CERAS

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

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





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.





- Local smart home device network robust and secure
- 2. Wifi network segmentation & disabling SSID broadcast required (to stop Ukranian port scanning)
- Default passwords 3.
- 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.

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

DRAFT)	
The goal of this page is help consumers purchas comprehensive list of considerations, and should	e secure products in the Internet of Things space. The guidance below is at a basic level, giving consumers a basic set of guidelines to consider from their perspective. This is not a I not be treated as such, but ensuring that these fundamentals are covered will greatly aid the consumer in purchasing a secure IoT product.
Category	IoT Security Consideration
11: Insecure Web Interface	If your system has the option to use HTTPS, ensure it is enabled If your system has a two factor authentication option, ensure that it is enabled If your system has a two factor authentication option, ensure that it is enabled If your system has web application firewall option, ensure that it is enabled If your system has a local or cloud-based web application, ensure that you change the default password to a strong one and if possible change the default username as well If the system has a local or cloud-based web application, ensure that is enabled Consider employing network segmentation technologies such as firewalls to isolate IoT systems from critical IT systems
12: Insufficient Authentication/Authorization	If your system has a local or cloud-based web application, ensure that you change the default password to a strong one and if possible change the default username as well If the system has account lockout functionality, ensure that it is enabled If the system has the option to require strong passwords, ensure that is enabled If the system has the option to require new passwords after 90 days for example, ensure that is enabled If your system has a two factor authentication option, ensure that it is enabled If your system has the option to require rew passwords after 90 days for example, ensure that is enabled If your system has the option to set user privileges, consider setting user privileges to the minimal needed for operation Consider employing network segmentation technologies such as firewalls to isolate IoT systems from critical IT systems
13: Insecure Network Services	If your system has a firewall option available, enable it and ensure that it can only be accessed from your client systems Consider employing network segmentation technologies such as firewalls to isolate IoT systems from oritical IT systems
14: Lack of Transport Encryption	If your system has the option to use HTTPS, ensure it is enabled
15: Privacy Concerns	Do not enter sensitive information into the system that is not absolutely required, e.g. address, DOB, CC, etc. Deny data collection if it appears to be beyond what is needed for proper operation of the device (if provided the choice)
i6: Insecure Cloud Interface	If your system has the option to use HTTPS, ensure it is enabled If your system has a two factor authentication option, ensure that it is enabled If your system has a local or cloud-based web application, ensure that it is enabled If your system has a local or cloud-based web application, ensure that you change the default password to a strong one and if possible change the default username as well If the system has account lockout functionality, ensure that it is enabled If the system has account lockout functionality, ensure that is enabled If the system has the option to require strong passwords, ensure that is enabled If the system has the option to require new passwords after 90 days for example, ensure that is enabled
17: Insecure Mobile Interface	If the mobile application has the option to require a PIN or password, consider using it for extra security (on client and server) If the mobile application has the option to use two factory authentication such as Apple's Touch ID, ensure it is enabled If the system has account lockout functionality, ensure that it is enabled If the system has the option to require strong passwords, ensure that is enabled If the system has the option to require new passwords after 00 days for example, ensure that is enabled If on ther sensitive information into the mobile application that is not absolutely required, e.g. address, DOB, CC, etc.
18: Insufficient Security Configurability	If your system has the option, enable any logging functionality for security-related events If your system has the option, enable any alert and notification functionality for security-related events If your system has security options for passwords, ensure they are enabled for strong passwords If your system has security options for encryption, ensure they are set for an accepted standard such as AES-256
19: Insecure Software/Firmware	If your system has the option to verify updates, ensure it is enabled If your system has the option to download updates securely, ensure it is enabled If your system has the ability to schedule updates on a regular cadence, consider enabling it
110: Poor Physical Security	If your system has the ability to limit administrative capabilities possible by connecting locally, consider enabling that feature

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

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



