DEF CON 101: The Panel

Mike Petruzzi (wiseacre), Senior Cyber Security Penetration Tester
Nikita Kronenberg, Not a Security Researcher, DEF CON
PushPin
Plug
Russ Rogers, Chief of Operations, DEF CON

DEF CON has changed for the better since the days at the Alexis Park. It has evolved from a few speaking tracks to an event that still offers the speakers, but also Villages, where you can get hands-on experience and Demo Labs where you can see tools in action. Of course, there is still the entertainment and Contest Area, as well as, Capture The Flag. There is so much more to DEF CON than there was in the past and it is our goal to help you get the best experience possible. In addition to introducing each of the different aspects and areas of DEF CON, we have a panel of speakers that will talk about how they came to be part of DEF CON and their personal experiences over the years.

Mike Petruzzi has been hacking managers for over 25 years. Mike is a Senior Cyber Security Penetration Testing Specialist working at various Federal Civil Agencies for the last 15 years. Yup, that's the title he was given. Naturally, he got all his IT experience as the result of selling beer, wine and liquor. He has tricked everyone into believing that he can do anything at all.

Twitter: @wiseacre_mike

Nikita works full time for DEF CON doing stuff, and things. She is DEF CON's administrator, director of the CFP review board, speaker liaison, workshop manager, and overall cat herder. Helping out over the past decade she has been involved in some capacity for over a dozen departments, activities, contests, and events. She provides annoyance, planning, and support in many ways, thus dubbed the "administrator of chaos". If you hate the schedule, or are mad your talk was rejected, you can blame her. Nikita likes to think of herself as approachable, and loves to make people feel welcome at DEF CON, despite having R.B.F. Her hardest job yet was writing a serious third person bio.

Twitter: @niki7a

PushPin is an uptight, perfectionist, who is very rarely content working with idiots and enjoys his Jell-O Pudding cups. He can neither confirm nor deny working for any of the three letter agencies that oversee WMDs, high energy weapons [LASERS, YO], and play around with other countries. It is literally impossible to see him without his laptop at any given time during the day and has been told frequently to put it away in public; otherwise, you'll find him at work devoid of any form of social life. I hate you all, seriously..

Twitter: @X72

Plug is a Mexican immigrant that immigrated to the States at age 18. While learning to read English found a 2600 magazine that lead him to his first LA2600 meeting in 1998, from that point forward he

has been a computer security enthusiast. Over the years he has worked a System's Administrator with a focus in security, eventually moving full time to work in information security. Plug currently works as a Senior Security Engineer securing the network of a prominent finance and foreign exchange company. He is also working on a volunteer project to teach 5th graders basic computer security skills. In his free time he enjoys playing with synthesizers and modular systems, when possible he volunteers his time to computer security events.

This is Russ' 17th year as a DEF CON goon, and he has over 25 years experience in hacking. Russ first learned to program around the 1982 timeframe, when he received a Timex Sinclair, which used only programs keyed in via BASIC. He's been involved in a numbers of aspects of DEF CON over the years, including the vendors, contests, DEF CON Groups, security, Hardware Hacking Village, and planning. Russ currently works a the Chief of Operations, where he depends heavily upon the other experienced hackers and goons that help run the world's largest hacker conference.

When the Secretary of State says: "Please Stop Hacking Us..."

David An, Former U.S. State Department

Senior American officials routinely hold dialogues with foreign officials to discuss cyber espionage. However, if a cyber attack can be performed through proxy servers jumping several countries before reaching the U.S., then can anyone ever be sure of who is really behind the attack? Yet we often see newspaper headlines clearly identifying that one country is hacking another country through state-sponsored, cyber criminal, or hacktivist means. Even if government cyber analysts with TS/SCI security clearances have high confidence in the identity of an attacker based on forensics and human intelligence, what are the challenges in effectively addressing the topic in a diplomatic or military dialogue with the attacker country?

Two major roadblocks in cyber diplomacy are the "attribution problem," and the related "disclosure dilemma." If there is indeed an attribution problem--when a country cannot be sure which other state is hacking it because a third country could be using it as a proxy--then a country could never accuse another countries of state-sponsored cyber attacks. Yet, countries routinely accuse others of cyber attacks, the public sees this in newspapers almost every day, and it is often an important topic in bilateral dialogues. Furthermore, the disclosure dilemma occurs when a country has both incentives and disincentives to disclose details on how it was hacked. On one hand, evidence will prove its case, but on another hand, evidence will make the attacker more savvy and careful not to repeat the same mistakes next time. Disclosure could create a stronger adversary. These are major concerns in the practice of cyber diplomacy today.

My presentation identifies how government-to-government cyber diplomacy works, examines the attribution problem and disclosure dilemma more fully, and shows how the U.S. approaches this topic differently with partners versus potential adversaries. This is not a technical presentation, but rather it is a policy presentation on cyber diplomacy drawing from political science and my diplomatic experience.

David was a tenured U.S. diplomat before leaving the U.S. government to consult for the private sector, and to write policy and academic papers. At the State Department, he was the senior political-military affairs officer covering the East Asia region and his responsibilities included coordinating diplomatic dialogues, formulating plans with the Pentagon, notifying Congress of U.S. arms sales, writing the Secretary of State's talking points, and traveling overseas with the Secretary of State and Secretary of Defense for bilateral dialogues. His other assignments included the U.S. embassies in Beijing, Tokyo, Wellington; U.S. consulates in Sydney and Perth; American Institute in Taiwan; and U.S. Pacific Command. He completed his B.A. at UC Berkeley; M.A. in international affairs and business management, and political science Ph.D. courses at UC San Diego.

Obligatory disclaimer: The comments are his own, and do not represent the U.S. government. Since Jeff Moss famously said in 2013: "Feds, we need some time apart," David emphasizes that he is no longer a fed.

Game of Hacks: Play, Hack & Track

Amit Ashbel, Product Evangelist Checkmarx
Maty Siman, CTO and Founder Checkmarx

Fooling around with some ideas we found ourselves creating a hacker magnet. Game of Hacks, built using the node.js framework, displays a range of vulnerable code snippets challenging the player to locate the vulnerability. A multiplayer option makes the challenge even more attractive and the leaderboard spices up things when players compete for a seat on the iron throne.

Within 24 hours we had 35K players test their hacking skills...we weren't surprised when users started breaking the rules. Join us to:

- Play GoH against the audience in real time and get your claim for fame
- Understand how vulnerabilities were planted within Game of Hacks
- See real attack techniques (some caught us off guard) and how we handled them
- Learn how to avoid vulnerabilities in your code and how to go about designing a secure application
- Hear what to watch out for on the ultra-popular node.js framework.

Check it out at www.Gameofhacks.com

Amit Ashbel joined Checkmarx From Trusteer (acquired by IBM). He has been with the security community for more than a decade where he has taken on multiple tasks and responsibilities over the years, including technical and Senior Product lead positions.

Amit adds valuable product knowledge including experience with a wide range of security platforms and familiarity with emerging threats and the hi-tech security industry.

Maty is the CTO and founder of Checkmarx. Maty has more than a decade of experience in software development, IT security and source-code analysis. Prior to founding Checkmarx, Maty worked for two years at the Israeli Prime Minister's Office as a senior IT security expert and project manager. Prior to that, he spent six years with the Israel Defense Forces (IDF), where he established and led a

development team in the IDF's Information Security Center. Maty regularly speaks at IT security conferences and is CISSP certified since 2003.

Web: www.Gameofhacks.com

Abusing XSLT for Practical Attacks

Fernando Arnaboldi, Senior Security Consultant at IOActive

Over the years, XML has been a rich target for attackers due to flaws in its design as well as implementations. It is a tempting target because it is used by other programming languages to interconnect applications and is supported by web browsers. In this talk, I will demonstrate how to use XSLT to produce documents that are vulnerable to new exploits.

XSLT can be leveraged to affect the integrity of arithmetic operations, lead to code logic failure, or cause random values to use the same initialization vector. Error disclosure has always provided valuable information, but thanks to XSLT, it is possible to partially read system files that could disclose service or system's passwords. Finally, XSLT can be used to compromise end-user confidentiality by abusing the same-origin policy concept present in web browsers.

This presentation includes proof-of-concept attacks demonstrating XSLT's potential to affect production systems, along with recommendations for safe development.

Fernando Arnaboldi is a senior security researcher and consultant at IOActive, Inc. He has over 10 years of experience in the security research space (Deloitte, Core Security Technologies and IOActive) and holds a Bachelor's degree in Computer Science.

RFIDiggity: Pentester Guide to Hacking HF/NFC and UHF RFID

Francis Brown, Partner - Bishop Fox
Shubham Shah , Security Analyst at Bishop Fox

Have you ever attended an RFID hacking presentation and walked away with more questions than answers? This talk will finally provide practical guidance for penetration testers on hacking High Frequency (HF - 13.56 MHz) and Ultra-High Frequency (UHF - 840-960 MHz). This includes Near Field Communication (NFC), which also operates at 13.56 MHz and can be found in things like mobile payment technologies, e.g., Apple Pay and Google Wallet. We'll also be releasing a slew of new and free RFID hacking tools using Arduino microcontrollers, Raspberry Pis, phone/tablet apps, and even 3D printing.

This presentation will NOT weigh you down with theoretical details or discussions of radio frequencies and modulation schemes. It WILL serve as a practical guide for penetration testers to better understand the attack tools and techniques available to them for stealing and using RFID tag information,

specifically for HF and UHF systems. We will showcase the best-of-breed in hardware and software that you'll need to build an RFID penetration toolkit. Our goal is to eliminate pervasive myths and accurately illustrate RFID risks via live attack DEMOS:

- High Frequency / NFC - Attack Demos:
    - HF physical access control systems (e.g., iCLASS and MIFARE DESFire 'contactless smart card' product families)
    - Credit cards, public transit cards, passports (book), mobile payment systems (e.g., Apple Pay, Google Wallet), NFC loyalty cards (e.g., MyCoke Rewards), new hotel room keys, smart home door locks, and more
- Ultra-High Frequency - Attack Demos:
    - Ski passes, enhanced driver's licenses, passports (card), U.S. Permanent Resident Card ('green card'), trusted traveler cards

Schematics and Arduino code will be released, and 100 lucky audience members will receive one of a handful of new flavors of our Tastic RFID Thief custom PCB, which they can insert into almost any commercial RFID reader to steal badge info or use as a MITM backdoor device capable of card replay attacks. New versions include extended control capabilities via Arduino add-on modules such as Bluetooth low energy (BLE) and GSM/GPRS (SMS messaging) modules.

This DEMO-rich presentation will benefit both newcomers to RFID penetration testing as well as seasoned professionals.

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.

Shubham Shah is a Security Analyst at Bishop Fox (formerly Stach & Liu), a security consulting firm providing IT security services to the Fortune 500, global financial institutions, and high-tech startups. Shubham's primary areas of expertise are application security assessment, source code review, and mobile application security.

Shubham is a former bug bounty hunter who has submitted medium-high risk bugs to the bug bounties of large corporations such as PayPal, Facebook, and Microsoft. He regularly conducts web application security research and frequently contributes to the security of open-source projects. He has presented at Ruxcon and is known in Australia for his identification of high-profile vulnerabilities in the infrastructures of major mobile telecommunication companies.

Prior to joining Bishop Fox, Shubham worked at EY. At EY, he performed web application security assessments and application penetration tests. Additionally, Shubham has been a contractor for companies such as Atlassian. As a contractor, he conducted external web application security penetration tests. Shubham also develops and maintains open-source projects such as Websec Weekly that assist the web application security industry.

Twitter: @bishopfox
Facebook: https://www.facebook.com/BishopFoxConsulting
LinkedIn: https://www.linkedin.com/company/bishop-fox

It's The Only Way To Be Sure: Obtaining and Detecting Domain Persistence

Grant Bugher, Perimeter Grid

When a Windows domain is compromised, an attacker has several options to create backdoors, obscure his tracks, and make his access difficult to detect and remove. In this talk, I discuss ways that an attacker who has obtained domain administrator privileges can extend, persist, and maintain control, as well as how a forensic examiner or incident responder could detect these activities and root out an attacker.

Grant Bugher has been hacking and coding since the early 90's and working professionally in information security for the last 11 years. He is currently a security consultant and engineer for a cloud service provider, and has previously been an architect, program manager and software engineer on a variety of online services, developer tools and platforms. Grant is a prior speaker at BlackHat and DEF CON and a regular DEF CON attendee since DEF CON 16. Most of his research and work is on cloud computing and storage platforms, application security, and detecting attacks against web-scale applications.

Twitter: @fishsupreme
Web: http://perimetergrid.com

Introduction to SDR and the Wireless Village

DaKahuna
satanklawz

In many circumstances, we all have to wear different hats when pursuing hobbies, jobs and research. This session will discuss the exploration and use of software defined radio from two perspectives; that of a security researcher and Ham Radio operator. We will cover common uses and abuses of hardware to make them work like transceivers that the Ham crowed is use too, as well as extending the same hardware for other research applications. Additionally we will highlight some of the application of this knowledge for use at The Wireless Village! Come and join this interactive session; audience participation is encouraged.

By day DaKahuna works for a small defense contractor as a consultant to large government agencies providing critical reviews of customer organizations compliance with Federal Information Systems information Security Act (FISMA) requirements, effectiveness of their implementation of National Institute for Science and Technology (NIST) Special Publication requirements, cyber security policies, cyber security program plans, and governmental standards and guidance. By night he enjoys roaming the airwaves , be it the amateur radio bands or wireless networks. He is a father of two, grandfather to three, 24 year Navy veteran communicator, holder of an amateur radio Extra Class license and a staunch supporter and exerciser of his 2nd Amendment rights who enjoys shooting targets out to 1200 yards.

Satanklawz has been in the information security realm for 15 years. He built and sold a wireless ISP, worked info sec in the financial services industry and now is a public servant of sorts. His hobbies and interests have always involved radio in some sort of fashion. When he has spare time, he is completing his PhD, teaches, create mischief, and is working on his dad jokes.

Flowers, red and blue,

satanklawz loves *SDR*.

This is a haiku.

Guests N' Goblins: Exposing Wi-Fi Exfiltration Risks and Mitigation techniques

Peter Desfigies, Cyber Security Investigations Unit, TELUS Security Solutions
Joshua Brierton, Sr. Security Analyst, TELUS Communications
Naveed Ul Islam, Managing Consultant, TELUS

Wi-Fi is a pervasive part of everyone's everyday life. Whether it be home networks, open hotspots at cafes, corporate networks or corporate guest networks they can be found virtually everywhere. Fortunately, for the security minded, some steps are taken to secure these weak points in one's infrastructure. Usually this is done through some form of registration page which is common in the case of guest networks. But is this enough? And what new threats could be unleashed from even the most isolated of Wi-Fi networks?

In the most paranoid of cases, companies will generally attempt to isolate Wi-Fi networks from their official networks in order to protect their own assets from attacks, while still ensuring that Wi-Fi is convenient for end users. But there is another way to attack a company that could be damaging to the host company and harmful to other targets. This presentation will go over the utilization of various techniques of getting onto and getting out through publicly accessible Wi-Fi networks for nefarious purposes, termed Wi-Fi Exfiltration. Through this technique one is able to obfuscate their identity by using the host of the Wi-Fi's identity, thus implicating the host in the attack.

During the presentation we will cover the findings through our tests along with a list of recommendations for what can be done to mitigate this risk. This is a must attend session to all security professionals and high level management.

Peter Desfigies is a Security Consultant at TELUS Communications Inc. where he works with a team of other operations analysts to proactively investigate and analyze customer traffic, while also providing threat intelligence on attacks, campaigns, and zero-days in order to protect customer's environment and enhance their security posture. During his time at TELUS, he has worked with a variety of teams providing LAN, WAN, Telco, Security and hardware break/fix support, and now Security Analysis for government and corporate customer. Prior to TELUS, he worked for 12 years in IT operation roles to provide backbone network support including DNS, SMTP, POP, dialup, T1 to OC12 , and Ethernet at various companies, with the bulk of his experience at UUNET / MCI.

Joshua Brierton is a Sr. Security Analyst at TELUS Communications Inc. where he works with a team of SIEM specialists to provide customers with a cloud SIEM service offering. Primarily working on rule development and user work flows his other interests in the field includes developing tools to help automate and expedite repetitive work to increase user efficiency. During his time at TELUS he has worked with various teams providing security solutions from VPN services to IPS services along with outsourced development for a variety of other well-known SIEM's. Prior to TELUS he worked for 5 years with Intellitactics Inc. doing development and device support for the content of the SIEM they provided. Collectively Josh has been working with a variety of SIEM's for 10 years.

Naveed Ul Islam (BEE Telecom/DSP, CISSP, SABSA-SCF) is a Managing Consultant at TELUS and Security Intelligence architect within the TELUS Cyber Security Investigation Unit. Naveed's other interests are in application forensics and enterprise security architecture. Naveed's prior duties with TELUS include securing of then world's largest PKI infrastructure known as Secure Channel. In addition, he was responsible for secure implementation of TELUS Health Space infrastructure. He led application security practices within TELUS Health, where he was able to incorporate software security lifecycle into software development practices. Also, he has been a part of security incident response and penetration testing teams. Previous to TELUS, Naveed was a security consultant for Microsoft USA, where he performed security and privacy audits of Microsoft's core-business related websites. He has secured several key sites such as Microsoft XBOX 360 host web site and Microsoft's internal auction site known as Micronews.

Let's Encrypt - Minting Free Certificates to Encrypt the Entire Web

Peter Eckersley, Electronic Frontier Foundation
James Kasten, Electronic Frontier Foundation
Yan Zhu, Electronic Frontier Foundation

Let's Encrypt is a new certificate authority that is being launched by EFF in collaboration with Mozilla, Cisco, Akamai, IdenTrust, and a team at the University of Michigan. It will issue certificates for free, using a new automated protocol called ACME for verification of domain control and issuance.

This talk will describe the features of the CA and available clients at launch; explore the security challenges inherent in building such a system; and its effect on the security of the CA marketplace as a whole. We will also update our place on the roadmap to a Web that uses HTTPS by default.

Peter Eckersley is Chief Computer Scientist for the Electronic Frontier Foundation. He leads a team of technologists who watch for technologies that, by accident or design, pose a risk to computer users' freedoms-and then look for ways to fix them. They write code to make the Internet more secure, more open, and safer against surveillance and censorship. They explain gadgets to lawyers and policymakers, and law and policy to gadgets.

Aside from Let's Encrypt, Peter's other work at EFF has included privacy and security projects such as Panopticlick, HTTPS Everywhere, SSDI, and the SSL Observatory; helping to launch a movement for open wireless networks; fighting to keep modern computing platforms open; and running the first controlled tests to confirm that Comcast was using forged reset packets to interfere with P2P protocols.

Peter holds a PhD in computer science and law from the University of Melbourne.

James Kasten is a PhD candidate in Computer Science and Engineering at the University of Michgan and a STIET fellow. James is also a contractor at the Electronic Frontier Foundation. His research focuses on practical network security and PKI.

James has published on the state of TLS, its certificate ecosystem and its vulnerabilities. Most notably, James has helped design the protocol and launch the technology behind Let's Encrypt.

Yan is a security engineer at Yahoo, mostly working on End-to-End email encryption and improving TLS usage. She is also a Technology Fellow at EFF and a core developer of Let's Encrypt, HTTPS Everywhere, Privacy Badger Firefox, and SecureDrop. Yan has held a variety of jobs in the past, ranging from hacking web apps to composing modern orchestra music. She got a B.S. from MIT in 2012 and is a proud PhD dropout from Stanford.

Yan has been a speaker at HOPE, DEFCON 22, jQuerySF, Real World Crypto, SXSW, and various other human gatherings. She is @bcrypt on Twitter.

Ubiquity Forensics - Your iCloud and You

Sarah Edwards, Test Engineer, Parsons Corporation & Author/Instructor, SANS Institute

Ubiquity or "Everything, Everywhere" - Apple uses this term describe iCloud related items and its availability across all devices. iCloud enables us to have our data synced with every Mac, iPhone, iPad, PC as well as accessible with your handy web browser. You can access your email, documents, contacts, browsing history, notes, keychains, photos, and more all with just a click of the mouse or a tap of the finger - on any device, all synced within seconds.

Much of this data gets cached on your devices, this presentation will explore the forensic artifacts related to this cached data. Where is the data stored; how to look at it; how is it synced; and what other sensitive information can be found that you may not have known existed!

Sarah is an digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal, counter intelligence, counter-narcotic, and counter terrorism. Sarah's research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering. Sarah has presented at many industry conferences including; Shmoocon, CEIC, various Bsides, DEF CON, and the SANS DFIR Summit. Sarah is author and instructor of the SANS Mac Forensic Analysis Course - FOR518.

Crypto for Hackers

Eijah, Founder, Demonsaw

Hacking is hard. It takes passion, dedication, and an unwavering attention to detail. Hacking requires a breadth of knowledge spread across many domains. We need to have experience with different platforms, operating systems, software packages, tools, programming languages, and technology trends. Being overly deficient in any one of these areas can add hours to our hack, or even worse, bring us total failure.

And while all of these things are important for a well-rounded hacker, one of the key areas that is often overlooked is cryptography. In an era dominated by security breaches, an understanding of encryption and hashing algorithms provides a tremendous advantage. We can better hone our attack vectors, especially when looking for security holes. A few years ago I released the first Blu-Ray device key, AA856A1BA814AB99FFDEBA6AEFBE1C04, by exploiting a vulnerability in an implementation of the AACS protocol. As hacks go, it was a simple one. But it was the knowledge of crypto that made it all possible.

This presentation is an overview of the most common crypto routines helpful to hackers. We'll review the strengths and weaknesses of each algorithm, which ones to embrace, and which ones to avoid. You'll get C++ code examples, high-level wrapper classes, and an open-source library that implements all the algorithms. We'll even talk about creative ways to merge algorithms to further increase entropy

and key strength. If you've ever wanted to learn how crypto can give you an advantage as a hacker, then this talk is for you. With this information you'll be able to maximize your hacks and better protect your personal data.

Eijah is the founder of demonsaw, a secure and anonymous content sharing platform, and a Senior Programmer at a world-renowned game development studio. He has over 15 years of software development and IT Security experience. His career has covered a broad range of Internet and mid-range technologies, core security, and system architecture. Eijah has been a faculty member at multiple colleges, has spoken about security and development at conferences, and holds a master's degree in Computer Science. Eijah is an active member of the hacking community and is an avid proponent of Internet freedom.

Twitter: @demon_saw
Web: https://www.demonsaw.com
Facebook: https://www.facebook.com/Demonsaw
Github: https://github.com/eijah/demonsaw
Email: eijah at demonsaw dot com

Extending Fuzzing Grammars to Exploit Unexplored Code Paths in Modern Web Browsers

Saif El-Sherei, Analyst, SensePost
Etienne Stalmans, Analyst, SensePost

Fuzzing is a well-established technique for finding bugs, hopefully exploitable ones, by brute forcing inputs to explore code paths in an application. In recent years, fuzzing has become a near mandatory part of any major application's security team efforts. Our work focused on fuzzing web browsers, a particularly difficult challenge given the size and quality of some of their security teams, the existing high-quality fuzzers available for this, and, of late, bug bounty programs.

Despite this, our improved fuzzing approach was able to find four confirmed bugs within Google Chrome and two within Microsoft Internet Explorer 11. The bugs had varying potential exploitability. Interestingly, some had been independently discovered indicating others are active in this field. The work is on going, and we hope to have more before the presentation.

As browsers continue to grow as the new universal interface for devices and applications, they have become high value targets for exploitation. Additionally, with the growth of browser fuzzing since 2004, this is a complex field to get started in. Something we hope to help address.

Our research and presentation will consist of two parts:

The first part is an introduction to fuzzing for the security practitioner. Here we combine the approaches, tool sets and integrations between tools we found to be most effective into a recipe for fuzzing various browsers and various platforms.

The second part is a description of our work and approach used to create, and extend, browser fuzzing grammars based on w3c specifications to discover new and unexplored code paths, and find new browser security bugs. In particular, example of real bugs found in the Chrome and IE browser will be demonstrated.

Saif is the body double for Borat, but couldn't pull off a mankini and ended up in information security. His focus is on fuzzing and vulnerability research.

Etienne hopes he will outlive his beard, but in the meantime, this hacking schtick pays for beard oil. His other interests lie in mobile applications and no-sql databases. Both are analysts within SensePost's London office.

Secure Messaging for Normal People

Justin Engler, Senior Security Engineer, iSEC Partners

"Secure" messaging programs and protocols continue to proliferate, and crypto experts can debate their minutiae, but there is very little information available to help the rest of the world differentiate between the different programs and their features. This talk will discuss the types of attacks various secure messaging features can defend against so those who are tech-savvy but not crypto-experts can make informed decisions on which crypto applications to use.

This talk is intended for people with no preexisting cryptography knowledge. There will be no math or programming knowledge required. The goal is to explain secure messaging concepts such as PKI, PFS, and key validation without diving into heavier crypto, math, or programming content.

Justin Engler is a Principal Security Engineer with NCC Group. Justin has been involved in application security assessments of many open and closed source messaging applications and other related technologies. He has spoken previously at DEF CON, BlackHat, Toorcon, and other regional events. Justin has 5 years of security consulting experience and has been involved in security, software development, and IT professionally for over 10 years.

Seeing through the Fog

Zack Fasel, Urbane Security

Yes. "The Cloud" (drink). Even though many of us would much like to see use of public clouds decline, they're not going away any time soon. And with such, a plethora of companies now have revolutionary new solutions to solve your "cloud problems". From crypto to single sign on with two step auth, proxies to monitoring and DLP, every vendor has a solution, even cloud based for the cloud!

What we haven't seen is much of an open source or community lead solution to these problems. So let's change that.

Zack will review the laundry list of security problems with various cloud providers (and their pluthera of APIs), provide some easy fixes to the common issues seen, and introduce a few new open source tools to help monitor and defend the data and access in the wild.

Zack Fasel is a Founding Partner at Urbane Security, a solutions-focused vendor-agnostic information security services firm focusing on providing innovative defense, sophisticated offense and refined compliance services. Heading up Urbane's Research and Security Services divisions, Zack brings his years of diverse internal and external experience to drive Urbane's technical solutions to organizations top pain points. His previous research and presentations at conferences have spread across numerous domains including Windows authentication flaws, femtocells, open source defensive security solutions and unique network and application attack vectors. When not selling out, he can be found lost in the untz unce wubs, dabbling in instagram food photography, or eating scotch and drinking gummy bears (that's right, right?). More information on him can be found at zfasel.com and on Urbane Security at UrbaneSecurity.com.

Twitter: @zfasel

Linux Containers: Future or Fantasy?

Aaron Grattafiori, Principal Security Consultant, iSEC Partners/NCC Group

Containers, a pinnacle of fast and secure deployment or a panacea of false security? In recent years Linux containers have developed from an insecure and loose collection of Linux kernel namespaces to a production-ready OS virtualization stack. In this talk, the audience will first learn the basics of how containers function, understanding namespaces, capabilities and cgroups in order to see how Linux containers and the supporting kernel features can offer an effective application and system sandboxing solution yet to be widely deployed or adopted. Understanding LXC or Docker use, weaknesses and security for PaaS and application sandboxing is only the beginning.

Leveraging container technologies is rapidly becoming popular within the modern PaaS and devops world but little has been publicly discussed in terms of actual security risks or guarantees. Understanding prior container vulnerabilities or escapes, and current risks or pitfalls in major public platforms will be explored in this talk. I'll cover methods to harden containers against future attacks and common mistakes to avoid when using systems such as LXC and Docker. This will also include an analysis and discussion of techniques such as Linux kernel hardening, reduced capabilities, Mandatory Access Controls (MAC), the User kernel namespace and seccomp-bpf (syscall filtering); all of which help actually contain containers. The talk will end on some methods for creating minimal, highly-secure containers and end on where containers are going and why they might show up where you least expect them.

Aaron Grattafiori (@dyn___) is a Principal Security Consultant and Research Lead with iSEC Partners/NCC Group. A jack-of-all-security, Aaron leads projects dealing with complex system analysis, mobile and web application security to network, protocol, and design reviews to red teams and other hybrid testing. With over nine years of security experience, Aaron utilizes a wide array of technology skills, historical research and security knowledge to consistently discover critical vulnerabilities. Aaron

has spoke on a wide range of topics at security conferences such as Blackhat, DEF CON Kids, Toorcon:Seattle+SanDiego, ToorCamp, Source Seattle, EELive! and SecureWorld in addition to being a guest speaker at Stanford University. Prior to working at iSEC Partners, Aaron worked as a Security Consultant for Security Innovation and is a retired long time member of the Neg9 CTF team. This will be Aaron's 12th DEF CON, w00t!

Twitter: @dyn___

How to Shot Web: Web and mobile hacking in 2015

Jason Haddix, Director of Technical Operations, Bugcrowd

2014 was a year of unprecedented participation in crowdsourced and static bug bounty programs, and 2015 looks like a trendmaker. Join Jason as he explores successful tactics and tools used by himself and the best bug hunters. Practical methodologies, tools, and tips make you better at hacking websites and mobile apps to claim those bounties. Convert edge-case vulnerabilities to practical pwnage even on presumably heavily tested sites. These are tips and tricks that the every-tester can take home and use. Jason will focus on philosophy, discovery, mapping, tactical fuzzing (XSS, SQLi, LFI, ++), CSRF, web services, and mobile vulnerabilities. In many cases we will explore these attacks down to the parameter, teaching the tester common places to look when searching for certain bugs. In addition he will cover common evasions to filters and as many time saving techniques he can fit in.

Jasonis the Director of Technical Operations at Bugcrowd. Jason trains and works with internal application 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/infrastructural security assessments, binary reverse engineering, and static analysis.

Alice and Bob are Really Confused

David Huerta, Cryptoparty Organizer

There have been over 20 cryptoparties in New York City, in which people are introduced to open source cryptography software. This doesn't always go smoothly. Usability experts have only recently being included in the design process for encryption tools, but by and large what we have to work with were designed by cryptography experts in the 90s. I'll be going over some pain points between real-world users and their real-life encounters with open source cryptography tools.

David Huerta ships critical art in suspicious packages and helps organize cryptoparties, which bring technologists and everyone else in New York together to learn how to protect their online privacy. Before arriving in New York, he dropped out of Arizona State University and was one of the founding members for HeatSync Labs, an Arizona hackerspace which brings makers, hackers, and the occasional futurist together to build things and teach others how to do the same.

LTE Recon and Tracking with RTLSDR

Ian Kline, Wolf Den Associates

Since RTLSDR became a consumer grade RX device, numerous talks and open source tools enabled the community to monitor airplanes, ships, and cars... but come on, what we really want to track are cell phones. If you know how to run cmake and have $50 to pick up an RTLSDR-E4000, I'll make sure you walk out of here with the power to monitor LTE devices around you on a slick Kibana4 dashboard. You'll also get a primer on geolocating the devices if you've got a second E4000 and some basic soldering skills.

Ian has 10 years of experience studying the global RF emissions environment. Professionally, he uses this knowledge to rapidly hack up communication platforms and conduct RF surveys for pentesting and red teaming activities. Personnally, he can be found listening to satellites and building databses of all the cars that park on his block with TPMS. He currently supports Wolf Den Associates as Red Team leader and Digital Signature Specialist.

Forensic Artifacts From a Pass the Hash Attack

Gerard Laygui, Security Researcher

A pass the hash (PtH) attack is one of the most devastating attacks to execute on the systems in a Windows domain. Many system admins are unaware about this type of attack and the amount of damage it can do. This presentation is for the system admins that don't have a full time forensics person working with them. This presentation will help identify key windows events and explain why these events are important. The presentation will also show various free tools that can assist in examining some of the common evidence left behind. The presentation will explain and demonstrate a pass the hash attack against common windows systems in an example domain. In the end, the presentation may offer some insight into what an attacker wants and needs to use PtH to pivot in a network.

Gerard has been in the IT industry for almost 20 years. He has held various network admin, system admin, web admin and security related positions throughout his career. He currently works for a Fortune 50 company doing compromise forensics and malware reverse engineering.

I'm A Newbie Yet I Can Hack ZigBee - Take Unauthorized Control Over ZigBee Devices

LI Jun, Graduate student from CUIT(Chengdu University of Information Technology , Chengdu ,China),Intern at Qihoo 360 Technology Co. Ltd.
YANG Qing, Team Leader of Unicorn Team, Qihoo 360 Technology Co. Ltd.

With the advent of the Internet of Thingsï¼Œmore and more objects are connected via various communication protocols like Bluetoothï¼ŒZ-waveï¼ŒWiFi , ZigBee etc. Among those protocols ZigBee accounts for the largest market shareï¼Œit has been adapted to various applications like WSNï¼ˆWireless Sensor Networkï¼‰ï¼ŒSmart Home . Over the last few years, large amount of research has been conducted on the security of ZigBee. In this presentation we will introduce a new technique to beat the security of ZigBee, we found the "signature" of the location of the security key . We will go through a specific example and share the thinking process along the way. The techniques used throughout this example can be generalized and used by other hardware reverse engineers.

LI Jun is currently a hardware security intern in Unicorn Team of Qihoo 360 ,China. He is also a second year graduate student at Chengdu University of Information Technology. He received his bachelor's degree from University of Electronic Science and Technology of China in 2013.During his college life, he switched between different majors, 2 years in Automobile Electronics,2 years in Electronic and Electric Engineering. He is interested in the security of the Internet of Things and the security of automobile electronics.

Linkedin: LI Jun
Weibo: GoRushing
Twitter: @bravo_fighter

YANG Qing is the team leader of Unicorn Team in Qihoo 360 Technology Co. Ltd. He has rich experiences in wireless and hardware security area, including WiFi penetration testing, cellular network interception, IC card cracking etc. His interests also cover embedded system hacking, firmware reversing, automotive security, and software radio .He is the first one who reported the vulnerabilities of WiFi system and RF IC card system used in Beijing subway.

Are We Really Safe? - Bypassing Access Control Systems

Dennis Maldonado, Security Consultant - KLC Consulting

Access control systems are everywhere. They are used to protect everything from residential communities to commercial offices. People depend on these to work properly, but what if I had complete control over your access control solution just by using my phone? Or perhaps I input a secret keypad combination that unlocks your front door? You may not be as secure as you think.

The world relies on access control systems to ensure that secured areas are only accessible to authorized users. Usually, a keypad is the only thing stopping an unauthorized person from accessing the private space behind it. There are many types of access control systems from stand-alone keypads to telephony access control. In this talk, Dennis will be going over how and where access control systems are used. Dennis will walk through and demonstrate the tips and tricks used in bypassing common access control systems. This presentation will include attack methods of all nature including physical attacks, RFID, wireless, telephony, network, and more.

Dennis Maldonado is a Security Consultant at KLC Consulting. His current work includes vulnerability management, penetration testing, infrastructure risk assessment and security research. Dennis' focus is

encompassing all forms information security into an assessment in order to better simulate a real world attack against systems and infrastructure.

As a security researcher and evangelist, Dennis spends his time sharing what he knows about Information Security with anyone willing to learn. Dennis has presented at numerous workshops and meetups in the Houston area. Dennis co-founded Houston Locksport in Houston, Texas where he shares his love for lock-picking physical security.

Twitter: @DennisMald

Sorry, Wrong Number: Mysteries Of The Phone System - Past and Present

"Unregistered436" Patrick McNeil, Security Architect
"Snide" Owen, Security Researcher

Exploring the phone system was once the new and exciting realm of "phone phreaks," an ancestor of today's computer "hackers." The first phreaks "owned" and explored the vague mysteries of the telephone network for a time until their activities drew too much attention from the phone companies and law enforcement. The phone system evolved, somewhat, in an attempt to shut them out, and phreaking became both difficult and legally dangerous. Such events paralleled a new personal computer "revolution" wherein phone phreaks made the transition from the secret subtleties of telephony to the new and mystical frontier of personal computing. Private BBS(s) and, eventually, the Internet was not only the next logical step forward, but also provided "safer" alternatives that still allowed for the thrill of exploring the mysteries of a new modern age. Telephony, and voice security in general, became, as the years passed, something of a lost art to all but those who remember...

In this presentation we begin our adventure with a journey back in time, starting in the post-war Film Noir era of the 40's and 50's, when users required an operator at the switchboard to make a call, investigating some of the early roots of phreaking that many have forgotten. We will briefly take a look at the weaknesses of early telephone systems and the emergence of the original phreaks in the 50's and 60's who found and exploited them. Our journey will also allow us to demonstrate how some of the same basic phreaking approaches are still applicable to today's "advanced" VoIP systems.

Certainly the initial creation and emergence of VoIP opened a variety of attack vectors that were covered at security conferences at the time. Commercial VoIP adoption, however, remained stagnant until standards and carriers caught up. Some VoIP hacking tools were left unmaintained, and VoIP wasn't the sexy and mysterious attack vector it once was with the exception of tricksters who found old or insecure systems to be easy targets. Due to increased VoIP adoption over the last few years, however, telephony attacks are provocative once again.

As hardboiled VoIP detectives, we'll unravel the mysteries of the curious, shadowy, and secretive world of phreaks, tricksters, and VoIP hackers. We'll compare and contrast old school phreaking with new advances in VoIP hacking. We'll explain how voice systems are targeted, how they are attacked using

old and new methods, and how to secure them - with demonstrations along with practical and actionable tips along the way. We may even drop a new VoIP telephony phishing tool to fuse the past and the present..

Patrick spoke about telephony fraud last year at DEF CON Skytalks ("How To Make Money Fast Using A Pwned PBX"), and is a #telephreak at heart. He has over twenty years of experience, mostly with telecom manufacturers, and spent time in charge of product security for the communications security business of a fortune 100 company. When not working you can find him practicing Kung Fu, brewing beer, or picking locks with Oak City Locksport.

Twitter: @unregistered436

Owen used to be a professional developer code monkey. He's worked in various IT fields including Server Administration, DevOps, Application Security and most recently as a penetration tester. He enjoys tinkering with various technologies, and has experimented for prolonged periods with PBXs and the obscure side of VoIP.

Twitter: @linuxblog

Backdooring Git

John Menerick, Security @ NetSuite

Join us for a fun-filled tour of source control management and services to talk about how to backdoor software. We will focus on one of the most popular, trendy SCM tools and related services out there - Git. Nothing is sacred. Along the way, we will expose the risks and liabilities one is exposed to by faulty usage and deployments. When we are finished, you will be able to use the same tools and techniques to protect or backdoor popular open source projects or your hobby project.

John Menerick works on Security @ NetSuite. John's interests include cracking clouds, modeling complex systems, developing massive software-defined infrastructures, and is the outlier in your risk model.

Hacking SQL Injection for Remote Code Execution on a LAMP stack

Nemus, Software Engineer

Remember that web application you wrote when you where first learning PHP? Ever wonder how vulnerable that code base is? Through the perspective of an attacker you will see how SQL injection can lead to data loss and system compromise. This presentation will take you through the techniques and tools used to take control of a PHP web application starting from an injection point moving to PHP web shells, and ending with a Linux wildcard attack.

Nemus works as a software engineer in the payment industry developing software that transfers money between banking systems. He is a founding member of 801 Labs, a hackerspace located in Salt Lake City, and is an active member of his local DEF CON group DC801. Nemus has a BS in Computer Science and is a certified GIAC Web Application Penetration Tester (GWAPT).

Twitter: @Nemus801

Abusing native Shims for Post Exploitation

Sean Pierce, Technical Intelligence Analyst for iSIGHT Partners

Shims offer a powerful rootkit-like framework that is natively implemented in most all modern Windows Operating Systems. This talk will focus on the wide array of post-exploitation options that a novice attacker could utilize to subvert the integrity of virtually any Windows application. I will demonstrate how Shim Database Files (sdb files / shims) are simple to create, easy to install, flexible, and stealthy. I will also show that there are other far more advanced applications such as in-memory patching, malware obfuscation, evasion, and system integrity subversion. For defenders, I am releasing 6 open source tools to prevent, detect, and block malicious shims.

Sean Pierce is a Technical Intelligence Analyst for iSIGHT Partners. Sean currently specializes in reverse engineering malware & threat emulation and in the past has worked on incident response, botnet tracking, security research, automation, and quality control. Prior working at iSIGHT Partners, he was an academic researcher and part time lecturer at the University of Texas at Arlington where he earned a Bachelors of Computer Engineering with a minor in Math. Sean also does freelance consulting, penetration testing, forensics, and computer security education. He is an Eagle Scout and enjoys learning how things work.

Twitter: @secure_sean

Hacker in the Wires

Dr. Phil Polstra, Professor, Bloomsburg University

This talk will show attendees how to use a small ARM-based computer that is connected inline to a wired network for penetration testing. The computer is running a full-featured penetration testing Linux distro. Data may be exfiltrated using the network or via a ZigBee mesh network or GSM modem.

The device discussed in this talk is easily integrated into a powerful penetration test that is performed with an army of ARM-based small computer systems connected by XBee or ZigBee mesh networking.

Some familiarity with Linux and penetration testing would be helpful, but not required.

Phil was born at an early age. He cleaned out his savings at age 8 in order to buy a TI99-4A computer for the sum of $450. Two years later he learned 6502 assembly and has been hacking computers and electronics ever since.

Dr. Phil currently works as a professor at Bloomsburg University of Pennsylvania. His research focus over the last few years has been on the use of microcontrollers and small embedded computers for forensics and pentesting. Phil has developed a custom pentesting Linux distro and related hardware to allow an inexpensive army of remote pentesting drones to be built using the BeagleBone Black computer boards. This work is described in detail in Phil's book "Hacking and Penetration Testing With Low Power Devices" (Syngress, 2015).

Prior to entering academia, Phil held several high level positions at well-known US companies. He holds a couple of the usual certs one might expect for someone in his position. When not working, he likes to spend time with his family, fly, hack electronics, and has been known to build airplanes.

Twitter: @ppolstra
http://facebook.com/ppolstra

A Hacker's Guide to Risk

Bruce Potter, The Shmoo Group

When the latest and greatest vulnerability is announced, the media and PR frenzy can be dizzying. However, when the dust settles, how do we actually measure the risk represented by a given vulnerability. When pen testers find holes in an organization, is it really "ZOMG, you're SO 0WNED!" or is it something more manageable and controlled? When you're attempting to convince the boss of the necessity of the latest security technology, how do really rank the importance of the technology against the threats facing the organization.

Understanding risk can be tricky, especially in an industry that often works on gut feelings and values quantity over quality. But risk and risk management doesn't need to be complicated. With a few basic formulas and access to some simple models, understanding risk can be a straightforward process. This talk will discuss risk, why its important, and the poor job the hacker community has done when it comes to properly assessing risk. It will also touch on some existing risk assessment and management systems, as well as provide worked examples of real world vulnerabilities and systems and the risks they pose. Finally, this talk will examine some practical guidance on how you, as hackers, security researchers, and security practitioners can better measure risk in your day to day life

Bruce Potter is the founder of The Shmoo Group, one of the organizers of ShmooCon, and a director at KEYW Corporation. Bruce's lack of degrees and certifications hasn't stopped him from discussing infosec in numerous articles, books, and presentations. Bruce has been in the computer security field for nearly 2 decades which means he is getting old and increasingly jaded. His primary focus areas are trusted computing, cyber security risk management (yikes!), and large scale vulnerability analysis. Bruce believes that while attackers have the upper hand, we can still do better with the tools we have than most people realize. Bruce also believes in using fake names when ordering coffee but occasionally uses his real name to throw people off his scent.

Twitter: @gdead

Chellam - a Wi-Fi IDS/Firewall for Windows

Vivek Ramachandran, Founder, SecurityTube.net and Pentester Academy

This talk will introduce techniques to detect Wi-Fi attacks such as Honeypots, Evil Twins, Mis-association , Hosted Network based backdoors etc. on a Windows client without the need for custom hardware or drivers. Our attack detection techniques will work for both Encrypted (WPA/WPA2 PSK and Enterprise) and Unencrypted networks.

We will also release a proof of concept tool implementing our detection techniques. Even though the focus of this talk is Windows, the same principles can be used to protect other Operating Systems, both workstation and mobile.

Vivek Ramachandran discovered the Caffe Latte attack, broke WEP Cloaking and publicly demonstrated enterprise Wi-Fi backdoors. He is the author of "Backtrack 5: Wireless Penetration Testing" which has sold over 13,000+ copies worldwide. He is the founder of SecurityTube.net and runs SecurityTube Training & Pentester Academy which has trained professionals from 90 countries. He has spoken/trained at DEF CON, Blackhat USA/Europe/Abu Dhabi, Brucon, Hacktivity etc. conferences.

Twitter: @securitytube
Facebook: https://www.facebook.com/pagesectube

Hardware and Trust Security: Explain it like I'm 5

Teddy Reed, Security Engineer Facebook
Nick Anderson, Research Scientist

There are a lot of presentations and suggestions that indicate HSMs, TrustZone, AMT, TrEE, SecureBoot, Attestation, TPMs, IOMMU, DRTM, etc. are silver bullets. What does it all mean, should we be afraid, excited, hopeful? Hardware-based security features are not the end of the world, nor its savior, but they can be fun and useful. Although these technologies are vulnerability research targets, their trust concepts can be used to build secure software and devices.

This primer covers practical defensive uses of existing and upcoming hardware security and mobile trust technologies. We will overview the strengths, pitfalls, gotchas of these esoteric acronyms; and explain the capabilities of related features built into consumer and enterprise laptops, mobile, and embedded devices. Let's take a tour around the wild world of hardware and trust security!

Teddy is a Security Engineer at Facebook developing production security tools. He is very passionate about trustworthy, safe, and secure code development. He loves open source and collaborative engineering when scale, resiliency, and performance enable defensive and protective software design. Teddy has published at security conferences on trusted computing, hardware trusted systems, UAVs, botnet development, human performance engineering, competition game theory, biometric vulnerabilities, and PaaS API vulnerabilities.

Nick Anderson is a research scientist at a US super serious secret laboratory. When Nick is not fighting cyber warriors in the cyber threatscape in his cyber career, he is actively engaged in malware research and enjoys failing at web development. Nick received his masters degree from NYU Polytechnic School of Engineering after completing his bachelors degree in Mathematics from the University of Wyoming.

Bruce Schneier Q&A

Bruce Schneier, CTO, Resilient Systems

Bruce Schneier Talks Security. Come hear about what's new, what's hot, and what's hype in security. NSA surveillance, airports, voting machines, ID cards, cryptography -- he'll talk about what's in the news and what matters. Always a lively and interesting talk.

Bruce Schneier is an internationally renowned security technologist, called a Â“security guruÂ” by the Economist. He is the author of 12 booksÂ—including the New York Times best-seller Data and Goliath: The Hidden Values to Collect Your Data and Control Your WorldÂ—as well as hundreds of articles, essays, and academic papers. His influential newsletter Â“Crypto-GramÂ” and his blog Â“Schneier on SecurityÂ” are read by over 250,000 people. He has testified before Congress, is a frequent guest on television and radio, has served on several government committees, and is regularly quoted in the press. Schneier is a fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America FoundationÂ's Open Technology Institute, a board member of the Electronic Frontier Foundation, and an advisory board member of the Electronic Privacy Information Center. He is the CTO of Resilient Systems.

Twitter: @schneierblog

Applied Intelligence: Using Information That's Not There

Michael Schrenk, Security Researcher

Organizations continue to unknowingly leak trade secrets on the Internet. To those in the know, these leaks are a valuable source of competitive intelligence. This talk describes how the speaker collects competitive intelligence for his own online retail business. Specifically, you learn how he combines, trends, and analyzes information within specific contexts to manufacture useful data that is real, but technically doesn't exist on it's own. For example, you will learn about the trade secrets that are hidden within sequential numbers, how he uses collected intelligence to procure inventory, and how and why he gauges the ongoing health of his industry and that of his competitors. And on a related note, you'll also learn how the federal government nearly exposed an entire generation to identity fraud.

Michael Schrenk has presented six DEF CON talks on intelligence and organizational privacy, including last year's talk "You're Leaking Trade Secrets". He has developed Internet-based intelligence campaigns since 1995 for organizations as diverse as: Fortune 500 Companies, Private Investigators, Asian Art Dealers, and Investigative Journalists. His adventures in intelligence have taken him around the world, with speaking opportunities in The Middle East, Eastern Europe, The UK, Silicon Valley, and

most places in between. Mike is also the author of "Webbots, Spiders, and Screen Scrapers (2007 & 2012, No Starch Press, San Francisco)". He is again teaming with No Starch Press to write a non-technical Intelligence and Counterintelligence book scheduled for publication in Q1 2016.

Twitter: @mgschrenk
Facebook: facebook.com/webbots

I Am Packer And So Can You

Mike Sconzo, Security Researcher

Automating packer and compiler/toolchain detection can be tricky and best and downright frustrating at worst. The majority of existing solutions are old, closed source or aren't cross platform. Originally, a method of packer identification that leveraged some text analysis algorithms was presented. The goal is to create a method to identify compilers and packers based on the structural changes they leave behind in PE files. This iteration builds upon previous work of using assembly mnemonics for packer detection and grouping. New features and analysis are covered for identification and clustering of PE files.

Mike Sconzo has been around the Security Industry for quite some time, and is interested in creating and implementing new methods of detecting unknown and suspicious network activity as well as different approaches for file/malware analysis. This includes looking for protocol anomalies, patterns of network traffic, and various forms of static and dynamic file analysis. He works on reversing malware, tool creation for analysis, and threat intelligence. Currently a lot of his time is spent doing data exploration and tinkering with statistical analysis and machine learning.

NSM 101 for ICS

Chris Sistrunk, Sr. ICS Security Consultant, FireEye

Is your ICS breached? Are you sure? How do you know?

The current state of security in Industrial Control Systems is a widely publicized issue, but fixes to ICS security issues are long cycle, with some systems and devices that will unfortunately never have patches available. In this environment, visibility into security threats to ICS is critical, and almost all of ICS monitoring has been focused on compliance, rather than looking for indicators/evidence of compromise. The non-intrusive nature of Network Security Monitoring (NSM) is a perfect fit for ICS. This presentation will show how NSM should be part of ICS defense and response strategy, various options for implementing NSM, and some of the capabilities that NSM can bring to an ICS security program. Free tools such as Security Onion, Snort IDS, Bro IDS, NetworkMiner, and Wireshark will be used to look at the ICS environment for anomalies. It will be helpful if attendees have read these books (but they aren't required): The Cuckoo's Egg by Cliff Stoll, The Practice of Network Security Monitoring by Richard Bejtlich, and Applied Network Security Monitoring by Chris Sanders and Jason Smith.

Chris Sistrunk is a Senior Consultant at Mandiant, focusing on cyber security for industrial control systems (ICS) and critical infrastructure. Prior to joining Mandiant, Chris was a Senior Engineer at

Entergy (over 11 years) where he was the Subject Matter Expert (SME) for SCADA systems. He has 10 years of experience in SCADA systems with tasks such as standards development, system design, database configuration, testing, commissioning, troubleshooting, and training. He was the co-overseer of the SCADA, relay, and cyber security labs at Entergy for 6 years. Chris has been working with Adam Crain of Automatak on Project Robus, an ICS protocol fuzzing project that has found and helped fix many implementation vulnerabilities in DNP3, Modbus, and Telegyr 8979.

Chris helped organize the first ICS Village, which debuted at DEF CON 22.

He is a Senior Member of IEEE, Mississippi Infragard President, member of the DNP Users Group, and also is a registered PE in Louisiana. He holds a BS in Electrical Engineering and MS in Engineering and Technology Management from Louisiana Tech University. Chris also founded and organizes BSidesJackson, Mississippi's only cyber security conference.

Twitter: @chrissistrunk
https://www.facebook.com/chrissistrunk

Beyond the Scan: The Value Proposition of Vulnerability Assessment

Damon Small, Security Researcher

Vulnerability Assessment is, by some, regarded as one of the least "sexy" capabilities in information security. However, it is the presenter's view that it is also a key component of any successful infosec program, and one that is often overlooked. Doing so serves an injustice to the organization and results in many missed opportunities to help ensure success in protecting critical information assets. The presenter will explore how Vulnerability Assessment can be leveraged "Beyond the Scan" and provide tangible value to not only the security team, but the entire business that it supports.

Damon Small began his career studying music at Louisiana State University. Pursuing his desire to actually make money, he took advantage of computer skills learned in the LSU recording studio to become a systems administrator in the mid 1990s. Following the dotcom bust in the early 2000s, Small began focusing on cyber security. This has remained his passion, and over the past 15 years as a security professional he has supported infosec initiatives in the healthcare, defense, and oil and gas industries. In addition to his Bachelor of Arts in Music, Small completed the Master of Science in Information Assurance degree from Norwich University in 2005.

Twitter: @damonsmall

The Bieber Project: Ad Tech 101, Fake Fans and Adventures in Buying Internet Traffic

Mark Ryan Talabis, Chief Security Scientist, zVelo

In the past year, I found myself immersed in the multi-billion dollar digital advertising industry. This gave me the opportunity to investigate the unique security challenges and issues facing the industry. It was a shock to me at first how complex the advertising ecosystem was particularly in the advent of programmatic advertising. But I dove in head first and learned a lot which I would like to share with my fellow security professionals. During this time, I got involved with unscrupulous publishers, apathetic ad networks, angry advertisers and activist malware researchers. I encountered self proclaimed experts with fantastic claims, vendors using scare tactics, and a glaring disconnect between the security and ad tech worlds.

In this presentation, I would like to be able to provide the audience with my experience plus a number of things. Among which are:

- Provide security professionals a 101 type of introduction to the world of digital advertising ecosystem. Among the things we will tackle is what is programmatic advertising, what the roles are of the different players like ad networks are and how money is made off all this interplay.
- Provide the audience a perspective on what security challenges the advertising industry is facing and opportunities for us security professionals to be involved. We all know about malvertising and its a big deal to us security guys but there are bigger, and in an advertisers perspective, more relevant issues that needs to be taken care of first. All of this will be discussed in this talk.
- An introduction about the different and creative ways unscrupulous publishers can pad their earnings. We will be talking about hidden ads, ad stacking, intrusive ads, auto-refreshes, popups, popunders, blackhat SEO techniques and dirty inventory.
- An in depth discussion on the problems caused by non-human traffic (NHT). We will talk about what it is, why is it a problem, how it is generated, and more importantly, how do we catch it? In fact, this presentation is named the "Bieber Project" which is the experiment which I leveraged to understand non-human traffic and determine how we can identify it.

Mark Ryan Talabis is the Chief Security Scientist for zVelo Inc where he conducts research on advertising fraud and non-human traffic. He is also formerly the Director of the Cloud Business Unit of FireEye. He is an alumni member of the Honeynet Project and a member of the anti-malware working group of the Interactive Advertising Bureau (IAB) where he is contributing in the promotion of threat intel sharing across the advertising industry.

His current work focuses on helping the advertisers and ad networks in finding ways to identify non-human traffic through various browser impression and behavioral based anomaly detection techniques. This also includes work on detecting various impression and click padding techniques by unscrupulous publishers.

He is a graduate of Harvard University and is a co-author of two books from Elsevier Syngress: "Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data" (2014) and "Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis" (2012). Techniqies He has presented in various security and academic conferences and organizations around the world including Blackhat, DEF CON, Shakacon, INFORMS, INFRAGARD, ISSA, and ISACA.

Hijacking Arbitrary .NET Application Control Flow

Topher Timzen, Security Researcher - Intel

This speech will demonstrate attacking .NET applications at runtime. I will show how to modify running applications with advanced .NET and assembly level attacks that alter the control flow of any .NET application. New attack techniques and tools will be released to allow penetration testers and attackers to carry out advanced post exploitation attacks.

This presentation gives an overview of how to use these tools in a real attack sequence and gives a view into the .NET hacker space.

Topher Timzen has had a research emphasis on reverse engineering malware, incident response and exploit development. He has instructed college courses in malware analysis and memory forensics while managing a cybersecurity research lab. Focusing on .NET memory hijacking, he has produced tools that allow for new post exploitation attack sequences. Topher is currently a Security Researcher at Intel.

Twitter: @TTimzen

Hackers Hiring Hackers - How to Do Things Better

Tottenkoph, Security Consultant, Rapid7
IrishMASMS, Hacker

There are a lot of talks about how to be a better pen tester and workshops that show you how to use all of the cool new tools that are available to make our jobs easier, but there are only a few talks that address what some of us consider to be the hardest part of getting a job in security: the hiring process. The information security field is in desperate need of people with the technical skills hackers have to fill a myriad of roles within organizations across the world. However, both sides of the table are doing horribly when it comes to hiring and interviewing for work.

Organizations are doing poorly trying to communicate expectations for a job, there are people going to interviews without knowing how to showcase their (limited or vast) experience, and some people posture themselves so poorly that the hiring managers don't think the candidates are really interested in the job. This talk takes the experiences of the speakers as both interviewers and interviewees as well as from others within the scene in order to help better prepare hackers to enter (or move within) "the industry" as well as let the people making hiring decisions know what they can do to get the people and experience they need for their teams.

Tottenkoph has been hacking for the past 10 years and is currently a security consultant for Rapid7. Tottie has spoken at several hacker cons and is currently pursuing her Master's degree in Industrial and Organizational Psychology, planning to apply its practices to the hacker and infosec communities.

Twitter: @Tottenkoph

IrishMASMS is an old school hacker, fighting the good fight in Computer Network Defence (CND)/blue team efforts for over 16 years. Been lurking about since DEF CON 10, DJing the B&W ball at DEF CON 18 (with quite a few AP pool shindigs and private parties along the way). Panel member at HOPE 5, presenter at a couple of Notacon's, and some other conferences that are hard to remember what really happened. Having progressed through the ranks to hiring manager and director level, he has experienced the pain from both sides of the hiring process and desires to improve the situation for the InfoSec community. Is this where we mention cyberderp?

Twitter: @IrishMASMS

QARK: Android App Exploit and SCA Tool

Tony Trummer, Staff Information Security Engineer/LinkedIn
Tushar Dalvi, Sr. Security Engineer/LinkedIn

Ever wonder why there isn't a metasploit-style framework for Android apps? We did! Whether you're a developer trying to protect your insecure app from winding up on devices, an Android n00b or a pentester trying to pwn all the things, QARK is just what you've been looking for! This tool combines SCA, teaching and automated exploitation into one, simple to use application!

Tony Trummer (@SecBro1) - has been working in the IT industry for nearly 20 years and has been focused on application security for the last 5 years. He is currently an in-house penetration tester for LinkedIn, running point on their mobile security initiatives and has been recognized in the Android Security Acknowledgements. When he's not hacking, he enjoys thinking about astrophysics, playing devil's advocate and has been known to dust his skateboard off from time-to-time.

Twitter: @SecBro1
LinkedIn: www.linkedin.com/in/tonytrummer

Tushar Dalvi (@tushardalvi) - Loves breaking web applications and ceramic bowls. Tushar Dalvi is a security enthusiast, and currently works as a Senior Information Security Engineer at LinkedIn. He specializes in the area of application security, with a strong focus on vulnerability research and assessment of mobile applications. Previously, Tushar has worked as a security consultant at Foundstone Professional Services (McAfee) and as a Senior developer at ACI Worldwide.

Twitter: @tushardalvi
LinkedIn: www.linkedin.com/in/tdalvi

Hacking Web Apps

Brent White, Security Consultant, Solutionary, Inc.

Assessing the security posture of a web application is a common project for a penetration tester and a good skill for developers to know. In this talk, I'll go over the different stages of a web application pen test, from start to finish. We'll start with the discovery phase to utilize OSINT sources such as search engines, sub-domain brute-forcing and other methods to help you get a good idea of targets "footprint", all the way to fuzzing parameters to find potential SQL injection vulnerabilities. I'll also discuss several of the tools and some techniques that I use to conduct a full application penetration assessment. After this talk, you should have a good understanding of what is needed as well as where to start on your journey to hacking web apps.

Brent is an Offensive Security Consultant at Solutionaryâ€¹An NTT Group Security Company and has spoken at numerous security conferences, including DEF CON 22â€¹SE Village. He has held the role of Web/Project Manager and IT Security Director at the headquarters of a global franchise company. His experience includes Internal and External Penetration Assessments, Social Engineering and Physical Security Assessments, Wireless and Application Vulnerability Assessments and more.

Twitter: @BrentWDesign

And That's How I Lost My Other Eye: Further Explorations In Data Destruction

Zoz, Robotics Engineer and Security Researcher

How much more paranoid are you now than you were four years ago? Warrantless surveillance and large-scale data confiscation have brought fear of the feds filching your files from black helicopter territory into the mainstream. Recent government snatch-and-grabs have run the gamut from remotely imaging foreign servers to straight up domestic coffeeshop muggings, so if you think you might need to discard a lot of data in hurry you're probably right. In their legendary DEF CON 19 presentation Shane Lawson, Bruce Potter and Deviant Ollam kicked off the discussion, and now it's time for another installment. While purging incriminating material residing on spinning disks remains the focus, the research has been expanded to encompass solid state storage and mobile solutions to your terabyte trashing needs. With best efforts to comply with the original constraints, the 2015 update features more analysis of the efficacy of kinetic projectiles, energetic materials and high voltages for saving your freedom at the potential cost of only a redundant body part... or two.

Zoz is a robotics engineer, rapid prototyping specialist and lifelong enthusiast of the pyrotechnic arts. Once he learned you could use a flamethrower and a coffee creamer bomb to fake a crop circle for TV he realized there are really no limits to creative destruction.

Malware in the Gaming Micro-economy

Zack Allen, Lead Research Engineer, ZeroFOX
Rusty Bower, Information Security Engineer

Microeconomics focuses on how patterns of supply and demand determine price and output in individual markets [1]. Within recent years, micro-economies have flourished within the video game industry. Companies like Valve rely heavily on a business model that depends on gamers making purchases for in-game items. Players can trade these items in bulk for a rare item, make bets on a competitive gaming match or gift the item for a charity event.

While originally well-intentioned, creating these micro-economies also created an incentive for criminals to scam and even steal from unsuspecting victims. Traditional scams date as far back to games like Diablo or Runescape where players were duped in trade windows and in game messaging systems were used to steal items. These low-tech strategies are effective, but recently a new, high-tech scam strategy has emerged relying upon malware specifically targeting the Steam micro-economy.

Over the last year, we have collected and reversed dozens of samples of malware that target Steam users. Pieces of malware can be sophisticated RAM scrapers that pilfer an item in memory and send trade requests through the Steam trading API, or as simple as a remote login service. The end result is the same - the hacker loots the victim's backpack of in game items to sell them on the market for profit. This talk focuses on the techniques we have found in these samples, surveys of victims of these scams and the distribution of money lost from them (up to the $1000s of dollars for users in some cases) and the defenses Steam has put in place to combat this hacker underground.

Zack Allen is an RIT graduate, majoring in Information Security. He is also an alum of the Advanced Course for Engineering (ACE) held at AFRL every summer. After working for a government contractor, he joined the exciting startup world and is currently a Research team lead at ZeroFOX. His security specialties include research and development, threat intelligence, tool creation and red teaming.

Rusty Bower graduated from the Rochester Institute of Technology with a degree in Information Security. He has been employed at Lockheed Martin and Palantir Technologies tackling a variety of security challenges. His experience is mainly focused in security operations, incident response, tool development, and infrastructure management. He is currently an Information Security Engineer in the Los Angeles area, tackling security challenges at scale.

How to secure the keyboard chain

Paul Amicelli, Student from IT Engineering School - ESIEA in Laval, France
Baptiste David, Engineer from IT Engineer School - ESIEA in Laval, France

Keyloggers are hardware or software tools that record keystrokes. They are an overlooked threat to the computer security and user's privacy. As they are able to retrieve all sensitive information typed on a keyboard in an almost invisibly way , they need to be seriously considered both for companies and individuals. Almost all the security measures against keyloggers are post-active and static.

*So what if the solution were to be proactive, and use the same technology as keyloggers do, in order to fool them ? This is all about this presentation, a way of fooling all known and unknown keyloggers (physicals, kernel-mode and user-mode) through a kernel mode driver developed under Windows. The technical details will be presented during the presentation, as well as the results and propositions.

Basically, the idea is to use a kernel mode driver which encrypts each keyboard key hit, at a very low level in the system (near the driver port). The encryption is made according to a common key, exchanged with a client application which needs to ensure that the entered text is secured and not recorded. After the driver has encrypted a key, it spreads it to the entire system. Thus, only the client application, holding the encryption key, can decrypt the keyboard key. In this way, the whole system is fooled.

Paul Amicelli is a French engineering student at ESIEA, an IT Engineering School in Laval, France. Fascinated by the world of computer security, he is currently involved as a student researcher in the Operational Cryptology and Virology research lab of its school, where some projects like the encryption solution Gostcrypt, in which he is taking part of, are developed. Prior to that, he has done a two-year preparatory class for the Grandes Ecoles in mathematics and physics (CPGE).

Baptiste David is a computer science engineer who has been working for the CVO laboratory for many years. His research areas are based on operational and offensive computer security for protection of critical systems. He is specialized n reverse engineering, kernel development and malware analysis. He has especially worked on GostCrypt and many antivirus project for many years. He made numerous conferences all over the world about security and offensive techniques.

How to hack your way out of home detention

AmmonRa, Security Researcher

Home detention and criminal tracking systems are used in hostile environments, and because of this, the designers of these trackers incorporate a range of anti-removal and tamper detection features. Software security, however, is an area on which less focus is placed.

This talk will cover practical attacks against home detention tracking systems, with a focus on software security. Intercepting and modifying tracking information sent from the device in order to spoof the tracker's location will be demonstrated.

General information about how home detention tracking systems operate will be discussed, including the differences between older proximity based systems which used landlines, and newer models which use GPS and cellular networks. Topics will include how to (legally) get hold of and test a real world device, and how to use cheap software defined radios to spoof GSM cell towers. Focus will be on the details of how one particular device is constructed, how it operates and the vulnerabilities it was found to contain. How these vulnerabilities can be exploited and the challenges of doing so in the wild will also be covered.

AmmonRa is a former dev who now works in infosec as a pentester. Both at work and in his spare time AmmonRa hacks things. As well as hacking computers, AmmonRa is a DIY cyborg, designing and implanting in himself a range of devices, including NFC/RFID chips, biometric sensors and subdermal lights.

Twitter: @amm0nra

Fun with Symboliks

atlas, dude at Grimm

Asking the hard questions... and getting answer! Oh binary, where art thine vulns?

Symbolic analysis has been a "thing" for 20 years, and yet it's still left largely to the obscure and the academic researchers (and NASA). several years ago, Invisigoth incorporated the Symboliks subsystem into the Vivisect binary analysis framework. due to that inclusion, the very nature of binary analysis has been broken down, rethought, and arisen out of the ashes. this talk will give an introduction into Symboliks, Graph Theory, and the path forward for reverse engineering and vulnerability research, all from an interactive Python session or scripts.

A four time winner of DEF CON capture the flag and retired captain of the team "1@stplace", over the past decade atlas has proved expertise in programmatic reverse-engineering, automated vulnerability discovery and exploitation, and braking into or out of nearly every type of computer system/subsystem. areas of specialty include exmpedded/IoT exploitation, power systems and industrial control systems exploitation, automotive exploitation, and client/server/application exploitation.
Twitter: @at1as

Quantum Computers vs. Computers Security

Jean-Philippe Aumasson, Principal Cryptographer, Kudelski Security, Switzerland

We've heard about hypothetical quantum computers breaking most of the public-key crypto in use-RSA, elliptic curves, etc.-and we've heard about "post-quantum" systems that resist quantum computers. We also heard about quantum computers' potential to solve other problems considerably faster than classical computers, such as discrete optimization, machine learning, or code verification problems. And we heard about a commercial quantum computer, and we heard vendors of quantum key distribution or quantum random number generators promise us security as solid as the laws of physics. Still, most of us are clueless regarding:

- How quantum computers work and why they could solve certain problems faster than classical computers?
- What are the actual facts and what is FUD, hype, or journalistic exaggeration?
- Could quantum computers help in defending classical computers and networks against intrusions?
- Is it worth spending money in post-quantum systems, quantum key distribution, or in purchasing or developing of a quantum computer?
- Will usable quantum computers be built in the foreseeable future?

This talk gives honest answers to those questions, based on the latest research, on analyses of the researchers' and vendors' claims, and on a cost-benefit-risk analyses. We'll expose the fundamental principles of quantum computing in a way comprehensible by anyone, and we'll skip the technical

details that require math and physics knowledge. Yet after this talk you'll best be able to assess the risk of quantum computers, to debunk misleading claims, and to ask the right questions.

Jean-Philippe (JP) Aumasson is Principal Cryptographer at Kudelski Security, in Switzerland. He is known for designing the cryptographic functions BLAKE, BLAKE2, SipHash, and NORX. He has spoken at conferences such as Black Hat, RSA, and CCC, and initiated the Crypto Coding Standard and the Password Hashing Competition projects. He co-wrote the 2015 book "The Hash Function BLAKE". He is member of the technical advisory board of the Open Crypto Audit Project and of the Underhanded Crypto Contest. JP tweets as @veorq.

Twitter: @veorq

Key-Logger, Video, Mouse - How To Turn Your KVM Into a Raging Key-logging Monster

Yaniv Balmas, Security Researcher, Check Point Software Technologies
Lior Oppenheim, Security Researcher, Check Point Software Technologies

Key-Loggers are cool, really cool. It seems, however, that every conceivable aspect of key-logging has already been covered: from physical devices to hooking techniques. What possible innovation could be left in this field?

Well, that's what we used to think too. That is until we noticed that little grey box sitting there underneath a monitor, next to yesterday's dirty coffee cup. The little grey box that is most commonly known as 'KVM'.

The talk will tell the tale of our long journey to transform an innocent KVM into a raging key-logging monster. We will safely guide you through the embedded wastelands, past unknown IC's, to explore uncharted serial protocols and unravel monstrous obfuscation techniques.

Walking along the misty firmware woods of 8051 assembly we will challenge ambiguous functions and confront undebuggable environments.

Finally, we will present a live demo of our POC code and show you that air-gapped networks might not be as segregated as you imagined.

You will witness that malware code could actually reside outside your computer, persisting through reboots, wipes, formats, and even hardware replacements. You might laugh, you might cry, but one thing is certain - you will never look at your KVM the same as before.

Yaniv is a software engineer and a seasoned professional in the security field. He wrote his very first piece of code in BASIC on the new Commodore-64 he got for his 8th birthday. As a teenager, he spent his time looking for ways to hack computer games and break BBS software. This soon led to diving into more serious programming, and ultimately, the security field where he has been ever since. Yaniv is

currently working as a security researcher and deals mainly with analyzing malware and vulnerability research

Twitter: @ynvb

Lior Oppenheim is a vulnerability researcher in the Malware and Vulnerability Research group at Check Point Software Technologies. Oppenheim was trained and served in an elite technological unit performing security research in the IDF. In his spare time, he loves tap dancing, reversing, playing his guitar and pwning embedded devices.

Twitter: @oppenheim1

Canary: Keeping Your Dick Pics Safe(r)

Rob Bathurst (evilrob), Security Engineer and Penetration Tester
Jeff Thomas (xaphan), Senior Cyber Security Penetration Testing Specialist

The security of SSL/TLS is built on a rickety scaffolding of trust. At the core of this system is an ever growing number of Certificate Authorities that most people (and software) take for granted. Recent attacks have exploited this inherent trust to covertly intercept, monitor and manipulate supposedly secure communications. These types of attack endanger everyone, especially when they remain undetected. Unfortunately, there are few tools that non-technical humans can use to verify that their HTTPS traffic is actually secure.

We will present our research into the technical and political problems underlying SSL/TLS. We will also demonstrate a tool, currently called "Canary", that will allow all types users to validate the digital certificates presented by services on the Internet.

Evilrob is a Security Engineer and Penetration Tester with over 14 years of experience with large network architecture and engineering. His current focus is on network security architecture, tool development, and high-assurance encryption devices. He currently spends his days contemplating new and exciting ways to do terrible things to all manner of healthcare related systems in the name of safety.

Twitter: @knomes

xaphan is a "Senior Cyber Security Penetration Testing Specialist" for a happy, non-threatening US government agency. He has been a penetration tester for 17 years, but maintains his sanity with a variety of distractions. He is the author of several ancient and obsolete security tools and the creator of DEFCOIN.

Twitter: @slugbait

Extracting the Painful (blue)tooth

Matteo Beccaro
Matteo Collura

Do you know how many Bluetooth-enabled devices are currently present in the world? With the beginning of the IoT (Internet of Things) and Smart Bluetooth (Low energy) we find in our hands almost a zillion of them. Are they secure? What if I tell you I can unlock your Smartphone? What if I tell you I'm able to open the new shiny SmartLock you are using to secure your house's door?

In this talk we will explain briefly how the Bluetooth (BDR/EDR/LE) protocols work, focusing on security aspects. We will show then some known vulnerabilities and finally we will consider deeply undisclosed ones, even with live demonstrations.

Matteo Beccaro is a young security researcher. His interest focus on WiFi networks, networking and NFC implementations. He finished high school studies in July 2013 and actually he is a student at Politecnico di Torino in Computer Engineering course.

He has been selected as speaker at DEF CON 21, 30C3, BlackHat US Arsenal, DEF CON 22's Skytalks and BlackHat EU 2014 and Tetcon, for his research in vulnerabilities of NFC transport systems.

Since 2013 he is also pentester and security engineer at Secure Network s.r.l. Since 2015 he is also technical leader of the Security Research Team of OPFOR, the physical security division of Secure Network s.r.l.

*Twitter: @_bughardy_*

Matteo Collura is a student of Electronics Engineering at Politecnico di Torino. He has been studying Wireless networks and in the last few years he focused on NFC. He presented the results of a progressive work of research at several conferences: DEF CON 21 (Las Vegas, 2013), 30C3 (Hamburg 2013), DEF CON Skytalks (Las Vegas, 2014), BlackHat USA 2014 Arsenal (Las Vegas). Currently he is studying Bluetooth protocols and their implementations.
Twitter: @eagle1753

802.11 Massive Monitoring

Andres Blanco, Sr Researcher, Core Security
Andres Gazzoli, Sr Developer, Core Security

Wireless traffic analysis has been commonplace for quite a while now, frequently used in penetration testing and various areas of research. But what happens when channel hopping just doesn't cut it anymore -- can we monitor all 802.11 channels?

In this presentation we describe the analysis, different approaches and the development of a system to monitor and inject frames using routers running OpenWRT as wireless workers. At the end of this presentation we will release the tool we used to solve this problem.

Andres Blanco is a researcher at CoreLabs, the research arm of Core Security. His research is mainly focused on wireless, network security and privacy. He has presented at Black Hat USA Arsenal, Hacklu and Ekoparty, and has published several security advisories.

Twitter: @6e726d

Andres Gazzoli works at Core Security and is part of the Core Impact Pro developer team. He is a C++ developer with extensive experience in UI development. He enjoys everything related to wireless technologies and privacy.

Exploring Layer 2 Network Security in Virtualized Environments

Ronny L. Bull, Ph.D. Graduate Student, Clarkson University
Jeanna N. Matthews, Associate Professor, Clarkson University

Cloud service providers offer their customers the ability to deploy virtual machines in a multi-tenant environment. These virtual machines are typically connected to the physical network via a virtualized network configuration. This could be as simple as a bridged interface to each virtual machine or as complicated as a virtual switch providing more robust networking features such as VLANs, QoS, and monitoring. In this paper, we explore whether Layer 2 network attacks that work on physical switches apply to their virtualized counterparts by performing a systematic study across four major hypervisor environments - Open vSwitch, Citrix XenServer, Microsoft Hyper-V Server and VMware vSphere - in seven different virtual networking configurations. First, we use a malicious virtual machine to run a MAC flooding attack and evaluate the impact on co-resident VMs. We find that network performance is degraded on all platforms and that it is possible to eavesdrop on other client traffic passing over the same virtual network for Open vSwitch and Citrix XenServer. Second, we use a malicious virtual machine to run a rogue DHCP server and then run multiple DHCP attack scenarios. On all four platforms, co-resident VMs can be manipulated by providing them with incorrect or malicious network information.

Mr. Bull is a Computer Science Ph.D. graduate student at Clarkson University focusing on Layer 2 network security in virtualized environments. He presented his preliminary research involving MAC flooding attacks against virtualized networks at the DerbyCon 4.0 computer security conference held in Louisville, KY in September 2014. Mr. Bull earned an A.A.S. degree in Computer Networking at Herkimer College in 2006 and completed both a B.S. and M.S. in Computer Science at the State University of New York Institute of Technology in 2011. He was a founding faculty member of the School of Engineering at SUNY Polytechnic Institute in Utica, NY teaching undergraduate and graduate courses in both the Network and Computer Security and Telecommunications programs, and also served as an advisor to the SUNY Poly Network and Computer Security club. Mr. Bull recently made a transition to Utica College as an Assistant Professor of Computer Science with a focus in networking and cybersecurity. He also co-founded and is one of the primary organizers of the Central New York

Intercollegiate Hackathon event which brings together local cybersecurity students from colleges in Central New York to compete against each other in offensive and defensive cybersecurity activities.

Dr. Matthews is an Associate Professor of Computer Science at Clarkson University. Her research interests include virtualization, cloud computing, computer security, computer networks and operating systems. Jeanna received her Ph.D. in Computer Science from the University of California at Berkeley in 1999. She is currently the chair of the ACM Special Interest Group on Operating Systems (SIGOPS), the co-editor of ACM Operating System Review and a member of the Executive Committee of US-ACM, the U.S. Public Policy Committee of ACM. She has written several popular books including "Running Xen: A Hands-On Guide to the Art of Virtualization" and "Computer Networking: Internet Protocols In Action".

Attacking Hypervisors Using Firmware and Hardware

Yuriy Bulygin, Advanced Threat Research, Intel Security
Mikhail Gorobets, Advanced Threat Research, Intel Security
Alexander Matrosov, Advanced Threat Research, Intel Security
Oleksandr Bazhaniuk, Advanced Threat Research, Intel Security
Andrew Furtak, Security Researcher

In this presentation, we explore the attack surface of modern hypervisors from the perspective of vulnerabilities in system firmware such as BIOS and in hardware emulation. We will demonstrate a number of new attacks on hypervisors based on system firmware vulnerabilities with impacts ranging from VMM DoS to hypervisor privilege escalation to SMM privilege escalation from within the virtual machines.

We will also show how a firmware rootkit based on these vulnerabilities could expose secrets within virtual machines and explain how firmware issues can be used for analysis of hypervisor-protected content such as VMCS structures, EPT tables, host physical addresses (HPA) map, IOMMU page tables etc. To enable further hypervisor security testing, we will also be releasing new modules in the open source CHIPSEC framework to test issues in hypervisors when virtualizing hardware.

Mikhail Gorobets is a security researcher in the Advanced Threat Research team. His area of expertise includes hardware security, virtualization technologies, reverse engineering, and vulnerability analysis. Previously, he led a team of security researchers working on Intel Virtualization Technology (VTx) and Intel Atom core security evaluation. Mikhail holds a MS in computing machines, systems, and networks from the Moscow Institute of Electronics and Mathematics.

Alexander Matrosov has more than ten years of experience with malware analysis, reverse engineering, and advanced exploitation techniques. He is currently a senior security researcher in the Advanced Threat Research team at Intel Security Group. Prior to this role, he spent four years focused on advanced malware research at ESET. He is co-author of numerous research papers, including "Stuxnet Under the Microscope," "The Evolution of TDL: Conquering x64," and "Mind the Gapz: The most complex bootkit ever analyzed?". Alexander is frequently invited to speak at security conferences such as REcon, Ekoparty, Zeronigths, AVAR, CARO, and Virus Bulletin. Nowadays, he specializes in

the comprehensive analysis of advanced threats, modern vectors of exploitation, and hardware security research.

Oleksandr Bazhaniuk is a security researcher in the Advanced Threat Research team. His primary interests are low-level hardware security, bios/uefi security, and automation of binary vulnerability analysis. His work has been presented at world-renowned conferences, including Black Hat USA, Hack In The Box, Hackito Ergo Sum, Positive Hack Days, Toorcon, CanSecWest. He is also a co-founder of DCUA, the first DEF CON group in Ukraine.

Andrew Furtak is a security researcher focusing on security analysis of firmware and hardware of modern computing platforms. He was previously a security software engineer. Andrew holds a MS in applied mathematics and physics from the Moscow Institute of Physics and Technology.

Yuriy Bulygin is chief threat researcher at Intel Security Group where he is leading the Advanced Threat Research team in identifying and analyzing new threats impacting modern platforms and researching mitigations in hardware and software against these threats. He joined Intel's Security Center of Excellence in 2006, where he was responsible for conducting security analysis and penetration testing of microprocessors, chipsets, graphics, and various other components, firmware, and technologies on Intel PCs, servers, and mobile devices. Yuriy is also a member of the core security architecture team reviewing Intel's future products. Prior to joining Intel, he was teaching undergrad seminars in information security at Moscow Institute of Physics and Technology.
Twitter: @c7zero

Who Will Rule the Sky? The Coming Drone Policy Wars

Matt Cagle, Technology and Civil Liberties Policy Attorney, ACLU of Northern California
Eric Cheng, General Manager, DJI SF and Director of Aerial Imaging, DJI

Your private drone opens up limitless possibilities - how can manufacturers and policymakers ensure you are able to realize them? As private drone ownership becomes the norm, drone makers and lawmakers will need to make important policy decisions that account for the privacy and free speech issues raised by this new technology. What legal and technical rules are being considered right now, and how might they affect your ability to do things like record footage at a city park, monitor police at a protest, or fly near a government building? These decisions will dictate the technical limitations (or lack thereof) placed on drones, and the legal consequences of operating them. Join Eric Cheng, General Manager of DJI SF and DJI's Director of Aerial Imaging, and Matt Cagle, a Technology and Civil Liberties Policy Attorney with the ACLU of Northern California, to discuss the policy issues at this leading edge of law and consumer technologies.

Matt Cagle is a Technology and Civil Liberties Policy Attorney at the ACLU of Northern California. At the ACLU-NC, Matt's work focuses on the privacy and free speech issues raised by new services and technologies, including surveillance equipment, social media services, and connected devices. Last fall, Matt co-authored Making Smart Decisions About Surveillance: A Guide for Communities, a paper that provides a framework for communities considering surveillance technology proposals. Matt has worked in private practice advising technology companies on the privacy issues related to new products and

services. Matt has substantial experience responding to state and federal law enforcement requests for online user information, and he co-authored reddit's first ever transparency report. Matt regularly speaks at conferences ranging from SXSW to RightsCon, and he served on the privacy committee for Oakland's controversial surveillance complex, the Domain Awareness Center. He grew up in Southern Arizona, studied Latin American history in Guatemala, and holds a JD from Stanford Law School.

Twitter: @matt_cagle

Eric Cheng is an award-winning photographer and publisher, and is the Director of Aerial Imaging and General Manager of the San Francisco office at DJI, the creators of the popular Phantom aerial-imaging quadcopter. Throughout his career, Cheng has straddled passions for photography, entrepreneurship, technology and communication. He publishes Wetpixel.com, the leading underwater-photography community on the web, and writes about his aerial-imaging pursuits at skypixel.org. His work as a photographer has been featured at the Smithsonian's Natural History Museum and in many media outlets including Wired, Outdoor Photographer, Popular Photography, Washington Post, Wall Street Journal, Make, ABC, Good Morning America, CBS, CNN and others. His video work has been shown on the Discovery Channel, National Geographic Channel, and on virtually every news network around the world.

Caught between technical and creative pursuits, Eric holds bachelor's and master's degrees in computer science from Stanford University, where he also studied classical cello performance. He leads regular photography expeditions and workshops around the world, and has given seminars and lectures internationally at events including TEDx, the Churchill Club, Photoshelter Luminance, CES, SXSW, AsiaD, DEMA, and others.

Twitter: @echeng

Switches Get Stitches

Colin Cassidy, Senior Security Consultant at IOActive
Éireann Leverett
Robert M. Lee

This talk will introduce you to Industrial Ethernet Switches and their vulnerabilities. These are switches used in industrial environments, like substations, factories, refineries, ports, or other homes of industrial automation. In other words: DCS, PCS, ICS & SCADA switches.

The researchers focus on attacking the management plane of these switches, because we all know that industrial system protocols lack authentication or cryptographic integrity. Thus, compromising any switch allows the creation of malicious firmwares for further MITM manipulation of a live process. Such MITM manipulation can lead to the plant or process shutting down (think: nuclear reactor SCRAM) or getting into a unknown and hazardous state (think: damaging a blast furnace at a steel mill)

Not only will vulnerabilities be disclosed for the first time, but the methods of finding those vulnerabilities will be shared. All vulnerabilities disclosed will be in the default configuration state of the devices. While

these vulnerabilities have been responsibly disclosed to the vendors, SCADA/ICS patching in live environments tends to take 1-3 years. Because of this patching lag, the researchers will also be providing live mitigations that owner/operators can use immediately to protect themselves. At least four vendors switches will be examined: Siemens, GE, Garrettcom and Opengear.

Colin Cassidy is a security consultant for IOActive where he focuses on Industrial Control Systems. He has a strong development and software engineering background. He is also a seasoned leader in the areas of security and software engineering. Before joining IOActive, Cassidy served for a number of years as Technical Manager and Security Technical Lead for IGE Energy Services, Ltd, part of GE Energy. He has hands-on experience with PowerOn Fusion, a leading Outage Management System/Distribution Management System (OMS/DMS) solution for electricity distribution management. He also led a team of developers in producing new functionality within the core product and worked with customers to understand their requirements. Colin Cassidy has a BSc (Hons) in Computing Science from the University of Glasgow.
Twitter: @parttimesecguy

Éireann Leverett hates writing bios in the third person. He once placed second in an Éireann Leverett impersonation contest. He likes teaching the basics, and learning the obscure. He is sometimes jealous of his own moustache for being more famous than he is. If he could sum up his life in one sentence; he wouldn't. That would be a life-sentence! He is primarily known for smashing the myth of the air-gap in industrial systems with his master's thesis, finding authentication bypasses for industrial ethernet switches, and working with incident response teams to improve their understanding of industrial control systems security. He believes security takes an awful lot more than penetration-testing and speaks often about the wider effects of embedded system insecurity.
Twitter: @blackswanburst

Robert M. Lee is a co-founder of Dragos Security LLC where he has a passion for control system protocol analysis, digital forensics, and threat intelligence research. He is also an active-duty U.S. Air Force Cyber Warfare Operations Officer where he has been a member of multiple computer network defense teams including his establishing and leading of a first-of-its-kind ICS/SCADA threat intelligence and intrusion analysis mission. Robert received his BS from the United States Air Force Academy and his MS in Cybersecurity Digital Forensics from Utica College. He is a passionate educator and teaches in the ICS and Forensics programs at SANS and is an Adjunct Lecturer at Utica College where he teaches in their MS Cybersecurity program. Robert is also the author of 'SCADA and Me' and is currently pursuing his PhD at Kings College London with research in control system cyber security. He routinely publishes academic and industry focused works in a wide variety of journals and publications; additionally he has presented at conferences around the world.
Twitter: @RobertMLee

Cracking Cryptocurrency Brainwallets

Ryan Castellucci, Security Researcher, White Ops

Imagine a bank that, by design, made everyone's password hashes and balances public. No two-factor authentication, no backsies on transfers. Welcome to "brainwallets", a way for truly paranoid cryptocurrency users to wager their fortunes on their ability to choose a good password or passphrase. Over the last decade, we've seen the same story play out dozens of times - a website is broken into, the user database is posted online, and most of the password hashes are cracked. Computers are now able make millions, billions or even trillions of guesses per second. Every eight character password you can type on a standard keyboard and every combination of five common english words could be tried in less than a day by today's botnets. Can people come up with passphrases able to stand up to that when money is on the line? Let's find out.

For this talk, I will be releasing my high speed brainwallet cracker, "Brainflayer". I'll cover a history of brainwallets, safer passphrase-based wallet generation, passphrase security, in-the-wild cracking activity, and how I accidently stole 250 Bitcoins (and tracked down the owner to give them back).

Ryan Castellucci has been interested in cryptography since childhood when his parents gave him a copy of "Codes, Ciphers and Secret Writing". He soon learned to program and wrote a tool to crack simple substitution ciphers. More recently, he co-spoke with Dan Kaminsky at DEF CON 22 and was a finalist in the 2014 Underhanded Crypto Contest. For his day job at White Ops, he finds new and exciting ways to tease out the subtle differences between bots and human-controlled web browsers.
Twitter: @ryancdotorg
Web: https://rya.nc

Paranoia and ProxyHam: High-Stakes Anonymity on the Internet

Benjamin Caudill, Founder, Rhino Security Labs
CANCELLED
From the US to China and beyond, anonymity on the internet is under fire - particularly for whistleblowers. National interests are pushing for greater control and monitoring of internet content, often invoking harsh punishments for informers and journalists, if caught. While a range of technologies (such as ToR) can provide some level of anonymity, a fundamental flaw still exists: a direct relationship between IP address and physical location. If your true IP is ever uncovered, it's game over - a significant threat when your adversary owns the infrastructure.

To resolve this issue, I present ProxyHam, a hardware device which utilizes both WiFi and the 900Mhz band to act as a hardware proxy, routing local traffic through a far-off wireless network - and significantly increasing the difficulty in identifying the true source of the traffic. In addition to a demonstration of the device itself, full hardware schematics and code will be made freely available.

Benjamin Caudill is founder and Principal Consultant of Rhino Security Labs, an information security consultancy in Seattle, WA. As a security professional, Benjamin has broken and secured environments from mobile startups to government agencies and Fortune 500's. His security research and exploits have been published in Wired Magazine, CNN, CNET, Forbes and Geekwire, as well as presented at security conferences such as DEF CON 21.

Why nation-state malwares target Telco Networks: Dissecting technical capabilities -Regin and its counterparts

Omer Coskun, Ethical Hacker with KPN REDteam, KPN (Royal Dutch Telecom)

The recent research in malware analysis suggests state actors allegedly use cyber espionage campaigns against GSM networks. Analysis of state-sponsored malwares such like Flame, Duqu, Uruborus and the Regin revealed that these were designed to sustain long-term intelligence-gathering operations by remaining under the radar. Antivirus companies made a great job in revealing technical details of the attack campaigns, however, it exclusively has almost focused on the executables or the memory dump of the infected systems - the research hasn't been simulated in a real environment.

GSM networks still use ancient protocols; Signaling System 7 (SS7), GPRS Tunneling Protocol (GTP) and the Stream Control Transmission Protocol (SCTP) which contain loads of vulnerable components. Malware authors totally aware of it and weaponing exploits within their campaigns to grab encrypted and unencrypted streams of private communications handled by the Telecom companies. For instance, Regin was developed as a framework that can be customized with a wide range of different capabilities, one of the most interesting ability to monitor GSM networks.

In this talk, we are going to break down the Regin framework stages from a reverse engineering perspective - kernel driver infection scheme, virtual file system and its encryption scheme, kernel mode manager- while analyzing its behaviors on a GSM network and making technical comparison of its counterparts - such as TDL4, Uruborus, Duqu2.

Omer works as an Ethical Hacker for KPN's (Royal Dutch Telecom) REDteam in Amsterdam, the Netherlands. He enjoys diving into lines of code to spot bugs, tinkering in front of the debugger and developing wise tactics/tools to break applications on his day to day work. Prior to joining KPN REDteam, Omer worked for companies like IBM ISS, Verizon and as an external government contractor. He holds an Honour's Engineering degree in Computer Science.

Bugged Files: Is Your Document Telling on You?

Daniel "unicornFurnace" Crowley, Security Consultant, NCC Group
Damon Smith, Associate Security Consultant, NCC Group

Certain file formats, like Microsoft Word and PDF, are known to have features that allow for outbound requests to be made when the file opens. Other file formats allow for similar interactions but are not well-known for allowing such functionality. In this talk, we explore various file formats and their ability to make outbound requests, as well as what that means from a security and privacy perspective. Most interestingly, these techniques are not built on mistakes, but intentional design decisions, meaning that they will not be fixed as bugs. From data loss prevention to de-anonymization to request forgery to

NTLM credential capture, this presentation will explore what it means to have files that communicate to various endpoints when opened.

Daniel (aka "unicornFurnace") is a Security Consultant for NCC Group. Daniel denies all allegations regarding unicorn smuggling and questions your character for even suggesting it. Daniel has developed configurable testbeds such as SQLol and XMLmao for training and research regarding specific vulnerabilities. Daniel enjoys climbing large rocks. Daniel has been working in the information security industry since 2004 and is a frequent speaker at conferences including Black Hat, DEF CON, Shmoocon, and SOURCE. Daniel does his own charcuterie. Daniel also holds the title of Baron in the micronation of Sealand.

Damon Smith is an Associate Security Engineer with NCC Group, an information security firm specializing in application, network, and mobile security. Damon specializes in web application assessments, embedded device/point of sale assessments, network penetration testing, and mobile testing. Damon graduated with a BS is Computer Science from the University of Texas, with a focus on Information Security. He has experience working as an IT consultant in the legal and retail industries and further as a security consultant focusing on application assessments.

Do Export Controls on "Intrusion Software" Threaten Vulnerability Research?

Tom Cross aka Decius, CTO, Drawbridge Networks
Collin Anderson, Independent Researcher

At the end of 2013, an international export control regime known as the Wassenaar Arrangement was updated to include controls on technology related to "Intrusion Software" and "IP Network Surveillance Systems." Earlier this year, the US Government announced a draft interpretation of these new controls, which has kicked off a firestorm of controversy within the information security community. Questions abound regarding what the exact scope of the proposed rules is, and what impact the rules might have on security researchers. Is it now illegal to share exploit code across borders, or to disclose a vulnerability to a software vendor in another country? Can export controls really keep surveillance technology developed in the west out of the hands of repressive regimes? This presentation will provide a deep dive on the text of the new controls and discuss what they are meant to cover, how the US Government has indicated that it may interpret them, and what those interpretations potentially mean for computer security researchers, and for the Internet as a whole.

Tom Cross is the CTO of Drawbridge Networks. He is credited with discovering a number of critical security vulnerabilities in enterprise class software and has written papers on collateral damage in cyber conflict, vulnerability disclosure ethics, security issues in internet routers, encrypting open wireless networks, and protecting Wikipedia from vandalism. Tom was previously Director of Security Research at Lancope, and Manager of the IBM Internet Security Systems X-Force Advanced Research team. He has spoken at numerous security conferences, including DEF CON, Blackhat Briefings, CyCon, HOPE, Source Boston, FIRST, and Security B-Sides.
*Twitter: @_decius_*

Collin Anderson is a Washington D.C.-based researcher focused on measurement and control of the Internet, including network ownership and access restrictions, with an emphasis on countries that restrict the free flow of information. Through open research and cross-organizational collaboration, these efforts have included monitoring the international sale of surveillance equipment, identifying consumer harm in disputes between core network operators, exploring alternative means of communications that bypass normal channels of control, and applying big data to shed new light on increasingly sophisticated restrictions by repressive governments. These involvements extend into the role of public policy toward promoting online expression and accountability, including regulation of the sale of surveillance technologies and reduction of online barriers to the public of countries under sanctions restrictions.
Twitter: @cda

REvisiting RE:DoS

Eric (XlogicX) Davisson, Not a security researcher

Regular Expression Denial of Service has existed for well over a decade, but has not received the love it deserves lately. There are some proof of concept attacks out there currently, most of which are ineffective due to implementation optimizations. Regardless of the effectiveness most of these PoC's are geared only to NFA engines.

This talk will demonstrate working PoC's that bypass optimizations. Both NFA and DFA engines will get love. Tools will be released (with demonstration) that benchmark NFA/DFA engines and automate creation of 'evil strings' given an arbitrary regular expression. Attendees can expect a review of regex and a deep under the hood explanation of both regex engines before abuses ensue.

^ *Not a security researcher*

Licensed to Pwn: The Weaponization and Regulation of Security Research

Jim Denaro
Dave Aitel
Matt Blaze
Nate Cardozo
Mara Tam
Special Guest - TBA

Security research is under attack. Updates to the Wassenaar Arrangement in 2013 established among its 41 member nations an agreement to place a variety of previously undesignated "cybersecurity items" under export control. After 18 months and a half-dozen open advisory meetings, the U.S. has taken the entire security research community by surprise with its proposed rule; we are confronted by a sweeping

implementation with profound consequences for academia, independent research, commercial cybersecurity, human rights, and national security.

While the outcome of this round of regulatory intervention is still uncertain, the fact that there will be more is not. This panel of experts will discuss the context, history, and general process of regulation, as well the related question of "weaponized" research in regulatory discourse.

There is significant daylight between the relatively lax text of the Wassenaar Arrangement itself and the extraordinarily broad implementation proposed in the U.S. What will the practical effects of those differences be, and why did the U.S. diverge from the Wassenaar text? Regulators are, even now, still struggling to comprehend what the consequences of this new "cyber rule" might be. So, how are we to understand this regulatory process? What are its objectives? Its impacts? Its limits? How can we influence its outcomes?

Eleventh-hour interventions are quickly becoming a hallmark of regulatory activities with implications for the wider world of information security; the fight here is almost exclusively a rearguard action. Without resorting to the usual polemics, what failures of analysis and advice are contributing to these missteps - on both sides? What interests might encourage them? How are security researchers being caught so off-balance? Come victory or despair in the present case, this panel aims to answer the question of whether there is a solution that prevents technology transfer to hostile nations while still enabling free markets, freedom of expression, and freedom of research.

Dave Aitel (@daveaitel) is an offensive security expert whose company, Immunity, Inc., consults for major financial institutions, Fortune/Global 500s, etc. At the age of 18, he was recruited by the National Security Agency where he served six years as a "security scientist" at the agency's headquarters at Fort Meade, Maryland. He then served as a security consultant for @stake before founding Immunity in 2002. Today, Dave's firm is hired by major companies to try to hack their computer networks - in order to find and fix vulnerabilities that criminal hackers, organized crime and nation-state adversaries could use. Immunity is also a past contractor on DARPA's cyber weapons project, known as Cyber Fast Track. The company is well-known for developing several advanced hacking tools used by the security industry, such as Swarm, Canvas, Silica, Stalker, Accomplice, Spike, Spike Proxy, Unmask - and, most recently Innuendo, the first US-made nation-grade cyber implant with Flame/Stuxnet-like malware capabilities. Immunity has offices in Florida, D.C., Canada, Italy and Argentina. eWeek Magazine named Dave one of "The 15 Most Influential People in Security." He is a past keynote speaker at BlackHat and DEF CON. He is a co-author of "The Hacker's Handbook," The Shellcoder's Handbook" and "Beginning Python." He is also the founder of the prestigious Infiltrate offensive security conference (Businessweek article) and the widely read "Daily Dave Mailing List," which covers the latest cybersecurity news, research and exploit developments.

Twitter: @daveaitel

Matt Blaze (@mattblaze) is a professor in the computer science department at the University of Pennsylvania. From 1992 until he joined Penn in 2004, he was a research scientist at AT&T Bell Laboratories. His research focuses on the architecture and design of secure systems based on cryptographic techniques, analysis of secure systems against practical attack models, and on finding

new cryptographic primitives and techniques. In 1994, he discovered a serious flaw in the US Government's "Clipper" encryption system, which had been proposed as a mechanism for the public to encrypt their data in a way that would still allow access by law enforcement. He has testified before various committees of the US Congress and European Parliament several times, providing technical perspective on the problems surrounding law enforcement and intelligence access to communications traffic and computer data. He is especially interested in the use of encryption to protect insecure systems such as the Internet. Recently, he has applied cryptologic techniques to other areas, including the analysis of physical security systems; this work yielded a powerful and practical attack against virtually all commonly used master-keyed mechanical locks.

Twitter: @mattblaze

Nate Cardozo (@ncardozo) is a Staff Attorney with the Electronic Frontier Foundation. He focuses on the intersection of technology, privacy, and free expression. He has defended the rights of anonymous bloggers, sued the United States government for access to improperly classified documents, and lobbied Congress for sensible reform of American surveillance laws. In addition, he works on EFF's Coders' Rights Project, counseling hackers, academics, and security professionals at all stages of their research. Additionally, Nate manages EFF's Who Has Your Back? report, which evaluates service providers' protection of user data. Nate has projects involving automotive privacy, speech in schools, government transparency, hardware hacking rights, anonymous speech, public records litigation, and resisting the expansion of the surveillance state. Nate has a B.A. in Anthropology and Politics from the University of California, Santa Cruz and a J.D. from the University of California, Hastings where he has taught legal writing and moot court.

Twitter: @ncardozo

Jim Denaro (@CipherLaw; moderator) is the founder of CipherLaw, a Washington, D.C.-based intellectual property law firm and focuses his practice on legal and technical issues faced by innovators in information security. He is a frequent speaker and writer on the subject and works in a wide range of technologies, including cryptography, intrusion detection, botnet investigation, and incident response. Jim advises clients on legal issues of particular concern to the information security community, including active defense technologies, government-mandated access (backdoors), export control, exploit development and sales, bug bounty programs, and confidential vulnerability disclosure (Disclosure as a Service). He has a degree in computer engineering and has completed various professional and technical certifications in information security and is engaged in graduate studies in national security at Georgetown University. Before becoming an attorney, Jim spent obscene amounts of time looking at PPC assembly in MacsBug.

Twitter: @CipherLaw

Mara Tam (@marasawr) is a semi-feral researcher and historian of policy, justice, culture, and security. She has authored, co-authored, and contributed research for technical policy papers in the fields of international security and arms control. After earning a first class degree in art history, Mara's work supported bilateral negotiations towards peaceful nuclear cooperation between the United States and India. She has been a participant, speaker, and panellist for academic conferences in cultural studies,

languages, and history, as well as for strategic programmes like 'The Intangibles of Security' initiative convened by NATO and the European Science Foundation. She is currently a doctoral candidate and freelance thinkfluencer.

Twitter: @marasawr

Special Guest - TBA

Dark side of the ELF - leveraging dynamic loading to pwn noobs

Alessandro Di Federico, PhD Student, Politecnico di Milano
Yan Shoshitaishvili, PhD Student, UC Santa Barbara

The ELF format is ancient, and much mystery lurks in its dark depths. For 16 years, it has safely encompassed our software, providing support for binary loading, symbol resolution, and lots of very useful binary stuff. In that time, security has become a key concern, resulting in binary defenses like NX and ASLR, which have made exploiting vulnerabilities quite difficult. ASLR, for example, randomizes the location of the stack, the heap, libraries, and (optionally), the binary itself at every execution of an application.

There is no easy way to say this: ELF has let us down. In this talk, we'll explore the dark side of ELF. Specifically, we'll show how ELF, by design, implicitly trusts data structures in the ELF headers. Even in the presence of ASLR, an attacker able to corrupt these headers can trick the ELF loader into calling any function in any linked-in library, providing nothing but the name of the binary. In essence, this technique allows an attacker to call arbitrary library functions (such as system()!) without leaking memory addresses. We call this technique Leakless.

While developing Leakless, we checked many different implementations of the standard C library and found that Leakless can be adapted to attack the ELF loader implementations in all of the common ones (i.e., GNU libc, the libc of the major BSDs, and uClibc). In this talk, we'll describe the internals of the ELF format, show how Leakless works to subvert library function resolution, and demonstrate how it can be use to carry out attacks without information disclosures. And, of course, we'll open-source the tool that we developed to make carrying out this attack easier.

Alessandro is a PhD student at Politecnico Di Milano, right under that leaning tower. In his spare time, he hacks with Tower of Hanoi. He likes exploitation and doing really crazy stuff, on and off the computer!

Hacking since the age of eight, Yan Shoshitaishvili is fascinated by understanding and commandeering the computation and actions carried out by binary code. He is currently pursuing his PhD in the Seclab at UC Santa Barbara and is one of the hacking aces behind team Shellphish. In the little spare time he has left, he develops and releases computer security tools on the Internet.

Fighting Back in the War on General Purpose Computers

Cory Doctorow, Author & Activist, Electronic Frontier Foundation

EFF's Apollo 1201 project is a 10-year mission to abolish all DRM, everywhere in the world, within a decade. We're working with security researchers to challenge the viability of the dread DMCA, a law that threatens you with jail time and fines when you do your job: discover and disclosing defects in systems that we rely on for life and limb.

Cory Doctorow (craphound.com) is a science fiction author, activist, journalist and blogger - the co-editor of Boing Boing (boingboing.net) and the author of the YA graphic novel 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 and co-founded the UK Open Rights Group. Born in Toronto, Canada, he now lives in London.

REpsych: Psychological Warfare in Reverse Engineering

Chris Domas, Security Researcher

Your precious 0-day? That meticulously crafted exploit? The perfect foothold? At some point, they'll be captured, dissected, and put on display. Reverse engineers. When they begin snooping through your hard work, it pays to have planned out your defense ahead of time. You can take the traditional defensive route - encryption, obfuscation, anti-debugging - or you can go on the offense, and attack the heart and soul of anyone who dare look at your perfect code. With some carefully crafted assembly, we'll show how to break down a reverse engineer by sending them misleading, intimidating, and demoralizing messages through the control flow graphs of their favorite RE tools - turning their beloved IDA (Hopper, BinNavi, Radare, etc) into unwitting weapons for devastating psychological warfare in reverse engineering.

Chris is an embedded systems engineer and cyber security researcher, focused on innovative approaches to low level hardware and software RE and exploitation.

Twitter: @xoreaxeaxeax

USB Attack to Decrypt Wi-Fi Communications

Jeremy Dorrough, Senior Network Security Architect / Genworth Financial

The term "Bad USB" has gotten some much needed press in last few months. There have been talks that have identified the risks that are caused by the inherent trust between the OS and any device attached by USB. I found in my research that most of the available payloads for the USB rubber ducky would be stopped by common enterprise security solutions. I then set out to create a new exploit that would force the victim to trust my Man-In-The-Middle access point. After my payload is deployed, all

Wi-Fi communications will be readable, including usernames, passwords and authentication cookies. The attack will work without the need of elevating privileges, which makes it ideal for corporate environments.

Jeremy has built his career around protecting assets in the most critical IT sectors. He started his career working in a Network Operations Security Center for the US Army. He then went on to work as a Network Security Engineer defending Dominion's North Anna Nuclear Power Station. He is currently a Senior Network Security Engineer/Architect at Genworth Financial. He is a MBA, CISSP, CEH, GIAC GPPA, CSA CCSK, ABCDEFG... Blah Blah Blah. Jeremy has spent over 10 years researching and implementing new ways to defend against the latest attacks. He enjoys creating new exploits and feels it makes him a more well-rounded defensive Security Engineer. He is happily married and a father to two soon to be hackers. When he's not staring at a command prompt, he is busy building and driving demolition derby cars.
Twitter: @jdorrough1

BurpKit - Using WebKit to Own the Web

Nadeem Douba, Founding Principal, Red Canari

Today's web apps are developed using a mashup of client- and server-side technologies. Everything from sophisticated Javascript libraries to third-party web services are thrown into the mix. Over the years, we've been asked to test these web apps with security tools that haven't evolved at the same pace. A common short-coming in most of these tools is their inability to perform dynamic analysis to identify vulnerabilities such as dynamically rendered XSS or DOM-based XSS. This is where BurpKit comes in - a BurpSuite plugin that integrates the power of WebKit with that of BurpSuite. In this presentation we'll go over how one can leverage WebKit to write their own web pen-testing tools and introduce BurpKit. We'll show you how BurpKit is able to perform a variety of powerful tasks including dynamic analysis, BurpSuite scripting, and more! Best of all, the plugin will be free and open source so you can extended it to your heart's desire!
Nadeem Douba is the founding principal of Red Canari, an information security consulting firm that specializes in the areas of technical security assessments. With over 15 years experience, Nadeem provides consulting and training services for organizations within the public and private sector. He has also presented at some of the world's largest security conferences and is the author of many well-known open source security tools, including PyMiProxy (used by the Internet Archive), Sploitego, and the Canari Framework (previously presented at DEF CON 20). His primary research interests include open source intelligence, application and operating system security, and big data.
Twitter: @ndouba

Stagefright: Scary Code in the Heart of Android

Joshua J. Drake, Sr. Director of Platform Research and Exploitation, Zimperium

With over a billion activated devices, Android holds strong as the market leading smartphone operating system. Underneath the hood, it is primarily built on the tens of gigabytes of source code from the Android Open Source Project (AOSP). Thoroughly reviewing a code base of this size is arduous at best

-- arguably impossible. Several approaches exist to combat this problem. One such approach is identifying and focusing on a particularly dangerous area of code.

This presentation centers around the speaker's experience researching a particularly scary area of Android, the Stagefright multimedia framework. By limiting his focus to a relatively small area of code that's critically exposed on 95% of devices, Joshua discovered a multitude of implementation issues with impacts ranging from unassisted remote code execution down to simple denial of service. Apart from a full explanation of these vulnerabilities, this presentation also discusses; techniques used for discovery, Android OS internals, and the disclosure process. Finally, proof-of-concept code will be demonstrated.

After attending this presentation, you will understand how to discover vulnerabilities in Android more effectively. Joshua will show you why this particular code is so scary, what has been done to help improve the overall security of the Android operating system, and what challenges lie ahead.

Joshua J. Drake is the Sr. Director of Platform Research and Exploitation at Zimperium and lead author of the Android Hacker's Handbook. Joshua focuses on original research such as reverse engineering and the analysis, discovery, and exploitation of security vulnerabilities. He has over 10 years of experience auditing and exploiting a wide range of application and operating system software with a focus on Android since early 2012. In prior roles, he served at Metasploit and VeriSign's iDefense Labs. Joshua previously spoke at BlackHat, RSA, CanSecWest, REcon, Ruxcon/Breakpoint, Toorcon, and DerbyCon. Other notable accomplishments include exploiting Oracle's JVM for a win at Pwn2Own 2013, successfully compromising the Android browser via NFC with Georg Wicherski at BlackHat USA 2012, and winning the DEF CON 18 CTF with the ACME Pharm team in 2010.
Twitter: @jduck

Medical Devices: Pwnage and Honeypots

Scott Erven, Associate Director, Protiviti
Mark Collao, Security Consultant, Protiviti

We know medical devices are exposed to the Internet both directly and indirectly, so just how hard is it to take it to the next step in an attack and gain remote administrative access to these critical life saving devices? We will discuss over 20 CVEÃs Scott has reported over the last year that will demonstrate how an attacker can gain remote administrative access to medical devices and supporting systems. Over 100 remote service and support credentials for medical devices will be presented.

So is an attack against medical devices a reality or just a myth? Now that we know these devices have Internet facing exposure and are vulnerable to exploit, are they being targeted? We will release and present six months of medical device honeypot research showing the implications of these patient care devices increasing their connectivity.

Scott Erven is an Associate Director at Protiviti. He has over 15 years of information security and information technology experience with subject matter expertise in medical device and healthcare security. Scott has consulted with the Department of Homeland Security, Food and Drug Administration

and advised national policymakers. His research on medical device security has been featured in Wired and numerous media outlets worldwide. Mr. Erven has presented his research and expertise in the field internationally. Scott also has served as a subject matter expert and exam writer for numerous industry certifications. His current focus is on research that affects human life and public safety issues inside todayÃs healthcare landscape.

Mark Collao is a Security Consultant at Protiviti. He has over 5 years of experience in information security consulting, primarily in network and application penetration tests, red team assessments, and social engineering exercises. Mark also researches botnet activity and maintains several custom protocol and application honeypots on the net. He holds an Offensive Security Certified Professional (OSCP) certification, is a member of the MWCCDC red team, and graduated from DePaul University.

NSA Playset: JTAG Implants

Joe FitzPatrick, SecuringHardware.com
Matt King, Security Researcher

While the NSA ANT team has been busy building the next generation spy toy catalog for the next leak, the NSA Playset team has been busy catching up with more open hardware implementations. GODSURGE is a bit of software that helps to persist malware into a system. It runs on the FLUXBABBIT hardware implant that connects to the depopulated JTAG header of certain models of Dell servers.

This talk will introduce SAVIORBURST, our own implementation of a jtag-based malware delivery firmware that will work hand-in-hand with SOLDERPEEK, our custom hardware design for a standalone JTAG attack device. We will demonstrate how to this pair enables the persistent compromise of an implanted system as well as release all the hardware and software necessary to port SAVIORBURST and SOLDERPEEK to your jtag-equipped target of choice. Anyone curious to know more about JTAG, regardless of previous hardware experience, will learn something from this talk.

Joe has spent a decade working on low-level silicon debug, security validation, and penetration testing of CPUS, SOCs, and microcontrollers. He develops and delivers hardware security training at https://SecuringHardware.com, including Software Exploitation via Hardware Exploits and Applied Physical Attacks on x86 Systems. In between, he keeps busy with contributions to the NSA Playset and other misdirected hardware projects.

Twitter: @securelyfitz

Matt is a hardware designer and security researcher who has over a decade of experience designing, securing and exploiting hardware test and debug features on CPUs and SoCs. When not performing pointless hardware tricks Matt tries to help educate integrated circuit designers on the risks posed by hardware debug capabilities.

Twitter: @syncsrc

Unbootable: Exploiting the PayLock SmartBoot Vehicle Immobilizer

fluxist, Hacker, Entrepreneur

Many of us have seen the big yellow "boot" on the wheel of a parked car, marking like a scarlet letter some poor sap who hasn't paid his parking tickets. Since 2005 many US municipalities have switched from a manual boot to the PayLock SmartBoot. With just a phone call and a credit card you can pay your fines and extortionate fees and fill the county coffers -- and in return they'll give you the secret code to type in and unlock the electronic vehicle immobilizer. But what if there were another way to remove the boot, quicker than a phone call and a credit card payment? Join me in a thorough reverse engineering of the PayLock SmartBoot as we disassemble one, recover and analyze the firmware from the embedded controller, and find the secrets to thoroughly pwn the device. This talk will reveal a backdoor that can be used to disarm every SmartBoot in over 50 municipalities.

fluxist (Robert Testagrossa) is an independent security researcher; Director - Special Projects at Dulotech Inc; and Owner of Cloud99 Vapes, a NY-based chain of retail vape shops. He is not available for comment.

Hooked Browser Meshed-Networks with WebRTC and BeEF

Christian (@xntrik) Frichot, Principal Security Consultant at Asterisk Information Security

One of the biggest issues with BeEF is that each hooked browser has to talk to your BeEF server. To try and avoid detection, you often want to try and obfuscate or hide your browsers, particularly if you're heavily targeting a single organization. Don't worry Internet-friends, those crazy pioneers at Google, Mozilla and Opera have solved this problem for you with the introduction of Web Real-Time Communications (WebRTC). Initially designed to allow browsers to stream multimedia to each other, the spec has made its way into most Chrome and Firefox browsers, not to mention it's enabled by default.
Using this bleeding-edge web technology, we can now mesh all those hooked browsers, funnelling all your BeEF comms through a single sacrificial beach-head. Leveraging WebRTC technologies (such as STUN/TURN and even the fact the RTC-enabled browsers on local subnets can simply UDP each other), meshing browsers together can really throw a spanner into an incident-responders work. The possibilities for a browser-attacker are fairly endless, channeling comms through a single browser, or, making all the browsers communicate with each other in round-robin. This is just another tool tucked into your belt to try and initiate and maintain control over browsers.

This presentation will present a background into WebRTC, and then demonstrate the WebRTC BeEF extension. (Bloody JavaScript...)

Christian is an Australian security professional and founder of Asterisk Information Security based in Perth. He is one of the co-authors of the recently published Browser Hacker's Handbook (by Wiley), and long-term code-funkerer of the BeEF project. When not performing application security or penetration testing gigs, Christian spends his time either ranting about appsec or pining to get behind his drumkit. He has a deep love/hate relationship with web browsers and JavaScript. Christian has presented at numerous Australian security conferences, including OWASP AppSec APAC, the Australian Information Security Association's Perth Con, ISACA's Perth Con, OWASP Melbourne, and Ruxmon. In addition, Christian was fortunate to present at Kiwicon 8 in New Zealand at the end of 2014. s that Christian has been involved with include BeEF, OWASP's SAMM Self Assessment Tool, Prenus (the pretty Nessus thing), Burpdot (graphing connectivity between URLs from Burp), and the Devise Google Authenticator extension.
Christian has been blogging on un-excogitate.org and labs.asteriskinfosec.com.aufor ages now, and is often found on twitter (@xntrik) raging about various security topics.

Twitter: @xntrik

Abusing Adobe Reader's JavaScript APIs

Brian Gorenc, Manager, HP's Zero Day Initiative
Abdul-Aziz Hariri, Security Researcher, HP's Zero Day Initiative
Jasiel Spelman, Security Researcher, HP's Zero Day Initiative

Adobe Reader's JavaScript APIs offer a rich set of functionality for document authors. These APIs allow for processing forms, controlling multimedia events, and communicating with databases, all of which provide end-users the ability to create complex documents. This complexity provides a perfect avenue for attackers to take advantage of weaknesses that exist in Reader's JavaScript APIs.

In this talk, we will provide insight into both the documented and undocumented APIs available in Adobe Reader. Several code auditing techniques will be shared to aid in vulnerability discovery, along with numerous proofs-of-concept which highlight real-world examples. We'll detail out how to chain several unique issues to obtain execution in a privileged context. Finally, we'll describe how to construct an exploit that achieves remote code execution without the need for memory corruption.

Brian Gorenc is the manager of Vulnerability Research with Hewlett-Packard Security Research (HPSR). In this role, Gorenc leads the Zero Day Initiative (ZDI) program, which is the world's largest vendor-agnostic bug bounty program. His focus includes analyzing and performing root-cause analysis on hundreds of zero-day vulnerabilities submitted by ZDI researchers from around the world. The ZDI works to expose and remediate weaknesses in the world's most popular software. Brian is also responsible for organizing the ever-popular Pwn2Own hacking competitions.

Prior to joining HP, Gorenc worked for Lockheed Martin on the F-35 Joint Strike Fighter (JSF) program. In this role, he led the development effort on the Information Assurance (IA) products in the JSF's mission planning environment.

Twitter: @maliciousinput

Abdul-Aziz Hariri is a security researcher with Hewlett-Packard Security Research (HPSR). In this role, Hariri analyzes and performs root-cause analysis on hundreds of vulnerabilities submitted to the Zero Day Initiative (ZDI) program, which is the world's largest vendor-agnostic bug bounty program. His focus includes performing root-cause analysis, fuzzing and exploit development.

Prior to joining HP, Hariri worked as an independent security researcher and threat analyst for Morgan Stanley emergency response team. During his time as an independent researcher, he was profiled by Wired magazine in their 2012 article, "Portrait of a Full-Time Bug Hunter".

Twitter: @abdhariri

Jasiel Spelman is a vulnerability analyst and exploit developer for the Zero Day Initiative (ZDI) program. His primary role involves performing root cause analysis on ZDI submissions to determine exploitability, followed by developing exploits for accepted cases. Prior to being part of ZDI, Jasiel was a member of the Digital Vaccine team where he wrote exploits for ZDI submissions, and helped develop the ReputationDV service from TippingPoint. Jasiel's focus started off in the networking world but then shifted to development until transitioning to security. He has a BA in Computer Science from the University of Texas at Austin.

Twitter: @wanderingglitch

HP's Zero Day Initiative, Twitter: @thezdi

WhyMI so Sexy? WMI Attacks, Real-Time Defense, and Advanced Forensic Analysis

Matt Graeber, Reverse Engineer, FireEye Inc.
Willi Ballenthin, Reverse Engineer, FireEye Inc.
Claudiu Teodorescu, Reverse Engineer, FireEye Inc.

Windows Management Instrumentation (WMI) is a remote management framework that enables the collection of host information, execution of code, and provides an eventing system that can respond to operating system events in real time. FireEye has recently seen a surge in attacker use of WMI to carry out objectives such as system reconnaissance, remote code execution, persistence, lateral movement, covert data storage, and VM detection. Defenders and forensic analysts have largely remained unaware of the value of WMI due to its relative obscurity and completely undocumented file format. After extensive reverse engineering, our team has documented the WMI repository file format in detail, developed libraries to parse it, and formed a methodology for finding evil in the repository.

In this talk, we will take a deep dive into the architecture of WMI, reveal a case study in attacker use of WMI in the wild, describe WMI attack mitigation strategies, show how to mine its repository for forensic artifacts, and demonstrate how to detect attacker activity in real-time by tapping into the WMI eventing

system. By the end of this talk, we will have convinced the audience that WMI is a valuable asset not just for system administrators and attackers, but equally so for defenders and forensic analysts.

Matt Graeber is a reverse engineer in the FireEye Labs Advanced Reverse Engineering (FLARE) team with a varied background in reverse engineering, red teaming, and offensive tool development. Since joining FireEye, Matt has reversed a vast quantity of targeted and commodity malware samples and served as an instructor of Mandiant's Advanced Malware Analysis course. Matt is the author of various PowerShell modules used for pentesting and reverse engineering including PowerSploit and PowerShellArsenal. He has also been designated a Microsoft "Most Valuable Professional" in PowerShell.
Twitter: @mattifestation

Willi Ballenthin is a reverse engineer in the FLARE team who specializes in incident response and computer forensics. He can typically be found investigating intrusions at Fortune 500 companies and enjoys reverse engineering malware, developing forensic techniques, and exploring the cutting edge. Willi is the author of a number of cross-platform Python libraries including python-registry, python-evtx, and INDXParse.py.
Twitter: @williballenthin

Claudiu Teodorescu is a reverse engineer in the FLARE team. Prior to joining FireEye, Claudiu worked for Guidance Software, writing forensic parsers for different file formats to support the EnCase forensic tool. Also, as the Cryptographic Officer of the company, he supported EnCase integration with different disk/volume/file based encryption products including Bitlocker, McAfee EEPC, Checkpoint FDE, Symantec EEPC, etc.

Goodbye Memory Scraping Malware: Hold Out Till "Chip And Pin"

Weston Hecker, SR Pentester, Sr Systems Security Analyst at "KLJ Security"

Proof of concept for stopping credit card theft in memory skimming operations . Alternative methods of stopping credit card skimming

I am leading project on Free Open Source software that attacks POS skimming malware. Launching platform and concept for stores to not be low hanging fruit In effect making it no longer possible to sell credit card numbers from skim breaches. Better collection of forensic data with cannery features (such as putting flagged card into memory so if it is skimmed it will be flagged at processor and catch the breaches much faster)Injects 1-500 false random CC numbers for every one legitimate CC number that is entered. In effect making stolen credit card batches harder to sell. I will go in detail of how criminals Steal and sell credit cards at this time. This is a software for making credit cards numbers harder to steal in the methods that have been happening in larger breaches Target, Home Depot.

10 Years Pen-testing, 11 years security research and programming experience. Working for a security Company in the Midwest, Weston has recently Spoken at DEF CON 22 and over 40 other speaking

engagements from telecom regional events to Universitys on security subject matter. Working with A major University's research project with Department of Homeland Security on 911 emergency systems and attack mitigation. Attended school in Minneapolis Minnesota. Computer Science and Geophysics. Co-Author of "SkimBad" Anti-malware framework Found several vulnerability's in very popular software and firmware. Including Microsoft, Qualcomm, Samsung, HTC, Verizon.

Low-cost GPS simulator - GPS spoofing by SDR

Lin Huang, Senior wireless security researcher, Qihoo 360 Technology Co. Ltd.
Qing Yang, Team Leader of Unicorn Team, Qihoo 360 Technology Co. Ltd.

It is known that GPS L1 signal is unencrypted so that someone can produce or replay the fake GPS signal to make GPS receivers get wrong positioning results. There are many companies provide commercial GPS emulators, which can be used for the GPS spoofing, but the commercial emulators are quite expensive, or at least not free. Now we found by integrating some open source projects related to GPS we can produce GPS signal through SDR tools, e.g. USRP / bladeRF. This makes the attack cost very low. It may influence all the civilian use GPS chipset. In this presentation, the basic GPS system principle, signal structure, mathematical models of pseudo-range and Doppler effect will be introduced. The useful open source projects on Internet will be shared with attendees.

HUANG Lin is a wireless security researcher, from Unicorn Team of Qihoo 360 China. Before entering Qihoo, she worked for telecom operator Orange, for 9 years, as a wireless researcher. Her interests include the security issues in wireless communication, especially the cellular network security, and also other problems in ADS-B, GPS, Bluetooth, Wifi, and automotive electronics.
Twitter: @huanglin_bupt

She is one of the earliest users of USRP in China, and keeps active in SDR/USRP research and development since 2006. She contributed to several UMTS/LTE soft base station projects, e.g. Open Air Interface. In 2009, She wrote one free e-book for GNU Radio training, which is very popular in China.

YANG Qing is the team leader of Unicorn Team in Qihoo 360 Technology Co. Ltd. He has rich experiences in wireless and hardware security area, including WiFi penetration testing, cellular network interception, IC card cracking etc. His interests also cover embedded system hacking, firmware reversing, automotive security, and software radio.

He is the first one who reported the vulnerabilities of WiFi system and RF IC card system used in Beijing subway.

I want these * bugs off my * Internet

Dan Kaminsky, Chief Scientist, White Ops

Are you interested in the gory details in fixing ugly bugs? No? Just like watching stuff blow up? Go to some other talk! But if you want to see what it takes to comprehensively end an entire bug class -- how

you dive into a code base, what performance and usability and maintainability and debuggability constraints it takes to make a web browser more secure -- oh do I have some dirt for you.

Drive It Like You Hacked It: New Attacks and Tools to Wirelessly Steal Cars

Samy Kamkar

Gary Numan said it best. Cars. They're everywhere. You can hardly drive down a busy freeway without seeing one. But what about their security?

In this talk I'll reveal new research and real attacks in the area of wirelessly controlled gates, garages, and cars. Many cars are now controlled from mobile devices over GSM, while even more can be unlocked and ignitions started from wireless keyfobs over RF. All of these are subject to attack with low-cost tools (such as RTL-SDR, GNU Radio, HackRF, Arduino, and even a Mattel toy).

We will investigate how these features work, and of course, how they can be exploited. I will be releasing new tools and vulnerabilities in this area, such as key-space reduction attacks on fixed-codes, advanced "code grabbers" using RF attacks on encrypted and rolling codes, and how to protect yourself against such issues.

By the end of this talk you'll understand not only how vehicles and the wirelessly-controlled physical access protecting them can be exploited, but also learn about various tools for car and RF research, as well as how to use and build your own inexpensive devices for such investigation.

Ladies and gentlemen, start your engines. And other people's engines.

Samy Kamkar is a security researcher, best known for creating The MySpace Worm, one of the fastest spreading viruses of all time. He (attempts to) illustrate terrifying vulnerabilities with playfulness, and his exploits have been branded:

"Controversial", -The Wall Street Journal
"Horrific", -The New York Times
"Now I want to fill my USB ports up with cement", -Gizmodo

He's demonstrated usurping typical hardware for surreptitious means such as with KeySweeper, turning a standard USB wall charger into a covert, wireless keyboard sniffer, and SkyJack, a custom drone which takes over any other nearby drones allowing them to be controlled as a massive zombie swarm. He's exposed issues around privacy, such as by developing the Evercookie which appeared in a top-secret NSA document revealed by Edward Snowden, exemplifying techniques used by governments and corporations for clandestine web tracking, and has discovered and released research around the illicit GPS and location tracking performed by Apple, Google and Microsoft mobile devices. He continues to produce new research and tools for the public as open source and open hardware. Twitter: @samykamkar

Harness: Powershell Weaponization Made Easy (or at least easier)

Rich Kelley, security researcher & co-founder of Gray Tier Technologies

The Harness toolset aims to give penetration testers and red teams the ability to pull a remote powershell interface with all the same features of the native Powershell CLI and more. Several tools and utilities have been released to solve the powershell weaponization problem, but no freely available tool give operators the full capabilities of powershell through a remote interface. We'll start the talk with a quick survey of the previous methods of weaponizing powershell, and then move into the capabilities of the Harness toolset which includes a fully interactive powershell CLI, and remote importing of modules across the wire without staging. We'll conclude with taking a look at the underlying code that makes the toolset work, and briefly discuss planned features. The Harness toolset will be released open source in conjunction with this talk.

Rich Kelley (@RGKelley5) is a security researcher and the co-founder of Gray Tier Technologies, a small InfoSec start-up based out of Alexandria, VA. After his time in the military he held positions as a network engineer, software engineer, and penetration tester for various government agencies. He recently moved into exploit development and reverse engineering, and is pretty sure he knows less than when he started.

Twitter: @RGKelley5

ThunderStrike 2: Sith Strike

Trammel Hudson, Vice President, Two Sigma Investments
Xeno Kovah, Co-founder, LegbaCore, LLC
Corey Kallenberg, Co-Founder, LegbaCore, LLC

The number of vulnerabilities in firmware disclosed as affecting Wintel PC vendors has been rising over the past few years. Although several attacks have been presented against Mac firmware, unlike their PC counterparts, all of them required physical presence to perform. Interestingly, when contacted with the details of previously disclosed PC firmware attacks, Apple systematically declared themselves not vulnerable.

This talk will provide conclusive evidence that Mac's are in fact vulnerable to many of the software only firmware attacks that also affect PC systems. In addition, to emphasize the consequences of successful exploitation of these attack vectors, we will demonstrate the power of the dark side by showing what Mac firmware malware is capable of.

Trammell Hudsonenjoys taking things apart and understanding how they work. He presented the Thunderstrike firmware vulnerability at 31C3, created the Magic Lantern firmware for Canon cameras, and teaches classes at the Brooklyn hackerspace NYC Resistor.

Twitter: @qrs
Web: https://trmm.net/

Xeno Kovah's speciality area is stealth malware and its ability to hide from security software and force security software to lie. To combat such attacks he researches trusted computing systems that can provide much stronger security guarantees than normal COTS. He co-founded LegbaCore in 2014 to help improve security at the foundation of computing systems. He is also the founder and lead contributor to OpenSecurityTraining.info. He has posted 9 full days of class material material on x86 assembly, architecture, binary formats (PE and ELF), and Windows rootkits to OpenSecurityTraining.info.
Twitter: @XenoKovah
Twitter: @legbacore

Corey Kallenberg is a co-founder of LegbaCore, a consultancy focused on evaluating and improving host security at the lowest levels. His specialty areas are trusted computing, vulnerability research and low level development. In particular, Corey has spent several years using his vulnerability research expertise to evaluate limitations in current trusted computing implementations. In addition, he has used his development experience to create and improve upon trusted computing applications. Among these are a timing based attestation agent designed to improve firmware integrity reporting, and an open source Trusted Platform Module driver for Windows. Corey is also an experienced trainer, having created and delivered several technical courses. He is an internationally recognized speaker who has presented at BlackHat USA, DEF CON, CanSecWest, Hack in the Box, NoSuchCon, SyScan, EkoParty and Ruxcon.
Twitter: @CoreyKal
Twitter: @legbacore

Rocking the Pocket Book: Hacking Chemical Plant for Competition and Extortion

Marina Krotofil, Senior Security Consultant. European Network for Cyber Security
Jason Larsen, Principal Security Consultant, IOActive

The appeal of hacking a physical process is dreaming about physical damage attacks lighting up the sky in a shower of goodness. Let's face it, after such elite hacking action nobody is going to let one present it even at a conference like DEF CON. As a poor substitute, this presentation will get as close as using a simulated plant for Vinyl Acetate production for demonstrating a complete attack, from start to end, directed at persistent economic damage to a production site while avoiding attribution of production loss to a cyber-event. Such an attack scenario could be useful to a manufacturer aiming at putting competitors out of business or as a strong argument in an extortion attack.

Picking up a paper these days it's easy to find an article on all the "SCADA insecurity" out there associated with an unstoppable attacker with unsophisticated goal of kicking up another apocalypse. Sorry to disappoint excited crowd but formula "Your wish is my command" does not work for control systems. The target plant is not designed in a hacker friendly way. Hopefully by the end of the

presentation, the audience will understand the difference between breaking into the system and breaking the system, obtaining control and being in control. An attacker targeting a remote process is not immediately gifted with complete knowledge of the process and the means to manipulate it. In general, an attacker follows a series of stages before getting to the final attack. Designing an attack scenario is a matter of art as much as economic consideration. The cost of attack can quickly exceed damage worth. Also, the attacker has to find the way to compare between competing attack scenarios.

In traditional IT hacking, a goal is to go undetected. In OT (operational technologies) hacking this is not an option. An attack will change things in the real world that cannot be removed by simply erasing the log files. If a piece of equipment is damaged or if a plant suddenly becomes less profitable, it will be investigated. The attacker has to create forensic footprint for investigators by manipulating the process and the logs in such a way that the analysts draw the wrong conclusions.

Exploiting physical process is an exotic and hard to develop skill which have so far kept a high barrier to entry. Therefore real-world control system exploitation has remained in the hands of a few. To help the community mastering new skills we have developed "Damn Vulnerable Chemical Process" - first open source framework for cyber-physical experimentation based on two realistic models of chemical plants. Come to the session and take your first master class on complex physical hacking.

Marina is Senior Security Consultant at European Network for Cyber Security. Through her life she has accumulated vast hands-on experience in several engineering fields. Most recently she completed her doctoral degree in ICS security at Hamburg University of Technology, Germany. Her research over the last few years has been focused on the bits and peac.hes of the design and implementation of cyber-physical attacks aiming at both physical and economic damage. Marina used her pioneering destructive knowledge for designing process-aware defensive solutions and risk assessment approaches. During her PhD she collaborated with several industrial partners, participated in EU projects and collaborated with cool dudes from the hacking community. She has written more than a dozen papers on the subject of cyber-physical exploitation. Marina gives workshops on cyber-physical exploitation and is a frequent speaker at the leading ICS security and hacking venues around the world. She holds MBA in Technology Management, MSc in Telecommunications and MSc in Information and Communication Systems.

Jason Larsen is a professional hacker that specializes in critical infrastructure and process control systems. Over the last several years he has been doing focused research into remote physical damage. Jason graduated from Idaho State University where he worked doing Monte Carlo and pharmacokinetic modeling for Boron-Neutron Capture Therapy. He was one of the founding members of the Cyber-Security department at the Idaho National Labs, which hosts the ICS -CERT and the National SCADA Tested .Jason has audited most of the major process control and SCADA systems as well as having extensive experience doing penetration tests against live systems. His other activities include two years on the Window 7 penetration testing team, designing the anti-malware system for a very large auction site, and building anonymous relay networks. He is currently a Principle Security Consultant for IOActive in Seattle.

Hack the Legacy! IBM i (aka AS/400) Revealed.

Bart Kulach (Bartlomiej Jakub Kulach), Security Researcher

Have you ever heard about the famous "green screen"? No, it's not a screensaver... Believe me, it still does exist!
In many industries, although the front-end systems are all new and shiny, in the back-end they still rely on well-known, proven IBM i (aka AS/400) technology for their back-office, core systems. Surprisingly, nobody truly seems to care about the security. Even if these nice IBM heavy black boxes are directly connected to the Internet...

The aim of the talk is to give you more insight in a number of techniques for performing a security test of / securing an IBM i system from perspective of an external and internal intruder. Methods like privilege escalation by nested user switching, getting full system access via JDBC or bypassing the "green screen" (5250) limitations will be presented.

Last but not least: I will also show a undocumented output format of the built-in password transfer API, giving you direct access to all password hashes. Even IBM engineers may wonder...

Bart Kulach: Aged 31, with 14 years of work experience within IT security, risk management and IT operations. Security specialist and experienced supervisor for IT audits, CISA, CISM. Working currently for NN Group in the Netherlands as coordinator for IT audits within Investment and Insurance business units in Europe and Asia. The past 7 years he held various security and risk management related positions. Focused on security of IBM i (aka AS/400, iSeries), website security as well as lean IT processes and architecture.
Facebook: (bart.kulach)

Remote Access, the APT

Ian Latter, Midnight Code

ThruGlassXfer (TGXf) is a new and exciting technique to steal files from a computer through the screen.
Any user that has screen and keyboard access to a shell (CLI, GUI or browser) in an enterprise IT environment has the ability to transfer arbitrary data, code and executables in and out of that environment without raising alarms, today. This includes staff, partners and suppliers, both on and off-shore. And implementation of best practice Data Center (Jump hosts), Perimeter / Remote Access (VPN, VDI, ..) and End Point Security (DLP, AV, ..) architectures have no effect on the outcome.

In this session I will take you from first principles to a full exploitation framework. At the end of the session you'll learn how build on this unidirectional file transfer and augment the solution into a full duplex communications channel (a virtual serial link) and then a native PPP link, from an user owned device, through the remote enterprise-controlled screen and keyboard, to the most sensitive infrastructure in the enterprise. In this special DEF CON presentation I will also be releasing the new high-speed data exfiltration tool, hsTGXf.

This is an exciting and cross-discipline presentation that picks up the story in the DEC VT220 terminal era and will take you on a journey to exploiting modern enterprise security architectures. So join me, whatever your knowledge or skill-set and learn something interesting!

A 20 year veteran of the IT industry, Ian has spent 15 years working in security in a number of positions including Penetration Tester, Security Architect and most recently, a Security Governance role at a blue chip corporate. Ian teaches the Practical Threat Intelligence course at Black Hat and has spoken at key international hacking and security conferences including COSAC (Ireland), Ruxcon (Australia), and Kiwicon (New Zealand). If he had spare time, Ian would be pursuing a number of private software and robotics projects, including the Barbie Car that he promised his daughter (wiser friends have advised that I finish this project before she's old enough to ask for a real Corvette).

Let's Talk About SOAP, Baby. Let's Talk About UPNP

Ricky "HeadlessZeke" Lawshae, Security Researcher, HP TippingPoint

Whether we want it to be or not, the Internet of Things is upon us. Network interfaces are the racing stripes of today's consumer device market. And if you put a network interface on a device, you have to make it do something right? That's where a Simple Object Access Protocol (SOAP) service comes in. SOAP services are designed with ease-of-access in mind, many times at the expense of security. Ludicrous amounts of control over device functionality, just about every category of vulnerability you can think of, and an all-around lack of good security practice about sums it up. In this talk, I will discuss this growing attack surface, demonstrate different methods for attacking/fuzzing it, and provide plenty of examples of the many dangers of insecure SOAP/ UPnP interfaces on embedded and "smart" devices along the way.

Ricky "HeadlessZeke" Lawshae is a Security Researcher for DVLabs at HP TippingPoint with a medium-sized number of years' experience in professionally voiding warranties. He has spoken at the DEF CON, Recon, Insomni'hack, and Ruxcon security conferences, and is an active participant in the extensive Austin, TX hacker community. In his meager spare time, he enjoys picking locks, reading comic books, and drinking expensive beers.

Twitter: @HeadlessZeke

Tell me who you are and I will tell you your lock pattern

Marte Løge, Security Researcher

You are predictable. Your passwords are predictable, and so are your PINs. This fact is being used by the hackers, as well as the agencies watching you. But what about your Android lock patterns? Can who you are reveal what patterns you create?

This presentation will present the result from an analysis of 3400 user-selected patterns. The interesting part is that we collected additional information about the respondents, not just the patterns themselves.

Will being left-handed and having experience with security affect the way you create your lock patterns? There are 389,112 possible patterns. Your full device encryption won't save you if your lock pattern is L - as in "looser".

Marte has just finished her master degree in computer science at the Norwegian University of Technology and Science (...NUTS <3) and has discovered the beauty of security.

She likes passwords and colors, resulting in a special interest in graphical passwords. She is probably the only person that has survived after studying the Android Pattern Lock for a whole year.

Responsible Incident: Covert Keys Against Subverted Technology Latencies, Especially Yubikey

LosT

We're no strangers to love
You know the rules and so do I
A full commitment's what I'm thinking of
You wouldn't get this from any other guy
I just wanna tell you how I'm feeling
Gotta make you understand

Never gonna give you up
Never gonna let you down
Never gonna run around and desert you
Never gonna make you cry
Never gonna say goodbye
Never gonna tell a lie and hurt you

LosT also runs the annual Mystery Box Challenge contest at DEF CON, which he launched at DEF CON 9. L0s7 says he likes to create the kind of challenges and puzzles that he wishes someone else would create for him to solve. 1057 has allegedly created the badges for DEF CON 23. Lo5t also appreciates jokes.

Twitter: @1o57
Web: www.LostboY.net

F*ck the attribution, show us your .idb!

Morgan Marquis-Boire, Senior Researcher, Citizen Lab
Marion Marschalek, Malware reverse engineer, Cyphort Inc
Claudio Guarnieri, Creator and lead developer, Cuckoo Sandbox

Over the past few years state-sponsored hacking has received attention that would make a rockstar jealous. Discussion of malware has shifted in focus from 'cyber crime' to 'cyber weapons', there have been intense public debates on attribution of various high profile attacks, and heated policy discussion surrounding regulation of offensive tools. We've also seen the sale of 'lawful intercept' malware become a global trade.

While a substantial focus has revolved around the activities of China, Russia, and Iran, recent discoveries have revealed the capabilities of Western nations such as WARRIORPRIDE aka. Regin (FVEY) and SNOWGLOBE aka. Babar (France). Many have argued that digital operations are a logical, even desirable part of modern statecraft. The step from digital espionage to political persecution is, however, a small one. Commercially written, offensive software from companies like FinFisher and Hacking Team has been sold to repressive regimes under the guise of 'governmental intrusion' software.

Nation state hacking operations are frequently well-funded, difficult to attribute, and rarely prosecuted even if substantive evidence can be discovered. While efforts have been made to counter this problem, proof is hard to find and even more difficult to correctly interpret. This creates a perfect storm of conditions for lies, vendor lies, and flimsy attribution.

In this talk we will unveil the mess happening backstage when uncovering nation state malware, lead the audience on the track of actor attribution, and cover what happens when you find other players on the hunt. We will present a novel approach to binary stylometry, which helps matching binaries of equal authorship and allows credible linking of binaries into the bigger picture of an attack. After this session the audience will have a better understanding of what happened behind the scenes when the next big APT report surfaces.

Morgan Marquis-Boire is a Senior Researcher at the Citizen Lab, University of Toronto. He is the Director of Security for First Look Media and a contributing writer for The Intercept. Prior to this, he worked on the security team at Google. He is a Special Advisor to the Electronic Frontier Foundation in San Francisco and an Advisor to the United Nations Inter-regional Crime and Justice Research Institute. In addition to this, he serves as a member of the Freedom of the Press Foundation advisory board and as an advisor to Amnesty International.

Marion is a malware reverse engineer on duty for Cyphort Inc., focussing on the analysis of emerging threats and exploring novel methods of threat detection. She teaches malware analysis at University of Applied Sciences St. Pölten and frequently appears as speaker at international conferences. Two years ago Marion won Halvar Flake's reverse engineering challenge for females, since then she set out to threaten cyber criminals. She practices martial arts and has a vivid passion for taking things apart. Preferably, other people's things.

Claudio is a security researcher mostly specialized in the analysis of malware, botnets and computer attacks in general. He's a core member of The Honeynet Project and created the open source malware analysis software Cuckoo Sandbox and Viper and runs the Malwr free service. Claudio published abundant research on botnets and targeted attacks and presented at conferences such as Hack In The Box, BlackHat, Chaos Communication Congress and many more. In recent years he devoted his

attention especially on issues of privacy and surveillance and published numerous articles on surveillance vendors such as FinFisher and HackingTeam with the Citizen Lab as well as on NSA/GCHQ and Five Eyes surveillance capabilities with The Intercept and Der Spiegel. Claudio also contributes to Global Voices Advocacy. He continuously researches and writes on government surveillance and threats to journalists and dissidents worldwide and supports human rights organisations with operational security and emergency response.

Inter-VM data exfiltration: The art of cache timing covert channel on x86 multi-core

Etienne Martineau, Software engineer, Cisco Systems

On x86 multi-core covert channels between co-located Virtual Machine (VM) are real and practical thanks to the architecture that has many imperfections in the way shared resources are isolated.

This talk will demonstrate how a non-privileged application from one VM can ex-filtrate data or even establish a reverse shell into a co-located VM using a cache timing covert channel that is totally hidden from the standard access control mechanisms while being able to offer surprisingly high bps at a low error rate.

In this talk you'll learn about the various concepts, techniques and challenges involve in the design of a cache timing covert channel on x86 multi-core such as:

- An overview of some of the X86 shared resources and how we can use / abuse them to carry information across VMs.
- Fundamental concept behind cache line encoding / decoding.
- Getting around the hardware pre-fetching logic (without disabling it from the BIOS!)
- Data persistency and noise. What can be done?
- Guest to host page table de-obfuscation. The easy way.
- Phase Lock Loop and high precision inter-VM synchronization. All about timers.

At the end of this talk we will go over a working VM to VM reverse shell example as well as some surprising bandwidth measurement results. We will also cover the detection aspect and the potential countermeasure to defeat such a communication channel. The source code is going to be release at that time on 'github'

Etienne holds bachelor's degree in electrical engineering from University Laval at Quebec and is currently a senior technical leader at Cisco Systems. He has over 15 years' mission critical Linux in telecom and space industry experience. His career has covered broad range of high performance / high availability hardware and software technologies, system level architecture and since 2008 a very special focus on the KVM hypervisor. He likes to work on complex and challenging problems but when not working, he likes to spend time with his family and during the night hack virtual machines or rebuild car engines.

Working together to keep the Internet safe and secure

Alejandro Mayorkas , Deputy Secretary of Homeland Security

We all have a role to play when it comes to ensuring the safety and security of the Internet, whether you are a federal employee, the CEO of a company, or a private citizen. Today's threats require the engagement of our entire society. This shared responsibility means that we have to work with each other in ways that is often new for the government and the private sector. This means that we also have to trust each other and share information. While we have achieved some successes, we have much more work to do. Deputy Secretary Mayorkas will highlight the role that DHS plays in securing the Internet and discuss the challenges and opportunities to collaborate across our society and across borders.

Alejandro Mayorkas was sworn in as Deputy Secretary of Homeland Security on December 23, 2013. Since 2009, following his nomination by President Obama and subsequent confirmation, Deputy Secretary Mayorkas served as the Director of the Department of Homeland Security's United States Citizenship and Immigration Services (USCIS), the agency charged with operating the largest immigration system in the world. In that position, he led a workforce of 18,000 members throughout more than 250 offices worldwide and oversaw a $3 billion annual budget. While at USCIS he oversaw a number of important programs and enhancements, including the implementation of Deferred Action for Childhood Arrivals (DACA) as well as important reforms that safeguard our nation's security, and ensure the integrity of the immigration system.

Prior to his appointment at USCIS, Deputy Secretary Mayorkas was a partner in the law firm of O'Melveny & Myers LLP. In 2008, the National Law Journal recognized Deputy Secretary Mayorkas as one of the "50 Most Influential Minority Lawyers in America."

In 1998, Deputy Secretary Mayorkas was nominated by President Clinton and confirmed by the Senate to be the United States Attorney for the Central District of California, becoming the youngest U.S. Attorney to serve the nation at that time. In addition to leading an office of 240 Assistant U.S. Attorneys, Mayorkas served as the ViceChair of the Attorney General's Advisory Subcommittee on Civil Rights and as a member of the Subcommittee on Ethics in Government. From 1989 to 1998, Mayorkas served as an Assistant U.S. Attorney for the Central District of California.

Deputy Secretary Mayorkas is a graduate of the University of California at Berkeley and received his law degree from Loyola Law School.

I Hunt Penetration Testers: More Weaknesses in Tools and Procedures

Wesley McGrew, Assistant Research Professor Distributed Analytics and Security Institute, Mississippi State University

When we lack the capability to understand our tools, we operate at the mercy of those that do. Penetration testers make excellent targets for bad actors, as the average tester's awareness and understanding of the potential risks and vulnerabilities in their tools and processes is low, and the value

of the information they gather and gain access to among their client base is very high. As demonstrated by Wesley's DEF CON 21 talk on vulnerabilities in penetration testing devices, and last year's compromise of WiFi Pineapple devices, the tools of offensive security professionals often represent a soft target. In this talk, operational security issues facing penetration testers will be discussed, including communication and data security (not just "bugs"), which impact both testers and clients. A classification system for illustrating the risks of various tools is presented, and vulnerabilities in specific hardware and software use cases are presented. Recommendations are made for improving penetration testing practices and training. This talk is intended to be valuable to penetration testers wanting to protect themselves and their clients, and for those who are interesting in profiling weaknesses of opposing forces that may use similar tools and techniques.

Wesley McGrew (@McGrewSecurity) is an assistant research professor at Mississippi State University's Distributed Analytics and Security Institute. At DASI, he is involved in malware and vulnerability research. In the spring 2013 semester, he began teaching a self-designed course on reverse engineering to students at MSU, using real-world, high-profile malware samples, as part of gaining NSA CAE Cyber Ops certification for MSU. Wesley has presented at Black Hat USA and DEF CON on forensics, malware, and penetration testing topics, and is the author of security and forensics tools that he publishes through his personal/consultancy website, McGrewSecurity.com.

Twitter: @mcgrewsecurity

How to Hack Government: Technologists as Policy Makers

Terrell McSweeny, Commissioner, Federal Trade Commission
Ashkan Soltani, Chief Technologist, Federal Trade Commission

As the leading federal agency responsible for protecting your privacy rights online, technology is at the core of the Federal Trade Commission's work. You may be familiar with the agency's enforcement actions against some of the world's biggest tech companies for privacy/data security violations - but you may not know how your research skills can inform its investigations and policy. Come hear about some of the Commission's recent tech-related actions, research and reports, plus how its work impacts both consumers and businesses. You'll also learn how you can directly or indirectly help the agency protect consumers, guide businesses to develop better/strong data security, and much more.

Terrell McSweeny serves as a Commissioner of the Federal Trade Commission - sometimes referred to as the Federal Technology Commission. This year marks her second DEF CON adventure. When it comes to tech issues, Commissioner McSweeny wants companies to implement security by design, to be transparent about their data collection practices, and to give consumers as much control as possible.
Twitter: @TMcSweenyFTC

Ashkan Soltani serves as the FTC's fourth Chief Technologist. He is a privacy and security researcher whose work draws attention to privacy problems online, demystifies technology for the non-technically inclined, and provides data-driven insights to help inform policy. Ashkan was recognized as part of the

2014 Pulitzer winning team at the Washington Post and was the primary technical consultant on the Wall Street Journal's "What They Know" investigative series on online privacy.
Twitter: @TechFTC

Red vs. Blue: Modern Active Directory Attacks & Defense

Sean Metcalf, CTO, DAn Solutions, Inc.

Kerberos "Golden Tickets" were unveiled by Alva "Skip" Duckwall & Benjamin Delpy in 2014 during their Black Hat USA presentation. Around this time, Active Directory (AD) admins all over the world felt a great disturbance in the Force. Golden Tickets are the ultimate method for persistent, forever AD admin rights to a network since they are valid Kerberos tickets and can't be detected, right?

This talk explores the latest Active Directory attack vectors and describes how Golden Ticket usage can be detected. When forged Kerberos tickets are used in AD, there are some interesting artifacts that can be identified. Yes, despite what you may have read on the internet, there are ways to detect Golden & Silver Ticket usage.

Skip the fluff and dive right into the technical detail describing the latest methods for gaining and maintaining administrative access in Active Directory, including some sneaky AD persistence methods. Also covered are traditional security measures that work (and ones that don't) as well as the mitigation strategies that disrupts the attacker's preferred game-plan. Prepare to go beyond "Pass-the-Hash" and down the rabbit hole.

Some of the topics covered:

- Sneaky persistence methods attackers use to maintain admin rights.
- How attackers go from zero to (Domain) Admin
- MS14-068: the vulnerability, the exploit, and the danger.
- "SPN Scanning" with PowerShell to identify potential targets without network scans (SQL, Exchange, FIM, webservers, etc.).
- Exploiting weak service account passwords as a regular AD user.
- Mimikatz, the attacker's multi-tool.
- Using Silver Tickets for stealthy persistence that won't be detected (until now).
- Identifying forged Kerberos tickets (Golden & Silver Tickets) on your network.
- Detecting offensive PowerShell tools like Invoke-Mimikatz.
- Active Directory attack mitigation.

Kerberos expertise is not required since the presentation covers how Active Directory leverages Kerberos for authentication identifying the areas useful for attack. Information presented is useful for both Red Team & Blue Team members.

Sean Metcalf is the Chief Technology Officer at DAn Solutions, a company that provides Microsoft platform engineering and security expertise. Mr. Metcalf is one of about 100 people in the world who holds the elite Microsoft Certified Master Directory Services (MCM) certification. Furthermore, he assisted Microsoft in developing the Microsoft Certified Master Directory Services certification program for Windows Server 2012.

Mr. Metcalf has provided Active Directory and security expertise to government, corporate, and educational entities since Active Directory was released. He currently provides security consulting services to customers with large Active Directory environments and regularly posts useful Active Directory security information on his blog, ADSecurity.org. Follow him on Twitter @PyroTek3

Twitter: @PyroTek3
Web: ADSecurity.org

Put on your tinfo_t hat if you're my type

miaubiz, Senior Dr. at Azimuth Security

The IDA Pro APIs for interacting with type information are full of opportunities (horrible problems). I will show you how to create unparseable types, how to apply these types to functions and variables and how to transfer these types from one IDB to another.

miaubiz is a senior doctor of security at Azimuth Security. he has previously found bugs in web browsers and has spoken at SyScan, Infiltrate, T2. his interests are bad APIs and sniffing ARMpits.

Remote Exploitation of an Unaltered Passenger Vehicle

Charlie Miller, Security engineer at Twitter
Chris Valasek, Director of Vehicle Security Research at IOActive

Although the hacking of automobiles is a topic often discussed, details regarding successful attacks, if ever made public, are non-comprehensive at best. The ambiguous nature of automotive security leads to narratives that are polar opposites: either we're all going to die or our cars are perfectly safe. In this talk, we will show the reality of car hacking by demonstrating exactly how a remote attack works against an unaltered, factory vehicle. Starting with remote exploitation, we will show how to pivot through different pieces of the vehicle's hardware in order to be able to send messages on the CAN bus to critical electronic control units. We will conclude by showing several CAN messages that affect physical systems of the vehicle. By chaining these elements together, we will demonstrate the reality and limitations of remote car attacks.

Charlie Miller is a security engineer at Twitter, a hacker, and a gentleman. Back when he still had time to research, he was the first with a public remote exploit for both the iPhone and the G1 Android phone. He is a four time winner of the CanSecWest Pwn2Own competition. He has authored three information security books and holds a PhD from the University of Notre Dame. He has hacked browsers, phones, cars, and batteries. Charlie spends his free time trying to get back together with Apple, but sadly they still list their relationship status as "It's complicated".
Twitter: @0xcharlie

Christopher Valasek is the Director of Vehicle Security Research at IOActive, an industry leader in comprehensive computer security services. Valasek specializes in offensive research methodologies

with a focus in reverse engineering and exploitation. Valasek is known for his extensive research in the automotive field and his exploitation and reverse engineering of Windows. Valasek is also the Chairman of SummerCon, the nation's oldest hacker conference. He holds a B.S. in Computer Science from the University of Pittsburgh.

Twitter: @nudehaberdasher

Separating Bots from the Humans

Ryan Mitchell, Software Engineer, LinkeDrive Inc

There's an escalating arms race between bots and the people who protect sites from them. Bots, or web scrapers, can be used to gather valuable data, probe large collections of sites for vulnerabilities, exploit found weaknesses, and are often unfazed by traditional solutions like robots.txt files, Ajax loading, and even CAPTCHAs. I'll give an overview of both sides of the battle and explain what what really separates the bots from the humans. I'll also demonstrate and easy new tool that can be used to crack CAPTCHAs with high rates of success, some creative approaches to honeypots, and demonstrate how to scrape many "bot-proof" sites.

Ryan Mitchell is Software Engineer at LinkeDrive in Boston, where she develops their API and data analysis tools. She is a graduate of Olin College of Engineering, and is a masters degree student at Harvard University School of Extension Studies. Prior to joining LinkeDrive, she was a Software Engineer building web scrapers and bots at Abine Inc, and regularly does freelance work, building web scrapers for clients, primarily in the financial and retail industries.

Ryan is also the author of two books: "Instant Web Scraping with Java" (Packt Publishing, 2013) and "Web Scraping with Python" (O'Reilly Media, 2015)

Twitter: @Kludgist
Amazon Author Page: http://www.amazon.com/Ryan-Mitchell/e/B00MQI8TVQ
Website: http://ryanemitchell.com

Spread Spectrum Satcom Hacking: Attacking The GlobalStar Simplex Data Service

Colby Moore, Manager of Special Activities, Synack

Recently there have been several highly publicized talks about satellite hacking. However, most only touch on the theoretical rather than demonstrate actual vulnerabilities and real world attack scenarios. This talk will demystify some of the technologies behind satellite communications and do what no one has done before - take the audience step-by-step from reverse engineering to exploitation of the GlobalStar simplex satcom protocol and demonstrate a full blown signals intelligence collection and spoofing capability. I will also demonstrate how an attacker might simulate critical conditions in satellite connected SCADA systems.

In recent years, Globalstar has gained popularity with the introduction of its consumer focused SPOT asset-tracking solutions. During the session, I'll deconstruct the transmitters used in these (and commercial) solutions and reveal design and implementation flaws that result in the ability to intercept, spoof, falsify, and intelligently jam communications. Due to design tradeoffs these vulnerabilities are realistically unpatchable and put millions of devices, critical infrastructure, emergency services, and high value assets at risk.

Colby Moore is Synack's Manager of Special Activities. He works on the oddball and difficult problems that no one else knows how to tackle and strives to embrace the attacker mindset during all engagements. He is a former employee of VRL and has identified countless 0day vulnerabilities in embedded systems and major applications. In his spare time you will find him focusing on that sweet spot where hardware and software meet, usually resulting in very interesting consequences.
Twitter: @colbymoore

Docker, Docker, Give Me The News, I Got A Bad Case Of Securing You

David Mortman, Chief Security, Architect & Distinguished Engineer, Dell Software

Docker is all the rage these days. Everyone is talking about it and investing in it, from startups to enterprises and everything in between. But is it secure? What are the costs and benefits of using it? Is this just a huge risk or a huge opportunity? There's a while lot of ranting and raving going on, but not nearly enough rational discourse. I'll cover the risks and rewards of using Docker and similar technologies such as AppC as well as discuss the larger implications of using orchestration systems like Mesos or Kubernetes. This talk will cover the deep technical issues to be concerned about as well as the pragmatic realities of the real world.

David Mortman is the Chief Security Architect and Distinguished Engineer at Dell Software and is a Contributing Analyst at Securosis. Before Dell, he ran operations and security for C3. Formerly the Chief Information Security Officer for Siebel Systems, Inc., Previously, Mr. Mortman was Manager of IT Security at Network Associates. Mr. Mortman has also been a regular panelist and speaker at RSA, Blackhat, DEF CON and BruCon as well. Mr.Mortman sits on a variety of advisoryboards including Qualys, Lookout and Risk I/O. He holds a BS in Chemistry from the University of Chicago. David writes for Securosis, Emergent Chaos and the New School blogs.

Detecting Randomly Generated Strings; A Language Based Approach

Mahdi Namazifar, Senior Data Scientist, Talos Team, Cisco Systems

Numerous botnets employ domain generation algorithms (DGA) to dynamically generate a large number of random domain names from which a small subset is selected for their command and control. A vast majority of DGA algorithms create random sequences of characters. In this work we present a

novel language-based technique for detecting strings that are generate by chaining random characters. To evaluate randomness of a given string (domain name in this context) we lookup substrings of the string in the dictionary that we've built for this technique, and then we calculate a randomness score for the string based on several different factors including length of the string, number of languages that cover the substrings, etc. This score is used for determining whether the given string is a random sequence of characters. In order to evaluate the performance of this technique, on the one hand we use 9 known DGA algorithms to create random domain names as DGA domains, and on the other hand we use domain names from the Alexa 10,000 as likely non-DGA domains. The results show that our technique is more than 99% accurate in detecting random and non-random domain names.

Mahdi Namazifar is currently a Senior Data Scientist with Talos team of Cisco Systems' San Francisco Innovation Center (SFIC). He graduated his PhD in Operations Research from the University of Wisconsin-Madison in 2011. His PhD work was on theoretical and computational aspects of mathematical optimization. During his PhD Mahdi was also affiliated with Wisconsin Institute for Discovery (WID) and the French Institute for Research in Computer Science and Automation (INRIA). Also he was a National Science Foundation (NFS) Grantee at the San Diego Supercomputer Center in 2007 and a Research Intern at IBM T.J. Watson Research Lab in 2008. After graduate school and before his current position at Cisco he was a Scientist at Opera Solutions working on applications of machine learning in a variety of problems coming from industries such as healthcare and finance.

Don't Whisper my Chips: Sidechannel and Glitching for Fun and Profit

Colin O'Flynn, Dalhousie University

If you thought the security practices of regular software was bad, just wait until you start learning about the security of embedded hardware systems. Recent open-source hardware tools have made this field accessible to a wider range of researchers, and this presentation will show you how to perform these attacks for equipment costing $200.

Attacks against a variety of real systems will be presented: AES-256 bootloaders, internet of things devices, hardware crypto tokens, and more. All of the attacks can be replicated by the attendees, using either their own tools if such equipped (such as oscilloscopes and pulse generators), the open-hardware ChipWhisperer-Lite, or an FPGA board of their own design.

The hands-on nature of this talk is designed to introduce you to the field, and give you the confidence to pick up some online tutorials or books and work through them. Even if you've never tried hardware hacking before, the availability of open-source hardware makes it possible to follow published tutorials and learn all about side-channel power analysis and glitching attacks for yourself.

Colin O'Flynn has been working with security on embedded systems for several years. He has designed the open-source ChipWhisperer project which won 2nd place in the 2014 Hackaday Prize, and developed an even lower-cost version called the ChipWhisperer-Lite, which was the focus of a Kickstarter in 2015.

Twitter: @colinoflynn

Advances in Linux Process Forensics Using ECFS

Ryan O'Neill, Security Consultant, Leviathan Security Group

Many hackers today are using process memory infections to maintain stealth residence inside of a compromised system. The current state of forensics tools in Linux, lack the sophistication used by the infection methods found in real world hacks. ECFS (Extended core file snapshot) technology, https://github.com/elfmaster/ecfs is an innovative extension to regular ELF core files, designed to be used as forensics-friendly snapshots of process memory. A brief showcasing of the ECFS technology was featured in POC||GTFO 0x7 (Innovations with core files).

However this talk will reveal deeper insight on the many features of this technology, such as full symbol table reconstruction, builtin detection heuristics, and how common binutils such as objdump, and readelf can be used to quickly identify complex infections such as PLT/GOT hooks and shared library injection. We will also cover the libecfs API that was created specifically for malware and forensics analysts who aim to implement support for ECFS snapshots into new or existing malware detection software.
While the ECFS core format was initially designed for runtime malware and forensics purposes, another very neat aspect to this technology was quickly extrapolated on; the ECFS snapshots can also be reloaded into memory and executed. Very similar to VM snapshots, which opens many more doors for research and exploration in a vast array of areas from dynamic analysis to migrating live processes across systems. ECFS is still a work in progress, but for those who understand the arduous nature of dissecting a process and identifying anomalies, will surely acquire a quick respect for the new technology that makes all of this so much easier.

Ryan 'elfmaster' O'Neill is a computer security researcher at Leviathan Security and the maintainer of Bitlackeys.org, a hub for much of his independent research. He is a Reverse engineer, and a Software engineer, who also specializes in the ELF binary format, and delivers on going workshops in this area to interested parties, including the US government. Ryan has worked on many security technologies including but not limited to:

- *Maya's Veil : anti-tamper / anti-exploitation protection for Linux ELF binaries*
- *VMA Vudu : automated forensics analysis of process runtime infections in Linux*
- *kernelDetective : Linux kernel forensics software*

Ryan has produced alot of research and publications in areas pertaining to Linux kernel and userland malware, such as "Linux kprobe instrumentation from phrack 66", and is author of soon to be released book "The art of Linux binary analysis" which focuses on everything from ELF internals to Linux Viruses, and Binary protection techniques. Ryan has been involved in the computer security scene since 1999.

Ask the EFF: The Year in Digital Civil Liberties

Kurt Opsahl, General Counsel, Electronic Frontier Foundation
Nate Cardozo, EFF Staff Attorney

Mark Jaycox, EFF Legislative Analyst
Corynne McSherry, EFF Legal Director
Nadia Kayyali, EFF Activist
Peter Eckersley, EFF Technology Projects Director

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 session will include updates on current EFF issues such as surveillance online 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. Half the session will be given over to question-and-answer, so it's your chance to ask EFF questions about the law and technology issues that are important to you.

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.

Nate Cardozo is a 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.

Mark Jaycox is a Legislative Analyst for EFF. His issues include user privacy, civil liberties, surveillance law, and "cybersecurity." When not reading legal or legislative documents, Mark can be found reading non-legal and legislative documents, exploring the Bay Area, and riding his bike. He was educated at Reed College, spent a year abroad at the University of Oxford (Wadham College), and concentrated in Political History. The intersection of his concentration with advancing technologies and the law was prevalent throughout his education, and Mark's excited to apply these passions to EFF. Previous to

joining EFF, Mark was a Contributor to ArsTechnica, and a Legislative Research Assistant for LexisNexis.

Peter Eckersley is Technology Projects Director for the Electronic Frontier Foundation. He leads a team of technologists who watch for technologies that, by accident or design, pose a risk to computer users' freedoms-and then look for ways to fix them. They write code to make the Internet more secure, more open, and safer against surveillance and censorship. They explain gadgets to lawyers and policymakers, and law and policy to gadgets. Peter's work at EFF has included privacy and security projects such as the Let's Encrypt CA, Panopticlick, HTTPS Everywhere, SSDI, and the SSL Observatory; helping to launch a movement for open wireless networks; fighting to keep modern computing platforms open; and running the first controlled tests to confirm that Comcast was using forged reset packets to interfere with P2P protocols. Peter holds a PhD in computer science and law from the University of Melbourne; his research focused on the practicality and desirability of using alternative compensation systems to legalize P2P file sharing and similar distribution tools while still paying authors and artists for their work. He is an affiliate of the Center for International Security and Cooperation at Stanford University.

Nadia Kayyali is a member of EFF's activism team. Nadia's work focuses on surveillance, national security policy, and the intersection of criminal justice, racial justice, and digital civil liberties issues. Nadia has been an activist since high school, when they participated in the World Trade Organization protests in Seattle. Nadia is one of the creators of the Canary Watch website, which tracks and classifies warrant canaries.

Corynne McSherry is the Legal Director at EFF, specializing in intellectual property, open access, and free speech issues. Her favorite cases involve defending online fair use, political expression, and the public domain against the assault of copyright maximalists. As a litigator, she has represented Professor Lawrence Lessig, Public.Resource.Org, the Yes Men, and a dancing baby, among others, and one of her first cases at EFF was In re Sony BMG CD Technologies Litigation (aka the "rootkit" case). Her policy work includes leading EFF's effort to fix copyright (including the successful effort to shut down the Stop Online Privacy Act, or SOPA), promote net neutrality, and promote best practices for online expression. In 2014, she testified before Congress about problems with the Digital Millennium Copyright Act. Corynne comments regularly on digital rights issues and has been quoted in a variety of outlets, including NPR, CBS News, Fox News, the New York Times, Billboard, the Wall Street Journal, and Rolling Stone. Prior to joining EFF, Corynne was a civil litigator at the law firm of Bingham McCutchen, LLP. Corynne has a B.A. from the University of California at Santa Cruz, a Ph.D from the University of California at San Diego, and a J.D. from Stanford Law School. While in law school, Corynne published Who Owns Academic Work?: Battling for Control of Intellectual Property (Harvard University Press, 2001).

Twitter: @eff, @kurtopsahl

DEF CON Comedy Inception: How many levels deep can we go?

Larry Pesce, Senior Security Analyst, InGuardians
Chris Sistrunk, Mandiant/FireEye
Adam Crain, Automatak
Chris Blow, Rook Security
Dan Tentler, Carbon Dynamics
Amanda Berlin, Hurricane Labs
Katie Moussouris, HackerOne

This year at DEF CON a former FAIL PANEL panelist attempts to keep the spirit alive by playing moderator. Less poetry, more roasting. A new cast of characters, more lulz, and no rules. Nothing is sacred, not the industry, not the audience, not even each other. Our cast of characters will bring you all sorts of technical fail, ROFLCOPTER to back it up. No waffles, but we have other tricks up our sleeve to punish, er, um, show love to our audience, all while raising money of the EFF and HFC. The FAIL PANEL may be dead, but the "giving" goes on.

Larry Pesce is a Senior Security Analyst with InGuardians. His recent experience includes providing penetration assessment, architecture review, hardware security assessment, wireless/radio analysis, and policy and procedure development for a wide range of industries including those in the financial, retail, and healthcare verticals.

Larry is an accomplished speaker, having presented numerous times at industry conferences as well as the co-host of the long running multi-award winning Security Podcast, Paul's Security Weekly. and is a certified instructor with the SANS Institute.

Larry is a graduate of Roger Williams University. In his spare time he likes to tinker with all things electronic and wireless. Larry is an amateur radio operator holding his Extra class license and is regularly involved in emergency communications activities.

In 1972 a crack commando unit was sent to prison by a military court for a crime they didn't commit. These men promptly escaped from a maximum security stockade.... making the decision to leave Amanda behind. Ms. Berlin is now rumored to have illegitimate children by Saudi Oil barons hidden all over the world in at least 27 countries but this can neither be confirmed nor denied.

Amanda Berlin is a Network Security Engineer at Hurricane Labs. She is most well known for being a breaker of hearts, knees, and SJW's. Bringing "Jack of All Trades" back to being sexy, she has worked her fingers to the bone securing ISPs, Healthcare facilities, Artificial Insemination factories, and brothels. Amanda managed the internal phishing campaign at a medium size healthcare facility to promote user education about phishing and hacking through an awards based reporting program. She is a lead organizer for CircleCityCon, volunteers at many other conferences, and enjoys writing and teaching others.

Twitter: @InfoSystir

Chris Blow is a Senior Technical Advisor with Rook Security. His most recent experience includes: penetration testing, social engineering, red team exercises, policy and procedure guidance focused on

HIPAA and PCI DSS, developing security awareness programs, performing HIPAA assessments and serving as a Qualified Security Assessor for the Payment Card Industry.

In reality, his primary duties are to be told by various clients that "security is hard" and to just "accept the risk." He's also well-versed in being told to keep vulnerable assets and people "out of scope."

Chris is a graduate of Purdue University in West Lafayette, IN. Besides trying to keep up with all-things-InfoSec, Chris enjoys playing guitar, singing, and DJing.

Twitter: @b10w

Katie Moussouris is the Chief Policy Officer for HackerOne, a platform provider for coordinated vulnerability response & structured bounty programs, though she is open to suggestions on how to make her title abbreviation C3PO because for once, these actually are the droids you're looking for. She is a noted authority on vuln disclosure & advises lawmakers, customers, & researchers to legitimize & promote security research & help make the internet safer for everyone. Katie fights for your right to party at ring zero, and get paid for it.

Katie's earlier Microsoft work encompassed industry-leading initiatives such as Microsoft's bounty programs & Microsoft Vulnerability Research. She is also a subject matter expert for the US National Body of the International Standards Organization (ISO) in vuln disclosure (29147), vuln handling processes (30111), and secure development (27034). Katie fell on some policy grenades for ya there, and you should take her to a karaoke bar to celebrate.

Katie is a visiting scholar with MIT Sloan School, doing research on the vulnerability economy and exploit market, because while she knows money can't buy you love, it can buy you bugs. Katie is a New America Foundation Fellow, and hopes to be a jolly good one, as she helps develop better policies. Katie is an ex-hacker, ex-Linux developer, and persistent disruptor. Follow her and HackerOne on Twitterhttp://twitter.com/k8em0 and http://twitter.com/hacker0x01 where you can expect to get some tweets talking nerdy to you, and some delivered in the Karaoke Message Control Protocol (KCMP).

Dan Tentler likes to break things. He's also an expert on failure. Ask him about it. But ask with scotch.

Twitter: @viss

@chrissistrunk, @jadamcrain, @b10w, @k8emo

Hacking Smart Safes: On the "Brink" of a Robbery

Dan "AltF4" Petro, Security Associate, Bishop Fox
Oscar Salazar, Senior Security Associate at Bishop Fox

Have you ever wanted to crack open a safe full of cash with nothing but a USB stick? Now you can!

The Brink's CompuSafe cash management product line provides a "smart safe as a service" solution to major retailers and fast food franchises. They offer end-to-end management of your cash, transporting it safely from your storefront safe to your bank via armored car.

During this talk, we'll uncover a major flaw in the Brink's CompuSafe and demonstrate how to crack one open in seconds flat. All you need is a USB stick and a large bag to hold all of the cash. We'll discuss how to remotely takeover the safe with full administrator privileges, and show how to enumerate a target list of other major Brink's CompuSafe customers (exposed via configuration files stored right on the safe).

At any given time, up to $240,000 can be sitting in each of the 14,000 Brink's CompuSafe smart safes currently deployed across the United States - potentially billions of dollars just waiting to be stolen.

So come ready to engage us as we explore these tools and more in this DEMO-rich presentation. And don't forget to call Kenny Loggins... because this presentation is your highway to the Danger Zone...

Note - This presentation is about exposing flaws in the Brinks's Compusafe to improve security and allow pentesters to demonstrate these flaws to their customers. Please use this information responsibly.

Dan Petro is a Security Associate at Bishop Fox (formerly Stach & Liu), 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 application penetration testing and secure development.

Dan has presented at numerous conferences, including DEF CON, BlackHat, HOPE, and BSides, and is the founding member of the Pi Backwards CTF team.

Prior to joining Bishop Fox, Dan served as Lead Software Engineer for a security contracting firm.

Dan holds a Bachelor of Science from Arizona State University with a major in Computer Science, as well as a Master's Degree in Computer Science from Arizona State University.

Oscar Salazar is a Senior Security Associate at Bishop Fox (formerly Stach & Liu), 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 application penetration testing, source code review, and secure software design.

Oscar has presented at RSA, Bsides, and Adobe's annual private Security Summit conference.

Prior to joining Bishop Fox, Oscar served as a web security research engineer at Hewlett-Packard's Application Security Center where he designed and developed security checks for the WebInspect web application security scanner. In addition, his research involved developing more effective methods of scanning Web 2.0 applications.

Oscar holds a Bachelor of Science from the Georgia Institute of Technology with a major in Computer Science and a focus on Networking and Security.

https://www.facebook.com/BishopFoxConsulting
https://twitter.com/bishopfox
https://www.linkedin.com/company/bishop-fox

Staying Persistent in Software Defined Networks

Gregory Pickett, Cybersecurity Operations, Hellfire Security

The Open Network Install Environment, or ONIE, makes commodity or WhiteBox Ethernet possible. By placing a common, Linux-based, install environment onto the firmware of the switch, customers can deploy the Network Operating Systems of their choice onto the switch and do so whenever they like without replacing the hardware. The problem is, if this gets compromised, it also makes it possible for hackers to install malware onto the switch. Malware that can manipulate it and your network, and keep doing it long after a Network Operating System reinstall.

With no secure boot, no encryption, no authentication, predictable HTTP/TFTP waterfalls, and exposed post-installation partition, ONIE is very susceptible to compromise. And with Network Operating Systems such as Switch Light, Cumulus Linux, and Mellanox-OS via their agents Indigo and eSwitchd not exactly putting up a fight with problems like no authentication, no encryption, poor encryption, and insufficient isolation, this is a real possibility.

In this session, we'll cover the weaknesses in ONIE, ways to reach the platform through these Network Operating Systems, and what can happen if we don't properly protect the Control Plane these switches run on. I'll even demonstrate with a drive-by web-attack that is able to pivot through a Windows management station to reach the isolated control plane network, and infect one of these ONIE-based switches with malware, malware that's there even after a refresh. You'll even get the source code to take home with you to see how easily it's done. Finally, we'll talk about how to compensate for these issues so that your network doesn't become infected with and manipulated by this sort of persistent firmware-level malware.

Gregory Pickett CISSP, GCIA, GPEN has a background in intrusion analysis for Fortune 100 companies but now heads up Hellfire Security's Managed Security Services efforts and participates in their assessment practice as a network security subject matter expert. As a security professional, his primary area of focus and occasional research is networks with an interest in using network traffic to better understand, to better defend, and sometimes to better exploit the hosts that live on them. He holds a B.S. in Psychology which is completely unrelated but interesting to know. While it does nothing to contribute to how he makes a living, it does demonstrate how screwed up he actually is.
Twitter: @Shogun7273

One Device to Pwn Them All

Dr. Phil Polstra, Professor, Bloomsburg University

This talk will present a device that can be used as a dropbox, remote hacking drone, hacking command console, USB writeblocker, USB Mass Storage device impersonator, or scripted USB HID device. The device is based on the BeagleBone Black, can be battery operated for several days, and is easily constructed for under $100.

The dropbox, remote hacking drone, and hacking command console functionality were presented at DEF CON 21. This talk will emphasize the new USB-based attack functionality. Topics will include injecting payloads by emulating an optionally write-protected USB mass storage device, rapidly executing commands on a target using the BeagleBone Black operating as a scripted USB HID device, USB mass storage device impersonation, and other attacks that can be performed with brief physical access to the target.

Some familiarity with Linux and USB devices would be helpful, but not required. All hardware and software to be discussed is 100% open source.

Phil was born at an early age. He cleaned out his savings at age 8 in order to buy a TI99-4A computer for the sum of $450. Two years later he learned 6502 assembly and has been hacking computers and electronics ever since.

Dr. Phil currently works as a professor at Bloomsburg University of Pennsylvania. His research focus over the last few years has been on the use of microcontrollers and small embedded computers for forensics and pentesting. Phil has developed a custom pentesting Linux distro and related hardware to allow an inexpensive army of remote pentesting drones to be built using the BeagleBone Black computer boards. This work is described in detail in Phil's book "Hacking and Penetration Testing With Low Power Devices" (Syngress, 2015).

Prior to entering academia, Phil held several high level positions at well-known US companies. He holds a couple of the usual certs one might expect for someone in his position. When not working, he likes to spend time with his family, fly, hack electronics, and has been known to build airplanes.

NetRipper - Smart traffic sniffing for penetration testers

Ionut Popescu, Senior Security Consultant at KPMG Romania

The post-exploitation activities in a penetration test can be challenging if the tester has low-privileges on a fully patched, well configured Windows machine. This work presents a technique for helping the tester to find useful information by sniffing network traffic of the applications on the compromised machine, despite his low-privileged rights. Furthermore, the encrypted traffic is also captured before being sent to the encryption layer, thus all traffic (clear-text and encrypted) can be sniffed. The implementation of this technique is a tool called NetRipper which uses API hooking to do the actions mentioned above and which has been especially designed to be used in penetration tests, but the concept can also be used to monitor network traffic of employees or to analyze a malicious application.

Ionut works as a Senior Security Consultant at KPMG in Romania. He is passionate about ASM, reverse engineering, shellcode and exploit development and he has a MCTS Windows Internals certification.

He spoke at various security conferences in Romania like: Defcamp, OWASP local meetings and others and also at the yearly Hacknet KPMG international conference in Helsinki and Berlin.

Ionut is also the main administrator of the biggest Romanian IT security community: rstforums.com and he writes technical articles on a blog initiated by a passionate team: securitycafe.ro.

Twitter: @NytroRST

Chigula - a framework for Wi-Fi Intrusion Detection and Forensics

Vivek Ramachandran, Founder, SecurityTube.net and Pentester Academy

Most of Wi-Fi Intrusion Detection & Forensics is done today using million dollar products or spending hours applying filters in Wireshark :) Chigula aims to solve this by providing a comprehensive, extensible and scriptable framework for Wi-Fi intrusion detection and forensics.

A non-exhaustive list of attacks which will be detected using this framework include:

- Attack tool detection - Aireplay-NG, Airbase-NG, Mdk3 etc.
- Honeypot, Evil Twin and Multipot attacks
- Rogue devices
- Vulnerable clients based on Probed SSIDs
- Hosted network based backdoors
- MAC spoofing
- Deauthentication attacks
- Disassociation attacks
- Channel Jamming attacks using duration field

Vivek Ramachandran discovered the Caffe Latte attack, broke WEP Cloaking and publicly demonstrated enterprise Wi-Fi backdoors. He is the author of "Backtrack 5: Wireless Penetration Testing" which has sold over 13,000+ copies worldwide. He is the founder of SecurityTube.net and runs SecurityTube Training & Pentester Academy which has trained professionals from 90 countries. He has spoken/trained at DEF CON, Blackhat USA/Europe/Abu Dhabi, Brucon, Hacktivity etc. conferences.

Twitter: @securitytube
Facebook: https://www.facebook.com/pagesectube

Knocking my neighbor's kid's cruddy drone offline

Michael Robinson, Professor, Stevenson University

My neighbor's kid is constantly flying his quad copter outside my windows. I see the copter has a camera and I know the little sexed crazed monster has been snooping around the neighborhood. With all of the hype around geo-fencing and drones, this got me to wondering: Would it be possible to force a commercial quad copter to land by sending a low-level pulse directly to it along the frequencies used by GPS? Of course, radio signal jamming is illegal in the U.S and, frankly, it would disrupt my electronics, too. In this presentation, we'll look at some of the research and issues we encountered, when we attempted to force land two commercial drones (the new DJI Phantom 3 and the Parrot Bepop Drone) by sending GPS signals directly at the drones (while staying under the threshold for jamming and not disrupting anyone else).

Michael Robinson has over 15 years of computer security experience and is currently a computer and mobile device forensic examiner in the Washington, DC area, where he deals with intrusion analysis, incident response, and criminal cases. For over four years he ran IT and IA operations for a Department of Defense agency. He has conducted research on security of mobile devices and is starting to play around in the drone space. He teaches computer forensics at the graduate level at Stevenson University in Maryland.

I Will Kill You

Chris Rock, Kustodian Pty Ltd

Have you ever wanted to kill someone? Do you want to get rid of your partner, your boss or your arch nemesis? Perhaps you want to enjoy your life insurance payout whilst you're still alive. Do you have rich elderly parents that just won't die quick enough? Or do you want a "Do Over" new identity.

Then, this presentation is for you! I'll provide you with the insight and techniques on how to "kill" someone and obtain a real death certificate and shutdown their lives. It focuses on the lack of security controls that allow any of us to virtually kill off anyone or any number of people. Forget the Dexter way of killing someone, I'll show you how to avoid the messy clean up and focusing in on the digital aspects. You could be dead right now and not even know it.

The presentation will explain the death process and will highlight the vulnerabilities and its implications world-wide.

You will learn:

- How to fill in a doctor's medical cause of death certificate anonymously.
- How to become a funeral director and dispose of the body.
- How to obtain a Death Certificate.

Once you've wrapped your mind around that concept, I will also show you how to "birth" Virtual identities that obtain real birth certificates. You will learn the birth registration process and the security vulnerabilities associated with this as well.

The third and final step of the presentation is "The baby harvest", a concept that I've developed, which involves creating and raising virtual identities. This technique is similar to a shelf company. Virtuals will be "born", registered with the government complete with birth certificates and social security numbers.

They can open up bank accounts, get a virtual job to launder money, pay taxes, obtain home loans and obtain life insurance policies. They can be married to anyone (virtual or not) and be directors of companies.... the list is endless and to complete the circle of life, they can be killed off when they are ready for "harvest" for their life insurance payouts or sold as permanent I.D.'s. With no victim, this is taking identity theft to the next level.

Chris Rock has been active in the security industry for the last 20 years and is the founder and CEO of Kustodian, a specialized security company that specializes in Security Operations Centres, Penetration testing and independent research. Kustodian is an Australian, Middle East and Hong Kong registered company that has been operational for over 9 years. Chris has also spent 12 years in the banking sector and provides security services around the world for small, medium and large companies.

How to Hack a Tesla Model S

Marc Rogers, Principle Security Researcher for CloudFlare
Kevin Mahaffey, CTO of Lookout Inc

The Tesla Model S is the most connected car in the world. It might surprise you to hear that it is also one of the most secure. In this talk we will walk you through the architecture of a Tesla Model S noting things that Tesla got right as well as identifying those that they got wrong. From this talk you will get an intimate understanding of how the many interconnected systems in a Tesla model S work and most importantly how they can be hacked. You will also get a good understanding of the data that this connected car collects and what Tesla does with this telemetry. We will also be releasing a tool that will enable Tesla Model S owners to view and analyse that telemetry in real time. Finally we will also be releasing several 0day vulnerabilities that will allow you to hack a Tesla Model S yourself - both locally and remotely. Note - only one of the 6 vulnerabilities we will discuss and release has been fixed. Disclaimer: With great access comes great responsibility - In other words we are not responsible for any Tesla Model S bricked by over enthusiastic attendees of this talk :)

Marc Rogers aka Cyberjunky has been a prominent member of the hacking scene since the 80's. Some of his most notable achievements are co-founding the notorious British hacker group, "The Agents of a Hostile Power" and his role in creating and appearing in the award winning BBC TV series "The Real Hustle". Marc's professional career spans more than twenty years, including a decade managing security for the UK operator Vodafone. Marc is currently the principal security researcher for web optimization and security company "CloudFlare. As well as his work in the infosec and telecoms industries, Marc has also been a CISO in South Korea and co-founder of a disruptive Bay Area start-up. Some of Marc's notable recent hacks include Google Glass, Apple TouchID and most recently the Tesla Model S.

Kevin is an entrepreneur and technologist with a background in mobile and web technology, security, and privacy. He is the CTO of Lookout, a company dedicated making the world a safer place as it becomes more connected, starting with smartphones and tablets. He co-founded Lookout in 2007 and is responsible for driving Lookout's technology to protect people from current and future threats while keeping the product simple and easy to use. He started building software when he was 8 years old and

it has been a love affair ever since. Kevin is a frequent speaker on security, privacy, mobile, and other topics.

Hacking Electric Skateboards: Vehicle Research For Mortals

Mike Ryan, Red Team, eBay
Richo Healey, Security Engineer, Stripe

In the last year there's been an explosion of electric skateboards onto the market- seemingly volleyed into popularity by the Boosted Boards kickstarter.

Following on from the success of their original Boosted Board exploit, the team went on to get their hands on the other popular boards on the market, and predictably broke all of them.

Richo and Mike will investigate the security of several popular skateboards, including Boosted's flagship model and demonstrate several vulnerabilities that allow complete control of a an unmodified victim's skateboard, as well as other attacks on the firmware of the board and controller directly.

Richo likes his ducks flat and his instruction sets reduced. By day he works at Stripe as a security engineer, by night he writes (lots of) open source code, on everything from the rust compiler to debugging aids like voltron.
Twitter: @rich0H

Mike Ryan is a computer jerk who gets paid to do stupid crap like this. He spends roughly 40 hours a week steamrolling through eBay's network and likes to relax at home by sniffing Bluetooth.

Twitter: @mpeg4codec

When IoT attacks: hacking a Linux-powered rifle

Runa A. Sandvik
Michael Auger

TrackingPoint is an Austin startup known for making precision-guided firearms. These firearms ship with a tightly integrated system coupling a rifle, an ARM-powered scope running a modified version of Linux, and a linked trigger mechanism. The scope can follow targets, calculate ballistics and drastically increase its user's first shot accuracy. The scope can also record video and audio, as well as stream video to other devices using its own wireless network and mobile applications.

In this talk, we will demonstrate how the TrackingPoint long range tactical rifle works. We will discuss how we reverse engineered the scope, the firmware, and three of TrackingPoint's mobile applications. We will discuss different use cases and attack surfaces. We will also discuss the security and privacy implications of network-connected firearms.

Runa A. Sandvik is a privacy and security researcher, working at the intersection of technology, law and policy. She is a technical advisor to both the Freedom of the Press Foundation and the TrueCrypt Audit Project, and a member of the review board for Black Hat Europe.
Twitter: @runasand

Michael Auger is an experienced IT Security specialist with extensive experience in integrating and leveraging IT security tools. He has leveraged a wide range of IT security solutions, integrating them, to deliver leading edge incident response and security operations capabilities. His 15+ year career includes:

Â· Supporting security incidents during the event and the subsequent remediation phases
Â· Implementing and managing IT security infrastructures for public and private organizations.
Â· Design and implement global SIEM infrastructure for F100 organizations
Â· Delivering training on advanced SIEM solutions and network discovery tools
Â· Presenting and publishing security articles on security vulnerabilities and best practices

Drinking from LETHE: New methods of exploiting and mitigating memory corruptioh2>vulnerabilities

Daniel Selifonov, Engineer, Skyport Systems Inc
Memory corruption vulnerabilities have plagued computer systems since we started programming software. Techniques for transforming memory corruption primitives into arbitrary code execution exploits have evolved significantly over the past two decades, from "smashing the stack for fun and profit" to the current apex of "just in time code reuse" while playing a cat and mouse game with similarly evolving defensive mitigations: from PaX/NX-bit to fine-grained ASLR and beyond. By contextualizing this battle between attack and defense, I will demonstrate new defense strategies based on augmenting fine-grained ASLR with memory disclosure mitigations to render existing exploitation techniques unreliable. Modifications to the Xen hypervisor exploiting hardware accelerated virtualization extensions on the modern Intel platform enable realizing these new defense strategies without imposing significant runtime CPU overhead.
Daniel Selifonov is currently an engineer focused on information security, and in prior consultancies has built systems for information technology where security was considered throughout design and implementation, rather than as an afterthought. His research interests in security include reverse engineering, applied cryptography, client side security, and user acceptable information system design.
Social media names/links:
** GitHub: https://github.com/thyth/*
** Personal Website: http://thyth.com/*

Breaking SSL Using Time Synchronisation Attacks

Jose Selvi, Senior Security Consultant, NCC Group

What time? When? Who is first? Obviously, Time is strongly present in our daily life. We use time in almost everything we do, and computers are not an exception to this rule. Our computers and devices use time in a wide variety of ways such as cache expiration, scheduling tasks or even security technologies. Some of those technologies completely relies on the local clock, and they can be affected by a clock misconfiguration.

However, since most operating system providers do not offer secure time synchronisation protocols by default, an attacker could manipulate those protocols and control the local clock. In this presentation, we review how different operating systems synchronise their local clocks and how an attacker could exploit some of them in order to bypass different well-known security protections.

Jose Selvi is a Senior Penetration Tester at NCC Group. His 11 years of expertise performing advanced security services and solutions in various industries (government, telecom, retail, manufacturing, healthcare, financial, technology...) include mainly penetration tests and information security research in new technologies. He is also a SANS Institute community instructor for penetration testing courses and a regular speaker at security conferences (mostly in Spain)

"Quantum" Classification of Malware

John Seymour, Ph.D. student, University of Maryland, Baltimore County

Quantum computation has recently become an important area for security research, with its applications to factoring large numbers and secure communication. In practice, only one company (D-Wave) has claimed to create a quantum computer which can solve relatively hard problems, and that claim has been met with much skepticism. Regardless of whether it is using quantum effects for computation or not, the D-Wave architecture cannot run the standard quantum algorithms, such as Grover's and Shor's. The D-Wave architecture is instead purported to be useful for machine learning and for heuristically solving NP-Complete problems.

We'll show why the D-Wave and the machine learning problem for malware classification seem especially suited for each other. We also explain how to translate the classification problem for malicious executables into an optimization problem which a D-Wave machine can solve. Specifically, using a 512-qubit D-Wave Two processor, we show that a minimalist malware classifier, with cross-validation accuracy comparable to standard machine learning algorithms, can be created. However, even such a minimalist classifier incurs a surprising level of overhead.

John Seymour is a Ph.D. student at the University of Maryland, Baltimore County, where he performs research at the intersection of machine learning and information security. He's mostly interested in avoiding and helping others avoid some of the major pitfalls in machine learning, especially in dataset preparation (seriously, do people still use malware datasets from 1998?) In 2014, he completed his Master's thesis on the subject of quantum computation applied to malware analysis. He currently works at CyberPoint International, a company which performs network and host-based machine learning, located in Baltimore, MD.

Insteon' False Security And Deceptive Documentation

Peter Shipley, Security Researcher
Ryan Gooler

Insteon is a leading home automation solution for controlling lights, locks, alarms, and much more. More than forty percent of homes with automation installed use Insteon.

For the last fifteen years, Insteon has published detailed documentation of their protocols-documentation that is purposely misleading, filled with errors, and at times deliberately obfuscated. As my research over the last year has revealed, this sad state of affairs is the direct result of Insteon papering over the fact that it is trivial to wirelessly take control, reprogram, and monitoring any Insteon installation.

Worse still, the embedded nature of the Insteon protocol coupled with devices that do not support flash updates means that there are no current fixes or workarounds short of ripping out the Insteon products.

I will be presenting my research, and releasing tools demonstrating the vulnerabilities throughout the Insteon home automation system.

Peter Shipley has been working with security for over 30 years. In the late 80's he wrote one of the first network security scanners and maintained one of the first bug databases (later used to seed similar lists at CERT and llnl.gov). Around the same time Peter co-founded UC Berkeley's OCF (Open Computing Facility).

In the mid 90's Peter Shipley became a founding member of cypherpunks & setup up one of the first official PGP distribution sites.

In '98 (DEF CON 6) Peter Shipley did a independent security research on war-dialing, exposing a significant security problem that was being ignored in most corporate environments making phone security.

At DEF CON 9 Peter Shipley introduced wardriving to the world. Recently Peter has written and released several APIs using python to link various networked automation appliances via REST and other interfaces.

Peter Shipley currently manages for a dot-com by day, and helps raise two kids by night.

Ryan Gooler (@jippen) is a cloud security guy, known for luck, sarcasm, and getting into things. Avid lockpicker, lover of cats, and disrespector of authority.

Scared Poopless - LTE and *your* laptop

Mickey Shkatov, Security researcher, Intel Advanced Threat Research.

Jesse Michael, Security researcher

With today's advancement in connectivity and internet access using 3G and LTE modems it seems we all can have a device that's always internet capable, including our laptops, tablets, 2 in 1's ultrabook. It becomes easier to be online without using your WiFi at all. In our talk we will demonstrate and discuss the exploitation of an internal LTE modem from Huawei which can be found in a number of devices including laptops by HP.

Mickey Shkatov is a security researcher and a member of the Intel Advanced Threat Research team. His areas of expertise include vulnerability research, hardware and firmware security, and embedded device security. Mickey has presented some of his past research at DEF CON, Black Hat USA, BruCON, and BsidesPDX
Twitter: @laplinker

Jesse Michael has been working in security for over a decade and is currently a security researcher at a Fortune 50 company who spends his time causing trouble and finding low-level hardware security vulnerabilities in modern computing platforms.

Twitter: @jessemichael

Angry Hacking - the next generation of binary analysis

Yan Shoshitaishvili, PhD Student, UC Santa Barbara
Fish Wang, PhD Student, UC Santa Barbara

Security has gone from a curiosity to a phenomenon in the last decade. Fortunately for us, despite the rise of memory-safe, interpreted, lame languages, the security of binaries is as relevant as ever. On top of that, (computer security) Capture the Flag competitions have skyrocketed in popularity, with new and exciting binaries on offer for hacking every weekend.

This all sounds great, and it is. Unfortunately, the more time goes by, the older we get, and the more our skills fade. Whereas we were happy to stare at objdump a decade ago, today, we find the menial parts of reversing and pwning more and more tiring and more and more difficult. Worse, while security analysis tools have been evolving to make life easier for us hackers, the core tools that we use (like IDA Pro) have remained mostly stagnant. And on top of that, the term "binaries" have expanded to regularly include ARM, MIPS, PPC, MSP430, and every other crazy architecture you can think of, rather than the nice, comfortable x86 of yesteryear.

New tools are required, and we're here to deliver. Over the last two years, we have been working on a next-generation binary analysis framework in an attempt to turn back the tide and reduce our mounting noobness. The result is called angr.

angr assists in binary analysis by providing extremely powerful, state-of-the-art analyses, and making them as straightforward to use as possible. Ever wanted to know *what freaking value* some variable could take on in a function (say, can the target of a computed write point to the return address)? angr

can tell you! Want to know what input you need to trigger a certain code path and export a flag? Ask angr! In the talk, we'll cover three of the analyses that angr provides: a powerful static analysis engine (able to, among other things, automatically identify potential memory corruption in binaries through the use of Value-Set Analysis), its symbolic execution engine, and dynamic emulation of various architectures (*super* useful for debugging shellcode).

On top of that, angr is designed to make the life of a hacker as easy as possible -- for example, the whole system is 98% Python, and is designed to be a breeze to interact with through iPython. Plus, it comes with a nifty GUI with nice visualizations for symbolically exploring a program, tracking differences between different program paths, and understanding value ranges of variables and registers. Finally, angr is designed to be easily extensible and embeddable in other applications. We'll show off a semantic-aware ROP gadget finder ("are there any gadgets that write to a positive offset of rax but don't clobber rbx" or "given this program state, what are the gadgets that won't cause a segfault") and a binary diffing engine, both built on angr.

We've used angr to solve CTF binaries, analyze embedded devices, debug shellcode, and even dabble in the DARPA Cyber Grand Challenge. We'll talk about our experiences with all of that and will release angr to the world, hopefully revolutionizing binary analysis and making everyone ANGRY!

Yan and Fish are two members of Shellphish, a pretty badass hacking team famous for low SLA and getting the freaking exploit JUST A FREAKING MINUTE LATE. Their secret identities are those of PhD students in the security lab of UC Santa Barbara. When they're not CTFing or surfing, they're doing next-generation (what does that even mean?) security research. Their works have been published in numerous academic venues. For example, in 2013, they created an automatic tool, called MovieStealer, a tool to automatically break the DRM of streaming media services [1]. After taking 2014 to work on angr, in 2015, they followed this up with an analysis of backdoors in embedded devices [2].

Now, they've set their sights on helping the world analyze binaries faster, better, stronger, by revolutionizing the analysis tool landscape!

[1] https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/wang_ruoyu
[2] http://www.internetsociety.org/doc/firmalice-automatic-detection-authentication-bypass-vulnerabilities-binary-firmware

Twitter: @zardus

High-Def Fuzzing: Exploring Vulnerabilities in HDMI-CEC

Joshua Smith, Senior Security Researcher, HP Zero Day Initiative

The HDMI (High Definition Multimedia Interface) standard has gained extensive market penetration. Nearly every piece of modern home theater equipment has HDMI support and most modern mobile devices actually have HDMI-capable outputs, though it may not be obvious. Lurking inside most modern HDMI-compatible devices is something called HDMI-CEC, or Consumer Electronics Control.

This is the functionality that allows a media device to, for example, turn on your TV and change the TV's input. That doesn't sound interesting, but as we'll see in this presentation, there are some very surprising things an attacker can do by exploiting CEC software implementations. Then there's something called HEC or HDMI Ethernet Connection, which allows devices to establish an Ethernet connection of up to 100Mbit/s over their HDMI connections (newer HDMI standards raise the speed to 1Gbit/s).

Don't think your mobile phone implements CEC? You might be wrong. Most modern Android-based phones and tablets have a Slimport(r) connection that supports HDMI-CEC. Ever heard of MHL (Mobile High-Definition Link)? Think Samsung and HTC (among other) mobile devices, and many JVC, Kenwood, Panasonic, and Sony car stereos - as many as 750 million devices in the world so far. Guess what? MHL supports HDMI-CEC as well. Let's explore, and own, this attack space.

Kernelsmith is senior vulnerability researcher with Hewlett-Packard Security Research (HPSR). In this role, he analyzes and performs root-cause analysis on hundreds of vulnerabilities submitted to the Zero-Day Initiative (ZDI) program, which represents the world's largest vendor-agnostic bug bounty program. His focus includes analyzing and performing root-cause analysis on hundreds of zero-day vulnerabilities submitted by ZDI researchers from around the world. Joshua is also a developer for the Metasploit Framework and has spoken at a few conferences and holds a few certifications.

Prior to joining HP, Smith served in the U.S. Air Force in various roles including as an Intercontinental Ballistic Missile (ICBM) Crew Commander and Instructor, but more relevantly as a penetration tester for the 92d Information Warfare Aggressor Squadron. Post-military, he became a security engineer at the John Hopkins University Applied Physics Lab, where he began contributing to the Metasploit Framework. Smith performed research into weapons systems vulnerabilities as well as evasion and obfuscation techniques to add depth and realism to security device tests. Smith received a B.S. in Aeronautical Engineering from Rensselaer Polytechnic Institute and an M.A. in Management of Information Systems from the University of Great Falls.

Smith was drawn to ZDI for the chance to work with a world-wide network of security researchers while continuing his own vulnerability research. When not researching software vulnerabilities, Josh enjoys raising his two young hackers-to-be and watching sci-fi since he can't play sports anymore (there's no tread left on his knees).

Twitter: @kernelsmith, @thezdi

Dissecting the Design of SCADA Web Human Machine Interfaces (HMIs) - Hunting Vulnerabilities

Aditya K Sood, Architect - Threat Research Labs, Elastica inc.

Human Machine Interfaces (HMIs) are the subsets of the Supervisory Control and Data Acquisition (SCADA) systems. HMIs are control panels that provide interfaces for humans to interact with machines and to manage operations of various types of SCADA systems. HMIs have direct access to

SCADA databases including critical software programs. The majority of SCADA systems have web-based HMIs that allow the humans to control the SCADA operations remotely through Internet. This talk unveils various flavors of undisclosed vulnerabilities in web-based SCADA HMIs including but not limited to remote or local file inclusions, insecure authentication through clients, weak password hashing mechanisms, firmware discrepancies, hardcoded credentials, insecure web-services, weak cryptographic design, cross-site request forgery, and many others. This talk digs deeper into the design models of various SCADA systems to highlight security deficiencies in the existing SCADA HMI deployments. The research is driven with a motivation to secure SCADA devices and to build more intelligent solutions by hunting vulnerabilities in SCADA HMIs. The vulnerabilities presented in this talk are completely undisclosed and will be revealed for the first time with live demonstrations.

Aditya K Sood (Ph.D) is a senior security researcher and consultant. Dr. Sood has research interests in malware automation and analysis, application security, secure software design and cybercrime. He has worked on a number of projects pertaining to penetration testing specializing in product/appliance security, networks, mobile and web applications while serving Fortune 500 clients for IOActive, KPMG and others. He is also a founder of SecNiche Security Labs, an independent web portal for sharing research with security community. He has authored several papers for various magazines and journals including IEEE, Elsevier, CrossTalk, ISACA, Virus Bulletin, Usenix and others. His work has been featured in several media outlets including Associated Press, Fox News, Guardian, Business Insider, CBC and others. He has been an active speaker at industry conferences and presented at BlackHat, DEF CON, HackInTheBox, RSA, Virus Bulletin, OWASP and many others. Dr. Sood obtained his Ph.D from Michigan State University in Computer Sciences. Dr. Sood is also an author of "Targeted Cyber Attacks" book published by Syngress.

Company Website: http://www.elastica.net
Personal website: http://adityaksood.secniche.org
Twitter: @AdityaKSood

Shall We Play a Game?

Tamas Szakaly, Lead security researcher @ PR-Audit Ltd., Hungary

Everybody plays games, and a whole lot of people plays computer games. Despite this fact, very few of us, security researchers consider them as interesting targets. Granted, you won't likely be able to directly hack into a big corporate network via game exploits, but you could for example target the people running the company via their favorite games. Or their children's favorite games. Another scenario: you should consider that a hacked game could allow Not So Admirable people access to your internal network - which at first does not seem that big of a deal considering it's "just" a home network, but when you realize all your mobile phones, your TV set, your VOIP phones, your security cameras, and even your smart house sensors and controllers are part of that network, it looks much more scary.

Games are also interesting from a technical standpoint too, since they tend to be quite complex. The majority of them have networking, and they process complex data structures (maps, saved games, etc.) which makes them ideal fuzzing targets. But this talk is not about those kind of exploits. Hackers tend to ignore the low hanging fruits in favor of beautiful exploits, but we really shouldn't - bad guys don't care

about how sophisticated some exploit is, they only care about the results. This is why I have decided to take a look around and see what's already there in the games that allows access to the gamers' network. Thus this research about how game scripting engines can be abused started.

I'll show in this talk that playing on custom game servers and playing community created maps could easily lead to code execution on our machines - more so, in most cases without the need to bypass the operating system's exploit mitigation techniques. My targets include popular games and game engines like CryEngine 3, Dota 2, Garry's Mod, ARMA3 and Digital Combat Simulator. I'll show a wide range of script abuse from a simple direct command execution in an unrestricted scripting environment through brute forcing a security camera via HTTP requests to complex script sandbox escapes.

Tamas is the lead IT security researcher at PR-Audit Ltd., a company focusing mainly on penetration testing and SIEM software developing. Previously he participated in a cooperation between ELTE Department of Meteorology and the Paks Nuclear Power Plant Ltd. which goal was to develop TREX, a toxic waste emission simulator using CUDA. The scene from RoboCop where the kid defeats the evil robot with just a laptop and a serial cable made a huge impression on him, and after seeing the movie, his path was set: he was bound to be a hacker. His first experiences in this field involved poking around various copy protection schemes, and for this day his favorite areas of expertise are the ones that require some mangling of binary files. Besides computer security he also loves mountain biking and flight simulators.
Twitter: @sghctoma

DIY Nukeproofing: a new dig at "data-mining"

3AlarmLampscooter, enigmatic armored mammal

Does the thought of nuclear war wiping out your data keep you up at night? Don't trust third party data centers? Few grand burning a hole in your pocket and looking for a new Sunday project to keep you occupied through the fall? If you answered yes to at least two out of three of these questions, then 3AlarmLampscooter's talk on extreme pervasive communications is for you! You'll learn everything from calculating radiation half layer values to approximating soil stability involved in excavating your personal apocalypse-proof underground data fortress.

3AlarmLampscooter is an enigmatic armored mammal of the genus homo sapiens sapiens sapiens troglodytae found in caves and tunnels across the southeastern United States. As moderator of the subreddit /r/Neutron, 3AlarmLampscooter's enunciation espouses pervasive communication via excavation to protect from radiation and conflagration. When above-ground, 3AlarmLampscooter is a vocal transhumanism advocate developing 3D printed construction materials.

www.reddit.com/u/3AlarmLampscooter

Hacking the Human Body/brain: Identity Shift, the Shape of a New Self, and Humanity 2.0

Richard Thieme, Author and Professional Speaker, ThiemeWorks

This presentation is beyond fiction.

Current research in neuroscience and the extension and augmentation of senses is proceeding in directions that might sound to a twentieth century mind like science fiction. Progress is rapid but unevenly distributed: Some is directed by military, intelligence and corporate interests but beyond their concerns, we can discern the future shape of human identity itself in nascent forms.

The human body/brain is being hacked to explore radical applications for helping, healing, and harming this and future generations. Some can be done in garage-hacking style. The presenter, in fact, recently had lenses in both eyes removed and replaced with artificial ones engineered for the vision he wanted, a now-trivial surgery. The reach of new technologies promises an even more radical transformation in what it means to be human.

One area of research is the recovery of memories, the deletion of emotional charges from memories, the removal of specific memories, the alteration of the content of memories, and the implantation of new memories. Another seeks to read the mind at a distance and extract information. Another explores the use of genomes to understand and replicate thinking, feeling, and behavior patterns. Another implements mind-to-mind communication, using neuroscience to understand brains best suited for remote viewing as well as implants and non-invasive technologies that control the electromagnetic energies of the brain to enable psychokinesis, clairvoyance and telepathy.

Augmentation of human abilities is being achieved by splicing information from sensors integrated with existing neurological channels. To feel the magnetic field of the earth, see the infrared and ultraviolet parts of the electromagnetic spectrum, discern the yaw and pitch of airplanes, see and hear by going around our eyes and ears -- all this means we will experience the "self" in new ways.

Thieme concludes with quotes from remote viewer Joe McMoneagle, astronaut Edgar Mitchell, and his new novel FOAM to suggest the shape of the mind of the future. If you're 20 years old, you have at least a century of productive life ahead of you, so you had better be on board with the shape of your future selves. :-)

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 and identify shift. He has explored issues raised in this DEF CON 23 presentation for 20 years but raises his game to outline the shape of the future self, defining it as a system open to modification and hacking, giving the term "biohacking" new and compelling meaning.

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 NSA said after they worked together on 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." He is 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 50 university libraries. A recently completed novel FOAM explores

the existential challenges of what it means to be human in the 21st century. "The UFO History Group" is exploring a second volume and Thieme is selecting "the best of" his diverse writings for "A Richard Thieme Reader" and writing more fiction.

Thieme's 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, and the "Design Matters" lecture series at the University of Calgary. He keynoted a conference on metadata this spring for the U of Texas-San Antonio. He addressed the reinvention of "Europe" as a "cognitive artifact" for curators and artists at Museum Sztuki in Lodz, Poland and keynoted "The Real Truth: A World's Fair" at Raven Row Gallery, London. He has spoken for the National Security Agency, the FBI, the Secret Service, the US Department of the Treasury, Los Alamos National Labs and has keynoted "hacker" and security conferences around the world.

Twitter and skype: neuralcowboy:
Facebook and LinkedIn: Richard Thieme

From 0 To Secure In 1 Minute - Securing IAAS

Nir Valtman, CISO - Retail, NCR
Moshe Ferber, Co-chairman of the board, Cloud Security Alliance Israel

Recent hacks to IaaS platforms reveled that we need to master the attack vectors used: Automation and API attack vector, insecure instances and management dashboard with wide capabilities. Those attack vectors are not unique to Cloud Computing but there are magnified due to the cloud characteristics. The fact is that IaaS instance lifecycle is accelerating, nowadays we can find servers that are installed, launched, process data and terminate - all within a range of minutes. This new accelerated lifecycle makes traditional security processes such as periodic patches, vulnerability scanning, hardening, and forensics impossible. In this accelerated lifecycle, there are no maintenance windows for patches or ability to mitigate vulnerability, so the security infrastructure must adapt to new methods. In this new thinking, we require automation of instance security configuration, hardening, monitoring, and termination. Because there are no maintenance windows, Servers must be patched before they boot up, security configuration and hardening procedures should be integrated with server installation and vulnerability scanning and mitigation processes should be automatic.

In the presentation, we plan to announce the full version of a new open source tool called "Cloudefigo" and explain how it enables accelerated security lifecycle. We demonstrate how to launch a pre-configured, already patched instance into an encrypted storage environment automatically while evaluating their security and mitigating them automatically if a vulnerability is found. In the live demo, we leverage Amazon Web Services EC2 Cloud-Init scripts and object storage for provisioning automated security configuration, integrating encryption, including secure encryption key repositories for secure server's communication. The result of those techniques is cloud servers that are resilient, automatically configured, with the reduced attack surface.

Nir is employed at NCR Corporation as the CISO of NCR Retail. Before the acquisition of Retalix by NCR, he was Chief Security Officer of R&D at the company. As part of his previous positions in the last decade, he worked as Chief Security Architect, Senior Technology Consultant, Application Security Consultant, Systems Infrastructure Security Consultant, and a Technological Trainer. While in these positions, Nir was not only consulting, but also performing hands-on activities in various fields, i.e. hardening, penetration testing, and development for personal/internal applications. In addition, Nir is a public speaker (spoke on BlackHat, DEF CON, OWASP, InfoSec etc.) and open source contributor. Among his contributions, he released an open source anti-defacement tool called AntiDef, and wrote a publication about QRbot, an iPhone QR botnet POC he developed. His latest open source tool is Cloudefigo, which planned to be presented in the conference. Nir has a BSc in Computer Science but his knowledge is based mainly on cowboy learning and information sharing with the techno-oriented communities.
Moshe Ferber is an information security entrepreneur and one of the cornerstones of the information security industry in Israel, with over 20 years of experience in various industry the leading positions such as the Security manager for Ness Technologies and founder of leading MSSP services provider. Currently Mr. Ferber focuses in promoting innovation in the Israeli startup scene as an investor, lecturer and evangelist for various cloud security topics. Mr. Ferber is a popular industry speaker and promote cloud security best practices and official lecturer for the Cloud Security Alliance.

Looping Surveillance Cameras through Live Editing of Network Streams

Eric Van Albert, independent security researcher
Zach Banks, independent security researcher

This project consists of the hardware and software necessary to hijack wired network communications. The hardware allows an attacker to splice into live network cabling without ever breaking the physical connection. This allows the traffic on the line to be passively tapped and examined. Once the attacker has gained enough knowledge about the data being sent, the device switches to an active tap topology, where data in both directions can be modified on the fly. Through our custom implementation of the network stack, we can accurately mimic the two devices across almost all OSI layers.

We have developed several applications for this technology. Most notable is the editing of live video streams to produce a "camera loop," that is, hijacking the feed from an Ethernet surveillance camera so that the same footage repeats over and over again. More advanced video transformations can be applied if necessary. This attack can be executed and activated with practically no interruption in service, and when deactivated, is completely transparent.

Eric is a recent MIT graduate who spends his days building 3D printers for Formlabs and his nights crawling around places he probably shouldn't. He has taught seminars on lockpicking and physical security vulnerabilities to various audiences at the Institute, and done a small bit of security consulting work. When he runs out of projects to hack on, he reads the leaked NSA ANT catalog for ideas.

Zach is also a recent MIT graduate with over 0 years of security experience. He's particularly interested in the security of embedded devices and knots. In his free time, he enjoys putting household appliances on the internet and refactoring his old code.

Machine vs. Machine: Inside DARPA's Fully Automated CTF

Michael Walker, Program Manager, DARPA/I2O
Jordan Wiens, CTF A(p|nthro)pologist @vector35.com

For 22 years, the best binary ninjas in the world have gathered at DEF CON to play the world's most competitive Capture-the-Flag. At DEF CON 24, DARPA will challenge machines to play this game for the first time, with the winner taking home a $2 million prize. This talk will include a first public look at the machines, teams, technology, and visualization behind Cyber Grand Challenge. The technology: machines that discover bugs and build patches? We're bringing our qualifier results to show just how real this is. The teams: we'll talk about the finalists who prevailed to make it to the CGC final round. Visualization: the product of CTF players working with game designers, this talk will include a live interactive demo of a graphical debugger for everyone that will let an audience follow along in real time. The machines: we're bringing high performance computing to the DEF CON stage. The event: In 2016, machines will Capture the Flag! Follow DARPA Cyber Grand Challenge on Twitter: #DARPACGC

Mike Walker joined DARPA as a program manager in January 2013. His research interests include machine reasoning about software in situ and the automation of application security lifecycles.

Prior to joining DARPA, Mr. Walker worked in industry as a security software developer, Red Team analyst, enterprise security architect and research lab leader. As part of the Computer Science Corporation "Strikeforce" Red Team, Mr. Walker helped develop the HEAT Vulnerability Scanner and performed Red Team engagements. Serving as a principal at the Intrepidus Group, Mr. Walker worked on Red Teams that tested America's financial and energy infrastructure for security weaknesses. Also, on the DARPA SAFER Red Team, Mr. Walker discovered flaws in prototype communications technologies.

Mr. Walker has participated in various roles in numerous applied computer security competitions. He contributed challenges to DEF CON Capture the Flag (CTF) and competed on and led CTF teams at the highest levels of international competition. Mr. Walker was formerly a mentor of the Computer Security Competition Club at Thomas Jefferson High School for Science and Technology (TJHSST).

Jordan started his professional career at the University of Florida where he got to do a little bit of everything security related. His love of CTFs, however, drove him to a job at a government contractor where he honed his reverse engineering and vulnerability research skills. Now, his goal in life is to become a professional CTF e-sports caster so he founded a startup Vector 35 to try to get paid to do stuff with CTFs and gaming.

Pivoting Without Rights - Introducing Pivoter

Geoff Walton, Senior Security Consultant for Cleveland-based TrustedSec
Dave Kennedy, (ReL1K/HackingDave), founder of TrustedSec and Binary Defense Systems

One of the most challenging steps of a penetration test is popping something and not having full administrative level rights over the system. Companies are cutting back on administrative level rights for endpoints or how about those times where you popped an external web application and were running as Apache or Network Service? Privilege escalation or pillaging systems can be difficult and require extensive time if successful at all. One of the most challenging aspects around pentesting was the need to have administrative level rights, install your tools, and from there leverage the compromised machine as a pivot point for lateral movement in the network. Well, the time has changed. Introducing Pivoter - a reverse connection transparent proxy that supports the ability to pivot with ease. Pivoter is a full transparent proxy that supports the ability to use limited rights on a system to pivot to other systems and attack transparently from your system at home. Port scans, exploits, brute forcing, anything you could do like you were on that network is now available through Pivoter. As part of this talk, we'll be releasing a new Metasploit module for shell DLL injection for AV evasion, a Linux version of Pivoter, a Windows version of Pivoter, and a PowerShell version of Pivoter. msf> run pivoter -> pentest as if you are on the internal network even if you don't have admin rights. Also during this talk, we'll be releasing a new major release of the Social-Engineer Toolkit (SET) which incorporates Pivoter into the payload delivery system.

Geoff Walton is a Senior Security Consultant for Cleveland-based TrustedSec. He joined after years of working in information security. Geoff's expertise in pen testing, network security, and software analysis comes form over ten years experience in a variety of information technology roles including software development, network operations and information security specific functions; Geoff brings broad vision to assessments and penetration test engagements. Geoff has been part of diverse IT teams at organizations both large and small. He has experience across several industries including retail, professional services, and manufacturing.

Dave Kennedy is founder of TrustedSec and Binary Defense Systems. Both organizations focus on the betterment of the security industry from an offense and a defense perspective. David was the former Chief Security Officer (CSO) for a Fortune 1000 company where he ran the entire information security program. Kennedy is a co-author of the book "Metasploit: The Penetration Testers Guide," the creator of the Social-Engineer Toolkit (SET), and Artillery. Kennedy has been interviewed by several news organizations including CNN, Fox News, MSNBC, CNBC, Katie Couric, and BBC World News. Kennedy is the co-host of the social-engineer podcast and on a number of additional podcasts. Kennedy has testified in front of Congress on two occasions on the security around government websites. Kennedy is one of the co-authors of the Penetration Testing Execution Standard (PTES); a framework designed to fix the penetration testing industry. Kennedy is the co-founder of DerbyCon, a large-scale conference in Louisville Kentucky. Prior to Diebold, Kennedy was a VP of Consulting and Partner of a mid-size information security consulting company running the security consulting practice. Prior to the private sector, Kennedy worked for the United States Marine Corps and deployed to Iraq twice for intelligence related missions.

Twitter: @HackingDave

'DLL Hijacking' on OS X? #@%& Yeah!

Patrick Wardle, Director of R&D, Synack

Remember DLL hijacking on Windows? Well, turns out that OS X is fundamentally vulnerable to a similar attack (independent of the user's environment).

By abusing various 'features' and undocumented aspects of OS X's dynamic loader, this talk will reveal how attackers need only to plant specially-crafted dynamic libraries to have their malicious code automatically loaded into vulnerable applications. Through this attack, adversaries can perform a wide range of malicious actions, including stealthy persistence, process injection, security software circumvention, and even 'remote' infection. So come watch as applications fall, Gatekeeper crumbles (allowing downloaded unsigned code to execute), and 'hijacker malware' arises - capable of bypassing all top security and anti-virus products! And since "sharing is caring" leave with code and tools that can automatically uncover vulnerable binaries, generate compatible hijacker libraries, or detect if you've been hijacked.

Patrick Wardle is the Director of Research at Synack, where he leads cyber R&D efforts. Having worked at NASA, the NSA, and Vulnerability Research Labs (VRL), 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 OS X security tools. Both can be found on his website Objective-See.com

Stick That In Your (root)Pipe & Smoke It

Patrick Wardle, Director of R&D, Synack

You may ask; "why would Apple add an XPC service that can create setuid files anywhere on the system - and then blindly allow any local user to leverage this service?" Honestly, I have no idea!

The undocumented 'writeconfig' XPC service was recently uncovered by Emil Kvarnhammar, who determined its lax controls could be abused to escalate one's privileges to root. Dubbed 'rootpipe,' this bug was patched in OS X 10.10.3. End of story, right? Nope, instead things then got quite interesting. First, Apple decided to leave older versions of OS X un-patched. Then, an astute researcher discovered that the OSX/XSLCmd malware which pre-dated the disclosure, exploited this same vulnerability as a 0day! Finally, yours truly, found a simple way to side-step Apple's patch to re-exploit the core vulnerability on a fully-patched system. So come attend (but maybe leave your MacBooks at home), as we dive into the technical details XPC and the rootpipe vulnerability, explore how malware exploited this flaw, and then fully detail the process of completely bypassing Apple's patch. The talk will conclude by examining Apple's response, a second patch, that appears to squash 'rootpipe'...for now.

Patrick Wardle is the Director of Research at Synack, where he leads cyber R&D efforts. Having worked at NASA, the NSA, and Vulnerability Research Labs (VRL), 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 OS X security tools. Both can be found on his website Objective-See.com

Confessions of a Professional Cyber Stalker

Ken Westin, Sr. Security Analyst with Tripwire Inc.

For several years I developed and utilized various technologies and methods to track criminals leading to at least two dozen convictions. In the process of recovering stolen devices, larger crimes would be uncovered including drugs, theft rings, stolen cars, even a violent car jacking. Much of the evidence in these cases would be collected by stolen devices themselves, such as network information, photos captured from laptops and cell phones, but often times there was additional data that would need to be gathered for a conviction. In this presentation I will walk through actual real cases and discuss in depth the technologies used and additional processes I went through utilizing open source data and other methods to target criminals. I will also discuss how these same tools and methods can be used against the innocent and steps users and developers can take to better protect privacy.

In this presentation here are a few examples of cases I worked on which I will reveal details of:

- How a theft ring targeting Portland, Oregon schools was unveiled leading to multiple convictions
- How I tracked and recovered $9K worth of stolen camera equipment sold multiple times a year after it was stolen based on data extracted from images online
- How mobile phones stolen from a wireless store were tracked leading to the arrest of a theft ring, leading to the conviction of six people and the recovery of a stolen car
- Embedding of custom designed trojan for thermal imaging devices for theft tracking and export controls
- Tracking of a stolen flash drive to a university computer lab and correlation of security camera and student access ID cards
- Tracking a stolen laptop across state lines and how I gathered mountains of evidence in another theft ring case
- Several other cases....

Ken is a security analyst and "creative technologist" with 15 years experience building and breaking things through the use/misuse of technology. His technology exploits and endeavors have been featured in Forbes, Good Morning America, Dateline, the New York Times and others. He has worked with law enforcement and journalists utilizing various technologies to unveil organized crime rings, recover stolen cars, even a car jacking amongst other crimes.

How to Train Your RFID Hacking Tools

Craig Young, Security Researcher, Tripwire VERT

With insecure low frequency RFID access control badges still in use at businesses around the world and high frequency NFC technology being incorporated into far more consumer products, RFID hacking tools are invaluable for penetration testers and security researchers alike. Software defined radio has revolutionized this field with powerful devices like Proxmark3 and RFIDler available for a modest price. 3D printing has also presented new opportunities for makers to create custom antennas and cases to fit specific tasks. While there is a lot of great information out there about how people use these tools, there is relatively little more than source code available for learning how to develop new firmware to equip these devices with purpose-built logic. This presentation will discuss the overall architecture of the Proxmark3 and RFIDler tools and provide tutorial style examples for enhancing the firmware. Proxmark3 development will be demonstrated by upgrading the stand-alone mode to support NFC operations. For the new kid on the block, RFIDler, we will take a look at how to tweak the system for optimal reliability using 3D printing and enhanced diagnostic tools.

Craig Young (@CraigTweets) is a computer security researcher with Tripwire's Vulnerability and Exposures Research Team (VERT). He has identified and responsibly disclosed dozens of vulnerabilities in products from Google, Amazon, IBM, NETGEAR, Adobe, HP, and others. His research has resulted in numerous CVE assignments and repeated recognition in the Google Application Security Hall of Fame. Craig's presentations on Google authentication weaknesses have led to considerable security improvements for all Google users. Craig won in track 0 and track 1 of the first ever SOHOpelessly Broken contest at DEF CON 22 by demonstrating 10 0-day flaws in SOHO wireless routers. Craig has more recently turned his attention to a different part of the wireless spectrum with research into home automation products as well as RFID/NFC technology.

Twitter: @CraigTweets

Investigating the Practicality and Cost of Abusing Memory Errors with DNS

Luke Young, Information Security Engineer, Hydrant Labs LLC

In a world full of targeted attacks and complex exploits this talk explores an attack that can simplified so even the most non-technical person can understand, yet the potential impact is massive:

Ever wonder what would happen if one of the millions of bits in memory flipped value from a 0 to a 1 or vice versa? This talk will explore abusing that specific memory error, called a bit flip, via DNS.

The talk will cover the various hurdles involved in exploiting these errors, as well as the costs of such exploitation. It will take you through my path to 1.3 million mis-directed queries a day, purchasing hundreds of domain names, wildcard SSL certificates, getting banned from payment processors, getting banned from the entire Comcast network and much more.

Luke Young (@innoying) - is a freshman undergraduate student pursuing a career in information security. As an independent researcher, he has investigated a variety of well-known products and network protocols for design and implementation flaws. His research at various companies has resulted

in numerous CVE assignments and recognition in various security Hall of Fames. He currently works as an Information Security Intern at LinkedIn.

Twitter: @innoying
LinkedIn: www.linkedin.com/in/innoying

Security Necromancy: Further Adventures in Mainframe Hacking

Philip Young, aka Soldier of Fortran, Chief Mainframe Hacker
Chad "Bigendian Smalls" Rikansrud, President of Mainframe Hacking

You thought they were dead didn't you? You thought "I haven't seen a mainframe since the 90s, no one uses those anymore." Well you're wrong. Dead wrong. If you flew or drove to DEF CON your information was hitting a mainframe. Did you use credit or cash at the hotel? Doesn't matter, still a mainframe. Did you pay taxes, or perhaps call 911? What about going to the doctor? All using mainframes. At multiple points throughout the day, even if you don't do anything, your data is going through some mainframe, somewhere. 1984? Yeah right, man. That's a typo. Orwell is here now. He's livin' large. So why is no one talking about them?

SoF & Bigendian Smalls, aka 'the insane chown posse', will dazzle and amaze with feats of hackery never before seen on the mainframe. From fully breaking network job entry (NJE) and their concept of trusted nodes, to showing you what happens when you design security in the 80s and never update your frameworks. We'll demonstrate that, yes Charlie Brown, you can in fact overflow a buffer on the mainframe. New tools will be released! Things like SET'n'3270 (SET, but for mainframes!) and VTAM walker (profiling VTAM applications). Updates to current tools will be released (nmap script galore!) everything from accurate version profiling to application ID brute forcing and beyond. You'll also learn how to navigate IBM so you can get access to your very own mainframe and help continue the research that we've started!

All of your paychecks rely on mainframes in one form or another, so maybe we should be talking about it.

Soldier of Fortran: Protect ya REXX! Soldier of Fortran has an unhealthy relationship with mainframes. Being a hacker from way back in the day (BBS and X.25 networks) he was always enamored by the idea of hacking mainframes. Always too expensive and mysterious he settled on hacking windows and linux machines. However, despite not having his own he conducted numerous security engagements against mainframes, slowly developing his skills, until 2010 when he finally got his very own. Not having to worry about system uptime or affecting users he dove in head first and was surprised by what he found. Ever since he has been telling anyone who will listen to him the importance of mainframe security, hacking and research. He's spoken both domestically and internationally on the topic, been a guest speaker at multiple conferences, developed tools for mainframe penetration testing and has even keynoted at large mainframe conferences about this topic.

Bigendian Smalls: BS ain't no chump, takin' apart everything as a child just to see how it works invariable led him to security. From BBSin' back in the day to placing second in the network forensics challenge last year he knows what he's doing. At work and at home he does vulnerability research, forensics and disassembly of all things both on hardware and software. Knowing no system is secure and seeing how closed the source, community and information around the mainframe is he got worried. Worried that the code was as secure as they said it was. Worried that because no one is looking, developers are getting away with murder. Sure, IBM says they got their shit together, but then again so does Oracle, CISCO, Fireeye etc . Having worked on mainframes for more than a decade he knows how frustrating this is. With books from the 80s and forum posts from the 90s being of very little value, he aims to help drive the future of mainframe security research.

Build a free cellular traffic capture tool with a vxworks based femoto

Yuwei Zheng, Senior security researcher, Qihoo 360 Technology Co. Ltd.
Haoqi Shan, Wireless/hardware security researcher, Qihoo 360 Technology Co. Ltd.

In recent years, more and more products, are integrated with cellular modem, such as cars of BMW, Tesla, wearable devices, remote meters, i.e. Internet of things. Through this way, manufactories can offer remote service and develop a lot of attractive functions to make their product more valuable. However, many vulnerabilities have also been introduced into these systems.

It puts new questions to black-box penetration testing engineer. How to capture the SMS command between the cellular modem and the remote server? How to intercept the data link?

Some existing solutions, such as USRP based OpenBTS, commercial product nanoBTS can be used to build a fake base station and capture data traffic. However all of them cannot access the real operator's core network so that they cannot capture real SMS and voice traffic.

With the inspiration from social engineering, we got a femto-cell base station from a telecom operator. After a series of hacking and modifications, we built it as a powerful SMS, voice and data link inception tool. Furthermore, not like a fake station, it's a legal base station and authorized to access the operator's core network. By this tool, we can conveniently explore vulnerabilities of cellular modem inside products.

Yuwei Zheng is a senior security researcher concentrated in embedded systems over 10 years. He had reversed blackberry BBM, PIN, BIS push mail protocol , and decrypted the network stream successfully in 2011. After that, one year later, he finished a MITM attack for blackberry BES, which based on a modified ECMQV protocol of RIM. At the Qtr4 of 2014, he entered wireless security research group, Unicorn Team, in Qihoo 360 China. Now he is focusing on the security issues of embedded hardware and IOT systems.
Twitter: @hwiosec

Haoqi Shan is currently a wireless/hardware security researcher in Unicorn Team, Qihoo 360 Technology Corporation. He obtained bachelor degree of electronic engineering in Harbin Engineering University, China, in 2015. He focuses on Wi-Fi penetration, GSM system, router/switcher hacking etc. Other research interests include mobile phone application security, reverse engineering on embedded devices such as femto-cell base station, video cameras.