Practitioner Perspectives

WOLF DEN ASSOCIATES, LLC

September 2016 (Vol. 5; Issue 9)

Top 15 Products with Known Vulnerabilities

1. *Google Android Operating System 385 vulnerabilities*
2. *Debian Linux Operating System 278 vulnerabilities*
3. *Canonical Ubuntu Linux Operating System 238 vulnerabilities*
4. *Adobe Flash Player Application 226 vulnerabilities*
5. *Novell Leap Operating System 217 vulnerabilities*
6. *Novell OpenSuSE Operating System 216 vulnerabilities*
7. *Apple Mac OS X Operating System 166 vulnerabilities*
8. *Adobe Acrobat Reader Dc Application 152 vulnerabilities*
9. *Adobe Acrobat DC Application 152 vulnerabilities*
10. *Linux Kernel Operating System 151 vulnerabilities*
11. *Adobe Acrobat Application 149 vulnerabilities*
12. *Google Chrome Application 149 vulnerabilities*
13. *Adobe Reader Application 129 vulnerabilities*
14. *Apple iPhone Operating System 118 vulnerabilities*
15. *Mozilla Firefox Application 114 vulnerabilities*

Pwning DEF CON 24

- The pervasive use of networking in the office and home has opened up numerous – and ever-increasing – security holes
- While individual components comprising IoT products may be secure, their amalgamation is often quite vulnerable
- We are just seeing the tip of the IoT threat iceberg and extensive investment in training and testing is required to avoid disaster
- The market to secure the IoT is wide-open, but the burden of proof is higher than ever before and third party IV&V is required
- Next-gen hacking will be conducted by autonomous machines, not humans; expect vulnerability identification rates to soar
- Very few traditional government IT or defense contractors competed in DARPA's Cyber Grand Challenge and those that did fared poorly

Wall of Sheep

Since we wrote in August 2014 about how to protect yourself on the Cyber Serengeti, the stakes have gotten higher, the adversaries have gotten fiercer, and we are far more vulnerable. With the growth of the Internet of Things (IoT), there are more weak points than ever, providing attackers with nearly limitless possibilities for network entry and lateral movement, and all of us are now unwitting sheep. While competing in the IoT ethical hacking challenge at DEF CON 24, we generated hacks to lock your home thermostat, to disable your home network, and to remotely control motorized hospital wheelchairs. Within the IoT, we are seeing a resurgence of old-school hacks that eschew advanced memory manipulation techniques, instead deploying insecure maintenance interfaces that allow arbitrary code execution.

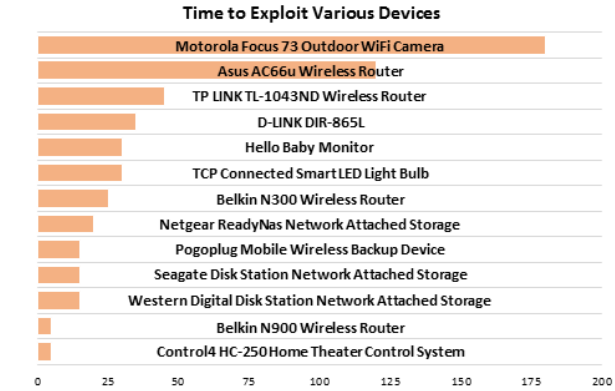

Figure shows how many minutes it took for Wolf Den engineers to compromise various devices during the IoT Challenge at DEF CON 24 last month. How many are in your office? How many are in your home?

Source: Wolf Den Analysis

Get Baked

In a world where security is a requirement, but formal definitions of "Security" are scarce, it is increasingly difficult for product vendors to stand out. Making a demonstrably secure product is difficult and expensive. The competing priorities of adding new features, getting to market quickly, and containing cost often result in unintentional security vulnerabilities. One possible solution – albeit a relatively low tech one – is the bake-off. Sunlight is the best disinfectant, and testing products against competitors out in the open under the watchful eye of public scrutiny is an important part of establishing confidence and benchmarking. As demonstrated by the list of popular products to the left, vulnerabilities are everywhere, and you cannot pretend to be immune to them. Those that take vulnerabilities head-on have the intellectual high ground to ask if similar flaws exist in competitors' products.

Got Bugs?

In a similar vein as bake-offs, we have written many times before about the value of bug bounties and their effectiveness. The primary difference is that while bake-offs are best for underlying components, bug bounties can help identify weaknesses that result from the combination of secure components in a system. To mitigate the potentially significant cost to initiate bug bounty efforts, many firms are turning to outsourced platforms to manage their programs and responsible disclosures. From humble beginnings at emerging players, these platforms are now used by tech giants including Adobe, Twitter, SurveyMonkey, and Uber to manage "white hat" freelance programs. By outsourcing bug bounties, companies get trusted third-party submissions and payout management, with better results and lower total cost of ownership.

HAL 9000

This year at DEF CON 24, DARPA conducted its first ever Cyber Grand Challenge. This pitted seven teams against each other in a fully autonomous Cyber Capture The Flag (CTF) event. A CTF typically consists of teams hosting services (think email or a website), while analyzing these services for security flaws. When exploits are created, teams use them to attack others while inoculating themselves. This year, teams demonstrated that computers could discover novel exploits, as well as weaponize them into attacks and defenses, without a human in the loop. Perhaps more concerning than the *2001: A Space Odyssey* sound of robot-controlled Computer Network Defense/Operations is that only two traditional defense contractors participated in the challenge, with neither faring well. There is room for industry to help mitigate IoT security flaws, but the cost to play requires exceptional tech prowess and a whimsical spirit.

1751 Pinnacle Drive
McLean, VA 22102
wolfdenassociates.com

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

Ian K.
(571) 253-2522
Ian@wolfdenassociates.com

Will K.
(404) 939-7364
Will@wolfdenassociates.com