

# 1000 - \$BIGNUM steps forward, \$TRUMPNUM steps back: how can we tell if we're winning?

Saturday at 10:00 in Track 2

45 minutes

**Cory Doctorow**\*[craphound.com](http://craphound.com), science fiction author, activist, journalist and blogger.\*

Is Net Neutrality on the up or down? Is DRM rising or falling? Is crypto being banned, or will it win, and if it does, will its major application be ransomware or revolution? Is the arc of history bending toward justice, or snapping abruptly and plummeting toward barbarism?

It's complicated.

A better world isn't a product, it's a process. The right question isn't, "Does the internet make us better or worse," its: "HOW DO WE MAKE AN INTERNET THAT MAKES THE WORLD BETTER?" We make the world better with code, sure, but also with conversations, with businesses, with lawsuits and with laws.

We don't know how to get to a better world, but we know which direction it's in, and we know how to hill-climb towards it. If we keep heading that way, we'll get *somewhere*. Somewhere good. Somewhere imperfect. Somewhere where improvement is possible.

Cory Doctorow

Cory Doctorow ([craphound.com](http://craphound.com)) is a science fiction author, activist, journalist and blogger - the co-editor of Boing Boing ([boingboing.net](http://boingboing.net)) and the author of WALKAWAY, a novel for adults, a YA graphic novel called IN REAL LIFE, the nonfiction business book INFORMATION DOESN'T WANT TO BE FREE, and young adult novels like HOMELAND, PIRATE CINEMA and LITTLE BROTHER and novels for adults like RAPTURE OF THE NERDS and MAKERS. He works for the Electronic Frontier Foundation, is a MIT Media Lab Research Affiliate, is a Visiting Professor of Computer Science at Open University and co-founded the UK Open Rights Group. Born in Toronto, Canada, he now lives in Los Angeles.

@doctorow

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

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

## 1000 - Get-\$pwnd: Attacking Battle-Hardened Windows

## Server

Saturday at 10:00 in Track 3

20 minutes | Demo, Tool

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

Windows Server has introduced major advances in remote management hardening in recent years through

PowerShell Just Enough Administration ("JEA"). When set up correctly, hardened JEA endpoints can provide

a formidable barrier for attackers: whitelisted commands, with no administrative access to the underlying operating system.

In this presentation, watch as we show how to systematically destroy these hardened endpoints by exploiting insecure coding practices and administrative complexity.

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.

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

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

## 1000 - Persisting with Microsoft Office: Abusing Extensibility Options

Saturday at 10:00 in 101 Track

20 minutes | Demo

**William Knowles\***MWR InfoSecurity\*

One software product that red teamers will almost certainly find on any compromised workstation is Microsoft Office. This talk will discuss the ways that native functionality within Office can be abused to obtain persistence. The following opportunities for Office-based persistence will be discussed:

- (1) WLL and XLL add-ins for Word and Excel - a legacy add-in that allows arbitrary DLL loading.
- (2) VBA add-ins for Excel and PowerPoint - an alternative to backdoored template files, which executes whenever the applications load.
- (3) COM add-ins for all Office products - an older cross-application add-in that leverages COM objects.
- (4) Automation add-ins for Excel - user defined functions that allow command execution through spreadsheet formulae.
- (5) VBA editor (VBE) add-ins for all VBA using Office products - executing commands when someone tries to catch you using VBA to execute commands.
- (6) VSTO add-ins for all Office products - the newer cross-application add-in that leverages a special Visual Studio runtime.

Each persistence mechanism will be discussed in terms of its relative advantages and disadvantages for red teamers. In particular, with regards to their complexity to deploy, privilege requirements, and applicability to Virtual Desktop Infrastructure (VDI) environments which hinder the use of many traditional persistence mechanisms.

The talk isn't all red - there's also some blue to satisfy the threat hunters and incident responders amongst us. The talk will finish with approaches to detection and prevention of these persistence mechanisms.

William Knowles

William Knowles is a Security Consultant at MWR InfoSecurity. He is primarily involved in purple team activities, which involves objective-based testing to simulate real-world threats, and helping organizations to identify effective defenses against them with regards to both prevention and detection. Prior to joining the security industry, he completed a PhD in Computer Science at Lancaster University. His research interests include post-exploitation activities and offensive PowerShell.

@william\_knows

#defcon25/by\_track/101/saturday

#defcon25/By\_Day/\_saturday

## 1000 - The spear to break the security wall of S7CommPlus

Saturday at 10:00 in Track 4

20 minutes | Exploit

Cheng\*ICS Security Researcher, NSFOCUS\*

In the past few years, attacks against industrial control systems (ICS) have increased year over year. Stuxnet in 2010 exploited the insecurity of the S7Comm protocol, the communication protocol used between Siemens Simatic S7 PLCs to cause serious damage in nuclear power facilities. After the exposure of Stuxnet, Siemens has implemented some security reinforcements into the S7Comm protocol. The current S7CommPlus protocol implementing encryption has been used in S7-1200 V4.0 and above, as well as S7-1500, to prevent attackers from controlling and damaging the PLC devices.

Is the current S7CommPlus a real high security protocol? This talk will demonstrate a spear that can break the security wall of the S7CommPlus protocol. First, we use software like Wireshark to analyze the communications between the Siemens TIA Portal and PLC devices. Then, using reverse debugging software like WinDbg and IDA we can break the encryption in the S7CommPlus protocol. Finally, we write a MFC program which can control the start and the stop of the PLC, as well as value changes of PLC's digital and analog inputs & outputs. Based on the research above, we present two security proposals at both code level and protocol level to improve the security of Siemens PLC devices.

Cheng

Cheng Lei is an Industrial Control System Security researcher at NSFOCUS. His interest is mainly about PLC and DCS vulnerability exploitation and security enhancement. Over the years he has released three Siemens CVE vulnerability

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

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

## 1030 - (Un)Fucking Forensics: Active/Passive (i.e. Offensive/Defensive) memory hacking/debugging.

Saturday at 10:20 in Track 4

20 minutes | Hacker History, Art of Defense, Demo, Tool

**K2\*Director, IOACTIVE\***

How to forensic, how to fuck forensics and how to un-fuck cyber forensics.

Defense: WTF is a RoP, why I care and how to detect it statically from memory. Counteract "Gargoyle" attacks.

Defense: For one of DEF CON 24's more popular anti-forensics talks (see int0x80 - Anti

Forensics). In memory (passive debugging) techniques that allows for covert debugging of attackers (active passive means that we will (try hard to) not use events or methods that facilities are detectable by attackers).

Offense: CloudLeech - a cloud twist to Ulf Frisk Direct Memory Attack

K2

K2 (w00w00, ADM, undernet, efnet, The Honeynet Project) is a devil in the details person who does not take themselves too serious and appreciates a good laugh. Earlier DEF CON presentations included polymorphic shellcode in the form of ADMMutate (see ADM Crew), low-level process detection, with page table analysis (Weird-Machine motivated shell code) and using the branch tracing store backdoor trick on Windows to counter Ransom ware, detect RoP (RunTime + HW Assisted) and draw cool graphs – "BlockFighting with a Hooker: BlockfFghter2!". All three of these are open source tools available [github.com/K2](https://github.com/K2) (EhTrace and [inVtero.Net](#) are under active development).

@ktwo\_K2

GitHub: <https://github.com/K2>

#defcon25/by\_track/track4/saturday

#defcon25/By\_Day/\_saturday

## 1030 - Breaking Wind: Adventures in Hacking Wind Farm Control Networks

Saturday at 10:20 in 101 Track

20 minutes

**Jason Staggs\***Security Researcher at the University of Tulsa\*

Wind farms are becoming a leading source for renewable energy. The increased reliance on wind energy makes wind farm control systems attractive targets for attackers. This talk explains how wind farm control networks work and how they can be attacked in order to negatively influence wind farm operations (e.g., wind turbine hijacking). Specifically, implementations of the IEC 61400-25 family of communications protocols are investigated (i.e., OPC XML-DA). This research is based on an empirical study of a variety of U.S. based wind farms conducted over a two year period. We explain how these security assessments reveal that wind farm vendor design and implementation flaws have left wind turbine programmable automation controllers and OPC servers vulnerable to attack. Additionally, proof-of-concept attack tools are developed in order to exploit wind farm control network design and implementation vulnerabilities.

Jason Staggs

Dr. Jason Staggs is an independent information security researcher with strong interests in critical infrastructure protection, telecommunications, penetration testing, network security and digital forensics. Jason has spoken at national and international conferences, authored various peer-reviewed publications and lectured undergraduate and graduate level courses on a variety of cyber security topics. His expertise in digital forensics has enabled him to provide invaluable assistance to law enforcement agencies at the local, state and federal levels in order to solve high-profile cybercrimes. In his spare time, Jason enjoys reverse engineering proprietary network stacks in embedded devices and diving through ancient RFCs to demystify obscure network protocols. Jason attended graduate school at The University of Tulsa where he earned his M.S. and Ph.D. degrees in Computer Science.

#defcon25/by\_track/101/saturday

#defcon25/By\_Day/\_saturday

## 1030 - WSUSpendu: How to hang WSUS clients

Saturday at 10:30 in Track 3

h

20 minutes | Demo, Tool

**Romain Coltel\***Lead product manager at Alsid\*

**Yves Le Provost\***Security auditor at ANSSI\*

You are performing a pentest. You just owned the first domain controller. That was easy. All the computers are belong to you. But unfortunately, you can't reach the final goal. The last target is further in the network, non accessible and heavily filtered. Thankfully, one last hope remains. You realize the target domain pulls its updates from the WSUS server of the compromised domain, the one you fully control. Hope is back... But once again, it fails. The only tools available for controlling the updates are not working: they require a network attack that is prevented by the network architecture and the server configuration. All hope is lost...

We will present you a new approach, allowing you to circumvent these limitations and to exploit this situation in order to deliver updates. Thus, you will be able to control the targeted network from the very WSUS server you own. By extension, this approach may serve as a basis for an air gap attack for disconnected networks.

Our talk will describe vulnerable architectures to this approach and also make some in-context demonstration of the attack with new public tooling. Finally, as nothing is

inescapable, we will also explain how you can protect your update architecture.

Romain Coltel

Romain Coltel is the lead product manager in a french startup, Alsid IT, tackling Active Directory problems down to the core, and he's thus currently doing a lot of research and development on various Active Directory technologies. He's also teaching the well-received SANS SEC660 in France, each time with the author's congratulations at the end of the session.

Before that, he was acquiring his experience in the french National Cybersecurity Agency (ANSSI) as an IT auditor, where he performed penetration testing, various security researches and tools development. As a development example, he's the lead developer of dislocker, a tool to decrypt BitLocker-encrypted partitions on Linux, OSX and FreeBSD. He also implemented the AES-XEX and -XTS modes for the famous mbedTLS library.

Yves Le Provost

Yves Le Provost is a security auditor for more than 10 years. He's working for ANSSI, the french National Cybersecurity Agency since 5 years ago. During these five years defending french administrations, he specialized in database security, OS internals, SCADA architecture and penetration testing.

In parallel, he's teaching french engineering schools about various security topics.

#defcon25/by\_track/track3/saturday

#defcon25/By\_Day/\_saturday

## 1100 - Evading next-gen AV using artificial intelligence

Saturday at 11:00 in Track 4

20 minutes | Demo

**Hyrum Anderson\***Technical Director of Data Science, Endgame\*

Much of next-gen AV relies on machine learning to generalize to never-before-seen malware. Less well appreciated, however, is that machine learning can be susceptible to attack by, ironically, other machine learning models. In this talk, we demonstrate an AI agent trained through reinforcement learning to modify malware to evade machine learning malware detection. Reinforcement learning has produced game-changing AI's that top human level performance in the game of Go and a myriad of hacked retro Atari games (e.g., Pong). In an analogous fashion, we demonstrate an AI agent that has learned through thousands of "games" against a next-gen AV malware detector which sequence of functionality-preserving changes to perform on a Windows PE malware file so that it bypasses the detector. No math

or machine learning background is required; fundamental understanding of malware and Windows PE files is a welcome; and previous experience hacking Atari Pong is a plus.

Hyrum Anderson

Hyrum Anderson is technical director of data scientist at Endgame, where he leads research on detecting adversaries and their tools using machine learning. Prior to joining Endgame he conducted information security and situational awareness research as a researcher at FireEye, Mandiant, Sandia National Laboratories and MIT Lincoln Laboratory. He received his PhD in Electrical Engineering (signal and image processing + machine learning) from the University of Washington and BS/MS degrees from Brigham Young University. Research interests include adversarial machine learning, deep learning, large-scale malware classification, active learning, and early time-series classification.

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

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

## 1100 - If You Give a Mouse a Microchip... It will execute a payload and cheat at your high-stakes video game tournament

Saturday at 11:00 in Track 3

45 minutes | Demo

**skud (Mark Williams)\*Embedded Software Engineer\***

**Sky (Rob Stanley)\*Security Software Engineer, Lead\***

The International, a recent esports tournament, had a 20 million dollar prize pool with over five million people tuned in to the final match. The high stakes environment at tournaments creates an incentive for players to cheat for a competitive advantage. Cheaters are always finding new ways to modify software, from attempting to sneak executables in on flash drives, to using cheats stored in Steam's online workshop which bypasses IP restrictions.

This presentation describes how one can circumvent existing security controls to sneak a payload (game cheat) onto a target computer. Esports tournaments typically allow players to provide their own mouse and keyboard, as these players prefer to use specific devices or may be obligated to use a sponsor branded device. These "simple" USB input devices can still be used to execute complex commands on a computer via the USB Human Interface Device (HID) protocol.

Our attack vector is a mouse with an ARM Cortex M series processor. The microcontroller



stores custom user profiles in flash memory, allowing the mouse to retain user settings between multiple computers. We modify the device's firmware to execute a payload delivery program, stored in free space in flash memory, before returning the mouse to its original functionality. Retaining original functionality allows the mouse to be used discreetly, as it is an "expected" device at these tournaments. This concept applies to any USB device that uses this processor, and does not require obvious physical modifications.

This delivery method has tradeoffs. Our exploit is observable, as windows are created and in focus during payload delivery. The advantage to this approach is that it bypasses other security measures that are commonly in place, such as filtered internet traffic and disabled USB mass storage.

skud (Mark Williams)

Mark Williams is an embedded software engineer with experience in robotics and computer vision. His interest in embedded systems security and research builds off of a love for DIY projects, microcontrollers, and breaking things.

@skudmunky

Sky (Rob Stanley)

Rob Stanley is a lead security software engineer with a background in reverse engineering. He enjoys working with low-level software, taking things apart and putting them back together, and malware analysis. Lately, he has turned his passion towards sharing his knowledge by teaching, and authoring CTF challenge problems.

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

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

## 1100 - Microservices and FaaS for Offensive Security

Saturday at 11:00 in 101 Track

20 minutes | Demo

**Ryan Baxendale**

There are more cloud service providers offering serverless or Function-as-a-service platforms for quickly deploying and scaling applications without the need for dedicated server instances and the overhead of system administration. This technical talk will cover the basic concepts of microservices and FaaS, and how to use them to scale time consuming offensive security testing tasks. Attacks that were previously considered impractical due to time and resource constraints can now be considered feasible with the availability of cloud services and the never-ending free flow of public IP addresses to avoid attribution and blacklists.

Key takeaways include a guide to scaling your tools and a demonstration on the practical benefits of utilising cloud services in performing undetected port scans, opportunistic attacks against short lived network services, brute-force attacks on services and OTP values, and creating your own whois database, shodan/censys, and searching for the elusive internet accessible IPv6 hosts.

Ryan Baxendale

Ryan Baxendale works as a penetration tester in Singapore where he leads a team of professional hackers. While his day is filled mainly with web and mobile penetration tests, he is more interested developing security tools, discovering IPv6 networks, and mining the internet for targeted low hanging fruit. He has previously spoken at XCon in Beijing on automating network pivoting and pillaging with an Armitage script, and has spoken at OWASP chapter and Null Security group meetings. <https://www.linkedin.com/in/ryanbaxendale>

@ryancancomputer

<https://github.com/ryanbaxendale>

#defcon25/by\_track/101/saturday

#defcon25/By\_Day/\_saturday

## 1100 - Secure Tokin' and Doobiekeys: How to roll your own counterfeit hardware security devices

Saturday at 11:00 in Track 2

45 minutes | Demo, Tool

Joe FitzPatrick\*SecuringHardware.com\*

Michael Leibowitz\*Senior Trouble Maker\*

Let's face it, software security is still in pretty bad shape. We could tell ourselves that everything is fine, but in our hearts, we know the world is on fire. Even as hackers, it's incredibly hard to know whether your computer, phone, or secure messaging app is pwned. Of course, there's a Solution(tm) - hardware security devices.

We carry authentication tokens not only to secure our banking and corporate VPN connections, but also to access everything from cloud services to social networking. While we've isolated these 'trusted' hardware components from our potentially pwnd systems so that they might be more reliable, we will present scenarios against two popular hardware

tokens where their trust can be easily undermined. After building our modified and counterfeit devices, we can use them to circumvent intended security assumptions made by their designers and users. In addition to covering technical details about our modifications and counterfeit designs, we'll explore a few attack scenarios for each.

Sharing is Caring, so after showing off a few demonstration, we'll walk you through the process of rolling your own Secure Tokin' and Doobiekey that you can pass around the circle at your next cryptoparty.

Joe FitzPatrick

Joe is an Instructor and Researcher at <https://SecuringHardware.com>. Joe has spent over a decade working on low-level silicon debug, security validation, and penetration testing of CPUS, SOCs, and microcontrollers. He has spent the past 5 years developing and leading hardware security related training, instructing hundreds of security researchers, pen testers, hardware validators worldwide. When not teaching Applied Physical Attacks training, Joe is busy developing new course content or working on contributions to the NSA Playset and other misdirected hardware projects, which he regularly presents at all sorts of fun conferences.

@securelyfitz

Michael Leibowitz

Michael has done hard-time in real-time. An old-school computer engineer by education, he spends his days hacking the mothership for a large semiconductor company. Previously, he developed and tested embedded hardware and software, dicked around with strap-on boot roms, mobile apps, office suites, and written some secure software. On nights and weekends he hacks on electronics, writes DEF CON CFPs, and contributes to the NSA Playset.

@r00tkillah

#defcon25/by\_track/track2/saturday

#defcon25/By\_Day/\_saturday

## 1130 - Abusing Webhooks for Command and Control

Saturday at 11:30 in 101 Track

20 minutes | Demo, Tool

**Dimitry Snezhkov\***Security Consultant, X-Force Red, IBM\*

You are on the inside of the perimeter. And maybe you want to exfiltrate data, download a tool, or execute commands on your command and control server (C2). Problem is - the first

leg of connectivity to your C2 is denied. Your DNS and ICMP traffic is being monitored. Access to your cloud drives is restricted. You've implemented domain fronting for your C2 only to discover it is ranked low by the content proxy, which is only allowing access to a handful of business related websites on the outside.

We have all been there, seeing frustrating proxy denies or triggering security alarms making our presence known.

Having more choices when it comes to outbound network connectivity helps. In this talk we'll present a technique to establish such connectivity with the help of HTTP callbacks (webhooks). We will walk you through what webhooks are, how they are used by organizations. We will then discuss how you can use approved sites as brokers of your communication, perform data transfers, establish almost realtime asynchronous command execution, and even create a command-and-control communication over them, bypassing strict defensive proxies, and even avoiding attribution.

Finally, we'll release the tool that will use the concept of a broker website to work with the external C2 using webhooks.

Dimitry Snezhkov

Dimitry Snezhkov does not like to refer to himself in the third person ;) but when he does he is a Sr. Security Consultant for X-Force Red at IBM, currently focusing on offensive security testing, code hacking and tool building.

@Op\_Nomad

#defcon25/by\_track/101/saturday

#defcon25/By\_Day/\_saturday

## 1130 - All Your Things Are Belong To Us

Saturday at 11:30 in Track 4

75 minutes | Demo, Exploit

**Zenofex\*Hacker\***

**0x00string\*Hacker\***

**CJ\_000\*Hacker\***

**Maximus64\*Hacker\***

Get out your rollerblades, plug in your camo keyboard, and fire up your BLT drive. It's 25 years later and we're still hacking the planet. The [Exploitee.rs](#) are back with new 0day, new exploits and more fun. Celebrating a quarter century of DEF CON the best way we know how: hacking everything!

Our presentation will showcase vulnerabilities discovered during our research into thousands of dollars of IoT gear performed exclusively for DEF CON. We will be releasing all the vulnerabilities during the presentation as 0days to give attendees the ability to go home and unlock their hardware prior to patches being released. As always, to give back to the community that has given us so much, we will be handing out free hardware during the presentation so you can hack all the things too! Come party with us while we make "All Your Things Are Belong To Us."

Zenofex

Zenofex (@zenofex) is a researcher with [Exploitee.rs](#). Amir founded "[Exploitee.rs](#)" which is a public research group and has released exploits for over 45 devices including the Amazon FireTV, Roku Media Player and the Google Chromecast. Amir is also a member of Austin Hackers and has spoken at a number of security conferences including DEF CON, B-Sides Austin, and InfoSec Southwest.

@exploiteers

@zenofex

0x00string

0x00string (@0x00string) is hacker and security researcher, a recent addition to [Exploitee.rs](#) who has presented at BSidesSATX and ISSW. His previous published work includes Reverse Engineering The Kankun Smart Plug, and Hacking The Samsung Allshare Cast Hub. His hobbies include bug collecting and hacking all the things.

@0x00string

CJ\_000

Cj\_000 (@cj\_000) is a researcher in the Cyber and Information Security directorate at *redacted* and also a member of [Exploitee.rs](#). CJ has been involved in the release and responsible disclosure of vulnerabilities in a number of devices including TV's, media players, and refrigerators. CJ has presented at multiple DEF CON's and believes that a simple approach is often the most elegant solution.

@cj\_000

Maximus64

Maximus64 (@maximus64\_) is an undergraduate student at the University of Central Florida. Khoa enjoys a hardware based approach in researching embedded devices and is a master

of the soldering iron. Khoa has disclosed numerous vulnerabilities in various set-top boxes and other "smart" devices to multiple vendors. He is currently listed on various "Security Hall of Fame" pages for successful bug bounty submissions including AT&T, Samsung and Roku.

@maximus64\_

#defcon25/by\_track/track4/saturday

#defcon25/By\_Day/\_saturday

## 1200 - DNS - Devious Name Services - Destroying Privacy & Anonymity Without Your Consent

Saturday at 12:00 in Track 3

45 minutes | Art of Defense

**Jim Nitterauer\*Senior Security Specialist, AppRiver, LLC\***

You've planned this engagement for weeks. Everything's mapped out. You have tested all your proxy and VPN connections. You are confident your anonymity will be protected. You fire off the first round and begin attacking your target. Suddenly something goes south. Your access to the target site is completely blocked no matter what proxy or VPN you use. Soon, your ISP contacts you reminding you of their TOS while referencing complaints from the target of your engagement. You quickly switch MAC addresses and retry only to find that you are quickly blocked again!

What happened? How were you betrayed? The culprit? Your dastardly DNS resolvers and more specifically, the use of certain EDNS0 options by those resolvers.

This presentation will cover the ways in which EDNS OPT code data can divulge details about your online activity, look at methods for discovering implementation by upstream DNS providers and discuss ways in which malicious actors can abuse these features. We will also examine steps you can take to protect yourself from these invasive disclosures.

The details covered will be only moderately technical. Having a basic understanding of RFC 6891 and general DNS processes will help in understanding. We will discuss the use of basic tools including Wireshark, Packetbeat, Graylog and Dig.

Jim Nitterauer

Currently a Senior Security Specialist at AppRiver, LLC., his team is responsible for global network deployments and manages the SecureSurf global DNS infrastructure and SecureTide global spam & virus filtering infrastructure as well as all internal applications. They

also manage security operations for the entire company. He holds a CISSP certification. He is also well-versed in ethical hacking and penetration testing techniques and has been involved in technology since the late 1980s when punch cards were still a thing.

Jim has presented at NolaCon, ITEN WIRED, BSides Las Vegas, BSides Atlanta, CircleCityCon and several smaller conferences. He regularly attends national security conferences and is passionate about conveying the importance of developing, implementing and maintaining security policies for organizations. His talks convey unique and practical techniques that help attendees harden their security in practical and easy-to-deploy ways.

Jim is a senior staff member with BSides Las Vegas, a member of the ITEN WIRED Planning Committee and the president of the Florida Panhandle (ISC)2 Chapter. When not at the computer, Jim can be found working out, playing guitar, traveling or just relaxing with an adult beverage.

Twitter: @jnitterauer

LinkedIn: <https://www.linkedin.com/in/jnitterauer/>

#defcon25/by\_track/track3/saturday

#defcon25/By\_Day/\_saturday

## 1200 - Driving down the rabbit hole

Saturday at 12:00 in 101 Track

45 minutes | Demo

**Mickey Shkatov**\*Security Researcher, McAfee.\*

**Jesse Michael**\*Security Researcher, McAfee.\*

**Oleksandr Bazhaniuk**\*Security Researcher\*

Over the past few years, cars and automotive systems have gained increasing attention as cyber-attack targets. \_ Cars are expensive. \_ Breaking cars can cost a lot. \_ So how can we find vulnerabilities in a car with no budget? \_ We'll take you with us on a journey from zero car security validation experience through the discovery and disclosure of \_ multiple remotely-exploitable automotive vulnerabilities. \_ Along the way, we'll visit a wrecking yard, \_ reassemble (most) of a 2015 Nissan Leaf in our lab, discuss how we picked our battles, fought them, and won. \_ During our talk, we'll examine the details of three different classes of vulnerabilities we found in this vehicle, \_ how they can be exploited, and the potential

ramifications to the owner of their real-world exploitation. We'll also discuss the broader scope of the vulnerabilities discovered, how they extend beyond just this specific vehicle, and what the industry can do better to prevent these types of problems in the future.

Mickey Shkatov

Mickey Shkatov is a security researcher and a member of the McAfee Advanced Threat Research team. His areas of expertise include vulnerability research, hardware and firmware security, and embedded device security

@HackingThings

Jesse Michael

Jesse Michael has been working in security for over a decade and is currently a member of the McAfee Advanced Threat Research team who spends his time causing trouble and finding low-level hardware security vulnerabilities in modern computing platforms

@jessemichael

Oleksandr Bazhaniuk

Oleksandr Bazhaniuk is a security researcher and reverse engineer with background in automation of binary vulnerability analysis. He is also a co-founder of DCUA, the first DEF CON group in Ukraine.

@ABazhaniuk

#defcon25/by\_track/101/saturday

#defcon25/By\_Day/\_saturday

## 1200 - When Privacy Goes Poof! Why It's Gone and Never Coming Back

Saturday at 12:00 in Track 2

45 minutes | 0025

**Richard Thieme a.k.a. neuralcowboy**

"Get over it!" as Scott McNealey said - unhelpfully. Only if we understand why it is gone and not coming back do we have a shot at rethinking what privacy means in a new context.

Thieme goes deep and wide as he rethinks the place of privacy in the new social/cultural context and challenges contemporary discussions to stop using 20th century frames. Pictures don't fit those frames, including pictures of "ourselves."

We have always known we were cells in a body, but we emphasized "cell-ness". Now we have to emphasize "body-ness" and see ourselves differently. What we see depends on the level of



abstraction at which we look. The boundaries we imagine around identities, psyches, private internal spaces," are violated in both directions, going in and going out, by data that, when aggregated, constitutes "us". We are known by others more deeply in recombination from metadata than we know ourselves. We are not who we think we are.

To understand privacy - even what we mean by "individuals" who want it - requires a contrary opinion. Privacy is honored in lip service, but not in the marketplace, where it is violated every day. To confront the challenges of technological change, we have to know what is happening to "us" so we can re-imagine what we mean by privacy, security, and identity. We can't say what we can't think. We need new language to grasp our own new "human nature" that has been reconstituted from elements like orange juice.

The weakest link in discussions of privacy is the definition of privacy, and the definition of privacy is not what we think. Buddhists call enlightenment a "nightmare in daylight", yet it is enlightenment still, and that kind of clarity is the goal of this presentation.

Richard Thieme a.k.a. neuralcowboy

Richard Thieme is an author and professional speaker focused on the challenges posed by new technologies and the future, how to redesign ourselves to meet these challenges, and creativity in response to radical change. His column, "Islands in the Clickstream," was distributed to subscribers in sixty countries before collection as a book in 2004. When a friend at the National Security Agency said after they worked together on ethics and intelligence issues, "The only way you can tell the truth is through fiction," he returned to writing short stories, 19 of which are collected in "Mind Games". His latest work is the stunning novel "FOAM", published by Exurban Press September 2015. He is also co-author of the critically extolled "UFOs and Government: A Historical Inquiry", a 5-year research project using material exclusively from government documents and other primary sources, now in 65 university libraries

His work has been taught at universities in Europe, Australia, Canada, and the United States, and he has guest lectured at numerous universities, including Purdue University (CERIAS), the Technology, Literacy and Culture Distinguished Speakers Series of the University of Texas, the "Design Matters" lecture series at the University of Calgary, and as a Distinguished Lecturer in Telecommunications Systems at Murray State University. He addressed the reinvention of "Europe" as a "cognitive artifact" for curators and artists at Museum Sztuki in Lodz, Poland, keynoted CONFidence in Krakow 2015, and keynoted "The Real Truth: A World's Fair" at Raven Row Gallery, London. He recently keynoted Code Blue in Tokyo. He loved Tokyo. He has spoken for the National Security Agency, the FBI, the Secret Service, the US Department of the Treasury, and Los Alamos National Labs and has keynoted "hacker", security, and technology conferences around the world. He spoke at DC 24 in 2016 for the 21st year.

Twitter and skype: neuralcowboy

Linked In and FB: Richard Thieme

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

#defcon25/by\_track/track2/saturday

#defcon25/By\_Day/\_saturday

## 1300 - A Picture is Worth a Thousand Words, Literally: Deep Neural Networks for Social Stego

Saturday at 13:00 in Track 4

45 minutes | Tool

**Philip Tully\***Principal Data Scientist, ZeroFOX\*

**Michael T. Raggo\***Chief Security Officer, 802 Secure\*

Images, videos and other digital media provide a convenient and expressive way to communicate through social networks. But such broadcastable and information-rich content provides ample illicit opportunity as well. Web-prevalent image files like JPEGs can be disguised with foreign data since they're perceivably robust to minor pixel and metadata alterations. Slipping a covert message into one of the billions of daily posted images may be possible, but to what extent can steganography be systematically automated and scaled?

To explore this, we first report the distorting side effects rendered upon images uploaded to popular social network servers, e.g. compression, resizing, format conversion, and metadata stripping. Then, we build a convolutional neural network that learns to reverse engineer these transformations by optimizing hidden data throughput capacity. From pre-uploaded and downloaded image files, the network learns to locate candidate metadata and pixels that are least modifiable during transit, allowing stored hidden payloads to be reliably recalled from newly presented images. Deep learning typically requires tons of training data to avoid over fitting. But data acquisition is trivial using social networks' free image hosting services, which feature bulk uploads and downloads of thousands of images at a time per album.

We show that hidden data can be predictably transmitted through social network images with high fidelity. Our results demonstrate that AI can hide data in plain sight, at large-scale, beyond human visual discernment, and despite third-party manipulation. Steganalysis and other defensive forensic countermeasures are notoriously difficult, and our exfiltration

techniques highlight the growing threat posed by automated, AI-powered red teaming.

Philip Tully

Philip Tully is a Principal Data Scientist at ZeroFOX. He employs natural language processing and computer vision techniques in order to develop predictive models for combating security threats emanating from social networks. He earned his joint doctorate degree in computer science from the Royal Institute of Technology (KTH) and the University of Edinburgh, and has spoken at Black Hat, DEF CON , ShowMeCon and across the neuroscience conference circuit. He's a hackademic that's interested in applying brain-inspired algorithms to both blue and red team operations.

@phtully

Michael T. Raggo

Michael T. Raggo, Chief Security Officer, 802 Secure (CISSP, NSA-IAM, CSI) has over 20 years of security research experience. His current focus is wireless IoT threats impacting the enterprise. Michael is the author of "Mobile Data Loss: Threats & Countermeasures" and "data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols" for Syngress Books, and contributing author for "Information Security the Complete Reference 2nd Edition". A former security trainer, Michael has briefed international defense agencies including the FBI and Pentagon, is a participating member of FSISAC/BITS and PCI, and is a frequent presenter at security conferences, including Black Hat, DEF CON , Gartner, RSA, DoD Cyber Crime, OWASP, HackCon, and SANS.

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

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

## 1300 - Demystifying Windows Kernel Exploitation by Abusing GDI Objects.

Saturday at 13:00 in 101 Track

45 minutes | Demo, Exploit

**5A1F (Saif El-Sherei)\*Security Analyst, SensePost\***

Windows kernel exploitation is a difficult field to get into. Learning the field well enough to write your own exploits require full walkthroughs and few of those exist. This talk will do that, release two exploits and a new GDI object abuse technique.

We will provide all the detailed steps taken to develop a full privilege escalation exploit. The process includes reversing a Microsoft's patch, identifying and analyzing two bugs, developing PoCs to trigger them, turning them into code execution and then putting it all

together. The result is an exploit for Windows 8.1 x64 using GDI bitmap objects and a new, previously unreleased Windows 7 SP1 x86 exploit involving the abuse of a newly discovered GDI object abuse technique.

5A1F (Saif El-Sherei)

Saif is a senior analyst with SensePost. He has a keen interest in exploit development and sharing everything he learns. Over the years he has released several exploitation tutorials, examples and a grammar-based browser fuzzer, wadi (DEF CON 23).

@saif\_sherei

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

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

## 1300 - Koadic C3 - Windows COM Command & Control Framework

Saturday at 13:00 in Track 2

45 minutes | Demo, Tool

**Sean Dillon (zerosum0x0)\*Senior Security Analyst, RiskSense, Inc.\***

**Zach Harding (Aleph-Naught-)\*Senior Security Analyst, RiskSense, Inc.\***

Koadic C3, or COM Command & Control, is a Windows post-exploitation tool similar to other penetration testing rootkits such as Meterpreter and Powershell Empire. The major difference is that Koadic does most of its operations using the Windows Script Host (a.k.a. JScript/VBScript), with compatibility in the core to support a default installation of Windows 2000 with no service packs (and potentially even versions of NT4) all the way through Windows 10.

An in-depth view of default COM objects will be provided. COM is a fairly underexplored, large attack surface in Windows. We will share lots of weird Windows scripting quirks with interesting workarounds we discovered during the course of development. Post exploitation with PowerShell has grown in popularity in recent years, and seeing what can be done with just the basic Windows Script Host is an interesting exploration. In addition, defenses against this type of tool will be discussed, as the Windows Script Host is more tightly coupled to the core of Windows than PowerShell is.

It is possible to serve payloads completely in memory from stage 0 to beyond, as well as use cryptographically secure communications over SSL and TLS (depending on what the victim OS has available). We also found numerous ways to "fork to shellcode" in an environment

which traditionally does not provide such capabilities. This talk is based on original research by ourselves, as well as the previous amazing work of engima0x3, subTee, tiraniddo, and others.

Sean Dillon (zerosum0x0)

Sean Dillon is a senior security analyst at RiskSense, Inc. He has an established research focus on attacking the Windows kernel, and was the first to reverse engineer the DOUBLEPULSAR SMB backdoor. He is a co-author of the ETERNALBLUE Metasploit module and contributions to the project. He has previously been a software engineer in the avionics and insurance industries, and his favorite IDE is still GW-Basic on DOS.

<https://twitter.com/zerosum0x0>

<https://zerosum0x0.blogspot.com>

<https://github.com/zerosum0x0>

Zach Harding (Aleph-Naught-)

Zach Harding is a senior security analyst at RiskSense, Inc. Zach formerly served in the US Army as a combat medic. He, along with Sean Dillon and others, improved leaked NSA code to release the "ExtraBacon 2.0" Cisco ASA exploit package. He is an avid tester of every penetration tool he can get a hold of. You know the guy who's always looking for available public WiFi, or fiddling with a kiosk machine? That's Zach.

<https://github.com/Aleph-Naught->

#defcon25/by\_track/track2/saturday

#defcon25/By\_Day/\_saturday

## 1300 - Twenty Years of MMORPG Hacking: Better Graphics, Same Exploits

Saturday at 13:00 in Track 3

45 minutes | Demo, Exploit

**Manfred (@\_EBFE)\*Security Analyst at Independent Security Evaluators\***

In theme with this year's DEF CON this presentation goes through a 20 year history of exploiting massively multiplayer online role-playing games (MMORPGs). The presentation technically analyzes some of the virtual economy-devastating, low-hanging-fruit exploits that are common in nearly every MMORPG released to date. The presenter, Manfred (@\_EBFE), goes over his adventures in hacking online games starting with 1997's Ultima Online and subsequent games such as Dark Age of Camelot, Anarchy Online, Asherons Call 2, ShadowBane, Lineage II, Final Fantasy XI/XIV, World of Warcraft, plus some more recent titles

such as Guild Wars 2 and Elder Scrolls Online and many more!

The presentation briefly covers the exploit development versus exploit detection/prevention arms race and its current state. Detailed packet analysis and inference on what the code looks like server side in order for some of the exploits to be possible is presented.

This presentation includes a live demonstration of at least one unreleased exploit to create mass amounts of virtual currency in a recent and popular MMORPG.

Manfred (@\_EBFE)

Manfred (@\_EBFE) has been reverse engineering and exploiting MMORPGs for 20 years.

During that time, he ran a successful business based solely on exploiting online games in order to supply virtual goods to retailers. He has reverse engineered communication

protocols for over 22 well known and popular MMORPGs and in certain cases circumvented anti tampering and software/hardware fingerprinting countermeasures. Manfred is currently a security researcher and analyst at Independent Security Evaluators (@ISEsecurity).

@\_EBFE

#defcon25/by\_track/track3/saturday

#defcon25/By\_Day/\_saturday

## 1400 - Attacking Autonomic Networks

Saturday at 14:00 in 101 Track

45 minutes | Demo, Exploit

**Omar Eissa\***Security Analyst, ERNW GmbH\*

Autonomic systems are smart systems which do not need any human management or intervention. Cisco is one of the first companies to deploy the technology in which the routers are just "Plug and Play" with no need for configuration. All that is needed is 5 commands to build fully automated network. It is already supported in pretty much all of the recent software images for enterprise level and carrier grade routers/switches.

This is the bright side of the technology. On the other hand, the configuration is hidden and the interfaces are inaccessible. The protocol is proprietary and there is no mechanism to know what is running within your network.

In this talk, we will have a quick overview on Cisco's Autonomic Network Architecture, then I will reverse-engineer the proprietary protocol through its multiple phases. Finally, multiple

vulnerabilities (overall 5) will be presented, one of which allows to crash systems remotely by knowing their IPv6 address.

Omar Eissa

Omar Eissa is a security Analyst working for ERNW. His interests are network security and reverse-engineering. He is a professional Cisco engineer with various years of experience in enterprise and ISPs networks. He has given talks and workshops at various telco events and conferences like Troopers17 and Black Hat USA 2017.

#defcon25/by\_track/101/saturday

#defcon25/By\_Day/\_saturday

## 1400 - Linux-Stack Based V2X Framework: All You Need to Hack Connected Vehicles

Saturday at 14:00 in Track 3

45 minutes | Demo, Tool

**p3n3troot0r (Duncan Woodbury)\*Hacker\***

**ginsback (Nicholas Haltmeyer)\*Hacker\***

Vehicle-to-vehicle (V2V) and, more generally, vehicle-to-everything (V2X) wireless communications enable semi-autonomous driving via the exchange of state information between a network of connected vehicles and infrastructure units. Following 10+ years of standards development, particularly of IEEE 802.11p and the IEEE 1609 family, a lack of available implementations has prevented the involvement of the security community in development and testing of these standards. Analysis of the WAVE/DSRC protocols in their existing form reveals the presence of vulnerabilities which have the potential to render the protocol unfit for use in safety-critical systems. We present a complete Linux-stack based implementation of IEEE 802.11p and IEEE 1609.3/4 which provide a means for hackers and academics to participate in the engineering of secure standards for intelligent transportation systems.

p3n3troot0r (Duncan Woodbury)

Car hacker by trade, embedded systems security engineer by day. Entered the field of cyberauto security in 2012 through the Battelle CAVE red team and had the opportunity to improve the world by hacking transportation systems. Co-founded multiple security companies focused on building tools for automated exploitation of automotive systems (<http://www.silent-cyber.com/>), open-source frameworks for V2X, secure digital asset management, and 3D printing electric cars (<https://hackaday.com/tag/lost-pla/>) out of your garage (<http://foss-car.faikvm.com/trac/>). DEF CON lurker since the age of 17, recently having

joined forces with friends and mentors to organize and host the DEF CON Car Hacking Village.

p3n3troot0r began working V2X with ginsback two years ago and realized the opportunity, in lieu of any open-source or full-stack V2X implementation, to bring the security community in to the driver's seat in the development of next-gen cyberauto standards. Together they have engaged the thought leaders in this space, and via the long-awaited integration of this stack into the mainline Linux kernel, the global development community is given the opportunity to participate in the development of automated and connected transportation systems.

ginsback (Nicholas Haltmeyer)

AI researcher and security professional. Began work in automotive security through the DEF CON Car Hacking Village and have since developed V2X software and routing schemes. Extensive experience in signal processing and RF hacking, including vital sign monitoring, activity recognition, and biometric identification through RF.

Given the (abyssal) state of automotive cybersecurity, ginsback aims to develop and field tools for V2X that open collaboration with the hacker community. As intelligent transit reaches critical mass, attacks on V2X infrastructure have the potential to cause incredible damage. ginsback partnered with p3n3troot0r to develop a free as in freedom V2X interface and extend an invitation for the community to discover and fix flaws in the design of what will soon be a massive network of connected vehicles.

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

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

## 1400 - Trojan-tolerant Hardware & Supply Chain Security in Practice

Saturday at 14:00 in Track 2

45 minutes | Art of Defense, Demo, Tool

**Vasilios Mavroudis\*** Doctoral Researcher, University College London\*

**Dan Cvrcek\*** Co-founder, Enigma Bridge Ltd\*

The current consensus within the security industry is that high-assurance systems cannot tolerate the presence of compromised hardware components. In this talk, we challenge this perception and demonstrate how trusted, high-assurance hardware can be built from untrusted and potentially malicious components.



The majority of IC vendors outsource the fabrication of their designs to facilities overseas, and rely on post-fabrication tests to weed out deficient chips. However, such tests are not effective against: 1) subtle unintentional errors (e.g., malfunctioning RNGs) and 2) malicious circuitry (e.g., stealthy Hardware Trojans). Such errors are very hard to detect and require constant upgrades of expensive forensics equipment, which contradicts the motives of fabrication outsourcing.

In this session, we introduce a high-level architecture that can tolerate multiple, malicious hardware components, and outline a new approach in hardware compromises risk management. We first demo our backdoor-tolerant Hardware Security Module built from low-cost commercial off-the-shelf components, benchmark its performance, and delve into its internals. We then explain the importance of "component diversification" and "non-overlapping supply chains", and finally discuss how "mutual distrust" can be exploited to further reduce the capabilities of the adversaries.

Vasilios Mavroudis

Vasilios Mavroudis is a doctoral researcher in the Information Security Group at University College London. He studies security and privacy aspects of digital ecosystems, with a focus on emerging technologies and previously unknown attack vectors.

He is currently working on a high-assurance cryptographic hardware. In cooperation with industrial partners, he has recently prototyped a high-assurance hardware architecture, that maintains its security properties even in the presence of malicious hardware components.

Past works include his recent publication on the ultrasound tracking ecosystem which received wide-spread attention and is considered the seminal work on that ecosystem, and auditing tools for the Public Key Infrastructure of Deutsche Bank. Moreover, he has participated in an international consortium studying large-scale security threats in telecommunication networks, and cooperated with UC Santa Barbara in several projects, including a detection system for evasive web-malware.

Vasilios holds an Information Security MSc from UCL, and a BSc on Computer Science from University of Macedonia, Greece.

Dan Cvrcek

Dan Cvrcek is a security architect and engineer learning how to run his start-up Enigma Bridge. He has extensive experience with large banking systems from operational procedures to system architectures: Swift, card payment processing, UK Faster Payments, large key management systems. His hardware encounters include smart cards, custom and embedded systems, and hardware security modules, from design, testing, defences to attacks. He reverse-engineered a hidden API of Chrysalis-ITS crypto modules (now SafeNet) with Mike

Bond, Steven Murdoch and others. Dan got his uni degrees (PhD and Associate Prof.) from Brno University of Technology, and had fun as a post-doc at the University of Cambridge (2003-2004, 2007-2008), Deloitte London (2008-2009), start-ups, freelance security consultant (2010-2016) - clients include Barclays and Deutsche Bank, co-founded Enigma Bridge in 2015.

@dancvrcek

Contributor Acknowledgement:

The Speakers would like to acknowledge the following for their contribution to the presentation.

George Danezis, Professor (University College London)

Petr Svenda, Security Researcher (Masaryk University)

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

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

## 1400 - XenoScan: Scanning Memory Like a Boss

Saturday at 14:00 in Track 4

45 minutes | Demo, Tool

**Nick Cano\*Hacker\***

XenoScan is the next generation in tooling for hardcore game hackers. Building on the solid foundation from older tools like Cheat Engine and Tsearch, XenoScan makes many innovations which take memory scanning to a whole new level.

This demo-heavy talk will skip the fluff and show the power of the tool in real-time. The talk will demonstrate how the tool can scan for partial structures, detect complex data structures such as binary trees or linked lists, detect class-instances living on the heap, and even group detected class instances by their types. Additional, these demos will take a look at the tool's extensibility by working not only on native processes, but also on Nintendo games running in emulators. You're not all game hackers, so the talk will also show how XenoScan can be useful in the day-to-day workflow of reverse engineers and hackers.

When I'm not doing demos, I'll be drilling down to the low-level to talk about the nitty gritty details of what's happening, how it works, and why it works.

By the end of the talk, you'll see the true power of a well-made, smart memory scanner. You'll be empowered to use it in your day to day hacking, whether that is on games, malware, or otherwise. For those of you that are really interested in the tool, it is completely open-source and all development is done on an interactive livestream, meaning you can participate in and learn from future development.

Nick Cano

Nick Cano is the author of "Game Hacking: Developing Autonomous Bots for Online Games" (No Starch Press), a Senior Security Architect at Cylance, and a life-long programmer and hacker. Programming since the age of 12 and hacking games since the age of 15, Nick has a strong background with both software development and Reverse Engineering. Nick has a history developing and selling bots for MMORPGs, advising game developers on hardening their games against bots, and making innovations in the EDR space for next-gen AV companies.

@nickcano93

<https://github.com/nickcano><http://www.nostarch.com/gamehacking>

[https://www.livecoding.tv/darkstar\\_xeno](https://www.livecoding.tv/darkstar_xeno)

#defcon25/by\_track/track4/saturday

#defcon25/By\_Day/\_saturday

## 1500 - Digital Vengeance: Exploiting the Most Notorious C&C Toolkits

Saturday at 15:00 in Track 4

45 minutes | Demo, Tool, Exploit

**Professor Plum\*Hacker\***

Every year thousands of organizations are compromised by targeted attacks. In many cases the attacks are labeled as advanced and persistent which suggests a high level of sophistication in the attack and tools used. Many times, this title is leveraged as an excuse that the events were inevitable or irresistible, as if the assailants' skill set is well beyond what defenders are capable of. To the contrary, often these assailants are not as untouchable as many would believe.

If one looks at the many APT reports that have been released over the years some clear patterns start to emerge. A small number of Remote Administration Tools are preferred by actors and reused across multiple campaigns. Frequently sited tools include Gh0st RAT, Plug-

X, and XtremeRAT among others. Upon examination, the command and control components of these notorious RATs are riddled with vulnerabilities. Vulnerabilities that can be exploited to turn the tables from hunter to hunted.

The presentation will disclose several exploits that could allow remote execution or remote information disclosure on computers running these well-known C&C components. It should serve as a warning to those actors who utilize such toolsets. That is to say, such actors live in glass houses and should stop throwing stones.

Professor Plum

Professor Plum is an experienced reverse engineer, developer, and digital forensics examiner. He holds a graduate degree in Information Security from Johns Hopkins University, and has worked numerous computer incident investigations spanning the globe. He currently works as a Senior Threat Researcher for a Fortune 500 cybersecurity company and previously worked for the Department of Defense performing vulnerability research, software development, and Computer Network Operations.

@professorplum

#defcon25/by\_track/track4/saturday

#defcon25/By\_Day/\_saturday

## 1500 - DOOMed Point of Sale Systems

Saturday at 15:00 in Track 3

45 minutes | Demo, Exploit

**trixr4skids\*Security Engineer\***

In response to public security breaches many retailers have begun efforts to minimize or completely prevent the transmission of unencrypted credit card data through their store networks and point of sale systems. While this is definitely a great improvement over the previous state of affairs; it places the security of transactions squarely in the hands of credit card terminals purchased from third party vendors. These terminals have a security posture that is often not well understood by the retail chains purchasing them. To better understand if the trust placed in these devices is warranted, the attack surface and hardening of a commonly deployed credit card terminal series is reviewed and a discussion of reverse engineered security APIs is presented. Despite the reduced attack surface of the terminals and hardened configuration, attacks that allow recovery of magstripe track data and PIN codes are demonstrated to be possible.

trixr4skids

trixr4skids is a security engineer and a recovering consultant. He enjoys hardware hacking, reverse engineering, the occasional webapp RCE, robots, beer, and of course robots that bring him beer. As a child he enjoyed taking apart everything he could get his hands on in a quest to figure out how it worked (his parents did not always appreciate this). He could never figure out what the green rectangles with the black rectangles on them did and often resorted to smashing them with a hammer to see what was inside. Since then he has learned more effective ways to go about discovering the secrets those black things are hiding and even how to make them do different things than intended. His current research projects include attacking embedded devices based on the rabbit 2000/3000 CPUs, studying the security of payment card systems, and hacking anything interesting that he can buy off eBay.

@trixr4skids

#defcon25/by\_track/track3/saturday

#defcon25/By\_Day/\_saturday

## 1500 - MS Just Gave the Blue Team Tactical Nukes (And How Red Teams Need To Adapt)

Saturday at 15:00 in 101 Track

45 minutes | Demo, Tool

**Chris Thompson\***Red Team Ops Lead, IBM X-Force Red\*

Windows Defender Advanced Threat Protection will soon be available for all Blue Teams to utilize within Windows 10 Enterprise, which includes detection of post breach tools, tactics and techniques commonly used by Red Teams, as well as behavior analytics. Combined with Microsoft Advanced Threat Analytics for user behavior analytics across the Domain, Red Teamers will soon face a significantly more challenging time maintaining stealth while performing internal recon, lateral movement, and privilege escalation in Windows 10/Active Directory environments.

This talk highlights challenges to red teams posed by Microsoft's new tools based on common hacking tools/techniques, and covers techniques which can be used to bypass, disable, or avoid high severity alerts within Windows Defender ATP and Microsoft ATA, as well as TTP used against mature organizations that may have additional controls in place such as Event Log Forwarding and Sysmon

Chris Thompson

Chris is Red Team Operations Lead at IBM X-Force Red. He has extensive experience

performing penetration testing and red teaming for clients in a wide variety of industries. He's led red teaming operations against defense contractors and some of North America's largest banks.

He's on the board for CREST USA ([crest-approved.org](http://crest-approved.org)), working to help mature the pentesting industry. Chris also teaches Network & Mobile Pentesting at one of Canada's largest technical schools.

Hacking his way through life, Chris likes to pretend he's a good drone pilot, lock picker, and mountain biker.

Twitter: @retBandit

#defcon25/by\_track/101/saturday

#defcon25/By\_Day/\_saturday

## 1500 - Tracking Spies in the Skies

Saturday at 15:00 in Track 2

45 minutes | Art of Defense, 0025, Tool

**Jason Hernandez\***Hacker / Technical Editor, North Star Post\*

**Sam Richards\***Editor and Journalist, North Star Post\*

**Jerod MacDonald-Evoy\***Journalist, North Star Post\*

Law enforcement agencies have used aircraft for decades to conduct surveillance, but modern radio, camera, and electronics technology has dramatically expanded the power and scope of police surveillance capabilities. The Iraq War and other conflicts have spurred the development of mass surveillance technologies and techniques that are now widely available to domestic police. The FBI, DEA, and other agencies flew powerful surveillance aircraft over cities for years in relative secrecy before breaking in to public attention in 2015. This presentation will discuss the capabilities of these aircraft, the discovery of the FBI and others' surveillance fleets, and continued efforts to shed light on aerial surveillance. We will discuss a method for detecting surveillance indicators in real time based on mutilation of aggregated ADS-B data, and introduce code for detecting surveillance indicators from flight behavior.

Jason Hernandez

Jason Hernandez researches surveillance technology and reports on it for the North Star Post. Jason has a BS in economics, and has worked in the mining and technology industries. Jason has worked on algorithms to detect surveillance aircraft from ADS-B flight data.

@jason\_nstar

Sam Richards

Sam Richards is an independent journalist, and founder of the North Star Post. Sam pieced together hundreds of FAA and corporate records to uncover the FBI's secret fleet of surveillance aircraft.

@minneapolisam

Jerod MacDonald-Evoy

Jerod MacDonald-Evoy is a journalist with the North Star Post, and a documentary filmmaker.

@jerodmacevoy

#defcon25/by\_track/track2/saturday

#defcon25/By\_Day/\_saturday

## 1600 - CableTap: Wirelessly Tapping Your Home Network

Saturday at 16:00 in Track 3

45 minutes | Demo, Tool, Exploit

**Marc Newlin\***Security Researcher at Bastille Networks\*

**Logan Lamb\***Security Researcher at Bastille Networks\*

**Chris Grayson\***Founder and Principal Engineer at Web Sight.IO\*

Abstract will be released prior to DEF CON.

Marc Newlin

Marc is a wireless security researcher at Bastille, where he discovered the MouseJack and KeySniffer vulnerabilities affecting wireless mice and keyboards. A glutton for challenging side projects, Marc competed solo in two DARPA challenges, placing third in the DARPA Shredder Challenge, and second in the first tournament of the DARPA Spectrum Challenge.

Logan Lamb

Logan joined Bastille Networks in 2014 as a security researcher focusing on applications of SDR to IoT. Prior to joining Bastille Networks, he was a member of CSIR at Oak Ridge National Lab where his focus was on symbolic analysis of binaries and red-teaming critical

infrastructure.

Chris Grayson

Christopher Grayson (OSCE) is the founder and principal engineer at Web Sight.IO. In this role he handles all operations, development, and research efforts. Christopher is an avid computing enthusiast hailing from [Atlanta, Georgia](#). Having made a habit of pulling things apart in childhood, Chris has found his professional home in information security. Prior to founding Web Sight.IO, Chris was a senior penetration tester at the security consultancy Bishop Fox, and a research scientist at the Georgia Institute of Technology. During his tenure at these organizations, Chris became a specialist in network penetration testing and in the application of academic tactics to the information security industry, both of which contributed to his current research focus of architecting and implementing high-security N-tier systems. Chris attended the Georgia Institute of Technology where he received a bachelor's degree in computational media, a master's degree in computer science, and where he organized and led the Grey H@t student hacking organization.

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

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

## 1600 - Dealing the perfect hand - Shuffling memory blocks on z/OS

Saturday at 16:00 in 101 Track

45 minutes | Demo, Tool

**Ayoul3\*Pentester, Wavestone\***

Follow me on a journey where we p0wn one of the most secure platforms on earth. A giant mammoth that still powers the most critical business functions around the world: The Mainframe! Be it a wire transfer, an ATM withdrawal, or a flight booking, you can be sure that you've used the trusted services of a Mainframe at least once during the last 24 hours. In this talk, I will present methods of privilege escalation on IBM z/OS: How to leverage a simple access to achieve total control over the machine and impersonate other users. If you are interested in mainframes or merely curious to see what a shell looks like on MVS, you're welcome to tag along.

Ayoul3

Ayoub is a pentester working for Wavestone, a consulting firm based in France. He got interested in Mainframe security in 2014 when, during an audit, he noticed the big security gap between this platform and standard systems like Windows and Unix. A gap that makes little sense since z/OS has been around for a while and is used by most major companies to perform critical business operations: wire transfer, claim refunds, bookings, etc.



If you want to test some of the tools showcased during the talk, you can check out his tools:

<https://github.com/ayoul3/>

@ayoul3\_\_

#defcon25/by\_track/101/saturday

#defcon25/By\_Day/\_saturday

## 1600 - From "One Country - One Floppy" to "Startup Nation" - the story of the early days of the Israeli hacking community, and the journey towards today's vibrant startup scene

Saturday at 16:00 in Track 2

45 minutes | Hacker History

**Inbar Raz\***Principal Researcher, PerimeterX Inc.\*

**Eden Shochat\***Equal Partner, Aleph\*

The late 80's and early 90's played a pivotal role in the forming of the Israeli tech scene as we know it today, producing companies like Checkpoint, Waze, Wix, Mobileye, Viber and billions of dollars in fundraising and exits. The people who would later build that industry were in anywhere from elementary school to high school, and their paths included some of the best hacking stories of the time (certainly in the eyes of the locals). The combination of extremely expensive Internet and international dial system, non-existent legal enforcement and a lagging national phone company could not prevent dozens of hungry-for-knowledge kids from teaching themselves the dark arts of reversing, hacking, cracking, phreaking and even carding. The world looked completely different back then and we have some great stories for you. We will cover the evolution of the many-years-later-to-be-named-Cyber community, including personal stories from nearly all categories. Come listen how the Israeli Cyber "empire" was born, 25 years ago, from the perspectives of 2:401/100 and 2:401/100.1.

Inbar Raz

Inbar has been reverse engineering for nearly as long as he has been living. It started with a screwdriver, pliers, wire cutters, and his grandfather's ECG machine, and gradually transitioned into less destructive research. In 1984, aged 9, he started programming on his Dragon 64. At 13 he got his first PC - Amstrad PC1512 - and within a year was already into reverse engineering. It wasn't long before he discovered how to access the X.25 network, Bitnet and Fidonet, and through high-school he was a key figure in the Israeli BBS scene.

Inbar spent most of his career in the Internet and Data Security field, and the only reason he's not in jail right now is because he chose the right side of the law at an early age. In fact, nowadays he commonly lectures about Ethical Hacking and Coordinated Vulnerability Disclosure.

Inbar specializes in outside-the-box approach to analyzing security and finding vulnerabilities, and is currently the Principal Researcher at PerimeterX, researching and educating the public on Automated Attacks on Websites.

@inbarraz

<https://www.linkedin.com/in/inbar-raz-90a7913/>

Eden Shochat

Eden Shochat builds stuff, most recently Aleph, +\$330MM venture capital fund; The Junction, voted #1 startup program in Israel; [face.com](#), a massive face recognition API acquired by Facebook; Aternity, the leading user-centric enterprise IT platform, acquired by Riverbed; and GeekCon, Europe's biggest makers conference. Eden grew up in Nigeria, where he was bored into assembly programming for the Z80 chip, graduated into the demo and cracking scenes while being thrown out of high-school but ended up being a (somewhat) productive member of society.

@eden

<https://www.linkedin.com/in/edens/>

#defcon25/by\_track/track2/saturday

#defcon25/By\_Day/\_saturday

## 1600 - Game of Drones: Putting the Emerging "Drone Defense" Market to the Test

Saturday at 16:00 in Track 4

45 minutes | Art of Defense, Demo, Tool

**Francis Brown\***Partner, Bishop Fox\*

**David Latimer\***Security Analyst, Bishop Fox\*

When you learned that military and law enforcement agencies had trained screaming eagles to pluck drones from the sky, did you too find yourself asking: "I wonder if I could throw these eagles off my tail, maybe by deploying delicious bacon countermeasures?" Well you'd be wise to question just how effective these emerging, first generation "drone defense"

solutions really are, and which amount to little more than "snake oil".

There is no such thing as "best practices" when it comes to defending against "rogue drones", period. Over the past 2 years, new defensive products that detect and respond to "rogue drones" have been crawling out of the woodwork. The vast majority are immature, unproven solutions that require a proper vetting.

We've taken a MythBusters-style approach to testing the effectiveness of a variety of drone defense solutions, pitting them against our DangerDrone. Videos demonstrating the results should be almost as fun for you to watch as they were for us to produce. Expect to witness epic aerial battles against an assortment of drone defense types, including:

- trained eagles and falcons that hunt "rogue drones"
- fighter drones that hunt and shoot nets
- drones with large nets that swoop in and snatch up 'rogue drones'
- surface-to-air projectile weapons, including bazooka-like cannons that launch nets, and shotgun shells containing nets
- signal jamming and hijacking devices that attack drone command and control interfaces
- even frickin' laser beams and Patriot missiles!

We'll also be releasing DangerDrone v2.0, an upgraded version of our free Raspberry Pi-based pentesting quadcopter (basically a ~\$500 hacker's laptop, that can also fly). We'll be giving away a fully functional DangerDrone v2.0 to one lucky audience member!

So come see what's guaranteed to be the most entertaining talk this year and find out which of these dogs can hunt!

Francis Brown

Francis Brown, CISA, CISSP, MCSE, is a Managing Partner at Bishop Fox (formerly Stach & Liu), a security consulting firm providing IT security services to the Fortune 1000 and global financial institutions as well as U.S. and foreign governments. Before joining Stach & Liu, Francis served as an IT Security Specialist with the Global Risk Assessment team of Honeywell International where he performed network and application penetration testing, product security evaluations, incident response, and risk assessments of critical infrastructure. Prior to that, Francis was a consultant with the Ernst & Young Advanced Security Centers and conducted network, application, wireless, and remote access penetration tests for Fortune 500 clients.

Francis has presented his research at leading conferences such as Black Hat USA, DEF CON , RSA, InfoSec World, ToorCon, and HackCon and has been cited in numerous industry and

academic publications.

Francis holds a Bachelor of Science and Engineering from the University of Pennsylvania with a major in Computer Science and Engineering and a minor in Psychology. While at Penn, Francis taught operating system implementation, C programming, and participated in DARPA-funded research into advanced intrusion prevention system techniques.

David Latimer

David Latimer is a Security Analyst at Bishop Fox, a security consulting firm providing IT security services to the Fortune 500, global financial institutions, and high-tech startups. In this role, he focuses on network and web application penetration testing.

He won a state Cisco Networking Skills competition for Arizona in 2013. He has acted as a network engineer for one of Phoenix's largest datacenters, PhoenixNAP, where he architected large-scale virtualization clusters and assisted with backup disaster recovery services.

#defcon25/by\_track/track4/saturday

#defcon25/By\_Day/\_saturday

## 1700 - Here to stay: Gaining persistency by abusing advanced authentication mechanisms

Saturday at 17:00 in 101 Track

45 minutes | Demo

**Marina Simakov**\*Security researcher, Microsoft\*

**Igal Gofman**\*Security researcher, Microsoft\*

Credentials have always served as a favorite target for advanced attackers, since these allow to efficiently traverse a network, without using any exploits.

Moreover, compromising the network might not be sufficient, as attackers strive to obtain persistency, which requires the use of advanced techniques to evade the security mechanisms installed along the way.

One of the challenges adversaries must face is: How to create threats that will continuously evade security mechanisms, and even if detected, ensure that control of the environment can be easily regained?

In this talk, we briefly discuss some of the past techniques for gaining persistency in a network (using local accounts, GPOs, skeleton key, etc.) and why they are insufficient nowadays.

Followed by a comprehensive analysis of lesser known mechanisms to achieve persistency, using non-mainstream methods (such as object manipulation, Kerberos delegation, etc.).

Finally, we show how defenders can secure their environment against such threats.

Marina Simakov

Marina Simakov is a security researcher at Microsoft, with a specific interest in network based attacks.

She holds an M.Sc in computer science, with several published articles. Gave a talk at BlueHat IL 2016 regarding attacks on local accounts.

@simakov\_marina

Igal Gofman

Igal Gofman is a security Researcher at Microsoft. Igal has a proven track record in network security, research oriented development and threat intelligence.

His research interests include network security, intrusion detection and operating systems.

Before Microsoft, Igal was a Threat Response Team Lead at Check Point Software Technologies leading the development of the intrusion detection system.

@IgalGofman

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

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

## 1700 - Introducing HUNT: Data Driven Web Hacking & Manual Testing

Saturday at 17:00 in Track 3

45 minutes | Demo, Tool

**Jason Haddix\*Head of Trust and Security @ Bugcrowd\***

What if you could super-charge your web hacking? Not through pure automation (since it can miss so much) but through powerful alerts created from real threat intelligence? What if you

had a Burp plugin that did this for you? What if that plugin not only told you where to look for vulns but also gave you curated resources for additional exploitation and methodology? What if you could organize your web hacking methodology inside of your tools? Well, now you do! HUNT is a new Burp Suite extension that aims to arm web hackers with parameter level suggestions on where to look for certain classes of vulnerabilities (SQLi, CMDi, LFI/RFI, and more!). This data is parsed from hundreds of real-world assessments, providing the user with the means to effectively root out critical issues. Not only will HUNT help you assess large targets more thoroughly but it also aims to organize common web hacking methodologies right inside of Burp suite. As an open source project, we will go over the data driven design of HUNT and it's core functionality.

Jason Haddix

Jason is the Head of Trust and Security at Bugcrowd. Jason trains and works with internal security engineers to triage and validate hardcore vulnerabilities in mobile, web, and IoT applications/devices. He also works with Bugcrowd to improve the security industries relations with the researchers. Jason's interests and areas of expertise include mobile penetration testing, black box web application auditing, network/infrastructure security assessments, and static analysis. Jason lives in Santa Barbara with his wife and three children. Before joining Bugcrowd Jason was the Director of Penetration Testing for HP Fortify and also held the #1 rank on the Bugcrowd leaderboard for 2014.

@jhaddix

Contributor Acknowledgement:

The Speaker would like to acknowledge the following for their contribution to the presentation.

JP Villanueva is a Trust & Security Engineer at Bugcrowd. Before Bugcrowd, JP spent 2 years as an Application Security Engineer and another 2 years as a Solutions Architect at WhiteHat Security helping customers become more secure. JP has also presented at OWASP and Interop DarkReading events. In his free time, JP enjoys playing classic video games and hacking on bug bounty programs.

Fatih is an Application Security Engineer at Bugcrowd and Bug Hunter located in Istanbul/Turkey. Before Bugcrowd, he was a security consultant at InnoveraBT and performed penetration testing for clients including government, banks, trade, and finance companies. His expertise includes network, web applications, mobile security assessments, and auditing. He also holds OSCP, OSCE, GWAPT certifications.

Ryan Black is the Director of Technical Operations at Bugcrowd where he heads strategy and

operations for the Application Security Engineering team. This group reviews and validates tens of thousands of vulnerability reports to bug bounty programs.

Prior to joining Bugcrowd, Ryan developed and led the static analysis and code review team for HP Fortify on Demand, later expanding to DevOps tooling and integrations for the enterprise. He has also held various InfoSec and technology positions at companies such as Aflac and Apple in the last decade. In addition to professional experience, he holds several industry certifications and participates in a variety of open source software projects and initiatives. On personal time he enjoys coding, gaming, various crafts, and nature activities with his wife, two kids, and three dogs.

Vishal Shah is an Application Security Engineer specializing in web and mobile security at Bugcrowd. Prior to Bugcrowd, Vishal spent time as a Security Consultant with Cigital hacking and building automation for hackers. In his free time, Vishal enjoys working out, CTFs, and playing video games.

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

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

## 1700 - Popping a Smart Gun

Saturday at 17:00 in Track 4

45 minutes | Demo, Exploit

**Plore\*Hacker\***

Smart guns are sold with a promise: they can be fired only by authorized parties. That works in the movies, but what about in real life? In this talk, we explore the security of one of the only smart guns available for sale in the world. Three vulnerabilities will be demonstrated. First, we will show how to make the weapon fire even when separated from its owner by a considerable distance. Second, we will show how to prevent the weapon from firing even when authorized by its owner. Third, we will show how to fire the weapon even when not authorized by its owner, with no prior contact with the specific weapon, and with no modifications to the weapon.

Plore

Plore is an electrical engineer and embedded software developer based in the United States. At DEF CON 24, he spoke about cracking high-security electronic safe locks.

@\_plore

# 1700 - Taking Windows 10 Kernel Exploitation to the next level - Leveraging write-what-where vulnerabilities in Creators Update

Saturday at 17:00 in Track 2

45 minutes | Demo, Exploit

**Morten Schenk**\*Security Advisor, Improsec\*

Since the release of Windows 10 and especially in the Anniversary and Creators Updates, Microsoft has continued to introduce exploit mitigations to the Windows kernel. These include full scale KASLR and blocking kernel pointer leaks.

This presentation picks up the mantle and reviews the powerful read and write kernel primitives that can still be leveraged despite the most recent hardening mitigations. The presented techniques include abusing the kernel-mode Window and Bitmap objects, which Microsoft has attempted to lock down several times. Doing so will present a generic approach to leveraging write-what-where vulnerabilities.

A stable and precise kernel exploit must be able to overcome KASLR, most often using kernel driver leaks. I will disclose several previously unknown KASLR bypasses in Windows 10 Creators Update. Obtaining kernel-mode code execution on Windows has become more difficult with the randomization of Page Table entries. I will show how a generic de-randomization of the Page Table entries can be performed through dynamic reverse engineering. Additionally, I will present an entirely different method which makes the usage of Page Table entries obsolete. This method allocates an arbitrary size piece of executable kernel pool memory and transfers code execution to it through hijacked system calls

Morten Schenk

Morten Schenk (@blomster81) is a security advisor and researcher at Improsec ApS, with a background in penetration testing, red teaming and exploit development. Having a high craving for learning and torture based on taking certifications like OSCP, OSCE and OSEE, Morten's research is specifically focused on binary exploitation and mitigation bypasses on Windows. He blogs about his research at <https://improsec.com/blog/>

@Blomster81



## 2000 - Saturday - D0 No H4RM: A Healthcare Security Conversation

Saturday at 20:00 - 22:00 in Modena Room

Evening Lounge

Christian "quaddi" Dameff MD MS\*Hacker\*

Jeff "r3plicant" Tully MD\*Hacker\*

Beau Woods\*Deputy director of the Cyber Statecraft Initiative in the Brent Scowcroft on International Security\*

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

Michael C. McNeil\*Privacy and security expert, Philips Healthcare\*

Jay Radcliffe\*Senior Security Consultant and Researcher, Rapid7\*

Suzanne Schwartz, MD, MBA\*Associate Director for Science & Strategic Partnerships, FDA'Center for Devices & Radiological Health (CDRH)\*

Previously a free-flowing, fast moving conversation between old friends and new colleagues in a dimly lit and alcohol soaked off-strip hotel suite, the third annual edition of "D0 No H4rm" moves to the better lit and even more alcohol soaked auspices of the DEF CON 25 Evening Lounge for a two hour session that links makers, breakers, and wonks in the healthcare space for a continuation of what may be one of the most important conversations in all of hackerdom- how to ensure the safety and security of patients in a system more connected and vulnerable than ever before. Join physician researchers quaddi and r3plicant, and researcher turned wonk Beau Woods as they offer an update on the state of the field and curate an interactive and engaging panel before breaking out the bottle and getting social. Continuing a tradition that has sparked professional connections, project ideas, and enduring friendships, "D0 No H4rm" aims to offer a prescription for the future, and we want your voice to be heard.

Christian "quaddi" Dameff MD MS

Christian (quaddi) Dameff is an emergency medicine physician, former open capture the flag champion, prior DEF CON speaker, and researcher. Published works include topics such as

therapeutic hypothermia after cardiac arrest, novel drug targets for myocardial infarction patients, and other Emergency Medicine related works with an emphasis on CPR optimization. Security research topics including hacking critical healthcare infrastructure and medical devices. This is his thirteenth DEF CON.

@cdameffMD

Jeff "r3plicant" Tully MD

Jeff Tully is an anesthesiologist, pediatrician, and researcher with an interest in understanding the ever-growing intersections between health care and technology. Prior to medical school he worked on "hacking" the genetic code of Salmonella bacteria to create anti-cancer tools, and throughout medical training has remained involved in the conversations and projects that will secure healthcare and protect our patients as we face a brave new world of remote care, implantable medical devices, and biohacking.

@jefftullymd

Beau Woods

Beau Woods is the deputy director of the Cyber Statecraft Initiative in the Brent Scowcroft on International Security. His focus is the intersection of cyber (yes, he'll drink for that) security and the human condition, primarily around Cyber Safety. This comes out of the I Am The Cavalry initiative, ensuring the connected technology that can impact life and safety is worthy of our trust. Beau started his career working at a regional health provider, protecting patients by defending medical data and devices.

@beauwoods

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. Michael C. McNeil

Michael C. McNeil is a noted privacy and security expert who leads the Global Product Security and Services organization at Philips Healthcare. In this capacity, McNeil leads the global product security and data protection program for the company. He is also a member of the Visual Privacy Advisory Council (VPAC) , Medical Device Privacy Consortium (MDPC),

Medical Device Innovation, Safety and Services Consortium (MDISS) and a frequent speaker at privacy and security conferences around the world.

Jay Radcliffe

Jay Radcliffe is a Senior Security Consultant and Researcher at Rapid7. He is an offensive penetration tester with a knack for hardware hacking and embedded device security. He has given dozens of presentations at conferences around the world including DEF CON and Blackhat including several on the security of insulin pumps.

Suzanne Schwartz, MD, MBA

Suzanne Schwartz, MD, MBA is the Associate Director for Science & Strategic Partnerships at FDA's Center for Devices & Radiological Health (CDRH). Among other public health concerns, her portfolio has most notably included medical device cybersecurity, for which she chairs CDRH's Cybersecurity Working Group. She also co-chairs the Government Coordinating Council for Healthcare & Public Health critical infrastructure sector. Before FDA, Suzanne was a full time surgical faculty member at Weill Cornell Medical College.

[#defcon25/eveninglounges](#)

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

## 2000 - Saturday - Panel - Meet the Feds (who care about security research)

Saturday at 20:00 - 22:00 in Capri Room

Evening Lounge

**Allan Friedman\***Director of Cybersecurity, National Telecommunications and Information Administration, US Department of Commerce\*

**Amélie E. Koran\***Deputy Chief Information Officer, U.S. Department of Health and Human Services, Office of the Inspector General\*

**Leonard Bailey\***Special Counsel for National Security, Computer Crime & Intellectual Property Section, Criminal Division, U.S. Department of Justice\*

**Nick Leiserson\***Legislative Director, Office of Congressman James R. Langevin (RI-02)\*

Security research is no longer a foreign concept in [Washington, DC](#). A growing number of policymakers are not only thinking about its importance, but are eager to work with hackers to better understand the implications of policy and to help hackers navigate laws that affect security research. Officials from the Department of Commerce, the Department of Justice,

and Congress will talk about how security policy has been evolving; help you understand how you can get involved and make your voice heard; and host an extended Q&A. Hear about everything from making laws more hacker friendly to encryption to IoT security. It's your opportunity to meet the feds and ask them anything.

Allan Friedman

Allan Friedman is the Director of Cybersecurity Initiatives at National Telecommunications and Information Administration in the US Department of Commerce. He coordinates NTIA's multistakeholder processes, bringing together the community on issues like vulnerability disclosure and IoT Security. Prior to joining the Federal Government, Friedman spent over a decade as a noted cybersecurity and technology policy researcher at Harvard's Computer Science Department, the Brookings Institution, and George Washington University's Engineering School. He has a degree in computer science from Swarthmore College and a Ph.D. in public policy from Harvard University, and is the Co-Author of "Cybersecurity and Cyberwar: What Everyone Needs to Know".


Amélie E. Koran

serves as the Deputy Chief Information Officer for the U.S. Department of Health and Human Services, Office of the Inspector General. Amélie's path to DHHS OIG took her the long way around - through multiple industry sectors, academia, and the public sector. Her professional experience includes time spent at The Walt Disney Company, Carnegie Mellon University CERT/CC, Mandiant, The World Bank, and The American Chemical Society. She began her time in the public sector as Lead Enterprise Security Architect for the U.S. Department of the Interior, eventually moving on to lead Continuous Diagnostics and Mitigation implementation for the U.S. Treasury Department. Amélie later spent time on a leadership development rotation as part of the President's Management Council Fellowship serving the Federal CIO in supporting cybersecurity policy analysis and legislative review, where she took an active role in the government-wide Open Data Initiative and helped in giving "birth" to the United States Digital Service (USDS). She's an ardent advocate for innovative approaches to hiring talent and rationally applying security strategies and technologies for the Federal Government space.

@webjedi

Leonard Bailey

Mr. Bailey is Special Counsel for National Security in the Computer Crime and Intellectual Property Section. He has prosecuted computer crime cases and routinely advises on cybersecurity, searching and seizing electronic evidence, and conducting electronic surveillance. He has managed DOJ cyber policy as Senior Counselor to the Assistant Attorney General for the National Security Division and then as an Associate Deputy Attorney General. He has also served as Special Counsel and Special Investigative Counsel for DOJ's Inspector General. Mr. Bailey is a graduate of Yale University and Yale Law School. He has taught

courses on cybercrime and cybersecurity at Georgetown Law School and Columbus School of Law in  [Washington, D.C.](#)

Nick Leiserson

Nick Leiserson is Legislative Director to Congressman Jim Langevin (RI-02), a senior member of the House Armed Services and Homeland Security Committees and the co-founder of the Congressional Cybersecurity Caucus. Leiserson serves as Rep. Langevin's principal advisor on an array of issues, particularly homeland security; judiciary; and technology policy. He holds a degree in computer science from Brown University.

[#defcon25/eveninglounges](#)

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