Practitioner Perspectives

WOLF DEN ASSOCIATES, LLC

August 2018 *(Vol. 7; Issue 8)*

Top 10 Activities for DEF CON Newbies

1. ***Roll the dice on the open Wi-Fi for the chance to make it on the "Wall of Sheep"***
2. ***Visit MohawkCon and get your head buzzed for charity***
3. ***Compete in the tin foil hat contest and stop Big Brother from listening to your innermost thoughts***
4. ***Partake in a DEF CON ritual by having a shot with a first-time speaker***
5. ***Test out your soldering skills and create a badge at the BadgeLife contest***
6. ***Brush up on your RF skills and take the HAM radio exams***
7. ***Dress like a Fed for the chance to get called out by a security "Goon" and win a coveted "Spot the Fed" t-shirt***
8. ***Remember 3-2-1: get at least three hours of sleep each night, two meals per day, and one shower per day – no exceptions!***
9. ***Pay $40 for the Skytalks badge so you can skip the line and maximize your time in this forum***
10. ***Participate in the Wireless Village and go fox hunting – seek out wireless signals roaming throughout the conference***

The Best of DEF CON 26

- DEF CON unites experts from the hacker community and has continued to grow with twice as many villages in '18 relative to '17
- DEF CON is an excellent forum to stay abreast of cyber security trends, with AI, drones, and ethics getting their own villages this year
- AI, machine learning, and software defined radio advances featured prominently in the various talks and DEF CON 101 addresses
- After Russian tampering in US elections, DEF CON 26 stressed that Social Engineering is a growing and high-risk cyber security threat
- DEF CON speakers also highlighted healthcare technology, where security is often sacrificed for patient convenience and lower costs
- Who says nerds can't be social beings – DEF CON 26's badges were hackable, but you had to connect with 7 others to unlock everything

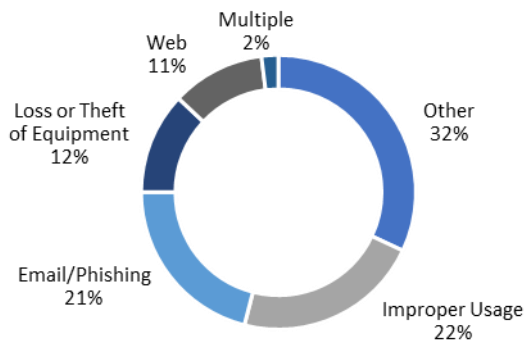
I Can Hear You Now

After focusing on IOT last year, at DEF CON 26 we concentrated on a new, prolific, and rapidly growing cyber threat vector: wireless communications. Wireless operates over radio frequency (RF) and includes applications ranging from Cellular, Wi-Fi, Satellite TV, GPS, Bluetooth, and Near Field Communications. The arrival of Software Defined Radios (SDRs) has drastically reduced operating costs, replacing expensive hardware radio components with low cost software. RF operators are no longer limited to government and large corporations – script kiddies can now sink their teeth into the untapped new world of RF, full of vulnerabilities waiting to be discovered. To minimize exposure to these growing threats, deploy trusted protocols and secure devices inside your network perimeter, providing multiple levels of security.

Do you DevOps?

The focus of this year's DevOps presentation was on not making DevOps too easy – an idea that sounds absurd. DevOps is rapidly leading us down a path where developers effectively deploy their own code to production, with nearly half of all Sysadmin positions being replaced by developers. While this may suggest a tremendous increase in efficiency, it also increases the likelihood that no one understands the CI/CD pipeline, which erects huge barriers for maintenance and upgrades over time. To mitigate this risk, developers must always have several belly buttons with the complete knowledge of the development pipeline. While this step is necessary for DevOps practitioners in all industries, the presentation did highlight that, apart from leading software companies like Spotify and Google, the government is keeping pace with industry in the DevOps world – an admirable achievement for a customer set that is usually a lagging adopter of technological advancements.

Federal Information Security Incidents by Category



Improper Usage (i.e., violation of usage policies) and Email/Phishing (i.e., email messages or attachments) comprised nearly half of 35,277 federal information security incidents in FY17.
Source: GAO-18-645T Report

Greetings from Your Friendly IT Department

As every CNO practitioner knows, humans are the weakest link in gaining system access. The Social Engineer Village (SECTF) at DEF CON 26 put this idea on display by testing – in front of a live audience – how much information participants could gather about a company (e.g., type of operating system) through open source intelligence (OSINT) and 20 minutes of phone calls. For the Fortune 500 companies tested, many participants were alarmingly successful. They found information online, in employee postings, and in phone calls with a pretext. Large companies are particularly vulnerable to these hacks as their large and dispersed workforce increases the attack surface. To combat this, employees must be trained to look for attacks, empowered to make decisions, and tested regularly through red teaming exercises.

Healthcare Scares

Speakers at DEF CON 26 stressed that the healthcare industry is particularly susceptible to many of the vulnerabilities we have listed. With the push to cut costs by getting patients out of the hospital and home quickly, and the increased use of wearable and implantable health technologies, more critical systems are becoming either wireless, plugged directly into the Internet, or both. To demonstrate the vulnerability of these systems, researchers at DEF CON 26 were able to easily change the data being sent back to the nursing station from a patient's bedside monitor. In addition, many patient monitoring systems are directly connected to the Internet (e.g., monitoring systems in ambulances that wirelessly transmit data back to the hospital through public cellular systems), which leads to the possibility that a bad actor could adversely affect patient care from a distance. While there has been a lot of spending on health data interoperability, health data is perilously vulnerable and overdue for investment.

1751 Pinnacle Drive
McLean, VA 22102
wolfdenassociates.com

Samuel Krehnbrink
Sam@wolfdenassociates.com
(703) 336-7847

Laura McElhaney
Laura@wolfdenassociates.com
(703) 403-4127

Bo Slaughter
Bo@wolfdenassociates.com
(770) 490-6655