RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SBX1-W3

Yet Another IoT Hack

Joshua Meyer

Associate Security Analyst
Independent Security Evaluators
@ISEsecurity

Yet Another IoT Hack

- Introduction
- Threat modeling
- Using prebuilt tools
- Types of attacks
- Exploiting Issues
- What to do next

IoT and (In)Security

- Well documented history of IoT security failure
- More devices every year
- Vulnerabilities can be trivial to exploit

Meet Our Assistant

TerraMaster F2-420

- Network-Attached Storage (NAS)
- Quad-core Intel Celeron J1900
- 4GB RAM
- 2 x 3.5” HDD bays
- 2 x 1Gbps Ethernet ports
- TOS 3.1.03

Threat Modeling

- Internal threats
  - Attackers on the local network
- External threats
  - Attackers not on the local network
- Authentication
  - Can attackers exploit a device without credentials?

Prebuilt Tools and Exploits

- Allow for easy deployment of exploits
- Caveats
  - Tend to rely on known exploits that may be patched
  - Not really finding new vulnerabilities
- Can be very helpful in attacking IoT devices

Common Attacks—Cross-Site Scripting

What is it?

- Cross-Site Scripting (XSS)
  - Vulnerability that allows attackers to run code in a victim's web browser
- Attack Points
  - Input fields
  - URL and POST parameters
  - Impact:

Impact

- Credential theft
- Phishing
- Sensitive data exposure

Common Attacks—SQL Injection

What is it?

- SQL injection
  - Execution of arbitrary SQL queries in a database
- Attack Points
  - Input a database might handle
  - Search features

Impact

- Information disclosure
- Denial-of-service
- Modification of stored data

Common Attacks—Command Injection

What is it?

- Command Injection
  - An attack that executes operating system commands
- Attack Points
  - Input that might be handled by the operating system
    - Filenames
    - Usernames and passwords

Impact

- Denial-of-service
- Information disclosure
- Credential theft
- Game over?

RSAConference2019

Demo Time

What's Next?

Manufacturers and Developers

- Short-term
  - Use audited components when available
  - Consider security throughout the development process
- Long-term
  - Security training
  - Talk to a professional
  - Third-party security assessment

Users

- Short-term
  - Secure your devices
    - Disable extraneous services
    - Disable remote access
    - Update firmware
- Long-term
  - Request better device security from manufacturers
  - Perform security audits regularly