Protect 2014

Washington, D.C. September 8-11

The Internet of (insecure) Things

HP Bad Guy Lair staff

#HPProtect

Agenda

- Introduction
- Misconception
- The OWASP Internet of Things Top 10 Project
- The Internet of Things State of the Union report
- Takeaways
- Questions

26 billion by 2020

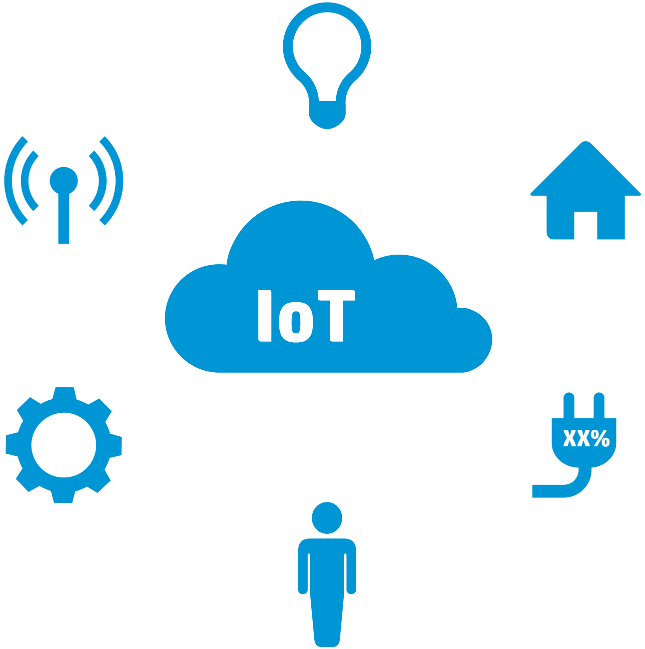
- 30 fold increase from 2009 in Internet of Things install base
- Revenue exceeding $300 billion in 2020
- $1.9 trillion in global economic impact

*Gartner Internet of Things Report 2013

Misconception

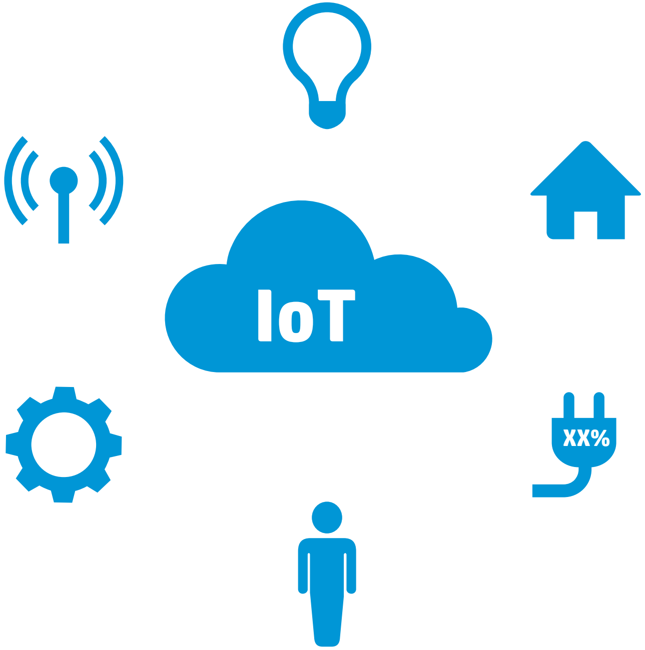
Misconception: It’s all about the device and internet

- It’s not just about the device, or the network, or the clients
- There are **many** surface areas involved
- Each of these need to be evaluated



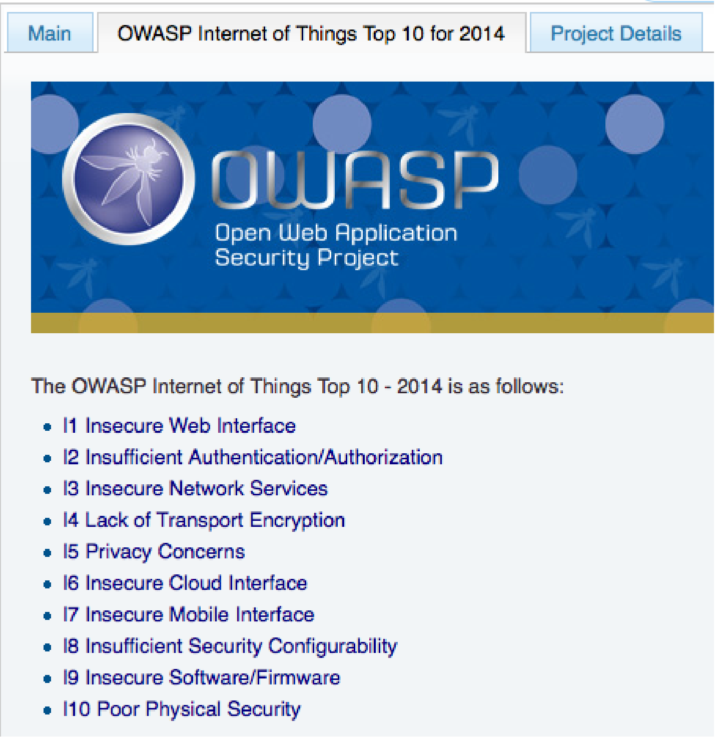
Considerations: A holistic approach is required

- All elements need to be considered
  - The Internet of Things device
  - The cloud
  - The mobile application
  - The network interfaces
  - The software
  - Use of encryption
  - Use of authentication
  - Physical security
  - USB ports
- Enter the OWASP Internet of Things Top Ten Project



OWASP Internet of Things Top Ten Project

Internet of Things Top Ten Project: A complete IoT review


Main
OWASP Internet of Things Top 10 for 2014
Project Details
OWASP
Open Web Application Security Project

The OWASP Internet of Things Top 10 - 2014 is as follows:

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

- Review all aspects of Internet of Things
- Top Ten categories
- Covers the entire device
- Without comprehensive coverage like this, it would be like getting your physical but only checking one arm
- We must cover all surface area to get a good assessment of overall security

The Internet of Things State of the Union report

State of the Union: Devices tested

- Tested 10 devices from various Internet of Things areas
- TVs, webcams, home thermostats, remote power outlets, sprinkler controllers, hubs for controlling multiple devices, door locks, home alarms, scales and garage door openers
- Tested using the OWASP Internet of Things Top Ten Project which includes assessments of all primary surface areas

State of the Union: Common areas of concern

- Privacy
- Authorization/authentication
- Transport encryption
- Web interface
- Software/firmware

Six out of 10

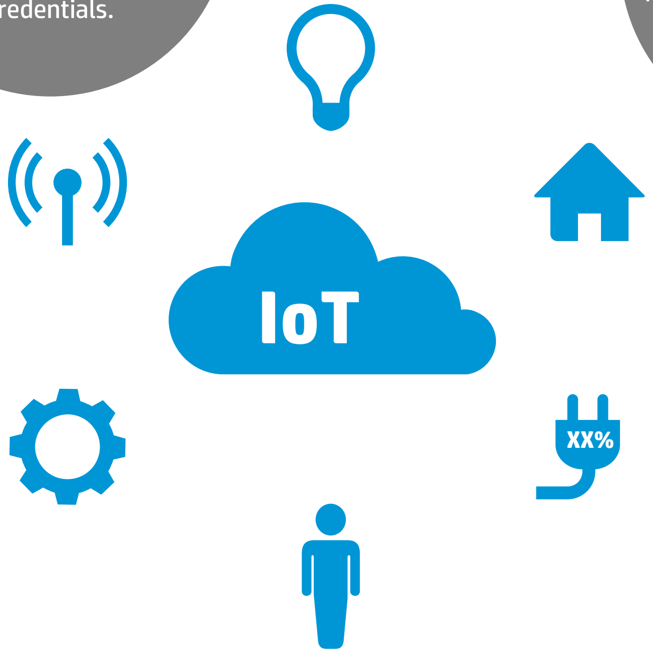
devices that provide user interfaces were vulnerable to a range of issues such as persistent XSS and weak credentials.

90%

of devices collected at least one piece of personal information via the device, the cloud or its mobile application.

80%

of devices along with their cloud and mobile application components failed to require passwords of a sufficient complexity and length.



70%

of devices used unencrypted network services.

70%

of devices along with their cloud and mobile application enabled an attacker to identify valid user accounts through account enumeration.

Takeaways

Takeaways: Exciting time for Internet of Things

- Manufacturers want their devices to be connected
- Consumers want their devices to be connected
- Connected devices have many benefits to offer

Takeaways: Dangerous time for Internet of Things

- Current security is one dimensional focusing only on one element of Internet of Things security
- Each new connected device brings along it’s own set of vulnerabilities
- Attackers will benefit in two ways: 1) getting closer to your data by being on your network, and 2) gaining a foothold to launch attacks against others

Takeaways: There is hope

- The Internet of Things is early in its life
- Security reviews using the OWASP Top Ten Project can detect vulnerabilities for all aspects of Internet of Things
- It’s more important than ever to bake in security and maintain security throughout the product lifecycle
- The OWASP Internet of Things Top Ten Project is here to help (contributions and suggestions are welcome)

Takeaways: Let us help

HP Fortify on Demand

- Cloud-based application security testing
- Both static and dynamic testing, using automated and manual techniques
- Integrates with your SDLC and build environment to provide critical security checkpoint
- Single portal for code uploads and reviewing results
- Announcing The Fortify on Demand Internet of Things Testing Practice (testing, database of devices tested)

HP Fortify
Assessed ☑

For more information

Visit these demos

- Hacking the Internet of Things, DEMO3544
- HP Fortify

After the event

- Visit www.hp.com/go/fortify
- Download whitepaper and reports:

HP Internet of Things Blog and Research Study

OWASP Internet of Things Top 10

Your feedback is important to us.
Please take a few minutes to complete the session survey.

Please give me your feedback

Session BGL3620 **Speaker** HP Bad Guy Lair staff

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.

Thank you

Make it matter.