The Security of the Internet of Things

Alex Bauert

Zoa Buske

Nathan Larson

OWASP
Open Web Application
Security Project

About the speakers

Alex Bauert has been working on App Sec for over 15 years in various roles. He has participated in OWASP for 10 yrs and spoken at several OWASP events.

Zoa Buske was a Software Engineer for over 20 years, during which she was a Security advocate in all things. She moved to InfoSec and AppSec a year and a half ago. She has been a local OWASP member since 2013 and has recently joined the leadership team.

Nathan Larson wrote vulnerable software for two decades before wandering into an OWASP talk and catching the security bug. His favorite AppSec defect is *H. sapiens*.

OWASP
Open Web Application
Security Project

Agenda

- Expectations
- IoT and Security Landscape
- Comparing IoT to legacy defects
- Security - commercial vs commodity
- The OWASP IoT Top 10
- How we can prevent breaches
- Discussion

Ground Rules and Expectations

- Interactive
- Share the knowledge/experience
- Presenting base info and topics
- Did we mention Interactive?
- No Silver Bullets in the presentation

OWASP
Open Web Application
Security Project

1982 - Carnegie Mellon University

> “Convenience and ‘magic’ will overwhelm concerns. The history of technology is clear on this front – ATMs, e-commerce, credit cards, the list is endless.”

— Sunil Paul

Tech entrepreneur and investor

OWASP
Open Web Application
Security Project

IoT and Security Landscape

How did this happen?

- ...of Things - on the web estimate of beginnings in 2008-9
- Kevin Ashton - coined the term in 1999 in describing “ubiquitous” sensors (RFID)
- Where else do we use “sensors” and devices via the Internet
    - Utilities
    - Agriculture
    - Industrial use
    - Everywhere else - commoditization
    - ALL of the Things
- Does everything need to be internet accessible?

How much trouble are we in?

- Evolution of sensors and single/limited function tech
  - Like everywhere else security was not there at first
- It’s a client
- Cheap solutions for consumer market
  - FOSS
  - Limited hardware/software capabilities
  - Adding computing because everybody else
  - What need was ‘solutioned’?
  - Convenience
- SMART everything - maybe not so smart?

Fighting Perception

- Outside of the Perimeter
    - Our tools don’t reach there
- It’s just a sensor
- Sending data back
    - It’s not financial or PII
- Receiving the data from our device
    - It’s our device of course we trust it
- Who would do that?

Comparing IoT to legacy defects

Insecurity Redux

OWASP
Open Web Application
Security Project

Desktop software defects

- Ease of reverse engineering
- Memory mishandling
  - Buffer overflows
  - Use after free
- Remote code execution
- Authentication
- Authorization
- Vulnerable components

Web application defects

- Injection: SQL, command, etc.
- Input validation
- Deserialization
- Poor encryption
- Data exposure
- Authentication
- Authorization
- Vulnerable components

Mobile app defects

- Ease of reverse engineering
- Input validation
- Deserialization
- Poor encryption
- Data exposure
- Authentication
- Authorization
- Vulnerable components

IoT device defects

- Default passwords (defpass.com)
- Default settings
- Insecure / unneeded services
- Insecure base OS
- Difficulty in patching
- No physical hardening

IoT device defects (Vol. 2)

- Ease of reverse engineering
- Poor encryption
- Insecure interfaces
- Authentication
- Authorization
- Vulnerable components

Security - commercial vs commodity

What’s on the internet?

OWASP
Open Web Application
Security Project

Do we do it differently

- We should
  - Threat cases are different
- Gas meter
  - What should we care about and impact
- Fridge
  - What should we care about and impact
- Fill level meter
  - What should we care about and impact

Can we say threat model?

OWASP
Open Web Application
Security Project

The OWASP IoT Top 10

OWASP
Open Web Application
Security Project

The OWASP IoT Top 10 2014

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

The OWASP IoT Top 10 2018

1. Weak Guessable, or Hardcoded Passwords
2. Insecure Network Services
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanism
5. Use of Insecure or Outdated Components
6. Insufficient Privacy Protection
7. Insecure Data Transfer and Storage
8. Lack of Device Management
9. Insecure Default Settings
10. Lack of Physical Hardening

OWASP
Open Web Application
Security Project

Weak Guessable, or Hardcoded Passwords

- Most IoT devices come with default passwords
  - They either aren’t changed
  - They are embedded and can’t be changed
  - There are diagnostic backdoors that expect the defaults

Insecure Network Services

- Network security tools, like firewalls, scanning, IDS are also important for IoT
- Ensure secure connections
- Close unneeded ports
- Disable remote access (or secure it)
- Put the IoT devices on their own network
- Keep the devices up to date

Insecure Ecosystem Interfaces

- All interfaces should be secured with authentication and authorization
- All traffic should be encrypted using a good algorithm
- Filter input and output to all interfaces

OWASP
Open Web Application Security Project

Lack of Secure Update Mechanism

- Device should provide firmware validation
- There should be a rollback mechanism
- There should be notifications of security changes due to updates
- All updates should be encrypted using a good algorithm

Use of Insecure or Outdated Components

- Ensure all software is up to date and secure
- This includes all third-party software
- This includes all customization of OS or other components
    - If you customize you need a path to port that to any needed updates

OWASP
Open Web Application
Security Project

Insufficient Privacy Protection

- User data may be stored on the device. It needs to be protected by
  - Properly securing it
  - Using for appropriate use cases
  - Having permission to use it

Insecure Data Transfer and Storage

- Data must be properly encrypted
- Access controls must be in place
- This is true for when the data is
  - at rest
  - in transit
  - being processed

Lack of Device Management

- For all devices in production provide
  - asset management
  - update management
  - secure decommissioning
  - systems monitoring
  - response capabilities

Insecure Default Settings

- Devices should be shipped with secure defaults
- Configuration changes that improve security should be available.
- Settings should not be fixed if they are not set securely

Lack of Physical Hardening

- Use a secure boot process
- Disable or remove debug ports (or at least secure them)
- Make it difficult to remove memory or drives and read them

How we can prevent breaches

Root causes

- Development pace driven by the market
- Insufficient training
- Immature security testing
- “No one would think of this” mentality
- Insufficient threat modeling

Network Segmentation

- Information Technology
  In every department
  - Data
  - Employees
  - Customers

- Operational Technology
  In specific areas
  - Control
  - Sensors
  - Robotics

Authentication/Authorization

- Many devices have limited control
  - Default “all access” account
  - Default easy-to-find password
    - Force installer to change on first login
  - Replace amateurish web app interfaces

Secure Firmware and Hardware

- Many devices do not protect either
  - Use SecureBoot
  - Disallow flashing arbitrary code to device
  - Disable development interfaces
    - JTAG
    - UART
  - Encrypt stored secrets

Insecure Components

- Use up-to-date, secure libraries
- Notify customers when updates available
- Automate firmware updates

Discussion

References

https://www.digitalocean.com/community/tutorials/what-is-immutable-infrastructure
https://dzone.com/articles/infrastructure-as-code-security
https://thenewstack.io/new-security-challenges-with-infrastructure-as-code-and-immutable-infrastructure/
https://blog.sensu.io/infrastructure-as-code-testing-and-monitoring

https://geekflare.com/iac-security-scanner/

https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project