Homeland Security

TLP:GREEN

Big Expensive Problems in Cheap Little Things

Tom Millar
Technical Advisor
US Department of Homeland Security

Osaka 2018 FIRST Technical Colloquium
March 15, 2018

Disclaimer

This presentation is intended for informational and discussion purposes only.

The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

The display of the DHS official seal or other DHS visual identities, including the US-CERT or ICS-CERT name or logo shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security, including US-CERT and ICS-CERT. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS, US-CERT, ICS-CERT or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

DHS does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

What if Internet, but of Things?

Estimated size of the market for Smart Homes in North America by 2021:

$27 Billion[1]

Scale comparison:

Brig. Gen. Gregory Gutterman, who leads the directorate that handles FMS sales to 109 foreign allies as part of the Air Force Lifecycle Management Center at Wright-Patterson Air Force Base, said the service usually sells between around $9 billion to $10 billion on average per year.

"Twenty-seven billion, that's a great number," he told National Defense Dec. 15. "If you look at the Fortune 500, McDonald's sold $24 billion worth of hamburgers last year, and we brought in $27 billion worth of military revenue."[2]

1. https://www.statista.com/statistics/296113/north-america-smart-home-market-revenue/
2. http://www.nationaldefensemagazine.org/articles/2017/12/18/air-force-reaps-high-returns-from-fms-improvements

TLP:GREEN

Some Things on the Internet

- Home cricket scoreboards[1]
- Pharmaceutical storage refrigeration monitors[2]
- Home hockey goal lights[3]
- Fluid level alarms for sump, sewage and effluent pump systems[4]
- Home door locks[5]
- Gymnasium treadmills[6]
- Sous-vide machines[7]
- Gas & Electric[8]
- Your Children[9]
- Their School Bus[10]
- Osaka Castle

1. http://www.buzzproducts.com/design/agency/victoria-bitter-live-cricket-scoreboard.html
2. http://www.thermodata.us/hardware
3. https://shop.budweiser.ca/products/red-light
4. http://www.libertypumps.com/Product/ALM-2-Eye
5. https://lockitron.com/
6. http://www.cybexintl.com/technology/cybex-care-asset-management.aspx
7. https://www.cookmellow.com/
8. https://devicelynk.com/
9. https://www.shodan.io/search?query=Minecraft+Server+port%3A25565
10. https://blog.particle.io/2018/01/04/safetransporter_case_study/

Old and bad ideas

CWE-798: The software contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.[1]

- Hughes Network Systems Broadband Global Area Network (BGAN) satellite terminal firmware contains multiple vulnerabilities[2]
- Iridium Pilot and OpenPort contain multiple vulnerabilities[3]

1. https://cwe.mitre.org/data/definitions/798.html
2. https://www.kb.cert.org/vuls/id/250358
3. https://www.kb.cert.org/vuls/id/578598

Lots of old and bad ideas, everywhere[1]

- "54% (7 of 13) of tested routers are vulnerable to cross-site request forgery (CSRF), which can be used in tandem with default or hard-coded credentials to remotely alter router settings by loading a specially crafted website. Proofs of concept, found in Appendix C of this report, demonstrate this forced alteration by changing the Domain Name System (DNS) server settings and enabling remote management, although all settings controllable over the web-management interface can be manipulated.
- 85% (11 of 13) of tested routers use non-unique default credentials. All of the routers found to be vulnerable to CSRF have common default credentials.
- 64% (7 of 11) of tested routers are vulnerable to DNS spoofing attacks due to the use of insufficiently random source ports and/or transaction IDs (TXIDs) in DNS queries.
- 100% (11 of 11) of router firmware analyzed use BusyBox versions from 2011 or earlier and embedded Linux kernel versions from 2010 or earlier."

1. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_502618.pdf

Testing procedures don't scale well

"The analysis process developed and used in this work can be a largely manual process. While there is some opportunity for automation, certain tasks are time consuming and inefficient, even using state-of-the-art tools. A full User Datagram Protocol (UDP) port scan, for instance, frequently takes more than 19 hours to complete. Further, any time serial interfacing is required, there must be an analyst available with the proper tools, time, and expertise to carry out the research."[1]

1. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_502618.pdf

Shrug

“Ultimately, the CERT/CC attempted to coordinate with ten vendors. Of these, four eventually produced fixes and six did not. Five of the no-fix vendors were completely unreachable.

...The case of the Belkin N600 (F9K1102 v2) is unfortunately typical of router vendors. Despite having a known security contact, the vendor did not respond to our report and subsequent requests for updates. Even after reaching out to another contact in the company who explicitly looped in the appropriate security contact for network devices, the coordination effort made no headway. The threat of disclosure was met with continued silence, and on August 31, 2015, VU#201168 was published.”[1]

Five of the no-fix vendors were completely unreachable.

1. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_502618.pdf

Certification standards are finally here

UL 2900-1: Standard for Software Cybersecurity for Network-Connectable Products, was published as a national standard for the US and Canada in July 2017. It details:

a) Requirements regarding the software developer (vendor or other supply chain member) risk management process for their product.
b) Methods by which a product shall be evaluated and tested for the presence of vulnerabilities, software weaknesses and malware.
c) Requirements regarding the presence of security risk controls in the architecture and design of a product.[1]

Recognized by the US Food & Drug Administration in August, 2017[2]

1. https://standardscatalog.ul.com/standards/en/standard_2900-1_1
2. https://www.gpo.gov/fdsys/pkg/FR-2017-08-21/html/2017-17603.htm

Adoption is not exactly taking off

The Electric Imp Platform is the first IoT platform to be independently certified to UL 2900-2-2 (Standard for Software Cybersecurity for Network-Connectable Devices, Part 2-2: Particular Requirements for Industrial Control Systems).[1]

LG webOS 3.5 is the first smart TV platform to receive UL 2900-1 certification.[2]

That's all so far.

1. http://blog.electricimp.com/post/160731320415/what-it-means-to-be-the-worlds-first-iot-platform
2. http://www.lg.com/sg/press-release/lg-webos-3.5-security-manager-attains-cyberse-curity-assurance-program-certification

What about the things behind the Things?

Amazon's Alexa "smart speaker" started arbitrarily laughing at some of its owners earlier this month.

"To understand why this is important, think about how you might deal with a problem on a computer (or how the person who you call to deal with problems on your computer would deal with a problem on your computer). Maybe you'll run diagnostic software, or take a look at the log files or activity monitor, or try to figure out which component is buggy and install a patch for it. Maybe you just turn it off and on again.
You can do none of these things with smart speakers (save for turning it off and on). Much of this is attributable to the fact that these devices are "headless" — they operate without a screen or inputs such as a mouse and keyboard. It's very difficult to diagnose problems when you literally cannot see how the computer is processing information."[1]

Device ecosystems will probably end up being the larger issue – along with configuration management and educating end users and operators about how to deploy their Things safely.

1. http://nymag.com/selectall/2018/03/this-is-why-alexa-is-laughing-at-you.html

Another old idea

"As the Industrial Revolution began, workers naturally worried about being displaced by increasingly efficient machines. But the Luddites themselves "were totally fine with machines," says Kevin Binfield, editor of the 2004 collection Writings of the Luddites. They confined their attacks to manufacturers who used machines in what they called 'a fraudulent and deceitful manner' to get around standard labor practices. 'They just wanted machines that made high-quality goods,' says Binfield, 'and they wanted these machines to be run by workers who had gone through an apprenticeship and got paid decent wages. Those were their only concerns.'"[1]

1. https://www.smithsonianmag.com/history/what-the-luddites-really-fought-against-264412/

TLP:GREEN

Homeland Security