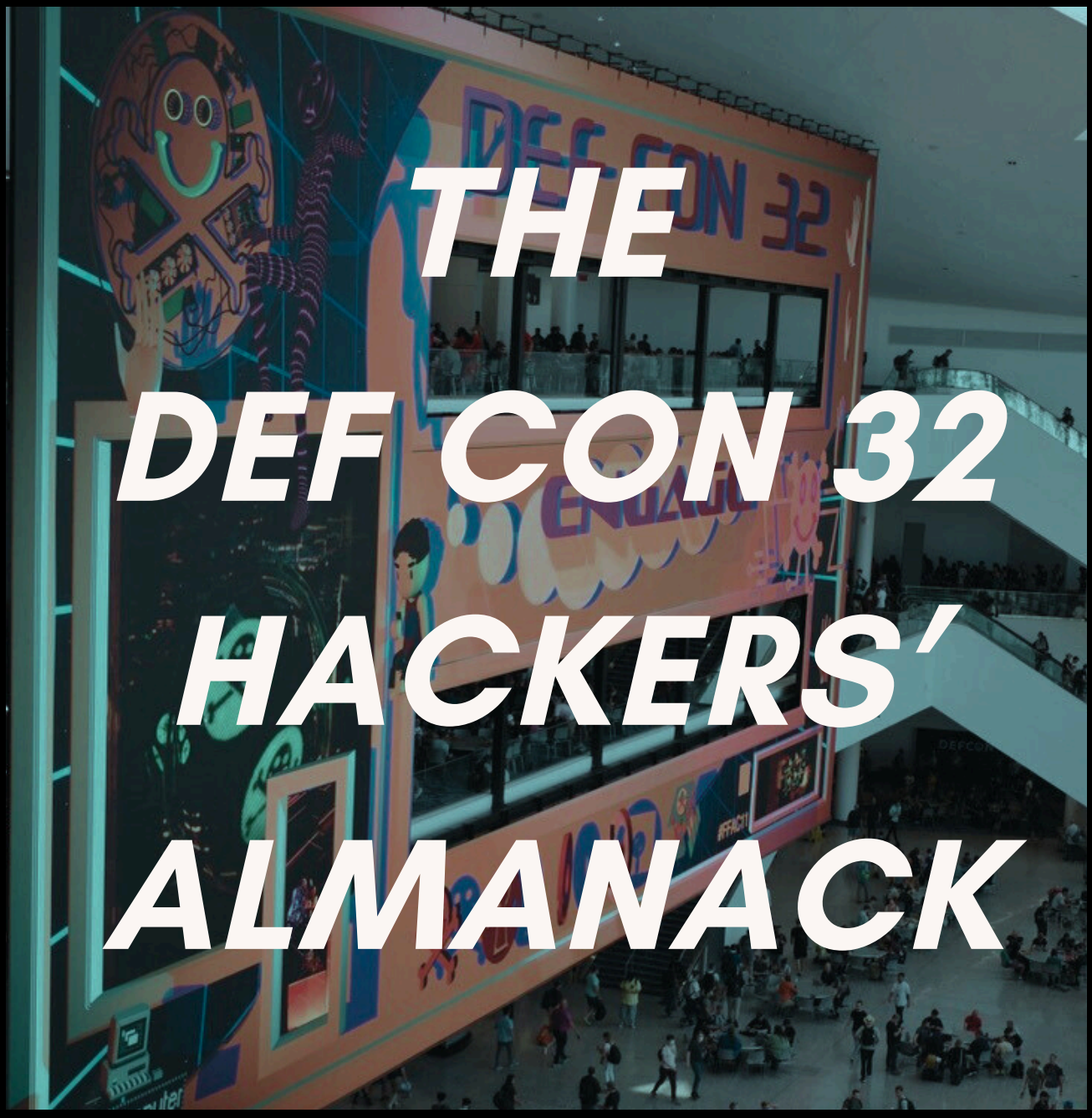


THE DEF CON 32 HACKERS' ALMANACK

A
DEF CON *FRANKLIN*
PRODUCT

TABLE OF CONTENTS

FOREWORD

BY JAKE BRAUN

EXECUTIVE DIRECTOR, UNIVERSITY OF CHICAGO HARRIS CYBER POLICY INITIATIVE
FORMER ACTING PRINCIPAL DEPUTY NATIONAL CYBER DIRECTOR, THE WHITE HOUSE

A few years ago at DEF CON, the Secretary of Homeland Security mentioned we were entering a "New Great Game" over cyberspace. I helped work on that speech, and in considering how to frame the inaugural Hackers *Almanack*, it seemed relevant to revisit here. Late in the 19th century, Russia and Britain became engaged in the "Great Game," a rivalry over influence that spanned modern Afghanistan, Iran, and Tibet. Today, the world is again engulfed in a "New Great Game." Yet, the venue has changed. Though Russia, Iran, China and the West remain key players, what was once a battle over rugged terrain has now evolved into a battle over cyberspace. Moreover, while physical and territorial violence continues to ravage or bubble up in nations such as Ukraine or Taiwan, the corresponding cyber threat remains much more pervasive. Even many nations considered at low risk for conventional warfare are on the frontlines of digital assault. In short, our freedom to pursue life, liberty and happiness online is at stake.

However, history lends an important insight. During the "Great Game," the Brits and Russians only gained ground after one side or the other strategically partnered with key local leaders who possessed in depth knowledge of the terrain, customs, and inner workings of Central Asia. Similarly, to win the New Great Game, our alliance of democratic nations must learn to work with technologists. Like the local leaders in Central Asia before them, the technologists, creators and hackers in the DEF CON community possess in-depth knowledge of the topography, code, and structure of our digital world. In order to emerge victorious in the New Great Game, we must help policymakers strategically partner with these technologists and learn from these "digital natives."

Such a partnership requires close-knit cooperation between policymakers and technologists to understand highly technical AND in-depth policy points of view. For democracies to overcome threats to the freedom of cyberspace from autocracies, we must bridge the chasm between technologists and policy makers in order to win this "New Great Game." At DEF CON, we believe the best strategy to bridge the chasm is to double down on the central principles initially developed during The Enlightenment like empiricism, the scientific method, reason, and liberty.

For the last 30 years, DEF CON has operated on a foundation of these Enlightenment Principles at the core of democratic society initially set in motion by the founders of modern science such as Galileo, Newton and Bacon. Like their Enlightenment forbearers, DEF CON community members are committed to principles such as democracy, liberty, tolerance, transparency, and an insistence on evidence-backed, empirically testable discoveries (as some would put it, POC or GTFO). Ben Franklin, is perhaps the person who most personifies these Enlightenment Principles of both commitment to scientific research AND civic engagement.

One noteworthy manifestation of Ben's commitment was *Poor Richard's Almanack*, which provided both technical information related to crops and weather as well as commentary on key policy issues of the age. Taking a page from Ben, this report is the inaugural issue of the annual *Hackers' Almanack*. *The DEF CON 32 Hackers' Almanack* is a novel first cut at bridging the chasm between policy makers and technologists. Through a new initiative, dubbed "Franklin," the *Almanack* will elevate the most interesting, impactful and cutting edge talks, research, and vulnerabilities identified across the DEF CON community. It also synthesizes these findings to be palatable for consumption by key policymakers across the globe. I believe we can make better, more rigorous policy if we infuse the ethos, and research, of the DEF CON community into the policy making process. By establishing this feedback loop between policymakers and technologists, we can make better policy and ultimately win the New Great Game and preserve freedom in our digital world.

INTRODUCTION

BY ADAM SHOSTACK

FOUNDER, SHOSTACK + ASSOCIATES
AFFILIATE PROFESSOR, UNIVERSITY OF WASHINGTON

Every year, tens of thousands of hackers converge in Las Vegas for a joyous, crazy exploration of the edges of technology. The events that have grown up around DEF CON are fondly called "Hacker Summer Camp." They include many communities with different perspectives, all with a core commitment to hacking and exploration. As DEF CON has grown, formal "villages" have been recognized and allocated rooms with their own talk tracks. Many of these villages now converge at many conferences over the course of a year. Other events that make up the "summer camp" focus on the commercial (BlackHat), community (BSides) and underrepresented in information security (Diana Initiative). Unfortunately, we can't cover them all in this report.

Hacking includes breaking systems, empirically testing the claim "it's secure." DEF CON also includes over 20 official challenges and contests, from digital Capture the Flag to building the machine that will chill ~~beer~~ beverages fastest to who can discover the most passwords that might have been leaked in a data breach. As the events have grown, many communities come together in Villages. Contests, events and villages are sponsored by the community, interested firms, and even government agencies. For example, Rivian and Aptiv sponsored a car hacking village, while the U.S. Space Force sponsored a hacking competition whose target was an actual satellite in orbit. Most other competitions are more down to Earth.

As you'll see, hackers speak with a degree of forthrightness that's been rare in Washington, D.C. Our first major section is titled, "AI Redteaming is Bullshit." While we delight in shocking language, the DEF CON community expects it to be backed with demonstrable facts. Extraordinary claims require extraordinary evidence, and many of the claims made at DEF CON are extraordinary. Products of all stripes are routinely shown to have problems, and the community expects factual demonstrations, proofs, and explanations. We also enjoy a good show, especially while we're in Las Vegas. And depending on your point of view, the community is either "forthright", "aggressive" or "rude" about demanding that evidence.

In that vein, we are proud to present *The DEF CON 32 Hackers' Almanack*. This year's iteration will mark the inaugural release of this first-of-its kind report compiled by DEF CON Franklin, a new collaborative effort between DEF CON and the University of Chicago Harris School of Public Policy - Cyber Policy Initiative. The *Hackers' Almanack* will compile the most interesting, impactful, and innovative research and vulnerabilities identified at DEF CON - presented in typically extraordinary fashion.

When appropriate, each of the vulnerabilities identified below have been disclosed in advance to someone who can fix it to minimize harm to bystanders. Please see the appendix on disclosure for more on the community's approach.

EXECUTIVE SUMMARY

Artificial Intelligence: AI Red Teaming is Bullshit

While security firms and policymakers often tout "red teaming" as a method to secure AI, a collection of great hacks has not resulted in systems being made secure. In order to engineer effective AI without hallucination, bias, or vulnerability to prompt-injection, we need to think first about what these AI systems are supposed to do - or not - in a systematic way, which will require design, definition, and testing (including, but not limited to) red-team sorts of attacks. We will need to move beyond "penetrate and patch" and integrate "secure by design," rather than relying only on AI red teaming. Without this paradigm shift, we risk embarking upon a technological revolution without trustworthy models or secure systems. This is especially relevant in light of new models like DeepSeek, which continue to shape narratives around the performance, security, and national security implications of AI.

Biohacking: Bioterrorism Today, Personalized Medicine Tomorrow

The realm of biology and medicine has been transformed - and along with it, our responsibilities as patients, providers, and regulators. The Four Thieves Vinegar Collective has shown a complete drug synthesis pipeline can be built by engaged hobbyists and produce vital medicines. Others talked about 3D precision printing for personal patient use, from a cellular to a prosthetic device. The future where everyone can produce their own drugs and devices is both fascinating and worrisome. What if the drug synthesis pipeline has an error or is hacked? What happens when a 3D printed device is printed with a low quality plastic? Snake oil medicine was replaced with safe and effective drugs and devices long ago. How do we preserve those properties while gaining value from experimentation and innovation?

Ransomware: Governments Failed, So Hackers Step Up

The DEF CON way is to celebrate achievement and progress. Our contests and demos are what we celebrate, not appointments to a task force and fancy powerpoint decks. Individuals such as Vangelis Stykas have actively disrupted ransomware operations despite the overwhelming financial and technical advantages that ransomware organizations possess. As these threats continue to grow, policymakers need to either defend society against this transnational criminal activity, or ensure that defending ourselves isn't a crime. Maybe even both.

Elsewhere, in the DEF CON Universe...

- As vehicle infotainment systems grow in functionality, wireless protocols such as Bluetooth present a new attack surface and threat to users.
- The clean energy transition needs to be secured, especially electric vehicle networks.
- The modems in your house are likely susceptible to attackers posing as members of a support team.
- Researchers showed how to break physical security systems including lockers and building access to the systems through their digital components.
- Cloud providers seem to make similar insecure design choices over and over, leading to massive vulnerabilities and secrets available for capture.
- DEF CON community volunteers are already helping provide free, scalable hands-on support in a pilot program with six under-resourced water utilities across the nation.
- A number of critical and fundamental vulnerabilities were discovered in a mobile voting product, and new vulnerabilities were discovered in several widely-fielded ballot-marking and DRE (direct-recording electronic) voting machines.

AI Red Teaming is Bullshit

The Emergence of DeepSeek Highlights Need for AI and Security Communities to Urgently Come Together and Define Parameters and Methods for Red Teaming AI

OVERVIEW

The AI Village featured its second iteration of the Generative Red Team exercise (GRT2) for generative AI, where attendees were asked to improve AI model evaluation. The Village focused on a bounty program where the model makers gave feedback to participants and guided them to reports that provided insight from model creators and the stated goals of their model. Nearly 500 participants took part, and the village paid $7850 in bounties to 48 people, with the top earner having never heard of the concept of model evaluations before the event. Said Village lead Sven Cattell: "We can now iterate on this and slowly build up to a complete program of coordinated disclosure and evaluations for AI models." The exercise also generated two takeaways: 1) ideas need to be thoroughly tested before testing yet another framework, and 2) AI red teaming needs integration, similar to what the CVE (Common Vulnerabilities and Exposures) did for traditional security starting in 1999.

FEATURED VILLAGE EXCERPT

SVEN CATTELL - *WE NEED TO INTEGRATE AND UNIFY FOR SECURITY*

After running the first two Generative Red Teams at DEF CON 31 and 32, I believe that the focus on AI red teaming is missing the forest for the trees. Public red teaming an AI model is not possible because documentation for what these models are supposed to even do is fragmented and the evaluations we include in the documentation are inadequate. Model cards were supposed to be the description document, but in most instances they just don't fulfill this objective. The evaluations, largely built by researchers, focused on technical questions, also miss large aspects of their intended domain. When dealing with a technology as powerful as LLMs there will always be "unknown unknowns" that the description and evaluations miss.

The evaluations used in AI and the unit tests and integration tests deployed in traditional software probe for known problems. Red teaming, on the other hand, looks for unknown problems. As AI pushes us into this new frontier of technology, these unknown unknowns are often the most elusive yet critical vulnerabilities to uncover. In traditional software we deal with these with disclosure programs and bug bounties. We need to repurpose and expand VDP for AI models and design a model card system that aids with disclosure programs. This will achieve what the original model card paper asked for, and create a system that will produce and maintain the best evaluations.

Generative AI, like Large Language Models (LLMs) will always make mistakes, will always have exploitable vulnerabilities, and will always have behaviors the model creators and the public do not want. To address these issues, policy makers around the world demand vendors "red team" their models before release. However, for AI models this term is different from the traditional use in software. It more means "evaluate," and in practice amounts to running various evaluations of a model system (some automated, some manual) and reporting the results. The hope is, with good evaluation and investment in safe AI, over time the severity of the flaws and vulnerabilities in AI will become smaller and less critical.

That's the hope, but it will be impossible to achieve if we keep going as we are. Currently, evaluations and "red team" processes created to monitor the flaws and vulnerabilities of AI models are themselves siloed and inevitably flawed. There is no way to fully cover all the inputs to an AI model and guarantee safety or security. Even the largest companies cannot afford to create and maintain the massive, diverse datasets needed to cover all the uses and restrictions we would like to project onto Generative AI. For a small team at Microsoft, Stanford, NIST or the EU, there will always be a use or edge case that they didn't think of.

However, we have a time tested system of vulnerability disclosure programs, enabled by decades of work from security experts. For AI, we need to modify disclosure programs to the unique needs of AI and we need to include the evaluations as artifacts that could be flawed.

We need to start not with the harms the AI could perpetuate, but the uses and restrictions we want to place on it… While we are creating the uses and restrictions we also need to standardize a few formats for evaluations… Finally, to actually test if this can work we need to change the way the security community sees AI red teaming. The term is muddled and messy and there are two separate issues here. The first one is that the wider security community does not understand AI security. The goal of AI security is not to make it impossible to break a system, but to make any such break expensive and short lived…the second is that a vulnerability or flaw report needs to be a narrative with statistical proof that these speed bumps are too easy to break in an in-scope situation.

If we want to have a model that we can confidently say "does not output toxic content" or "helps with programming tasks in Javascript, but also does not help produce malicious payloads for bad actors" we need to work together… We saw this happen in micro during GRT2 held at DEF CON 32. Attendees created focused evaluations for security topics that were better than what is provided by existing evaluations. The line between writing "good" code and "malicious" code is delicate and blurry. Hackers, paid with bounties, can do an amazing job at this.

Critical medical devices are regulated in law by asking for vague "best efforts" before a product is released, and detailed requirements on a vulnerability disclosure program. Red teaming can be a part of the "best efforts, but the details of which should be left to the vendor. We now have the opportunity to build a system that creates and maintains the best evaluations for AI and keeps AI models transparent and honest.

--- end of excerpt ---

POLICY TAKEAWAY

As AI and Machine Learning are aggressively integrated into the products we rely on, companies and society must do a better job making models trustworthy and ensure they are deployed safely and securely. While policymakers are often told to focus on "red teaming" AI, a collection of great hacks has not resulted in systems being made secure. In order to engineer effective AI that protects against hallucination, bias, or prompt-injection, we need to think first about what these AI systems are supposed to do - or not - in a systematic way, which will require design, definition, and testing (including, but not limited to red-team sorts of attacks). This means improvements to "foundation models," complementing and backstopping the improvements hoped for in complete systems. AI companies prefer focusing on systems, perhaps because they want to protect trade secrets in how foundation models are trained to resist, but many foundation models have public weights. This is sometimes inaccurately referred to as "open source" models. Hackers know that published weights are more similar to compiled binary code than to source code. It's not easy to read the weights, and it's less easy to make changes, and those are fundamental freedoms we get with open source code.

CISA is leading a nascent international coalition for "Secure By Design." They're engaged in the modern equivalent of moving beyond blaming "the nut behind the wheel" for car crashes, noting that some cars — and some AI — simply can't be operated safely. Similarly, while some call the requirements for medical devices "vague," the FDA does have 48 pages on Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions,* and it also focuses a great deal on security by design, secure architectures and effective threat modeling, all techniques that align with secure by design.

When DEF CON, FDA, and CISA are aligned, it's time to move beyond siloed and flawed evaluation and "red team processes," and change the way that policy makers view AI red teaming. Without this paradigm shift, we risk taking on a technological revolution without accounting for model trust and security. Thus, we must urgently bring together the AI and security community to develop security analysis methods, based on the intended use of a particular AI and knowledge of potential harms should that AI perform erroneously.

*U.S. Food and Drug Administration. 2023. "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions." Guidance for Industry and Food and Drug Administration Staff, (September). https://www.fda.gov/media/119933/download.

Cyber Challenge Proves AI Can Find & Help Fix Vulnerabilities

New Techniques Pair Cyber Reasoning Systems, Program Analysis Tools & Techniques, Static & Dynamic Analysis Systems with AI, to Automatically Find and Fix Synthetic Vulnerabilities

OVERVIEW

This was the first year of the AIxCC, a DARPA-sponsored (Defense Advanced Research Projects Agency) competition. Teams were encouraged to find and fix vulnerabilities in software for critical infrastructure and national security. Hackers volunteered to use large language models (LLMs) to help defend a simulated city from a barrage of cyberattacks.

AIxCC AT A GLANCE

- Competitors' systems discovered 22 unique synthetic vulnerabilities in the Challenge Projects, and created fixes for 15 of them. (The number of vulnerabilities introduced has not been disclosed.)
- Competitors developed 11 unique patches for C-based challenges and four unique patches for Java-based challenges.
- One team, from Georgia Tech, leveraged AI to discover a zero-day vulnerability in the open-source SQLite3 software. Despite years of audits, this vulnerability hadn't been found. It was fixed in less than a week without any drama. (See appendix on disclosure.) This research inspired* Google's Project Zero to delve into the techniques.

FEATURED TALK

DR. KATHLEEN FISHER
"CLOSING THE SOFTWARE VULNERABILITY GAP"

In "Closing the Software Vulnerability Gap", Dr. Kathleen Fisher described legacy code in critical infrastructure as a national security problem. DARPA seeks to address this problem by leveraging the growing power of AI and large language models (LLMs) to identify and fix code vulnerabilities at scale. One key facet of the issue is the prevalence of open source software: according to a Synopsys open source risk assessment, 96% of code in industrial codebases contain at least some open source; 84% of these code bases contain at least one known vulnerability; 77% of code in codebases is open source, and 74% of codebases contain known high-risk vulnerabilities. While this does not mean open source is less secure - simply that there is more available data on it - there remain barriers to identifying and eliminating software vulnerabilities at scale.

To address these issues, Dr. Fisher makes a case for using AI tools to automate finding common vulnerabilities and fixing patches. Her hypothesis: you can pair cyber reasoning systems and traditional program analysis tools with machine learning models to better find and fix vulnerabilities in code bases.

"From Naptime to Big Sleep: Using Large Language Models To Catch Vulnerabilities In Real-World Code." 2024. Google Project Zero. https://googleprojectzero.blogspot.com/2024/10/from-naptime-to-big-sleep.html.

For instance, Dr. Fisher outlines how the AI Cyber Challenge hosted at DEF CON aims to test this hypothesis and is already producing positive results. Another DARPA effort, Translating All C to Rust (TRACTOR), aims to pair program analysis tools with LLMs to substantially automate the translation of memory-unsafe C code into the memory-safe language Rust. Memory safety is a technical property of computer languages that prevents systems from ever having certain classes of vulnerabilities.

POLICY TAKEAWAY

AIxCC and TRACTOR represent two approaches to making software more secure. The AIxCC focuses on finding and fixing vulnerabilities, TRACTOR transforms the code into new code that cannot have those vulnerabilities. If TRACTOR succeeds, and if developers are willing to use the code in a different language, it will lead to a dramatic increase in security as entire classes of vulnerability are removed. We can look at this as the "red team" vs "design" approaches to security. The AIxCC accelerates red teaming (against traditional software), while TRACTOR reduces the set of things we expect to find. But think back to our frank statement that "AI red teaming is bullshit." Where is the TRACTOR of AI?

Bioterrorism Today, Personalized Medicine Tomorrow

'Hacked' Biomedical Formulas Provide Historic Opportunities
For the World's Poor to Gain Access to Life-Saving Medicines

OVERVIEW

The Biohacking Village was founded in 2014 and is committed to bridging the gap by partnering with medical and pharmaceutical manufacturers, digital health experts, patient advocates, citizen scientists, physicians, and healthcare organizations like hospitals and clinics. The Biohacking Village is also dedicated to making patient care safer by raising awareness of the critical roles cybersecurity, biotechnology, and research play in our world while focusing on national security - because at the end of the day, we are all patients in this system.

BIOHACKING AT A GLANCE

Janine (Nina Alli) Medina and Jennifer Agüero of the Biohacking Village helped provide this overview of the Village's activities:

- Device Lab: 10 Medical Device Manufacturers; $13M estimated value of devices; $4T worth of brain power and IP; 3,095 Attendees; 42 Vulnerability Findings in 20 hours; 25 devices
- Capture the Flag: 142 users; 66 teams
- Workshops: "Med Team vs. Red Team: Adversarial Medical Device Testing 101 Workshop" offered hands-on learning for researchers and manufacturers while leaning into cybersecurity with the hacker mentality
- Speaker Lab: 21 speakers across 7 talks and 2 panels
- Tabletop Exercises: "Small Choices, Global Repercussions: A Tabletop Exercise about decisions making in Healthcare Cybersecurity", shedding light on fresh insights and reshaping understanding of healthcare and future trajectory; crafted by a CISO, Regulatory Strategist, Rare Disease Physician Researcher, and an A&E Artificial Intelligence Physician

FEATURED TALKS

DR. MIXÆL SWAN LAUFER ON BEHALF OF THE FOUR THIEVES VINEGAR COLLECTIVE "ERADICATING HEPATITIS C WITH BIOTERRORISM"

Civilian researchers are fighting deadly diseases with bioterrorism. Specifically, they are looking to solve the problem of prohibitive costs and legal restrictions for life-saving drugs such as epipens, abortion pills, certain medications for HIV / AIDS patients, and Hepatitis C treatments. In particular, this talk focused on the exponentially deadly epidemic of Hepatitis C in the US. As Hepatitis C continues to spread at an increasing rate, contemporary cures continue to be cost-prohibitive. As the researchers outlined, "A quarter of a million people die from Hepatitis C every year. Fifty million people are currently infected... those pills are one thousand US dollars... so if you have $84,000 USD, Hep C is not your problem." As a result, Dr. Laufer observed that the epidemic has worsened: "somebody dies every two minutes... when I talked about this five years ago, it was every three minutes. So again, not only is it getting worse, but it's getting worse faster."

BIOHACKING VILLAGE

"The feds say saving a life this way is bioterrorism. We say: So Be It."
– The Four Thieves Vinegar Collective

To do so, the researchers set up an at-home microlab, with hacked-together Raspberry PI computers and Arduino microcontrollers connected to a chemical reaction chamber. Essentially, the researchers create automated, easy-to-understand processes to discover chemical synthesis pathways, determine the materials needed, and perform lab reactor duties for the small-scale manufacturing of life-saving pharmaceuticals – in the case of Sovaldi, the Hepatitis C medication, at the price of $300 USD per course of treatment instead of $84,000 USD. Said Dr. Laufer, "Most medications you can make a better, cheaper version of yourself at home. Anybody can. It's entirely doable."

LACEY HARBOUR
"3DU:HOMO (E)X MACHINA"

AI is transforming the healthcare products ecosystem, driving a future that is precise, personalized, and centered at the Point of Care (PoC). One of the most groundbreaking technologies accelerating this shift is AI-enabled 3D printing (3DP), also known as additive manufacturing. Many orthopedic companies are now establishing medical device manufacturing (MDM) facilities within healthcare delivery organizations (HDOs), bringing production closer to both physicians and patients, reducing turnaround times for patient-specific, custom, or matched devices, and strengthening the collaboration between physicians and developers. This physician-developer synergy, along with on-site manufacturing within HDOs, serves as a precursor to the future of Medical Device Production Systems (MDPSs)—where the medical device encompasses both the manufacturing process (e.g., 3DP) and its final output (e.g., implants). However, Harbour poses a critical question: Is our complex and interconnected digital healthcare ecosystem secure enough to sustain this transformation?

Anticipating these challenges, the Food and Drug Administration (FDA)—in alignment with the International Medical Device Regulators Forum (IMDRF)—released the 2021 discussion paper "3D Printing Medical Devices at the Point of Care." This paper outlined key concerns, including regulatory responsibilities, training, supply chain logistics, and risk management, while inviting stakeholder feedback.

Harbour delves into the unique partnership between MDMs and HDOs as crucial for sustaining this model, yet it also introduces potential vulnerabilities within the emerging digital healthcare ecosystem. AI offers several key capabilities to support this transformation, including:

- Auto-segmentation of medical images – AI can process CT scan data, construct 3D models, and identify defects before final human confirmation.
- AI-assisted design – AI-driven algorithms can optimize product design and streamline the customization process.
- Intelligent manufacturing support – AI can assist in automating production workflows, improving precision and efficiency.

The key technical takeaway is that the current Industry 4.0 IT infrastructure in healthcare must evolve to address existing vulnerabilities. As MDPS integrates both manufacturing and the final device into a unified system, mitigating cybersecurity and interoperability risks will be paramount to ensuring a secure and scalable future.

BIOHACKING VILLAGE

V3GA
"DYSFUNCTIONAL UNITY: THE ROAD TO NOWHERE"

v3ga spoke about the urgent need to address the "dysfunction" between security researchers, manufacturers, and lawmakers in the medical device space. While technology advances, conceptions of security continue to lag behind, leading to vulnerable medical devices and hospital networks that are still cleared by regulatory organizations.

In particular, medical device manufacturers simply take a disclosed vulnerability at face value, without understanding deployed context, such as connection to a hospital network. This gives attackers a plethora of prime targets and attacks, such as stealing NLTM credentials to gain lateral access within the hospital network. One such vulnerability allowed v3ga to access a closed medical device system in just two minutes. Said v3ga:"I only needed two minutes 'on door,' to be able to get that exploit out the door… get code execution, and then now I'm… on the thing that's going to be cutting people up. (surgery)"

Organizations such as CISA and the FDA need to support offensive security experts to fully comprehend the gravity of such vulnerabilities. In the long run, v3ga argues that it is both safer - and more cost-efficient - to employ goal-based offensive testing against devices and hospital system networks. He argues that the ramifications of this are potentially catastrophic: "The second thing is that I don't get… when I turn in a report with a critical flaw but [the device was] still accepted by the FDA, and these are things that basically will either kill a patient, take over the entire hospital, or "mock" blow up the hospital in one instance. Basically, I was able to show how something that was supposed to clean items can be converted into a makeshift incendiary device because of the level of access for field service engineering combined with a weak UI vulnerable to kiosk escapes… as a result you now can modify the control temperatures past expected values and for extended times… in an environment with pure oxygen and pure alcohol."

Finally, v3ga offers recommendations to address this dysfunction, including stronger cohesion between all parties, consensus on how guidelines are enforced, and encouraging like-minded offensive security experts to identify these issues.

BIOHACKING VILLAGE

POLICY TAKEAWAY

The realm of biology and medicine has been transformed - and along with it, our responsibilities as patients, providers, and regulators. This transformation is practically unstoppable. Medical regulation has developed over more than a century to ensure that medicines and medical devices are safe and effective. The talks at the Biohacking Village (and the Embedded, IoT, and Hardware Hacking Villages) raise three related sets of challenges to the current administration:

- Advances in Precision medicine will result in increased cures for life altering illnesses - this may come with increased exposure of PHI and PII, specifically genetic material like DNA.
- At home pharmaceutical production outside the current system may be cheaper, with varying levels of reliability, and loss of traceability when problems happen.
- Medical devices made outside the current ecosystem may have more availability for right to repair, with the caveat that there may be varying levels of biomedical complexity and user technical experience.

Each of these takeaways carries two issues: Errors by well-intentioned people and harm from actively malicious people. There are legal, policy, and regulatory decisions about what and how to penalize these issues, but what and how do we promote this freedom while restraining it from converting into criminal conduct or bioterrorism?

Looking towards tomorrow, agencies like the FDA (and the IMDRF, the International Medical Device Regulators Forum) must engage with these new opportunities for medicine and develop frameworks where researchers can freely educate medical professionals, thus helping economically underprivileged communities, like international NGOs supporting the poor in developing countries, to leverage these options. The Biohacking Village, aligned with other Villages, and DEF CON or other civil society organizations can also play a critical role in educating the vast network of health-related NGOs about these DIY healthcare options, so that we may better serve those living in extreme poverty and assist with humanitarianism activities across the globe.

At the institutional level, we must first increase protections for good faith cybersecurity researchers who, upon finding problems, can be subjected to a host of legal threats and the associated costs and risks. Perhaps HHS and other health-centered agencies could recommit to advancing cybersecurity through the lens of the hacker community. (This is not to dismiss engagement by HHS or its administrative agencies, or to ignore the real danger that publicity for security vulnerabilities can cause patients to not use a live-saving or life improving device.) Again, please see the appendix on disclosure.

Lastly, ransomware, covered in the next section, has had an apparently outsized impact on hospitals. The policy takeaways in the following section on ransomware may be relevant to those who skipped to this section.

Governments Failed, So Hackers Step Up

Authorities Have Not Curbed The Scourge of Ransomware
It is Time to Break the Rules and Enable Cyber Vigilantism

OVERVIEW

How do you defeat ransomware cyber crime, a fast-growing and highly professional industry with a payout of over $1 billion per year? Vangelis Stykas outlines one possibility: quasi-vigilantism. Ransomware is now developed and deployed by companies whose purpose is either explicitly crime or a thin veneer to cover that real goal. These firms have become extremely skilled in their technical ability to develop ransomware, operate reliable infrastructure and even negotiation. Yet, Stykas was able to give the ransomware companies a taste of their own medicine. Among other exploits, he was able to gain key internal knowledge of various ransomware companies' workings, read internal messages, leak key decryptors to help victims decode ransomware without paying, and stop widespread cryptocurrency-based scams.

FEATURED TALK

VANGELIS STYKAS
"BEHIND ENEMY LINES: ENGAGING AND DISRUPTING RANSOMWARE WEB PANELS"

Ransomware groups have become notably proficient at wreaking havoc across various sectors, but we can turn the tables. A traditionally less explored avenue in the fight against these digital adversaries lies in the proactive defense against their web panels. One researcher, Vangelis Stykas, explored the frontiers by targeting the very command and control (C2) centers ransomware groups rely on, thus turning the tables in our ongoing battle against cyber threats. Stykas wrestles with the implications of fighting back against ransomware companies in this manner: "Are we the baddies?... I never wanted to become a vigilante... I wanted to be the one that reinvents the status quo and tries to... give them a taste of their own medicine."

These ransomware groups are after hospitals, critical national infrastructure, and almost every other facet of society. They are armed to the teeth with ransomware negotiators, money lenders and payment processing capabilities, and exploitation developers who may be developing either zero day or end day, and last but not least, highly skilled specialists in infrastructure and hosting. Through hard work, Stykas got internal knowledge of ransomware groups, gained access to nearly all the group's messages, and obtained decryptors which were relayed to the companies that were ransomed or abused. Stykas also levied a big financial hit against a group named BlackCat. By exploiting web panels, Stykas got all their information and understood their lateral movement, stopped the whole campaign, and prevented four companies from being ransomed.

POLICY TAKEAWAY

Government efforts to deal with ransomware have failed to defend our society against these criminals. The criminals often live in countries who will never extradite them to face charges in a victim's home country. It's widely believed that many of the worst ransomware actors are either directly tied to their respective governments, or enjoy a certain degree of protection from their government. Aside from particularly egregious attacks like the Colonial Pipeline attack, where the Department of Justice was able to seize the ransom, the government has accomplished little to stop the scourge of ransomware.*

** "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside." 2021. Department of Justice. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.*

RANSOMWARE

POLICY TAKEAWAY

Governments have criminalized "hacking back," even as our adversaries grow stronger. There is good reason to prohibit hacking back, like not inadvertently starting WWIII because some cowboy hacker at a company decides to hack an attacker that turns out to be a nation state and that nation state believes the U.S. government is the one attacking it.

Stykas is doing something more nuanced than just hacking back. What individuals such as Stykas have been able to do, in stark contrast with the government, is to actively disrupt ransomware operations despite the overwhelming financial and technical advantages that ransomware organizations possess. As these threats continue to grow despite our current efforts, policymakers and civil society need to seriously consider doing something else. Perhaps Stykas' activist, quasi-vigilante model is a better model of response.

As we determine if new models are warranted, we continue to live in an information vacuum. We still don't have an authoritative list of ransomware incidents. We have lists compiled by academics*, reports by vendors, and government sources like the HHS breach report portal**. Yet, none of these sources strictly reports on ransomware incidents. Thus, it can be hard to tell if the incidence of new ransomware incidents is rising or falling. Similarly, we have no authoritative, cross-sector data that would allow us to compare ransomware incidents per 1,000 organizations or per million computers and so forth across sectors. Hackers love transparency and data, and hackers especially love data in transparent formats that allows us to query, explore, and remix information into new uses. Cybersecurity could learn lessons from public health about the importance of data collection, analysis and publication, and the institutions that support it.

There are other approaches. One of the authors of this report has written that Microsoft could fix ransomware tomorrow, regarding rate limiting in Windows.*** The DEF CON community could explore other improvements to Windows that Microsoft doesn't like... it would be easy to say it could hardly be worse, and while that's not true, the spirit of experimentation and exploration might give us useful new tools. Perhaps those tasked with dealing with the problem could sponsor a contest, hackathon, village, or some other forum to explore new possibilities. It's not unusual to say things like "with the recent increase of ransomware and other attacks against under-resourced hospital systems, we must push for stronger global norms against hacking hospitals." Part of setting those norms (or "imposing costs") would be to stop threatening vigilantes with prosecution, start offering them assistance or information ("Please don't hack this system"). Despite disputes, society is gradually developing a mostly responsible set of disclosure norms even if there's disputes. We might be able to create something similar for vigilantism.

It's time to re-evaluate our hesitancy around vigilantism. As we've watched options fail, the "least crazy" next choice is worth exploring. (As an example, the "Sky Crane" rocket-powered descent is the least crazy way to put large rovers on Mars, and having a rocket-powered crane is clearly sort of nuts. But NASA made this very hackery idea work and it's worked every time, and landed two Mars Rovers. NASA has a wonderful 5 minute video explainer.****) Perhaps there are ways that vigilantes could better share information with law enforcement or victims without fully "hacking back." DEF CON attendees are focused on demonstrated success, demonstrated impact, and a willingness to try new things even if (or maybe especially if) they seem a little crazy.

*"Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information." 2025. U.S. Department of Health and Human Services Office for Civil Rights. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
**Cable, Jack, Ian W. Gray, and Damon McCoy. 2024. "Showing the Receipts: Understanding the Modern Ransomware Ecosystem." Symposium on Electronic Crime Research. https://arxiv.org/pdf/2408.15420.
***Shostack, Adam. 2023. "Microsoft Can Fix Ransomware Tomorrow." July 5, 2023. https://www.darkreading.com/vulnerabilities-threats/microsoft-can-fix-ransomware-tomorrow.
****NASA Jet Propulsion Laboratory. 2012. "7 Minutes of Terror: The Challenges of Getting to Mars." YouTube. https://www.youtube.com/watch?v=Ki_Af_o9Q9s.

ELSEWHERE, IN THE DEF CON UNIVERSE...

OVERVIEW

DEF CON's hacker summer camp had many great talks that don't fit the the top three themes we felt were most salient for policymakers. Yet many more talks have policy implications that are worth the reader's attention. Though these talks represent the tip of the iceberg in this year's DEF CON discoveries, they still speak to the breadth and depth of technical vulnerabilities in our cars, cloud infrastructure, modems, and beyond. Our policymaking processes must account for the near-universal nature of this revolution as technology continues to rapidly evolve. All companies named are as reported in the talks.

All companies named are as reported in the talks.

VLADYSLAV ZUBKOV & MARTIN STROHMEIER
"EXPLOITING BLUETOOTH: FROM YOUR CAR TO YOUR BANK ACCOUNT"

Zubkov and Strohmeier discovered over sixty vulnerabilities across twenty-two different cars from major manufacturers, as well as the Garmin Flight Stream flight management system currently deployed across several types of aircraft. These novel implementation-specific vulnerabilities could enable Bluetooth hackers to steal information from targeted vehicles, establish a man-in-the-middle position, or potentially escalate privileges to hijack accounts.

POLICY TAKEAWAY

As vehicle infotainment systems grow in functionality, wireless protocols such as Bluetooth grow in prominence. However, the lack of patches and the difficulty of patch installation combined, pose a new attack surface and threat to users. Although these researchers created an open-source tool for others to test the same Bluetooth vulnerabilities and extend it easily, testing methods are still scattered. It's easy for big tech companies to add connectivity while disclaiming any responsibility for the consequences. It's become hard to buy a vehicle that's not "connected."

SAM CURRY
"HACKING MILLIONS OF MODEMS AND INVESTIGATING WHO HACKED MY MODEM"

In 2022, Sam Curry discovered his Cox modem had been hacked when an unknown IP address replayed traffic, and began to look into the vulnerabilities behind this attack. By digging into the business portal of the internet service provider, Curry found weaknesses in TR-069. This is an industry standard admin access protocol that allows service providers like your ISP to work with your router remotely (to reset devices, etc.) The discovered vulnerability demonstrated how a malicious attacker could execute commands, modify the settings across potentially millions of modems, view any business customer's personal identifiable information, and assume the functions of an ISP support team.

POLICY TAKEAWAY

No vendor wants to invest in replacing that code, especially before service providers are demanding it. No service provider wants to update until all fielded devices are ready. As a result, nothing gets updated. When a standard has insecurities, it's a classic collective action problem, and government action is the classic way to address such problems. Both communications and information technology are critical infrastructures.

ELSEWHERE, IN THE DEF CON UNIVERSE...

BABAK JAVADI, AARON LEVY & NICK DRAFFEN
"HIGH-INTENSITY DECONSTRUCTION: CHRONICLES OF A CRYPTOGRAPHIC HEIST"

The researchers dig into HID Global's iCLASS SE solution, one of the world's "most widely-deployed Electronic Physical Access Control platforms." By reverse engineering the hardware and software chain of trust securing the platform, Javadi, Levy and Draffen uncovered "pitfalls and implementation defects" over a span of seven years. These defects ultimately opened the door for "an attack chain that allowed for the recovery of sensitive cryptographic key material from secure elements... result(ing) in revealing some cryptographic keys to the kingdom." The keys to the kingdom, such as authorization keys, media keys, and admin keys were found to be stored in secure elements within readers, encoders, and configuration cards.

POLICY TAKEAWAY

Many access control vendors store keys in encoders and similar devices used to program credentials and configuration cards. In cases where customer-specific or unique keys are used, the impact of the attack is lessened but not eliminated. Economics are important for security. Vendors must build a system that customers can afford to buy, install, and maintain. As deployment complexity is increased, appropriately skilled staff may need to spend more time maintaining the system.

System engineering is difficult. Business requirements for interoperability, functionality, and security are often at odds with each other. In turn, vendors are forced to make trade-offs to strike an economically viable balance for customers.

DENNIS GIESE & BRAELYNN LUEDTKE
"OPEN SESAME - OR HOW SECURE IS YOUR STUFF IN ELECTRONIC LOCKERS?"*

** Note: There was a cease-and-desist demand issued by Digilock for this talk, which was later retracted, allowing the talk to be completed successfully. (See the "Disclosure" appendix for more on irresponsible behavior by vendors.)*

An increasing number of physical security devices (read: locks) with smart components are entering the market, which offers an enticing attack surface to physical red teams. These locks - which often operate using standard PIN and RFID technology - can be found in offices, hospitals, schools, gyms, and so forth. Because people intrinsically trust that locks are secure, users reuse their personal PIN number for locker passcodes - not knowing that there are practical physical and side-channel attacks that target these locks. In particular, Giese and Luedtke tested Digilock and Schulte-Schlagbaum AG (SAG) locks, and found that they could extract firmware and keys, access all locks through access to one, and clone or emulate keys - all in a cheap and relatively straightforward manner. The researchers especially stressed the danger of re-using a personally significant PIN number for lockers, cabinets, or safes.

POLICY TAKEAWAY

It's easy for big tech companies to add connectivity while disclaiming any responsibility for the consequences. A vendor whose lock is this insecure because of physical flaws could be negligent.

ELSEWHERE, IN THE DEF CON UNIVERSE...

BILL DEMIRKAPI
"SECRETS AND SHADOWS: LEVERAGING BIG DATA FOR VULNERABILITY DISCOVERY AT SCALE"

Independent Security Researcher Bill Demirkapi used massive datasets—from antivirus scanning platforms to internet record logs—to expose how cloud provider design choices systematically put organizations at risk. His analysis uncovered two widespread vulnerabilities affecting thousands of major companies: over 66,000 abandoned website domains that attackers could hijack to impersonate legitimate businesses, and more than 15,000 exposed cloud access credentials that grant direct access to sensitive infrastructure and customer data. Despite the first issue being well-documented since 2015, cloud providers have not implemented architectural safeguards to prevent these vulnerabilities. Instead, their design choices often incentivize risky behavior - for example, traditional API secrets are designed to be easily copied into code, making accidental exposure more likely. Alarmingly, even when these leaked secrets are reported, some providers like Amazon Web Services opt not to revoke them automatically, leaving organizations vulnerable.

POLICY TAKEAWAY

This research exposed how cloud provider architectural choices and security practices can create systemic risks that individual organizations cannot easily address. While cloud providers prioritize ease of use, the resulting security trade-offs affect thousands of businesses and millions of consumers. The lack of provider action on long-standing issues, combined with inconsistent security practices across the industry, suggests a need for regulatory frameworks that better align cloud provider incentives with customer security needs.

HARRY KREJSA & SARAH HIPEL
"BUILDING A SECURE AND RESILIENT NATIONWIDE EV CHARGING NETWORK: THE ROLE OF HACKERS IN THE CLEAN ENERGY REVOLUTION"

There is a growing interplay between renewable energy and automotive infrastructure as the nationwide EV charging network continues to grow. There are also potential challenges ahead, especially as the convergence of physical-digital infrastructure starts to negate a decades-long "accidental air gap". Krejsa and Hipel also outlined five linchpin technologies that are critical to securing energy resources - and EV infrastructure - for the future of the clean energy transition. Those technologies are: batteries and battery management systems, inverter controls and power conversion equipment, distributed control systems, building energy management systems, and EVs or EV supply equipment. The speakers encouraged DEF CON attendees to probe these five prominent technologies at the Car Hacking Village.

ELSEWHERE, IN THE DEF CON UNIVERSE...

JAKE BRAUN

"A CYBER VOLUNTEER TASK FORCE MODEL TO SECURE OUR CRITICAL INFRASTRUCTURE"

Beyond producing this *Hackers' Almanack*, DEF CON Franklin also leverages the wealth of expertise and commitment to civic engagement in the DEF CON community to bolster the cybersecurity of our critical infrastructure. The DEF CON Franklin Cyber Volunteer Task Force empowers individuals in the DEF CON community to provide hands-on support for under-resourced critical infrastructure, with hopes that the Task Force will be a free and scalable solution. Franklin targets sectors that are the most vulnerable, increasingly under attack, and least protected from cyber threats, such as water utilities. With the help of a generous grant from Craig Newmark and newmark philanthropies, Franklin has recruited 331 volunteers from the DEF CON community. As part of its pilot project, Franklin also connected these volunteers to six water systems from across four states (Oregon, Indiana, Vermont, and Utah) and will soon expand to other water systems across the nation.

VOTING MACHINE HACKING VILLAGE: OVERVIEW

PROVIDED BY MATT BLAZE & CATHERINE TERRANOVA

The Voting Machine Hacking Village, a popular fixture at DEF CON since 2017, has become America's premier forum for educating technologists and advancing research on the practical problems of - and solutions for - securing civil elections. It has two main points of focus: the first is a hands-on open workshop, and the second is an invited talks program. At the hands-on open workshop, over 25,000 DEF CON participants are invited to examine, probe, and critically evaluate existing and proposed election technologies. This includes voting machines and electronic pollbooks, as well as commercial systems under consideration for mobile and remote voting. While the primary goal is educational, invariably participants discover new weaknesses and vulnerabilities in these systems. A detailed description of these discoveries will be included in the Village's forthcoming annual report.

Examples of discoveries from this year include:

- A proposed mobile voting system, brought to the Village by a vendor, in which a number of critical and fundamental vulnerabilities were discovered during the event and demonstrated. We applaud their constructive engagement.
- New vulnerabilities discovered in several widely-fielded ballot-marking and DRE voting machines.

These vulnerabilities, and the ease with which they can be discovered, exploited, and reproduced, viscerally underscore the critical importance of using only "software independent" voting systems, which can be achieved by using certain kinds of paper-ballot-based voting systems along with the use of risk-limiting audits. The invited talks program ran in parallel with the hands-on workshop over two days, in which researchers, technologists, and election officials shared insights and problems for future work.

POLICY EPILOGUE

BY JEFF MOSS

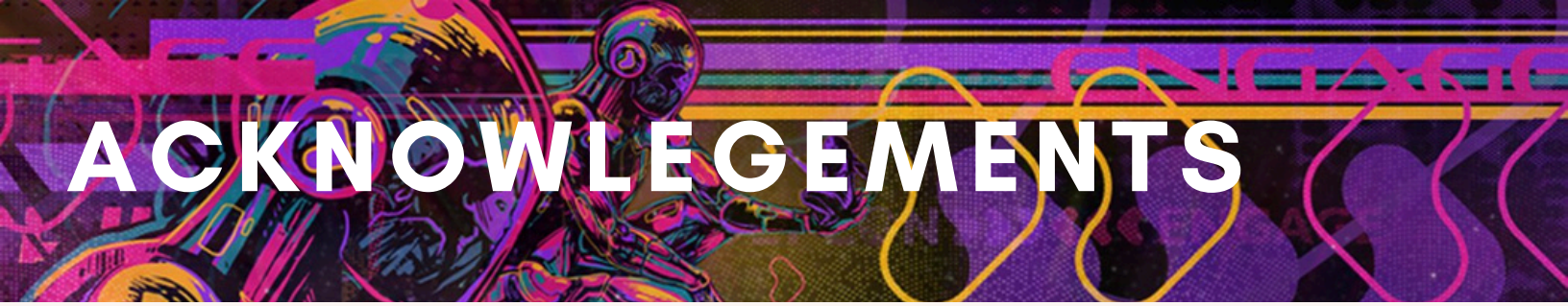
FOUNDER, DEF CON

Hackers are tinkerers, testers, and critical thinkers, interested in exploring technologies and problems. We like to ask questions to figure out how and why things work. When we fail we try again, curious why we failed and how to fail less the next time. Discovering the limits of technology, pushing it to behave in ways not imagined by its creators, is classic hacker thinking. Hackers have helped design, build, and secure some of the world's most critical technologies, from cars to satellites to all kinds of software. This curiosity is predicated on an openness that is a trait of hackers, we want the knowledge necessary for creation to be open, free, and easily accessible to all. As they say a rising tide lifts all boats. It is what DEF CON is all about - a platform for our community of hackers to publicly share findings, who don't gate-keep discoveries, and have an eye on the future for what comes next.

In the 21st century, I have seen a rise in attempts to keep knowledge out of the public domain. Market forces that have made the internet more efficient than ever have also made it more centralized, more controlled, more monitored and more brittle than ever before. This state of the internet is taken for granted without thinking if it would be better for users if the internet was structured differently—structured to be more open and more decentralized.

This *Almanack* certainly is not an attempt to change how the internet works, but it is an attempt to make a complicated topic more approachable. A lot has happened in the world of cybersecurity since DEF CON started over 30 years ago. Our community has grown, and like the internet, in order to thrive, it must remain open and innovative. The *Almanack* is not for experts but is purposefully written in a less-technical way to allow people to read a page and understand the threats and opportunities that lie ahead. Many of cybersecurity's most pressing problems cannot be solved by technical experts alone, there are social and regulatory equities involved, so a broad audience needs to understand the problems at hand before we can tackle them together as a community.

As you read this *Almanack*, I hope it inspires reflection on the implications of technology and society, and creates ideas that help safeguard our future. How do we protect the openness of the Internet without locking it down into walled gardens? Whether you are new to the DEF CON community or not I hope you contribute a little bit to help make things better - that is, after all, part of the hacker spirit.



ACKNOWLEGEMENTS

This year, a small team of DEF CON technologists and Harris graduate student volunteers worked together tirelessly to gather data, analyze top findings, and compile policy implications for cutting-edge insights. We are indebted to their efforts and those of the collective DEF CON community - a community that continues, year after year, to bring eye-opening exploits and technological weaknesses to light.

The Hackers' Almanack is especially grateful for:

- The organizers, subject matter experts, and partners from DEF CON 32 and the broader DEF CON community who make the conference a reality each year;
- The outstanding contributions and support of Jake Braun, Jeff Moss, Adam Shostack, Paul Chang, and Divyansha Sehgal;
- The speakers featured in this *Almanack* report, who provided such illuminating content and also helped review and provide edits (in order of appearance):

Sven Cattell, *Nina Alli*, *Jennifer Agüero*, *Dr. Mixæl Swan Laufer*, *Lacey Harbour*, *v3ga*, *Vangelis Stykas*, *Martin Strohmeier*, *Vladyslav Zubkov*, *Sam Curry*, *Babak Javadi*, *Aaron Levy*, *Nick Draffen*, *Dennis Giese*, *Braelynn Luedtke*, *Bill Demirkapi*, *Harry Krejsa*, *Sarah Hipel*, *Matt Blaze*, *Catherine Terranova*

- The University of Chicago Harris School of Public Policy, for providing academic and research resources to support this work; and
- The Hacker Summer Camp community, which brings together so much great work.

APPENDIX A: DISCLOSURE

BY ADAM SHOSTACK

The hackers at DEF CON generally want to make things better, and disclose security vulnerabilities to firms that have shown themselves able to responsibly handle the information. Often, work that would cost tens or hundreds of thousands of dollars if performed by a consultant is instead provided for free because the hackers did the research for the fun of it. We call these friendly heads up, or coordinated disclosure, and the main focus is to ensure that innocent customers or bystanders are not hurt by the disclosure.

For example, if Jeff Moss - DEF CON founder - finds a security problem in Microsoft's Windows Server and publishes the details, all the companies running Windows Server are suddenly at slightly greater risk of attack. If Jeff tells Microsoft so they can fix it, test the patch and release it, those companies are able to deal with the problem with less of a kerfuffle. As long as Microsoft is issuing fixes at a reasonable rate, everyone wins.

DEF CON speakers routinely reach out to companies well in advance of the conference in this coordinated disclosure model. Beyond that, during DEF CON, participants in the AIxCC competition found a real bug in the open source project SQLite.* They reported it on August 6, 2024 and a fix was developed, tested and released by SQLite in about a week. This open source project demonstrated responsible engineering when contacted.

As another example, in 2024, a researcher stumbled across a problem where a major insurer's benefits management site displays full social security numbers by default, and includes them — by default — in every data export. The site does not have any way to turn on multi-factor authentication. Disclosing this could draw a horde of attackers to the site, and its manifest insecurity would lead to a data breach. The researcher has contacted the insurer, the state insurance commissioner, and the problems are not yet fixed months later. Disclosing the problem to the media to generate pressure requires making a tradeoff: innocent people could be hurt as a result of the insurer not taking basic cybersecurity steps for the sensitivity of the data they demand. Without that disclosure, it is unclear how long the site will remain vulnerable and excessively lax in its handling of personal data.

Unfortunately, a few companies ignore the advice of CISA and others to accept such reports and fix the problems, and choose to send in their lawyers. This thin-skinned response is often employed by companies that should know better, such as when, in 2007, Cisco threatened to sue Blackhat over the work of researcher Mike Lynn.**

This year's example involved researchers who contacted the company Digilock *months in advance* of a presentation at DEF CON. The company irresponsibly sent a cease and desist demand containing possible "misunderstandings of the facts and the law" the day before the talk.***

Lately, the AI community has picked up the idea of coordinated disclosure, letting AI companies know about problems before the public. It's not clear if this has the same effect as security disclosure. For many uses of AI, the only organization that has a kerfuffle is the one with the AI system, and perhaps the arguments for coordinated disclosure come down differently.

Those who make products and services frequently tell us "Your security is important to us." Many of the world's largest companies have embraced the hackers at DEF CON: hiring us, throwing parties, sponsoring villages, and paying bounties as we report security problems. A few outlying firms still need to get the message and start behaving responsibly when they get bug reports.

*Wheeler, David A. 2024. "AI Cyber Challenge (AIxCC) semi-final results from DEF CON 32." Openwall. https://www.openwall.com/lists/oss-security/2024/08/16/7.
**Granick, Jennifer. 2005. "An Insider's View of 'Ciscogate.'" WIRED, August 5, 2005. https://www.wired.com/2005/08/an-insiders-view-of-ciscogate/.
***Roberts, Paul. 2024. "A Digital Lock Maker Tried To Squash A DEF CON Talk. It Happened Anyway. Here's Why." Security Ledger, August 18, 2024. https://securityledger.com/2024/08/a-digital-lock-maker-tried-to-squash-a-def-con-talk-it-happened-anyway-heres-why/.
Zhao, Hannah, Thorin Klosowski, and Andrew Crocker. 2024. "2 Fast 2 Legal: How EFF Helped a Security Researcher During DEF CON 32." Electronic Frontier Foundation, August 15, 2024. https://www.eff.org/deeplinks/2024/08/2-fast-2-legal-how-eff-helped-security-researcher-during-def-con-32.

APPENDIX B: DIGITAL RESOURCES

Links to all talks and villages referenced in the report are included in this section.

AI
- Village Website

AIxCC
- Village Website
- Georgia Tech zero-day discovery announcement
- Event recap post

Biohacking
- Village Website
- "Eradicating Hepatitis C with BioTerrorism" video
- "3DU: Homo (E)x Machina" video & presentation
- "Dysfunctional Unity: The Road to Nowhere" video & presentation

Ransomware
- "Behind Enemy Lines: Engaging and Disrupting Ransomware Web Panels" video & presentation

Elsewhere, in the DEF CON Universe
- "Exploiting Bluetooth from your car to the bank account$$" video & presentation
- "Hacking Millions of Modems (and Investigating Who Hacked My Modem)" video & blog post
- "Hi-Intensity Deconstruction: Chronicles of a Cryptographic Heist" video & presentation
- "Open Sesame: how vulnerable is your stuff in electronic lockers" video & presentation
- "Secrets and Shadows: Leveraging Big Data for Vulnerability Discovery at Scale" video & blog post
- "Building a secure resilient nationwide EV charging network" video
- "A Cyber Volunteer Task Force Model to Secure our Critical Infrastructure" video & website
- Voting Machine Hacking Village Website

DEF CON
- Website

University of Chicago Harris School of Public Policy - Cyber Policy Initiative
- Website

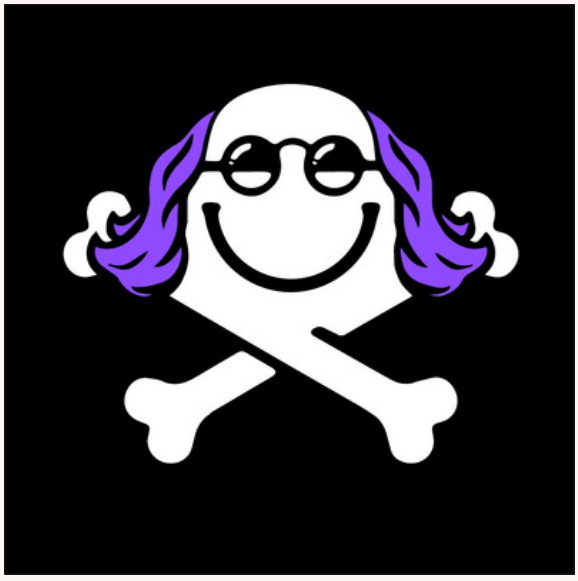
Images Used
- Cover Image - DEF CON Twitter
- Banner (body) - DEF CON Twitter

AN OPEN INVITATION TO POLICYMAKERS: COME TO DEF CON

The findings at DEF CON 32 demonstrated the depth, and breadth, of challenges in our nation. Amidst this "New Great Game," our environment is filled with new vulnerabilities and attack surfaces for adversaries. However, the double-edged nature of these technological exploits also gives us numerous advantages, if we choose to deploy them. If we are serious about winning, we should begin to consider hackers' exploits that also protect vulnerable people and organizations.

This report is an open invitation for policymakers to place further emphasis on DEF CON, its wealth of research, and its unique ethos. We invite policymakers to attend conferences, converse with our world-leading technologists and hackers, and attend keynote speeches and featured talks and villages (like the Policy Village) with an open mind. Without taking this community and many others like it seriously, we fear that the world's democracies will be outflanked, outmanned, and outgunned on the cyber battlefields of the New Great Game.

Thank you for reading the first ever *Hackers' Almanack.* Please stay tuned for updates and opportunities to engage by following DEF CON *Franklin* on our social media accounts.



Website: https://defconfranklin.com/
Email: defconfranklin@gmail.com
X & Bluesky: @DEFCONFranklin
LinkedIn: DEF CON Franklin

See you at DEF CON 33!