Practitioner Perspectives

WOLF DEN
ASSOCIATES, LLC

September 2015 *(Vol. 4; Issue 9)*

Top 10 Lessons of DEF CON 23

1. ***Insider threat is the #1 concern among security professionals***
2. ***A well-meaning software function can be just as dangerous as an inadvertent flaw***
3. ***Collect Open Source Intelligence (OSINT) on bugs/security issues to mitigate open source software risks***
4. ***Tier 1 support personnel will be replaced by bots within a few years***
5. ***Secure messaging apps are only as secure as underlying HW and SW infrastructure***
6. ***Social engineering is the most effective way to hack into a company's network***
7. ***A secure network is a by-product of well-trained people, appropriate tools, and well-tailored policies/procedures***
8. ***Shared repositories and databases that are accessible to all are treasure troves for malicious users***
9. ***Financial malware often cannot distinguish good data from bad; flood the system and anti-fraud devices will do the rest***
10. ***Nothing beats a white hat hacker and his toolbox to ferret out security flaws***

Cybersecurity's Bleeding Edge – Lessons for the Federal Market

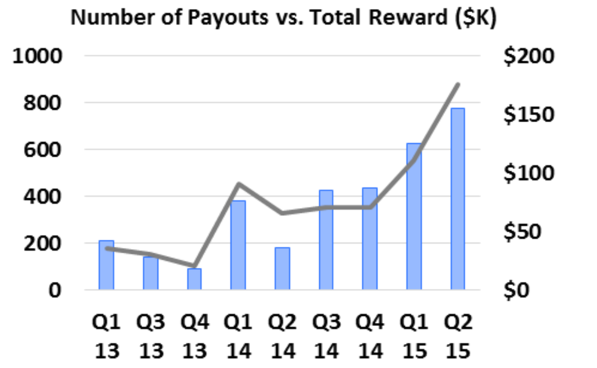
- DEF CON 23 attracted security professionals, hacktivists, hobbyists, and cyber criminals to showcase the latest trends in cybersecurity
- Everything with an IP address can be compromised, as evidenced by hackers taking over Tesla, Chrysler, Cadillac, and Toyota systems
- Services such as SurveyMonkey are vetting pentesters and hackers so companies know whom they are letting into their inner circle
- The Ashley Madison hack validates crypto-evangelists, but the ordeal could have been avoided with appropriate access restrictions
- Unstructured penetration testing trumps compliance checklists for intrusion prevention and can be effective at combating insider threats
- To minimize the threat profile from the IoT, place outside devices on a different subnet and limit data access to minimize spillage

It's About Who's Got the Information.

"How to Hack a Tesla Model S" was one of the most compelling and well-attended talks at DEF CON 23. By exploiting multiple security flaws, the presenters gained full access to the car's internal controls. Beyond the initial shock value in the reality of zero day attacks on cars, the presentation illuminated how Tesla has partnered with the presenters and other white hat hackers. Tesla's public bug bounty program enabled them to identify and fix security holes before a widespread exploit. At the time of presentation, Tesla had already pushed out a patch to these vulnerabilities via wireless update. This stands in stark contrast to Chrysler, who alienated hackers, downplayed threats, and ultimately recalled 1.4 million vulnerable vehicles. Federal market participants should emulate Tesla's approach and make friends, not enemies, of the hacker community.

Hack the Planet!

As shown in the chart on the right, companies are increasingly embracing crowdsourcing of bug bounty programs to stress test their applications. This approach has caught on because bounty programs attract many of the best and brightest white hat testers and only pay them for successful outcomes, rather than paying a relatively fixed fee, regardless of performance, to quality assurance or IV&V teams with limited resources and generalist experience. This can be a safe and inexpensive way to quickly test applications. The next evolution of this practice – one that is particularly relevant to federal market participants – is migrating from an open-to-public model to an invite-only model. This invite-only model combines the attractive network effects of crowdsourcing, with the ability to pre-screen hackers that have already met specific technical and ethical criteria. Several Silicon Valley firms, including one founded by ex-NSA employees as well as a few online survey services, are currently exploring this business model to meet the increasing demand.



According to BugCrowd, as the number of payouts and total rewards from bug bounty programs increases, more attention is being paid by researchers, resulting in more submissions and vulnerability resolutions.

No. It's *the* Code Breaker. No More Secrets.

Not only a boon for Tor downloads and cocktail party conversation, the recent Ashley Madison hack provides a revealing case study. On the positive side, this hack is a small victory for encryption, as credit card information remains unrecoverable. The long list of worst practices starts with relying on Payment Card Industry (PCI) standards, which are useless when user names reveal identities. Another failure was the lack of two-factor authentication. In an era of cluster computing, rainbow tables, and cheap hardware, passwords alone are obsolete. Ultimately, the core issue is the massive reuse of passwords, as well as employee possession of too many privileges. The hack might have been avoided by using unstructured pentesting to emulate the methodology of malicious adversaries. As we have said before, this is still the most effective prevention technique.

Shall We Play a Game?

Compounding the aforementioned security challenges is the fact that Bring Your Own Device (BYOD) policies and the Internet of Things (IoT) continue to expand the cyber threat profile. With connectivity increasing faster than protection mechanisms, security policies and enforcement cannot keep up. Reactions like adopting a "No Chinese" hardware policy or spending a fortune on Mobile Device Management (MDM) applications are stop-gap solutions. A home laptop – even an American-made one – can be a dangerous weapon, especially if it has an embedded adware "feature" that targets Secure Socket Layer (SSL) and a rootkit that preempts any operating system installation. Similarly, as every toaster, refrigerator, crockpot, and safe increasingly comes with an IP address, all outside devices should be placed on a different subnet in the office to minimize data access and potential spillage. If the Chinese do not have everything they need from the recent OPM breach, the Lenovo botnets running on corporate infrastructures can help them complete their records.

1751 Pinnacle Drive
McLean, VA 22102
wolfdenassociates.com

Rick T.
Rick@wolfdenassociates.com
(703) 638-5924

JJ A.
jjohn@wolfdenassociates.com
(443) 838-1202

Laura M.
laura@wolfdenassociates.com
(703) 403-4127