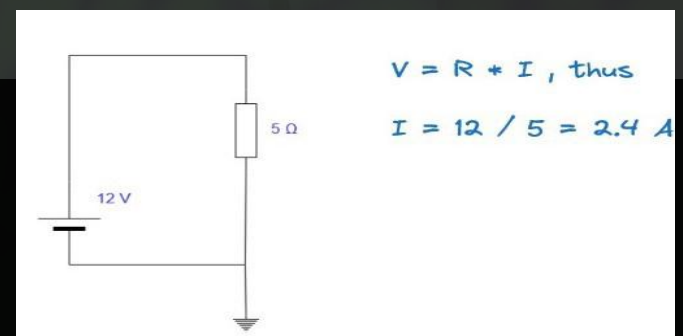


Figure 5 - Ohm law example.

Kirchoff law

Kirchoff's Voltage Law (KVL) is a fundamental principle in electrical engineering and physics (Boylestad, 2015). It states that the sum of all electrical potential differences (voltages) around any closed network or loop is zero (Boylestad, 2015). The Figure 6 illustrates the Kirchoff's voltage law.

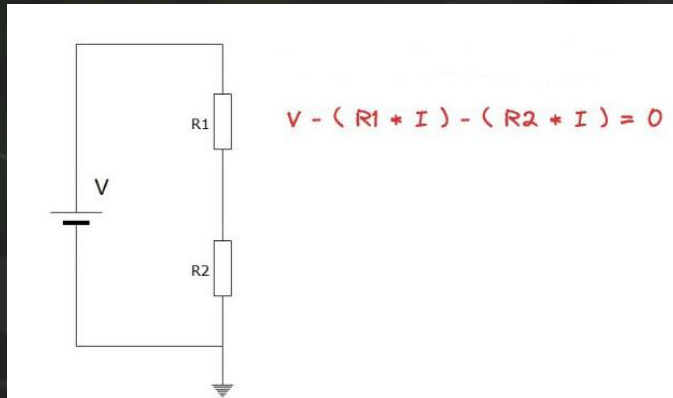


Figure 6 - Kirchhoff law illustration.

There is an example of the Kirchoff's law's application in the Figure 7 in order to find the current over the resistors R1 and R2.

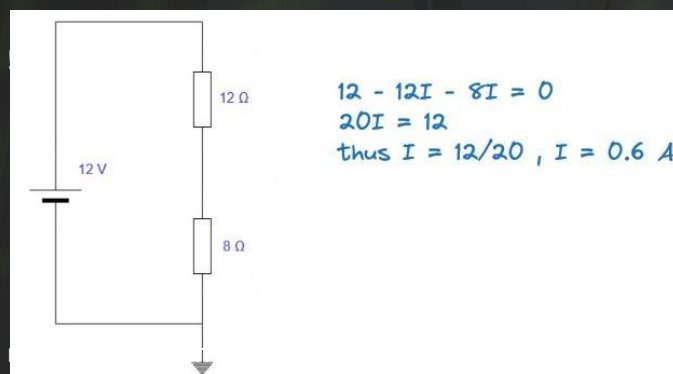
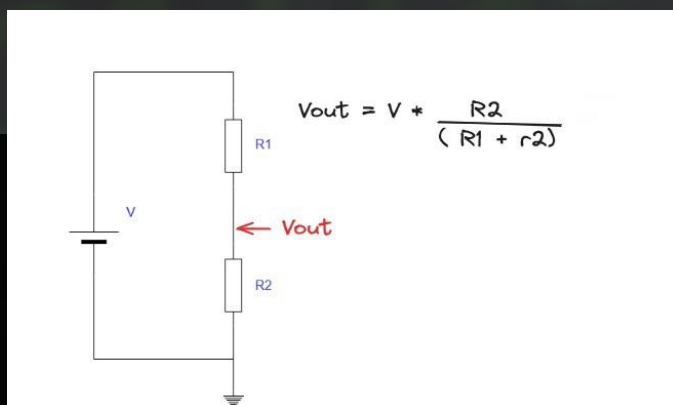


Figure 7 - Kirchhoff law example.

Voltage divider

The voltage divider is a consequence of Kirchoff's Voltage Law (KVL) and states a way to calculate the V_{out} that is the voltage between the resistor R1 and R2. The formula of the voltage divider is presented in the Figure 8. An example of voltage divider application is presented in the Figure 9.



[alt text](https://github.com/lord-feistel/power_analysis/blob/main/images/voltage_divisor.jpg)

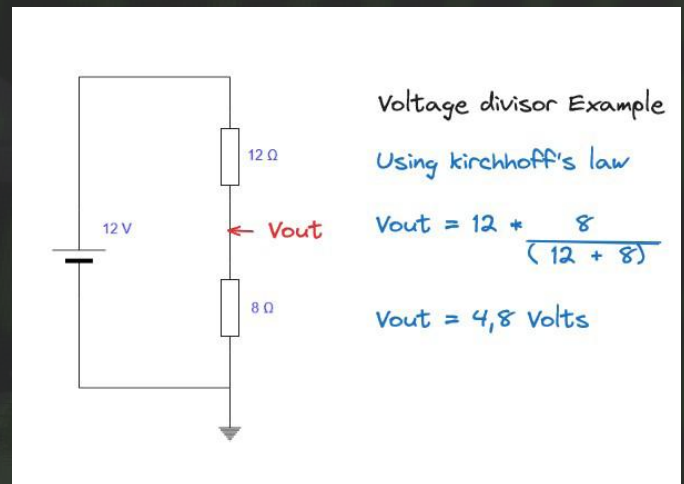


Figure 9 - Voltage divider example.

Shunt Resistor

A shunt resistor is a low-value resistor placed in series with the circuit's power supply to measure the current flowing through the circuit.

Using a Shunt to measure current is one of the techniques utilized in modern multimeters. (Boylestad, 2015). Measuring the voltage drop across the shunt resistor and knowing its resistance gives enough information to calculate the current using Ohm's Law.

To measure the current consumption of an Arduino device it is needed to place a shunt resistor in series with the VCC (positive). The way it will be connected is presented in the Figure 10.

Note 1: Please note that in the PoC, instead of using the Arduino Uno board, the target (microcontroller atmega328p) is transferred to a separated breadboard as presented in the Figure 11. It allows to easier manipulate the pinout of the microcontroller not requiring soldering.

Note 2: If you don't know how to do that, my previous article showing how glitching works teaches how to do that and can be found at https://github.com/lord-feistel/hardware_hacking_lab

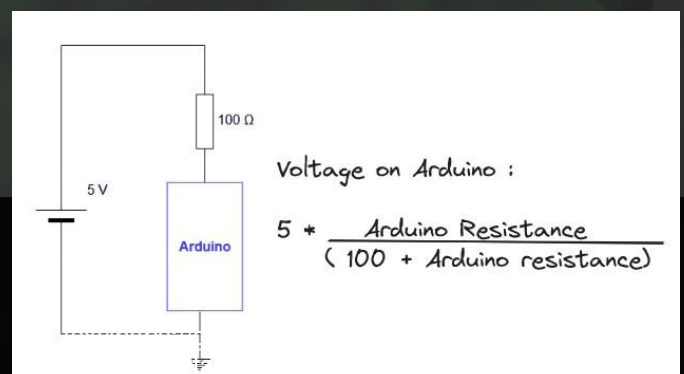


Figure 10 - Shunt with Arduino.

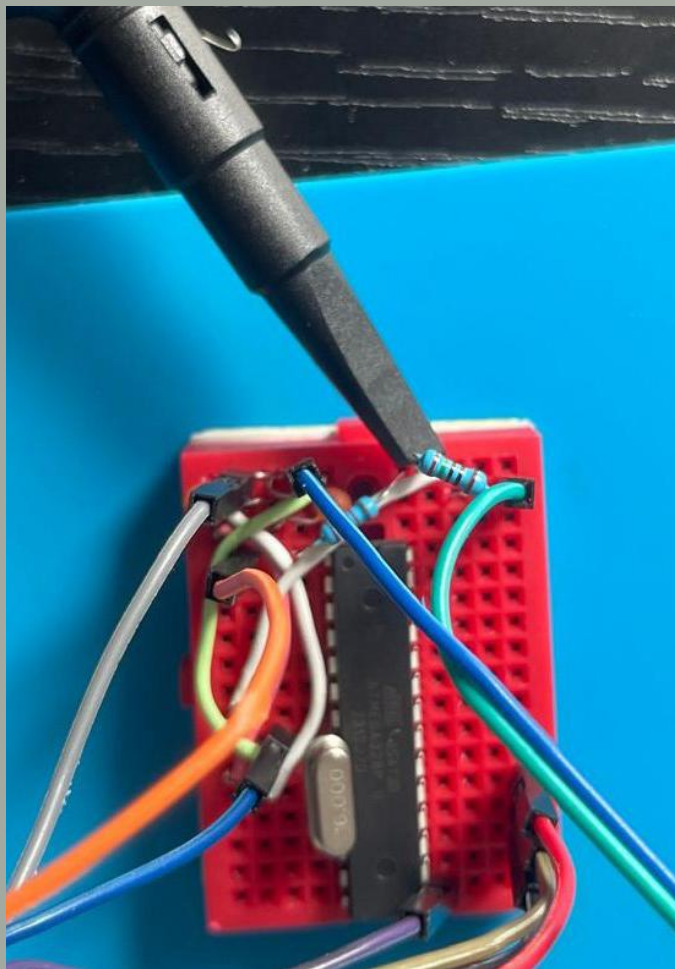


Figure 11 - Circuit of the shunt in the breadboard.

Example of power measurement

To demonstrate the measurement of current consumption using a shunt resistor, a LED (Sedra & Smith, 2014) will be connected to the microcontroller's GPIO (Figure12) and the oscilloscope will be used to observe how it affects the power consumption over the shunt resistor in the situations where the LED is on or off.

Observe to extract the Key or observing the charger effect over the power consumption is not needed to use the Ohms law to obtain the current, only the voltage drop is already enough (Johnson & Hilburn, 2013).

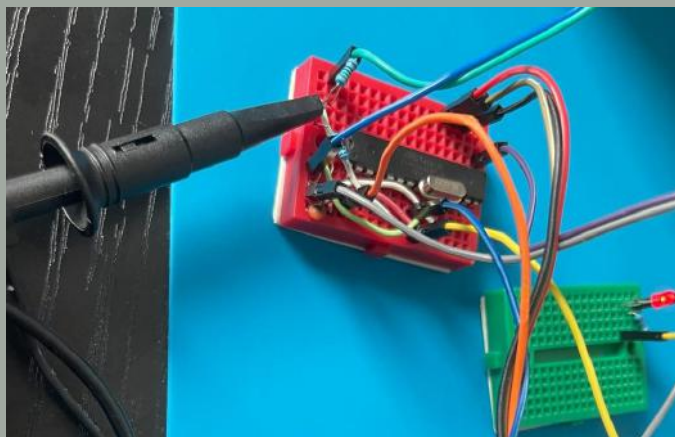
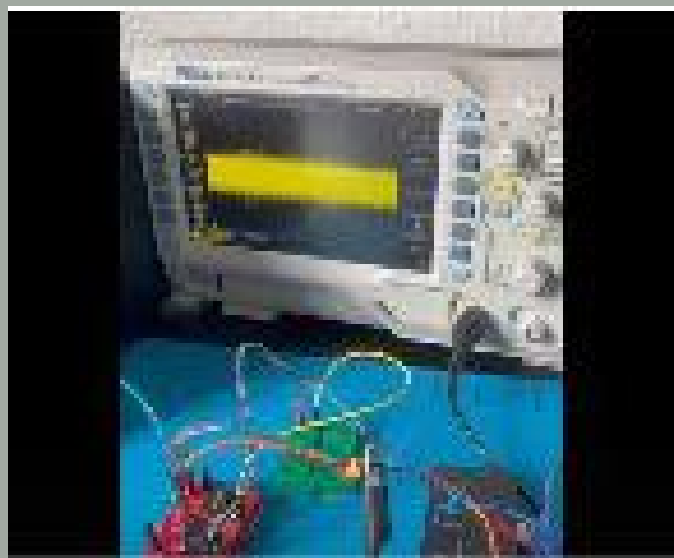


Figure 12 - Power measurement.

To better observe it, please check the Video 1 which shows how the voltage drop when led is on.



Video 1 - Voltage drop because led consumption.

The following code was utilized to blink the led. It also can be found in this repository.

```
const int PIN_CHARGE = 9 ;

void setup() {
    pinMode(PIN_CHARGE, OUTPUT);
}

void loop() {
    digitalWrite(PIN_CHARGE, HIGH);
    delay(10);
    digitalWrite(PIN_CHARGE, LOW);
    delay(10);
}
```

It is important to state that this voltage drop also occurs when an complex calculation happens (Kocher, Jaffe, & Jun, 1999). The following code causes the Voltage drop presented in the Figure 13

```
void setup() {
}

void loop() {
    volatile unsigned long i = 0;

    i = ((i + 1) * (i - 1) + (i * i) - (i / 2)
    * (i % 3) + (i * i * i * i)) * ((i + 2) *
    (i - 2) + (i * i) - (i / 3) * (i % 5) + (i *
    i * i * i));

    delayMicroseconds(100);
}
```

If the voltage drop reflects of calculation, thus it can be used to determine the data which is being processed.

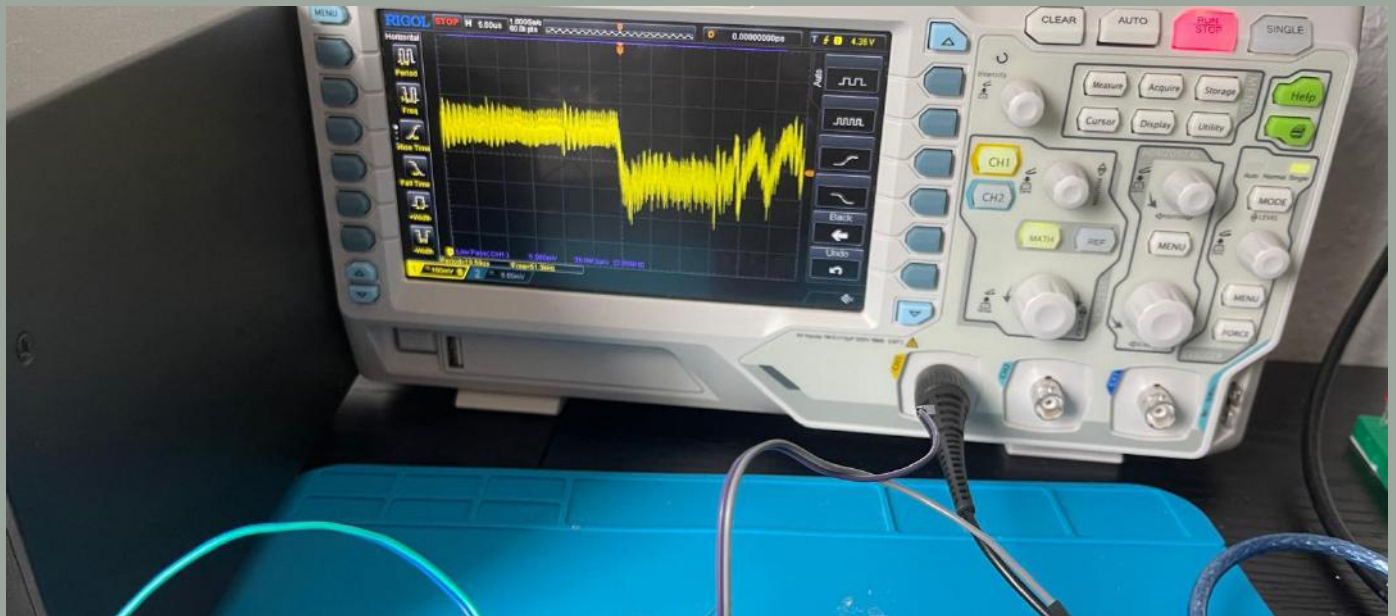


Figure 13 - Power consumption in the heavy calculation.

Fast exponentiation

The conventional way to perform the power operation is multiplying the base n times.

Suppose 2^3 will result in $2*2*2$ since 2 is the base and 3 is n . It works very good, but not efficiently enough to make RSA feasible. In order to achieve such an implementation it is used the fast exponentiation algorithm.

Fast exponentiation, also known as exponentiation by squaring, is an efficient method for raising a number to a power. Following the pseudo-code for the fast exponentiation can be found.

```
function fast_exponentiation(a, b):

    result = 1

    base = a

    exponent = b

    while exponent > 0:

        if (exponent % 2 == 1): // If exponent is odd

            result = result * base

        base = base * base    // Square the base

        exponent = exponent // 2 // Divide exponent by 2

    return result
```

The steps of the fast exponentiation of 2^4 can be found in the Table 1

Note that for smaller numbers nothing change or it will get worse, however for big numbers it obtains a significant achievement in the efficiency.

Iteration	Base value	Exponent in Binary	Operation	Result
Initial	2	100	Start	1
1	4	010	Square	1
2	16	001	Square	1
3	256	000	Multiply	16
Final	-	-	End	16

```
- **Initialization:**
    Start with base = 2 , exponent = 4 ( binary 100 ) , result = 1.

- **Iteration 1:** exponent = 4 (binary 100, even)
    Square base to get 4 .
    result remains 1.

- **Iteration 2:** exponent = 2 (binary 010, even)
    Square base to get 16 .
    result remains 1.

- **Iteration 3:** exponent = 1 (binary: 001, odd)
    Multiply result by a = 16 to get 16.
    result becomes 16.

- **Final:** n = 0 (binary: 000)
    The loop ends with result = 16.
```

It reduces the number of multiplicative operations compared to the naive approach, which is particularly useful for large exponents. Table 2 shows a comparison of the iterations for such a number using the naive exponentiation and the fast exponentiation.

Fast exponentiation is critical in RSA for both encryption and decryption processes, as these processes involve raising large numbers to large powers modulo some other large number (Paar & Pelzl, 2010). As presented in the RSA example section the key is the exponent and usually it will be a very large number.

As presented in the RSA example section the key is the exponent and usually it will be a very large number.

Exponent (b)	Binary (b)	Conventional Exponentiation Operations	Fast Exponentiation Operations
1	1	1	1
2	10	1	1
4	100	3	2
8	1000	7	3
16	10000	15	4
32	100000	31	5
64	1000000	63	6
128	10000000	127	7
256	100000000	255	8
512	1000000000	511	9
1024	10000000000	1023	10

Table 2 - Comparson of efficiency between conventional exponentiation and fast exponentiation.

Fast exponentiation in Arduino (Atmega328P)

An fast exponentiation was implemented in the arduino and uploaded in the atmega328p. As it is a PoC we implemented it in the easiest way to be visualized.

For instance, usually it is utilized shift operation over an integer variable, but we implemented the exponent as an array to be better understood.

Note the exponent representing the key is the array {0, 1, 0, 1, 0, 1, 0, 1} which will create a pattern in the measure acquired by the oscilloscope as a proof of that it works.

```
#include <Arduino.h>

volatile long long dumb_vulnerableExponentiation(volatile long long base,
const volatile int* exponentArray, volatile long long modulo) {
    volatile long long result = 1;
    base %= modulo;

    for (volatile int i = 0; i < arraylength; ++i) {
        result = (result * result) % modulo;
        if (exponentArray[i] == 1) {
            result = (result * base) % modulo;
        }
    }

    return result;
}

void setup() {
}
```

```
void loop() {
    volatile long long base = 3;
    volatile long long modulo = 1000000007;
    const volatile int exponentArray[] = {0, 1, 0, 1, 0, 1, 0, 1};
    volatile int arraylength = sizeof(exponentArray) / sizeof(exponentArray[0]);
    delay(2);
    volatile long long result = dumb_vulnerableExponentiation(base, exponentArray, arraylength, modulo);
}
```

Results

As presented in the begin for the encryption and decryption operation the key is the exponent, therefore discovering the exponent the RSA key is exposed.

Using the hardware previous mentioned it is possible to see the spectrum of power consumption in the oscilloscope as presented in the Figure 14 and Figure 15

The periods which the voltage drops for a long time it means the bit 1 of the key is being processed, otherwise is the bit 0.

Please, note that when the exponent is even there is one extra multiplication what makes the energy drop takes longer exposing key information.

Figure 14 - Key capturing

showing_key

Figure 15 - Exposing 0 and 1 of the key using oscilloscope

Video 2: Key_capture

Video 2 - Capturing the key with oscilloscope.

Such a attack can be used in a scenario whic the micro-controller is using an well-known library, however the firmware is locked not allowing the attacker to obtain the key directly from the memory.

This kind of attack also can be used against hardware.

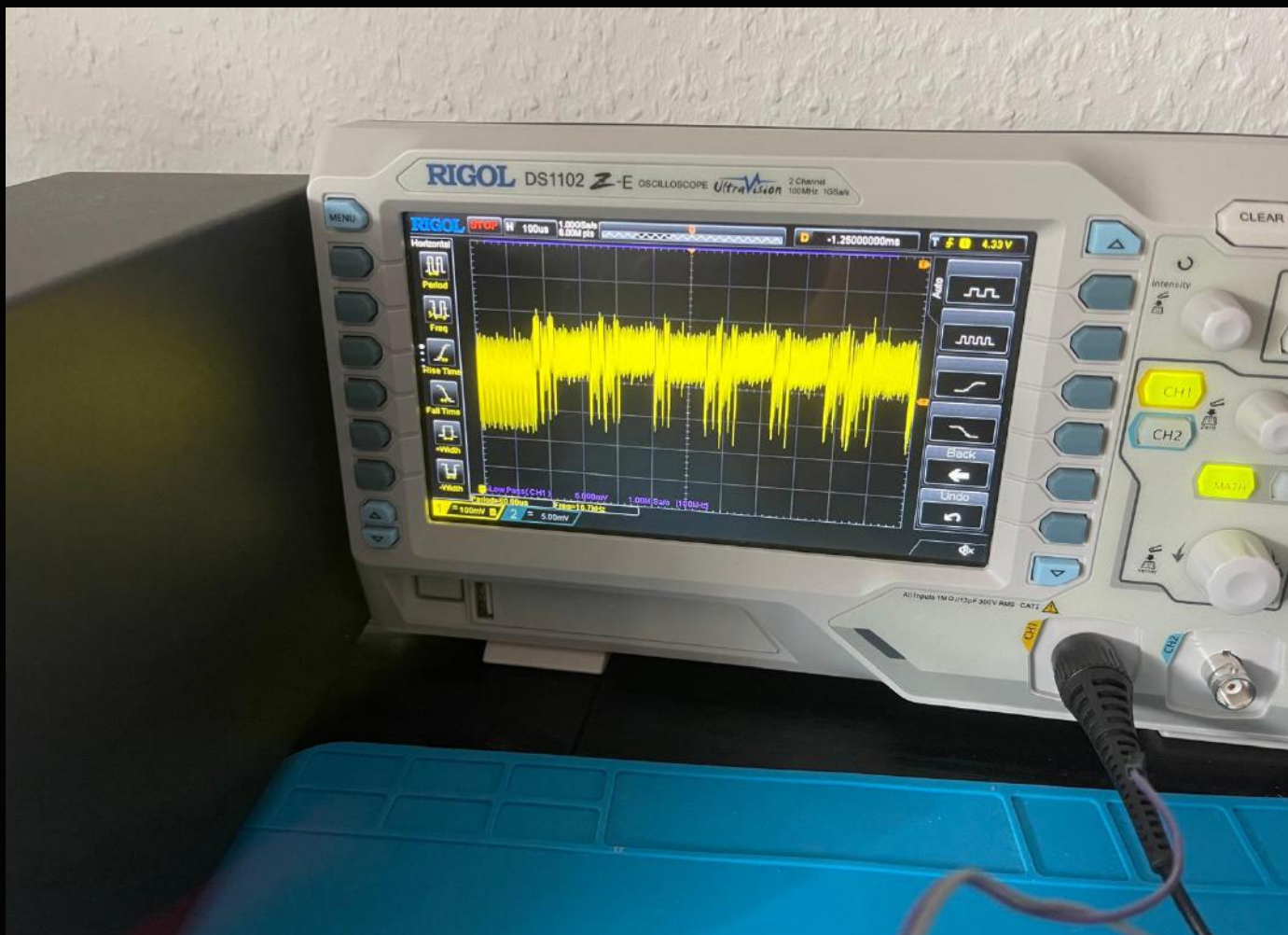
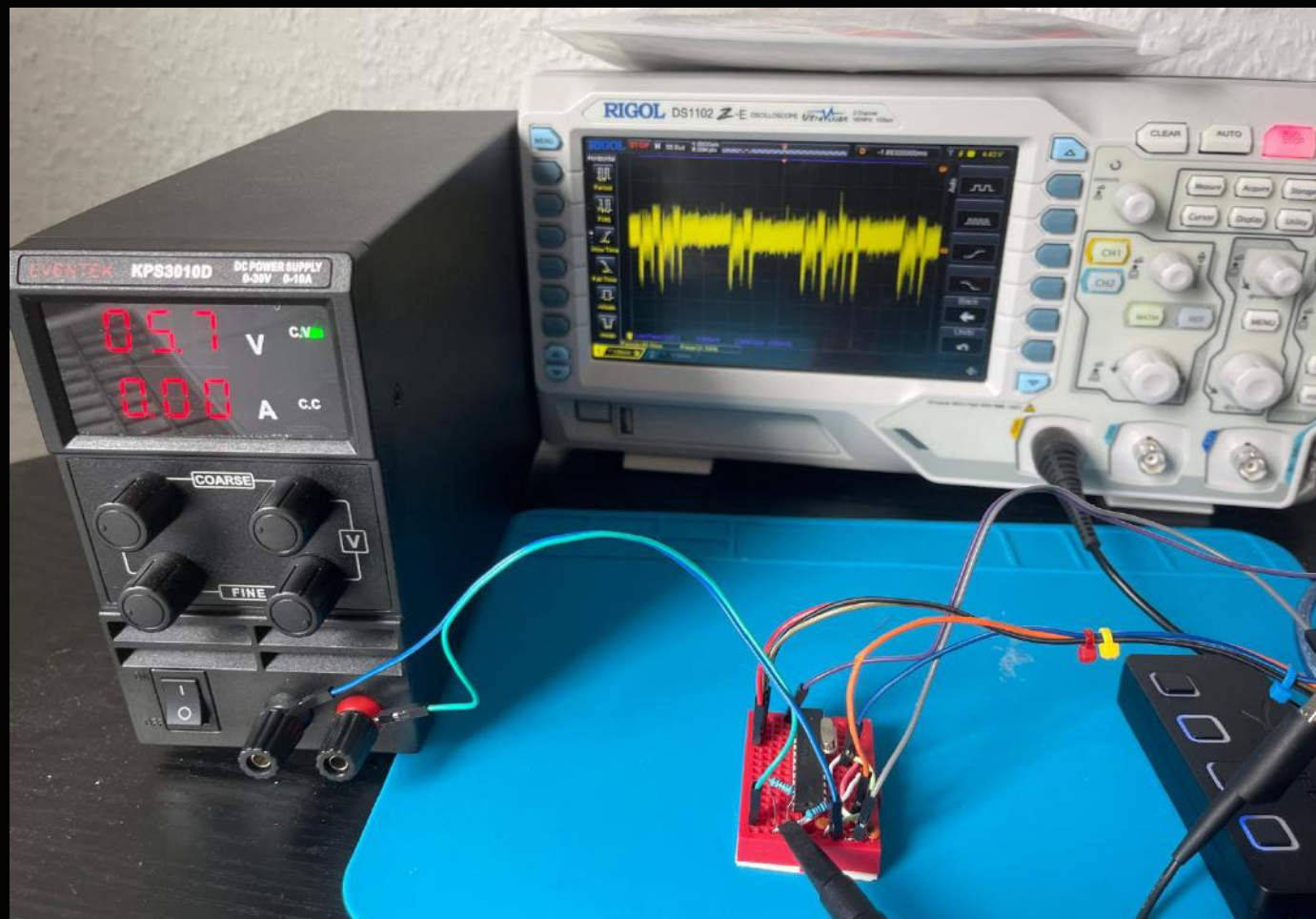
Conclusion

Implementing one's own RSA (Rivest-Shamir-Adleman) encryption system is highly discouraged due to several critical reasons, particularly vulnerability to sophisticated attacks like power analysis attacks.

RSA encryption, while mathematically robust when implemented correctly, requires meticulous attention to detail in its implementation to ensure security

Even minor implementation flaws or oversights can inadvertently leak information about the private key, compromising the entire security of the system.

Furthermore, established cryptographic libraries and frameworks undergo rigorous scrutiny and testing by the security community, ensuring they are resilient against known attacks and vulnerabilities. Using these vetted libraries not only saves time and effort but also significantly reduces the risk of inadvertently introducing vulnerabilities into the system.





security that stands out



HVA

CK
technique





Are you preparing for a Red Team Campaign but need to learn how to craft the narrative for your Social Engineering attacks or the needed Command and Control Infrastructure? Check out this guide.

Concepts

Breaking Down Barriers in Offensive Security
In the world of offensive security, “speaking the same language” isn’t just helpful—it’s crucial. Imagine two professionals trying to discuss a cyber threat but using different terms for the same tactic. Confusion ensues, explanations get long-winded, and the message gets lost in translation. Enter the MITRE ATT&CK Matrix.

More Than Just Words: Uniting the Security Community

The MITRE ATT&CK Matrix provides a standardized vocabulary for describing adversary tactics, techniques, and procedures (TTPs). This common language eliminates misunderstandings and makes communication clear and efficient among security professionals. With everyone on the same page, there’s no need for extra explanations or clarifications.

The ATT&CK Matrix isn’t just about smoother conversations. It’s about:

- Enhancing collaboration across teams and organizations
- Creating more realistic attack simulations
- Refining penetration testing methods
- Accurately describing real-world adversary techniques
- It’s like a language that professionals already speak that helps us all better understand threats during our endeavors to strengthen organizational security.

Putting Theory into Practice: ATT&CK in Action

Let’s dive into how we’ll use this powerful framework:

Mapping Tradecraft to Tactics: We’ll link each technique we discuss to its

corresponding ATT&CK tactic. This isn’t just jargon—it’s your key to understanding each action’s ‘why’ or goal.

From Theory to Practice: For instance, when discussing setting up hacking infrastructure, we’re exploring the “TA0042: Resource Development” phase. It’s like watching a master chef prep their kitchen before the culinary magic begins.

Your Launchpad for Deep Dives : Are you curious about a particular technique? Use its ATT&CK classification as your starting point. It’s like having a treasure map to a wealth of threat intelligence.

Decoding Common Hacking Tutorials: Have you ever wondered about the bigger picture behind those “How to Enumerate Kubernetes” guides? They often fall under “TA0007: Discovery” techniques—the digital equivalent of a burglar casing a joint.

Remember, each ATT&CK tactic is a piece of the puzzle. By understanding how they fit together, you’re not just learning isolated tricks but mastering the art of thinking like a sophisticated threat actor or offensive security professional.

Ready to speak fluent hacker?

Let’s get started!

Command and Control Infrastructure design and deployment - Setting the Stage with MITRE ATT&CK Tactic TA0042: Resource Development

Picture this: You’re a master chef preparing for the culinary battle of your life. What’s your first move? Setting up your kitchen, of course! This crucial prep work falls under the MITRE ATT&CK Tactic “TA0042: Resource Development” in the hacking world.

But what exactly are we cooking up?

Digital Real Estate: Domains that’ll host our secret communication channels

Fake Personas: Email accounts for some sneaky phishing (that's "TA0001: Initial Access" for the ATT&CK aficionados)

Our Secret Lair: Compute resources to orchestrate our sanctioned cyber-shenanigans

Today, we're focusing on that last ingredient - building the perfect hideout for our ethical hacking adventures.

Choosing Your Weapon: The C2 Server

Enter the star of our show: The Command and Control (C2) server. Think of it as your hacker's Swiss Army knife, packed with operations management tools.

For this culinary hacking experiment, we're using the Mythic C2 framework. It's:

- Highly capable with a large number of operational capabilities and features
- Well-maintained with new features being added all the time. Recently, version 3.0 was released.
- Extensible for those who like to tinker and customize
- But remember, Mythic isn't the only framework in town. You could also use:
- Sliver: We keep an Ansible role to install this C2 framework in our repo: <REPO_URL>
- Empire: Relic of yesteryear, but still a powerful option. Requires intensive customization to be evasive and effective in a modern enterprise environment but can be "OK" for a CTF or small lab environment to get around the basics.
- or even your own secret recipe (aka custom solution). I have some industry colleagues who are passionate about this and are working on amazing projects to address this need.

Ready to don your digital chef's hat and start cooking? Let's dive in!

C2 Server Design Considerations

This example is simplified to help us build a foundation that can be expanded over time as you gain more experience and your customer's operational needs evolve.

The first layer- Command-and-Control server layer will consist of the server running the C2 framework of your choice.

This server can be deployed on any primary cloud service provider that supports virtual

machines within your organization's own data center or, for advanced users, adapted to a managed compute service such as Amazon Elastic Container Service (ECS), Amazon Elastic Kubernetes Service (EKS), or Azure Kubernetes Service (AKS).

An affordable and less complex option for beginning practitioners is to use a "free-tier" Amazon Elastic Compute Cloud (EC2). According to EC2 documentation, "Amazon Elastic Compute Cloud (Amazon EC2) provides on-demand, scalable computing capacity in the Amazon Web Services (AWS) Cloud."

Securing Your C2 Server: The Fort Knox of Your Red Team Infrastructure

When setting up your C2 server, security should be your top priority. Here's how to turn your C2 server into an impenetrable fortress:

Complete Isolation: Your C2 server should be completely isolated from all ingress traffic. It's like a secret bunker, inaccessible from the outside world.

Exclusive Access: Only the Red Team Infrastructure specialist should have access to the C2 server. They act as gatekeepers, providing limited access to other operators via the C2 client.

Network Segmentation: The C2 server should be completely segmented from the C2 Redirector. Think of them as two separate islands connected only by a hidden underwater tunnel.

SSH Reverse Port Forwarding Incoming C2 channel traffic is forwarded from the C2 Redirector to the C2 server using SSH reverse port forwarding. This forwarding is directed to the VPN IP address of the C2 server, creating a secure, one-way communication channel.

RSA Key Authentication: The C2 server should only be protected with RSA key login. This provides a secure method of authentication using a public-private key pair. While the key itself doesn't change with each use, it offers significantly stronger security than password authentication. It's like having a complex,



unguessable password that's more difficult to compromise than the "user:password" pair-based authentication.

Strict IP Filtering: Configure the SSH daemon to explicitly deny traffic from any source other than the Red Team Infrastructure specialist's service VPN. It's like having a bouncer who only lets in people with a specific, secret handshake.

Here's a sample sshd_config to illustrate these principles:

```
# /etc/ssh/sshd_config
# Disable root login
PermitRootLogin no
# Disable password authentication
PasswordAuthentication no
# Enable RSA key authentication
PubkeyAuthentication yes
# Only allow RSA key authentication from the
Red Team Infrastructure specialist's VPN
# Ensure that vpn.example.com exists and is
correctly configured before using this setting
AllowUsers redteam_infra_specialist@vpn.
example.com
# If vpn.example.com does not exist, SSH
access will be completely blocked after the
next time sshd is restarted
# Make sure to test this configuration before
applying it in production
# Limit the number of authentication attempts
MaxAuthTries 3
# Set the grace time for users to authenticate
LoginGraceTime 60s
# Disable empty passwords (even though
PasswordAuthentication is already disabled,
this adds another layer of protection)
PermitEmptyPasswords no
# Limit which users can access the SSH server
(redundant with AllowUsers but good for
clarity)
AllowGroups sshusers
# Disable X11 forwarding (graphical interface
forwarding over SSH)
# X11 is a windowing system for Unix-like
systems. Disabling it enhances security by
preventing remote graphical applications
## If they are not needed for your use case
X11Forwarding no

# Allow TCP forwarding for Reverse SSH Port
Forwarding
AllowTcpForwarding yes
# Alternatively, to be more specific:
# AllowTcpForwarding local
# This setting allows local TCP forwarding but
turns off remote TCP forwarding.
# Local forwarding means that SSH clients can
forward their local ports to the SSH server,
# which is necessary for reverse SSH port
forwarding used in this C2 setup.
# By specifying 'local,' we're enhancing
security by preventing the SSH server from
# forwarding its ports to other remote hosts,
which could potentially be exploited.

# Use a more secure set of ciphers and key
exchange algorithms (optional, but strengthens
security)
Ciphers aes256-gcm@openssh.com,chacha20-
poly1305@openssh.com,aes128-gcm@openssh.com
KexAlgorithms curve25519-sha256,curve25519-
sha256@libssh.org,diffie-hellman-group14-
sha256
MACs hmac-sha2-512,hmac-sha2-256
# Disable agent forwarding (if not required)
AllowAgentForwarding no
# Enable logging for debugging and audit
purposes
LogLevel VERBOSE
# This option, when set to 'yes,' tells SSH to
perform strict file ownership and permissions
checks.
# It ensures that the user's home directory,
.ssh directory, and key files are not writable
by other users.
# This helps prevent potential security
vulnerabilities that could arise from
misconfigured permissions.
# For example, if a user's home directory is
world-writable, an attacker could potentially
add their own
# authorized_keys file, granting themselves
unauthorized access. Strict modes prevent such
scenarios.
# Set the maximum time for an unauthenticated
session before disconnecting (e.g., 300
seconds = 5 minutes)
StrictModes yes
ClientAliveInterval 300
ClientAliveCountMax 0
# Optional: Disable SSH protocol forwarding
# Note: This setting does not impact Reverse
Port Forwarding
# PermitTunnel controls the creation of tun/
tap devices for VPN tunneling
# Reverse Port Forwarding uses TCP forwarding,
which is controlled by AllowTcpForwarding
PermitTunnel no
# Optional: Limit max sessions per connection
MaxSessions 2
C2 Redirector Considerations
The second layer- Redirection layer will
consist of at least one web server application
functioning as a reverse proxy, and
optionally, a Content Delivery Network (CDN)
forwarding traffic to a designated "origin"—in
this case, our web server application.
```

While the options for the specific stack are vast and can be daunting if you've never configured a web server before, there's no need to worry. Sticking to the basics will serve us well, and we can rely on the widespread application of Apache 2.

Apache features a mature codebase and more Stack Overflow answers than you'll need to piece this together. Some interesting capabilities that Apache offers for our use case include:

Filtering traffic based on source IP address, "User-Agent" values, HTTP headers in the HTTP requests, and URI paths requested by the client. Additionally, Apache can filter based on:

- The HTTP method (GET, POST, PUT, etc.)
- The presence or absence of specific cookies
- The content of the request body
- The time of day or day of the week
- The protocol version (HTTP/1.0, HTTP/1.1, HTTP/2)
- The presence or absence of specific query string parameters
- The client's SSL/TLS protocol version and cipher suite (for HTTPS connections)

Conditional traffic forwarding based on any attributes above or a combination. This should be easy to understand if you've ever written a basic script using "if"/"else" conditional statements.

For example, if an HTTP request contains a specific "User-Agent" value, it can be redirected to a given domain; if it contains the expected value, it will be sent to the backend C2 server.

Obscuring the technology stack used by our web application to function as a reverse proxy. This is useful when automated scanners, incident responders, or threat hunters attempt to fingerprint the application or domain used in our C2 infrastructure. Apache offers several ways to achieve this:

- Modifying the 'ServerTokens' directive to control the server response header field

- Using the 'ServerSignature' directive to customize or remove the footer on server-generated documents
- Employing mod_security to rewrite or remove headers that might reveal server information
- Altering the 'ErrorDocument' directive to create custom error pages that don't reveal server details
- Configuring mod_headers to add, modify, or remove HTTP response headers
- Adjusting the Apache version string in the configuration files to mislead potential attackers
- Using mod_rewrite to alter URLs and hide the underlying directory structure
- Creating fake directories with misleading names (e.g., "/wordpress," "/Joomla," "/drupal") to suggest a different type of web application
- Enabling directory listing (using 'Options +Indexes') for these fake directories to further reinforce the deception
- Populating these directories with benign files that match the expected structure of the mimicked application

Setting up fake robots.txt and sitemap.xml files to further misdirect automated scanners
Implementing fake login pages or admin panels that lead to honeypot systems
These techniques can significantly increase the difficulty for adversaries in accurately identifying and targeting our C2 infrastructure.

CDN Considerations

If we decide to incorporate a Content Delivery Network (CDN) into our redirection layer, we would benefit from several features and benefits:

Geo-location filtering: When testing an organization in the U.S. or Europe, there must be more reason to allow traffic from regions like the Middle East, Africa, or Asia. CDNs often provide the capability to deny traffic based on location or to explicitly allow traffic only from the regions where our customers will be accessing our infrastructure.

To clarify, the C2 implant or malware we

deliver to our targets as part of our Red Team campaign or Purple Team exercise will need to connect back to our CDN distribution endpoint URL. We can ensure that the CDN permits traffic only from the country where our customer's traffic originates.

Concealment of critical Command-and-Control infrastructure components: Creating and configuring new CDN endpoints to forward traffic to our reverse-proxy Apache web server is relatively straightforward. However, creating, configuring, and provisioning our web application with valid TLS certificates requires more effort than setting up the CDN. By placing a CDN in front of our C2 redirector, we can protect it and increase the overall resiliency of our infrastructure.

Operational security: An option not often discussed in the industry is using the CDN as the exclusive entry point for C2 traffic into the C2 redirector while blocking all other traffic from directly accessing the C2 redirector.

Combined with the previous benefit of concealment, this approach reduces the risk of our most effort-intensive infrastructure components being “burned” or discovered and subsequently categorized as malicious by defenders, threat intelligence providers, or potential attackers.

Scalability: In theory, nothing but budget constraints prevent us from provisioning a theoretically unlimited number of CDN endpoints. We can configure our C2 implant to rotate callbacks among these endpoints, with all traffic being forwarded to our C2 redirector layer.

By combining this capability with providing CDN endpoints across multiple cloud service providers, we achieve an increased resiliency and operational security characteristic of mature Red and Offensive Security teams.

Beyond sheer numbers, this approach enhances resiliency by eliminating single points of failure and providing multiple backups in case Blue Team members block any of our CDN endpoints or an entire provider.

CDNs are not the only option for scalable, resilient, and “disposable” front-ends for our C2 traffic redirection layer. Most Cloud Service Providers (CSPs) offer server-less compute-managed services that can be used to forward traffic based on events or “when” traffic arrives and comes in and bills on a “per-use” basis.

AWS Lambda is an example of this service and can be effectively used to achieve this functionality. See [scottctaylor12/Red-Lambda](#) project for an example implementation.

C2 deployment

You always have the option to purchase all the necessary hardware to run your servers, acquire and provision network connectivity, and handle the racking and stacking in a data center of your choice—approved by the end customer for whom you are delivering the Red Team campaign or Purple Team exercise.

If you work for an internal Red Team, you must obtain approval to acquire and host the hardware in the company's or the organization's private data center. There is no one-size-fits-all solution; different companies have varying policies and requirements, so you must adjust your architecture accordingly.

Some companies may be comfortable with you keeping your Command-and-Control (C2) infrastructure in a private data center, provided you maintain appropriate data stewardship and chain of custody. If you are a consulting company, keeping data separated between campaigns and customers is critical.

We will use Amazon Web Services (AWS) as our cloud service provider for the examples we cover in this article. However, remember that you can apply the concepts demonstrated with any alternative provider, such as Microsoft Azure, Google Cloud Platform, Linode, or DigitalOcean. Terraform has API providers for each of these, and you may alternatively use their respective Cloud Development Kits (CDKs). But... What are CDKs?

Open-source software development

frameworks typically define cloud infrastructure as code using modern programming languages and deploy it through a specific cloud service provider.

On the other hand, Terraform is an infrastructure-as-code tool that lets you build, change, and version cloud and on-premises resources safely and efficiently. Users define and provision data center infrastructure using a declarative configuration language called HashiCorp Configuration Language (HCL), or optionally JSON.

We are leveraging Terraform to deploy our entire C2 infrastructure for the repository linked to this article. This includes:

- **C2 Server:** We use Terraform to provision a dedicated EC2 instance for our Mythic C2 server. This allows us to specify the exact instance type, security groups, and network configuration needed for optimal performance and security.
- **C2 Redirector(s):** Terraform is used to deploy one or more EC2 instances that act as our C2 redirectors. As discussed earlier, these are configured with Apache to handle traffic forwarding and filtering.
- **CDNs:** We utilize Terraform to set up and configure CloudFront distributions, AWS's Content Delivery Network service. This provides us with the geo-location filtering, concealment, and scalability benefits mentioned in the CDN Considerations section.

By using Terraform, we can version control our infrastructure, easily replicate our setup across different environments or AWS regions, and quickly spin up or tear down our entire C2 infrastructure as needed. This approach significantly enhances our operational efficiency and maintains consistency across deployments.

This Terraform project deploys a Command and Control (C2) server and a C2 redirector using AWS EC2 instances. Here's an overview of how it works:

Infrastructure Setup:

The project creates a VPC, subnet, internet gateway, and route table for network infrastructure (virtual_private_cloud.tf).

Security groups are defined for both the C2 server and redirector (security_groups.tf).

EC2 Instances:

Two EC2 instances are created: one for the C2 TeamServer and one for the C2 Redirector (instances.tf).

Both instances use a Kali Linux AMI specified in the variables.

Instance Configuration:

The instances are provisioned with specific instance types, volumes, and network settings. A script is created to update the EC2 instance hostnames (instances.tf, lines 2-38).

SSH Key Management:

SSH keys are generated to secure instances' access (ssh-keys.tf).

Elastic IP Allocation:

Elastic IPs are assigned to the instances for stable, public IP addresses (instances.tf, lines 186-190).

Variables and Customization:

Various deployment aspects are customizable through variables (variables.tf).

Provider Configuration:

AWS provider is configured in the provider.tf.

Outputs:

The public IP addresses of the C2 TeamServer and Redirector are output for easy access (outputs.tf).

Deployment Automation:

A shell script (terra_wrapper.sh) is provided to





automate the Terraform workflow, including initialization, planning, and applying changes.

Key files and their roles:

virtual_private_cloud.tf: Defines network infrastructure, including creating a Virtual Private Cloud (VPC), subnets, internet gateway, and route tables. This file establishes the foundational networking components for secure and isolated cloud resources.

security_groups.tf: Configures security groups, which act as virtual firewalls for EC2 instances. This file defines inbound and outbound traffic rules, specifying which ports are open and to what IP ranges, ensuring proper network security for both the C2 server and redirector.

instances.tf: Creates and configures EC2 instances for the C2 TeamServer and Redirector. This file specifies instance types, AMIs, network interfaces, and user data scripts for initial setup. It also manages the allocation of Elastic IPs for stable, public addressing.

ssh-keys.tf: Manages SSH key generation and association with EC2 instances. This file ensures secure, key-based authentication for accessing the deployed servers, enhancing the overall security posture.

variables.tf: This file defines customizable variables used throughout the Terraform configuration. It allows for easy customization of various deployment aspects, such as instance types, regions, and AMI IDs, without modifying the main configuration files.

provider.tf: Configures the AWS provider, specifying the required version and any global settings. This file sets up the connection to AWS, allowing Terraform to interact with and manage AWS resources. Additionally, it includes a commented-out block for optional storage of the Terraform state in an S3 bucket.

When uncommented and configured with appropriate values, this block enables remote state storage, which is beneficial for team collaboration and state persistence. The block specifies the S3 bucket name, the key for

the state file, and the AWS region where the bucket is located. Users can customize these values to match their specific S3 bucket setup.

outputs.tf: Specifies output values that are displayed after Terraform applies the configuration. This file typically includes essential information like public IP addresses of the deployed instances, making it easy to access and manage the infrastructure.

terrawrapper.sh: Automates the Terraform workflow by providing a shell script that handles initialization, planning, and applying changes. This script streamlines the deployment process, reducing manual steps and the potential for human error.

Explain what is the terraform state file and why it is essential to store it in an s3 bucket or storage other than in the local machine where the terraform commands are being run:

The Terraform state file is crucial as it maintains a record of the current state of the infrastructure managed by Terraform. It includes details such as the resources created, their current attributes, and the relationships between them. This file is essential for Terraform to understand the desired state of the infrastructure and make informed decisions about what changes need to be made to achieve that state.

Storing the Terraform state file in an S3 bucket or other storage solutions offers several benefits:

- **Centralized State Management:** By storing the state file in a centralized location, multiple team members can access and manage the infrastructure state without manually tracking changes or replicating configurations.
- **Version Control:** The state file can be versioned, allowing easy rollback to previous states or comparing configurations. This is particularly useful for debugging and troubleshooting infrastructure changes.
- **Backup and Recovery:** Storing the state

file in a remote location ensures that it is not lost in case of local machine failures or other issues. This provides a backup of the infrastructure state and allows for quick recovery in case of any problems.

- **Collaboration:** Multiple team members can access and modify the state file, allowing collaborative efforts to manage infrastructure. This is particularly useful in team environments where different members are responsible for various aspects of the infrastructure.
- **Security:** Storing the state file in a remote location can enhance security by reducing the risk of unauthorized access to sensitive infrastructure details. This is especially important in multi-tenant environments or when dealing with sensitive data.

By storing the Terraform state file in an S3 bucket or other storage solutions, we can leverage these benefits to streamline the infrastructure management process, enhance collaboration, and ensure the integrity and availability of our infrastructure.

Deploying Infrastructure with terrawrapper.sh
The terrawrapper.sh script simplifies deploying your infrastructure using Terraform. Before using this script, ensure you have set up your AWS CLI with your access and secret keys.

Here's how to do that:

Install the AWS CLI if you haven't already:

Using pip (for Python users)

`pip install awscli`

Using apt-get (for Ubuntu/Debian)

`sudo apt-get update`

`sudo apt-get install awscli`

Using yum

(for Amazon Linux, CentOS, RHEL)

`sudo yum install awscli`

Using Homebrew (for macOS)

`brew install awscli`

Using the bundled installer

(for Windows, macOS, Linux)

1. Download the installer from the AWS website
2. Run the installer
 - For Windows: AWSCLIV2.msi
 - For macOS/Linux: ./aws/install

Configure your AWS CLI with your credentials:

aws configure

This command initiates an interactive prompt to set up your AWS CLI configuration. It will ask you to enter your AWS Access Key ID, Secret Access Key, default region, and output format. Here's what the process looks like:

```
$ aws configure
```

```
AWS Access Key ID [None]:
AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]:
wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY
Default region name [None]: us-east-1
Default output format [None]: json
```

After configuration, you can verify your settings using:

```
$ aws configure list
```

This command will display your current AWS CLI configuration. Here's an example output:

Name	Value	Type	Location
profile	<not set>	None	None
access_key	*****	ODNN7	shared-credentials-file
secret_key	*****	iCYEX	shared-credentials-file
region	us-west-2	config-file	~/.aws/config

This output shows:

The profile being used (if any)

The access key and secret key (partially hidden for security)

The configured region

The location of these settings (usually in ~/.aws/credentials and ~/.aws/config files)

You'll be prompted to enter your AWS Access Key ID, Secret Access Key, default region, and output format.

Once your AWS CLI is configured, you can use the terrawrapper.sh script to deploy your infrastructure. Here's how to use it:

Make the script executable:

```
chmod +x terrawrapper.sh
```

Run the script:

```
Usage: terrawrapper.sh
[--deploy|--destroy]
[--workspace <workspace-name>]
[--plan-file <plan-file-name>]
```

Arguments:

```
--deploy
Deploy the Terraform infrastructure.
--destroy
Destroy the Terraform infrastructure.
--workspace <workspace>
Specify the Terraform workspace to use or create.
--plan-file <plan-file>
Specify the name of the plan file.
```

Examples:

Deploy infrastructure in the default workspace:

```
terrwrapper.sh --deploy
```

Destroy infrastructure in the default workspace:

```
terrwrapper.sh --destroy
```

Deploy infrastructure in a specific workspace:

```
terrwrapper.sh --deploy --workspace dev
```

Destroy infrastructure in a specific workspace:

```
terrwrapper.sh --destroy --workspace dev
```

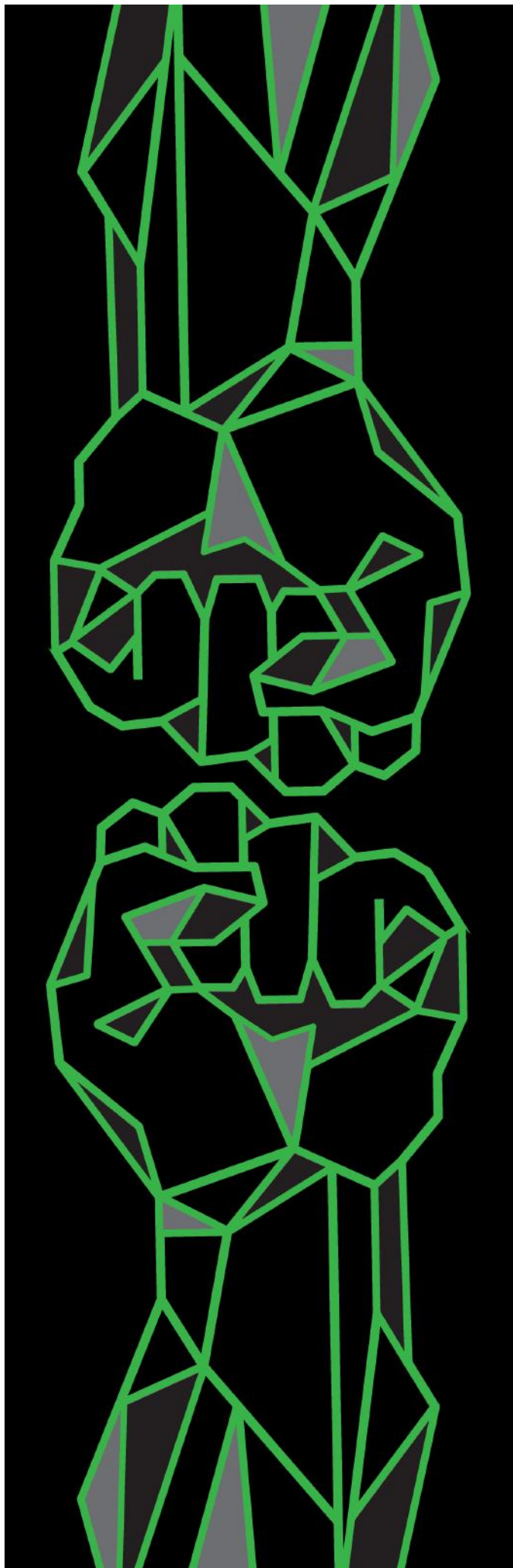
Deploy infrastructure with a specific plan file:

```
terrwrapper.sh --deploy --plan-file my_plan.tfplan
```

The script will perform the following actions:

```
Initialize Terraform (terraform init)
Create a Terraform plan (terraform plan)
Apply the Terraform configuration (terraform apply)
```

Example commands:



Deploy the Terraform infrastructure
`terrwrapper.sh --deploy`
`--workspace HVCK_x_HackerHermanos_`
`Is_Where_ITS_AT --plan-file`
`HVCK_x_HackerHermanos_Is_Where_`
`ITS_AT.tfplan`

This command does the following:

1. `--deploy`: Indicates we want to create or update our infrastructure
2. `--workspace HVCK_x_HackerHermanos_Is_Where_ITS_AT`: Specifies a unique Terraform workspace for this project
3. `--plan-file HVCK_x_HackerHermanos_Is_Where_ITS_AT.tfplan`: Names the Terraform plan file for this specific deployment

Destroy the Terraform infrastructure
`terrwrapper.sh --destroy`
`--workspace HVCK_x_HackerHermanos_`
`Is_Where_ITS_AT --plan-file`
`HVCK_x_HackerHermanos_Is_Where_`
`ITS_AT.tfplan`

This command does the following:

1. `--destroy`: Indicates we want to tear down our infrastructure
2. `--workspace HVCK_x_HackerHermanos_Is_Where_ITS_AT`: Uses the same workspace as the deploy command
3. `--plan-file HVCK_x_HackerHermanos_Is_Where_ITS_AT.tfplan`: Uses the same plan file as the deploy command

C2 configuration

After deploying our assets, we need to configure them. This can be easily accomplished using scripting languages like Bash or Python. In our demonstration, we utilize Ansible playbooks and roles. While scripts written in Python or Bash can be structured to install desired capabilities in a modular fashion—using patterns like cases and switches activated by user-provided arguments (e.g., “`--c2-framework Mythic`” or “`--redirector-webserver Apache`”)—I believe Ansible simplifies this process through its use



of roles.

Ansible roles can be employed in playbooks to install only the capabilities we want on the specific hosts we designate.

For example, we can use one Ansible role to install the Mythic C2 framework exclusively on our C2 server, another role to install Apache and configure it to forward our C2 traffic solely on our C2 redirector, and another role to install the Zsh shell, customize it with a user-provided “.zshrc” file, apply a theme like “powerlevel10k”, and more on all C2 infrastructure as a quality-of-life enhancement.

The takeaway of my point above is that we can pick and choose “what” we want installed and “where” in a straightforward manner.

Mythic C2: From Manual to Automated
Have you ever wished you could apply scientific precision to setting up your C2 server? Well, lab coat on, because we’re about to conduct a breakthrough experiment!

The Hacker Hermanos Formula

Sure, you could follow the official Mythic C2 docs and input commands like it’s 1999. Or... you could use our cutting-edge Ansible Role!

Access the Mythic C2 Ansible Role [here](#)

What’s in Our Lab?

Our Ansible Role is like a well-calibrated machine that does all the heavy lifting for you.

Here’s our scientific process:

- Acquiring the Specimen: Downloads Mythic C2 with electron-speed efficiency
- Synthesizing the CLI: Builds and tests the Mythic C2 CLI, ensuring optimal functionality
- Cloning Agents: Replicates your chosen Mythic C2 Agents, ready for deployment
- Engineering Profiles: Extracts the Mythic C2 Profiles you’ve selected, tailored to your specifications

Why Use Our Automated Approach?

- Efficiency: Deploy infrastructure rapidly and consistently
- Simplicity: Reduce manual configuration steps and potential for human error
- Reproducibility: Ensure identical setups across multiple deployments
- Reliability: Benefit from version-controlled, tested, and community-reviewed code
- Customizability: Easily adapt the setup to specific requirements through parameterization
- Scalability: Manage multiple C2 instances with minimal additional effort

Ready to transform your C2 setup from guesswork to a precise science? Let’s analyze the data!

C2 Redirector Configuration

Imagine a one-way mirror for your C2 traffic. That's what redirectors do:

- Securely proxy C2 traffic from target to listeners
- Keep your actual C2 hidden from prying eyes
- Easy to deploy and dismantle - like pop-up labs!

Redirector Species: A Field Guide

Redirectors come in various forms, each with unique properties:

socat: A simple yet versatile tool for creating bidirectional data transfers

iptables: A powerful firewall utility for network traffic filtering and NAT

CDNs: Global distribution networks that can forward traffic to a controlled origin server

Serverless functions: Scalable, event-driven compute services like AWS Lambda or Azure Functions

Reverse proxies: Intermediary servers that forward client requests to backend servers
Today, we're focusing on two high-powered specimens:

Content Delivery Networks (CDNs)

mod_rewrite module from Apache

These lab-tested redirectors offer scalability and fine-grained control!

Goals of the ansible role redirector setup

- Proxy legitimate C2 traffic to backend servers while filtering out unwanted requests
- Implement traffic filtering rules to block or redirect suspicious or non-C2 traffic
- Configure HTTPS using valid SSL/TLS certificates from trusted Certificate Authorities

- The Perfect Catalysts: CDNs and Apache mod_rewrite

To achieve these goals, we're using a combination of CDNs and Apache with mod_rewrite:

- **CDNs:** Globally distributed network of servers that cache and deliver content, capable of efficiently routing and redirecting traffic
- **Apache mod_rewrite:** A powerful and flexible URL manipulation engine that uses rule-based rewriting to alter incoming URL requests
- These technologies provide the necessary capabilities for implementing a robust and scalable redirector setup for the Command and Control (C2) infrastructure.

Imagine a web server that exists in multiple states simultaneously. That's mod_rewrite:

- Transparently proxies or redirects based on regex matches
- Makes 'amazonss.com' appear as 'amazon.com' - unless it's our C2 traffic
- Collapses the wavefunction only when our C2 traffic hits the server

Hat tip to @bluescreenofjeff for his groundbreaking research in this quantum realm!

We're using Ansible to deploy our redirectors - it's like quantum entanglement for your infrastructure:

- Agentless, operating purely through SSH tunnels
- Configs as YAML: the quantum state of your infrastructure

Ansible: A Quantum Primer

- **Playbooks:** The Wave Functions of Infrastructure
- YAML configs defining the quantum state of your servers
- Specify hosts, tasks, and variables
- Dive into the quantum foam of playbooks

- Roles: Quantum Entanglement for Reusability
- Organize playbooks into reusable structures
- Our redirector role: the fundamental particle of C2 infrastructure
- Explore the quantum realm of roles ready to manipulate the quantum state of your C2 infrastructure? Let's dive into the subatomic particles of our redirector setup!

Getting Started

To begin using the Ansible Redirector and Tailscale Kali Roles:

Include the Roles in Your Playbook

- hosts: C2 Redirector setup roles:
 - redirectors
 - tailscale_kali

Customize Variables

For the redirector role:

- Open the file: /path/to/ansible_roles/redirectors/vars/main.yml
- Modify the variables as needed

For the tailscale_kali role:

- Open the file: /path/to/ansible_roles/tailscale_kali/vars/main.yml

Add your Tailscale authentication key:

- tailscale_authkey: "tskey-XXX-XXX-XXX-XXX"

Note: Replace "XXX-XXX-XXX-XXX" with your actual Tailscale auth key.

Run the Playbook

Example:

```
ansible-playbook /tmp/project/ansible/C2_Redirector_playbook.yml  
-i '192.168.1.100, ' --private-key  
/path/to/ssh_key.pem --extra-vars  
'role_specific_var'
```



```
ansible-playbook /path/to/playbook.  
yaml -i 'target_ip, ' --private-key  
/path/to/private_key.pem
```

Note: Keep your Tailscale authentication key secure, and do not commit it to version control.

Key Features

tailscale_kali Role

- **Idempotency:** The role checks if Tailscale is already installed and only proceeds with installation if necessary.
- **Error Handling:** Uses `ignore_errors` and `failed_when` directives to handle potential issues gracefully.
- **Security:** Uses `no_log` to prevent sensitive information (like the auth key) from displaying in logs.
- **Flexibility:** Allows customization through variables, particularly the `tailscale_authkey`.
- **Comprehensive Checks:** Performs various checks to ensure Tailscale is appropriately installed, connected, and functioning.
- **redirectors Role**
- **Apache Configuration:** Installs and configures Apache web server with necessary modules.
- **SSL/TLS Support:** Integrates Let's Encrypt for automatic SSL certificate generation and renewal.
- **Virtual Host Management:** Allows for easy creation and management of multiple virtual hosts.
- **Modular Design:** Separates tasks into logical units (`apache.yml`, `letsencrypt.yml`, `vhosts.yml`) for improved maintainability.
- **Template-based Configuration:** Uses Jinja2 templates for flexible and customizable Apache configurations.
- **Security-focused:** Implements best practices for secure web server configuration.
- **Redirector Rules:** Easily configurable redirector rules using `mod_rewrite` for traffic management.
- **Role Requirements Checklist**

Before we dive into creating our Ansible Role for redirector provisioning, let's outline the essential requirements:

- **Apache Installation:** Ensure Apache is installed with the necessary modules
- **Apache Configuration:** Set up configurations for our redirectors using `vhosts` for domain-specific settings
- **Redirector Rules Implementation:** Install redirector rules in the Apache config's `vhost` section, avoiding `.htaccess` files
- **Let's Encrypt Setup:** Install Let's Encrypt and `python-certbot-apache` on the target servers
- **SSL Certificate Configuration:** Configure Let's Encrypt to generate legitimate public certificates for our sites

Preparing for Role Creation

With our requirements defined, we're ready to begin constructing our role. This role will serve as the foundation for our redirector infrastructure, determining how each task interacts with the others to create a cohesive, secure system.

The Quantum Dance of Specificity and Flexibility

As we choreograph our Ansible roles, we perform a delicate quantum dance between specificity and flexibility. It's like Heisenberg's uncertainty principle, but for infrastructure:

- The more precisely we define our tasks, the less adaptable our role becomes
 - The more general we make our role, the less precise our configurations may be
- We're aiming for that sweet spot—a role that's both powerful and adaptable, ready to gracefully pirouette through various deployment scenarios.

Ready to compose the symphony of your infrastructure? Let's orchestrate our Ansible roles!

Ansible roles, like a well-organized toolbox, use a specific folder structure. Behold the atomic structure of our redirectors role:

roles/redirectors/

```
├─ files           # Static files, ready for
deployment
├─ handlers       # Event handlers, waiting
to be triggered
├─ tasks          # The primary act - our
to-do list
├─ templates      # Jinja2 templates, the
shape-shifters of our setup
└─ vars           # Variables, the spice of
infrastructure life
```

But wait, there's more! Our playbook isn't just about redirectors. It's a double feature that also stars our VPN setup. For the Tailscale VPN role, we're rolling out the red carpet with this structure:

roles/tailscale_kali/

```
├─ defaults/      # Default variables, the
understudies of our play
|   └─ main.yml
├─ handlers/      # More handlers, because
one can never have too many
|   └─ main.yml
├─ meta/          # Metadata, for those who
like to read the credits
|   └─ main.yml
├─ tasks/         # The main event for our
VPN setup
|   └─ main.yml
├─ vars/          # VPN-specific variables,
the secret sauce
|   └─ main.yml
└─ README.md      # The playbill for our
infrastructure show
```

With these roles, our playbook becomes a blockbuster production, seamlessly integrating redirectors and VPN setup. It's infrastructure as code meets Hollywood—lights, camera, automation!

Folder Significance in Roles

Each folder serves a specific purpose within a role:

tasks: Contains all the tasks to be executed

files: Stores static files to be transferred to the managed nodes

templates: Houses Jinja2 templates

handlers: Defines handlers that tasks can call

vars: Specifies variables for the role

Task Execution in Roles

Ansible automatically executes the main.yml file in the tasks folder when importing or including a role in a playbook.

Streamlining Our Infrastructure Setup

Clarity is critical when organizing Ansible tasks. Instead of cramming everything into a single main.yml file, we're taking a more innovative approach by breaking tasks into logical, manageable chunks.

Our playbook is designed to install and configure two critical components: redirectors and the Tailscale VPN. Here's how we've organized the tasks for our redirectors role:

- Apache Setup: Installing and configuring the web server
- Let's Encrypt Configuration: Securing our connections with SSL certificates
- Virtual Host Deployment: Applying our custom configuration templates

For the Tailscale VPN role, we follow a similar pattern of organized, modular tasks.

This structured approach offers several benefits:

- Improved readability: Each file focuses on a specific aspect of the setup
- Enhanced maintainability: Updates and troubleshooting become more straightforward
- Greater flexibility: It's easier to reuse or modify individual components

By thoughtfully organizing our tasks, we're not just writing code - we're building a robust, scalable foundation for our infrastructure. This method ensures that our Ansible roles remain precise, efficient, and adaptable to future needs.

Directory Breakdown

- defaults/: Contains the default variables for the role.
- handlers/: Defines handlers that can be triggered by tasks (e.g., restarting Apache).
- tasks/: Holds the main tasks to be executed by the role.
- templates/: Stores Jinja2 templates used for generating configuration files.
- vars/: Contains variables specific to the role.
- files/: Includes static files to be transferred

to the managed nodes.

- **README.md:** Provides information about the role and its usage.

Tasks

The main tasks are organized into three separate files for better readability and maintainability:

- **main.yml**
Purpose: Acts as the entry point for the role.
Functionality: Includes other task files.
- **apache.yml**
Purpose: Handles the installation and configuration of Apache.
Functionality:
Installs Apache and necessary modules.
Configures virtual hosts for redirectors.
- **letsencrypt.yml**
Purpose: Manages Let's Encrypt certificate provisioning.
Functionality:
Installs Let's Encrypt and python-certbot-apache.
Configures SSL certificates for the virtual hosts.

Templates

The role utilizes several Jinja2 templates to generate Apache configuration files dynamically:

`apache_sslvhost.conf.j2`

Description: Template for SSL virtual host configuration.

`apache_vhost.conf.j2`

Description: Template for HTTP virtual host configuration.

`pre_cert_apache_sslvhost.conf.j2`

Description: Template for SSL virtual host configuration before certificate provisioning.

`pre_cert_apache_vhost.conf.j2`

Description: Template for HTTP virtual host configuration before certificate provisioning.
Variables

Variables are defined in both `vars/main.yml` and `defaults/main.yml`, allowing for customization and flexibility:

- **Virtual Hosts Configuration:** Settings for each virtual host, including domain names and document roots.
- **Backend Servers:** Details of backend servers to which traffic should be proxied.
- **SSL Settings:** Configuration options for SSL certificates and HTTPS settings.

Additional Files

`redirect.rules`

Contains Apache rewrite rules for redirecting traffic based on specific criteria. This file is based on CuriousJack's `htaccess` file, which provides a comprehensive set of rules for filtering and redirecting web traffic. It includes:

- A configurable destination URL for redirects
- Exclusions for large IP ranges from cloud providers like Azure and AWS - You'll have to ensure that these IP ranges are up to date for scanners and relevant source IPs are not excluded so you don't block your own C2 traffic coming from the CDN or other redirectors.
- Filters for various web crawlers and bots like Virus Total, expanse, Palo Alto scanners, A/V sandboxes vendors, etc
- Specific rules for services like Barracuda and Slack
- A list of TOR exit nodes to block These rules allow for fine-grained control over which traffic reaches the actual content and which is redirected, enhancing security and operational efficiency.
- **README.md:** Provides detailed information about the role, including setup instructions and usage examples.

Role Functionality

The Ansible redirectors Role performs the following key functions:

- Apache Installation
- Ensures Apache is installed with the necessary modules for redirecting and proxying traffic.

- Apache Configuration
- Set up virtual hosts for each domain using the provided Jinja2 templates.
- Redirector Rules Implementation
- Installs Apache rewrite rules directly in the virtual host configuration to manage traffic redirection efficiently.
- Let's Encrypt Installation and Configuration
- Installs Let's Encrypt along with python-certbot-apache to automate the provisioning of SSL certificates.
- Configures Apache to use the obtained SSL certificates, enabling secure HTTPS communication.

The tailscale_kali role is designed to install and configure Tailscale VPN on a Kali Linux system. Here's a breakdown of its main functions:

Validating Tailscale Installation:

- Check if Tailscale has already been installed on the system.
- Package Signing and Repository Setup:
- Adds the Tailscale package signing key and repository if not already present.
- Package Management:
- Removes existing Tailscale packages to prepare for a fresh installation.
- Tailscale Installation:
- Installs the latest version of Tailscale.
- Service Management:
- Enables and starts the Tailscale daemon/service.
- VPN Connection:
- Connects the machine to the Tailscale VPN network.
- Status Checking:
- Verifies the Tailscale connection and retrieves the assigned IP.
- Output the Tailscale status for confirmation.
- Flexibility and Customization

The redirectors, tailscale_kali, and c2 roles are all designed with flexibility as a core principle. They support multiple virtual hosts and allow you to customize configurations using variables.

Want to set up a simple redirector or a VPN connection or deploy a command and control server? These roles have you covered.

Remember, this is just a starting point - you can easily modify or expand these roles to fit your needs.

Whether you're following strict security policies or need to add new features, tweak the variables you're set. The goal here is to give you a solid foundation that you can build upon for any scenario you might encounter.

Bridging Infrastructure and Social Engineering

With our C2 infrastructure, redirectors, and VPN setup, we've laid the technical foundation for our operation. However, the most sophisticated technical setup is only as effective as the social engineering campaign that leverages it. This is where the art of pretexting comes into play, bridging the gap between our technical preparations and the human element of our target.

As we transition from infrastructure to execution, it's crucial to approach the social engineering phase with the same level of meticulousness and attention to detail. As we carefully configured our C2 servers and redirectors, we must now craft our pretexts methodically.

Ready to dive deeper into the art of tactical pretexting?

Ready to dive deeper into the art of tactical pretexting?

INFLUENCE OPS

TACTICAL
PRETEXTING



Take advantage of Jeff Tomkiewicz's groundbreaking InfluenceOps series, which was brought to you in collaboration with Hacker Hermanos. Join us as we explore the intricate world of social engineering and learn how to create pretexts that are not just believable but irresistibly compelling. Buckle up – your journey into the psychology of influence is about to begin!

InfluenceOps: Tactical Pretexting

Written by

The Gh0stface_ Killer

Before we dive in, let's be crystal clear: the strategies and techniques we'll be covering are for research and professional purposes only, and should only be used when you have legal authorization to do so.

The Foundations of Effective Pretexting
Definition and Evolution in Offensive Security
Pretexting is one of the essential techniques in social engineering. Pretexting involves an attacker creating a fake story or taking on an identity to trick a target into revealing sensitive information or allowing unauthorized access.

For pretexting to work, the attacker has to

create and maintain a believable story that fits the target's expectations, beliefs, and environment.

This tactic isn't new; it has deep roots in history. Spies from ancient times used disguises or fake stories to sneak into enemy camps, gather intel, or sabotage operations. In those cases, interactions happened face-to-face, where the attacker would pretend to be a trusted official, colleague, or service provider. The success of these early methods relied heavily on the attacker's ability to blend into the environment, understand social norms, and communicate convincingly. Psychological skills and an understanding of human behavior played key roles.

As science, technology, and communication have advanced, we've adapted these age-old techniques to the modern world.

- » Today, pretexting has moved beyond face-to-face interactions and expanded into digital and telecommunication spaces. It's scalable now, allowing attackers to target multiple individuals or organizations at once. Borrowing insights from marketing and behavioral science, pretexting has become a powerful tool in Red Team engagements, helping test the defenses of complex organizations.
- e Pretexting has transformed from a simple, localized tactic into a sophisticated component of modern offensive security. This shift reflects broader changes in how we communicate and interact today. Modern pretexting requires more than just creating a false narrative—it's about crafting an entire experience that leverages trust, authority, and psychological principles. As technology continues to evolve, so will pretexting tactics.

Ethical Considerations and Red Team Protocols

While pretexting has been used for many purposes throughout history, today, as professionals, we have a responsibility to approach it ethically. Pretexting is a powerful tool and needs to be used carefully, especially considering these concerns:

Trust and Deception: Pretexting inherently involves lying, which can create ethical conflicts.

Emotional and Psychological Impact: Pretexting can play on people's fears and anxieties, especially when impersonating authority figures in the company or potentially delivering bad news (Ex: HR cutting some company perks).

Important: NEVER impersonate law enforcement or any civil servant authority figure. This can get you into serious legal trouble, even if the client gives you permission.

Consent and Awareness: In some Red Team engagements, not all employees are aware that a security test is happening. This is done to make the scenario more realistic.

Because of these concerns, it's essential to stay within ethical and legal boundaries:

Legal Compliance: Always ensure that pretexting activities are within the law. Avoid actions that could be seen as fraud, identity theft, or illegal impersonation.

Client Agreement: Red Team activities, including pretexting, should be explicitly authorized by the client in a legally binding agreement.

Protection of Personal Data: Any personal data collected during pretexting must be handled securely, and data protection laws must be followed.

How to Stay Ethical in Pretexting:

Client Consent and Scope Definition: Clearly define the scope of the engagement, including the types of pretexts you will use, and ensure everything is documented and agreed upon. Informed consent is key. While not everyone in the organization might be aware of the test, senior leadership (such as the Chief Information Security Officer) should be.

Minimizing Harm: Use pretexts that are non-

distressing and avoid causing significant emotional or psychological harm. Be sure to offer debriefings and support after the operation to clear up any confusion.

Data Protection and Confidentiality: Handle any collected data with care—use encryption and limit access. When reporting to clients, anonymize sensitive information to protect privacy.

Ongoing Training: Red Team members should receive regular training in ethics and legal compliance to make sure they understand the full implications of their actions and can make ethical decisions in the field.

Pretexting is powerful, but it's ethically complex. By following strict guidelines, securing client consent, minimizing harm, and protecting data, Red Teams can effectively conduct operations while maintaining a commitment to ethical conduct.

Core Elements of Pretexting

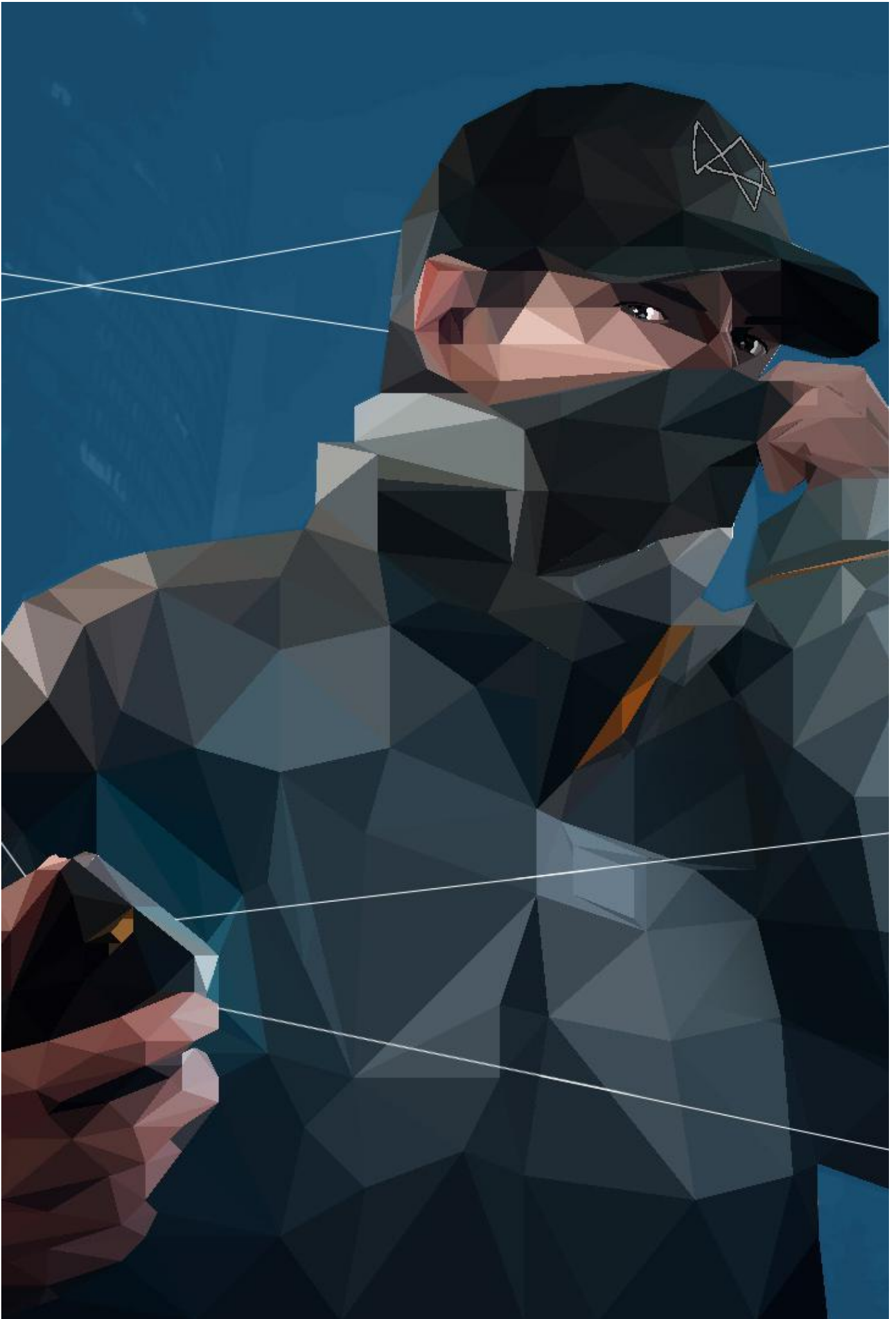
Now, let's explore the core elements that form the foundation of believable and effective pretexts in social engineering:

Deep Research and Intelligence Gathering
When building a pretext, there are three critical elements:

Foundation of Credibility: Success hinges on how believable your pretext is. The more authentic you appear, the more likely the target will engage with you—whether it's clicking a link or resetting an MFA device to your control. This is where deep research and intelligence gathering are essential.

Minimize Red Flags: Detailed research helps you avoid common mistakes that might expose your pretext, like failing to understand company jargon or misrepresenting key details.

Tailored Approach: Every pretext should be customized based on the intelligence gathered. Intelligence drives operations, and the same applies when creating a pretext.



There are two main methods for gathering intelligence:

Human Intelligence (HUMINT): Information gathered from human sources, like social engineering calls, networking events, or insider interviews.

Open Source Intelligence (OSINT): Information collected from public sources, like social media, company websites, or press releases. After analyzing this data, you can decide how to act on it.

By combining OSINT and HUMINT, social engineers can build highly credible and tailored pretexts. The focus should always be on developing strong research and analytical skills rather than relying solely on tools.

Building Complex and Layered Personas

Creating a believable persona is key to successful social engineering. If your persona feels authentic, people are more likely to trust you.

Start by defining your goal:

What is the purpose of the persona? Is it to gain access to a building or extract sensitive information?

Who is the target audience? Knowing who the persona will interact with is crucial to shaping it.

Once the objective is clear, gather intelligence using HUMINT and OSINT. Look for opportunities where your persona can fit into the target environment. Next, build a backstory:

Personal History: Develop a plausible backstory for your persona that fits with the target's expectations.

Professional Credentials: Ensure your persona's credentials align with their role in the pretext.

Current Context: Explain why the persona is reaching out now.

Next, develop a communication style that reflects the target's industry norms. Finally, test and refine the persona to ensure it's consistent and believable.

Crafting Realistic Scenarios with Supporting Evidence

To make a pretext truly effective, you need to create a realistic scenario with supporting evidence. Here's how:

Start with an End Goal: Define the outcome you want while keeping the target's roles and behaviors in mind.

Incorporate Realistic Context: Use current events and organizational culture to shape your pretext.

Create a Plausible Storyline: Keep it simple but include emotional hooks to prompt a response.

Support the pretext with "props," such as spoofed emails or fake documents, to add authenticity.

Conclusion - Part 1

By paying attention to detail and constructing well-thought-out scenarios, social engineers can create pretexts that lead to the desired outcome while minimizing detection risks.

Part 2 - Mastering the Art of Pretexting

Case Studies: Effective Pretexts

Analysis of Successful Pretexts

Real-world examples are invaluable for understanding what makes a pretext truly effective. Below, we'll dive into a few case studies from different areas, such as corporate espionage, phishing campaigns, and physical penetration tests. These examples will help illustrate how a well-crafted pretext can exploit psychological factors and specific contexts to achieve its goals.

Corporate Espionage:

Imagine a scenario where an attacker poses as an IT consultant during a corporate merger. The pretext is that they need access to systems to ensure compatibility between the merging companies. This approach works because it plays on the urgency

and complexity of the merger, a time when employees are more likely to bypass normal security protocols to keep operations running smoothly.

The Renault Espionage Scandal (2011)

Overview: In 2011, French car manufacturer Renault became embroiled in a corporate espionage scandal. Three senior executives were accused of selling company secrets about Renault's electric vehicle program to foreign entities. However, it later turned out that these executives were victims of a sophisticated pretexting campaign.

The Pretext: The attackers used a series of pretexts to convince Renault's top security officers that these executives were leaking information. This included fake bank accounts in Switzerland, supposedly tied to bribes, and fabricated evidence of espionage. The attackers posed as anonymous informants, providing Renault with false information about the supposed leaks.

Why It Was Effective: The pretext was effective because it exploited Renault's fears of industrial espionage—a legitimate concern in the highly competitive automotive industry. The attackers provided just enough convincing "evidence" to lead Renault's security team to believe that the executives were guilty, prompting them to take drastic actions based on the false narrative.

Lesson Learned: The key takeaway here is the importance of verifying the authenticity of information, especially when it comes from unknown or unverified sources. Organizations must be careful not to act hastily based on incomplete or manipulated data, which can lead to significant internal damage.

Phishing Campaigns:

In another case, a phishing email was sent to employees of a financial institution, disguised as an urgent message from the CEO about a new security protocol. The email included a link to a fake login page designed to capture credentials. This pretext succeeded because it leveraged the authority of the CEO and the urgency of the message, two factors that often lead individuals to act without fully scrutinizing the request.

The Target Data Breach (2013)

Overview: In late 2013, the retail giant Target suffered one of the largest data breaches in history, compromising the personal and financial information of over 40 million customers. The breach was traced back to a phishing email sent to one of Target's third-party HVAC vendors.

The Pretext: The attackers sent a phishing email that appeared to be a routine communication from a trusted source within Target. The email contained a link to what appeared to be a legitimate login page, but it was actually a phishing site designed to capture the vendor's credentials. Once the attackers had access to the vendor's network, they used it as a gateway to penetrate Target's internal systems.

Why It Was Effective: The phishing campaign succeeded because it targeted a vendor with lower security protocols than Target itself. By using a seemingly benign and routine email, the attackers exploited the trust between Target and its vendors. The attackers understood that third-party vendors are often a weak link in a company's security chain.

Lesson Learned: This case highlights the importance of securing the entire supply chain, not just the internal network. Organizations should ensure that all third-party vendors adhere to strict security standards and that their credentials are regularly monitored and updated.

Physical Penetration Tests:

A physical penetration tester successfully gained access to a secure facility by posing as a delivery person. Armed with a uniform and a clipboard, they claimed to have a package for a high-ranking executive, which required a signature. The security guards, not wanting to disrupt the executive's day, allowed the tester inside without the usual checks. This worked because it exploited the trust placed in service personnel and the perceived importance of the delivery.

The Bank of England Test (2018)

Overview: In 2018, the Bank of England conducted a physical penetration test as part of a broader effort to evaluate and improve its



security measures. The test was carried out by a team of professional security consultants who were tasked with gaining unauthorized access to the bank's sensitive areas.

The Pretext: The penetration testers used various pretexts to gain entry, including posing as delivery personnel, maintenance workers, and even as employees who had "forgotten" their security badges. One particularly effective tactic involved the testers posing as IT technicians who needed to repair critical equipment. By exploiting the perceived urgency of the situation, they convinced security staff to grant them access to secure areas without the usual verification process.

Why It Was Effective: The pretext worked because it played on the sense of urgency and the perceived authority of the testers posing as IT staff. In a high-stakes environment like the Bank of England, the security team was focused on avoiding disruptions to critical operations, leading them to bypass standard procedures in the face of an urgent technical issue.

Lesson Learned: This test demonstrated the importance of training security personnel to recognize social engineering tactics, even in high-pressure situations. It also reinforced the need for strict access control procedures, regardless of the perceived urgency or authority of the individual requesting access.

Lessons Learned

Each of the case studies above offer valuable lessons for anyone looking to craft effective pretexts:

Psychological Leverage: Successful pretexts often tap into basic psychological principles, like authority, urgency, or the desire to help. Understanding these triggers can make your pretexts much more convincing. Go ahead and grab yourself a copy of "Influence" by Dr. Robert Cialdini and study away.

Contextual Awareness: The context in which the pretext is deployed is critical. What works in one industry or situation might not succeed in another. For example, financial institutions may require a more formal approach, while a

tech startup might respond better to a casual, innovative angle.

Tailoring Strategies: Different industries and target profiles will require unique strategies. It's important to adapt your approach based on the specific environment, culture (see Contextual Awareness), and typical behaviors of your target.

How to Practice Crafting a Pretext

Crafting effective pretexts isn't just about theory—it's about practice, young grasshopper. The more you practice, the better you'll get at creating believable scenarios that can fool even the most vigilant of targets. Here are some crafty ways on how you can hone your pretexting skills:

Simulation Exercises

Simulation exercises are a great way to practice pretexting in a controlled environment, allowing you to experiment without real-world consequences. Think of a boxer using shadowboxing. Finally, just be sure to have permission from the appropriate parties before going off and trying any of these:

Setting Up Simulations:

Start by defining clear objectives for your simulation, such as testing the effectiveness of a phishing email or seeing if you can gain physical access to a secure area. Choose scenarios that reflect real-world situations you might encounter.

Types of Scenarios:

Over the Phone: Practice calling targets under a pretext that requires them to provide information or perform an action, like verifying account details or resetting a password.

In Person: Simulate physical pretexts by role-playing scenarios like visiting an office as a delivery person or technician.

Email: Craft phishing emails with various pretexts, such as pretending to be a colleague in need of urgent help or an IT department requesting security updates.

Importance of Feedback:

After each exercise, gather feedback from participants or colleagues. What worked well? What raised suspicion? Use this feedback to refine your approach and improve your skills.

Tools and Techniques for Practice

Several tools and techniques can help you develop and test your pretexts effectively:

Software Tools:

Use platforms like Canary Tokens to create tracking links and documents that alert you when they've been accessed, allowing you to measure the success of your pretexts. PhishMe by Cofense and similar platforms offer environments to test phishing campaigns, helping you to fine-tune your emails for maximum effectiveness.

Role-Playing:

Engage in role-playing exercises with colleagues or within a red team. Assign roles where one person plays the target while the other tries to execute the pretext. This helps you anticipate responses and think on your feet. One tool I personally use at my disposal: improv classes.

Mock Exercises:

Conduct mock social engineering attacks within your organization (with proper authorization) to test different pretexts in a safe, controlled manner. This provides real-world experience without the risks of an actual engagement.

Building Confidence

Deploying a pretext in a live operation requires not only skill but also confidence. Here are some tips to help you build that confidence:

Start Small: Begin with simpler pretexts in low-stakes situations. As you succeed, gradually move on to more complex and high-risk scenarios.

Learn to Improvise: No pretext goes exactly as planned, so be prepared to adapt on the fly. Practicing improvisation in role-playing exercises can help you stay calm and think creatively when the unexpected happens.

Stay Calm Under Pressure: The key to successful pretexting is maintaining

composure, even when things don't go as expected. Deep breathing techniques and mental rehearsals can help you manage nerves and maintain control during an engagement.

Part 2 - Conclusion

Crafting effective pretexts is both an art and a science. By studying successful examples, practicing in controlled environments, and building your confidence, you can develop the skills needed to create believable scenarios that achieve your objectives. Remember, the most effective pretexts are those that seamlessly blend into the target's world, making them question nothing while you achieve your goals.

References

1. Corporate Espionage Example: The Renault Espionage Scandal
Erlanger, S. (2011, March 14). Renault apologizes over botched spy case. The New York Times. <https://www.nytimes.com/2011/03/15/world/europe/15renault.html>

2. Phishing Campaign Example: The Target Data Breach
Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014, March 13). Missed alarms and 40 million stolen credit card numbers: How Target blew it. Bloomberg. <https://www.bloomberg.com/news/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data>

3. Physical Penetration Test Example: The Bank of England Test
Burgess, M. (2018, April 26). How the Bank of England stays secure in a time of cyber threats. Wired UK. <https://www.wired.co.uk/article/bank-of-england-cyber-security>

Part 3 - Pitfalls, Tips, and Tricks

As we wrap up this InfluenceOps: Tactical Pretexting article, it's time to dive into the challenges and common mistakes that can derail even the most well-planned pretexting operations. In this third and final part, we'll also explore pro tips to help you fine-tune your techniques and maximize the effectiveness of your social engineering engagements. Finally,

we'll look at the future of pretexting in the evolving landscape of offensive security. It's so bright you got to grab your shades...

Common Pitfalls and Pro Tips

Common Pitfalls in Pretexting

Even the best social engineers like D.B. Cooper, can fall into some common traps that can jeopardize the success of a pretext. Understanding these pitfalls is key to avoiding them during your pretexting efforts.

Overcomplicating the Scenario

The Issue: One of the most frequent mistakes is creating a pretext that's overly complex. An elaborate backstory with too many moving parts can be hard to keep track of and may raise suspicion. The more complicated your story, the higher the chance you'll slip up or be questioned about inconsistencies. So stop obsessing over your targets cool dog and leave them out the pretext.

How to Avoid It: Keep your pretexts simple and believable. Stick to details that align with the target's world and avoid adding unnecessary elements. Focus on crafting a realistic and direct story that fits naturally into the target's context, such as a common business problem or a service request that doesn't require too much explanation.

Inconsistent Persona Details

The Issue: Inconsistencies in the persona's background, communication style, or role can quickly unravel your pretext. For example, using the wrong industry jargon or forgetting key aspects of the persona's backstory can raise red flags for the target. Similarly, switching between formal and informal language inappropriately can create suspicion. So probably in best interest to hold off on the persona of being a cowboy astronaut millionaire.

How to Avoid It: Thorough preparation is crucial. Create a persona with a consistent and detailed backstory that you can easily recall. Practice sticking to this narrative in all communications, whether over the phone, in person, or through email. If possible, rehearse

your interactions with a colleague to ensure you can maintain consistency throughout the engagement.

Poor Timing

The Issue: Timing can make or break a pretext. If you attempt to deploy a pretext during a busy period or at an inconvenient time for the target, you may meet resistance or even hostility. For instance, sending an urgent email late at night or making a phone call during a crucial meeting can cause the target to question the legitimacy of the interaction. In this case, I would call at 4 PM on a Friday afternoon. They will love you for it. Promise...

How to Avoid It: Do your homework on the target's schedule and industry patterns. Consider the timing of your pretext carefully—ensure it feels natural and doesn't disrupt their daily workflow. Pay attention to key moments in the company's calendar, such as quarterly reviews, deadlines, or significant events like product launches, and align your pretext with the target's availability.

Pro Tips for Effective Pretexting

Experienced social engineers have developed several advanced techniques to enhance the success of pretexts. These tips can help you refine your approach and avoid common pitfalls.

Adaptability and Improvisation

Why It Matters: No matter how much planning goes into your pretext, you can't always predict the target's responses. Being adaptable and able to improvise is critical when things don't go according to plan.

Tip: Stay calm and think on your feet. If the target asks an unexpected question or challenges your pretext, don't panic. Respond confidently, using elements of the pretext that are flexible enough to handle minor deviations. Improvisation skills can make the difference between success and failure in a pretexting operation. I highly recommend taking a Improv 101 class. Most places have these types of classes and usually not too expensive.

Real-Time Feedback Adjustments

Why It Matters: Pretexting is dynamic, and you must be able to adjust your approach based on real-time feedback. If the target seems suspicious or hesitant, it's important to modify your strategy on the fly. Time to pull out the Sex Panther and increase those odds...

Tip: Pay close attention to verbal and non-verbal cues. Is the target rushing the conversation, showing impatience, or probing too much into your backstory? Adjust your approach to either offer more detail (if they seem interested) or streamline the conversation (if they seem busy or skeptical). The ability to pivot mid-interaction is a powerful skill in social engineering.

Staying Calm Under Pressure

Why It Matters: Social engineering often involves high-stress situations, especially when interacting with security-conscious individuals. If your persona is questioned, or your pretext begins to falter, maintaining composure is crucial.

Tip: If there is one thing I can stress..... Confidence is key!!!! Even if things aren't going smoothly, keep your voice steady, and avoid defensive or evasive language. Practice handling objections or tough questions ahead of time so you can respond confidently without breaking character. If necessary, be prepared to gracefully exit the situation without revealing the ruse—knowing when to retreat can save a pretext from full exposure. I have been in these situations and holding my ground quickly got them to drop their guard and cooperate.

Post-Engagement Reflection and Refinement

Why It Matters: After a pretexting engagement, reviewing what worked and what didn't is essential for improving your skills. Reflection helps you identify areas for improvement and refine your approach for future engagements.

Tip: Conduct a post-mortem analysis after every engagement. Take notes on the target's reactions, any deviations from the plan, and how well the pretext held up. Was there a particular moment when things felt shaky?

Did the target question certain details? Use these insights to refine your pretext for future attempts, ensuring it becomes stronger each time like the hands and skill of the great Pei Mei!

Conclusion: The Art and Science of Pretexting

Pretexting, at its core, is a delicate blend of art and science. The science lies in the data-driven research, psychological insights, and structured approach to building personas and scenarios. The art is in the delivery—how well you can adapt, improvise, and engage the target while maintaining believability. Throughout this series, we've explored the critical elements that make pretexts successful, the common pitfalls to avoid, and tips to elevate your skills.

Recap of Key Concepts

Let's take a nice walk together and recap what we have learned together over the past 3 articles:

Deep Research: Crafting a convincing pretext begins with thorough reconnaissance and intelligence gathering. Understanding your target's environment, behaviors, and pain points is essential.

Building Personas: Effective pretexting requires complex, layered personas that align with the target's expectations. Consistency and realism are key.

Scenario Crafting: The scenarios in which you deploy your pretext should be simple, believable, and supported by strong evidence.

Pitfalls and Pro Tips: Avoid common mistakes like overcomplicating your story or poor timing. Adaptability, confidence, and constant refinement are the hallmarks of a successful social engineer.

Looking Ahead: The Future of Pretexting
As social engineering continues to evolve, so too will the tactics and strategies behind pretexting. Emerging Trends in AI-driven tools, deepfakes, and social media manipulation are

creating new opportunities—and challenges—for attackers and defenders alike. Pretexts may increasingly incorporate more advanced psychological manipulation, as well as the use of fake personas that are bolstered by digital footprints across multiple platforms.

In the face of these developments, staying ahead of the curve will require continuous good old fashion learning and adaptation. Security professionals must keep refining their techniques, staying updated on the latest technology, and learning from both successes and failures. More importantly, ethical considerations must remain at the forefront. As offensive security practitioners, we have a responsibility to use pretexting tactics within legal and authorized contexts.

Final Thoughts

Pretexting is a powerful tool in the arsenal of social engineers. When executed thoughtfully and ethically, it can uncover critical vulnerabilities in both digital and physical security systems.

The art of pretexting lies in its ability to blend seamlessly into the target's world, manipulating human behaviors in subtle and sophisticated ways.

As you continue to hone your pretexting skills, remember that this craft requires both preparation and agility—and that ethical practice should always guide your approach.

Stay tuned for more articles focused on the art of Social Engineering with a future release of my full hands on course : InfluenceOps: Tactical Social Engineering currently in development.

Jeff Tomkiewicz
The_Gh0stface_Killer





NO F

TALES IN

SPYGLASS, the JAM, RAMONES.
K-RAY SPEX, BLONDIE, BUZZCOCKS
& MORE!

MAINT. EXPERIENCE
CHIMPS+RINE
CHILDREN
HUNG MONEY

SCHE-CON PRE

PAINTED CV

HELLBOASTARDS
energetic Thrashers based in London
SERIOUS BRUISES
regulars!

FUTURE

OF BACK
THE DAY

SENTS:
POWERED

AS WILL RISE

924 GILMAN STR

DON'T FORGET
YOUR MEMBERSHIP
CARDS!

punk show melet

OUT! TOUR 8
RECORDS
SHRINE
DINER

The Christ on a Cross
Show is NO Longer
At Post Road Commun
Center

WED Aug.

CHRIST ON A CROSS
FROM W

FROM Ca. GREEN DAY

Also TRUSTY \$5

FAIR



ere it's back in
e day, all day,
ery day.

UPRE

• This new section of HVCK aims to pull
from hackings past to reveal what may
lay in the future for as you will see
the more things change, the more they
stay the same.

Enjoy



and the Dawn of CyberWarfare

By d8t8r



In the late 1980s, as the world edged closer to the digital revolution, a silent war was brewing in the uncharted realms of cyberspace.

This is the story of how a seemingly innocuous message turned into a cyber onslaught that challenged some of the most advanced minds at NASA and the Department of Energy (DOE). It's a tale of hackers, worms, and the vulnerabilities that shook the foundations of early networked systems.

The Prelude: Father Christmas Worm

On December 22, 1988, deep within the corridors of NASA's Goddard Space Flight Center in Washington, D.C., system managers discovered a peculiar file named hi.com on their network. This file was more than just a festive greeting—it was the Father Christmas Worm, a program written in Digital Command Language (DCL) that targeted the Space Physics Analysis Network (SPAN).

SPAN was NASA's operating network, connecting various teams and facilities across the country. Built on the infrastructure provided by the Digital Equipment Corporation (DEC), SPAN used DECnet protocols and VAX computers, which were powerful but lacked robust security measures.

The worm propagated by searching for random node numbers within the DECnet network. Once it located a valid node, it attempted to gain access using default or weak credentials—often the default username and password decnet/decnet. If successful, it copied itself to the target system, deleted the original file to cover its tracks, and waited until a specific time to execute its payload: sending a whimsical Christmas message to all users on the system.

While the Father Christmas Worm was relatively benign, serving more as a festive prank than a malicious attack, it exposed glaring security flaws within NASA's network. System administrators were urged to enforce stronger passwords and implement better security protocols. However, these warnings would soon prove insufficient.

The WANK Worm Emerges

Less than a year later, on October 16, 1989, NASA employees preparing for a space shuttle launch were greeted with an unsettling message on their screens:

WANK

Your system has been officially WANKed.

You talk of times of peace for all and then prepare for war.

The WANK Worm—an acronym for Worms Against Nuclear Killers—was more than a nuisance. It was a sophisticated piece of malware that shared structural similarities with the Father Christmas Worm but carried a more ominous payload.

Using the same DECnet vulnerabilities, the WANK Worm exploited default accounts with weak credentials like system/system and field/field. Once inside a system, it altered login scripts to display its manifesto and simulated file deletions, causing panic among users who believed their data was being erased in real-time.



The Chaos Unfolds

John McMahon, the systems manager for SPAN, and Kevin Oberman, a network manager at a DOE lab in San Francisco, spearheaded the investigation into the worm. Their tasks were made more challenging due to the lack of a comprehensive network map and outdated contact information for key personnel.

As the worm spread, it caused significant disruptions—not by destroying data but by exploiting human psychology. The simulated deletions led some users to take drastic measures, including reinitializing their systems and inadvertently causing actual data loss.

Complicating matters further, the Jet Propulsion Laboratory (JPL) decided to disconnect from SPAN to prevent infection. However, this move disrupted critical network pathways, isolating segments of NASA's network and hindering coordination efforts to combat the worm.

The Earthquake and the Anti-Worm

On October 17, 1989, as Oberman was finalizing an anti-worm program to combat WANK, the Loma Prieta earthquake struck the San Francisco Bay Area. Amidst the chaos, he managed to distribute his solution, which cleverly tricked the worm into self-destructing by mimicking its process identification.

However, the relief was short-lived. Five days later, a more resilient version of the WANK Worm surfaced. This iteration was immune to Oberman's fix and actively destroyed any decoy processes designed to thwart it. It also changed user passwords, locking administrators out of their own systems.

Assistance came from Bernard Perrot, a systems manager at the French National Institute of Nuclear and Particle Physics. Perrot developed WANK_SHOT, an anti-worm that exploited the worm's reliance on the `writelist.dat` file—a directory of user accounts. By replacing this file with a decoy containing a hidden trap, Perrot's solution neutralized the worm's second version. Two weeks later, the WANK Worm was effectively

eradicated.

The Larger Context: NASA's Struggles

The WANK Worm incident occurred during a tumultuous period for NASA. The Challenger disaster in 1986 had already tarnished the agency's reputation, highlighting managerial failures and lapses in safety protocols. The upcoming launch of the Galileo spacecraft, which carried plutonium-based power sources, faced public outcry and legal challenges from anti-nuclear activists.

The WANK Worm's anti-nuclear message seemed to align with the sentiments of these activist groups, suggesting a politically motivated attack. The worm's ability to infiltrate critical systems on the eve of a significant launch underscored the vulnerabilities inherent in NASA's network infrastructure.

Tracing the Culprits: The Realm and Australian Hackers

Investigations into the WANK Worm pointed toward Australia, primarily due to linguistic clues and cultural references embedded in the worm's code. The term "wank" is British slang, more commonly used in Commonwealth countries, and the worm's internal processes included names like OILZ, a reference to the Australian band Midnight Oil.

This led authorities to focus on a group of Australian hackers known as The Realm, which included notorious figures like Phoenix (Nahshon Even-Chaim) and Electron (Richard Jones). Operating from Melbourne, these hackers had already made names for themselves by breaching numerous high-profile systems, including universities, corporations, and government agencies.

Their activities were characterized not by financial gain but by the pursuit of intellectual challenge and, at times, ideological statements. The WANK Worm's anti-nuclear stance and its method of operation bore the hallmarks of The Realm's *modus operandi*.

NASA OFFICE OF MANAGEMENT	INFORMATION RESOURCES MANAGEMENT
SPACE PHYSICS ANALYSIS NETWORK (SPAN) WORM INCIDENT	
DESCRIPTION OF ATTACK	
• ORIGIN TRACED TO FRANCE • WORM CODE: - EXPLOITS POOR PASSWORD MANAGEMENT PRACTICES - NASA VICTIMS FAILED TO FOLLOW PUBLISHED AGENCY POLICIES AND PROCEDURES - CAUSES - DISRUPTION AND DENIAL OF SERVICE - EXPENDITURE OF RESOURCES TO TECHNICALLY DIAGNOSE AND DISINFECT AFFECTED SYSTEMS - DISPLAY OF BANNER ON USER SCREENS • TWO PHASED ATTACK - OCT 16 ATTACK AFFECTED APPROXIMATELY 99 NODES - OCT 29 ATTACK AFFECTED OVER 500 NODES - USED IMPROVED VERSION TO EXPLOIT ADDITIONAL PASSWORDS • SPECIFIC IDENTIFICATION OF PENETRATED NODES UNDERWAY - ONLY 3 IDENTIFIED AT NASA TO DATE • ATTACK IS STILL ACTIVE	

NASA OFFICE OF MANAGEMENT	INFORMATION RESOURCES MANAGEMENT
SPACE PHYSICS ANALYSIS NETWORK (SPAN) WORM INCIDENT	
EFFORTS TO REDUCE FUTURE RISK EXPOSURE	
• INSTRUCTIONS BEING REISSUED TO ALL NODE MANAGERS TO STRENGTHEN PASSWORD MANAGEMENT PRACTICES • SELECTED NETWORK NODES (NASA AND NON-NASA) WILL BE AUDITED TO ASSURE COMPLIANCE WITH PASSWORD MANAGEMENT INSTRUCTIONS • NASA/IG AND FBI ARE INVESTIGATING FOR PROSECUTION	
HOWEVER	
• OPEN INTERNATIONAL NETWORKS WILL ALWAYS HAVE A CERTAIN LEVEL OF VULNERABILITY	

NASA OFFICE OF MANAGEMENT	INFORMATION RESOURCES MANAGEMENT
SPACE PHYSICS ANALYSIS NETWORK (SPAN) WORM INCIDENT	
WORMS AGAINST NUCLEAR KILLERS	
	
Your System Has Been Officially WANKed	

NASA OFFICE OF MANAGEMENT	AFFIRMATIVE ACTION PROGRESS REPORT FISCAL YEAR 1990
FY 1990-1992 COMMITMENT/TARGET	ACTION PLAN/ TARGET/DATE
• ESTABLISH OFFICE OF MANAGEMENT EQUALITY CIRCLE • SEPARATE EQUAL OPPORTUNITY AND MULTI-CULTURAL EDUCATION PROGRAM TRAINING FOR ALL EMPLOYEES • AVERAGE 1 PROFESSIONAL DEVELOPMENT TRAINING INCIDENT PER EMPLOYEE PER YEAR • DEVELOP CAREER COMPETENCY DEVELOPMENT PROGRAM PHOT PROJECT • MEET OR EXCEED 20% MINORITY MALE AND FEMALE PROFESSIONAL WORKFORCE (FTE, CO-OP, AND PMR) REPRESENTATION GOAL ESTABLISHED AS A RESULT OF THE MEAN AGREEMENT • INCREASE NUMBER OF MINORITY FEMALE EMPLOYEES AT OR ABOVE GS-14 FROM 6 TO 3	- FIRST MEETING SCHEDULED DECEMBER 5, 1989 - HAVE REQUESTED PROGRAM DEVELOPMENT DISCUSSIONS WITH CODE DP TO START BY EARLY DECEMBER 1989 - DEVELOP PROACTIVE CODE IN STRATEGY FOR MINORITY RECRUITMENT BY JANUARY 31, 1990

Operation Dabble: The Hunt for the Hackers

In response to the escalating cyber intrusions, the Australian Federal Police (AFP) launched Operation Dabble in 1988. This operation was groundbreaking—it was Australia's first major investigation into computer hacking and cybercrime. At the time, Australian law did not adequately address crimes committed via computers. Recognizing this gap, the government swiftly enacted the necessary legislation in June 1989, marking a significant milestone in Australian legal history. The new laws provided law enforcement with the authority to investigate and prosecute cybercrimes, setting a precedent for future cases.

Using a combination of traditional detective work and innovative surveillance techniques, the AFP identified key members of The Realm, including Phoenix and Electron. Undercover agents infiltrated hacker circles, and informants provided critical information that helped build a case against the suspects.

One of the significant challenges faced by the AFP was the technical limitations of the time. Capturing digital evidence required novel solutions, as existing technology was insufficient for intercepting data transmissions at the speeds necessary. The AFP collaborated with technical experts to develop new methods for data interception and analysis, effectively pioneering techniques that would become standard in cybercrime investigations.

In January 1990, armed with warrants, the AFP began tapping the phone lines of Even-Chaim and Jones. Over the next two months, they collected substantial evidence, including recorded conversations where the hackers openly discussed their activities, boasted about infiltrating high-profile systems like NASA, and expressed disdain for law enforcement's inability to catch them.

The Trials: An Australian First

The arrests in March 1990 marked the culmination of Australia's first significant cybercrime investigation under the new legislation. The subsequent trials were closely watched, not only because of the high-profile nature of the offenses but also because they would set legal precedents for how cybercrime was prosecuted in Australia.

Nahshon Even-Chaim faced 48 charges related to unauthorized access, property damage, and theft of data. Richard Jones faced 15 similar charges. The court proceedings delved into uncharted legal territory, addressing questions about the nature of digital evidence, the definition of property in the context of data, and the appropriate sentencing for crimes that were, at the time, poorly understood by the general public.

During the trial, prosecutors presented extensive evidence collected through wiretaps and data interception, demonstrating the hackers' extensive unauthorized access to computer systems across the globe. The defense argued that the accused were merely curious youths with no malicious intent, highlighting the lack of financial gain from their activities.

In a landmark decision, the court handed down its verdicts in 1993. Even-Chaim was convicted and sentenced to 12 months in prison, along with 500 hours of community service. Jones received a lighter sentence of six months in prison and 300 hours of community service. These sentences were considered lenient by some, given the scope of their

activities, but the judge took into account their young age and the novelty of the crimes.

The trials were a watershed moment in Australian legal history. They were the first successful prosecutions under the newly enacted computer crime legislation, setting important legal precedents. The cases underscored the need for robust cybersecurity measures and the importance of updating legal frameworks to keep pace with technological advancements.

The Legacy of the Trials

The successful prosecution of Phoenix and Electron had far-reaching implications. It signaled to the international community that cybercrime would not be tolerated and that law enforcement agencies were capable of adapting to new technological challenges. The methods developed during Operation Dabble became a blueprint for future cybercrime investigations, both in Australia and abroad.

Moreover, the trials highlighted the psychological and social factors contributing to hacking. Both Even-Chaim and Jones were young, intelligent individuals who became deeply engrossed in the world of hacking, partly as an escape from personal struggles. Their cases prompted discussions about the ethical responsibilities of technologists and the importance of providing positive outlets for talent in computing.

The Australian government's proactive approach in legislating and enforcing cybercrime laws ahead of many other nations positioned the country as a leader in cybersecurity policy. The events also spurred organizations to reevaluate their security practices, leading to improvements that would help protect against future threats.

The Legacy of the WANK Worm

While definitive proof linking The Realm to the WANK Worm was never publicly disclosed, the incident marked a pivotal moment in cybersecurity history. The WANK Worm was one of the first pieces of malware to carry a political message, demonstrating that code could be used as a form of protest or activism.

Moreover, the attacks exposed systemic vulnerabilities in networked systems, particularly those relying on default configurations and lacking proper segmentation. The ease with which the worm spread highlighted the necessity for robust security practices—a lesson that resonates in today's increasingly connected world.

Technical Analysis: How the Worms Exploited DECnet

Both the Father Christmas and WANK Worms exploited inherent weaknesses in DECnet Phase IV networks. Key vulnerabilities included:

Default Credentials: Many systems retained default usernames and passwords (decnet/decnet, system/system), providing easy access for unauthorized users.

Remote Task Loading: DECnet allowed for remote execution of tasks, which the worms leveraged to propagate themselves without needing physical access.

Lack of Network Segmentation: The networks were flat, meaning a breach in one area could rapidly spread to others, exacerbating the impact.





The worms used random node scanning to discover other systems within the network. Upon gaining access, they would attempt to:

Check for Existing Infection: To prevent multiple instances on the same system, the worm would look for specific process names (NETW_, OILZ).

Copy and Execute Payload: If the system was uninfected, the worm would copy itself over and execute, modifying login scripts and displaying messages.

Cover Tracks: The original files were deleted after execution to minimize detection.

Mitigation Strategies Implemented

In the wake of these attacks, several critical security measures were adopted:

Password Policies: Enforcing the change of default credentials and promoting the use of strong, unique passwords.

Network Segmentation: Dividing the network into isolated segments to contain breaches and prevent widespread propagation.

Security Auditing Tools: Development and deployment of software to monitor network activity, detect anomalies, and respond swiftly to threats.

User Education: Training personnel on cybersecurity best practices to reduce the risk of social engineering and human error.

Conclusion: The Dawn of Cybersecurity Awareness

The WANK Worm incident was more than a disruptive event; it was a seminal moment that heralded the complexities of a new digital era. It exposed the fragile underpinnings of early networked systems and highlighted the profound implications of cybersecurity—or the lack thereof—in a world becoming increasingly dependent on interconnected technologies.

This event underscored that cybersecurity is not solely a technical challenge confined to firewalls and encryption algorithms; it is intrinsically a human issue. The vulnerabilities exploited by the WANK Worm were as much about system misconfigurations and default passwords as they were about human oversight, complacency, and a lack of awareness. Even organizations staffed with some of the brightest minds—rocket scientists and nuclear physicists—were not immune to basic security lapses.

By embedding an anti-nuclear message within its code, the worm demonstrated that software could be wielded as a tool for political expression and protest, one of the earliest instances of hacktivism. This was a precursor to the modern landscape of cyber activism, where groups leverage digital means to advance social and political agendas on a global scale.

The trials of Phoenix and Electron were groundbreaking—not just for Australia but for the international community. They were Australia's first significant prosecutions under newly minted cybercrime laws, setting legal precedents and providing a framework for how nations could address the burgeoning threat of cyber offenses. The successful



investigation and prosecution showcased the necessity of updating legal systems to keep pace with technological advancements and the importance of international cooperation in combating cyber threats.

For organizations worldwide, the incident was a stark reminder of the critical importance of robust cybersecurity measures. It led to increased investment in security infrastructure, the development of more secure network protocols, and a greater emphasis on user education and awareness. The vulnerabilities that allowed the WANK Worm to propagate so effectively—weak passwords, lack of network segmentation, and insufficient monitoring—became focal points for security improvements.

As we reflect on the WANK Worm incident today, its lessons remain profoundly relevant. Cyber threats have evolved dramatically, becoming more sophisticated, targeted, and damaging. The rise of ransomware, state-sponsored cyber espionage, and advanced persistent threats illustrate that the challenges identified in the late 1980s have not only persisted but have intensified.

The foundational lessons are clear:

Vigilance is Crucial: Organizations must maintain constant vigilance, regularly updating and patching systems, monitoring for unusual activity, and staying informed about emerging threats.

Human Factors Matter: Employee training and awareness are vital. Users are often the first line of defense, and their actions can either mitigate or exacerbate security risks.

Legal Frameworks Need Evolution: Laws and regulations must adapt to address the changing landscape of cyber threats, providing law enforcement with the tools necessary to respond effectively.

International Cooperation is Essential: Cyber threats do not respect national borders. Collaborative efforts between nations, sharing intelligence and resources, are necessary to combat global cybercrime effectively.

Ethical Considerations: As technology becomes more integrated into daily life, ethical considerations around privacy, surveillance, and the use of technology for activism



become increasingly important.

The WANK Worm incident serves as both a historical milestone and a cautionary tale. It reminds us that technology, while empowering, also presents risks that must be managed proactively. The balance between innovation and security is delicate, requiring thoughtful strategies that encompass technical solutions, human factors, and policy considerations. By studying incidents like the WANK Worm, cybersecurity professionals, policymakers, and organizations can better anticipate challenges, develop more effective defenses, and foster a culture that prioritizes security.

As we move forward, embracing new technologies like artificial intelligence, the Internet of Things (IoT), and quantum computing, the lessons from the late 1980s remind us that the fundamentals of cybersecurity remain unchanged. Protecting our digital infrastructure requires a commitment to continuous improvement, adaptability, and a recognition that security is a collective responsibility.

The WANK Worm was not just an attack on NASA's network; it was a wake-up call to the world. It highlighted the interconnectedness of our systems and the potential

for individuals or small groups to impact global operations significantly. In honoring the lessons learned, we pay homage to the early challenges faced and reaffirm our commitment to securing the digital frontier for future generations.

About the Author

d8rh8r is a Security Consultant and writer with a passion for uncovering the hidden stories of the digital underworld. With a focus on historical cyber incidents, they aim to shed light on the evolution of cyber threats and the importance of robust security practices.

HACK

HACK