

1000 - macOS/iOS Kernel Debugging and Heap Feng Shui

Friday at 10:00 in 101 Track

20 minutes

Min(Spark) Zheng*Security Expert @ Alibaba Inc. Ph.D of CUHK.*

Xiangyu Liu*Security Engineer @ Alibaba Inc. Ph.D of CUHK.*

Kernel bug is always very difficult to reproduce and may lead to the entire system panic and restart. In practice, kernel debugging is the only way to analyze panic scenes. However, implementing such a technique in real world is not an easy task since kernel code cannot be executed in the debugger, thus is hard to be tracked. Luckily, macOS has provided a very powerful kernel debugging mechanism, KDK (Kernel Development Kit), to assist people to analyze and develop kernel exploits. While for iOS, although there is no official kernel debugger, it is also possible for us to achieve kernel debugging by leveraging some tricks.

In this talk, we will share some kernel debugging techniques and their corresponding tricks on the latest iOS/macOS. In addition, we will also introduce the new kernel heap mitigation mechanisms on iOS 10/macOS 10.12 and two heap feng shui techniques to bypass them. Finally, we will demonstrate how to debug a concrete kernel heap overflow bug and then leverage our new heap feng shui techniques to gain arbitrary kernel memory read/write on the iOS 10.2/macOS 10.12.

Min(Spark) Zheng

Min(Spark) Zheng, Security Expert @ Alibaba Inc. Ph.D of CUHK.

[#defcon25/by_track/101/Friday](#)

[#defcon25/By_Day/_Friday](#)

1000 - Secret Tools: Learning about Government Surveillance Software You Can't Ever See

Friday at 10:00 in Track 4

20 minutes | 0025

Peyton "Foofus" Engel*Attorney at Hurley, Burish & Stanton, S.C.*

Imagine that you're accused of a crime, and the basis of the accusation is a log entry generated by a piece of custom software. You might have some questions: does the software work? how accurate is it? how did it get the results that it did? Unfortunately, the software isn't

available to the public. And you can't get access to the source code or even a working instance of the software. All you get are assurances that the software is in use by investigators around the globe, and doesn't do anything that law enforcement isn't supposed to be doing. Because you can trust the government, right?

This talk will look at a family of tools designed for investigating peer-to-peer networks. By synthesizing information from dozens of search warrant affidavits, and a few technical sources, we're able to put together at least a partial picture of the software's capabilities. But we'll also look at the reasons the government offers for keeping these tools out of the public eye and talk about whether they make sense. Finally, we'll examine the implications that investigations based on secret capabilities have for justice.

Peyton "Foofus" Engel

After 18 years in IT, with 16 of those years spent in security and penetration testing, Foofus now works as an attorney. But because he's got significant experience with the Internet and security, one area of his practice focuses on consulting with litigants where digital evidence is at stake. In this capacity he does forensic analysis and assists other attorneys with strategy for presenting (or calling into question) computer-based evidence. In his spare time, Foofus enjoys cooking, playing guitar, and opera. Oh, and remember CoffeeWars? Foofus was pretty involved with that

[#defcon25/by_track/track4/Friday](#)

[#defcon25/By_Day/_Friday](#)

1000 - The Brain's Last Stand

Friday at 10:00 in Track 3

45 minutes

Garry Kasparov*Avast Security Ambassador*

Former world chess champion Garry Kasparov has a unique place in history as the proverbial "man" in "man vs. machine" thanks to his iconic matches against the IBM supercomputer Deep Blue. Kasparov walked away from that watershed moment in artificial intelligence history with a passion for finding ways humans and intelligent machines could work together. In the spirit of "if you can't beat'em, join'em," Kasparov has explored that potential for the 20 years since his loss to Deep Blue. Navigating a practical and hopeful approach between the utopian and dystopian camps, Kasparov focuses on how we can rise to the challenge of the AI revolution despite job losses to automation and refuting those who say our technology is

making us less human. He includes concrete examples and forward-looking strategies on AI.

Garry Kasparov

Garry Kasparov was born in Baku, Azerbaijan, in the Soviet Union in 1963. He became the youngest world chess champion in history in 1985 and was the world's top-rated player for 20 years, until he retired in 2005. His matches against arch-rival Anatoly Karpov and the IBM supercomputer Deep Blue popularized chess and machine intelligence in unprecedented ways. Kasparov became a pro-democracy leader in Russia and an outspoken defender of individual freedom around the world, a mission he continues as the chairman of the New York-based Human Rights Foundation. He is a Visiting Fellow at the Oxford-Martin School, where his lectures focus on human-machine collaboration. Kasparov is a provocative speaker who appears frequently before business, academic, and political audiences to speak about decision-making, strategy, technology, and artificial intelligence. His influential writings on politics, cognition, and tech have appeared in dozens of major publications around the world. He has written two acclaimed series of chess books and the bestsellers *How Life Imitates Chess* on decision-making and *Winter Is Coming* on Russia and Vladimir Putin. His new book, *Deep Thinking: Where Machine Intelligence Ends and Human Creativity Begins* comes out in May 2017. In 2016, he was named a Security Ambassador by Avast, where he discusses cybersecurity and the digital future. He lives in New York City with his wife Dasha and their two children.

@Kasparov63

[#defcon25/by_track/track3/friday](#)

[#defcon25/By_Day/_Friday](#)

1000 - Welcome to DEF CON 25

Friday at 10:00 in Track 2

20 minutes | Hacker History

The Dark Tangent*Founder, DEF CON*

The Dark Tangent welcomes everyone to DEF CON 25, our silver anniversary!

The Dark Tangent

[#defcon25/by_track/track2/friday](#)

[#defcon25/By_Day/_Friday](#)

1030 - Hacking travel routers like it's 1999

Friday at 10:30 in Track 2

20 minutes | Demo, Exploit

Mikhail Sosonkin*Security Researcher, Synack Inc.*

Digital nomads are a growing community and they need internet safety just like anyone else. Trusted security researchers have warned about the dangers of traveling through AirBnB's. Heeding their advice, I purchased a HooToo TM06 travel router to create my own little enclave while I bounce the globe. Being a researcher myself, I did some double checking.

So, I started fuzzing and reverse engineering. While the TM06 is a cute and versatile little device - protection against network threats, it is not. In this talk, I will take you on my journey revealing my methodology for discovering and exploiting two memory corruption vulnerabilities. The vulnerabilities are severe and while they've been reported to the vendor, they are very revealing data points about the security state of such devices. While the device employs some exploitation mitigations, there are many missing. I will be showing how I was able to bypass them and what mitigations should've been employed, such as NX-Stack/Heap, canaries, etc, to prevent me from gaining arbitrary shellcode execution.

If you're interested in security of embedded/IoT systems, travel routers or just good old fashioned MIPS hacking, then this talk is for you!

Mikhail Sosonkin

Mikhail Sosonkin is a Security Researcher at Synack where he digs into the security aspects of low level systems. He enjoys automating aspects of reverse engineering and fuzzing in order to better understand application internals. Mikhail has a CS degree from NYU, where he has also taught Application Security, and a Software Engineering masters from Oxford University. Being a builder and a hacker at heart, his interests are in vulnerability analysis, automation, malware and reverse engineering. Mikhail much enjoys speaking at such conferences as ZeroNights in Moscow and DEF CON in Las Vegas!

@hexlogic, Blog <http://debugtrap.com/>

#defcon25/by_track/track2/friday

#defcon25/By_Day/_Friday

1030 - Offensive Malware Analysis: Dissecting OSX/FruitFly via a Custom C&C Server

Friday at 10:30 in 101 Track

20 minutes | Demo, Tool

Patrick Wardle*Chief Security Researcher, Synack / Creator of Objective-See*

Creating a custom command and control (C&C) server for someone else's malware has a myriad of benefits. If you can take over it a domain, you then may be able to fully hijack other hackers' infected hosts. A more prosaic benefit is expediting analysis. While hackers and governments may be more interested in the former, malware analysts can benefit from the latter.

FruitFly, the first OS X/macOS malware of 2017, is a rather intriguing specimen. Selectively targeting biomedical research institutions, it is thought to have flown under the radar for many years. In this talk, we'll focus on the 'B' variant of FruitFly that even now, is only detected by a handful of security products.

We'll begin by analyzing the malware's dropper, an obfuscated perl script. As this language is rather archaic and uncommon in malware droppers, we'll discuss some debugging techniques and fully deconstruct the script.

While this dropper component also communicates with the C&C server and supports some basic commands, it drops a binary payload in order to perform more complex actions. However, instead of fully reversing this piece of the malware, the talk will focus on an initial triage and show how this was sufficient for the creation of a custom C&C server. With such a server, we can easily coerce the malware to reveal its full capabilities. For example, the malware invokes a handful of low-level mouse & graphics APIs, passing in a variety of dynamic parameters. Instead of spending hours reversing and debugging this complex code, via the C&C server, we can simply send it various commands and observe the effects.

Of course this approach hinges on the ability to closely observe the malware's actions. As such, we'll discuss macOS-specific tools that can monitor various events, and where necessary detail the creation of custom ones (e.g. a 'mouse sniffer' that locally observes and decodes commands sent from the malware to the OS, in order to control the mouse).

While some of this talk is FruitFly and/or macOS specific, conceptually it should broadly apply to analyzing other malware, even on other operating systems :)

Patrick Wardle

Patrick Wardle is the Chief Security Researcher at Synack, and founder of Objective-See. Having worked at NASA and the NSA, and well as presented at many security conferences, he is intimately familiar with aliens, spies, and talking nerdy. Currently, Patrick's focus is on automated vulnerability discovery, and the emerging threats of OS X and mobile malware. In his personal time, Patrick collects macOS malware and writes free macOS security tools.

#defcon25/by_track/101/Friday

#defcon25/By_Day/_Friday

1030 - Panel: Meet The Feds

Friday at 10:20 in Track 4

75 minutes

Andrea Matwyshyn*Cranky law professor.*

Terrell McSweeney*Commissioner, Federal Trade Commission*

Dr. Suzanne Schwartz*FDA*

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

More Information Coming soon!

Andrea Matwyshyn

Dr. Andrea M. Matwyshyn is an academic and author whose work focuses on technology and innovation policy, particularly information security, consumer privacy, intellectual property, and technology workforce pipeline policy. Her full vitae is available [here](#).

Professor Matwyshyn is a (tenured full) professor of law / professor of computer science (by courtesy) at Northeastern University, where she is the co-director of the Center for Law, Innovation, and Creativity (CLIC). She is also a faculty affiliate of the Center for Internet and Society at Stanford Law School and a visiting research collaborator at the Center for Information Technology Policy at Princeton University, where she was the Microsoft Visiting Professor of Information Technology Policy during 2014-15. Professor Matwyshyn is also a Senior Fellow of the Cyber Statecraft Initiative at the Atlantic Council's Brent Scowcroft Center on International Security and a US-UK Fulbright Commission Cyber Security Scholar award recipient in 2016-2017.

She has worked in both the public and the private sector. In 2014, she served as the Senior Policy Advisor/ Academic in Residence at the U.S. Federal Trade Commission. As public service, she has testified in Congress on issues of information security regulation, and she maintains ongoing policy engagement. Prior to entering the academy, she was a corporate attorney in private practice, focusing her work on technology transactions. She continues to

maintain collaborative technology industry relationships and has authored articles for the popular business press.

Professor Matwyshyn has previously held primary appointments in University of Pennsylvania's Wharton School, Northwestern University School of Law, and the University of Florida Levin College of Law. She has also held visiting appointments or affiliations at the University of Oxford, University of Cambridge, University of Edinburgh, Singapore Management University, Indian School of Business, University of Notre Dame, and Princeton University.

Her Erdos number is 4. Her primary hobbies are photography, documentary film, and collecting books about Grace Hopper.

Terrell McSweeney

Terrell McSweeney was sworn in as a Commissioner of the Federal Trade Commission on April 28, 2014, to a term that expires in September 2017.

Prior to joining the Commission, McSweeney served as Chief Counsel for Competition Policy and Intergovernmental Relations for the U.S. Department of Justice Antitrust Division. She joined the Antitrust Division after serving as Deputy Assistant to the President and Domestic Policy Advisor to the Vice President from January 2009 until February 2012, advising President Obama and Vice President Biden on policy in a variety of areas, including health care, innovation, intellectual property, energy, education, women's rights, criminal justice and domestic violence.

McSweeney's government service also includes her work as Senator Joe Biden's Deputy Chief of Staff and Policy Director in the U.S. Senate, where she managed domestic and economic policy development and legislative initiatives, and as Counsel on the Senate Judiciary Committee, where she worked on issues such as criminal justice, innovation, women's rights, domestic violence, judicial nominations and immigration and civil rights. She also worked as an attorney at O'Melveny & Myers LLP.

McSweeney is a graduate of Harvard University and Georgetown University Law School.

@TMcSweeneyFTC

Dr. Suzanne Schwartz

Bio coming soon.

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.](#)

[#defcon25/by_track/track4/Friday](#)

[#defcon25/By_Day/_Friday](#)

1100 - Hacking Smart Contracts

Friday at 11:00 in Track 3

45 minutes | Demo

Konstantinos Karagiannis*Chief Technology Officer, Security Consulting, BT Americas*

It can be argued that the DAO hack of June 2016 was the moment smart contracts entered mainstream awareness in the InfoSec community. Was the hope of taking blockchain from mere cryptocurrency platform to one that can perform amazing Turing-complete functions doomed? We've learned quite a lot from that attack against contract code, and Ethereum marches on. Smart contracts are a key part of the applications being created by the Enterprise Ethereum Alliance, Quorum, and smaller projects in financial and other companies. Ethical hacking of smart contracts is a critical new service that is needed. And as is the case with coders of Solidity (the language of Ethereum smart contracts), hackers able to find security flaws in the code are in high demand.

Join Konstantinos for an introduction to a methodology that can be applied to Solidity code review ... and potentially adapted to other smart contract projects. We'll examine the few tools that are needed, as well as the six most common types of flaws, illustrated using either public or sanitized real world" vulnerabilities.

Konstantinos Karagiannis

Konstantinos Karagiannis is the Chief Technology Officer for Security Consulting at BT Americas. In addition to guiding the technical direction of ethical hacking and security engagements, Konstantinos specializes in hacking financial applications, including smart contracts and other blockchain implementations. He has spoken at dozens of technical conferences around the world, including Black Hat Europe, RSA, and ISF World Security Congress.

@konstanthacker

#defcon25/by_track/track3/friday

#defcon25/By_Day/_Friday

1100 - Rage Against the Weaponized AI Propaganda Machine

Friday at 11:00 in 101 Track

45 minutes | 0025

Suggy (AKA Chris Sumner)*Researcher, The Online Privacy Foundation*

Psychographic targeting and the so called "Weaponized AI Propaganda Machine" have been blamed for swaying public opinion in recent political campaigns. But how effective are they? Why are people so divided on certain topics? And what influences their views? This talk presents the results of five studies exploring each of these questions. The studies examined authoritarianism, threat perception, personality-targeted advertising and biases in relation to support for communication surveillance as a counter-terrorism strategy. We found that people with an authoritarian disposition were more likely to be supportive of surveillance, but that those who are less authoritarian became increasingly supportive of such surveillance the greater they perceived the threat of terrorism. Using psychographic targeting we reached Facebook audiences with significantly different views on surveillance and demonstrated how tailoring pro and anti-surveillance ads based on authoritarianism affected return on marketing investment. Finally, we show how debunking propaganda faces big challenges as biases severely limit a person's ability to interpret evidence which runs contrary to their beliefs. The results illustrate the effectiveness of psychographic targeting and the ease with which individuals' inherent differences and biases can be exploited.

Suggy (AKA Chris Sumner)

Suggy is the lead researcher and co-founder of the not-for-profit Online Privacy Foundation, who contribute to the field of psychological research in online contexts. He has authored papers and spoken on this topic at DEF CON and other noteworthy security, psychology, artificial intelligence and machine learning conferences. For the past 4 years, Suggy has served as a member of the DEF CON CFP review board. By day, he works in security strategy at Hewlett Packard Enterprise.

@thesuggmeister, <https://www.onlineprivacyfoundation.org/>

#defcon25/by_track/101/Friday

#defcon25/By_Day/_Friday

1100 - Weaponizing the BBC Micro:Bit

Friday at 11:00 in Track 2

45 minutes | Demo, Tool, Exploit

Damien "virtualabs" Cauquil* Senior security researcher, Econocom Digital Security*

In 2015, BBC sponsored Micro:Bit was launched and offered to one million students in the United Kingdom to teach them how to code. This device is affordable and have a lot of features and can be programmed in Python rather than C++ like the Arduino. When we discovered this initiative in 2016, we quickly thought it was possible to turn this tiny device into some kind of super-duper portable wireless attack tool, as it is based on a well-known 2.4GHz RF chip produced by Nordic Semiconductor.

It took us a few months to hack into the Micro:Bit firmware and turn it into a powerful attack tool able to sniff keystrokes from wireless keyboards or to hijack and take complete control of quadcopters during flight. We also developed many tools allowing security researchers to interact with proprietary 2.4GHz protocols, such as an improved sniffer inspired by the mousejack tools designed by Bastille. We will release the source code of our firmware and related tools during the conference.

The Micro:Bit will become a nifty platform to create portable RF attack tools and ease the life of security researchers dealing with 2.4GHz protocols !

Damien "virtualabs" Cauquil

Damien Cauquil is a senior security researcher at Digital Security (CERT-UBIK), a French security company focused on IoT and related ground breaking technologies. He spoke at various international security conferences including Chaos Communication Camp, [Hack.lu](#), Hack In Paris and a dozen times at the Nuit du Hack (one of the oldest French security conferences).

@virtualabs, <https://www.digitalsecurity.fr>

[#defcon25/by_track/track2/friday](#)

[#defcon25/By_Day/_Friday](#)

1200 - A New Era of SSRF - Exploiting URL Parser in Trending Programming Languages!

Friday at 12:00 in Track 3

45 minutes | Demo, Tool, Exploit

Orange Tsai*Security Consultant from DEVCORE*

We propose a new exploit technique that brings a whole-new attack surface to bypass SSRF (Server Side Request Forgery) protections. This is a very general attack approach, in which we used in combination with our own fuzzing tool to discover many 0days in built-in libraries of very widely-used programming languages, including Python, PHP, Perl, Ruby, Java, JavaScript, Wget and cURL. The root cause of the problem lies in the inconsistency of URL parsers and URL requesters.

Being a very fundamental problem that exists in built-in libraries, sophisticated web applications such as WordPress (27% of the Web), vBulletin, MyBB and GitHub can also suffer, and 0days have been discovered in them via this technique. This general technique can also adapt to various code contexts and lead to protocol smuggling and SSRF bypassing. Several scenarios will be demonstrated to illustrate how URL parsers can be exploited to bypass SSRF protection and achieve RCE (Remote Code Execution), which is the case in our GitHub Enterprise demo.

Understanding the basics of this technique, the audience won't be surprised to know that more than 20 vulnerabilities have been found in famous programming languages and web applications aforementioned via this technique.

Orange Tsai

Cheng-Da Tsai, also as known as Orange Tsai, is member of DEVCORE and CHROOT from Taiwan. Speaker of conference such as HITCON, WooYun and AVTokyo. He participates numerous Capture-the-Flags (CTF), and won 2nd place in DEF CON 22 as team member of HITCON.

Currently focusing on vulnerability research & web application security. Orange enjoys to find vulnerabilities and participates Bug Bounty Program. He is enthusiasm for Remote Code Execution (RCE), also uncovered RCE in several vendors, such as Facebook, Uber, Apple, GitHub, Yahoo and Imgur.

[#defcon25/by_track/track3/friday](#)

[#defcon25/By_Day/_Friday](#)

1200 - CITL and the Digital Standard - A Year Later

Friday at 12:00 in 101 Track

45 minutes | Art of Defense

Sarah Zatko*Chief Scientist, Cyber ITL*

A year ago, Mudge and I introduced the non-profit Cyber ITL at DEF CON and its approach to automated software safety analysis. Now, we'll be covering highlights from the past year's research findings, including our in-depth analysis of several different operating systems, browsers, and IoT products.

Parts of our methodologies have now been adopted by Consumer Reports and rolled into their Digital Standard for evaluating safety, security, and privacy, in a range of consumer devices. The standard defines important consumer values that must be addressed in product development, with the goal of enabling consumer organizations to test, evaluate, and report on whether new products protect consumer security, safety, and privacy.

Sarah Zatko

Sarah Zatko is the Chief Scientist at the Cyber Independent Testing Lab (CITL), where she develops testing protocols to assess the security and risk profile of commercial software. She also works on developing automated reporting mechanisms to make such information understandable and accessible to a variety of software consumers. The CITL is a non-profit organization dedicated to empowering consumers to understand risk in software products. Sarah has degrees in Math and Computer Science from MIT and Boston University. Prior to her position at CITL, she worked as a computer security professional in the public and private sector.

cyber-itl.org

#defcon25/by_track/101/Friday

#defcon25/By_Day/_Friday

1200 - Hacking Democracy: A Socratic Dialogue

Friday at 12:00 in Track 4

45 minutes

Mr. Sean Kanuck*Stanford University, Center for International Security and Cooperation*


In the wake of recent presidential elections in the US and France, "hacking" has taken on new political and social dimensions around the globe. We are now faced with a world of complex influence operations and dubious integrity of information. What does that imply for democratic institutions, legitimacy, and public confidence?

This session will explore how liberal democracy can be hacked – ranging from direct manipulation of electronic voting tallies or voter registration lists to indirect influence over mass media and voter preferences – and question the future role of "truth" in open societies. Both domestic partisan activities and foreign interventions will be considered on technical, legal, and philosophical grounds. The speaker will build on his experience as an intelligence professional to analyze foreign capabilities and intentions in the cyber sphere in order to forecast the future of information warfare. Audience members will be engaged in a Socratic dialogue to think through how modern technologies can be used to propagate memes and influence the electorate. The feasibility of, and public policy challenges associated with, various approaches to hacking democracy will also be considered. This conceptual discussion of strategic influence campaigns will not require any specific technical or legal knowledge

Mr. Sean Kanuck

Sean Kanuck is an attorney and strategic consultant who advises governments, corporations, and entrepreneurs on the future of information technology. Sean is affiliated with Stanford University's Center for International Security and Cooperation and has received several international appointments, including: Chair of the Research Advisory Group for the Global Commission on the Stability of Cyberspace (Hague, Netherlands), Distinguished Visiting Fellow at Nanyang Technological University (Singapore), and Distinguished Fellow with the Observer Research Foundation (New Delhi, India). He regularly gives keynote addresses for global audiences on a variety of cyber topics, ranging from risk analysis to identity intelligence to arms control.

Sean served as the United States' first National Intelligence Officer for Cyber Issues from 2011 to 2016. He came to the National Intelligence Council after a decade of experience in the Central Intelligence Agency's Information Operations Center, including both analytic and field assignments. In his Senior Analytic Service role, he was a contributing author for the 2009 White House Cyberspace Policy Review, an Intelligence Fellow with the Directorates for Cybersecurity and Combating Terrorism at the National Security Council, and a member of the United States delegation to the United Nations Group of Governmental Experts on international information security.

Prior to government service, Sean practiced law with Skadden Arps in New York, where he specialized in mergers and acquisitions, corporate finance, and banking matters. He is admitted to the bar in New York and  Washington DC, and his academic publications focus on information warfare and international law. Sean holds degrees from Harvard University (A.B., J.D.), the London School of Economics (M.Sc.), and the University of Oslo (LL.M.). He also proudly serves as a Trustee of the Center for Excellence in Education, a charity

promoting STEM education that is based in McLean, Virginia.

@seankanuck

#defcon25/by_track/track4/Friday

#defcon25/By_Day/_Friday

1200 - Open Source Safe Cracking Robots - Combinations Under 1 Hour! (Is it bait? Damn straight it is.)

Friday at 12:00 in Track 2

45 minutes | Demo, Tool, Exploit

Nathan Seidle*Founder, SparkFun Electronics*

We've built a \$200 open source robot that cracks combination safes using a mixture of measuring techniques and set testing to reduce crack times to under an hour. By using a motor with a high count encoder we can take measurements of the internal bits of a combination safe while it remains closed. These measurements expose one of the digits of the combination needed to open a standard fire safe. Additionally, 'set testing' is a new method we created to decrease the time between combination attempts. With some 3D printing, Arduino, and some strong magnets we can crack almost any fire safe. Come checkout the live cracking demo during the talk!

Nathan Seidle

Nathan Seidle is the founder of SparkFun Electronics in Boulder, Colo. Nathan founded SparkFun in 2003 while an undergraduate student studying electrical engineering. After building the company across 14 years to over 130 employees he now heads the SparkX Lab within SparkFun, tinkering, hacking and building new products.

Nathan has built a large catalog of off the beaten path projects including a 12' GPS clock, a wall sized Tetris interface, an autonomous miniature electric bat-mobile, a safe cracking robot, and a hacked bathroom scale to measure the weight of his beehive. He believes strongly in the need to teach the next generation of technical citizens.

Nathan is a founding member of the Open Source Hardware Association. He has served on the board of OSHWA and continues to promote and serve the organization. Nathan has been invited to the White House to participate in discussions around intellectual property policy and patent reform and attended multiple White House Maker Faires. Nathan has spoken in front of Congress on copyright and trademark policy. He has presented on the many facets of manufacturing and open hardware at the National Science Foundation, Google, and

Sketching in Hardware. Nathan has guest lectured at numerous institutions including MIT, Stanford and West Point Academy.

In their off time, Nathan and his wife Alicia can be found making rather silly electronics projects together for their local Public Library, their nieces and nephews, and Burning Man. Nathan and Alicia live in Boulder, Colorado with their pet tree Alfonso.

@chipaddict, @sparkfun, www.sparkfun.com

#defcon25/by_track/track2/friday

#defcon25/By_Day/_Friday

1300 - Controlling IoT devices with crafted radio signals

Friday at 13:00 in 101 Track

45 minutes | Demo, Tool

Caleb Madrigal*Hacker, FireEye/Mandiant*

In this talk, we'll be exploring how wireless communication works. We'll capture digital data live (with Software-Defined Radio), and see how the actual bits are transmitted. From here, we'll see how to view, listen to, manipulate, and replay wireless signals. We'll also look at interrupting wireless communication, and finally, we'll even generate new radio waves from scratch (which can be useful for fuzzing and brute force attacks). I'll also be demoing some brand new tools I've written to help in the interception, manipulation, and generation of digital wireless signals with SDR.

Caleb Madrigal

Caleb Madrigal is a programmer who enjoys hacking and mathing. He is currently working as a senior software engineer on Incident Response software at Mandiant/FireEye. Most of his recent work has been in Python, Jupyter, Javascript, and C. Caleb has been into security for a while... in high school, he wrote his own (bad) cryptography and steganography software. In college, he did a good bit of "informal pen testing". Recently, Caleb has been playing around with SDR, IoT hacking, packet crafting, and a good bit of math/probability/AI/ML.

@caleb_madrigal, calebmadrigal.com

#defcon25/by_track/101/Friday

#defcon25/By_Day/_Friday

1300 - Next-Generation Tor Onion Services

Friday at 13:00 in Track 4

45 minutes | 0025

Roger Dingledine*The Tor Project*

Millions of people around the world use Tor every day to protect themselves from surveillance and censorship. While most people use Tor to reach ordinary websites more safely, a tiny fraction of Tor traffic makes up what overhyped journalists like to call the "dark web". Tor onion services (formerly known as Tor hidden services) let people run Internet services such as websites in a way where both the service and the people reaching it can get stronger security and privacy.

I wrote the original onion service code as a toy example in 2004, and it sure is showing its age. In particular, mistakes in the original protocol are now being actively exploited by fear-mongering "threat intelligence" companies to build lists of onion services even when the service operators thought they would stay under the radar.

These design flaws are a problem because people rely on onion services for many cool use cases, like metadata-free chat and file sharing, safe interaction between journalists and their sources, safe software updates, and more secure ways to reach popular websites like Facebook.

In this talk I'll present our new and improved onion service design, which provides stronger security and better scalability. I'll also publish a new release of the Tor software that lets people use the new design.

Roger Dingledine

Roger Dingledine is President and co-founder of the Tor Project, a non-profit that writes software to keep people around the world safe on the Internet.

Roger is a leading researcher in anonymous communications and a frequent public speaker. He coordinates and mentors academic researchers working on Tor-related topics, he is on the board of organizers for the international Privacy Enhancing Technologies Symposium (PETS), and he has authored or co-authored over two dozen peer-reviewed research papers on anonymous communications and privacy tools.

Among his achievements, Roger was chosen by the MIT Technology Review as one of its top 35 innovators under 35, he co-authored the Tor design paper that won a Usenix Security "Test of Time" award, and he has been recognized by Foreign Policy magazine as one of its top 100 global thinkers.

Roger graduated from The Massachusetts Institute of Technology and holds a Master's degree in electrical engineering and computer science as well as undergraduate degrees in computer science and mathematics.

[#defcon25/by_track/track4/Friday](#)

[#defcon25/By_Day/_Friday](#)

1300 - Starting the Avalanche: Application DoS In Microservice Architectures

Friday at 13:00 in Track 3

45 minutes | Demo, Tool

Scott Behrens*Senior Application Security Engineer*

Jeremy Heffner*Senior Cloud Security Engineer*

We'd like to introduce you to one of the most devastating ways to cause service instability in modern micro-service architectures: application DDoS. Unlike traditional network DDoS that focuses on network pipes and edge resources, our talk focuses on identifying and targeting expensive calls within a micro-services architecture, using their complex interconnected relationships to cause the system to attack itself – with massive effect. In modern microservice architectures it's easier to cause service instability with sophisticated requests that model legitimate traffic to pass right through web application firewalls.

We will discuss how the Netflix application security team identified areas of our microservices that laid the groundwork for these exponential-work attacks. We'll step through one case study of how a single request into an API endpoint fans out through the application fabric and results in an exponential set of dependent service calls. Disrupting even one point within the dependency graph can have a cascading effect throughout not only the initial endpoint, but the dependent services backing other related API services.

We will then discuss the frameworks we collaborated on building that refine the automation and reproducibility of testing the endpoints, which we've already successfully leveraged against our live production environment. We will provide a demonstration of the frameworks which will be open sourced in conjunction with this presentation. Attendees will leave this talk understanding architectural and technical approaches to identify and remediate application DDoS vulnerabilities within their own applications. Attendees will also gain a greater understanding on how take a novel new attack methodology and build an orchestration

framework that can be used at a global scale.

Scott Behrens

Scott Behrens is currently employed as a senior application security engineer for Netflix. Prior to Netflix Scott worked as a senior security consultant at Neohapsis and an adjunct professor at DePaul University. Scott's expertise lies in both building and breaking for application security at scale. As an avid coder and researcher, he has contributed to and released a number of open source tools for both attack and defense. Scott has presented security research at DEF CON , DerbyCon, OWASP AppSec USA, Shmoocon, Shakacon, Security Forum Hagenberg, Security B-sides Chicago, and others.

@helloarbit

#defcon25/by_track/track3/friday

#defcon25/By_Day/_Friday

1300 - Teaching Old Shellcode New Tricks

Friday at 13:00 in Track 2

45 minutes | Demo

Josh Pitts*Hacker*

Metasploit x86 shellcode has been defeated by EMET and other techniques not only in exploit payloads but through using those payloads in non-exploit situations (e.g. binary payload generation, PowerShell deployment, etc..). This talk describes taking Metasploit payloads (minus Stephen Fewer's hash API), incorporating techniques to bypass Caller/ EAF[+] checks (post ASLR/DEP bypass) and merging those techniques together with automation to make something better.

Josh Pitts

Josh Pitts has over 15 years experience conducting physical and IT security assessments, IT security operations support, penetration testing, malware analysis, reverse engineering and forensics. Josh has worked in US Government contracting, commercial consulting, and silicon valley startups. He likes to write code that patches code with other code via The Backdoor Factory (BDF), has co-authored an open-source environmental keying framework (EBOWLA), and once served in the US Marines.

@midnite_runr

#defcon25/by_track/track2/friday

#defcon25/By_Day/_Friday

1400 - Breaking the x86 Instruction Set

Friday at 14:00 in Track 3

45 minutes | Demo, Tool

Christopher Domas*Security Researcher, Battelle Memorial Institute*

A processor is not a trusted black box for running code; on the contrary, modern x86 chips are packed full of secret instructions and hardware bugs. In this talk, we'll demonstrate how page fault analysis and some creative processor fuzzing can be used to exhaustively search the x86 instruction set and uncover the secrets buried in your chipset. We'll disclose new x86 hardware glitches, previously unknown machine instructions, ubiquitous software bugs, and flaws in enterprise hypervisors. Best of all, we'll release our sandsifter toolset, so that you can audit - and break - your own processor.

Christopher Domas

Christopher Domas is a cyber security researcher and embedded systems engineer, currently investigating low level processor exploitation. He is best known for releasing impractical solutions to non-existent problems, including the world's first single instruction C compiler (M/o/Vfuscator), toolchains for generating images in program control flow graphs (REpsych), and Turing-machines in the vi text editor. His more relevant work includes the binary visualization tool ..cantor.dust.. and the memory sinkhole x86 privilege escalation exploit.

@xoreaxeaxeax

#defcon25/by_track/track3/friday

#defcon25/By_Day/_Friday

1400 - Death By 1000 Installers; on macOS, it's all broken!

Friday at 14:00 in Track 2

45 minutes | Demo, Exploit

Patrick Wardle*Chief Security Researcher, Synack*

Ever get an uneasy feeling when an installer asks for your password? Well, your gut was right! The majority of macOS installers & updaters are vulnerable to a wide range of priv-esc attacks.

It began with the discovery that Apple's OS updater could be abused to bypass SIP (CVE-2017-6974). Next, turns out Apple's core installer app may be subverted to load unsigned dylibs which may elevate privileges to root.

And what about 3rd-party installers? I looked at what's installed on my Mac, and ahhh, so many bugs!

Firewall, Little Snitch: EoP via race condition of insecure plist

Anti-Virus, Sophos: EoP via hijack of binary component

Browser, Google Chrome: EoP via script hijack

Virtualization, VMWare Fusion: EoP via race condition of insecure script

IoT, DropCam: EoP via hijack of binary component

and more!

...and 3rd-party auto-update frameworks like Sparkle -yup vulnerable too!

Though root is great, we can't bypass SIP nor load unsigned kexts. However with root, I discovered one could now trigger a ring-0 heap-overflow that provides complete system control.

Though the talk will discuss a variety of discovery mechanisms, 0days, and macOS exploitation techniques, it won't be all doom & gloom. We'll end by discussing ways to perform authorized installs/upgrades that don't undermine system security."

Patrick Wardle

Patrick Wardle is the Chief Security Researcher at Synack, and founder of Objective-See. Having worked at NASA and the NSA, and as well as presented at many security conferences, he is intimately familiar with aliens, spies, and talking nerdy. Currently, Patrick's focus is on automated vulnerability discovery, and the emerging threats of OS X and mobile malware. In his personal time, Patrick collects OS X malware and writes free OS X security tools.

@patrickwardle, objective-see.com

[#defcon25/by_track/track2/friday](#)

[#defcon25/By_Day/_Friday](#)

1400 - How we created the first SHA-1 collision and what it means for hash security

Friday at 14:00 in Track 4

45 minutes | Demo, Tool

Elie Bursztein*Anti-abuse research lead, Google*

In February 2017, we announced the first SHA-1 collision. This collision combined with a clever use of the PDF format allows attackers to forge PDF pairs that have identical SHA-1 hashes and yet display different content. This attack is the result of over two years of intense research. It took 6500 CPU years and 110 GPU years of computations which is still 100,000 times faster than a brute-force attack.


In this talk, we recount how we found the first SHA-1 collision. We delve into the challenges we faced from developing a meaningful payload, to scaling the computation to that massive scale, to solving unexpected cryptanalytic challenges that occurred during this endeavor.

We discuss the aftermath of the release including the positive changes it brought and its unforeseen consequences. For example it was discovered that SVN is vulnerable to SHA-1 collision attacks only after the WebKit SVN repository was brought down by the commit of a unit-test aimed at verifying that Webkit is immune to collision attacks.

Building on the Github and Gmail examples we explain how to use counter-cryptanalysis to mitigate the risk of a collision attacks against software that has yet to move away from SHA-1. Finally we look at the next generation of hash functions and what the future of hash security holds

Elie Bursztein

Elie Bursztein leads Google's anti-abuse research, which helps protect users against Internet threats. Elie has contributed to applied-cryptography, machine learning for security, malware understanding, and web security; authoring over fifty research papers in the field. Most recently he was involved in finding the first SHA-1 collision.

Elie is a beret aficionado, tweets at @elie, and performs magic tricks in his spare time. Born in Paris, he received a Ph.D from ENS-cachan in 2008 before working at Stanford University and ultimately joining Google in 2011. He now lives with his wife in  Mountain View, California.

@elie

#defcon25/by_track/track4/Friday

#defcon25/By_Day/_Friday

1400 - Using GPS Spoofing to control time

Friday at 14:00 in 101 Track

45 minutes | Tool

David "Karit" Robinson*Security Consultant, ZX Security*

GPS is central to a lot of the systems we deal with on a day-to-day basis. Be it Uber, Tinder, or aviation systems, all of them rely on GPS signals to receive their location and/or time.

GPS Spoofing is now a valid attack vector and can be done with minimal effort and cost. This raises some concerns when GPS is depended upon by safety of life applications. This presentation will look at the process for GPS and NMEA (the serial format that GPS receivers output) spoofing, how to detect the spoofing attacks and ways to manipulate the time on GPS synced NTP servers. We will also explore the implications when the accuracy of the time on your server can no longer be guaranteed.

David "Karit" Robinson

Dave/Karit has worked in the IT industry for over 10 years. In this time he has developed a skillset that encompasses various disciplines in the information security domain. Dave is currently part of team at ZX Security in Wellington and works as a penetration tester. Since joining ZX Security Dave has presented at Kiwicon, BSides Canberra and Unrestcon and also at numerous local meetups; along with running training at Kiwicon and Syscan. He has a keen interest in lock-picking and all things wireless.

@nzkarit

#defcon25/by_track/101/Friday

#defcon25/By_Day/_Friday

1500 - Abusing Certificate Transparency Logs

Friday at 15:00 in Track 4

45 minutes | Demo, Tool

Hanno Böck*Hacker and freelance journalist*

The Certificate Transparency system provides public logs of TLS certificates. While Certificate Transparency is primarily used to uncover security issues in certificates, its data is also valuable for other use cases. The talk will present a novel way of exploiting common web applications like Wordpress, Joomla or Typo3 with the help of Certificate Transparency.

Certificate Transparency has helped uncover various incidents in the past where certificate authorities have violated rules. It is probably one of the most important security improvements that has ever happened in the certificate authority ecosystem. In September 2017 Google will make Certificate Transparency mandatory for all new certificates. So it's a

good time to see how it could be abused by the bad guys.

Hanno Böck

Hanno Böck is a hacker and freelance journalist. He regularly covers IT security issues for the German IT news site [Golem.de](#) and publishes the monthly Bulletproof TLS Newsletter. He also runs the Fuzzing Project, an effort to improve the security of free and open source software supported by the Linux Foundation's Core Infrastructure Initiative.

@hanno

#defcon25/by_track/track4/Friday

#defcon25/By_Day/_Friday

1500 - Assembly Language is Too High Level

Friday at 15:00 in 101 Track

45 minutes | Demo, Tool, Exploit

XlogicX*Machine Hacker*

Do you have a collection of vulnerable programs that you have not yet been able to exploit? There may yet still be hope. This talk will show you how to look deeper (lower level). If you've ever heard experts say how x86 assembly language is just a one-to-one relationship to its machine-code, then we need to have a talk. This is that talk; gruesome detail on how an assembly instruction can have multiple valid representations in machine-code and vice versa. You can also just take my word for it, ignore the details like a bro, and use the tool that will be released for this talk: the Interactive Redundant Assembler (irasm). You can just copy the alternate machine code from the tool and use it in other tools like mona, use it to give yourself more options for self-modifying code, fork Hydan (stego) and give it more variety, or to create peace on earth.

XlogicX

XlogicX hacks at anything low level. He's unmasked sanitized IP addresses in packets (because checksums) and crafts his own pcaps with just xxd. He feeds complete garbage to forensic tools, AV products, decompression software, and intrusion detection systems. He made evil strings more evil (with automation) to exploit high consumption regular expressions. Lately he has been declaring war on assembly language (calling it too high-level) and doing all kinds of ignorant things with machine code. More information can be found on [xlogicx.net](#)

@XlogicX

1500 - Dark Data

Friday at 15:00 in Track 3

45 minutes

Svea Eckert*NDR*

Andreas Dewes*PhD*

A judge with preferences for hard core porn, a police officer investigating a cyber-crime, a politician ordering burn out medication - this kind of very personal and private information is on the market. Get sold to who is willing to pay for.

In a long time experiment, with the help of some social engineering techniques, we were able to get our hands on the most private data you can find on the internet. Click stream data of three million German citizens. They contain every URL they have looked at, every second, every hour, every day for 31 days. In our talk we will not only show how we got that data, but how you can de-anonymize it with some simple techniques.

This data is collected worldwide by big companies, whose legal purpose is to sell analytics and insights for marketers and businesses. In the shadow of Google and Facebook, companies have evolved, their names unknown to a broader public but making billions of dollars with your data. The new oil of the 20th century.

Our experiment shows in a drastic way, what the youngest decision reversing the Broadband Privacy Rule means. What the consequences for everyday life could be, when ISPs are allowed to sell your browsing data. And why that piece of regulation from the FCC was so important regarding privacy and constitutional rights.

Svea Eckert

Svea Eckert works as a freelance journalist for Germany's main public service broadcaster "Das Erste" (ARD). She is researching and reporting investigative issues for the PrimeTime news shows and high quality documentaries. Her main focus lies on new technology: computer and network security, digital economics and data protection.

Bigger projects and documentaries are for example "Superpower Wikileaks?" (ARD), "Facebook - Billion Dollar Business friendship" (ARD), her first book "Monitored and spied out: Prism, NSA, Facebook & Co" and in 2015 "Netwars" (ARD). Svea Eckert studied

"Journalism and Communications" and Economics in Hamburg. She completed her journalistic training at NDR, Hamburg and Hannover.

Twitter: @sveckert

Website: www.sveaeckert.de

Andreas Dewes

Andreas Dewes is a trained physicist with a PhD in experimental quantum computing and a degree in quantitative economics. He has a passion for data analysis and software development. He has received numerous awards for his work on data analysis and his work on data privacy and big data has been featured in the national and international press.

Twitter: @japh44

Github: adewes

#defcon25/by_track/track3/friday

#defcon25/By_Day/_Friday

1500 - Phone system testing and other fun tricks

Friday at 15:00 in Track 2

45 minutes | Demo, Tool

"Snide" Owen*Hacker*

Phone systems have been long forgotten in favor of more modern technology. The phreakers of the past left us a wealth of information, however while moving forward the environments as a whole have become more complex. As a result they are often forgotten, side tracked or neglected to be thoroughly tested. We'll cover the VoIP landscape, how to test the various components while focussing on PBX and IVR testing. The security issues that may be encountered are mapped to the relative OWASP category for familiarity. Moving on I'll demonstrate other fun ways that you can utilize a PBX within your future offensive endeavours.

"Snide" Owen

"Snide" Owen has worked in various IT fields from tech support to development. Combining that knowledge he moved into the security field by way of Application Security and is now on an offensive security research team. He enjoys both making and breaking, tinkering with various technologies, and has experimented for prolonged periods with PBX's and the obscure side of VoIP.

#defcon25/by_track/track2/friday

#defcon25/By_Day/_Friday

1600 - "Tick, Tick, Tick. Boom! You're Dead." – Tech & the FTC

Friday at 16:00 in Track 4

45 minutes

Whitney Merrill*Privacy, eCommerce & Consumer Protection Counsel, Electronic Arts*

Terrell McSweeney*Commissioner, Federal Trade Commission*

The Federal Trade Commission is a law enforcement agency tasked with protecting consumers from unfair and deceptive practices. Protecting consumers on the Internet and from bad tech is nothing new for the FTC. We will take a look back at what the FTC was doing when DEF CON first began in 1993, and what we've been doing since. We will discuss enforcement actions involving modem hijacking, FUD advertising, identity theft, and even introduce you to Dewie the e-Turtle. Looking forward, we will talk about the FTC's future protecting consumers' privacy and data security and what you can do to help.

Whitney Merrill

Whitney Merrill is a hacker, ex-fed, and lawyer. She's currently a privacy attorney at Electronic Arts (EA), and in her spare time, she runs the Crypto & Privacy Village (come say hi!). Recently, she served her country as an attorney at the Federal Trade Commission where she worked on a variety of consumer protection matters including data security, privacy, and deceptive marketing and advertising. Whitney received her J.D. and master's degree in Computer Science from the University of Illinois at Urbana-Champaign.

@wbm312

Terrell McSweeney

Terrell McSweeney serves as a Commissioner of the Federal Trade Commission. This year marks her fourth time at DEF CON . When it comes to tech issues, Commissioner McSweeney has focused on the valuable role researchers and hackers can play protecting consumer data security and privacy. She opposes bad policy and legislative proposals like mandatory backdoors and the criminalization of hacking and believes that enforcers like the FTC should work with the researcher community to protect consumers. She wants companies to implement security by design, privacy by design and data ethics design - but recognizes that, in the absence of regulation, enforcement and research are the only means of holding companies accountable for the choices they make in the ways that they hold and use consumer data.

1600 - An ACE Up the Sleeve: Designing Active Directory DACL Backdoors

Friday at 16:00 in Track 3

45 minutes | Demo

Andy Robbins*Red Team Lead*

Will Schroeder*Offensive Engineer*

Active Directory (AD) object discretionary access control lists (DACLS) are an untapped offensive landscape, often overlooked by attackers and defenders alike. The control relationships between AD objects align perfectly with the "attackers think in graphs" philosophy and expose an entire class of previously unseen control edges, dramatically expanding the number of paths to complete domain compromise.

While DACL misconfigurations can provide numerous paths that facilitate elevation of domain rights, they also present a unique chance to covertly deploy Active Directory persistence. It's often difficult to determine whether a specific AD DACL misconfiguration was set intentionally or implemented by accident. This makes Active Directory DACL backdoors an excellent persistence opportunity: minimal forensic footprint, and maximum plausible deniability.

This talk will cover Active Directory DACLS in depth, our "misconfiguration taxonomy", and enumeration/analysis with BloodHound's newly released feature set. We will cover the abuse of AD DACL misconfigurations for the purpose of domain rights elevation, including common misconfigurations encountered in the wild. We will then cover methods to design AD DACL backdoors, including ways to evade current detections, and will conclude with defensive mitigation/detection techniques for everything described.

Andy Robbins

As a Red Team lead, Andy Robbins has performed penetration tests and red team assessments for a number of Fortune 100 commercial clients, as well as federal and state agencies. Andy presented his research on a critical flaw in the ACH payment processing standard in 2014 at DerbyCon and the ISC2 World Congress, and has spoken at other conferences including DEF CON , BSidesLV, ekoparty, ISSA International, and Paranoia Conf

in Oslo. He has a passion for offensive development and red team tradecraft, and helps to develop and teach the "Adaptive Red Team Tactics" course at BlackHat USA.

@_wald0

Will Schroeder

Will Schroeder is a offensive engineer and red teamer. He is a co-founder of Empire/Empyre, BloodHound, and the Veil-Framework, developed PowerView and PowerUp, is an active developer on the PowerSploit project, and is a Microsoft PowerShell MVP. He has presented at a number of conferences, including DEF CON , DerbyCon, Troopers, BlueHat Israel, and various Security BSides.

@harmj0y

#defcon25/by_track/track3/friday

#defcon25/By_Day/_Friday

1600 - Radio Exploitation 101: Characterizing, Contextualizing, and Applying Wireless Attack Methods

Friday at 16:00 in 101 Track

45 minutes | Demo

Matt Knight*Senior Software Engineer, Threat Research at Bastille*

Marc Newlin*Security Researcher at Bastille*

What do the Dallas tornado siren attack, hacked electric skateboards, and insecure smart door locks have in common? Vulnerable wireless protocols. Exploitation of wireless devices is growing increasingly common, thanks to the proliferation of radio frequency protocols driven by mobile and IoT. While non-Wi-Fi and non-Bluetooth RF protocols remain a mystery to many security practitioners, exploiting them is easier than one might think.

Join us as we walk through the fundamentals of radio exploitation. After introducing essential RF concepts and characteristics, we will develop a wireless threat taxonomy by analyzing and classifying different methods of attack. As we introduce each new attack, we will draw parallels to similar wired network exploits, and highlight attack primitives that are unique to RF. To illustrate these concepts, we will show each attack in practice with a series of live demos built on software-defined and hardware radios.

Attendees will come away from this session with an understanding of the mechanics of

wireless network exploitation, and an awareness of how they can bridge their IP network exploitation skills to the wireless domain.

Matt Knight

Matt Knight is a software engineer and applied security researcher at Bastille, with a background in hardware, software, and wireless security. Matt's research focuses on preventing exploitation of the myriad wireless networking technologies that connect embedded devices to the Internet of Things. Notably, in 2016 he exposed the internals of the closed-source LoRa PHY based on blind signal analysis. Matt holds a BE in Electrical Engineering from Dartmouth College.

@embeddedsec

Marc Newlin

Marc Newlin 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.

@marcnewlin

#defcon25/by_track/101/Friday

#defcon25/By_Day/_Friday

1600 - The Adventures of AV and the Leaky Sandbox

Friday at 16:00 in Track 2

45 minutes | Demo, Tool

Itzik Kotler*Co-Founder & CTO, SafeBreach*

Amit Klein*VP Security Research, SafeBreach*

Everyone loves cloud-AV. Why not harness the wisdom of clouds to protect the enterprise? Consider a high-security enterprise with strict egress filtering - endpoints have no direct Internet connection, or the endpoints' connection to the Internet is restricted to hosts used by their legitimately installed software. Let's say there's malware running on an endpoint with full privileges. The malware still can't exfiltrate data due to the strict egress filtering.

Now let's also assume that this enterprise uses cloud-enhanced anti-virus (AV). You'd argue that if malware is already running on the endpoint with full privileges, then an AV agent can't

degrade the security of the endpoint. And you'd be completely wrong.

In this presentation, we describe and demonstrate a novel technique for exfiltrating data from highly secure enterprises which employ strict egress filtering. Assuming the endpoint has a cloud-enhanced antivirus installed, we show that if the AV employs an Internet-connected sandbox in its cloud, it in fact facilitates such exfiltration. We release a tool implementing the exfiltration technique, and provide real-world results from several prominent AV products. We also provide insights on AV in-the-cloud sandboxes. Finally we address the issues of how to further enhance the attack, and possible mitigations.

Itzik Kotler

Itzik Kotler is CTO and Co-Founder of SafeBreach. Itzik has more than a decade of experience researching and working in the computer security space. He is a recognized industry speaker, having spoken at DEF CON, Black Hat USA, Hack In The Box, RSA, CCC and H2HC. Prior to founding SafeBreach, Itzik served as CTO at Security-Art, an information security consulting firm, and before that he was SOC Team Leader at Radware. (NASDAQ: RDWR).

@itzikkotler

www.ikotler.org

Amit Klein

Amit Klein is a world renowned information security expert, with 26 years in information security and over 30 published technical papers on this topic. Amit is VP Security Research at SafeBreach, responsible for researching various infiltration, exfiltration and lateral movement attacks. Before SafeBreach, Amit was CTO for Trusteer (acquired by IBM) for 8.5 years. Prior to Trusteer, Amit was chief scientist for Cyota (acquired by RSA) for 2 years, and prior to that, director of Security and Research for Sanctum (acquired by Watchfire, now part of IBM security division) for 7 years. Amit has a B.Sc. from the Hebrew University in Mathematics and Physics (magna cum laude, Talpiot program), recognized by InfoWorld as a CTO of the year 2010, and has presented at BlackHat USA, HITB, RSA USA, OWASP, CertConf, BlueHat, CyberTech, APWG and AusCERT.

www.securitygalore.com

#defcon25/by_track/track2/friday

#defcon25/By_Day/_Friday

1700 - Cisco Catalyst Exploitation

Friday at 17:00 in 101 Track

45 minutes | Demo

Artem Kondratenko*Penetration Tester, Security Researcher*

On March 17th, Cisco Systems Inc. made a public announcement that over 300 of the switches it manufactures are prone to a critical vulnerability that allows a potential attacker to take full control of the network equipment.

This damaging public announcement was preceded by Wikileaks' publication of documents codenamed as "Vault 7" which contained information on vulnerabilities and description of tools needed to access phones, network equipment and even IOT devices.

Cisco Systems Inc. had a huge task in front of them - patching this vast amount of different switch models is not an easy task. The remediation for this vulnerability was available with the initial advisory and patched versions of IOS software were announced on May 8th 2017.

We all heard about modern exploit mitigation techniques such as Data Execution Prevention, Layout Randomization. But just how hardened is the network equipment? And how hard is it to find critical vulnerabilities?

To answer that question I decided to reproduce the steps necessary to create a fully working tool to get remote code execution on Cisco switches mentioned in the public announcement.

This presentation is a detailed write-up of the exploit development process for the vulnerability in Cisco Cluster Management Protocol that allows a full takeover of the device.

Artem Kondratenko

Artem is a Penetration Tester at Kaspersky Lab. On time between red team engagements he is doing security research of software and hardware appliances. Author of multiple CVE's on VMware Virtualization Platforms (CVE-2016-5331, CVE-2016-7458, CVE-2016-7459, CVE-2016-7460). Enjoys contributing to the community by writing penetration testing tools such as Invoke-Vnc (PowerShell vnc injector, part of CrackMapExec) and Rpivot (reverse socks4 proxy, now part of BlackArch Linux Distro).

@artkond, <https://github.com/artkond>,
<https://artkond.com>

#defcon25/by_track/101/Friday

#defcon25/By_Day/_Friday

1700 - MEATPISTOL, A Modular Malware Implant Framework

Friday at 17:00 in Track 3

45 minutes | Demo, Tool

FuzzyNop (Josh Schwartz)*Director of Offensive Security @ Salesforce*

ceyx (John Cramb)*Hacker*

Attention Red Teamers, Penetration Testers, and Offensive Security Operators, isn't the overhead of fighting attribution, spinning up infrastructure, and having to constantly re-write malware an absolute pain and timesink!?! It was for us too, so we're fixing that for good (well, maybe for evil). Join us for the public unveiling and open source release of our latest project, MEATPISTOL, a modular malware framework for implant creation, infrastructure automation, and shell interaction. This framework is designed to meet the needs of offensive security operators requiring rapid configuration and creation of long lived malware implants and associated command and control infrastructure. Say goodbye to writing janky one-off malware and say hello to building upon a framework designed to support efficient yoloscoped adversarial campaigns against capable targets.

FuzzyNop (Josh Schwartz) & ceyx (John Cramb)

FuzzyNop and ceyx were raised by computerized wolves with a penchant for fine art and rum based cocktails. While technically from different mothers and also sides of the world, they formed the first cyber wolf brotherhood shell-bent to ameliorate the state of targeted malware implants to support the ongoing war against the institutionalized mediocrity of the corporate shadow government. Working in tandem with dolphin researchers funded by the oligarch llamas they have found a way to synthesize powdered ethanol into mechanical pony fuel. Leading Offensive Security functions at Salesforce is merely a front to confuse the saurian overlords of their true purpose yet to be revealed...

[#defcon25/by_track/track3/friday](#)

[#defcon25/By_Day/_Friday](#)

1700 - Panel: DEF CON Groups

Friday at 17:00 in Track 2

45 minutes | Audience Participation

Jeff Moss (Dark Tangent)*Founder, DEF CON*

Waz*DCG*

Brent White (B1TKILL3R)*DCG and DC615*

Jayson E. Street*DCG Ambassador*

Grifter*DC801*

Jun Li*DC010*

S0ups*DC225*

Major Malfunction*DC4420*

Do you love DEF CON? Do you hate having to wait for it all year? Well, thanks to DEF CON groups, you're able to carry the spirit of DEF CON with you year round, and with local people, transcending borders, languages, and anything else that may separate us!

In this talk, you'll hear from DEF CON's founder, Dark Tangent, who is also moderating the panel. Jayson E. Street, the Ambassador of DEF CON groups will also discuss updates about the program and share information from his global travel to help start groups around the world. We will also discuss what DEF CON groups are, how to get involved, as well as ideas for how to run a group, location ideas, and how to spread the word.

Founders of their own local DEF CON groups will also discuss the awesome projects of their groups, as well as projects from other groups, to give ideas to take back to your own DEF CON group. Projects we'll discuss range from custom badge build, IoT devices, vintage gaming systems, custom built routers, smarthome devices and more!

Jeff Moss (Dark Tangent)

Bio Coming soon.

Waz

Bio Coming soon.

Brent White (B1TKILL3R)

Bio Coming soon.

Jayson E. Street

Bio Coming soon.

Grifter

Bio Coming soon.

Jun Li

Bio Coming soon.

S0ups

Bio Coming soon.

Major Malfunction

Bio Coming soon.

#defcon25/by_track/track2/friday

#defcon25/By_Day/_Friday

1700 - The Internet Already Knows I'm Pregnant

Friday at 17:00 in Track 4

45 minutes | Exploit

Cooper Quintin*Staff Technologist - EFF*

Kashmir Hill *Journalist - Gizmodo Media*

Women's health is big business. There are a staggering number of applications for Android to help people keep track of their monthly cycle, know when they may be fertile, or track the status of their pregnancy. These apps entice the user to input the most intimate details of their lives, such as their mood, sexual activity, physical activity, physical symptoms, height, weight, and more. But how private are these apps, and how secure are they really? After all, if an app has such intimate details about our private lives it would make sense to ensure that it is not sharing those details with anyone such as another company or an abusive partner/parent. To this end EFF and Journalist Kashmir Hill have taken a look at some of the privacy and security properties of over a dozen different fertility and pregnancy tracking apps. Through our research we have uncovered several privacy issues in many of the applications as well as some notable security flaws as well as a couple of interesting security features.

Cooper Quintin

Cooperq is a security researcher and programmer at EFF. He has worked on projects such as Privacy Badger, Canary Watch, Ethersheet, and analysis of state sponsored malware. He has also performed security trainings for activists, non profit workers and ordinary folks around the world. He previously worked building websites for non-profits, such as Greenpeace, Adbusters, and the Chelsea Manning Support Network. He also was a co-founder of the Hackbloc hacktivist collective. In his spare time he enjoys playing music and participating in street protests.

@cooperq

Kashmir Hill

Kashmir Hill is a journalist who writes about privacy and security. She is a senior reporter at Gizmodo Media and has previously written for Fusion, Forbes Magazine and Above The Law.

@kashhill

2000 - Friday - Hacking Democracy

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

Evening Lounge

Mr. Sean Kanuck*Stanford University, Center for International Security and Cooperation*


Are you curious about the impact of fake news and influence operations on elections? Are you concerned about the vulnerability of democratic institutions, the media, and civil society? Then come engage with your peers and the first US National Intelligence Officer for Cyber Issues on ways to hack democracy. He will: (1) provide a low-tech, strategic analysis of recent events, foreign intelligence threats, and the future of information warfare; (2) lead a Socratic dialogue with attendees about the trade-offs between national security and core democratic values (such as freedom, equality, and privacy); and (3) open the floor to audience questions and/or a moderated group debate.

This session is intended to be informal and participatory. It will cover a range of issues from supply chain attacks on voting machines to psychological operations by using an interdisciplinary approach that encompasses constitutional law, world history, game theory, social engineering, and international affairs. The discussion will occur against the backdrop of cyber security and critical infrastructure protection, but it will not examine any specific hardware or software systems; rather, it will concern the conceptual formulation and conduct of modern strategic influence campaigns. No specific knowledge is required, but a skeptical mind and mischievous intellect are a must.

Mr. Sean Kanuck

Sean Kanuck is an attorney and strategic consultant who advises governments, corporations, and entrepreneurs on the future of information technology. Sean is affiliated with Stanford University's Center for International Security and Cooperation and has received several international appointments, including: Chair of the Research Advisory Group for the Global Commission on the Stability of Cyberspace (Hague, Netherlands), Distinguished Visiting Fellow at Nanyang Technological University (Singapore), and Distinguished Fellow with the Observer Research Foundation (New Delhi, India). He regularly gives keynote addresses for global audiences on a variety of cyber topics, ranging from risk analysis to identity intelligence to arms control.

Sean served as the United States' first National Intelligence Officer for Cyber Issues from 2011 to 2016. He came to the National Intelligence Council after a decade of experience in the Central Intelligence Agency's Information Operations Center, including both analytic and field assignments. In his Senior Analytic Service role, he was a contributing author for the 2009 White House Cyberspace Policy Review, an Intelligence Fellow with the Directorates for Cybersecurity and Combating Terrorism at the National Security Council, and a member of the United States delegation to the United Nations Group of Governmental Experts on international information security.

Prior to government service, Sean practiced law with Skadden Arps in New York, where he specialized in mergers and acquisitions, corporate finance, and banking matters. He is admitted to the bar in New York and  Washington DC, and his academic publications focus on information warfare and international law. Sean holds degrees from Harvard University (A.B., J.D.), the London School of Economics (M.Sc.), and the University of Oslo (LL.M.). He also proudly serves as a Trustee of the Center for Excellence in Education, a charity promoting STEM education that is based in McLean, Virginia.

@seankanuck

#defcon25/eveninglounges

#defcon25/By_Day/_Friday

2000 - Friday - Horror stories of a translator and how a tweet can start a war with less than 140 characters

Friday at 20:00 - 22:00 in Modena

Evening Lounge

El Kentaro*Hacker*

Translators are invisible, when they are present it is assumed that they know the language and are accurately translating between the languages. But how do you assure that the translator is accurately translating or working without an agenda? Although many of the case studies presented in this talk will focus on translating between different languages, the basic premise can be applied in any case where information needs to be shared among 2 or more different contexts. (i.e.: Sales vs Engineering, Government vs Private sector etc) . The talk will showcase publicly known historical cases and personal experiences where translation errors (accidental and deliberate) have lead to misunderstandings some with dire consequences. Also the talk will showcase using translators as an offensive tool (i.e.:How to create more credible fake news). We as a society consume more information and consume it faster than before, we have

to be aware of the dangers that are inherit with bad translations. Also the infosec/cyber security profession because of the potential for large scale global impacts and or the need to maintain operational security poses unique considerations when translating or using a translator. This talk will highlight the unique challenges of using a translator or translations in such environments.

El Kentaro

El Kentaro / That Guy in Tokyo.

El Kentaro has been a communications facilitator between Japan and the rest of the world in the information technology industry since 1996. For the last 7 years Kentaro has solely focused on providing interpretation services for the infosec/cyber security industry in Japan. Kentaro also provided the Japanese subtitles for the DEF CON documentary released in 2015 and is a member of the CODE BLUE Security Conference held annually in Japan.

[#defcon25/eveninglounges](#)

[#defcon25/By_Day/_Friday](#)

2000 - Friday - Panel - An Evening with the EFF

Friday at 20:00 - 22:00 in Trevi Room

Evening Lounge | 0025

Kurt Opsahl*Deputy Executive Director & General Counsel, Electronic Frontier Foundation*

Nate Cardozo*EFF Senior Staff Attorney*

Eva Galperin*EFF Director of Cyber security*

Andrew Crocker*EFF Staff Attorney*

Kit Walsh*EFF Staff Attorney*

Relax and enjoy in an evening lounge while you get the latest information about how the law is racing to catch up with technological change from staffers at the Electronic Frontier Foundation, the nation's premiere digital civil liberties group fighting for freedom and privacy in the computer age. This Evening Lounge discussion will include updates on current EFF issues such as surveillance online, encryption (and backdoors), and fighting efforts to use intellectual property claims to shut down free speech and halt innovation, discussion of our technology project to protect privacy and speech online, updates on cases and legislation

affecting security research, and much more.

Kurt Opsahl

KURT OPSAHL is the Deputy Executive Director and General Counsel of the Electronic Frontier Foundation. In addition to representing clients on civil liberties, free speech and privacy law, Opsahl counsels on EFF projects and initiatives. Opsahl is the lead attorney on the Coders' Rights Project. Before joining EFF, Opsahl worked at Perkins Coie, where he represented technology clients with respect to intellectual property, privacy, defamation, and other online liability matters, including working on *Kelly v. Arribasoft*, *MGM v. Grokster* and *CoStar v. LoopNet*. For his work responding to government subpoenas, Opsahl is proud to have been called a "rabid dog" by the Department of Justice. Prior to Perkins, Opsahl was a research fellow to Professor Pamela Samuelson at the U.C. Berkeley School of Information Management & Systems. Opsahl received his law degree from Boalt Hall, and undergraduate degree from U.C. Santa Cruz. Opsahl co-authored "Electronic Media and Privacy Law Handbook." In 2007, Opsahl was named as one of the "Attorneys of the Year" by California Lawyer magazine for his work on the *O'Grady v. Superior Court* appeal. In 2014, Opsahl was elected to the USENIX Board of Directors.

@kurtopsahl, @eff

Nate Cardozo

NATE CARDOZO is a Senior Staff Attorney on the Electronic Frontier Foundation's digital civil liberties team. In addition to his focus on free speech and privacy litigation, Nate works on EFF's Who Has Your Back? report and Coders' Rights Project. Nate has projects involving cryptography and the law, automotive privacy, government transparency, hardware hacking rights, anonymous speech, electronic privacy law reform, Freedom of Information Act litigation, and resisting the expansion of the surveillance state. A 2009-2010 EFF Open Government Legal Fellow, Nate spent two years in private practice before returning to his senses and to EFF in 2012. Nate has a B.A. in Anthropology and Politics from U.C. Santa Cruz and a J.D. from U.C. Hastings where he has taught first-year legal writing and moot court. He brews his own beer, has been to India four times, and watches too much Bollywood.

Eva Galperin

EVA GALPERIN is EFF's Director of Cybersecurity. Prior to 2007, when she came to work for EFF, Eva worked in security and IT in Silicon Valley and earned degrees in Political Science and International Relations from SFSU. Her work is primarily focused on providing privacy and security for vulnerable populations around the world. To that end, she has applied the combination of her political science and technical background to everything from organizing EFF's Tor Relay Challenge, to writing privacy and security training materials (including Surveillance Self Defense and the Digital First Aid Kit), and publishing research on malware in Syria, Vietnam, Kazakhstan. When she is not collecting new and exotic malware, she practices aerial circus arts and learning new languages.

Andrew Crocker

ANDREW CROCKER is a staff attorney on the Electronic Frontier Foundation's civil liberties team. He focuses on EFF's national security and privacy docket, as well as the Coders' Rights Project. While in law school, Andrew worked at the Berkman Center for Internet and Society, the American Civil Liberties Union's Speech, Privacy, and Technology Project, and the Center for Democracy and Technology. He received his undergraduate and law degrees from Harvard University and an M.F.A. in creative writing from New York University. His interests include Boggle and donuts.

Kit Walsh

KIT WALSH is a staff attorney at EFF, working on free speech, net neutrality, copyright, coders' rights, and other issues that relate to freedom of expression and access to knowledge. She has worked for years to support the rights of political protesters, journalists, remix artists, and technologists to agitate for social change and to express themselves through their stories and ideas. Prior to joining EFF, Kit led the civil liberties and patent practice areas at the Cyberlaw Clinic, part of Harvard's Berkman Center for Internet and Society, and previously Kit worked at the law firm of Wolf, Greenfield & Sacks, litigating patent, trademark, and copyright cases in courts across the country. Kit holds a J.D. from Harvard Law School and a B.S. in neuroscience from MIT, where she studied brain-computer interfaces and designed cyborgs and artificial bacteria.

[#defcon25/eveninglounges](#)

[#defcon25/By_Day/_Friday](#)