- Menu
- Menu
- Home
- About
  - BSidesPDX
  - Code of Conduct
  - Volunteer Information
  - Contact
  - Past Events
- CFP
  - CFP
  - Review Board
- BsidesPDX 2019
  - Register
  - Schedule
  - Speakers
  - Sponsors
  - Contests and Events
  - Venue
  - Volunteer Signup
  - Workshops
  - Review Board

2019 Speakers

Friday Keynote: Eva Galperin

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

Saturday Keynote: Amber Case

Amber Case studies the interaction between humans and computers and how our relationship with information is changing the way cultures think, act, and understand their worlds.

A TED speaker and author, Case enjoys meeting and interacting with interesting audiences all over the world. Her speeches range from the future of technology and humanity to telecom, location-based applications and anthropology. Case is currently a fellow at Harvard University’s Berkman Klein Center for Internet and Society and a visiting researcher at the MIT Center for Civic Media. She is the author of Calm Technology, Design for the Next Generation of Devices. and, she’s been featured among Fast Company’s Most Influential Women in Technology.

Case lives in Somerville, Massachusetts and Portland, Oregon. She was previously the co-founder and former CEO of Geoloqi, a location-based software company acquired by Esri in 2012. You can follow her on Twitter @caseorganic and learn more at caseorganic.com.

How did 8 million developers download an exploit with no one noticing?

Jarrod Overson

In late 2018, a popular node.js package changed ownership. This package became the delivery mechanism for malicious code that traversed through multiple environments to inject its final payload into a mobile application. This exploit existed in the wild for 48 days and was downloaded over 8 million times before it was found. How was it found? What was its purpose and how did it happen in the first place?

This exploit is one example of a well-planned, sophisticated attack that targeted the most valuable and privileged computers in a company, development and build machines. In this session we will dive into how the attack happened, the three payloads, how they worked, how they were obfuscated, and what their goal ultimately was.

This is not node/npm specific and any public repository of source code is vulnerable. This is a growing risk that many companies are absorbing without fully understanding and, without better management, will inevitably lead to incredible exploits in the future.

Jarrod is a Director of Engineering at Shape Security where he led the development of Shape’s Enterprise Defense. Jarrod is a frequent speaker on modern web threats and cybercrime and has been quoted by Forbes, the Wall Street Journal, CNET among others. He’s the co-author of O’Reilly’s Developing Web Components, creator of Plato, a static analysis tool for web applications, and frequently writes and records topics about reverse engineering and automation.

Reversing Corruption in Seagate HDD Translators, the Naked Trill Data Recovery Project

Allison Marie Naaktgeboren & MrDe4d

Translation tables are a dynamic component of HDD firmware that translate logical addresses to physical locations on the disk. Corrupted translators can be the cause of drive failures in drives that appear undamaged and are without physical trauma. That failure can be reversed in many cases. We will present ways to identify if a drive's translator has been corrupted for the Moose & Pharaoh drive families specifically, how to force a translator rebuild, and open source tool(s) to help you repair the translator. Data recovery is a notoriously secretive field. Very little information about firmware and its internal data structures is public. By sharing what we've learned we hope to open this field up to more people, encourage repair, encourage re-use rather than disposal of hard drives, and encourage further publicly shared research. After the talk, attendees should be able to fix this type of error themselves in HDDs of the appropriate families using a TTL converter and the supplied code. Familiarity with the basic components of hard drive firmware is helpful, but not required.

Allison: Allison Marie Naaktgeboren is a Senior Software Engineer, currently working on defending the web at Signal Sciences. She holds a Bachelor's Degree in Computer Science from Carnegie Mellon University. She has written and regretted code at Mozilla, Amazon, Cisco, FactSet Research Systems, as well as the Biorobotics Laboratory of Carnegie Mellon's Robotics Institute. She is a hobbyist security researcher. Allison leads classes on computer science, captains a local CTF team, and mentors disadvantaged high school students in robotics, software, and hardware hacking in the Portland area.

MrDe4d: MrDe4d is the lead data recovery engineer and founder of Revenant Data Recovery. She is a hobbyist embedded systems security researcher currently focused on storage devices and data exfiltration. Most of her research is dedicated to the noble cause of breaking proprietary hardware. In early 2019 she began forming the idea for an open source data recovery suite and now dedicates just as much time to building as she does breaking. She has presented at HushCon, DEF CON, and Teardown as well as at hackerspaces around the USA. MrDe4d is passionate about learning, freedom of information, promoting self-advocacy and hacking the planet!

XXE for Dummies

Brian Myers (@brimy)

In 2017 OWASP added XML External Entity (XXE) Processing to its list of Top Ten Vulnerabilities. Do you know what XXE is, how it can be exploited, and how to defend against XXE attacks? Most of the standard examples use open source stacks. Have you seen XXE in .NET? This crystal-clear explanation and demo will give you all the facts.

Brian Myers, @brimy, (PhD, CISSP) has been working in security for five years and in software development long enough for his resume to include Borland and Netscape. He's written books and articles on Windows programming. In his current job as Director of Information Security at WebMD Health Services Brian guides multiple teams building a SaaS web application housing HIPAA-regulated data. He also serves on the CS/IS Industry Advisory Board at Western Oregon University.

Owning the Cloud through SSRF

Ben Sadeghipour

With how many apps are running in the cloud, hacking these instances becomes easier with a simple vulnerability due to an unsanitized user input. In this talk, we'll discuss a number of different methods that helped us exfil data from different applications using Server-Side Request Forgery (SSRF). Using these methods, we were able to hack some of the major transportation, hospitality, and social media companies and make $50,000 in rewards in 3 months.

Ben is the Head of Hacker Operations at HackerOne by day, and a hacker by night. He has helped identify and exploit over 600 security vulnerabilities across 100s of web and mobile applications for companies such as Yahoo, Airbnb, Snapchat, The US Department of Defense, Yelp, and more. He also invested time in the security community, by creating a community of 200+ active hackers who share ideas and their experiences. He has also held free workshops and trainings to teach others about security and web application hacking.

Attacking Serverless Architectures

Malcolm Heath

Serverless, AKA Function as a Service, is becoming common deployment strategy for all sorts of things. The benefits include reduced cost, easier deployment, and not having to worry about platform. The implementation details for Serverless vary by vendor, and are often not public. In this talk, I describe what serverless is, how it works, what sorts of ways you can find yourself inside it, and what you can do once you're there. Demos will make it abundantly clear that these platforms are eminently hackable, and a tool will be provided that will help assess risk.

Malcolm is a Senior Threat Research Evangelist with F5 Networks.

Modern Websites require Modern Vulnerabilities

Franklin Harding

Your web exploits are showing their age. This talk will outline why it's becoming harder for developers to mess stuff up with modern technologies and tooling (Go, Rust, Kotlin, React, AngularJS, Vue.js, DynamoDB/MongoDB/other NoSQL, OpenID, etc), as well as what mistakes developers can make with these new technologies, and how we can exploit those, featuring practical Go examples.

Software Engineer with a passion for building maintainable, performant, and secure web services with Go. Also hacking. See https://harding.coffee/

Designing ElectionGuard: The Tango of Usability and Security

Morgan Miller

Microsoft's ElectionGuard is designed to be a new standard of election security. Working with an amazing team of experts, I was able to be an interface between the security engineers and the UX professionals, culminating in the design of the ballot tracker ID. The ballot tracker ID would be the closest contact the end user, or voter, would have to the security back end. In this talk, I will showcase how our team discussed, ranked, and vetted priorities in order to come up with a v1 design.

While studying cryptography in graduate school, I was amazed how most difficult most security tools were to use. Noticing the frequency of user-introduced security flaws, I became convinced that usability was the only way to advance cryptographic tools. I have been a practicing UX architect since 2011. I have had the joy of working with many smart people to help build systems that meet business goals (security, profit, etc) and support user needs.

Swarm Intelligence and Human Systems

Nancy Eckert

Humans have used games for thousands of years to exchange information and facilitate cooperation. When we combine gamification with decentralized organization methods, we unlock a powerful tool for social engineering at scale.

In this talk, we will discuss the application of game theory and ““swarm”” strategies for motivating and networking large groups of individuals. We’ll compare the security implications of this approach alongside more traditional models, and examine how these strategies are already being used to empower (and disrupt) existing human systems.

Nancy Eckert, a hacker hailing from Seattle, Washington, has been playing games on the Internet since the early ’90s era of text-based MUDs. Now a champion strategist and community organizer in the world of competitive augmented reality gaming, Nancy leads hundreds of players in capture-the-flag style events across the world.

She picks locks and builds neural networks in her spare time.

SNAPTRAP: The Computer Is Lying: Open-source Deception Platform for Windows

Dave Greer

Attackers are pervasive on modern networks and nothing is safe. Giving up is no option, so let’s bring the fight to attackers with deception, lies, and all other trickery we can come up with. Let’s fool malware about the nature of the computer they’re on, let’s tempt malware with treasures that don’t exist.

This talk introduces SNAPTRAP, a modular open-source framework for orchestrating these deceptions across endpoint workstations on a Windows network. SNAPTRAP allows administrators and power users to set traps on workstations and let incautious malware and attackers stumble in to them.

We are providing a complete functional system along with a simple SDK and documentation. We aim to create an open community of researchers to draw techniques from the hacker tool chest, turn them around, and plant seeds of doubt that maybe, just maybe, their target computer is lying to them.

Dave Greer is a security researcher for Blackberry Cylance after having a bit of a mis-spent youth writing questionable-but-fun things. He has a practical background building security tools and an interest in laughing at security vendors while they try to keep up with the endless torrent of human vulnerabilities.

Argghh, yer kubernetes be now a shark bait!

Alex Ivkin (@alexivkinx)

With Kubernetes becoming a de-facto container orchestration platform, it’s only a matter of time before it becomes a major target. While there are some widely publicized kubernetes vulnerabilities, this talk is not about them. Turns out, the biggest threat to a kubernetes deployment is the person doing it. Many of the default deployment options open container infrastructure to easy pwnage. Come to see how easy it is to slip in and wreck havoc in a k8s cluster and how some simple config hardening can make it substantially harder to abuse.

Alex Ivkin (@alexivkinx) is a director of solutions at Eclypsium, a Portland security company. Alex specializes in security solution architecture, advisory and implementation of firmware and application security, container orchestration and IAM. Alex presented at numerous security industry conferences, co-authored the ISACA CSX Professional certification and spent a lot of time climbing mountains.

Airplane Mode: Cybersecurity @ 30,000+ Feet

Olivia Stella

Imagine being in charge of a system where you own the product. You do not own the software and the hardware is proprietary. You need to coordinate with multiple vendors for any updates or modifications and you're under strict government regulation. By the way, the product has a lifespan of 20 - 30 years. Welcome to the world of aviation cybersecurity, where safety and security live together. At a high level, this presentation will cover what is aviation cyber security, the unique challenges it represents and why the industry is captivating.

Olivia Stella is a senior security analyst for American Airlines. In her current role, she focuses on aviation security and vulnerability management including pen testing and coordinated disclosure. She has over ten years of experience in software development and information security. Previously, she worked at an in-flight entertainment company in product security supporting incident response, risk & compliance, and as the bug bounty lead. She holds a bachelor's degree in computer science, masters in software engineering, CISSP & CISM. When she's not wearing her security hat, she loves to curl and is an avid toastmaster. (That's right, ice curling.)

How to Hack OAuth

Aaron Parecki

OAuth is the foundation of most of modern online security, used everywhere from signing in to mobile apps, to protecting your bank accounts. Despite its ubiquity, it is still often difficult to implement safely and securely, especially in today's landscape, which is dramatically different from the world of online security as it existed when OAuth was initially created.

This talk will explore several real-world OAuth hacks that affected major providers like Twitter, Facebook and Google. I'll share the details of how each specific attack happened, as well as what they could have done to prevent it. Some of these attacks exploited technical flaws in the system, and some exploited the easier to hack, squishier component in the middle: people.

Aaron Parecki is a Senior Security Architect at Okta, an editor of several specifications at IETF and W3C, and maintains oauth.net. Aaron has spoken at conferences around the world about OAuth, data ownership, and quantified self, and his work has been featured in Wired, Fast Company and more.

Down the Dependency Rabbit Hole

John Andersen

As people with the word "security" in our titles, we come across a lot of questionable decisions. It's our job to scrutinize the dubious and guide the less paranoid. Wide eyed developers in a dependency wonderland can easily find themselves smoking opiumssl with a caterpillar from stackoverflow who assured them it's twice as performant than openssl. Nevermind the fact that it was written by @madhatter in 2012 and never touched since. In our infinite wisdom we set them back on the right track. But how wise are we really? Could a robot do just a good a job at guiding them through the looking glass?

Security research, embedded systems, machine learning, and data flow programming are his current interests. He's on the Open Source Security team at Intel. He's from Portland, went to PSU for computer engineering with a focus on embedded systems and did his honors college thesis on machine learning. He's been working at Intel as an intern then an employee for the past 5 years.

Building an intelligence team, it's not what you think.

Randy Waterhouse

Every vendor claims to be a threat intelligence company at least at their booths at…pick giant conference here. Many organizations have people who claim to be intelligence analysts. When in fact most vendors just provide data, and most of these so called intelligence analysts are doing IOC integration work for a SOC. Have you heard of being intelligence led? What do you really need to do to be intelligence led? It's not just a bunch of python scripts and IOCs for a SOC. There is a lot more work in growing into this. And the technology In this talk it's going to cover how you've been thinking about it incorrectly, how you can change your ways, and how you can get talented people from places you'd have never considered to run and build your program.

Randy_Waterhouse spends his days helping people understand the importance of Intelligence as a guiding principle for building out effective security processes and leveraging technologies responsibly to build their cyber defense centers and security operations practices. His alter ego, at one time developed a number of intelligence products and helped vendors bring these to market. These products have included threat and vulnerability management tools, IOC prediction algorithms, intelligence subscriptions, and strategic intelligence consulting. Randy_Waterhouse also appears at Defcon fairly regularly as a Goon, and every once in a while he can be found out in the desert on his Harley with a flamethrower, sometimes with just a flamethrower. He and his co-author's book "Ransomware: Defending Against Digital Extortion" has been used by many IT professional to aid in their programmatic response to the rise Ransomware.

Creepy Digital Forensics

Marcus Richerson

This talk will detail the techniques, process and outcome of an unusual digital forensics investigation.

Marcus has been working in information security over 13 years. He actively host and participates in capture the flag hacking competitions and enjoys reverse engineering, exploit development, lock picking, SCADA security, digital forensics, embedded device hacking, web hacking and mobile application hacking.

Giving Back: How to Support The Next Generation of InfoSec Professionals

Tobin Shields

Mt. Hood Community College launched a two-year Cybersecurity degree in 2011. Since that time the program has evolved dramatically: courses have been continually revised to teach only industry-relevant skills, the college has hired new faculty to lead even more advanced and updated topics, and also worked with partners to begin offering meaningful internships for students. But the college still faces a problem: academia lives in a slio. As an institution, we realize that if we want to elevate our students learning to the next level, we need to develop stronger relationships with InfoSec professionals, and their organizations. This talk will directly outline how professionals can give back by acting as student mentors, sitting on our advisory committees, developing internships, teaching courses, as well as being willing to review courses to ensure the correct content is being taught.

Tobin Shields is a full-time instructor at Mt. Hood Community College. There, he primarily teaches topics in IT and InfoSec as apart of their intensive, two-year CTE program. Tobin has two masters degrees, one in Education and the other in Cybersecurity and Information Assurance. He also holds his Security+, CEH, CHFI, and RHCSA certifications. Tobin has been working as an educator for the past five years, and has a passion for teaching STEM topics

Blarney and Brigandry - Physical Breach War Stories & Operations

Robert Moore

Even mature, robust, and well-funded cyber security programs can be bypassed entirely by poor physical security. Overt social engineering or covert physical security breaches have frequently and consistently compromised numerous Fortune 500 companies, regardless of the sophistication of their cyber security programs.

War stories and examples of successful compromises will be shown, showing the intimate relationship between physical and cyber security. Examples include subversive and surreptitious means, or shameless and brazen social engineering, resulting in total compromise achieved with negligible cost, a bit of bravado, and sometimes effort than can be measured in hours.

Robert is a Senior Security Consultant for NCC Group originally out of Milton Keynes (UK), and now based out of Seattle (US). Having a previous academic background in intelligence-based national security, he has pursued foreign language, lived, and studied abroad in multiple countries before moving into the technical side of security.

His focus delves heavily into all aspects of Red Team/Full Spectrum Attack Simulation (FSAS), with a particular knack for physical and network security. As part of these engagements, he has taken part in security assessments for multiple Fortune 500 companies by simulating attacks in the guise of a real-world adversary and demonstrating how simple gaps in physical security can lead to full-scale company compromise.

How Not to be Seen: Creating Non-Speculative Side-Channel Resistant Code

Matt Wood

Software side-channels have been a hot topic recently, and with good reason. Many of the techniques are used to liberate secret information from other processes or trusted execution environments (TEEs) such as Intel's SGX, ARM's TrustZone, and the like. Some of the techniques making headlines are related to speculative execution properties of modern processors, but there is an entire class of non-speculative techniques also receiving a lot of attention in recent research. Luckily there are a few techniques available for implementing algorithms that use secrets—like cryptography—so they present as few opportunities for leaking information as possible. In this talk you will learn the anatomy of a few classic non-speculative side-channels on mathematical algorithms used in just about every system in modern computing, followed by industry best practices for mitigating them, and finally what you can do to help minimize the risks for your applications.

Matt is a Principal Engineer in Intel's System Software Products (SSP) division, focusing on open source security. Part of his day to day job involves helping project teams understand how to implement and use cryptography properly.

They Put Money on the Internet!

Dean Pierce

We now live in a world where blockchains exist, and often times, they're full of what is now considered to be money. That's pretty neat. So how might one crack open these pinatas and obtain the delicious goodies within?

This talk will focus on using and abusing Ethereum smart contracts for fun and sometimes profit, starting with the basics and then diving deep into the latest dumpster fires and the latest tools and techniques for setting them.

Security researcher from Portland Oregon. Locally affiliated with PDX2600, RainSec, Sophsec, CtrlH, PDX Bitcoin, BSidesPDX. Hacks stuff @ ConsenSys Diligence

Interactive Threat Defense: Incident Response, Threat Intel, and Red Team (oh my!)

Eric Goldstrom

Incident Response, Cyber Threat Intelligence, and Red Teaming are critical components of a holistic security program; however, many companies have not implemented some of these capabilities. The goal of Interactive Threat Defense (ITD) is to provide a proactive, data driven, hands on approach to risk identification and security control validation. Throughout the presentation, you'll discover how to effectively integrate these capabilities into one program. Topics will range from methodologies and frameworks to tooling and actionable ways to improve your overall security posture.

Eric Goldstrom is the Security Incident Response Manager at Cambia Health Solutions in Portland. In his role, he built a new program called Interactive Threat Defense which will be the subject of the presentation. Prior to the private sector, Eric worked in the DoD conducting both Computer Network Exploitation (CNE) and Computer Network Defense (CND) operations. He has a MS in Cyber Security and his certifications include CISSP, OSCP, and SANS certifications.

2FA So Strong It Could Be 1FA: Integrating WebAuthn for Phishing-Resistant Authentication

Greg Stromire

The effort to protect users with strong, phishing-resistant authentication just got a huge win with the WebAuthn standard. Modern browsers already support it and many users already carry with them the necessary hardware. All that remains now is for us to integrate it into our web apps. This talk covers many of the important details for implementing WebAuthn as a second factor (and potentially even a first factor) authentication mechanism.

Greg Stromire is an application security engineer for Gemini where he works to shift security as far left as possible. When he's not developing features to enhance the security of Gemini's main products, he's performing security assessments, building developer tools, and creating secure coding curriculum.

ABC to XYZ of Writing System Management Mode (SMM) Drivers

Brian Delgado & Tejaswini Vibhute

“SMM is a special-purpose operating mode provided for handling system-wide functions like power management, system hardware control, or proprietary OEM-designed code.” – Intel Software Developer Manual

System Management Mode (SMM) has gotten a lot of attention for being the most privileged processor mode, which raises concerns over how software and firmware manage hardware. This session demystifies designing and writing System Management Interrupt (SMI) handlers, and covers challenges that developers face in the process. Content covers different types of SMI handlers and various methods of invoking them. The session also describes common vulnerabilities that can result from incorrect coding practices or oversights. Debugging is critical to developing quality SMM drivers, so this session also demonstrates debugging using virtual environments (OVMF) and physical platforms.

Brian Delgado is a Security Researcher in Intel’s Platform Armoring and Resiliency team (PAR). Brian has worked extensively in firmware security including Intel’s SMI Transfer Monitor (STM) feature to help protect a hypervisor against malicious BIOS code. Brian is currently focused on applying fuzzing on UEFI code to identify code security issues. Brian is working on completing a PhD at Portland State University (PSU) in firmware-assisted rootkit detection and learning about photography.

Tejaswini Vibhute is a Security Researcher in Intel’s PAR team. She develops security tools for automated firmware validation leveraging fuzzing and virtualization. She has worked extensively with System Management Mode (SMM) security at Intel. Prior to joining Intel, at PSU, she utilized Intel’s STM to enable firmware-assisted rootkit detection. Tejaswini also published the first publicly available Xen patches to launch Intel’s STM. In her free time, she can be found taking care of her furry friends or traveling around the country.

Improving Anonymous Networking

Kevin Froman

VPNs and Tor are used by average citizens, hackers, and movie characters alike to mask their identity online. However, my research has shown that these tools have shortcomings in usability and privacy preservation; none fulfill both key security and usability requirements.

This talk will begin with the philosophy of anonymity networks, their desired technical requirements, and a short introduction to a selection of existing networks, including my new project Onionr. Additionally, the talk will provide an overview of the major features to look for when picking an anonymous network to use. At the end, I will demonstrate how Onionr fulfills our requirements of a well-made anonymity network. Attend this talk to get beginner-friendly insight into the world of anonymity networks and a look at a new network project.

Kevin is a computer science college student with an interest in security and ethical technology. He has experience with web development and security, with a fondness for cryptography and decentralization.

Updates from the Crypto War 2.0

Wendy Knox Everette (@wendyck)

Federal law enforcement agencies recently demanded that Apple break the encryption used by iOS in the Apple v FBI fight in 2015, but backed down when an exploit was used to break into the iPhone.What followed was a pause in the demand for encryption backdoors for a few years, but that break has been short lived. This talk will update attendees on the history of the demands for encryption backdoors, from the Clipper chip to the creation of CALEA, and summarize recent demands from law enforcement to the tech industry to weaken strong encryption and allow law enforcement to access any data, any time.

Wendy (@wendyck) is a software developer who burned out and went to law school, where she completed a concentration in National Security Law and interned with the FTC, FCC, and some other three letter agencies (no, not the fun ones). After law school she completed a fellowship in privacy and information security law at ZwillGen. She currently lives in Seattle, where she is a Senior Security Advisor at Leviathan Security Group.

A Game Theoretic Analysis of Tor’s Resilience to Entry-Exit and End-to-End Attacks

Krisztian Gado

Tor is among the most used networks for anonymous communication. This anonymity can be undermined via entry-exit and end-to-end attacks. Using Game Theory, we introduce and analyze the viability of several methods for reducing Tor's vulnerability to such attacks. Entry-exit attacks rely upon controlling entry and exit nodes within the Tor Network, while end-to-end attacks utilize Autonomous Systems. Because both types of attacks rely on chance, we consider the success probability maximizing strategies of adversaries. We analyze changes to Tor's routing strategy that decrease the success probability of such attacks. Our goal is to support anonymity preserving systems against large Autonomous Systems providers and attackers with access to large computing power. We build upon previous work by eliminating exit node bandwidth quotas within Tor and decreasing asymmetric routing to make compromising anonymity less likely. We show the probability that anonymity is preserved if one uses Tor for a year can be increased from ~62% to ~85% if our suggestions are implemented.

Researcher at Lewis and Clark College

Hacking Hypebeasts: An exercise in threat modeling and reverse engineering the Nike's Self-Lacing Shoes

Aaron Wangugi

Ever since back to the future, the countdown had begun for Nike to create self lacing shoes, for a bad OTA to brick them and for someone to try and hack them. This talk will take you though my efforts to threat model and reverse engineer Marty McFly's shoes.

We'll be looking at a Nike BB Adapt. This talk will show how I reverse engineered the Nike Adapt Android application, took a look at Nike's account's management and poked at the Bluetooth protocol.

Aaron is an Security Engineer at Snap. At Snap he builds tools to help to help developers write more secure code and conducts security reviews. When he is not working he is hacking around on random things or drawing.

Literature Circles: Novel Ways to Learn about Cybersecurity

Veronica Hotton and Ellie Harmon

This talk is about how Literature Circles were a novel and effective way to teach middle and high school teachers about the GenCyber Cybersecurity Concepts (Defense in Depth, Availability, Confidentiality, Think Like an Adversary, Integrity & Keep it Simple) during the CyberPDX 2019 summer camp. The young adult novel "Warcross" by Marie Lu will be highlighted showing how fiction, poetry and art can be an innovative way to broaden public understanding of cybersecurity. More information about CyberPDX can be found here.

Veronica Hotton (PhD, Curriculum Theory and Implementation, Philosophy of Education, Simon Fraser University, Canada) is an Instructor in the University Studies program at Portland State University teaching interdisciplinary general education courses. Veronica is a co-director of CyberPDX, a summer camp for broadening participation in cybersecurity. More information at https://veronicahotton.com/

Ellie Harmon (PhD, Information and Computer Science, University of California, Irvine) is a Senior Instructor in the Department of Computer Science at Portland State University teaching courses in introductory computer science, human-computer interaction, and computing & society. Ellie also teaches in the University Studies program. Ellie is a co-director of CyberPDX, a summer camp for broadening participation in cybersecurity. More information at https://web.cecs.pdx.edu/~harmon8

[In]secure deserialization, and how [not] to do it

Alexei Kojenov

Serialized data is neither new nor exciting. Serialization and deserialization have been in use by countless applications, services and frameworks for a long time. Many programming languages support serialization natively, and most people seem to understand it well. However, many of us don't fully understand security implications of data deserialization, and in the last couple of years this topic got an increasing focus in the security community, up to the point that insecure deserialization made it to the list of OWASP Top 10 most critical web application security risks! Needless to say high-severity vulnerabilities in some well-known applications as well as popular frameworks such as Apache Struts and Apache Commons Collections raised awareness of this risk.

In this session, we'll discuss how serialized data are used in software, talk about different serialization formats and the dangers of deserializing untrusted input. We will review some real life vulnerabilities and related exploits. The presentation will contain several code examples with live demos of bypassing security controls by exploiting deserialization vulnerabilities. We'll forge a session cookie, elevate privileges, cause a denial of service, and even perform a remote code execution - all via insecure deserialization! The demos will use native Java, Python and .NET serialization, as well as JSON and XML formats. Of course, we'll also talk about how to deserialize in secure way!

Next time you develop your awesome web or mobile app or a microservice, keep in mind how a clever attacker could create and supply malicious data to your application, and thinking like a hacker you could write more secure code!

Alexei began his career as a software developer. A decade later, he realized that breaking code was way more fun than writing code, and decided to switch direction. He is now a full-time application security professional, with several years of assisting various development teams in delivering secure code, as well as security consulting. He currently works as a senior product security engineer for Salesforce, and occasionally speaks at local security events and global conferences.

Performance Hacks for SOC Training

Will Peteroy and Alex Sirr

Great people are the foundation of security operations. We'll discuss how to leverage intern programs and on-the-job training to increase the effectiveness of your existing team and to create a great pipeline to engage new team members. Alex will provide his perspective going through the program as an intern and continuing to develop it / lessons learned as a full time employee.

William Peteroy is the Chef Technology Officer for Security at Gigamon where he leads security strategy and innovation efforts. William is also the founder and CEO of ICEBRG (acquired by Gigamon in 2018) and has previously held a number of business and technology leadership positions at Microsoft and in the US Department of Defense.

BACKUP SPEAKER

Clearly seeing the value of Canaries for the year 20/20

Jared Folkins

This talk will walk the listener through the value and history of canary and honeypot projects going as far back as the early 90s. It will bring to light how the technology is still heavily under utilized in the new era of big data and epic breaches. The speaker will work to equip the listener with a persuasive argument to take back to their corporate class or leadership team. Finally he will reveal and discuss the development of a new open source canary project that focuses on simplicity and sustainability for under-resourced teams.

After surviving the dot-com crash of the late 90s, Jared Folkins has gone on to have a long career in systems and programming. In 2013 he turned a hobby into a career and has never looked back. Known for having technical chops and a high emotional IQ, he enjoys working with those who prioritize goals and people first while placing egos last. He currently Red Teams for ThreatHound.com, Blue Teams for Bend La Pine Schools, and breaks down software while building up people at OpsecEdu.com. If you want his help or you just need a new InfoSec friend contact him at https://www.JaredFolkins.com.