# Smart Home Security Challenges

Marc Schneider

MITRE





## What is a Smart Home?

- **A system that combines services and devices which sense and interact with the environment to improve the quality of life in the home.**
  - These services and devices are frequently called the Internet of Things (IoT)
  - Convenience
  - Efficiency
  - Security
- **It is a home where the systems interact to provide more than can be achieved without interaction.**
  - For example, a thermostat, air conditioning, and ceiling fan working together to cool the home in the most energy efficient manner.



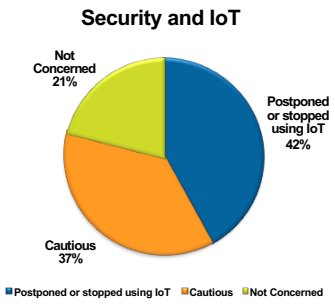
MITRE



## Security and Smart Home IoT

- **Security and privacy concerns are significant barriers to adoption of this technology.**
  - In a recent study[1], 47% of all surveyed cited "privacy risk/security concerns" as a barrier to adoption.
  - These concerns are even higher in the ASEAN region, for example, 60% of Indonesians cited "privacy risk/security concerns" as a barrier to adoption.

[1]Igniting Growth in Consumer Technology – Accenture, https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf






MITRE



## IoT Device Security Challenges

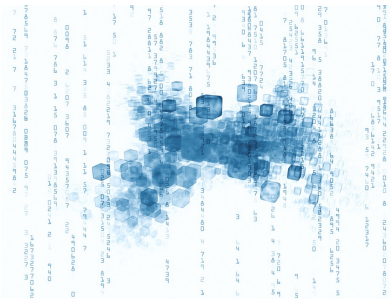
- **Device Constraints**
  - Size, weight, power, and storage
- **Lack of Market Incentives**
  - Low cost
  - Increased functionality
  - Short time to market
- **Lack of a Security Culture**
- **Lack of Standards**
  - Including interoperability
- **Monoculture of Subsystems**
- **Missing Security Functions**
  - Audit
  - Weak or non-existent cryptography
  - Patching
  - Security testing
- **Poor Practices**
  - Lack of certificate pinning, validation, and revocation status checks
  - Hardcoded passwords & keys
  - Security through obscurity



MITRE

## Smart Homes: A System of Systems

- **Smart homes are often assembled piecemeal and ad-hoc**
  - Multiple vendors, complex interactions
- **Vulnerabilities emerge from the interactions between components**
- **Impossible to test all interactions**
  - Balkanization of smart home ecosystems
  - Specialty devices and services to bridge the ecosystems



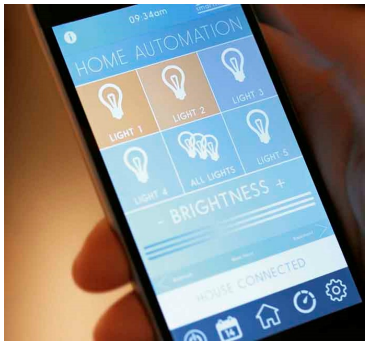


MITRE



## Security Analysis of IoT Systems

- **Risk Analysis**
  - What are the threats
  - What needs protecting
- **Vulnerability Analysis**
  - Many tools for IT vulnerability analysis are of limited use
  - Hardware and software are often much more closely tied than in traditional IT
  - Wireless networking predominates
    - Wi-Fi and other protocols






MITRE



## Example: Vulnerability Analysis of a Light Bulb

**What needs protecting on a light bulb?**
- Passwords, cryptographic keys, etc.

- **Hardware**
  - Understanding hardware helps to understand the attack surface
- **Software**
  - Understanding the OS and other software allows the analyst to check for common vulnerabilities and exposures
    - Example: Using an outdated version of OpenSSL.
- **Wireless**
  - Understand how the device connects to the home network and other devices
    - Wi-Fi, 6LoWPAN, proprietary
- **Network**
  - What network services are available?
  - What protocols does the device use?
    - Example: Universal Plug and Play (UPnP)

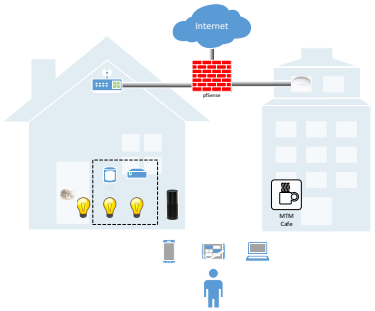


MITRE



## MITRE's Consumer Internet of Things Initiative Lab

- **Researching how to mitigate threats, vulnerabilities, and attacks unique to IoT using consumer IoT devices as a research platform**
- **Smart Home Project**
  - What are the cybersecurity challenges?
  - What can consumers do to address these challenges?
  - What do manufactures need to change to overcome these challenges?

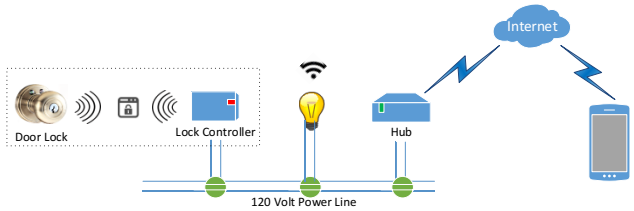





MITRE

## Example: Replay in a System of Systems

- **Defeating replay resistance in a smart door lock**
  - Multiple vendors products involved in smart home system
- **Setup**
  - Record radio signals emitted by smart lightbulb while locking/unlock door via cellphone



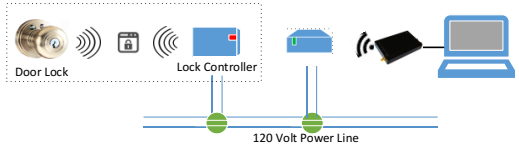



MITRE



## Example: Replay in a System of Systems

- **Replay radio signals for lock and unlock**
  - Bypassed replay resistance of door lock



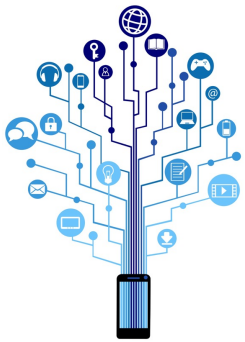



MITRE



## Addressing Smart Home IoT Challenges

- **Existing Devices and System**
  - Patch or reconfigure when possible
  - Use external compensating controls when possible
- **Future Systems**
  - Security needs to be considered a feature and designed into products
  - Systems must be resilient
    - Systems will always have vulnerabilities
    - Smart homes may appear resilient, but actually have common failure modes





MITRE



## IoT Device Security as a Feature

- **Create market incentives for security**
  - Consumers of smart home IoT need to ask for security
  - Independent third parties need to provide expertise
- **Standards need to be simple**
  - Compliance checking should be automatable
  - Easy to implement



MITRE

## Initiatives, Frameworks, and Standards

- **Online Trust Alliance**
  - IoT Trust Framework and Working Group
- **European Union Agency for Network and Information Security**
  - Threat Landscape and Good Practice Guide for Smart Home and Converged Media
  - Security and Resilience of Smart Home Environments
- **Trusted Computing Group**
  - Internet of Things Work Group
- **Industrial Internet Consortium**
  - Security Working Group
- **Cloud Security Alliance**
  - Mobile Working Group – IoT Initiative
- **OWASP**
  - Internet of Things Project
- **IEEE**
  - Standard 802.15.4
  - P2413 Working Group
  - IoT Technical Community
- **NIST**
  - Cyber Physical Systems Framework
- **ITU-T Y.2060**


Approved for Public Release; Distribution Unlimited. Case Number 16-3338
MITRE



## Questions?

MITRE
Approved for Public Release; Distribution Unlimited. Case Number 16-3338