

# 1000 - Breaking Bitcoin Hardware Wallets

Sunday at 10:00 in Track 3

20 minutes | Demo, Exploit

**Josh Datko**\*Principal Engineer, Cryptotronix LLC\*

**Chris Quartier**\*Embedded Engineer, Cryptotronix, LLC\*

The security of your bitcoins rests entirely in the security of your private key. Bitcoin hardware wallets help protect against software-based attacks to recover or misuse your key. However, hardware attacks on these wallets are not as well studied. In 2015, Jochen Hoenicke was able to extract the private key from a TREZOR using a simple power analysis technique. While that vulnerability was patched, he suggested the Microcontroller on the TREZOR, which is also the same on the KeepKey, may be vulnerable to additional side channel attacks.

In this presentation we will quickly overview fault injection techniques, timing, and power analysis methods using the Open Source Hardware tool, the ChipWhisperer. We then show how to apply these techniques to the STM32F205 which is the MCU on the Trezor and KeepKey. Lastly, we will present our findings of a timing attack vulnerability and conclude with software and hardware recommendations to improve bitcoin hardware wallets. We will show and share our tools and methods to help you get started in breaking your own wallet!

Josh Datko

Josh Datko is the owner of Cryptotronix, an embedded security consultancy. As a submarine officer, he was sent to Afghanistan to ensure that the Taliban did not develop a submarine force—mission accomplished! He wrote a book on BeagleBones and crypto hardware which not many people have read, talked about embedded security at Portland BSides and HOPE, and presented a better way to make a hardware implant at DEF CON 22 which hopefully helped the NSA improve their spying.

Chris Quartier

Chris is the lead embedded hacker at Cryptotronix. He has worked at both big companies and IoT startups as an embedded developer working on bare metal and embedded linux board bring up, driver development, and trying to get those little logic analyzer clips to stay connected to a target. He's hacked on radios, rail guns, and fitness trackers but not all at the same time.

[#defcon25/by\\_track/track3/sunday](#)

[#defcon25/By\\_Day/\\_Sunday](#)

# 1000 - I Know What You Are by the Smell of Your Wifi

Sunday at 10:00 in Track 2

20 minutes | Art of Defense, Demo, Tool, Audience Participation,

**Denton Gentry\*Software Engineer\***

Existing fingerprinting mechanisms to identify client devices on a network tend to be coarse in their identification. For example they can tell it is an iPhone of some kind, or that it is a Samsung Android device of some model. They might look at DHCP information to know its OS, see if the client responds to SSDP, or check DNS-SD TXT responses.

By examining Wi-Fi Management frames we can identify the device much more specifically. We can tell a iPhone 5S from an iPhone 5, a Samsung Galaxy S8 from an S7, an LG G5 from a G4. This talk describes how the signature mechanism works.

Specifically identifying the client is the first step toward further scanning or analysis of that client's behavior on the network.

Denton Gentry

Denton Gentry is a software engineer who has worked at a lot of places and plans to work at a few more.

[#defcon25/by\\_track/track2/Sunday](#)

[#defcon25/By\\_Day/\\_Sunday](#)

# 1000 - Unboxing Android: Everything you wanted to know about Android packers

Sunday at 10:00 in 101 Track

45 minutes | Demo, Tool

**Avi Bashan\*Mobile R&D Team Leader, Check Point\***

**Slava Makkaveev\*Security Researcher, Check Point\***

To understand the Android ecosystem today, one must understand Android packers. Whether used for protecting legitimate apps' business logic or hiding malicious content, Android packer usage is on the rise. Android packers continue to increase their efforts to prevent reverse engineers and static analysis engines from understanding what's inside the package. To do so they employ elaborate tactics, including state of the art ELF tampering, obfuscation and various anti-debugging techniques.

In this talk, we will provide an overview of the packer industry and present real world test cases. We will do a deep technical dive into the internal workings of popular Android packers, exposing the different methods which protect the app's code. As a countermeasure, we will provide various techniques to circumvent them, allowing hackers and security researchers to unpack the secrets they withhold.

Avi Bashan

Avi Bashan is a Team Leader at Check Point, former security researcher at Lagoon Mobile Security. His daily job is to play around with Android Internals, writing Linux kernel code and drinking a lot of coffee.

Slava Makkaveev

Slava Makkaveev is a Security Researcher at Check Point. Slava has vast academic and professional experience in the security field. Slava's day to day is mostly composed from reversing and hacking malwares and operating systems for fun and profit.

#defcon25/by\_track/101/Sunday

#defcon25/By\_Day/\_Sunday

## 1000 - Untrustworthy Hardware and How to Fix It

Sunday at 10:00 in Track 4

20 minutes | Demo, Tool

**Octane \*Hacker\***

Modern computing platforms offer more freedom than ever before. The rise of Free and Open Source Software has led to more secure and heavily scrutinized cryptographic solutions. However, below the surface of open source operating systems, strictly closed source firmware along with device driver blobs and closed system architecture prevent users from examining, understanding, and trusting the systems where they run their private computations. Embedded technologies like Intel Management Engine pose significant threats when, not if, they get exploited. Advanced attackers in possession of firmware signing keys, and even potential access to chip fabrication, could wreak untold havoc on cryptographic devices we rely on.

After surveying all-too-possible low level attacks on critical systems, we will introduce an alternative open source solution to peace-of-mind cryptography and private computing. By using programmable logic chips, called Field Programmable Gate Arrays, this device is more

open source than any common personal computing system to date. No blobs, no hidden firmware features, and no secret closed source processors. This concept isn't "unhackable", rather we believe it to be the most fixable; this is what users and hackers should ultimately be fighting for.

Octane

Octane is a longtime hobbyist hacker, with experience primarily in UNIX systems and hardware. Holding no official training or technical employment, Octane spends most of their free time building and restoring older computer systems, hanging out at surplus stores and tracking down X86 alternatives with an occasional dabbling in OSX and 802.11 exploitation. Other interests include SDR and RF exploration, networking, cryptography, computer history, distributed computing...really anything that sounds cool that I happen to stumble on at 3am.

[#defcon25/by\\_track/track4/sunday](#)

[#defcon25/By\\_Day/\\_Sunday](#)

## 1030 - BITSInject

Sunday at 10:30 in Track 3

20 minutes | Demo, Tool

**Dor Azouri**\*Security researcher, @SafeBreach\*

Windows' BITS service is a middleman for your download jobs. You start a BITS job, and from that point on, BITS is responsible for the download. But what if we tell you that BITS is a careless middleman? We have uncovered the way BITS maintains its jobs queue using a state file on disk, and found a way for a local administrator to control jobs using special modifications to that file

Comprehending this file's binary structure allowed us to change a job's properties (such as RemoteURL, Destination Path...) in runtime and even inject our own custom job, using none of BITS' public interfaces. This method, combined with the generous notification feature of BITS, allowed us to run a program of our will as the LocalSystem account, within session 0. So if you wish to execute your code as NT AUTHORITY/SYSTEM and the first options that come to mind are psexec/creating a service, we now add a new option: BITSInject.

Here, we will not only introduce the practical method we formed, but also: Reveal the binary structure of the state file for you to play with, and some knowledge we gathered while researching the service flow

We will also provide free giveaways: A one-click python tool that performs the described method; SimpleBITSServer - a pythonic BITS server; A struct definition file, to use for parsing your BITS state file

Dor Azouri

Dor Azouri is a security professional, having 6+ years of unique experience with network security, malware research and infosec data analysis. Currently doing security research @SafeBreach.

#defcon25/by\_track/track3/sunday

#defcon25/By\_Day/\_Sunday

## 1030 - Ghost in the Droid: Possessing Android Applications with ParaSpectre

Sunday at 10:30 in Track 4

20 minutes | Demo, Tool

**chaosdata** \*Senior Security Consultant, NCC Group\*

Modern Android applications are large and complex, and can be a pain to analyze even without obfuscation - static analysis can only get one so far, the debugger sucks, Frida doesn't give you enough access to the Java environment, and editing smali or writing Xposed hooks can be time consuming and error prone. There has to be a better way!

What if we could inject a command line REPL into an app to drive functionality? And what if we could also make writing function hooks fast and easy?

In this talk, I will introduce ParaSpectre, a platform for dynamic analysis of Android applications that injects JRuby into Android applications. It bundles a hook configuration web API, a web application interface to configure and edit hooks, and a connect-back JRuby REPL to aid application exploration from the inside-out. It supports various selectors to match classes and methods, can be reconfigured on-the-fly without requiring a device reboot, and takes the pain out of writing method hooks for Android apps.

ParaSpectre is for developers and security researchers alike. While not itself a debugger, it provides a level of access into a running application that a debugger generally won't.

chaosdata

chaosdata(aka "Jeff") is a security consultant by day, and sometimes by night. He hacks on embedded systems, mobile apps and devices, web apps, and complicated things that don't have names. He also likes exotic candies.

@chaosdatumz

#defcon25/by\_track/track4/sunday

#defcon25/By\_Day/\_Sunday

## 1030 - PEIMA (Probability Engine to Identify Malicious Activity): Using Power Laws to address Denial of Service Attacks

Sunday at 10:30 in Track 2

20 minutes | Art of Defense, Demo, Tool

**Redezem\*Hacker\***

Denial of service. It requires a low level of resources and knowledge, it is very easy to deploy, it is very common and it is remarkable how effective it is overall. PEIMA is a brand new method of client side malicious activity detection based on mathematical laws, usually used in finance, text retrieval and social media analysis, that is fast, accurate, and capable of determining when denial of service attacks start and stop without flagging legitimate heavy interest in your server erroneously. However, denial of service attacks aren't the only type of anomalous activity you can look at with PEIMA. Learn what kinds of unusual identifying metrics you can get out of your network and users to help detect intrusions and, ultimately, defend your assets.

Redezem

Redezem hails from the southern hemisphere, specifically Perth, Australia, the most isolated capital city on the planet. He's been an avid computer tinkerer in this desolate, sunny, beach-ridden wasteland from a young age, and has been a "hacker" since he stole his dad's passwords to get at the internet as a kid. Having worked part time as a web application developer during his undergraduate degree in computer science, he specialised into intrusion detection in his honours year, and is currently performing his PhD into new and fantastic network anomaly detection mechanisms at Curtin University. He currently also lectures, and works part-time as a security consultant.

#defcon25/by\_track/track2/Sunday

#defcon25/By\_Day/\_Sunday

## 1100 - 'Ghost Telephonist' Impersonates You Through LTE CSFB

Sunday at 11:00 in Track 4

45 minutes | Exploit

**Yuwei Zheng\*Hacker\***

**Lin Huang\*Hacker\***

One vulnerability in CSFB (Circuit Switched Fallback) in 4G LTE network will be presented. In the CSFB procedure, we found the authentication step is missing. This results in that an attacker can hijack the victim's communication. We named this attack as 'Ghost Telephonist'. Several exploitations can be made based on this vulnerability. When the call or SMS is not encrypted, or weakly encrypted, the attacker can impersonate the victim to receive the "Mobile Terminated" calls and messages or to initiate the "Mobile Originated" calls and messages. Furthermore, Telephonist Attack can obtain the victim's phone number and then use the phone number to make advanced attack, e.g. breaking Internet online accounts. These attacks can randomly choose victims, or target a given victim. We verified these attack with our own phones in operators' network in a small controllable scale. The experiments proved the vulnerability really exists. The attack doesn't need fake base station so the attack cost is low. The victim doesn't sense being attacked since no fake base station and no cell re-selection. Now we are collaborating with operators and terminal manufactures to fix this vulnerability.

Yuwei Zheng

Yuwei Zheng is a senior security researcher from Radio Security Research Dept. of 360 Technology. He has rich experiences in embedded systems over 10 years. He reversed blackberry BBM, PIN, BIS push mail protocol, and decrypted the network stream successfully in 2011. He successfully implemented a MITM attack for Blackberry BES based on a modified ECMQV protocol of RIM. He focuses on the security issues of embedded hardware and IOT systems. He was the speaker of DEF CON , HITB etc.

@huanglin\_bupt

Lin Huang

Lin HUANG is a wireless security researcher and SDR technology expert, from Radio Security Research Dept. of 360 Technology. Her interests include the security issues in wireless communication, especially the cellular network security. She was the speaker of some security conferences, DEF CON , HITB, POC etc. She is the 3GPP SA3 delegate of 360 Technology.

Contributor Acknowledgement:

The Speakers would like to acknowledge Qing YANG, for his contribution to the presentation.

Qing YANG is the founder of UnicornTeam & Radio Security Research Department in 360 Technology. He has rich experiences in information security area. He made presentations at BlackHat, DEF CON , CanSecWest, HITB, Ruxcon, POC, XCon, China ISC etc.

#defcon25/by\_track/track4/sunday

#defcon25/By\_Day/\_Sunday

## 1100 - Backdooring the Lottery and Other Security Tales in Gaming over the Past 25 Years

Sunday at 11:00 in Track 2

45 minutes

**Gus Fritschie\*CTO, SeNet International\***

**Evan Teitelman\*Engineer, SeNet International\***

In this talk Gus and Evan will discuss the recent Hot Lotto fraud scandal and how one MUSL employee, Eddie Tipton, was able to rig several state lotteries and win \$17 million (or perhaps more). Gus' firm is actively supporting the prosecution in this case. Evan was responsible for identifying and analyzing how Eddie was able to rig the RNG.

Details on the rigged RNG and other details from the case will be presented publicly for the first time during this talk.

For historical context other related attacks including the Ron Harris and hacking keno in the 1990's and a recent incident involving a Russian hacking syndicate's exploitation of slot machines will also be discussed.

Gus Fritschie

Gus Fritschie has been involved in information security since 2000. About 5 years ago (after his previous DEF CON presentation on iGaming security) he transitioned a significant portion of his practice into the gaming sector. Since then he has established himself and SeNet as the IT security leader in in gaming. He has supported a number of clients across the gaming spectrum from iGaming operators, land-based casinos, gaming manufacturer, lotteries, tribal gaming, and daily fantasy sports. In his free time he is a recreationally poker player (both online and B&M).

@gfritschie

@senetsecurity

Evan Teitelman



Bio coming soon.

#defcon25/by\_track/track2/Sunday

#defcon25/By\_Day/\_Sunday

## 1100 - Exploiting Continuous Integration (CI) and Automated Build systems

Sunday at 11:00 in Track 3

45 minutes | Demo, Tool, Exploit

**spaceB0x**\*Sr. Security Engineer at LeanKit Inc.\*

Continuous Integration (CI) systems and similar architecture has taken new direction, especially in the last few years. Automating code builds, tests, and deployments is helping hordes of developers release code, and is saving companies a great amount of time and resources. But at what cost? The sudden and strong demand for these systems have created some widely adopted practices that have large security implications, especially if these systems are hosted internally. I have developed a tool that will help automate some offensive testing against certain popular CI build systems. There has been a large adoption of initiating these builds through web hooks of various kinds, especially changes to public facing code repositories. I will start with a brief overview of some of the more popular CI tools and how they are being used in many organizations. This is good information for understanding, at a high level, the purpose of these systems as well as some security benefits that they can provide. From there we will dive into specific examples of how these different CI implementations have created vulnerabilities (in one case to a CI vendor themselves). Last we will explore the tool, its purpose, and a demonstration of its use. This tool takes advantage of the configurations of various components of the build chain to look for vulnerabilities. It then has the capability to exploit, persist access, command and control vulnerable build containers. Most of the demonstration will revolve around specific CI products and repositories, however the concepts are applicable across most build systems. The goal here is to encourage further exploration of these exploitation concepts. The tool is built "modularly" to facilitate this. If you are new to CI and automated build systems, or if you have been doing it for years, this talk and tool will help you to better secure your architecture

spaceB0x

spaceB0x is extremely dedicated to his work in information security. He is the Sr. Security Engineer at a software company called LeanKit. He likes, and occasionally succeeds at, security dev-opsing, web application and network penetration testing, and some other security things. He has written tools for secure key management within automation infrastructures, capturing netflow data, and pwning automated build systems. He loves the

hacker community, learning new things, and exploring new ideas.

@spaceB0xx

Website: [www.untamedtheory.com](http://www.untamedtheory.com)

#defcon25/by\_track/track3/sunday

#defcon25/By\_Day/\_Sunday

## 1100 - Total Recall: Implanting Passwords in Cognitive Memory

Sunday at 11:00 in 101 Track

45 minutes

### Tess Schrodinger

What is cognitive memory? How can you "implant" a password into it? Is this truly secure? Curiosity around these questions prompted exploration of the research and concepts surrounding the idea of making the authentication process more secure by implanting passwords into an individual's memory. The result? The idea is that you are not able to reveal your credentials under duress but you are still able to authenticate to a system. We will begin with an understanding of cognitive memory. Implicit versus explicit memory will be defined. The concepts of the subconscious, unconscious, and consciousness will be addressed. The stages of memory pertaining to encoding, storage and retrieval as well as the limitations of human memory along with serial interception sequence learning training will round out our build up to the current research and experimentation being done with the proposal to implant passwords into an individual's cognitive memory.

Tess Schrodinger

Tess is a security engineer and researcher with over twenty years of experience in security and counterintelligence. Her areas of interest are Insider Threat, Quantum Computing, Security Awareness, Cryptography, and Triathlons.

@TessSchrodinger

#defcon25/by\_track/101/Sunday

#defcon25/By\_Day/\_Sunday

## 1200 - Are all BSDs created equally? A survey of BSD kernel vulnerabilities.

Sunday at 12:00 in Track 2

45 minutes | Demo

**Ilja van Sprundel**\*Director of penetration testing, IOActive\*

In this presentation I start off asking the question "How come there are only a handful of BSD security kernel bugs advisories released every year?" and then proceed to try and look at some data from several sources. It should come as no surprise that those sources are fairly limited and somewhat outdated.

The presentation then moves on to try and collect some data ourselves. This is done by actively investigating and auditing. Code review, fuzzing, runtime testing on all 3 major BSD distributions [NetBSD/OpenBSD/FreeBSD]. This is done by first investigating what would be good places where the bugs might be. Once determined, a detailed review is performed of these places. Samples and demos will be shown.

I end the presentation with some results and conclusions. I will list what the outcome was in terms of bugs found, and who -based on the data I now have- among the 3 main BSD distributions can be seen as the clear winner and loser. I will go into detail about the code quality observed and give some pointers on how to improve some code. Lastly I will try and answer the question I set out to answer ("How come there are only a handful of BSD security kernel bugs advisories released every year?").

Ilja van Sprundel

Ilja van Sprundel is experienced in exploit development and network and application testing. As IOActive's Director of Penetration Testing, he performs primarily gray-box penetration testing engagements on mobile (specializing in iOS) and runtime (specializing in Windows kernel) applications that require customized fuzzing and source code review, identifying system vulnerabilities, and designing custom security solutions for clients in technology development telecommunications, and financial services. van Sprundel specializes in the assessment of low-level kernel code and architecture/infrastructure design, having security reviewed literally hundreds of thousands of lines of code. However, as a Director, he also functions in a managerial capacity by overseeing penetration testing engagements, providing oversight regarding technical accuracy, serving as the point of contact between technical consultants and technical stakeholders, and ensuring that engagements are delivered on time and in alignment with customer's expectations. van Sprundel also is responsible to mentor and guide Associate-level consultants as they grow both their penetration testing and general consulting skillsets. He is the driver behind the team's implementation of cutting-edge techniques and tools, guided by both research and successful exploits performed during client engagements.

# 1200 - Genetic Diseases to Guide Digital Hacks of the Human Genome: How the Cancer Moonshot Program will Enable Almost Anyone to Crash the Operating System that Runs You or to End Civilization...

Sunday at 12:00 in Track 4

45 minutes

**John Sotos\*Chief Medical Officer, Intel Corporation\***

The human genome is, fundamentally, a complex open-source digital operating system (and set of application programs) built on the digital molecules DNA and RNA.

The genome has thousands of publicly documented, unpatchable security vulnerabilities, previously called "genetic diseases." Because emerging DNA/RNA technologies, including CRISPR-Cas9 and especially those arising from the Cancer Moonshot program, will create straightforward methods to digitally reprogram the genome in free-living humans, malicious exploitation of genomic vulnerabilities will soon be possible on a wide scale.

This presentation shows the breathtaking potential for such hacks, most notably the exquisite targeting precision that the genome supports – in effect, population, and time – spanning annoyance to organized crime to civilization-ending pandemics far worse than Ebola.

Because humans are poor at responding to less-than-immediate threats, and because there is no marketplace demand for defensive technologies on the DNA/RNA platform, the hacker community has an important role to play in devising thought-experiments to convince policy makers to initiate defensive works, before offensive hacks can be deployed in the wild.

Hackers can literally save the world... from ourselves.

John Sotos

John Sotos is Chief Medical Officer at Intel Corporation. He has been programming computers continuously since 1970, excepting four years of medical school at Johns Hopkins, where he also trained as a transplantation cardiologist. His professional interests include hacking the medical diagnostic process, first with a book on edge cases, called "Zebra Cards: An Aid to Obscure Diagnosis," followed by six years as a medical technical consultant on the popular television series "House, MD." His masters degree in artificial intelligence is from Stanford, and he is a co-founder of [Expertscape.com](https://www.expertscape.com). He is a long-time air rescue flight

surgeon for the National Guard; however, the opinions presented here are his own, and do not necessarily represent those of the Department of Defense or Intel.

[www.intel.com](http://www.intel.com)

[www.sotos.com](http://www.sotos.com)

#defcon25/by\_track/track4/sunday

#defcon25/By\_Day/\_Sunday

## 1200 - The Black Art of Wireless Post Exploitation

Sunday at 12:00 in 101 Track

45 minutes | Demo, Tool

**Gabriel "solstice" Ryan\*Gotham Digital Science\***

Most forms of WPA2-EAP have been broken for nearly a decade. EAP-TTLS and EAP-PEAP have long been susceptible to evil twin attacks, yet most enterprise organizations still rely on these technologies to secure their wireless infrastructure. The reason for this is that the secure alternative, EAP-TLS, is notoriously arduous to implement. To compensate for the weak perimeter security provided by EAP-TTLS and EAP-PEAP, many organizations use port based NAC appliances to prevent attackers from pivoting further into the network after the wireless has been breached. This solution is thought to provide an acceptable balance between security and accessibility. The problem with this approach is that it assumes that EAP is exclusively a perimeter defense mechanism. In this presentation, we will present a novel type of rogue access point attack that can be used to bypass port-based access control mechanisms in wireless networks. In doing so, we will challenge the assumption that reactive approaches to wireless security are an acceptable alternative to strong physical layer protections such as WPA2-EAP using EAP-TLS.

Gabriel "solstice" Ryan

Gabriel is a pentester, CTF player, and Offsec R&D. He currently works for Gotham Digital Science, where he provides full scope red team penetration testing capabilities for a diverse range of clients. Previously he has worked at OGSysystems and Rutgers University. He also is a member of the BSides Las Vegas senior staff, coordinating wireless security for the event. Things that make him excited include obscure wireless attacks, evading antivirus, and playing with fire. In his spare time, he enjoys live music and riding motorcycles.

@s0lst1c3

[github.com/s0lst1c3](https://github.com/s0lst1c3)

[solstice.me](http://solstice.me)

## 1200 - The call is coming from inside the house! Are you ready for the next evolution in DDoS attacks?

Sunday at 12:00 in Track 3

45 minutes | Art of Defense

**Steinthor Bjarnason\***Senior Network Security Analyst, Arbor Networks\*

**Jason Jones\***Security Architect, Arbor Networks\*

The second half of 2016 saw the rise of a new generation of IoT botnets consisting of webcams and other IoT devices. These botnets were then subsequently used to launch DDoS attacks on an unprecedented scale against Olympic-affiliated organizations, OVH, the web site of Brian Krebs and Dyn.

Early 2017, a multi-stage Windows Trojan containing code to scan for vulnerable IoT devices and inject them with Mirai bot code was discovered. The number of IoT devices which were previously safely hidden inside corporate perimeters, vastly exceeds those directly accessible from the Internet, allowing for the creation of botnets with unprecedented reach and scale.

This reveals an evolution in the threat landscape that most organizations are completely unprepared to deal with and will require a fundamental shift in how we defend against DDoS attacks.

This presentation will include:

- An analysis of the Windows Mirai seeder including its design, history, infection vectors and potential evolution.
- The DDoS capabilities of typically infected IoT devices including malicious traffic analysis.
- The consequences of infected IoT devices inside the corporate network including the impact of DDoS attacks, originating from the inside, targeting corporate assets and external resources.
- How to detect, classify and mitigate this new threat.

Steinthor Bjarnason

Steinthor Bjarnason is a Senior Network Security Analyst on Arbor Networks ASERT team, performing applied research on new technologies and solutions to defend against DDoS

attacks.

Steinthor has 17 years of experience working on Internet Security, Cloud Security, SDN Security, Core Network Security and DDoS attack mitigation. Steinthor is an inventor and principal of the Cisco Autonomic Networking Initiative, with a specific focus on Security Automation where he holds a number of related patents.

@sbjarnas

Jason Jones

Jason Jones is the Security Architect for Arbor Networks' ASERT team. His primary role involves reverse engineering malware, architecting of internal malware processing infrastructure, feed infrastructure and botnet monitoring infrastructure in addition to other development tasks. Jason has spoken at various industry conferences including BlackHat USA, FIRST, BotConf, REcon, and Ruxcon

#defcon25/by\_track/track3/sunday

#defcon25/By\_Day/\_Sunday

## 1300 - Bypassing Android Password Manager Apps Without Root

Sunday at 13:00 in Track 2

45 minutes | Demo, Exploit

**Stephan Huber\***Fraunhofer SIT\*

**Siegfried Rasthofer\***Fraunhofer SIT\*

Security experts recommend using different, complex passwords for individual services, but everybody knows the issue arising from this approach: It is impossible to keep all the complex passwords in mind. One solution to this issue are password managers, which aim to provide a secure, centralized storage for credentials. The rise of mobile password managers even allows the user to carry their credentials in their pocket, providing instant access to these credentials if required. This advantage can immediately turn into a disadvantage as all credentials are stored in one central location. What happens if your device gets lost, stolen or a hacker gets access to your device? Are your personal secrets and credentials secure?

We say no! In our recent analysis of well-known Android password manager apps, amongst them are vendors such as LastPass, Dashlane, 1Password, Avast, and several others, we aimed to bypass their security by either stealing the master password or by directly accessing the

stored credentials. Implementation flaws resulted in severe security vulnerabilities. In all of those cases, no root permissions were required for a successful attack. We will explain our attacks in detail. We will also propose possible security fixes and recommendations on how to avoid the vulnerabilities.

Stephan Huber

Stephan Huber is a security researcher at the Testlab mobile security group at the Fraunhofer Institute for Secure Information Technology (SIT). His main focus is Android application security testing and developing new static and dynamic analysis techniques for app security evaluation. He found different vulnerabilities in well-known Android applications and the AOSP. In his spare time he enjoys teaching students in Android hacking.

Siegfried Rasthofer

Siegfried Rasthofer is a vulnerability- and malware-researcher at Fraunhofer SIT (Germany) and his main research focus is on applied software security on Android applications. He developed different tools that combine static and dynamic code analysis for security purposes and he is the founder of the CodeInspect reverse engineering tool. He likes to break Android applications and found various AOSP exploits. Most of his research is published at top tier academic conferences and industry conferences like DEF CON, BlackHat, HiTB, AVAR or VirusBulletin.

#defcon25/by\_track/track2/Sunday

#defcon25/By\_Day/\_Sunday

## 1300 - Game of Chromes: Owning the Web with Zombie Chrome Extensions

Sunday at 13:00 in 101 Track

45 minutes | Demo

**Tomer Cohen\***R&D Security Team Leader, Wix.com\*

On April 16 2016, an army of bots stormed upon Wix servers, creating new accounts and publishing shady websites in mass. The attack was carried by a malicious Chrome extension, installed on tens of thousands of devices, sending HTTP requests simultaneously. This "Extension Bot" has used Wix websites platform and Facebook messaging service, to distribute itself among users. Two months later, same attackers strike again. This time they used infectious notifications, popping up on Facebook and leading to a malicious Windows-runnable JSE file. Upon clicking, the file ran and installed a Chrome extension on the victim's browser. Then the extension used Facebook messaging once again to pass itself on to more victims.



Analyzing these attacks, we were amazed by the highly elusive nature of these bots, especially when it comes to bypassing web-based bot-detection systems. This shouldn't be surprising, since legit browser extensions are supposed to send Facebook messages, create Wix websites, or in fact perform any action on behalf of the user.

On the other hand, smuggling a malicious extension into Google Web Store and distributing it among victims efficiently, like these attackers did, is let's say - not a stroll in the park. But don't worry, there are other options.

Recently, several popular Chrome extensions were found to be vulnerable to XSS. Yep, the same old XSS every rookie finds in so many web applications. So browser extensions suffer from it too, and sadly, in their case it can be much deadlier than in regular websites. One noticeable example is the Adobe Acrobat Chrome extension, which was silently installed on January 10 by Adobe, on an insane number of 30 million devices. A DOM-based XSS vulnerability in the extension (found by Google Project Zero) allowed an attacker to craft a content that would run Javascript as the extension.

In this talk I will show how such a flaw leads to full and permanent control over the victim's browser, turning the extension into zombie. Additionally, Shedding more light on the 2016 attacks on Wix and Facebook described in the beginning, I will demonstrate how an attacker can use similar techniques to distribute her malicious payload efficiently on to new victims, through popular social platforms - creating the web's most powerful botnet ever.

Tomer Cohen

Tomer Cohen leads the team at [Wix.com](https://wix.com) responsible for all R&D and production systems security. Previous to that, Tomer has worked as an application security expert in several firms. Tomer was also one of the founders of "Magshimim" cyber training program, which teaches development and cyber security among high-school students in the periphery of Israel.

[#defcon25/by\\_track/101/Sunday](#)

[#defcon25/By\\_Day/\\_Sunday](#)

## 1300 - Malicious CDNs: Identifying Zbot Domains en Masse via SSL Certificates and Bipartite Graphs

Sunday at 13:00 in Track 3

45 minutes | Art of Defense

**Thomas Mathew\***OpenDNS (Cisco)\*

**Dhia Mahjoub\***Head of Security Research, Cisco Umbrella (OpenDNS)\*

Prior research detailing the relationship between malware, bulletproof hosting, and SSL gave researchers methods to investigate SSL data only if given a set of seed domains. We present a novel statistical technique that allow us to discover botnet and bulletproof hosting IP space by examining SSL distribution patterns from open source data while working with limited or no seed information. This work can be accomplished using open source datasets and data tools.

SSL data obtained from scanning the entire IPv4 namespace can be represented as a series of 4 million node bipartite graphs where a common name is connected to either an IP/CIDR/ASN via an edge. We use the concept of relative entropy to create a pairwise distance metric between any two common names and any two ASNs. The metric allows us to generalize the concept of regular and anomalous SSL distribution patterns.

Relative entropy is useful in identifying domains that have anomalous network structures. The domains we found in this case were related to the Zbot proxy network. The Zbot proxy network contains a structure similar to popular CDNs like Akamai, Google, etc but instead rely on compromised devices to relay their data. Through layering these SSL signals with passive DNS data we create a pipeline that can extract Zbot domains with high accuracy.

Thomas Mathew

Thomas Mathew is a Security Researcher at OpenDNS (now part of Cisco) where he works on implementing pattern recognition algorithms to classify malware and botnets. His main interest lies in using various time series techniques on network sensor data to identify malicious threats. Previously, Thomas was a researcher at UC Santa Cruz, the US Naval Postgraduate School, and as a Product and Test Engineer at handsfree streaming video camera company Looxcie, Inc. He presented at ISOI APT, BruCon, FloCon and Kaspersky SAS.

Dhia Mahjoub

Dr. Dhia Mahjoub is the Head of Security Research at Cisco Umbrella (OpenDNS). He leads the core research team focused on large scale threat detection and threat intelligence and advises on R&D strategy. Dhia has a background in networks and security, has co-authored patents with OpenDNS and holds a PhD in graph algorithms applied on Wireless Sensor Networks problems. He regularly works with prospects and customers and speaks at conferences worldwide including Black Hat, Defcon, Virus Bulletin, BotConf, ShmooCon, FloCon, Kaspersky SAS, Infosecurity Europe, RSA, Usenix Enigma, ACSC, NCSC, and Les Assises de la sécurité.

[#defcon25/by\\_track/track3/sunday](#)

[#defcon25/By\\_Day/\\_Sunday](#)

# 1300 - Revoke-Obfuscation: PowerShell Obfuscation Detection (And Evasion) Using Science

Sunday at 13:00 in Track 4

45 minutes | Art of Defense, Demo, Tool

**Daniel Bohannon (DBO)\*Senior Consultant, MANDIANT\***

**Lee Holmes\*Lead Security Architect, Microsoft\***

Attackers, administrators and many legitimate products rely on PowerShell for their core functionality. However, its power has made it increasingly attractive for attackers and commodity malware authors alike. How do you separate the good from the bad?

A/V signatures applied to command line arguments work sometimes. AMSI-based (Anti-malware Scan Interface) detection performs significantly better. But obfuscation and evasion techniques like Invoke-Obfuscation can and do bypass both approaches.

Revoke-Obfuscation is a framework that transforms evasion into a treacherous deceit. By applying a suite of unique statistical analysis techniques against PowerShell scripts and their structures, what was once a cloak of invisibility is now a spotlight. It works with .evtx files, command lines, scripts, ScriptBlock logs, Module logs, and is easy to extend.

Approaches for evading these detection techniques will be discussed and demonstrated.

Revoke-Obfuscation has been used in numerous Mandiant investigations to successfully identify obfuscated and non-obfuscated malicious PowerShell scripts and commands. It also detects all obfuscation techniques in Invoke-Obfuscation, including two new techniques being released with this presentation.

Daniel Bohannon (DBO)

Daniel Bohannon is a Senior Incident Response Consultant at MANDIANT with over seven years of operations and information security experience. He is the author of the Invoke-Obfuscation and Invoke-CradleCrafter PowerShell obfuscation frameworks

@danielhbohannon

Lee Holmes

Lee Holmes is the lead security architect of Microsoft's Azure Management group, covering Azure Stack, System Center, and Operations Management Suite. He is author of the Windows

PowerShell Cookbook, and an original member of the PowerShell development team.

@Lee\_Holmes, <http://www.leeholmes.com/blog/>

#defcon25/by\_track/track4/sunday

#defcon25/By\_Day/\_Sunday

## 1400 - Call the plumber - you have a leak in your (named) pipe

Sunday at 14:00 in 101 Track

45 minutes | Demo

**Gil Cohen\*CTO, Comsec group\***

The typical security professional is largely unfamiliar with the Windows named pipes interface, or considers it to be an internal-only communication interface.

As a result, open RPC (135) or SMB (445) ports are typically considered potentially entry points in "infrastructure" penetration tests.

However, named pipes can in fact be used as an application-level entry vector for well known attacks such as buffer overflow, denial of service or even code injection attacks and XML bombs, depending on the nature of listening service to the specific pipe on the target machine.

As it turns out, it seems that many popular and widely used Microsoft Windows-based enterprise applications open a large number of named pipes on each endpoint or server on which they are deployed, significantly increase an environment's attack surface without the organization or end user being aware of the risk.

Since there's a complete lack of awareness to the entry point, there's very limited options available to organizations to mitigate it, making it a perfect attack target for the sophisticated attacker.

In this presentation we will highlight how named pipes have become a neglected and forgotten external interface. We will show some tools that can help find vulnerable named pipes, discuss the mitigations, and demonstrate the exploitation process on a vulnerable interface.

Gil Cohen

Gil is an experienced application security instructor, architect, consultant and pentester just starting his 12th year in the field.

With past experience in the civilian, government and military cyber security industries, Gil currently serves as the CTO of Comsec Group, in charge of training, research, service lines, methodologies and quality assurance.

With a long time record as an SQL injection fanatic, Gil was responsible for publishing the "SQL Injection Anywhere" technique in 2010, which is currently in use in a variety of automated scanners in the market, and enables the blind detection and exploitation of potential injections in any part of the SQL statement.

He also has a taste for nostalgia, and has been working for a while on abuses to protocols that software developers would prefer to forget.

@Gilco83

[www.facebook.com/gilc83](https://www.facebook.com/gilc83)

#defcon25/by\_track/101/Sunday

#defcon25/By\_Day/\_Sunday

## 1400 - Friday the 13th: JSON attacks!

Sunday at 14:00 in Track 4

45 minutes | Demo, Exploit

**Alvaro Muñoz\***Principal Security Researcher,Hewlett Packard Enterprise\*

**Oleksandr Mirosh\***Senior Security QA Engineer, Hewlett Packard Enterprise\*

2016 was the year of Java deserialization apocalypse. Although Java Deserialization attacks were known for years, the publication of the Apache Commons Collection Remote Code Execution (RCE from now on) gadget finally brought this forgotten vulnerability to the spotlight and motivated the community to start finding and fixing these issues.

One of the most suggested solutions for avoiding Java deserialization issues was to move away from Java Deserialization altogether and use safer formats such as JSON. In this talk, we will analyze the most popular JSON parsers in both .NET and Java for potential RCE vectors.

We will demonstrate that RCE is also possible in these libraries and present details about the ones that are vulnerable to RCE by default. We will also discuss common configurations that make other libraries vulnerable.

In addition to focusing on JSON format, we will generalize the attack techniques to other serialization formats. In particular, we will pay close attention to several serialization formats in .NET. These formats have also been known to be vulnerable since 2012 but the lack of known RCE gadgets led some software vendors to not take this issue seriously. We hope this talk will change this. With the intention of bringing the due attention to this vulnerability class in .NET, we will review the known vulnerable formats, present other formats which we found to be vulnerable as well and conclude presenting several gadgets from system libraries that may be used to achieve RCE in a stable way: no memory corruption – just simple process invocation.

Finally, we will provide recommendations on how to determine if your code is vulnerable, provide remediation advice, and discuss alternative approaches.

Alvaro Muñoz

Alvaro Muñoz (@pwntester) works as Principal Software Security Researcher with HPE Security Fortify, Software Security Research (SSR). His research focuses on different programming languages and web application frameworks searching for vulnerabilities or unsafe uses of APIs. Before joining the research team, he worked as an Application Security Consultant helping enterprises to deploy their application security programs. Muñoz has presented at many Security conferences including DEF CON , RSA, AppSecEU, Protect, DISCCON, etc and holds several infosec certifications, including OSCP, GWAPT and CISSP, and is a proud member of int3pids CTF team. He blogs at <http://www.pwntester.com>.

@pwntester

Oleksandr Mirosh

Oleksandr Mirosh has over 9 years of computer security experience, including vulnerability research, penetration testing, reverse engineering, fuzzing, developing exploits and consulting. He is working for HPE Software Security Research team investigating and analyzing new threats, vulnerabilities, security weaknesses, new techniques of exploiting security issues and development vulnerability detection, protection and remediation rules. In the past, he has performed a wide variety of security assessments, including design and code reviews, threat modelling, testing and fuzzing in order to identify and remove any existing or potentially emerging security defects in the software of various customers.

[#defcon25/by\\_track/track4/sunday](#)

[#defcon25/By\\_Day/\\_Sunday](#)

## 1400 - Man in the NFC

Sunday at 14:00 in Track 3

45 minutes | Demo, Tool

**Haoqi Shan\*Wireless security researcher\***

**Jian Yuan\*Wireless security researcher\***

NFC (Near Field Communication) technology is widely used in security, bank, payment and personal information exchange fields now, which is highly well-developed. Corresponding, the attacking methods against NFC are also emerged in endlessly. To solve this problem, we built a hardware tool which we called "UniProxy". This tool contains two self-modified high frequency card readers and two radio transmitters, which is a master-slave way. The master part can help people easily and successfully read almost all ISO 14443A type cards, (no matter what kind of this card is, bank card, ID card, Passport, access card, or whatever. No matter what security protocol this card uses, as long as it meets the ISO 14443A standard) meanwhile replaying this card to corresponding legal card reader via slave part to achieve our "evil" goals. The master and slave communicate with radio transmitters and can be apart between 50 - 200 meters.

Haoqi Shan

Haoqi Shan is currently a wireless/hardware security researcher in UnicornTeam of 360 Radio Security Research Dept. He focuses on Wi-Fi penetration, GSM system, embedded device hacking, building hacking tools, etc. He made serial presentations about Femto cell hacking, RFID hacking and LTE devices hacking on DEF CON , Cansecwest, Syscan360 and HITB, etc.

Jian Yuan

Yuan Jian is a security researcher in UnicornTeam of 360 Radio Security Research Dept. He is mainly focused on the security of Internet of things, NFC, GPS, etc. He was a speaker at the DEF CON Car Hacking Village.

Contributor Acknowledgement:

The Speakers would like to acknowledge Yuan Jian, for his contribution to the presentation. Yuan Jian is a security researcher in UnicornTeam of 360 Radio Security Research Dept. He is mainly focused on the security of Internet of things, NFC, GPS, etc. He was a speaker at the DEF CON Car Hacking Village.

[#defcon25/by\\_track/track3/sunday](#)

[#defcon25/By\\_Day/\\_Sunday](#)

## 1400 - Weaponizing Machine Learning: Humanity Was

# Overrated Anyway

Sunday at 14:00 in Track 2

45 minutes | Demo, Tool

**Dan "AltF4" Petro\***Senior Security Associate, Bishop Fox\*

**Ben Morris\***Security Analyst, Bishop Fox\*

At risk of appearing like mad scientists, reveling in our latest unholy creation, we proudly introduce you to DeepHack: the open-source hacking AI. This bot learns how to break into web applications using a neural network, trial-and-error, and a frightening disregard for humankind.

DeepHack can ruin your day without any prior knowledge of apps, databases - or really anything else. Using just one algorithm, it learns how to exploit multiple kinds of vulnerabilities, opening the door for a host of hacking artificial intelligence systems in the future.

This is only the beginning of the end, though. AI-based hacking tools are emerging as a class of technology that pentesters have yet to fully explore. We guarantee that you'll be either writing machine learning hacking tools next year, or desperately attempting to defend against them.

No longer relegated just to the domain of evil geniuses, the inevitable AI dystopia is accessible to you today! So join us and we'll demonstrate how you too can help usher in the destruction of humanity by building weaponized machine learning systems of your own - unless time travelers from the future don't stop us first.

Dan "AltF4" Petro

Dan Petro is a Senior Security Associate at Bishop Fox, a consulting firm providing cybersecurity services to the Fortune 500, global financial institutions, and high-tech startups. In this role, he focuses on application penetration testing and network penetration testing.

Dan likes to hear himself talk, often resulting in conference presentations including several consecutive talks at Black Hat USA and DEF CON in addition to appearances at HOPE, BSides, and ToorCon. He is widely known for the tools he creates: the Rickmote Controller (a Chromecast-hacking device), Untwister (a tool used for breaking pseudorandom number generators) and SmashBot (a merciless Smash Bros noob-pwning machine). He also organizes Root the Box, a capture the flag security competition.



Dan holds has a Master of Science in Computer Science from Arizona State University and still doesn't regret it.

@BishopFox

@2600altf4

Ben Morris

Ben Morris is a Security Analyst at Bishop Fox, a consulting firm providing cybersecurity services to the Fortune 500, global financial institutions, and high-tech startups. In this role, he focuses on application penetration testing, network penetration testing, and red-teaming.

Ben also enjoys performing drive-by pull requests on security tools and bumbling his way into vulnerabilities in widely used PHP and .NET frameworks and plugins. Ben has also contributed to Root the Box, a capture the flag security competition.

[#defcon25/by\\_track/track2/Sunday](#)

[#defcon25/By\\_Day/\\_Sunday](#)

## 1500 - 25 Years of Program Analysis

Sunday at 15:00 in 101 Track

45 minutes | Hacker History, Demo

**Zardus (Yan Shoshitaishvili)\*Assitant Professor, Arizona State University\***

Last year, DARPA hosted the Cyber Grand Challenge, the culmination of humanity's research into autonomous detection, exploitation, and mitigation of software vulnerabilities. Imagine the CGC from the outside: huge racks of servers battling it out on stage, throwing exploit after exploit at each other while humans watch helplessly from the sidelines. But that vantage point misses the program analysis methods used, the subtle trade-offs made, and the actual capabilities of these systems. It also misses why, outside of the controlled CGC environment, most automated techniques don't quite scale to the analysis of real-world software!

This talk will provide a better perspective. On the 25th anniversary of DEFCON, we will go through these last 25 years of program analysis. We'll learn about the different disciplines of program analysis (and learn strange terms such as static, dynamic, symbolic, and abstract), understand the strength and drawbacks of each, and see if, and to what extent, they are used in the course of actual vulnerability analysis.

Did you know that every finalist system in the Cyber Grand Challenge used a combination of

dynamic analysis and symbolic execution to find vulnerabilities, but used static analysis to patch them? Why is that? Did you know that, to make the contest feasible for modern program analysis techniques, the CGC enforced a drastically-simplified OS model? What does this mean for you, if you want to use program analysis while finding vulns and collecting bug bounties? Come to this talk, become an expert, and go on to contribute to the future of program analysis!

Zardus (Yan Shoshitaishvili)

Zardus is one of the hacking aces on Shellphish, the oldest-running CTF team in the world. He's been attending DEFCON since 2001, playing DEFCON CTF since 2009, and talking at DEFCON since 2015. Through this time, he also pursued a PhD in Computer Security, focusing on Program Analysis. The application of cutting-edge academic program analysis techniques to CTF (and, later, to his participation in the DARPA Cyber Grand Challenge, where he led Shellphish to a 3rd-place victory and a big prize payout) gave Zardus a unique understanding of the actual capabilities of the state of the art of program analysis, which in turn drove his research and culminated in the release of the angr binary analysis framework and the Mechanical Phish, one of the world's first autonomous Cyber Reasoning Systems.

[#defcon25/by\\_track/101/Sunday](#)

[#defcon25/By\\_Day/\\_Sunday](#)

## 1500 - DC to DEF CON: Q&A with Congressmen James Langevin and Will Hurd

Sunday at 15:00 in 101 Track

**Representative James Langevin\*(D-RI)\***


**Representative Will Hurd\*(R-TX)\***

**Joshua Corman\*Director of the Cyber Statecraft Initiative at the Atlantic Council's Brent Scowcroft Center\***

The past year has seen major disruptions at the intersection of security and society. "Cybersecurity" has been thrust into the public consciousness frighteningly widely and quickly. Issues of public policy impact our colleagues and our community, beyond the technology layer. Some in the public policy community are actively encouraging our community to engage, recognizing the need for a technically literate voice of reason from the security research community. DEF CON is proud to host two members of Congress, who braved their way from DC to DEF CON as ambassadors from their community to ours.

Joshua Corman will engage Rep. Jim Langevin (D-RI) and Rep. Will Hurd (R-TX), in a candid, on-the-record “fireside chat” style conversation. DEF CON attendees will hear their perspectives on the state of cyber policy and what can be done to improve technical literacy in the dialogs. The members will also reflect on their experience at DEF CON, hanging out with hackers, and how they can make their voice known in the public policy conversation.

Rep. Will Hurd (R-TX)

Rep Hurd was born and raised in  [San Antonio, Texas](#). He attended John Marshall High School and Texas A&M University, where he majored in Computer Science and served as Student Body President.

After college, Will served as an undercover officer in the CIA in the Middle East and South Asia for nearly a decade, collecting intelligence that influenced the National Security agenda. Upon leaving the CIA, he became a Senior Advisor with a cybersecurity firm, covering a wide range of complex challenges faced by manufacturers, financial institutions, retailers, and critical infrastructure owners. He was also a partner with a strategic advisory firm helping businesses expand into international markets.

In 2015, Will was elected to the 114th Congress and currently serves on the Committee of Oversight and Government Reform and chairs the Information Technology Subcommittee. He also sits on the Committee on Homeland Security and is the Vice Chair of the Border and Maritime Security Subcommittee. In 2017, Will was appointed by Speaker Ryan to serve on the House Permanent Select Intelligence Committee, to replace Representative Mike Pompeo upon his confirmation as Director of the CIA.

Rep. James Langevin (D-RI)

Rep. Langevin first ran for office in 1986, when he was elected a Delegate to Rhode Island’s Constitutional Convention and served as its secretary. Two years later, he won election to the Rhode Island House of Representatives.

In 1994, Langevin defeated a Republican incumbent to become the nation’s youngest Secretary of State. He transformed the office into “the people’s partner in government” and took on the challenge of reforming Rhode Island’s outdated election system. Langevin also established the state’s Public Information Center and, with Brown University, published “Access Denied,” which examined the General Assembly’s compliance with the Open Meetings Law and documented routine and widespread violations.

In 1998, Langevin easily won re-election to his second term as Secretary of State, achieving the largest plurality of any general officer in this century, and in 2000, he made a successful run for the U.S. House of Representatives, where he has served the Second Congressional

District ever since.

Langevin graduated from Rhode Island College and earned a Master's Degree in Public Administration from the Kennedy School of Government at Harvard University. He resides in Warwick, Rhode Island

Joshua Corman

Joshua Corman is the director of the Cyber Statecraft Initiative at the Atlantic Council's Brent Scowcroft Center and a founder of I am The Cavalry (dot org). Corman previously served as CTO for Sonatype, director of security intelligence for Akamai, and in senior research and strategy roles for The 451 Group and IBM Internet Security Systems. He co-founded @RuggedSoftware and @IamTheCavalry to encourage new security approaches in response to the world's increasing dependence on digital infrastructure. Josh's unique approach to security in the context of human factors, adversary motivations, and social impact has helped position him as one of the most trusted names in security. He also serving as an adjunct faculty for Carnegie Mellon's Heinz College and on the 2016 HHS Cybersecurity Task Force.

[#defcon25/By\\_Day/\\_Sunday](#)

[#defcon25/by\\_track/101/Sunday](#)

## 1630 - Closing Ceremonies

[#defcon25/by\\_track/track4/sunday](#)

[#defcon25/by\\_track/track3/sunday](#)

[#defcon25/By\\_Day/\\_Sunday](#)