# IoT Security and Privacy

## IoT Application - Smart Home

YIER JIN

UNIVERSITY OF FLORIDA

EMAIL: YIER.JIN@ECE.UFL.EDU

SLIDES ARE ADAPTED FROM PROF. XINWEN FU @ UCF/UMASS

# Learning Outcomes

Upon completion of this unit:

- Student will be able to explain the concept of smart home
- Student will be able to analyze vulnerabilities in smart home networks
- Student will be able to analyze the impact of the vulnerabilities
- Student will be able to practice risk analysis of smart home systems

# Prerequisites and Module Time

## Prerequisites

- Students should have taken classes on operating system and computer architecture.
- Students should know basic concepts of networking.

## Module time

- Three-hour lecture
- One-hour homework

# Main References

[1] Grau, Alan., “Smart home security: Protecting wirelessly connected endpoints from cyber-attacks”, 2015

[2] D. Jacoby. (2014, August 21). IoT: How I hacked my home [online]. Available: https://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home/

[3] Jesus Molina, Learn how to control every room at a luxury hotel remotely: the dangers of insecure home automation deployment, Blackhat USA 2014

# Outline

Smart home security

Hack a home

Dangers of insecure home automation deployment

# Disney Film: “Smart House” in 1999

Pat, the smart house, controls everything

- door locks, laundry, cleaning and meals.

She goes crazy

# Benefits of Smart Home

Smart home devices connected to the internet

- Through WiFi, Bluetooth, WiMAX, Z-Wave, etc.

Monitor energy and water supply consumption

- Find out how to save cost and resources

Monitor security systems remotely

- Surveillance cameras

Remotely operate appliances

- For convenience
- Avoid accidents
- save energy

Rich features by running programs available on the internet

Challenge: security and privacy issues

# Risks Management

## Risk assessment

- “Risk is a function of the **likelihood** of a given **threat-source**’s exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organization. ” [3]

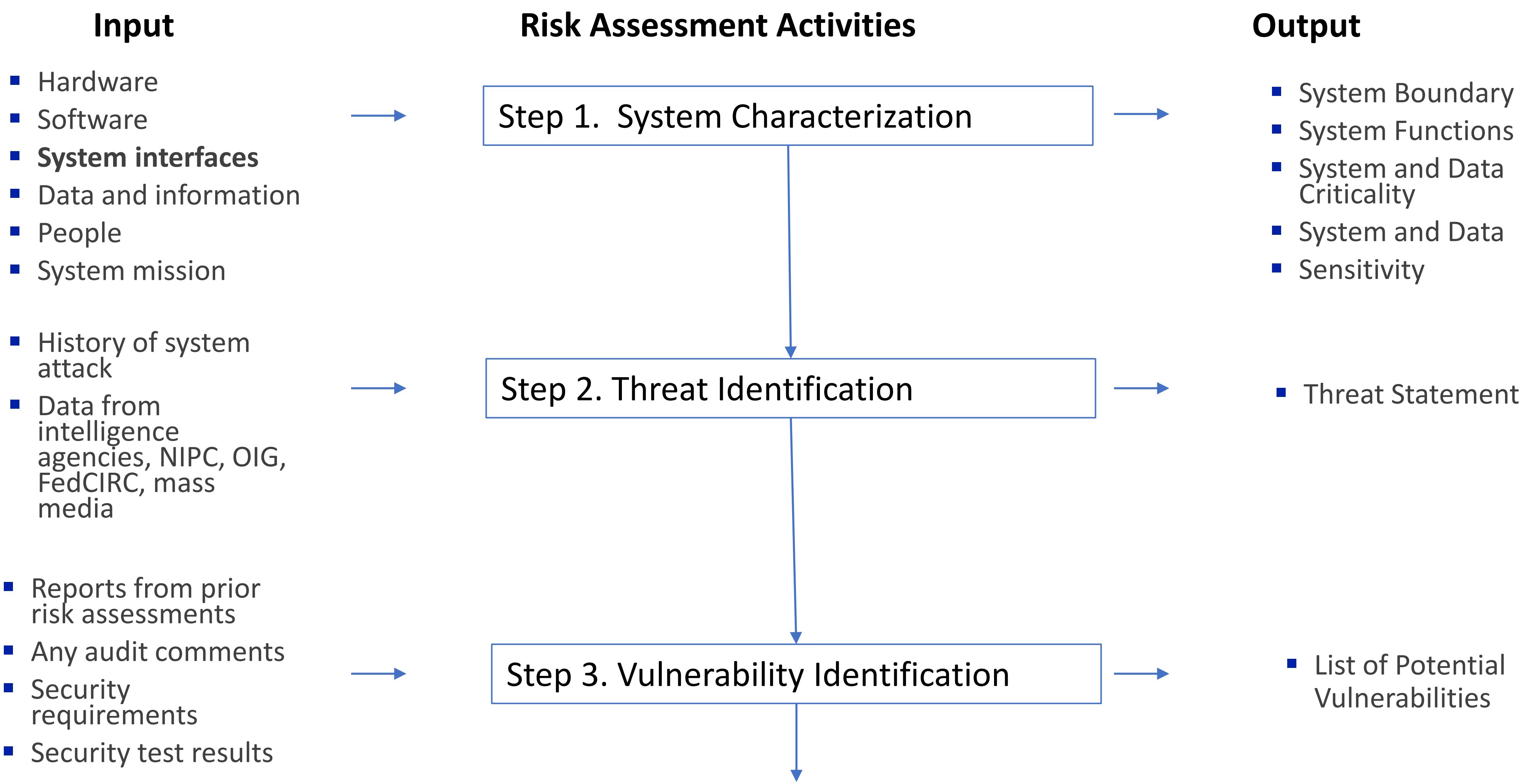
## Risk mitigation

- “Prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. ”

## Evaluation and assessment

- Risk management evolves as the organization evolves

# Risk Assessment Methodology Flowchart [4]



### Input

- Hardware
- Software
- **System interfaces**
- Data and information
- People
- System mission

→ Step 1. System Characterization →

### Output

- System Boundary
- System Functions
- System and Data Criticality
- System and Data
- Sensitivity

### Input

- History of system attack
- Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media

→ Step 2. Threat Identification →

### Output

- Threat Statement

### Input

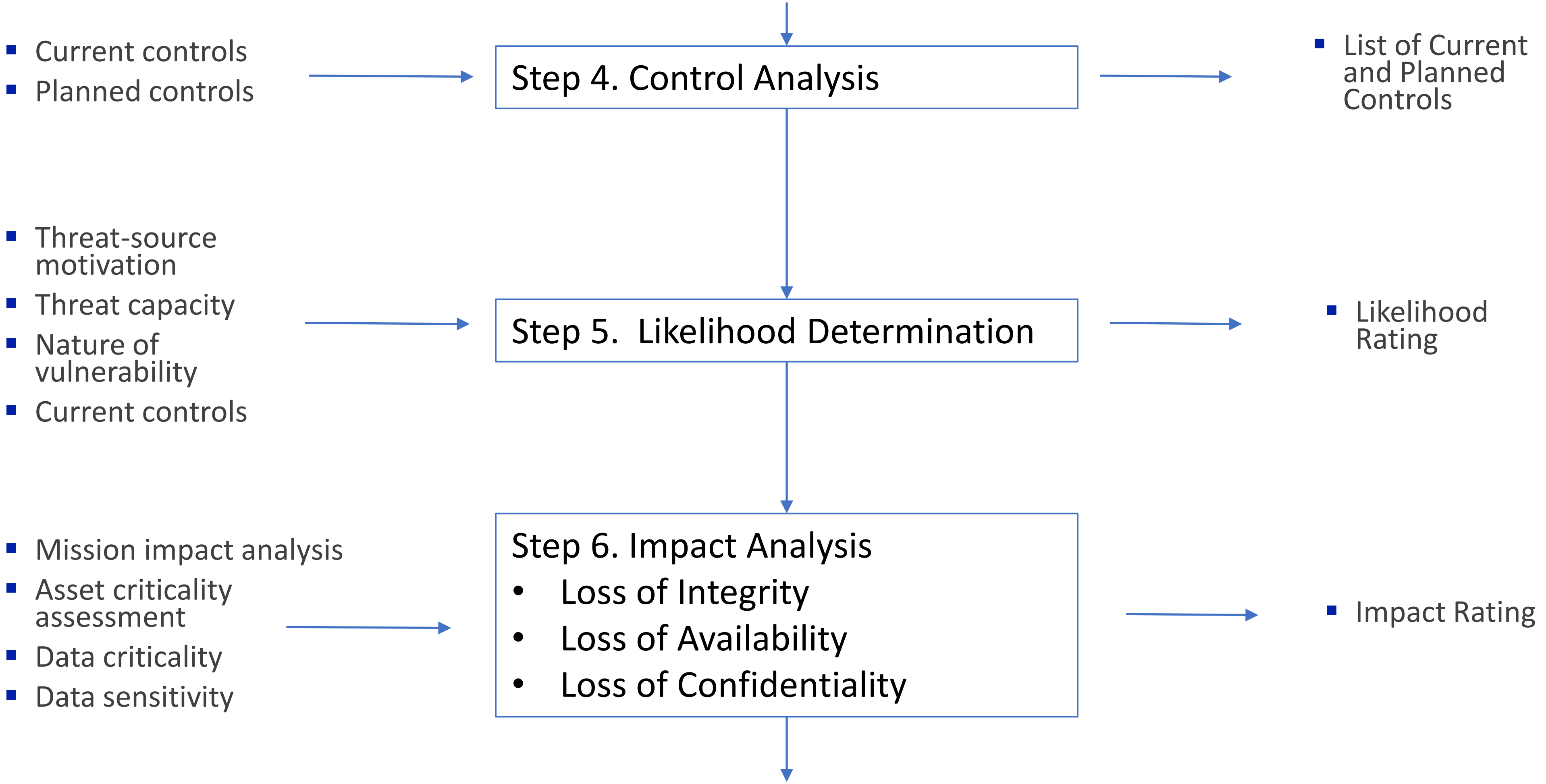
- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results

→ Step 3. Vulnerability Identification →

### Output

- List of Potential Vulnerabilities

# Risk Assessment Methodology Flowchart



- Current controls
- Planned controls

Step 4. Control Analysis

- List of Current and Planned Controls

- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Step 5. Likelihood Determination

- Likelihood Rating

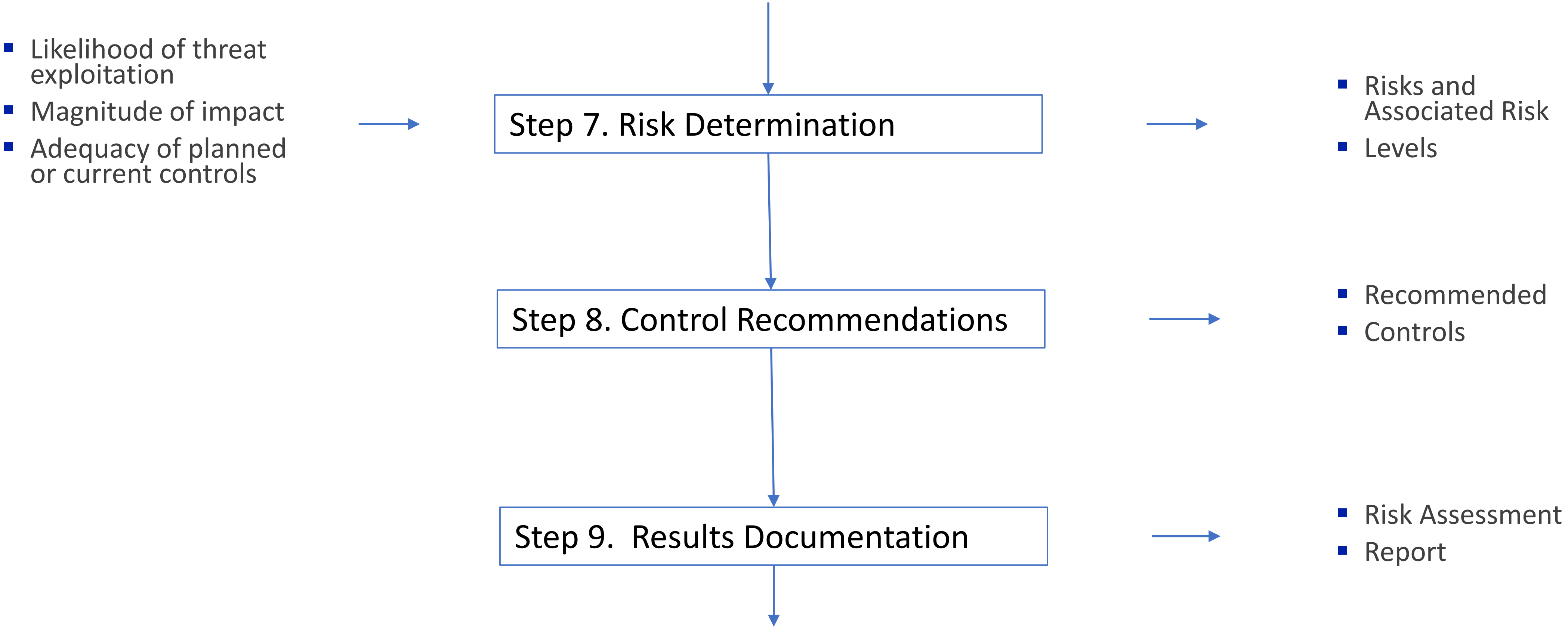
- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity

Step 6. Impact Analysis

- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

- Impact Rating

# Risk Assessment Methodology Flowchart



- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Step 7. Risk Determination

- Risks and Associated Risk
- Levels

Step 8. Control Recommendations

- Recommended
- Controls

Step 9. Results Documentation

- Risk Assessment
- Report

# Risks of Smart Homes

## Vulnerabilities

- No password
- Default password and account
- No encryption

## Threats

- Hacks of lightings, television, smart meters, hot tub water heater, garage door, video surveillance systems, doors and windows, etc.
- Intercepted private videos
- Flushing toilets

# Differences: PC Systems and Home Security Systems

No upgrading functionality for deployed smart home devices

- Security features
- Bug fixes

Need of specialists providing security solutions

- May use OS like VxWorks, INTEGRITY

Software only from the manufacturer

- No third party security enhancement

# Home Owner’s Difficulties and OEMs

Lack of computer knowledge

- Installation of software and patches

Lack of computer security knowledge and management expertise by home owners

Device security on OEMs (Original Equipment Manufacturer)

- Often no incentive because of no profits from computer security

All connected devices to be secured

# Resources in Security Devices

Very limited resources is available for the device

Devices are cost sensitive

Can only run a specialized embedded operating system

Devices are built with minimum memory and cheap CPUs to save production costs

# How to Protect Smart Devices?

Security features built into the device

- A security system with multiple layers

The security solution

- Need of minimum resources
- Sensitive to Internet attacks

NO universal solution

- Specific purpose devices for particular home security network
- No solution that fits all requirements

# What to Consider?

Risk assessment

- Chances of being attacked
- Vulnerable network sectors
- Implementation costs
- Security failure costs - economical and environmental costs

# Possible Security Features

Secure bootstrapping (signed code)

- Code in the device cryptographically signed by the manufacturer for integrity
- Use of the hardware to authenticate the code – root of trust

Secure code updates

# Possible Security Features (Cont’d)

Data Security

- Encrypted data in the device
- Encrypted communication
- Authentication and authorization before accessing a device

Authentication

- Strong passwords
- Appropriate authentication protocol

Secure communication

- Encrypted communication using SSH or SSL
- Secure encryption algorithm (long keys)

# Possible Security Features (Cont’d)

Intrusion prevention

- Use of firewalls to permit trusted hosts and block known bad sites and hackers

Intrusion detection and monitoring on devices

- Detect and report attacks and suspicious activities

Security management

- Update security policies
- Monitor emerging threats

# Requirements of Securing IoT

Build front line security features

Design customizable security features for the need of the device

Consider security in early design and development

Consider and acquire necessary hardware for security features such as secure boot

# Outline

Smart home security

Hack a home

Dangers of insecure home automation deployment

# Network Devices

Printers

External Storage Devices

Gaming systems:

- XBox
- PlayStation

Smart TV

Home Security System

Cable/Satellite Box

Internet service provider (ISP) Router

# Project Division

Identify what devices to hack

Set criteria for a successful hack

Web interface

Hardware

Software

# Discoveries

Device analysis

- Firmware updates
- Hardware capabilities

Device Vulnerability

Web interface vulnerabilities

# Device Analysis

Automatic updates or manual updates?

Is product obsolete or not supported anymore?

Capabilities:

- Operating system?
- Built in security measures, e.g. encryption?

# Device Analysis (Cont’d)

Obsolete software or no more updates.

- Average support period less than a year.

Many had Linux based OS.

- Easy for hackers
- GNU C compiler installed
- Interpreters installed (e.g., Perl, Python)

# Vulnerability

Access to configuration file and password hashes

External Storage Device (ESD)

- Could be compromised and turned into a backdoor

No intrusion detection systems

System commands as root user

Full access to file system

# Web Interface Vulnerabilities

URL manipulation

- Access to hidden tools and functions

External Storage Device

- Remote command execution with full permissions
- OS level

ISP Router

- Tunnels to other devices
- Remote admin interfaces

# Outline

Smart home security

Hack a home

Dangers of insecure home automation deployment

# Objectives and Outcomes

Analysis of control automation protocols of St. Regis ShenZhen, a gorgeous luxury hotel

- Guest controls devices such as lights and TV using an iPad.

Analysis of a home automation system

- Anatomy of the attack that allows remote control of any IoT device connected to this system
- Deployment flaws
- How to create an iPad Trojan to send commands outside the hotel
- Countermeasure guideline

# Home/Hotel Automation

Automation of electronic components

- Heating, ventilation and air conditioning (HVAC), lighting, music, TV

IoT connects users with electronic components.

Home automation makes our life more comfortable, help the environment, and in a long run help saving energy consumption.

Security in Home Automation is critical

# Home/Hotel Automation on Market Today

A panel or phone communicates with the devices through routers

Security often relies on the WiFi security

- No other security measures
- Anybody (such as another guest of a hotel) with access to the hotel may access devices in any hotel room

# Benefits of Hotel Room Automation

Centralized hotel room automation

Save cost

Guest comfort and satisfaction

- No need of looking physical controls everywhere

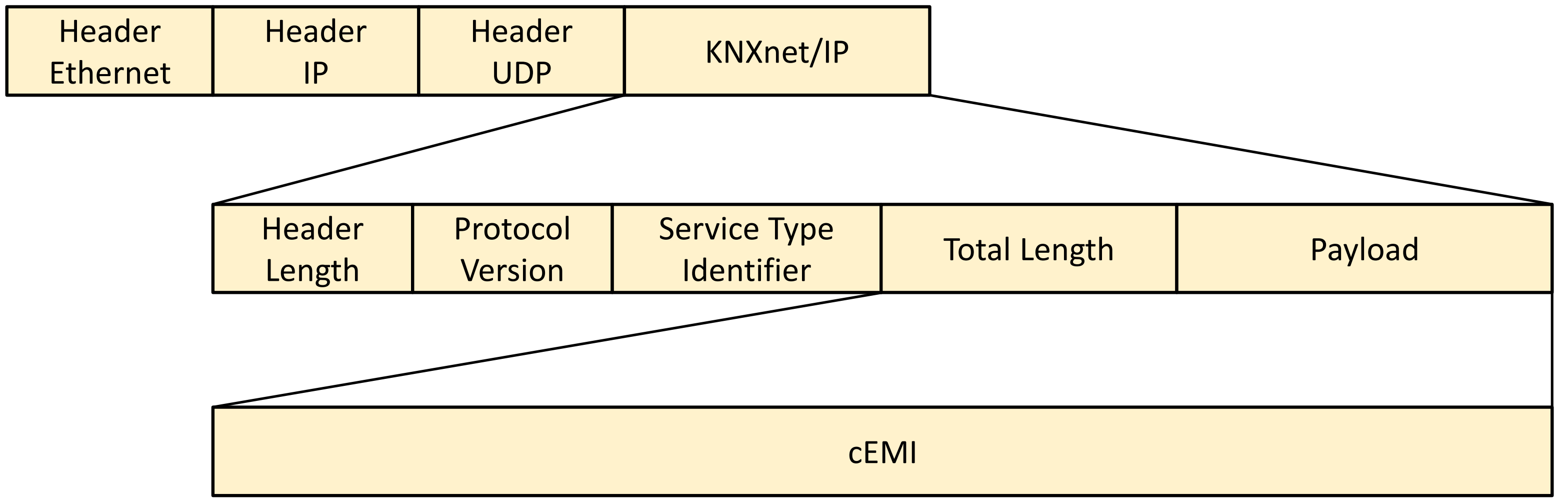
Increase utilization of amenities

# KNX

OSI-based network communication protocol for building automation.

Widely deployed bus communication standard

- Can be encapsulated inside IP



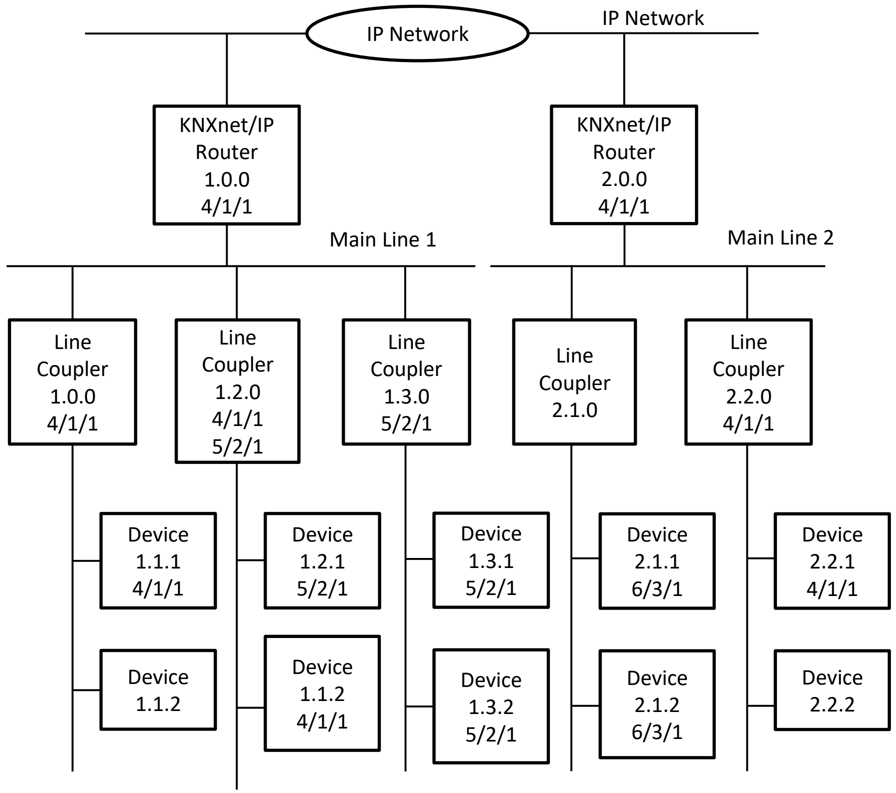
# KNX

Simple sequential handshake,

- CONNECTION_REQUEST, CONNECTIONSTATE_REQUEST, TUNNELING_REQUEST, DISCONNECT_REQUEST.

Sending messages to the KNX backbone

- Through TUNNELLING REQUEST



# KNX in the St. Regis ShenZhen

iPad, loaded with an app controlling all electronic devices.

KNX

- A wireless communication channel
- KNX backbone

# Wireless Communication Channel

WiFi with a WiFi key and captive web portal

The captive portal white lists device MAC address

Easy to intercept

# The Control iPad

No physical security.

- Can be connected to a computer
- Modify Configuration settings.

Control app using two types of UDP packets

- Track iPad’s IP address and room location.
- Communicate with end devices using KNX/IP protocol.

# KNX Network

Manipulate the protocol

- IP address inside the cEMI frame
- KNX destination address
- Action code
- Payload

IP address of each room accesses two KNX subnets

- First subnet has all KNX elements in the room
- Second subnet accesses every KNX/IP router in a floor

# The Attack

Collect information by using a sniffing tool such as Wireshark

- The KNX/IP router and KNX address of the room
- The KNX address of the appliance and a dictionary of actions,

With this knowledge the attack becomes trivial

- Use open source KNX tool - eidb
- Launch eidb with the target IP
- Send any arbitrary action to any room, e.g. raise all the blinds at the same time

Trojanize the iPad to control every room.

# Solutions

Use secure KNX protocol with authentication

Design a secure tunnel between the iPad and the KNX/IP router

- Adding a certificate and a tunnel code in the iPad
- Secure tunnel with SSL.

Revoke old certificate at check-out

- Grant a new certificate at check-in

# References

[1] Grau, Alan., “Smart home security: Protecting wirelessly connected endpoints from cyber-attacks”, 2015

[2] D. Jacoby. (2014, August 21). IoT: How I hacked my home [online]. Available: https://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home/

[3] Jesus Molina, Learn how to control every room at a luxury hotel remotely: the dangers of insecure home automation deployment, Blackhat USA 2014

[4] Gary Stoneburner, Alice Goguen, and Alexis Feringa, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, July 2002