CERIAS

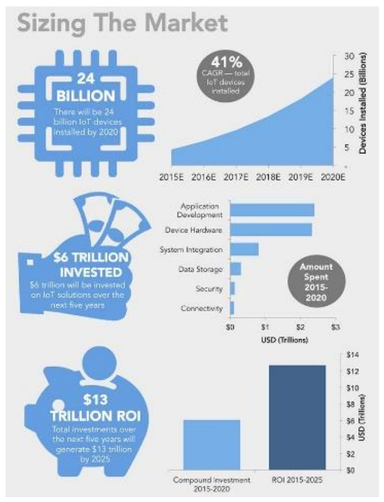
The Center for Education and Research in Information Assurance and Security

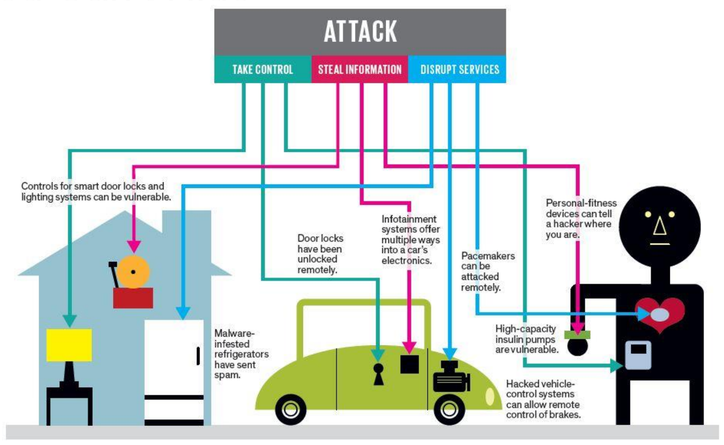
Checking, Increasing, and Confirming a Smart Home's IoT Security

E.J. Dietz, J.E. Lerums, B. Yang

1. Abstract - The Internet of Things (IoT) offers consumers the promise of future conveniences, and cost savings as their homes, appliances, entertainment systems and utilities become more interconnected. With specifications reviews and testing on a limited configuration this research focuses on what a consumer can do to ensure their smart home systems' IoT security.

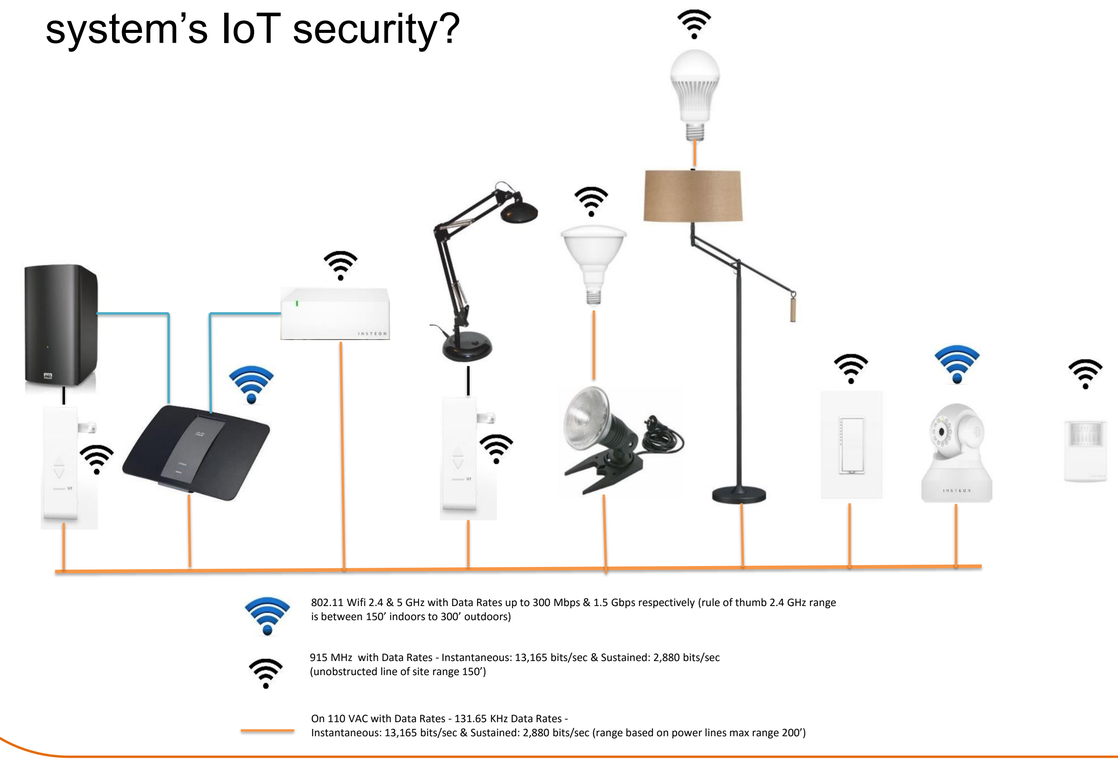
2. Motivation – IoT So Much More to Come & Even If You Run, You Can't Hide





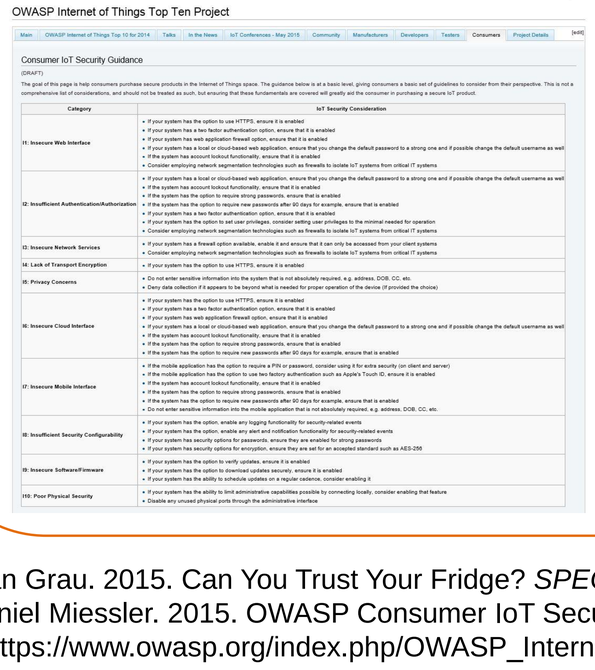
NO PLACE TO HIDE: With the Internet of Things spreading throughout our homes, cars, and even bodies, new vulnerabilities seem to emerge almost daily. The smart locks and security systems in your home could be disabled by a would-be burglar. Your car could be forced to unlock its doors and start its engines; a thief would only have to get in and drive. Implanted pacemakers and insulin pumps are also vulnerable to hacking.

3. Problem – How does a consumer ensure their smart home system's IoT security?



4. Methodology – Research for best IoT security practices and identify and test how consumers can check, improve, and confirm their smart home system's IoT security on a limited configuration.

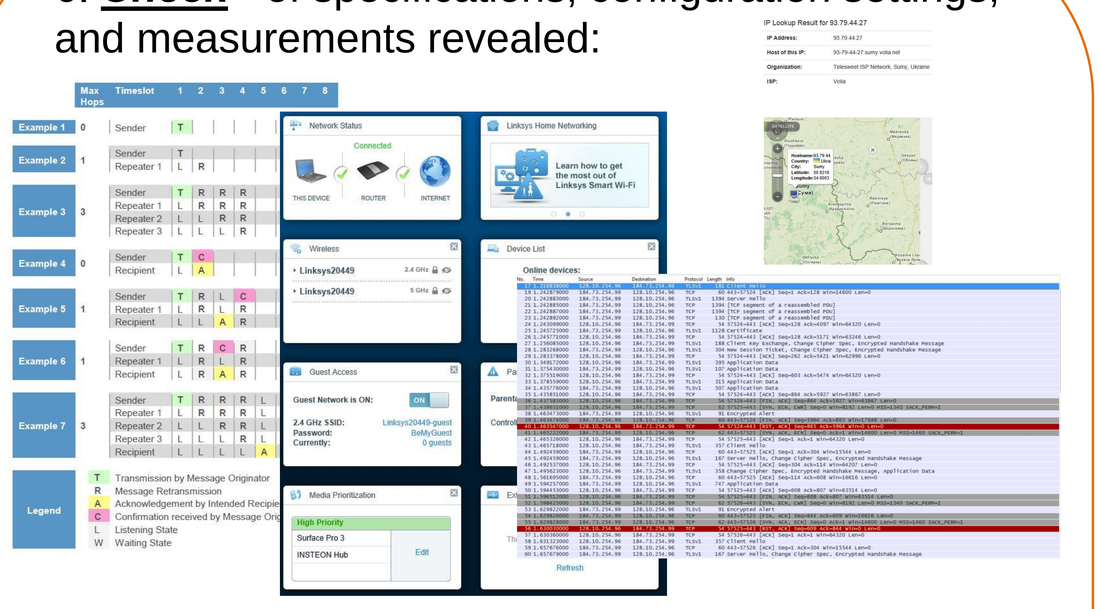
5. The Open Web Applications Security Project (OWASP) Identifies the Top Ten IoT security obstacles and solutions which require a team effort from manufacturers, developers, testers, and consumers



From the OWASP identified consumer security actions:

1. Check specifications
2. Check configuration settings
3. Check logs and network with instrumentation
4. Increase security by mitigating risks
5. Confirm improved security

6. ***Check*** - of specifications, configuration settings, and measurements revealed:



1. Local smart home device network robust and secure
2. Wifi network segmentation & disabling SSID broadcast required (to stop Ukranian port scanning)
3. Default passwords
4. Remote access secured with TLSv1 protocol

7. ***Increase*** – Enabled security settings on all devices, isolated smart home devices on one Wifi network from the PCs on the other, disabled the SSID, ensured camera not pointed at personal areas, ensured all passwords are robust and unique.

8. ***Confirm*** – Ensured all passwords changed, SSID's not broadcasting (Ukranian port scanning stopped), PCs and smart home devices on separate networks, checked router logs for unusual port activity

9. Conclusion and Future Work - To check, increase, and confirm their smart home IoT security, the most important step consumers must take is to purchase devices that incorporate the best OWASP IoT Top Ten solutions by manufacturers, designers, and testers.

The heterogeneity of the smart home/smart grid precludes a "one size fits all solution". In fact for some smart home devices a proprietary solution may be the best secure cost effective solutions if those devices are isolated via firewalled gateways from enterprise networks. The combination of IoT cyber security standardization and proprietary solutions will make smart home/smart grid security a challenge and promising research field for years to come.

Alan Grau. 2015. Can You Trust Your Fridge? *SPECTRUM.IEEE.ORG North Am.* (2015), 51–56.
Daniel Miessler. 2015. OWASP Consumer IoT Security Guidance. (2015). Retrieved May 9, 2015 from https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=Consumers

CERIAS

PURDUE UNIVERSITY