BSides Asheville 2017 – Schedule and Speakers

Friday July 28th RISC Networks
04:30PM – 05:00PM Registration
05:00PM – 09:00PM Training

Saturday July 29th RISC Networks
08:15AM – 09:00AM Registration
09:00AM – 09:50AM Bryan Austin
10:00AM – 10:50AM Roger Seagle, Brian Manifold, Blake Hitchcock
11:00AM – 11:50AM Jason Gillam
11:50AM – 01:00PM LUNCH
01:00PM – 01:50PM Ernest Wong
02:00PM – 02:50PM Brian Richardson
03:00PM – 03:50PM Nancy & Phoenix Snoke
04:00PM – 04:50PM Justin Troutman - Closing Keynote
04:50PM – 05:00PM Closing Comments and Raffle

Justin Troutman - Freedom of Press – Closing Keynote

Ernest Wong - Army Cyber Institute - Innovation Beyond Just 1s and 0s--Innovating for Cyber Warfare (aka What the Demi-Gods at NSA have Gotten Wrong)

Today innovation is a key buzzword within the US Army, and it is helping to shape the vision for the "Army of 2025 and Beyond" as an agile organization able to adapt and prevail in this complex world. But does our Army have the capabilities to protect vital national interests in cyber? The growth of the Internet in our globally connected world has meant that tools for cyber are constantly changing. Accordingly, do we have the capacity to gain the advantages needed to out-hack our adversaries in this domain? This presentation provides a simple framework for analyzing different types of innovation, and in doing so, asks us to think of new and better ways to promote how the US Army can defend and deter against attacks within cyberspace. By analyzing what innovation really means and by highlighting the differences between four distinct types of innovation (disruptive, breakthrough, sustaining, and incremental), this presentation shows us just how easy the US Army can develop and nurture successful innovations for the cyber domain to out-hack cyber crackers.

While most of this presentation focuses on innovations for the defense of the cyber domain, I will also provide key insights into how the US Army currently conducts (and is failing) at operationalizing cyber into tomorrow's battlefields. Fortunately, the talk does provide clues into how the military can bolster not just its defensive cyber operations but also its offensive ones as well, in spite of the controls and restrictions the NSA has imposed and directed.

Bryan Austin – Social Engineering a Better World

In today's modern world, communication is easier and faster than ever before, but still we are struggling to get our point across. It's time to start thinking about how to change the world, and it starts with good communication. This talk will outline the methods used by professional counselors, hostage negotiators and social engineers: active listening, empathy, rapport building, influence and behavior change, and how to leverage these simple principles into an effective method for influencing people to make better decisions. This class is useful for pentesters who need to gain rapid access to restricted areas, people who need to learn to better communicate with their significant other, and even business people to become more effective at communicating goals and results with clients or share holders. The personal example and experience of Bryan Austin as a social engineer and counselor will demonstrate the effectiveness of these techniques, as well as explain some of the science behind them. This will help you become the change you want to see in the world.

Bryan Austin is an information security researcher at Guidepoint Security with a background in social engineering, reverse engineering, analysis and a passion for makeing. By day, he secures people and organizations against scammers, malware, and hackers but by night he works with children with behavioral issues and a variety of other challenges. When not crusading against internet evil doers, he enjoys social engineering and hacking with his beautiful wife and 3 amazing children.

Brian Richardson - Intel - What you don't know about firmware might get you 0wn3d

In recent years, firmware has become a more attractive target for hackers. Insecure firmware can allow attackers to install persistent exploits below the OS layer. Developers need to understand why attackers target firmware, the makeup of common attacks, and how to secure platforms against common attacks. This session uses research from Intel and McAfee Advanced Threat Research (ATR) to describe common attacks on UEFI firmware, using open source examples to demonstrate best practices for detecting and preventing low-level system exploits.

Attendees will learn about common methods used by attackers to circumvent OS-level protections and install persistent attacks in platform firmware. The session will also demonstrate tools used to detect firmware issues, and best practices for firmware developers using open source UEFI examples.

Brian Richardson is an Intel technical evangelist who has spent most of his career as a "BIOS guy" working on the firmware that quietly boots billions of computers. Brian has focused on the industry transition to the Unified Extensible Firmware Interface (UEFI), demystifying how firmware works and simplifying firmware development tools. Brian has presented at conferences including LinuxCon, Linaro Connect, Bsides and Intel Developer Forum. When he's not blogging for the Intel Software Evangelists project, Brian shoots videos and photos of his travel around the world.

Nancy & Phoenix Snoke - Magick Security - Hacking The IoT: A Case

Study

An IoT device is made up of 5 different components: the hardware, webapp, mobile apps, network communication and API. Hacking an IoT device requires looking at each component individually, as well as looking at the whole picture. In this talk, husband and wife team — Nancy and Phoenix Snoke — go through the process and findings of hacking an actual IoT device: a baby monitor. Both general methodology and specific examples will be presented. This talk concludes with tips for setting up your own IoT device hacking lab. Note: As there has been no response from the manufacturer of the device we are not disclosing the manufacturer and model number or other identifying information of the IoT device.

Roger Seagle, Brian Manifold, Blake Hitchcock - Cisco - Scaling Security Testing at the Speed of DevOps

Recent software development trends, namely DevOps, Continuous

Integration, Continuous Delivery, and Continuous Deployment, have empowered developers and drastically reduced the DevTest window
forcing teams to adopt highly automated test infrastructures.

While the adoption of these trends and automated test frameworks have improved feature delivery and time to market, they have complicated security assessment, producing substantial gaps between the current release and the last security audited code. Consumers are now being forced to adopt new code releases daily or hourly without substantive security review, especially in the Software as a Service (SaaS) sector. As engineeringteams rapidly embrace these development methodologies, the community must evolve security testing strategies so as to enhance the security posture of products, services, and solutions.

This evolution must address three primary problems elucidated by the aforementioned development trends:
1. Testability: Security requirements should be testable and verifiable.
2. Scalability: Security requirements should be capable of being automated in a best-effort fashion so as to scale effectively.
3. Accessibility: Security tools and results should be easily digestible by software engineers and testers, and new security tools
should be accessible to all development and test engineers.

Therefore, we have developed and are preparing to open source a new distributed security testing framework called Norad which facilitates security assessment at scale. This framework automates multiple open-source and vendor security tools and aggregates their results for review. It also provides an SDK which promotes the development of community developed security test content. This talk will explain Norad's design philosophy, architecture, and demonstrate its usage.

Authors: Blake Hitchcock, Brian Manifold, Roger Seagle

Jason Gillam - Secure Ideas - Lockstepping the SDLC: A guide to securing your Agile development life cycle

A lot of security teams are facing challenges when they try to integrate traditional security testing methods with agile development groups. The lack of requirements documentation, baffling. In this talk, Jason will explore the agile manifesto and how it relates to application security in a way that can help produce more secure software from the ground up.