Smart Home

Gyandeep Reddy Vulupala

Agenda

- Smart Home
- Applications
- Attacks on Smart Home
- Security Services
- End User Concerns
- Solutions
- Conclusion

What is Smart Home

Smart devices integrated in home environment

Comfort and strengthen the feeling of safety

Automation, enhanced monitoring, and reduced energy consumption

Examples

- Google Nest Thermostat (Heating and Cooling Systems)
- Philips Hue (Lighting)
- Yale Assure Lock (Door Locks)

Smart Devices

Constrained Devices

- Limited power, memory, processing resources
- Smart bulbs, smart meters, sensors

Powerful Devices

- Powered by main supply
- Enough computational power, memory, and communication interfaces
- Home gateway, TV sets

Home Area Network (HAN)

High Speed Networks (Wi-Fi) and Personal Area Networks or Ad Hoc Networks

Powerful devices: own built-in web server

Constrained devices: web browser or smartphone application

Wide Area Networks (WAN): Internet Service Provider (ISP), Mobile Network Operator (MNO), Low-Power Wide Area Networks (LPWAN)

Applications

Energy Efficiency	E-health	Multimedia	Surveillance & Security
• Introduce event-based energy saving	• Monitor physical health • Reduce clinic-based assessment and labor-intensive procedures	• Connect various families of smart devices to provide entertainment for all • TV sets, set top boxes, media centers, game consoles	• Intrusion event detection

Security Problems or Risks

Heterogeneous environment with different vendors

Unrestricted interconnection

A single compromised device can provide access to other devices

Users overwhelmed with configuring their network

Unclear what permissions a specific device should have

Blindly trust devices connected to home network

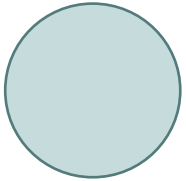
Interfaced with remote infrastructure

Security Threats

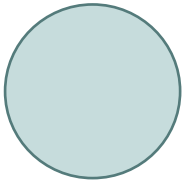
Privacy / Security	• Nefarious Activity • Eavesdropping / Interception • Loss of confidentiality
Physical Attacks	• Device manipulation • New firmware upload, changing device settings, extracting encryption keys
Disasters and Outages	• Denial of Service
Damage / Loss	• Remove vulnerable data from unused devices

Attacks on Smart Home

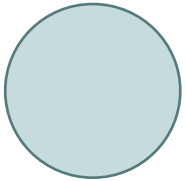
Real World



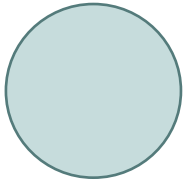
Intercept, impersonate, and disable devices communicating with Z-wave



Extract secret key from Z-wave packet exchange



Security loopholes in cryptographic libraries



Compromised home automation controllers and took control over door locks and alarm systems

Real World

- Glitch in Nest Thermostat lowered home temperatures
- Recent reports suggest smart TVs can be used to record conversations
- Baby Monitor was hacked
- Mirai malware compromised devices and created a botnet, disrupting the internet for millions of people

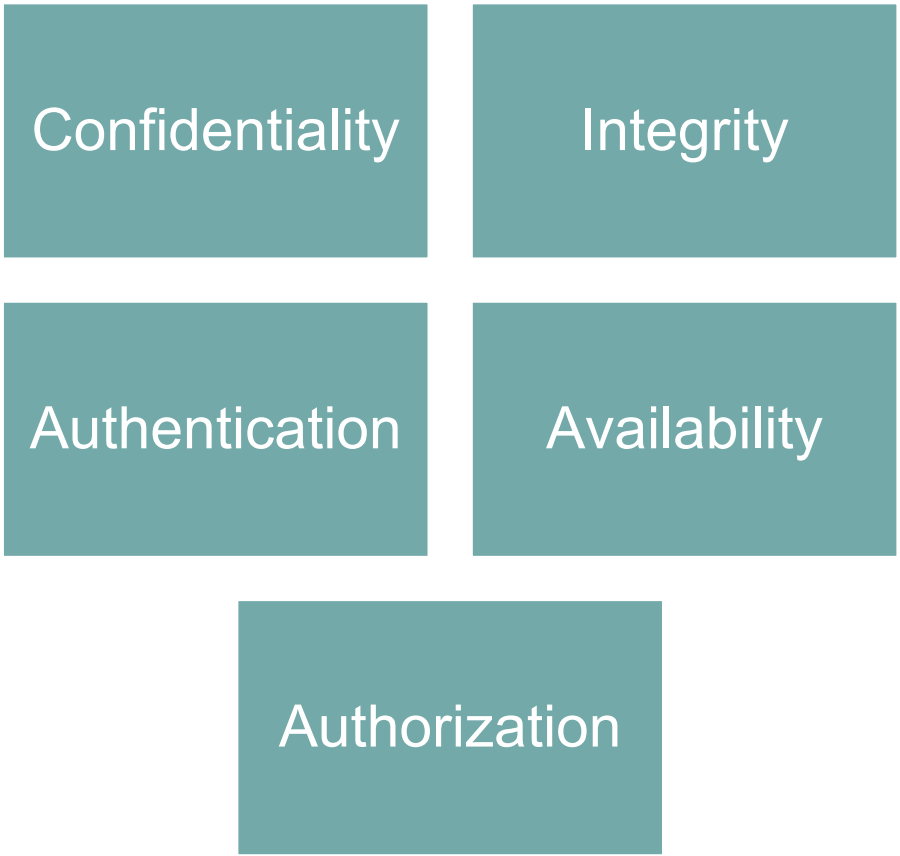
Mirai Malware

Link: https://www.youtube.com/watch?v=Ki-Yo7OS-yU. End at 1:21

Hypothetical

- User buys an IP camera to monitor driveway
- Connects to home Wi-Fi
- Remote access, automatically and unknowing to user, opens a port in the firewall
- Globally reachable and current firmware has security flaws
- Attacker gains access to IP camera from outside
- Malware scans the network for other vulnerable devices
- Infected devices expose private information and contribute to DDoS
- Firewall blocks unauthorized traffic from outside
- No measures to prevent attacks originating from infected device

Security Services


Confidentiality
Integrity
Authentication
Availability
Authorization

Confidentiality / Privacy

Exchanged user data is protected

Encryption Keys

- Resource consumption and efficient distribution
- Static Key Management
- Dynamic Key Management

AES for encryption of data transport, RSA for public key encryption, and digital signatures

Rabin’s Scheme, NtruEncrypt, Elliptic Curve Cryptography (ECC)

- Consume limited physical resources
- Satisfactory transmission effectiveness

Elliptic Curve Cryptography (ECC) for IoT devices

- Reduce processing and communication overhead

Integrity

Content digest calculation

- Hashing algorithms (SHA-2 family)
- If secret key involved:
  - Keyed-Hashing Function for Message Authentication (HMAC)
  - Cipher Based Message Authentication Code (CMAC)

Data trustworthiness based on historical data

- Reported result is close to aggregated value

Cumulative sum test

- Characteristics of data distributions at random times
- Quick intrusion detection
- Minimum number of observations
- Detect attack with high probability

Intrusion Detection System (IDS)

Intrusion Prevention System (IPS)

Authentication and Non-Repudiation

CMAC (MAC based on block ciphers)

- Guarantee non-repudiation of data in EnOcean network

Digital Signatures to protect raw data

- JSON (JavaScript Object Notation) structure became popular in the IoT domain
- JSON Web Signature (JWS) signs the JSON to ensure content security with digital signatures or MACs

Availability

Physical Protection

- Tamper resistance to resist sensitive information extraction

Access Control

- Wireless connection instability
- Short term wireless connection outages

Latest mechanisms through updates

Authorization

Restricts internal and external communication to only deliver intended functionality

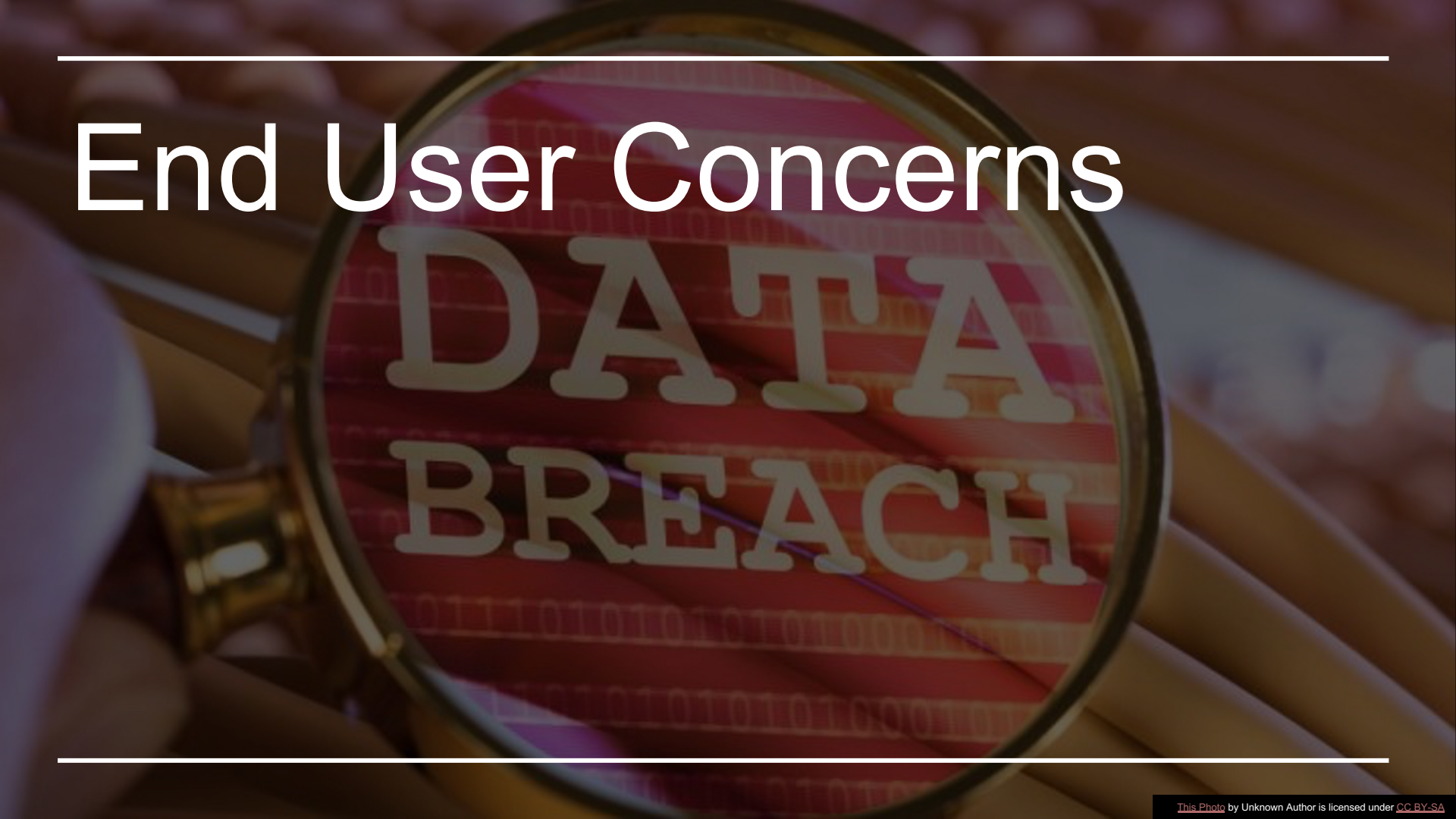
Access Control Lists

- CPU requirements too high
- No solutions implemented using this technique

Fuzzy identity-based encryption

- Differentiate access rights
- Apply assigned rules to protect data transmission

End User Concerns



Participants

15 participants

- 4 women
- 8 had no background in IT
- 2 were aged 55 or older

Use cases

- Physical safety
- Home automation
- Remote control
- In-home sensing

Most common devices

- Smart lights
- Thermostat
- Cameras
- Switches

Smart home interactions

- Smartphone app
- Contextual Triggers
- Amazon Echo or Google Home
- Motion Sensors

Threat Models

Physical Security

- People who used security cameras or other security systems

Audio or Behavior Logs

- Privacy, but half the participants were not concerned

Bandwidth, money, or personally-identifiable information (PII)

- Accidentally watered the lawn for a week and led to significant water bill

No mention of device availability as an asset that can be attacked

Threat Models (Cont.)

Adversaries

- Companies that manufactured the smart devices
  - Not irresponsible about privacy and security
- Government
  - Murder case requesting audio data from an Echo device

App Developers

- Not concerned
- Security experts mention app developers as adversaries

More technical: network attacks and network mapping

Less technical: weak passwords and unsecured Wi-Fi networks

Lack of Concern for Privacy

- Trust in companies handling user data
- Not a worthwhile target (DDoS)
- Nothing to hide
- Secure their systems by using strong passwords
- Tradeoff: security or privacy risks in exchange for functionality and convenience

Multi-User Interactions

- Incidental users
  - Less awareness of security / privacy concerns
  - Do not always have full access
  - Restricted access
  - Audio / Video Surveillance
  - Behavioral Surveillance

Non-Security and Privacy Concerns

Reliability

- Devices function as normal in the case of no internet connection
- Example: wall switches

Interoperability

- Devices compatible with smart home system
- Echo / Google Home or centralized app
- Third party apps to make devices interoperable

Cost

- Barrier to adoption
- A participant created their own smart sprinkler

Solutions

In-Network Approach

Restrict communication to just deliver desired functionality

Firewall protects unauthorized access from outside

No security mechanisms to prevent devices attacking inside the network

Unauthorized connections from home to other networks blocked

Different from intrusion detection

- Explicit permission vs generously allowing all traffic

Specification of Network Compliant Behavior

Minimum communication

Achieved through communication rules

- IP addresses
- Port numbers
- Packet sizes
- Packet interarrival times
- Number of parallel connections
- Consumed bandwidth

Communication rules provided by manufacturer

Certification agency or open-source for communication rules

Specification of Network Compliant Behavior

Observe new device communication during learning phase

- Apply default set of rules
- Not allowed to open connection to another device or server
- User explicitly grants permission

Rules installed at home router

Traffic Filtering

Software Defined Networks (SDN) and flexible packet matching

Communication rules converted to flow table entries for forwarding tables

Flexibility of SDN allows to dynamically adapt communication rules

De facto protocol for SDN deployments is OpenFlow

- Inflexible packet matching based on hard-coded header fields

Traffic Filtering

Programming Protocol-Independent Packet Processors (P4)

- Specifies the behavior of a network switch
- Specify communication rules in a small P4 program
- Translate to match + action rules independent of hardware

eBPF: Extended Berkeley Packet Filters

- Specify small filter programs
- Packet filtering in Linux Kernel
- Efficiency and powerfulness
- Match packets independently of any protocol implementation
- Changes in program do not require a recompilation of the target switch software
- Easy to implement and modify communication rules during operation

Anomaly Detection

New attack vectors not considered in communication rules

Communication rules might be incomplete and contain errors

Detect anomalies based on known traffic patterns

Must be complemented with an approach that dynamically adapts to the current smart home configuration

Anomaly Detection (Machine Learning)

Detect unknown attacks which were not considered in the system

Misclassification leads to restrictive network configuration

Complement the rule-based approach

- Adapt existing communication rules
- React on imminent threats

Trained for data flow during run time

- Known attack patterns can be used

In case of anomaly, communication rules are adapted to prevent further risks

Other Solutions

UI / UX for User Awareness and Control

- Inform users what devices are doing
- Auditing features or physical indicators (e.g., recording lights)
- Allow users to interact with devices physically

Design Consciously for Multiple Users

- Some users were denied access
- Physical recording indicators can help
- Future research

Develop Standard Best Practices for End Users

- Practices such as strong password and Wi-Fi security are not smart home specific
- Security experts must communicate best practices for smart home contexts

Design for Secure and Robust Interoperability

- Used third party apps just for interoperability
- Issues arise at boundaries between components
- User created interoperability links can present future points of weakness

Other Solutions

Collecting and transmitting sensitive information to cloud

- Mobile application and end user credentials must pass authorization

Use strong and standardized cryptography methods

Tools that simplify configuration and security installation process

Insights

Convenience and comfort

But security concerns such as privacy and physical safety

Cost

Echo Device

Link: https://www.youtube.com/watch?v=jttMEqmizDc. Stop at 1:12

Conclusion

- Smart devices in home make people’s lives and everyday duties easier
- Numerous applications including energy efficiency, e-health, multimedia, surveillance and security
- Security threats include privacy / security, physical attacks, disasters and outages, and damage / loss
- End users are more concerned about physical security than privacy
- In-network security model allows minimum communication needed for a device
- Solutions such as securing communication between devices and modifying UI / UX to inform users what a device is doing can be extremely helpful

Questions