Securing Smart Home: Technologies, Security Challenges, and Security Requirements

Changmin Lee, Luca Zappaterra, Kwanghee Choi, Hyeong-Ah Choi

George Washington University

Contents

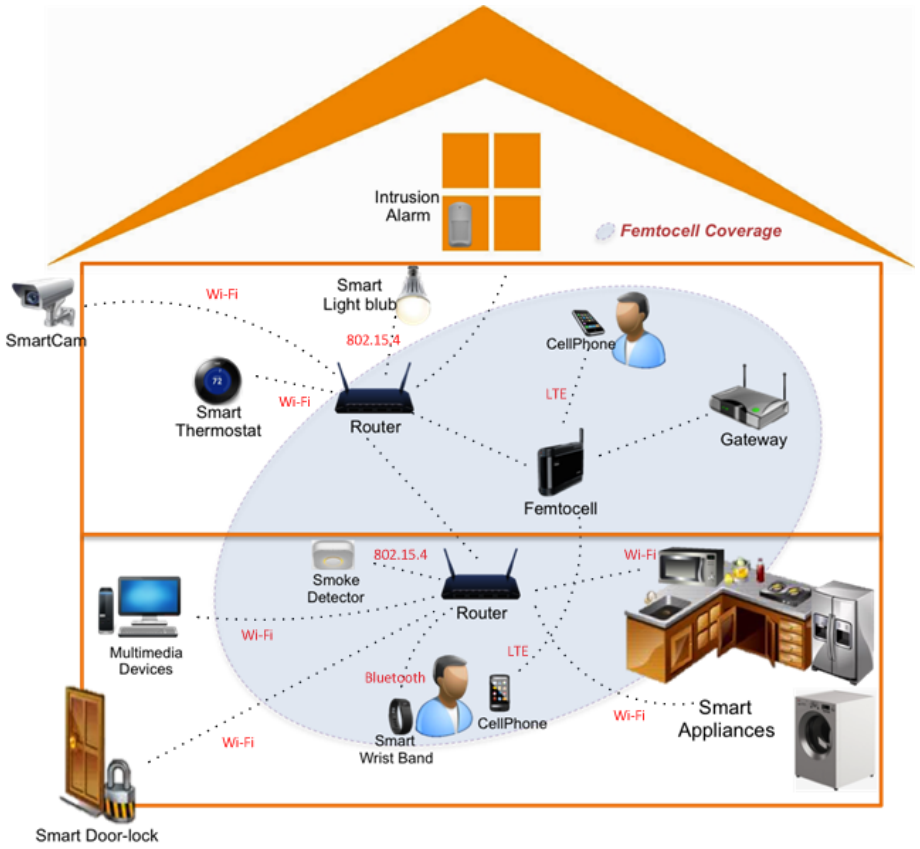
- Introduction
- Smart home
- Challenges
- Security Threats
- Security Requirements
- Future Direction
- Work in Progress

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Introduction

- Internet of Things (IoT)
  - Interaction and cooperation among every day objects
  - Will generate very large amounts of data transmissions
  - Requires guarantee of security and privacy

Smart home



An example of smart home

Smart home

- Equipped with various smart objects
- Various hardware specification and heterogeneous protocols
- Forming a distributed heterogeneous network

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Applications

- Lighting Control
- Appliance Control
- Entertainment
- Safety System
- Climate Control
- Assisted Living

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Operating System

- Contiki OS
- Tiny OS
- RIOT OS

Communication Protocols

- PHY and MAC Layer
  - IEEE 802.15.1 (Bluetooth)
  - IEEE 802.15.4 (ZigBee)
  - IEEE 802.11 (Wi-Fi)
- Network and Transport Layer
  - RPL/MPL (Routing Protocols)
  - TCP/UDP (Transport layer Protocols)
- Application Layer (Messaging Protocols)
  - CoAP
  - MQTT
  - XMPP

Challenges

- Resource Constraints
- Heterogeneous Communication Protocols
- Unreliable Communications
- Energy Constraints
- Physical Access

Resource Constraints

- Limited Memory and Computing Power
- Current security mechanisms are not feasible to cover all devices

TABLE I: Specifications of smart home devices

Device Type	Chipset	Core Freq.	RAM	Flash Memory	Power	Networks Protocols
iPhone	A7x Quad-core Processor	1.7Ghz	2GB	Up to 128GB	Battery	Wi-Fi, Bluetooth, NFC
Nest Learning Thermostat	ARM Cortex-A8	800Mhz	512MB RAM	2GB	Battery	Wi-Fi (802.11)
Nest Smoke Detector	ARM Cortex-M4	100Mhz	128KB RAM	512KB	Battery	Wi-Fi (802.11)
	ARM Cortex-M0	48Mhz	16KB RAM	128KB		
NETGEAR Router	Broadcom BCM4709A	1.0Ghz	256MB	128MB	AC Power	Wi-Fi (802.11)
Samsung Smart TV	ARM-based Exonys SoC	1.3Ghz	1GB	N/A	AC Power	Wi-Fi (802.11)
Samsung SmartCam	GM812x SoC	Up to 540Mhz	N/A	Up to 64GB	AC Power	Wi-Fi (802.11)
Elster REX2 Smart Meter	Teridian 71M6531F SoC	10Mhz	4KB	256KB	Battery	ZigBee (802.15.4)
Philips Hue Light bulb	TI CC2530 SoC	32Mhz	8KB	Up to 256KB	Battery	ZigBee (802.15.4)
Fitbit Smart Wrist Band	ARM Cortex-M3	32Mhz	16KB	128KB	Battery	Bluetooth LE
Sensor Devices	Microcontroller	4 – 32Mhz	4 – 16KB	16 – 128KB	Battery	ZigBee, Wi-Fi, Bluetooth

Heterogeneous Communication Protocols

- Various type of communication protocols
  - E.g.)802.15.4, Wi-Fi, Bluetooth, and NFC
- A need for an intermediate gateways
  - Data collection, handling different type of packets
- Poses a major limitation for the implementation of end-to-end security solutions

Unreliable Communications

- Resource constrained devices use UDP as a main transport layer protocol
  - UDP does not guarantee reliability of packet delivery
- Retransmission due to the transmission failure and damaged packet.
- Retransmissions and error handling mechanisms require large overhead
  - May not be tolerable in resource constrained devices

Energy Constraints

- Battery operated devices
  - Thus vulnerable to resource depletion attacks.
- Large energy consumption when applying complex computation

Physical Access

- Unattended devices
  - becoming easy targets of tampering attack
- Reverse Engineering
  - Sensitive information can be extracted through debugging port

Security Threats

- Attacks to the physical layer
- Attacks to the data link layer
- Attacks to the network layer
- Attacks to the transport layer
- Attacks to the application layer

TABLE II: Security threats from each protocol layer

Layer	Protocols	Threats & Attack Framework
Application	CoAP, XMPP, MQTT	XMPPloit(Framework)
Transport	TCP, UDP	UDP Flooding, TCP SYN Flooding, De-synchronization
Network	MPL, RPL, 6LoWPAN	KillerBee(Framework), Black-hole Attack, Change Rounting Information, Packet Capture & Injection, Selective-Forwarding, Sinkhole, Hello Flood, Wormhole, Sybil, Tiny Fragmentation
Data Link	802.15.4, 802.11, 802.15.1	KillerBee(Framework), GTS Attack, Back-off manipulation, ACK attack
Physical	802.15.4, 802.11, 802.15.1	Jamming, Tampering

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Attacks to the Physical Layer

- Jamming
  - An intentional wireless interference.
  - Used for DoS (Denial-of-Service) Attack
- Tampering
  - Extraction of Security Information
    - Pre-installed network encryption key can be extracted
  - Duplication of a device
    - Fake devices containing malicious code
      - Act as a genuine device in a network
  - Code injection
    - Malicious Code can be injected through debugging port

Attacks to the Data Link Layer

- KillerBee (Framework)
  - Monitoring data transmission
  - Injecting traffic
  - Packet manipulation
- GTS Attack
  - Causes collision and make devices retransmit packets
- Back-off Manipulation
  - Manipulating retransmission interval time
    - Can cause resource depletion

Attacks to the Network Layer

- Black hole attack on RPL
  - Attack RPL implementation of Contiki OS
  - Assumed that there exist a compromised node in a target network
  - Causing disruptions in the data flow of the network

- KillerBee
  - Sniffing encryption key during its transmission
    - Stolen encryption key will be used to extract data from the packet

Attacks to the Transport Layer

- No smart home specific attacks exist.
- Resource constrained devices use UDP for energy efficiency
- General well-known attacks can be applied
  - E.g.) TCP/UDP Flodding, Desynchronization

Attacks to the Application Layer

- XMPPloit
  - Targeting XMPP connections
  - Forces client device not to encrypt its communications
    - Allows attacker to modify packets

Security Requirements

- User Authentication
  - User must be authorized before use
- Device Authentication
  - Devices must be authenticated before they deployed in a network
- Network Monitoring
  - In order to detect malicious activity, network monitoring is necessary
- Secure Key Management
- Physical Protection

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Future Direction

- Building IoT security testbeds
- Experiments on possible attack scenarios at each protocol layer in a testbed
- Detailed analysis of each threats
- Develop security solutions against threats in a smart home

Work in Progress

- IoT Technologies adopted new networking protocols
  - However Wi-Fi will remain as a major role in IoT Environment
- US Wi-Fi Statistics 2014 [1]
  - 71% mobile communication flows over Wi-Fi
  - 2/3 of US consumers prefer Wi-Fi to cellular
  - There will be more than 7 billion new Wi-Fi enabled devices by 2017
- However some Wi-Fi networks do not use updated security protocol
  - Even WPA2 security is vulnerable

Security Protocol	Number of APs	Percentage
WPA2 (Personal & Enterprise)	16,465,859	30.78%
WPA (Personal & Enterprise)	4,238,622	7.92%
WEP	13,301,049	24.87%
Unknown	9,591,035	17.93%
Open	9,894,979	18.5%

US Wi-Fi Security Statistics 2014

[1] "50 incredible wifi tech statistics that businesses must know." http://www.huffingtonpost.com/vala-afshar/50- incredible- wifi- tech- sb 4775837.html.

Snoopy *

- Small (Size of deck of card)
- Easy to use (fully automated by script)
- Cheap (Can be built with $65)
- Running with solar battery
  - Can be up indefinitely

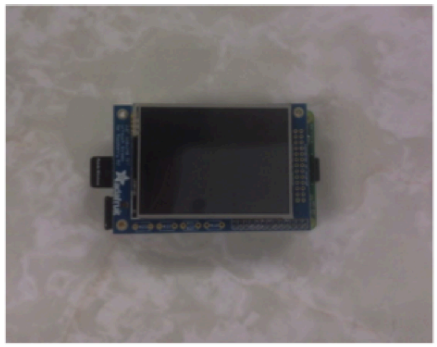


Fig. 1: The Snoopy Hardware

* H. Hijjawi and H.-A. Choi, "Solar-powered password theft - turning a raspberry pi into an automated data sequestration system," (Demo) *4th International Conference on the Internet of Things (IoT 2014)*, 2014, MIT.

Snoopy *

- Capable of performing multiple exploits
  - Deauthentication Attacks
    - Continuously sending deauthentication packets to AP to kick out users out of the Wi-Fi network
    - Even WPA2-EAP (Enterprise) network can be targeted
  - Creating Bogus AP
    - Creating a new AP and let the users join
  - SSLStrip
    - Obtain users` credentials even the connection is encrypted with SSL/TLS
  - Monitoring Network traffic
    - Snoopy makes to see every browsing history that is not encrypted with SSL/TLS

* H. Hijjawi and H.-A. Choi, "Solar-powered password theft - turning a raspberry pi into an automated data sequestration system," (Demo) *4th International Conference on the Internet of Things (IoT 2014*), 2014, MIT.

+ Changmin Lee and H.-A. Choi, "Leveraging Existing MITM Attacks to Explore New Techniques for Password Procurement on Wi-Fi Networks" (In Preparation).

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC