

SPEAKING SCHEDULE

FIRESIDE HAX

-THURSDAY-

FRIDAY

OH NOES! A ROLE PLAYING INCIDENT RESPONSE GAME

20:00-22:00 in Roman Chillout

Bruce Potter & Robert Potter

DO NO H4RM: A HEALTHCARE SECURITY CONVERSATION

20:00-22:00 in Octavius 9

Christian "quaddi" Dameff MD & Jeff "r3plicat" Tully MD

DISRUPTING THE DIGITAL DYSTOPIA OR WHAT THE HELL IS HAPPENING IN COMPUTER LAW

20:00-22:00 in Octavius 13

Nathan White & Nate Cardozo

SATURDAY

EFF FIRESIDE HAX (AKA ASK THE EFF)

20:00-22:00 in Roman Chillout

BEYOND THE LULZ: BLACK-HAT TROLLING, WHITE-HAT TROLLING, AND HACKING THE ATTENTION LANDSCAPE

20:00-22:00 in Octavius 9

Matt Goerzen & Jeanna Matthews

PRIVACY IS EQUALITY: AND IT'S FAR FROM DEAD

20:00-22:00 in Octavius 13

Sarah St.Vincent

101 Track	
10:00	ThinSIM-based Attacks on Mobile Money Systems Rowan Phipps
11:00	Pwning "the toughest target": the exploit chain of winning the largest bug bounty in the history of ASR program Guang Gong
12:00	Ring 0/2 Rootkits: bypassing defenses Alexandre Borges
13:00	A Journey Into Hexagon: Dissecting a Qualcomm Baseband Seamus Burke
14:00	Wagging The Tail - Covert Passive Surveillance And How To Make Their Life Difficult Si & Agent X
15:00	Building the Hacker Tracker Whitney Champion & Seth Law
15:30	DC 101 PANEL (Until 16:45)

-FRIDAY-

	DEF CON 101	Track 1	Track 2	Track 3
10:00	Synfuzz: Building a Grammar Based Re-targetable Test Generation Framework Joe Rozner	Badge/DT Welcome	De-anonymizing Programmers from Source Code and Binaries Rachel Greenstadt & Dr. Aylin Caliskan	Securing our Nation's Election Infrastructure Jeanette Manfra
10:30				Please do not Duplicate: Attacking the Knox Box and other keyed alike systems m010ch_
11:00	An Attacker Looks at Docker: Approaching Multi-Container Applications Wesley McGrew	NSA Talks Cybersecurity Rob Joyce	One-liners to Rule Them All Egypt	Lora Smart Water Meter Security Analysis Yingtao Zeng
12:00	It's Assembler, Jim, but not as we know it: (ab) using binaries from embedded devices for fun and profit Morgan "indrora" Gangwere	Vulnerable Out of the Box: An Evaluation of Android Carrier Devices Ryan Johnson	Breaking Paser Logic: Take Your Path Normalization Off and Pop 0days Out! Orange Tsai	Who Controls the Controllers - Hacking Crestron IoT Automation Systems Ricky "HeadlessZeke" Lawshae
13:00	Dissecting the Teddy Ruxpin: Reverse Engineering the Smart Bear Zenofex	Compromising online accounts by cracking voicemail systems Martin Vigo	Finding Xori: Malware Analysis Triage with Automated Disassembly Amanda Rousseau & Rich Seymour	One-Click to OWA William Martin
13:30	You can run, but you can't hide. Reverse engineering using X-Ray. George Tarnovsky	Dragnet - Your Social Engineering Sidekick Truman Kain	Attacking the Brain: Customize Evil Protocol to Pwn an SDN Controller Feng Xiao	Fasten your seatbelts: We are escaping iOS 11 sandbox! Min Zheng
14:00	UEFI exploitation for the masses Mickey Shkatov	GOD MODE UNLOCKED - hardware backdoors in x86 CPUs Christopher Domas	4G - Who is paying your cellular phone bill? Dr. Silke Holtmanns & Isha Singh	Revolting Radios Michael Ossmann & Dominic Spill
15:00	Weaponizing Unicode: Homographs Beyond IDNs The Tarquin	Bypassing Port-Security In 2018: Defeating MacSEC and 802.1x-2010 Gabriel Ryan	Playback: a TLS 1.3 story Alfonso Garcia Alguacil & Alejo Murillo	Privacy infrastructure, challenges and opportunities yawnbox
16:00	Automated Discovery of Deserialization Gadget Chains Ian Haken	Your Peripheral Has Planted Malware - An Exploit of NXP SOCs Vulnerability Yuwei Zheng	Practical & Improved Wifi MitM with Mana Singe	Your Voice is My Passport _delta_zero
17:00	Your Bank's Digital Side Door Steven Danneman	I'll See Your Missile and Raise You A MIRV: An overview of the Genesis Scripting Engine Alex Levinson	Panel - The L0pht Testimony, 20 Years Later (and Other Things You Were Afraid to Ask)	Reverse Engineering, hacking documentary series Michael Lee Nirenberg

-SATURDAY-

	DEF CON 101	Track 1	Track 2	Track 3
10:00	<p>Through the Eyes of the Attacker: Designing Embedded Systems Exploits for Industrial Control Systems</p> <p>Marina Krotofil</p>	<p>It WISN't me, attacking industrial wireless mesh networks</p> <p>Erwin Paternotte</p>	<p>You're just complaining because you're guilty: A Guide for Citizens and Hackers to Adversarial Testing of Software Used In the Criminal Justice System</p> <p>Jeanna Matthews</p>	<p>You may have paid more than you imagine - Replay Attacks on Ethereum Smart Contracts</p> <p>Zhenxuan Bai</p>
11:00	<p>Hacking PLCs and Causing Havoc on Critical Infrastructures</p> <p>Thiago Alves</p>	<p>Exploiting Active Directory Administrator Insecurities</p> <p>Sean Metcalf</p>	<p>Compression Oracle Attacks on VPN Networks</p> <p>Nafeez</p>	<p>Jailbreaking the 3DS through 7 years of hardening</p> <p>smea</p>
12:00	<p>Building Absurd Christmas Light Shows</p> <p>Rob Joyce</p>	<p>Tineola: Taking a Bite Out of Enterprise Blockchain</p> <p>Stark Riedesel</p>	<p>You'd better secure your BLE devices or we'll kick your butts!</p> <p>Damien "virtualabs" Cauquil</p>	<p>Ridealong Adventures - Critical Issues with Police Body Cameras</p> <p>Josh Mitchell</p>
13:00	<p>One Step Ahead of Cheaters -- Instrumenting Android Emulators</p> <p>Nevermoe</p>	<p>In Soviet Russia Smart-card Hacks You</p> <p>Eric Sesterhenn</p>	<p>Reaping and breaking keys at scale: when crypto meets big data</p> <p>Yolan Romailier</p>	<p>Looking for the perfect signature: an automatic YARA rules generation algorithm in the AI-era</p> <p>Andrea Marcelli</p>
13:30	<p>House of Roman - a "leakless" heap fengshui to achieve RCE on PIE Binaries</p> <p>Sanat Sharma</p>	<p>The ring 0 façade: awakening the processor's inner demons</p> <p>Christopher Domas</p>	<p>Detecting Blue Team Research Through Targeted Ads</p> <p>0x200b</p>	<p>Infecting The Embedded Supply Chain</p> <p>Zach</p>
14:00	<p>Having fun with IoT: Reverse Engineering and Hacking of Xiaomi IoT Devices</p> <p>Dennis Giese</p>	<p>SMBetray - Backdooring and breaking signatures</p> <p>William Martin</p>	<p>Digital Leviathan: a comprehensive list of Nation-State Big Brothers (from huge to little ones)</p> <p>Eduardo Izycki</p>	<p>Playing Malware Injection with Exploit thoughts</p> <p>Sheng-Hao Ma</p>
14:30			<p>Sex Work After SESTA/FOSTA</p> <p>Maggie Mayhem</p>	<p>Fire & Ice: Making and Breaking macOS Firewalls</p> <p>Patrick Wardle</p>
15:00	<p>Project Interceptor: avoiding counter-drone systems with nanodrones</p> <p>David Melendez Cano</p>	<p>All your math are belong to us</p> <p>sghtoma</p>	<p>Reverse Engineering Windows Defender's Emulator</p> <p>Alexei Bulazel</p>	<p>Booby Trapping Boxes</p> <p>Ladar Levison</p>
16:00	<p>Outsmarting the Smart City</p> <p>Daniel "unicornFurnace" Crowley</p>	<p>80 to 0 in under 5 seconds: Falsifying a medical patient's vitals</p> <p>Douglas McKee</p>	<p>All your family secrets belong to us - Worrisome security issues in tracker apps</p> <p>Dr. Siegfried Rasthofer</p>	<p>Inside the Fake Science Factory</p> <p>Dr. Isabella Stein</p>
17:00	<p>CLOSED</p>	<p>The Road to Resilience: How Real Hacking Redeems this Damnable Profession</p> <p>Richard Thieme</p>	<p>Relocation Bonus: Attacking the Windows Loader Makes Analysts Switch Careers</p> <p>Nick Cano</p>	

SUNDAY

	DEF CON 101	Track 1	Track 2	Track 3
10:00	The Mouse is Mightier than the Sword Patrick Wardle	Rock appround the clock: Tracking malware developers by Android "AAPT" timezone disclosure bug. Sheila A. Berta & Sergio De Los Santos	Defending the 2018 Midterm Elections from Foreign Adversaries Joshua M Franklin	For the Love of Money: Finding and exploiting vulnerabilities in mobile point of sales systems Leigh-Anne Galloway
11:00	Searching for the Light: Adventures with OpticSpy Joe Grand (Kingpin)	Breaking Extreme Networks WingOS: How to own millions of devices running on Aircrafts, Government, Smart cities and more. Josep Pi Rodriguez	Politics and the Surveillance State. The story of a young politician's successful efforts to fight surveillance and pass the nation's strongest privacy bills. Daniel Zolnikov	Demystifying MS17-010: Reverse Engineering the ETERNAL Exploits zerosum0x0
12:00	Breaking Smart Speakers: We are Listening to You. Wu HuiYu	Last mile authentication problem: Exploiting the missing link in end-to-end secure communication Thanh Bui	Attacking the macOS Kernel Graphics Driver Yu Wang	Designing and Applying Extensible RF Fuzzing Tools to Expose PHY Layer Vulnerabilities Matt Knight
13:00	Trouble in the tubes: How internet routing security breaks down and how you can do it at home Lane Broadbent	Man-In-The-Disk Slava Makkaveev	Micro-Renovator: Bringing Processor Firmware up to Code Matt King	barcOwned - Popping shells with your cereal box Michael West
13:30		Asura: A huge PCAP file analyzer for anomaly packets detection using massive multithreading Ruo Ando	Lost and Found Certificates: dealing with residual certificates for pre-owned domains Ian Foster	Edge Side Include Injection: Abusing Caching Servers into SSRF and Transparent Session Hijacking Idionmarcil
14:00	Betrayed by the keyboard: How what you type can give you away Matt Wixey	Your Watch Can Watch You! Gear Up for the Broken Privilege Pitfalls in the Samsung Gear Smartwatch Dongsung Kim	Hacking BLE Bicycle Locks for Fun and a Small Profit Vincent Tan Kwang Yue	One bite and all your dreams will come true: Analyzing and Attacking Apple Kernel Drivers Xiaolong Bai & Min Zheng
15:00	Closed	Panel DCGroups	What the Fax!? Yaniv Balmas	Fuzzing Malware For Fun & Profit. Applying Coverage-guided Fuzzing to Find and Exploit Bugs in Modern Malware Maksim Shudrak
16:30	Closed	Closing Ceremonies	Closed	Closed
17:00				