Hacking Intelligent Building

Pwning KNX & ZigBee Networks

Tencent Blade Team

Tencent Security
Platform Dpt.

About US

HuiYu Wu (Nicky)

- Bug Hunter
- Winner of GeekPwn 2015
- Speaker of POC2017
- http://www.droidsec.cn

YuXiang Li (Xbalien)

- Major experience is in Mobile Security and found several vulnerabilities in Android.
- Former ROIS CTF team member
- Twitter : https://twitter.com/Xbalien29

Tencent Security Platform Dpt.

About Tencent Blade Team

- A security research team from Tencent Security Platform Department
- Focus on security research of AI, IoT, Mobile
- Has found 70+ security vulnerabilities (Google, Apple, Adobe)
- Research output has been widely used in Tencent products

Tencent Security Platform Dpt.

Tencent Security Platform Dpt.

Agenda

Part 1:

- **Introduction to Intelligent Building**
- **Automatic Attack on ZigBee Network**

Part 2:

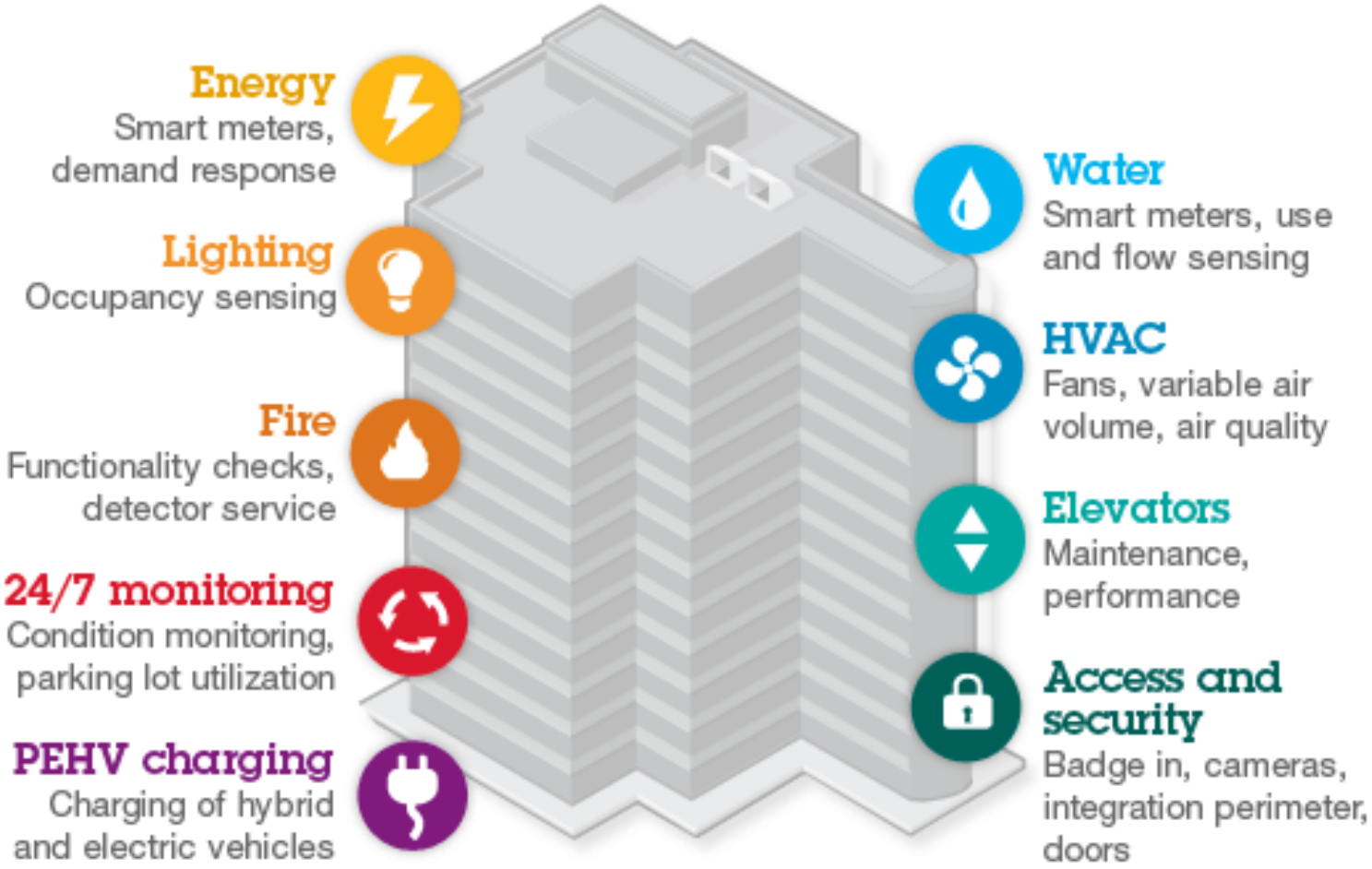
- **Practical Attack on KNX Network**
- **Security Advice**

Tencent Security
Platform Dpt.

Introduction to Intelligent Building

- What is Intelligent Building
- Why Intelligent Building
- Building Automation and Home Automation
- A Demo of Remote Attack Intelligent Building

What is Intelligent Building

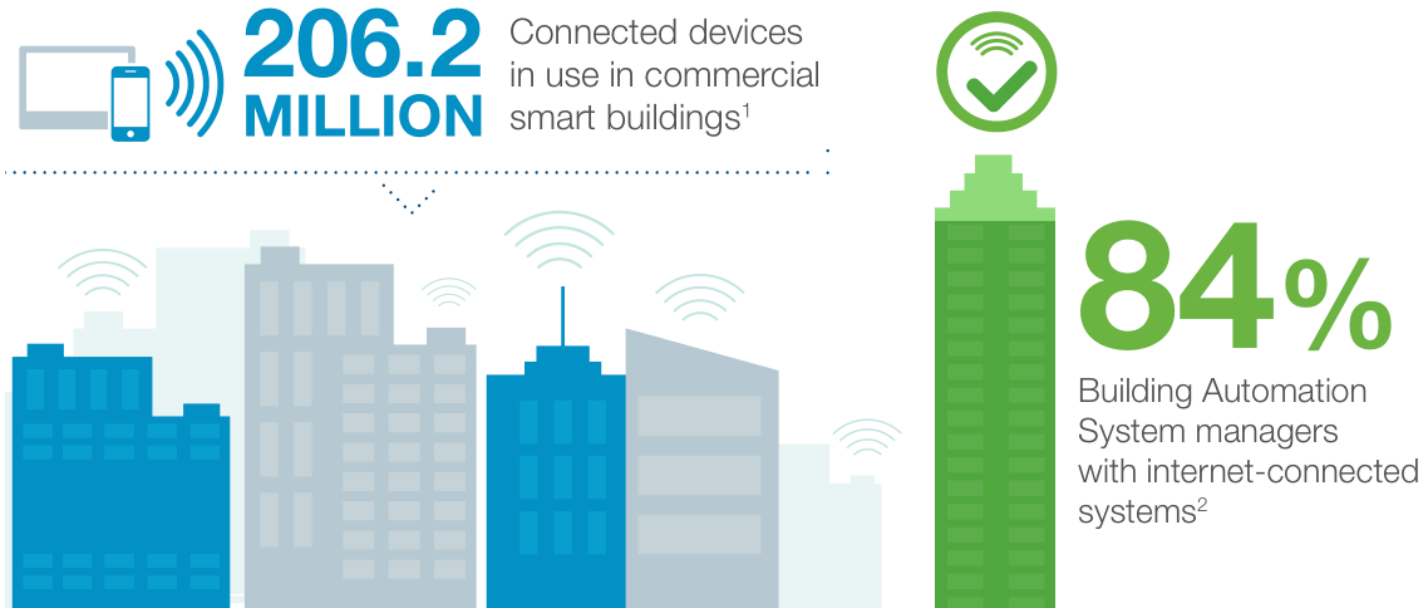


Tencent Security Platform Dpt.

Why Intelligent building

- There are few researches on the security of intelligent buildings, we think its security problem will become more serious.

- We want to work with the security community to enhance the safety of Intelligent building.



Tencent Security Platform Dpt.

Building Automation & Home Automation

Home Automation

Building Automation

Tencent Security Platform Dpt.

Building Automation & Home Automation

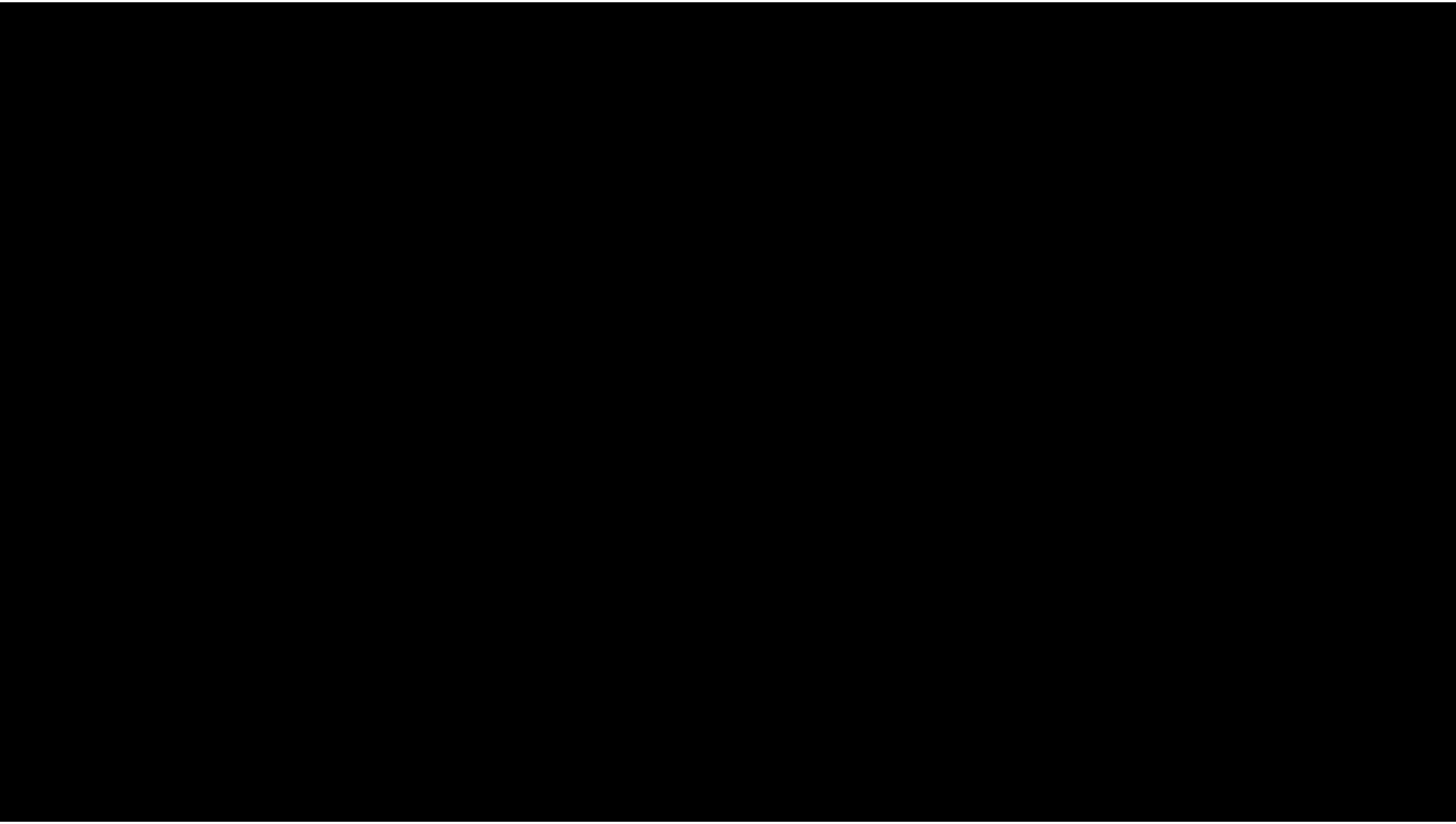
Home Automation	Building Automation
ZigBee®	KNX®
Wi Fi	ASHRAE BACnet™
Bluetooth™	DALI
Z-wave	LonWorks
	M-Bus

Tencent Security Platform Dpt.

Let’s set a small goal and make it possible

CAN WE REMOTE ATTACK INTELLIGENT BUILDINGS?

DEMO



It's cool, isn't it?

Let me show you how we did it.

Automatic Attack on ZigBee Network

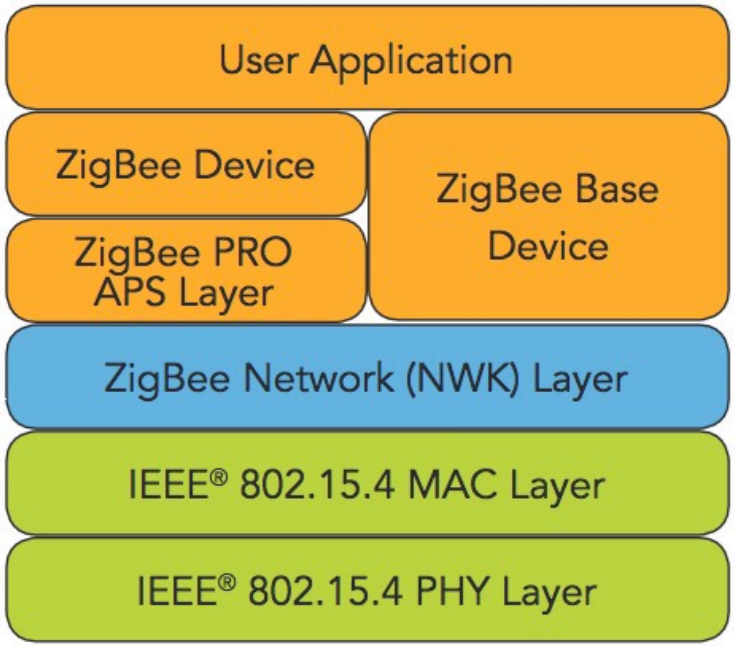
- What is ZigBee
- ZigBee Security Measure
- Current Risks on ZigBee
- Previous ZigBee Security testing tools
- Automated Attack ZigBee network
- ZomBee : A New ZigBee Pentest tools

Tencent Security
Platform Dpt.

What is ZigBee

- ZigBee is an open global standard for wireless technology designed to use low-power digital radio signals for personal area networks.

- ZigBee standard operates on the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz .



What is ZigBee

- **Coordinator**

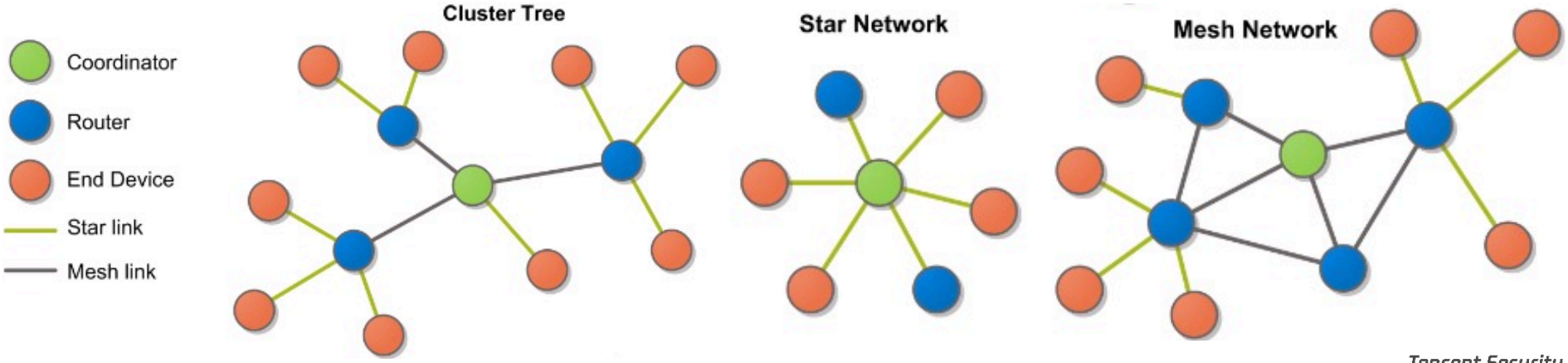
Network establishment and Control

- **Router**

Supports routing functionality, can talk to other routers ,coordinator, and end Devices

- **End Device**

Can only talk to routers and the coordinator



ZigBee Security Measure

- ZigBee Security Features
- ZigBee Security Keys
- ZigBee Security Security Model
- Security During Commissioning

ZigBee Security Features

ZigBee security is based on symmetric-key cryptography

- Uses the highly secure 128-bit AES-based encryption.
- Keys reusing among layers of the same device.
- Same security level for all devices on a given network and all layers of a device.
- ZigBee command includes a frame counter to stop replay attack.
- Access control lists.

ZigBee Security Keys

- **Link Key**

  This is uniquely shared between two devices and can be used to encrypt unicast messages between them. If a device shared a Link Key with the Trust Center it can be used to encrypt the transfer of the Network Key to a node joining the network.

- **Network Key**

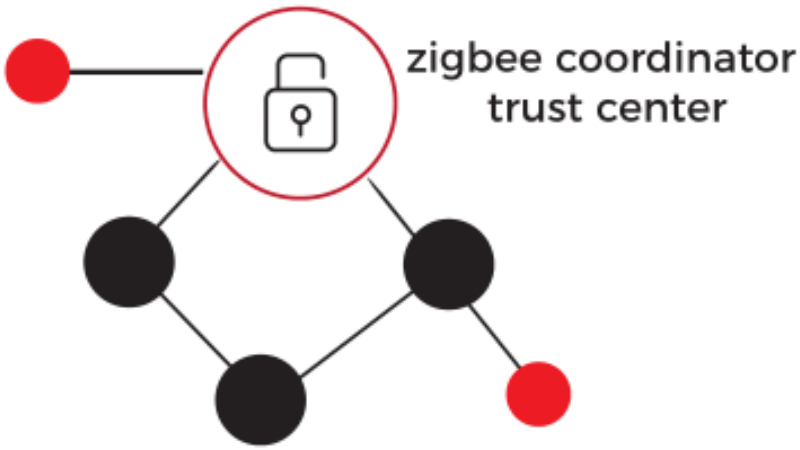
  Shared between every device on the network and can be used for NWK layer encryption and protecting broadcast traffic. They can be pre-installed on devices or transported from the Trust Center.

- **Master Key**

  Used for SKKE Establishment of Link Keys. Usually pre-installed.

ZigBee Security Model

Centralized Security Model

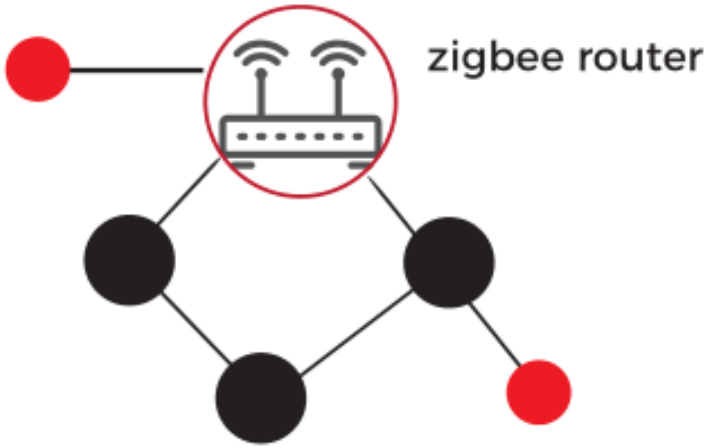


The TC establishes a unique TC Link Key for each device.

Node must support install codes (128 bits of random data + 16 bit CRC).

the Trust Center periodically creates, distributes, and then switches to a new network key.

Distributed Security Model



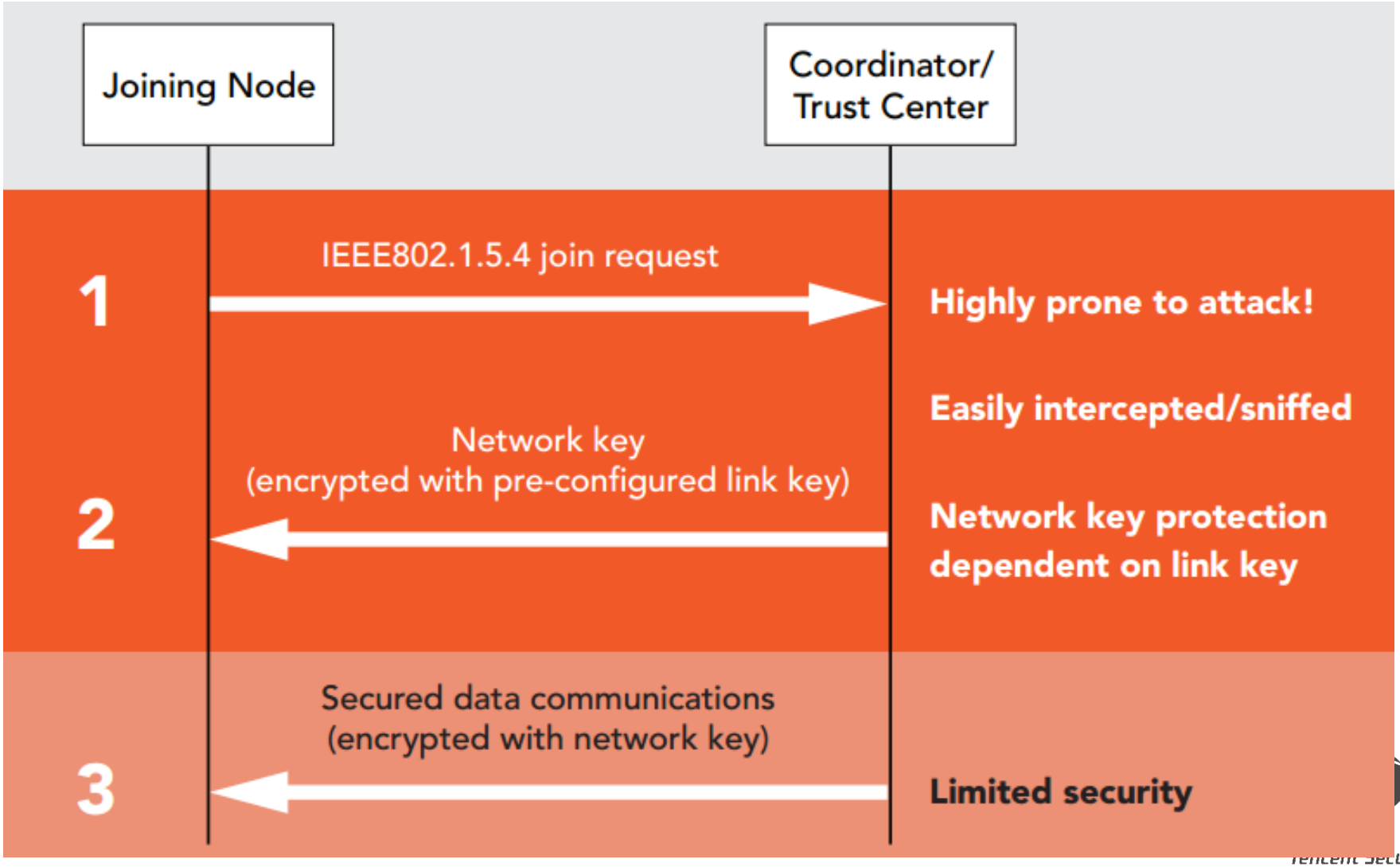
For easier-to-configure systems .

No Coordinator / Trust Center.

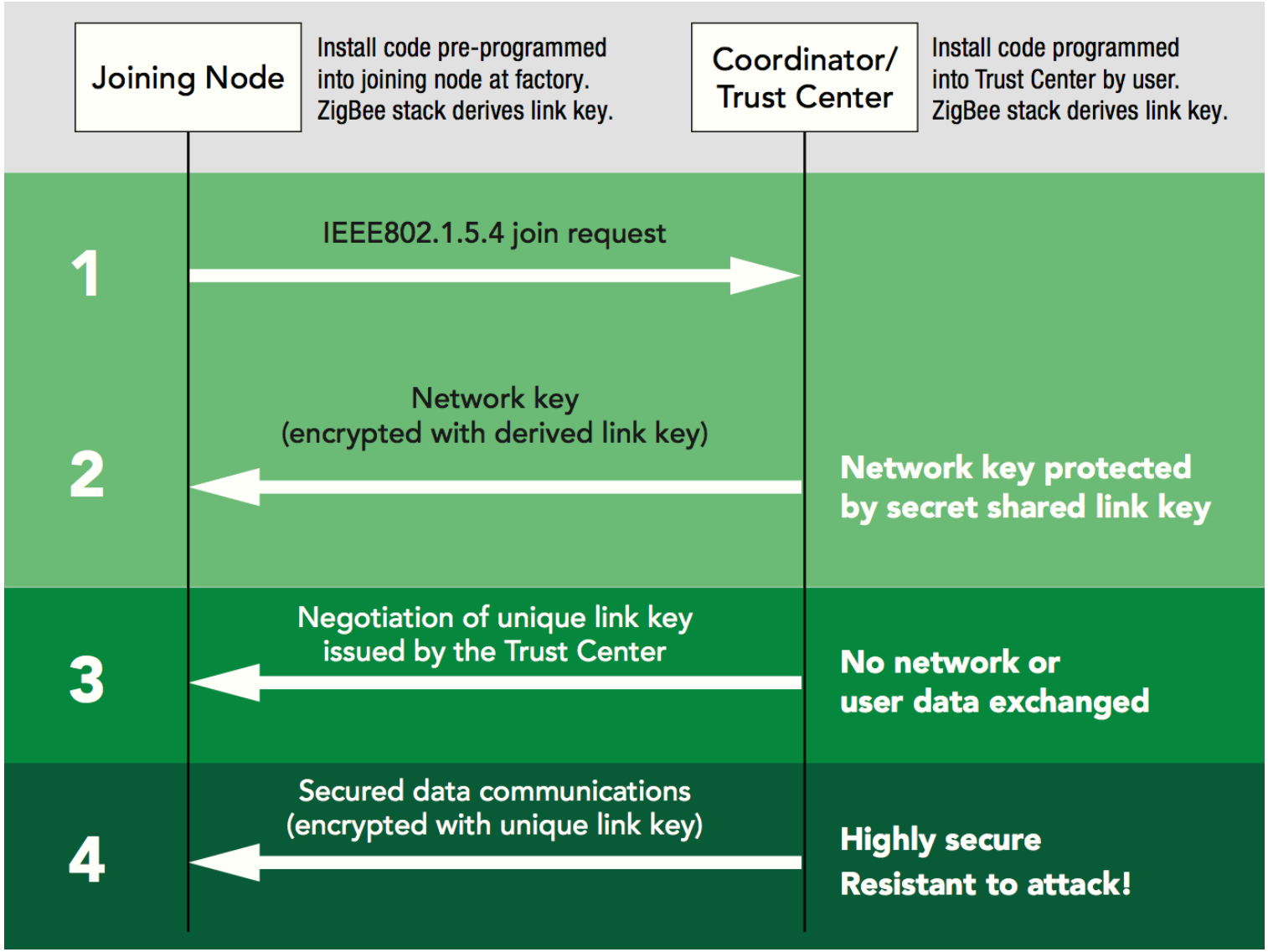
All devices must be pre-configured with a link key to encrypt the network key when a new node joining.

All the devices in the network encrypt messages with the same network key.

Security During Commissioning



Security During Commissioning



Tencent Security Platform Dpt.

Current Risks on ZigBee

- **Use a well-known security key**

(1) Default global link key: ZigBeeAlliance09

(2) Silicon Labs ZigBee chip default preconfigured Link key: Zigbee Security!

(3) Silicon Labs ZigBee chip default Network key: ember EM250 chip

- **Insecure key transport over the air**

(1) In some devices that use old ZigBee stack, it's easy to sniff the network key if transport key in clear text.

(2) A knowledge of the link key makes obtaining the network key possible by capturing over-the-air packets.

Current Risks on ZigBee

- **Insecure key storage**

In the device's firmware or flash chip hard-coded key in plaintext

- **Insecure rejoin and reuse the TC Link key**

A node device can send a rejoin request to the network, and the network key will be transported again. And if the same link key is used for every join attempt, it opens up the system to rejoin security attacks.

- **Replay protection bypass**

If the network key is obtained, we can decrypt the NwkSeq number and frame counter from the packet so that it is automatically updated to the new value when the packet is injected.

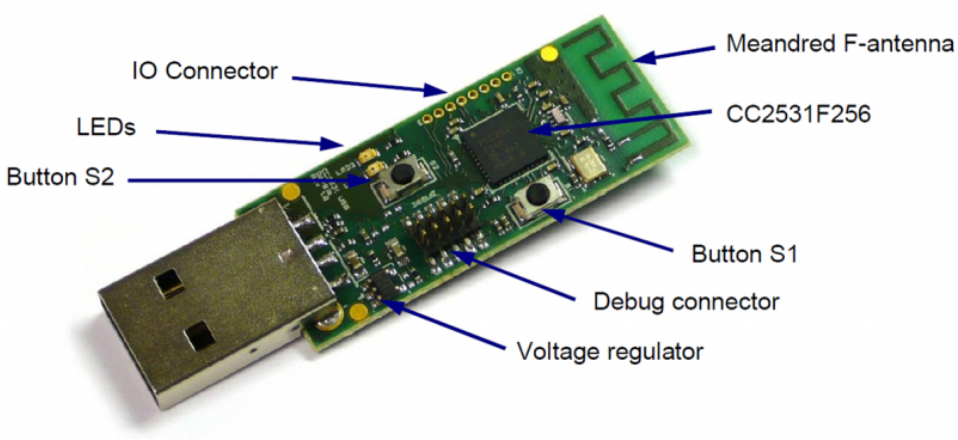
Previous ZigBee Security Testing Tools

ZigBee Sniffer Tools

- **Wireshark**
  https://wiki.wireshark.org/IEEE_802.15.4

- **SmartRF Protocol Packet Sniffer**
  http://www.ti.com/tool/PACKET-SNIFFER

- **Ubiqua Protocol Analyzer**
  https://www.ubilogix.com/ubiqua/



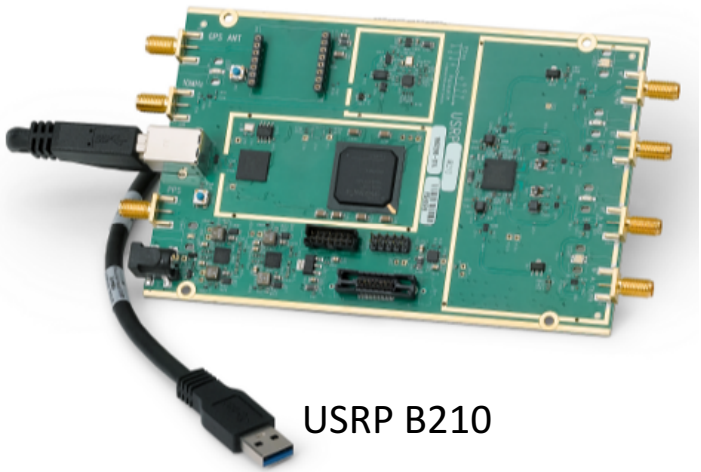
Tencent Security
Platform Dpt.

Previous ZigBee Security Testing Tools

- **KillerBee**
  https://github.com/riverloopsec/killerbee

- **SecBee**
  https://github.com/Cognosec/SecBee

- **Z3sec**
  https://github.com/IoTsec/Z3sec



USRP B210

Atmel RZ RAVEN USB Stick

Tencent Security Platform Dpt.

Automated Attack ZigBee network

If we want to quickly and automatically attack ZigBee devices in the city, we need to solve more problems:

- There are a lot of ZigBee devices in a building and it takes a lot of time to attack.
- The power of ZigBee transmitter is limited, which can't cover the whole floor at the same time.
- Multiple ZigBee networks are distributed in different rooms and channels, we can only specify one channel at a time to sniff and send packets.

Automated Attack ZigBee network

New improvements

- **Support attack multi ZigBee network quickly**

Increase the number of ZigBee sniffer and transmitter devices on raspberry pi to accelerate network scanning and attack speeds through multithreading.

Tencent Security Platform Dpt.

Automated Attack ZigBee network

New improvements

- **Support batch attack**

We create a virtual device in every network that collected, this virtual device will be set a random NwkAddr (0x0000 - - 0xfff7), and a IEEE/MAC address same as a device in the network, and its NwkSeq number and frame counter will start with 0.

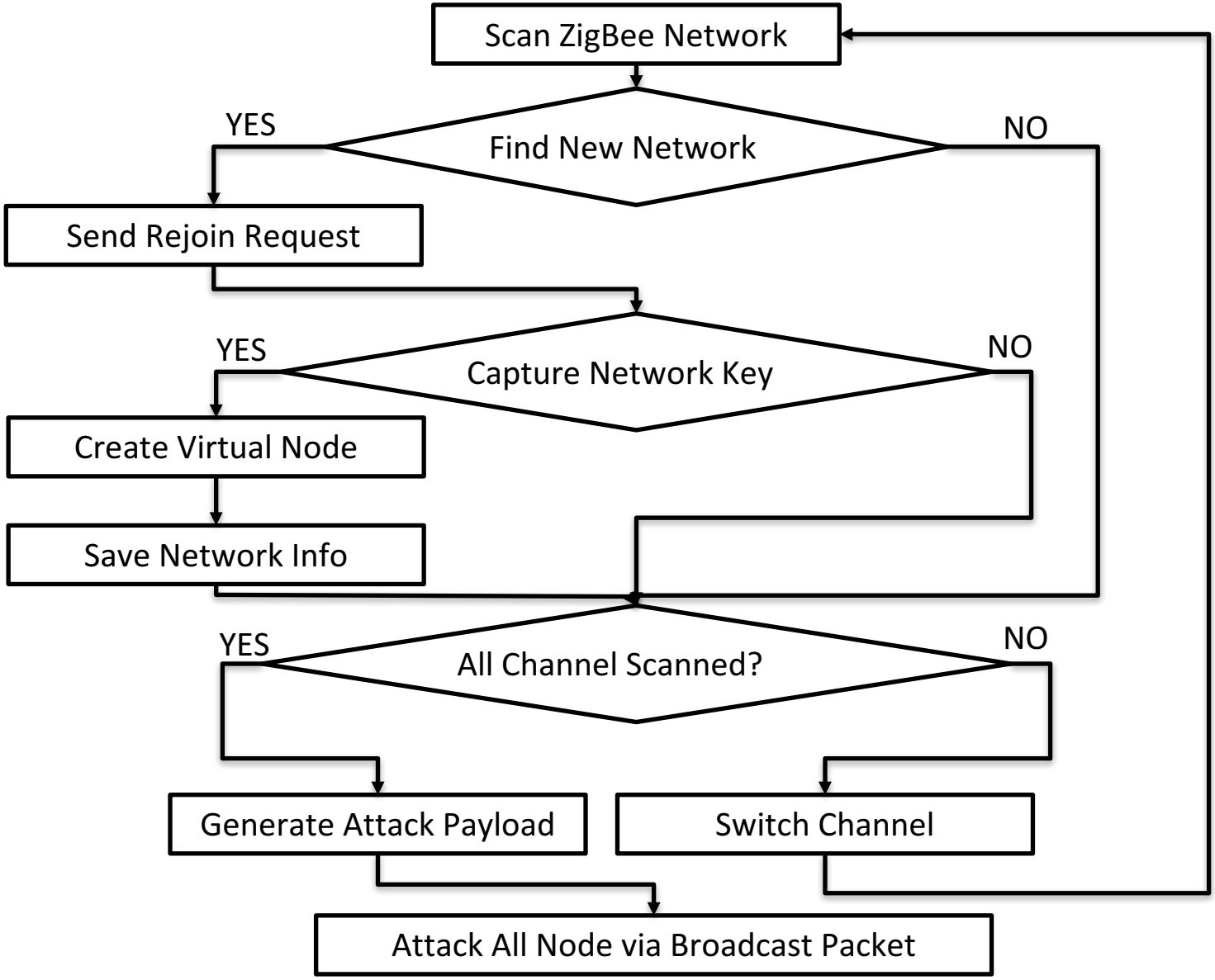
In most of ZigBee devices we tested , if we use this virtual device to send a broadcast packets with correct PANID, it can be used to batch attack all node device in ZigBee network.

ZomBee: A New ZigBee Pentest tools

- A ZigBee Network Automated Security Testing tool.
- Based On Raspberry Pi 3B and Atmel RZ RAVEN USB Stick.
- 64-bit OS inside.
- Can be carried in a drone or any other space that can hold a small box.

Tencent Security Platform Dpt.

ZomBee: A New ZigBee Pentest tools



ZomBee: A New ZigBee Pentest tools

	Sniff Packet	Network Scan	Replay Packet	Insecure Rejoin	Auto Update NwkSeq / Frame Counter	Command Inject	Capture NWK Key	Support Batch Attack
KillerBee	✓	✓	✓					
SecBee	✓	✓		✓			✓	
Z3sec	✓	✓			✓	✓	✓	
ZomBee	✓	✓	✓	✓	✓	✓	✓	✓

Review

Part 1:

- Introduction to Intelligent Building
- Automatic Attack on ZigBee Network

Part 2:

- Practical Attack on KNX Network
- Security Advice

Practical Attack on KNX Network

- Introduce KNX Network
- KNX Security Model
- Attack KNX Network

Why is KNX

- KNX is a widely used communication protocol for building automation
- KNX standard is administered by the KNX Association
- Less research on KNX security

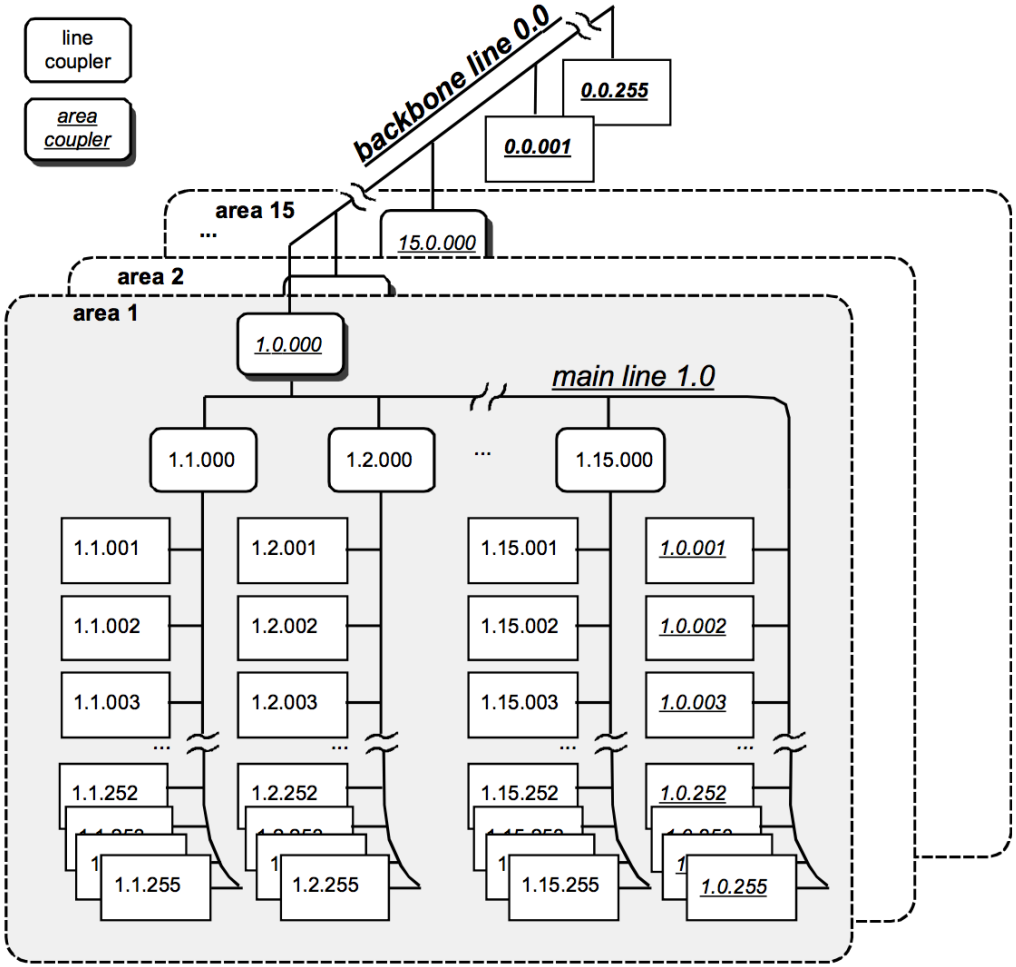
Basic Knowledge

- KNX devices categories
  - System devices and components
  - Terminal devices

- KNX communication media
  - Twisted Pair (TP)
  - IP (KNXnet/IP)
  - Power Line and Radio Frequency

Basic Knowledge

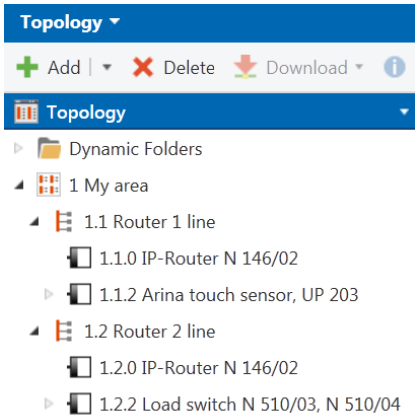
- The KNX topology

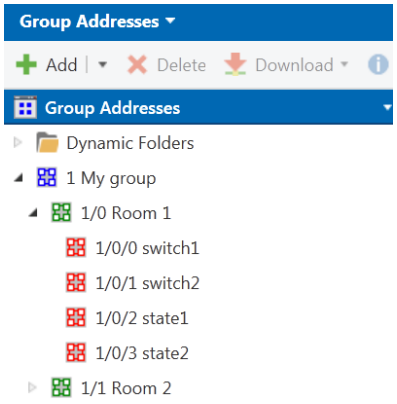


Tencent Security Platform Dpt.

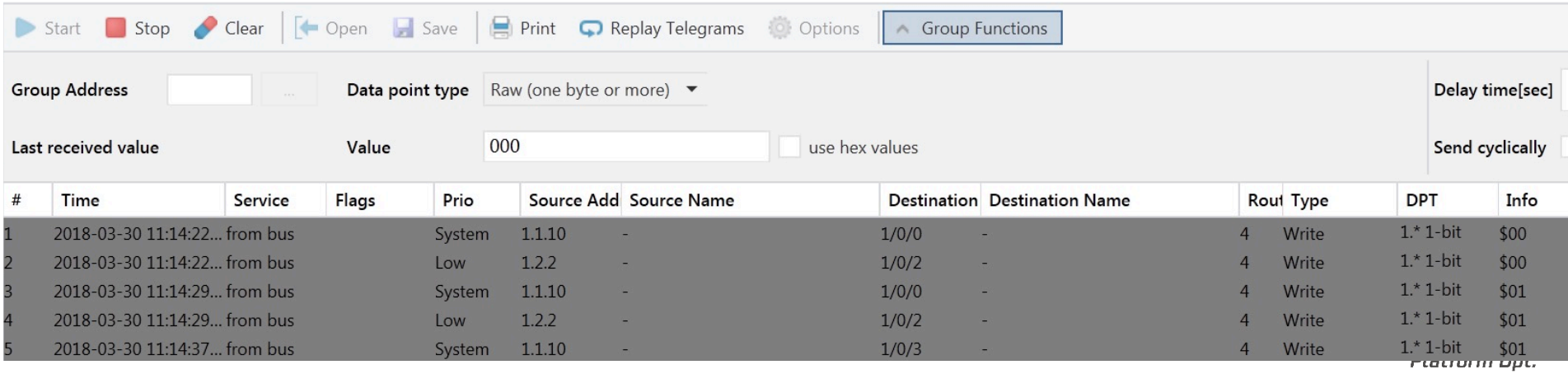
Basic Knowledge

- Addressing between devices
  - Individual address
  - Group address



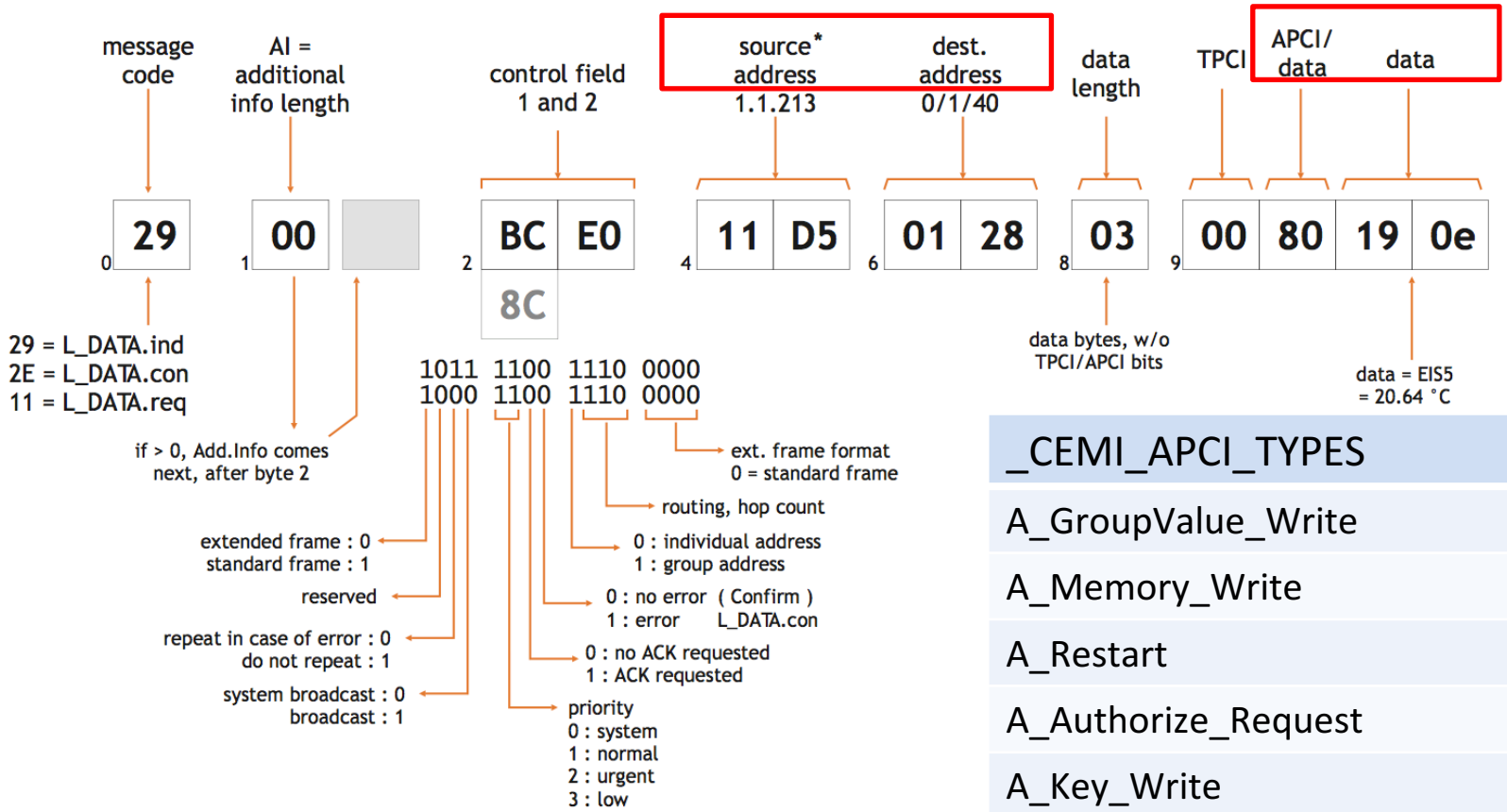


- ETS for KNX installation
  - Design topology architecture
  - Configure the device
  - Monitor bus or group telegram



KNX Protocol

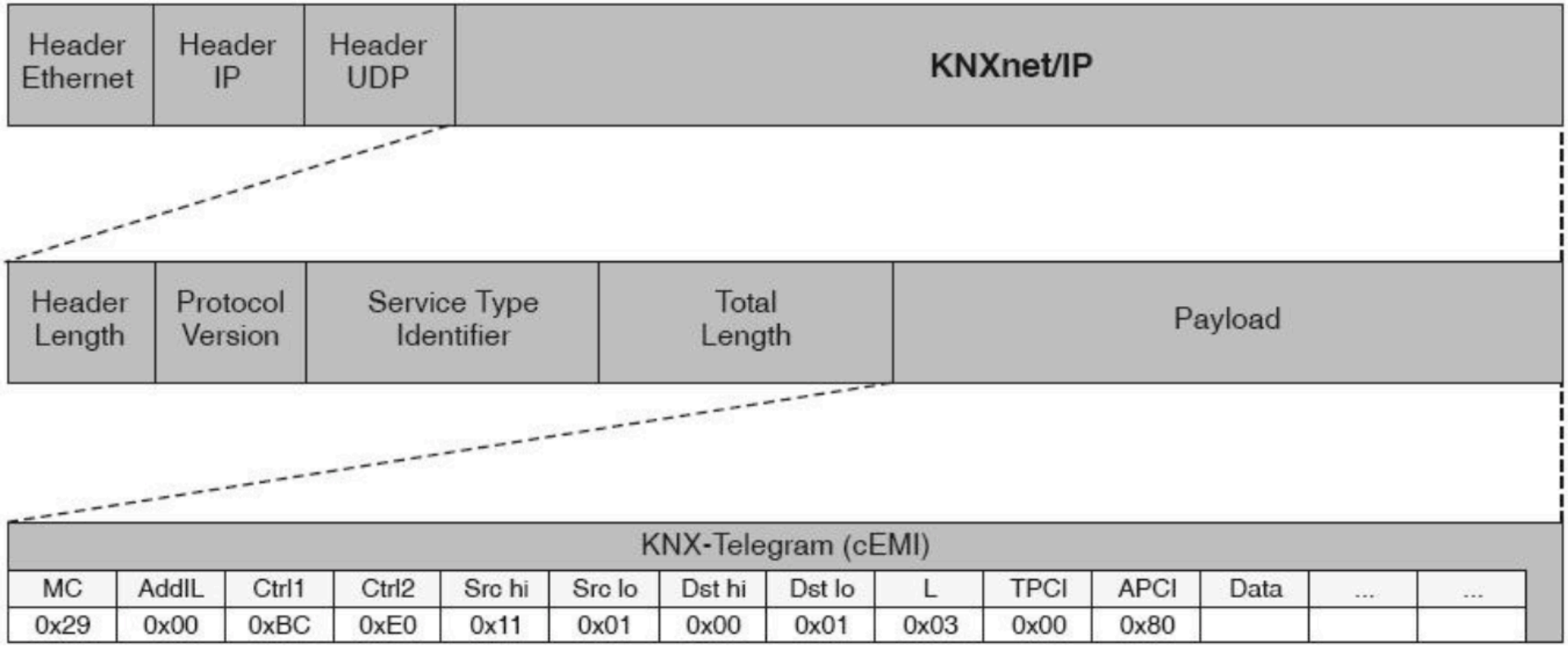
- KNX cEMI



_CEMI_APCI_TYPES
A_GroupValue_Write
A_Memory_Write
A_Restart
A_Authorize_Request
A_Key_Write

KNX Protocol

- KNXnet/IP
  - Encapsulated cEMI via UDP
  - Default port is 3671



KNX Protocol

- KNXnet/IP
  - Encapsulated cEMI via UDP
  - Default port is 3671
  - Protocol Reverse Engineering via Wireshark

```
◢ KNXnet/IP
  ◢ Header
      Header Length: 0x06
      Protocol Version: 0x10
      Service Type Identifier: ROUTING_INDICATION (0x0530)
      Total Length: 17 octets
  ◢ Body
    ◢ cEMI
        messagecode: L_Data.ind (0x29)
        add information length: 0 octets
      ▷ Controlfield 1: 0xb0
      ▷ Controlfield 2: 0x50
        Source Address 2.2.2
        Destination Address 1.1.2
        NPDU length: 1 octet
        01.. .... = TPCI: NDT (Numbered Data Packet) (0x1)
        ..00 00.. = sequence NCD/NDT: 0
        .... ..11  0000 0000 = APCI: A_DeviceDescriptor_Read (0x0300)
```

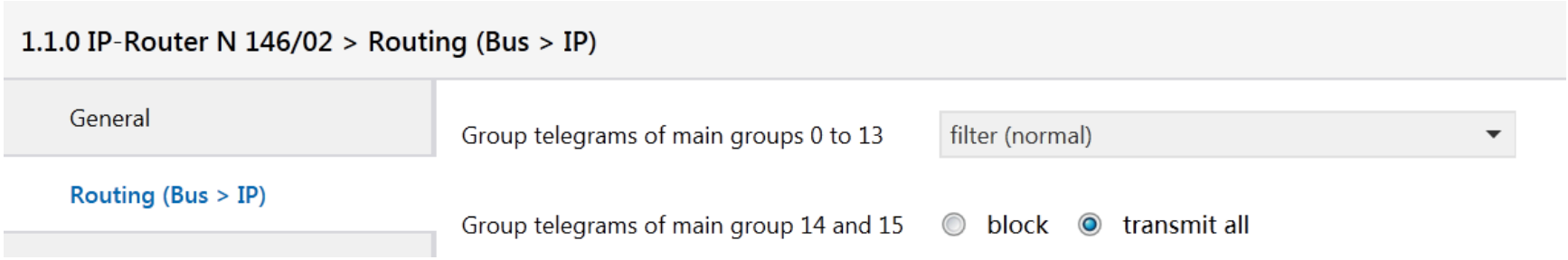
cEMI Here !

Tencent Security Platform Dpt.

Routing mechanism

- KNXnet/IP Router vs Interface
  - IP Interface supports KNXnet/IP Tunnelling only
  - IP Router also supports KNXnet/IP Routing

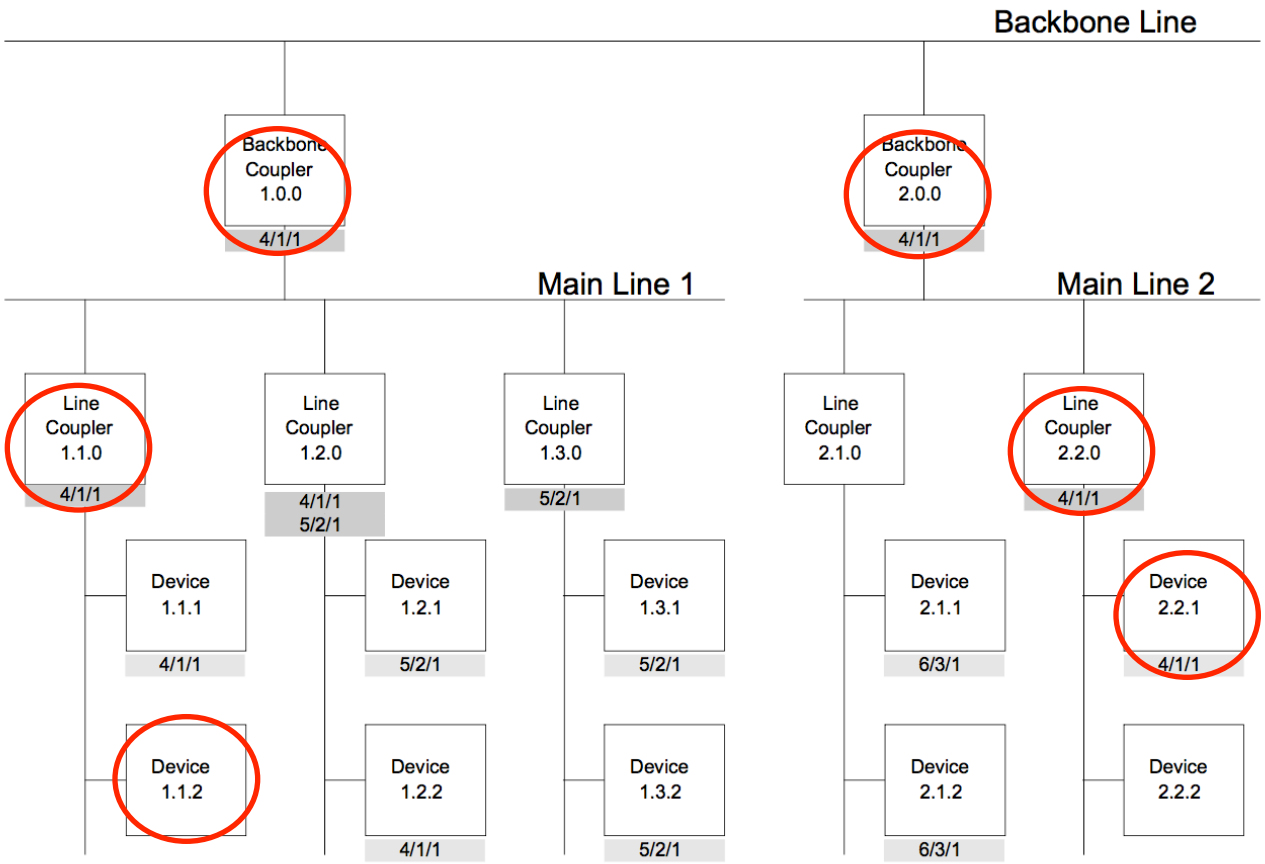
- Group Address Filtering
  - All KNX Group Address telegrams received by a KNXnet/IP Router shall be subject to Group Address filtering



Tencent Security Platform Dpt.

Routing mechanism

- Group Address Filtering



1.1.2 send 4/1/1
2.2.1 recv 4/1/1

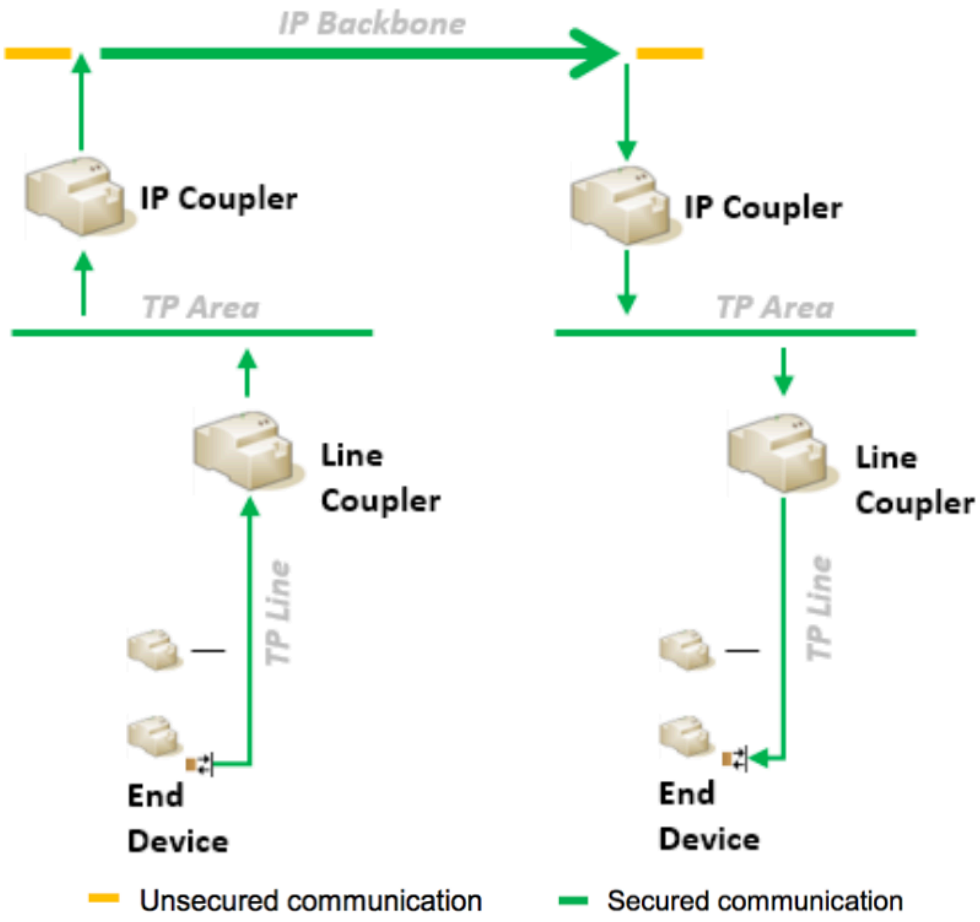
Tencent Security Platform Dpt.

KNX Security Model

- KNX Secure
  - KNX data secure
  - KNX IP secure
- Current Situation
- Attack Surface
  - The weakness of KNX protocol
  - Weak security awareness during installation

KNX Secure

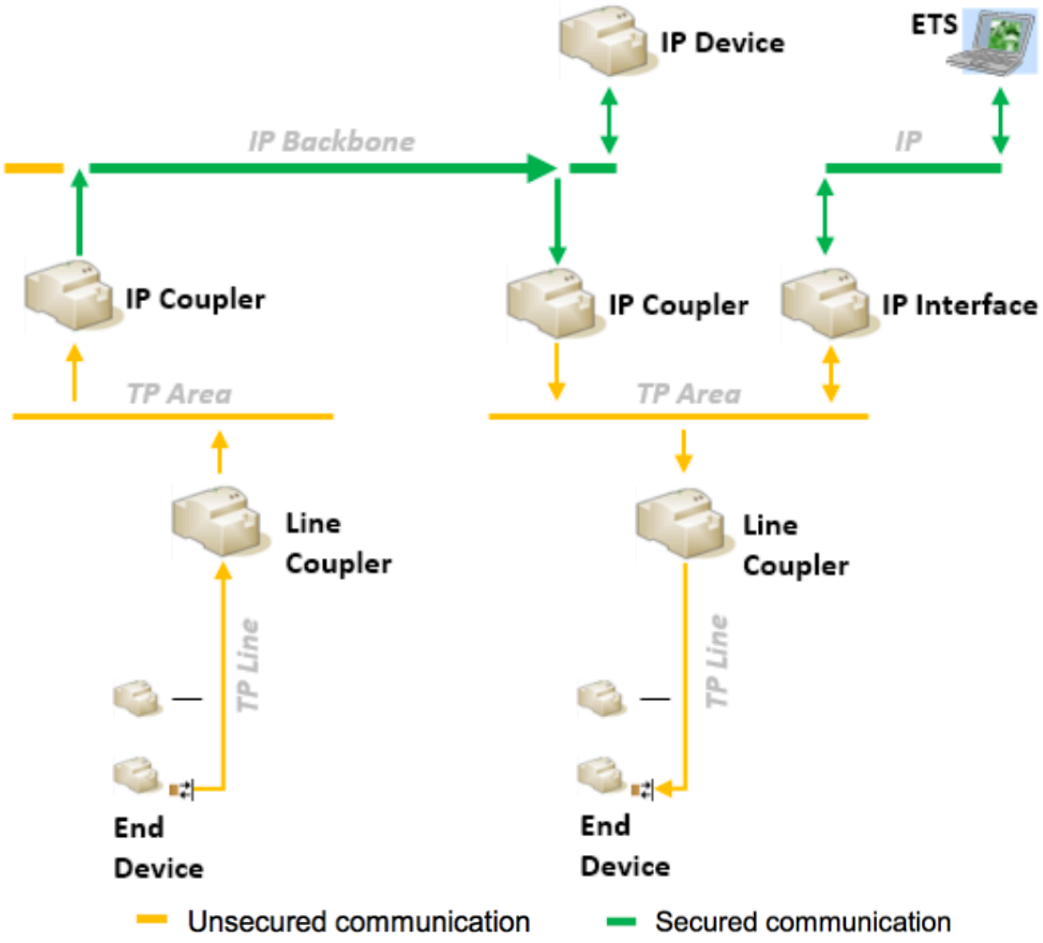
- KNX data secure
  - KNX Data Secure encrypts the APCI and the payload



Tencent Security Platform Dpt.

KNX Secure

- KNX IP secure
  - KNX IP Secure encrypts the entire KNXnet/IP frame



Tencent Security Platform Dpt.

Current Situation

- Attack surface still exists in most KNX networks
  - Some devices still do not support KNX secure.
  - Use earlier versions of ETS for installation
  - High renovation cost of existing buildings

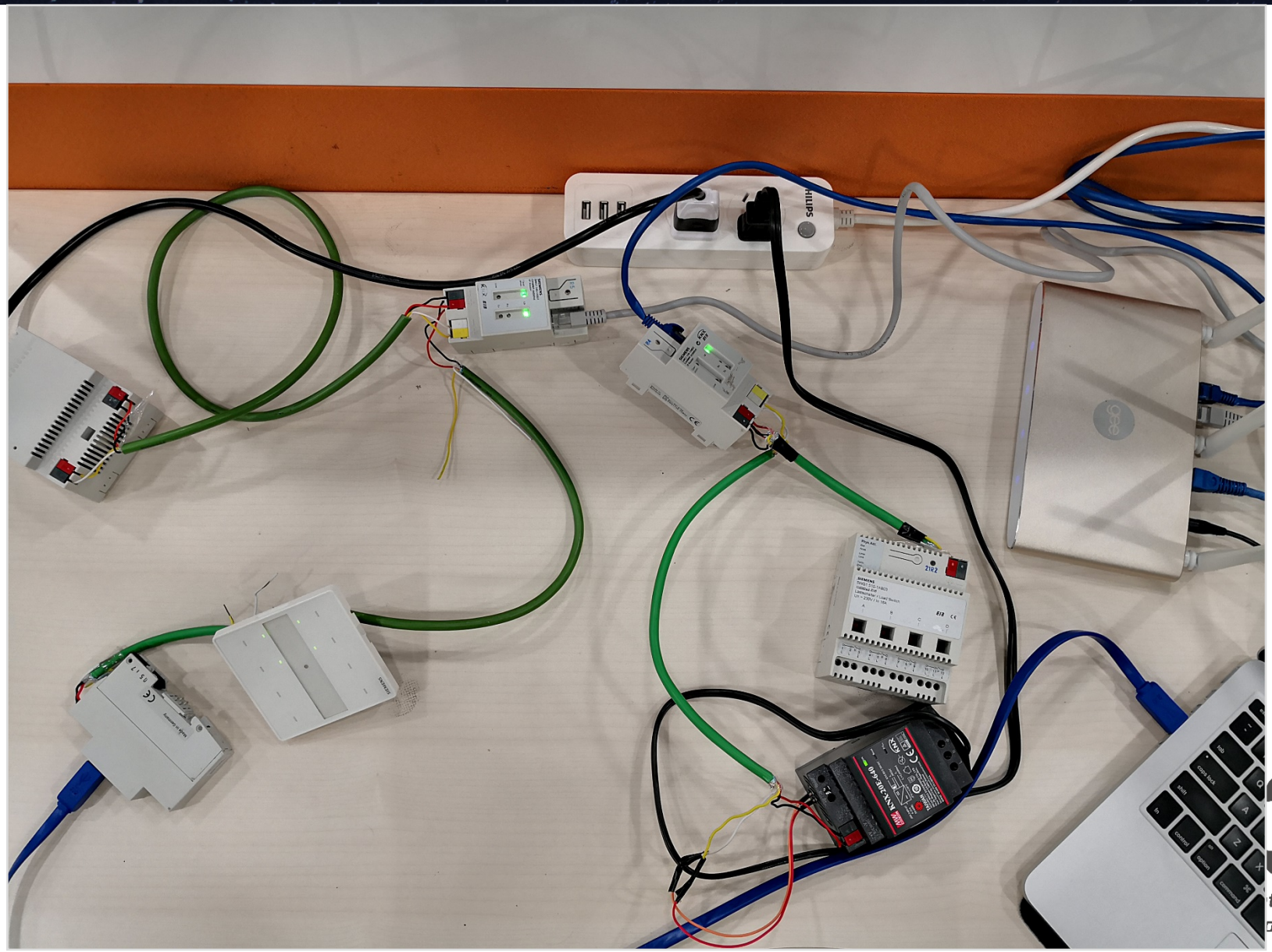
- Attack surface of KNX
  - The weakness of KNX protocol
  - Weak security awareness during installation

Attack Surface

- The weakness of KNX protocol
  - Traffic is not encrypted and can be sniffed
  - Unable to prevent replay attacks
  - Device can be reprogrammed

- Weak security awareness during installation
  - No isolation in each room
  - No set authentication key
  - No encryption and lack of access control in LAN

Experimental Setup



Experimental Setup

- KNX IP
  - IP-Router N146/02
- KNX USB
  - USB interface N148
- KNX Power
  - Power supply N125
- KNX Node
  - Load switch N 510
  - Arina touch sensor
- Router

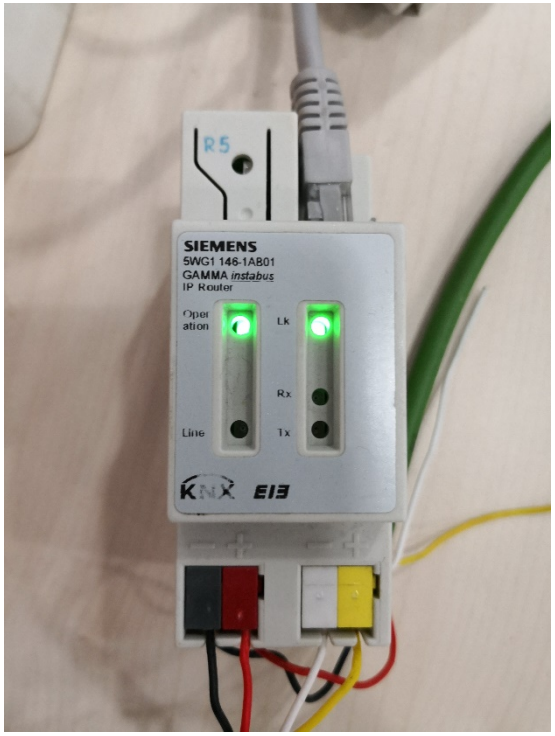
Tencent Security Platform Dpt.

Experimental Setup

- Tools for attack
  - ETS (https://www.knx.org/za/software/overview/index.php)
  - KNXmap (https://github.com/takeshixx/knxmap/)
  - Calimero (https://github.com/calimero-project)
  - Net'n Node (https://www.weinzierl.de/index.php)

Attack KNX Network via KNXnetIP

- Step1: Enter the LAN where KNX is located
  - Cracking WiFi password / Weak password
  - Access switchs physically in the room

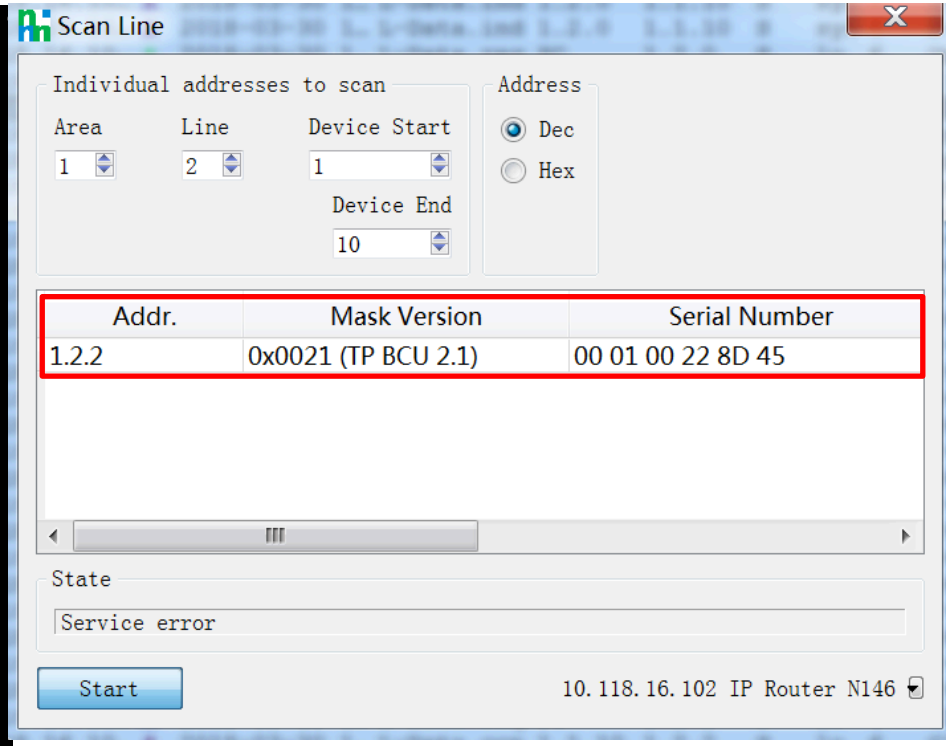


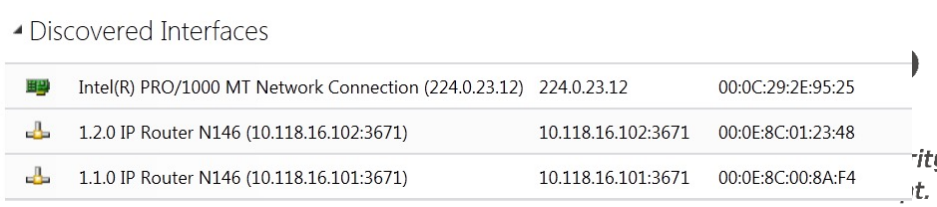
Tencent Security Platform Dpt.

Attack KNX Network via KNXnetIP

- Step2: Discover devices and build topology
  - Scan couplers and devices

```
C:\Users\lulu\knxmap-master>python main.py scan 10.
Scanning 1 target(s)

10.118.16.101
   Port: 3671
   MAC Address: 00:0E:8C:00:8A:F4
   KNX Bus Address: 1.1.0
   Additional Bus Addresses:
      1.1.9
   KNX Device Serial: 0001002043BE
   KNX Medium: KNX TP
   Manufacturer: Siemens
   Device Friendly Name: IP Router N146
   Device Status:
      Programming Mode: ENABLED
      Link Layer: disabled
      Transport Layer: disabled
      Application Layer: disabled
      Serial Interface: disabled
      User Application: disabled
      BC DM: 0
   Project Install Identifier: 0
   Supported Services:
      KNXnet/IP Core
      KNXnet/IP Device Management
      KNXnet/IP Tunnelling
      KNXnet/IP Routing
```





Attack KNX Network via KNXnetIP

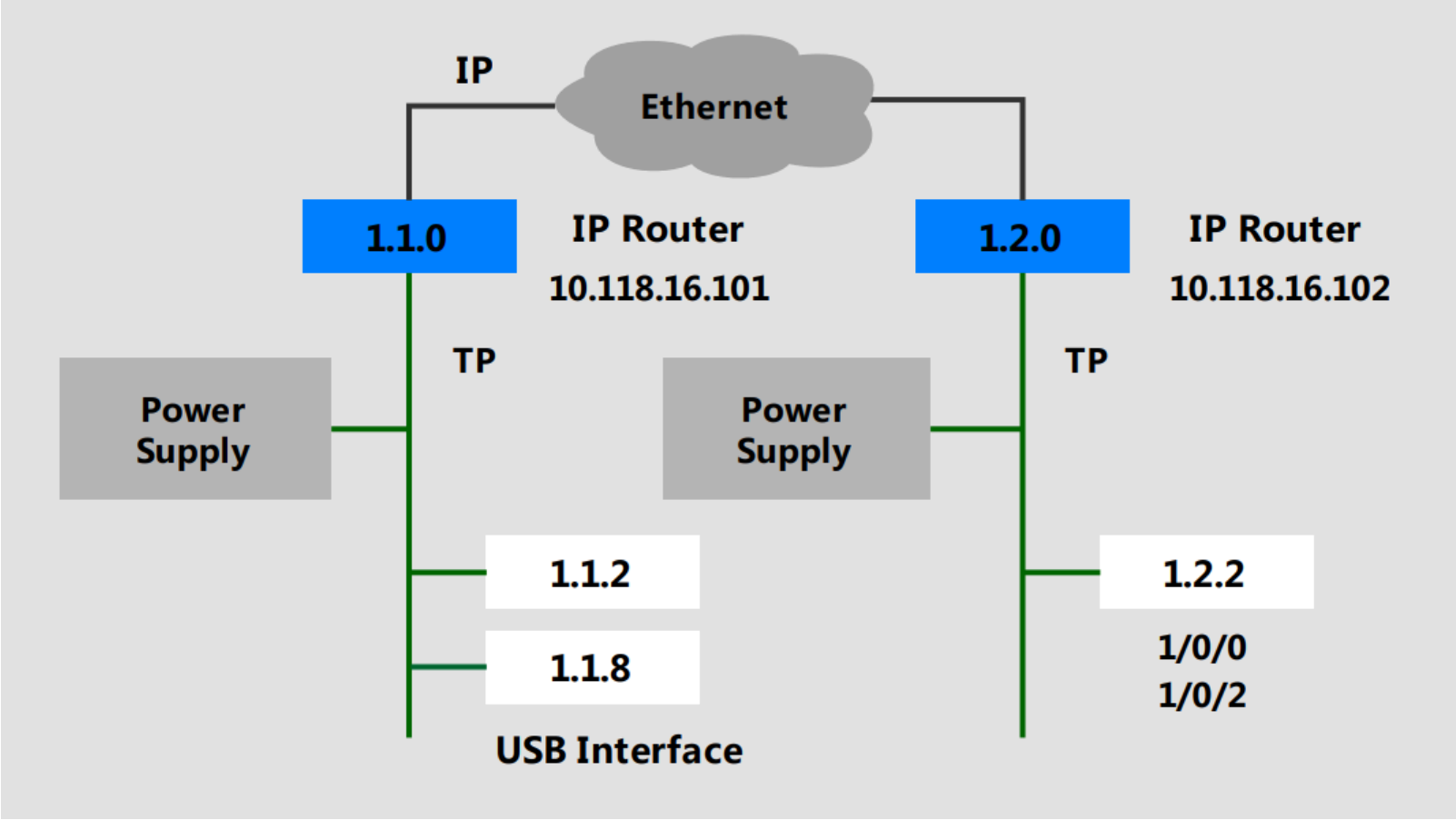
- Step2: Discover devices and build topology
  - Scan couplers and devices
  - Monitor group telegram / Sniff LAN traffic
  - Guess the group address of the other rooms

Interface	↕	Service	Src-Addr	Dest-Addr	Control	Prio	H-C	TPCI	;equ	APCI	AL-Data
10.118.16.102 ..	↑	L-Data.ind	15.15.255	1/0/0	S	sys	6	U-...		GrpValWrite	Data=0x01
10.118.16.102 ..	↑	L-Data.ind	15.15.255	1/0/0	S	sys	6	U-...		GrpValWrite	Data=0x00
10.118.16.102 ..	↑	L-Data.ind	1.2.2	1/0/2	S	lo	6	U-...		GrpValWrite	Data=0x00
10.118.16.102 ..	↓	L-Data.req	PC	1/0/2	S !R	lo	6	U-...		GrpValRead	
10.118.16.102 ..	↑	L-Data.con	1.1.10	1/0/2	S R	lo	6	U-...		GrpValRead	
10.118.16.102 ..	↑	L-Data.ind	1.2.2	1/0/2	S	lo	6	U-...		GrpValResp	Data=0x00
10.118.16.102 ..	↓	L-Data.req	PC	1/0/0	S	lo	6	U-...		GrpValWrite	Data=0x00
10.118.16.102 ..	↑	L-Data.con	1.1.10	1/0/0	S	lo	6	U-...		GrpValWrite	Data=0x00
10.118.16.102 ..	↑	L-Data.ind	15.15.255	1/0/0	S	sys	6	U-...		GrpValWrite	Data=0x01
10.118.16.102 ..	↑	L-Data.ind	1.2.2	1/0/2	S	lo	6	U-...		GrpValWrite	Data=0x01

Tencent Security Platform Dpt.

Attack KNX Network via KNXnetIP

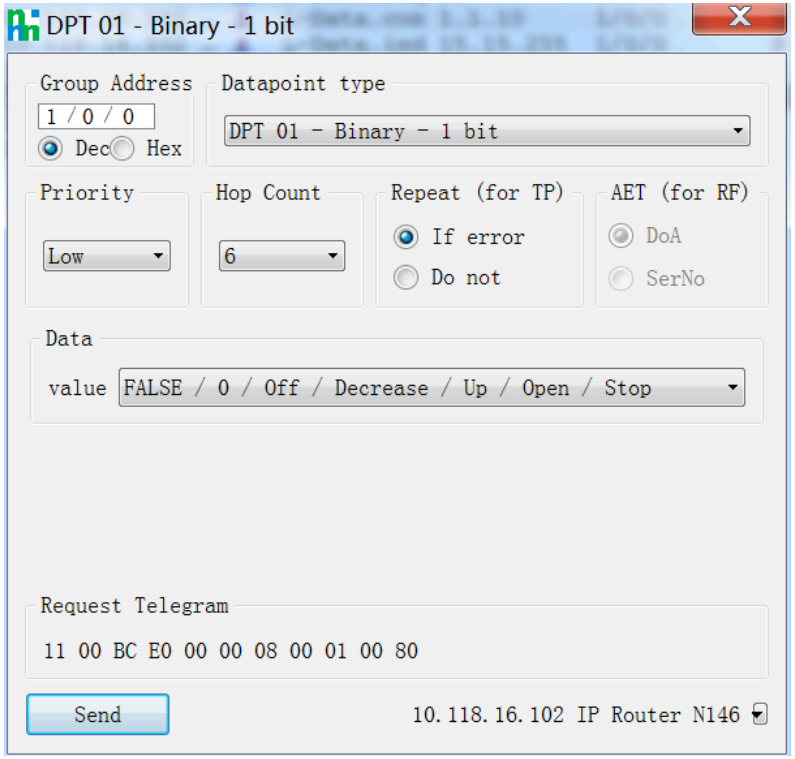
- Step2: Discover devices and build topology



Tencent Security Platform Dpt.

Attack KNX Network via KNXnetIP

- Step3: Send malicious data for attack
  - Traversing the IP of all couplers and send data
  - Send group telegram to control devices
  - Send APCI data to devices

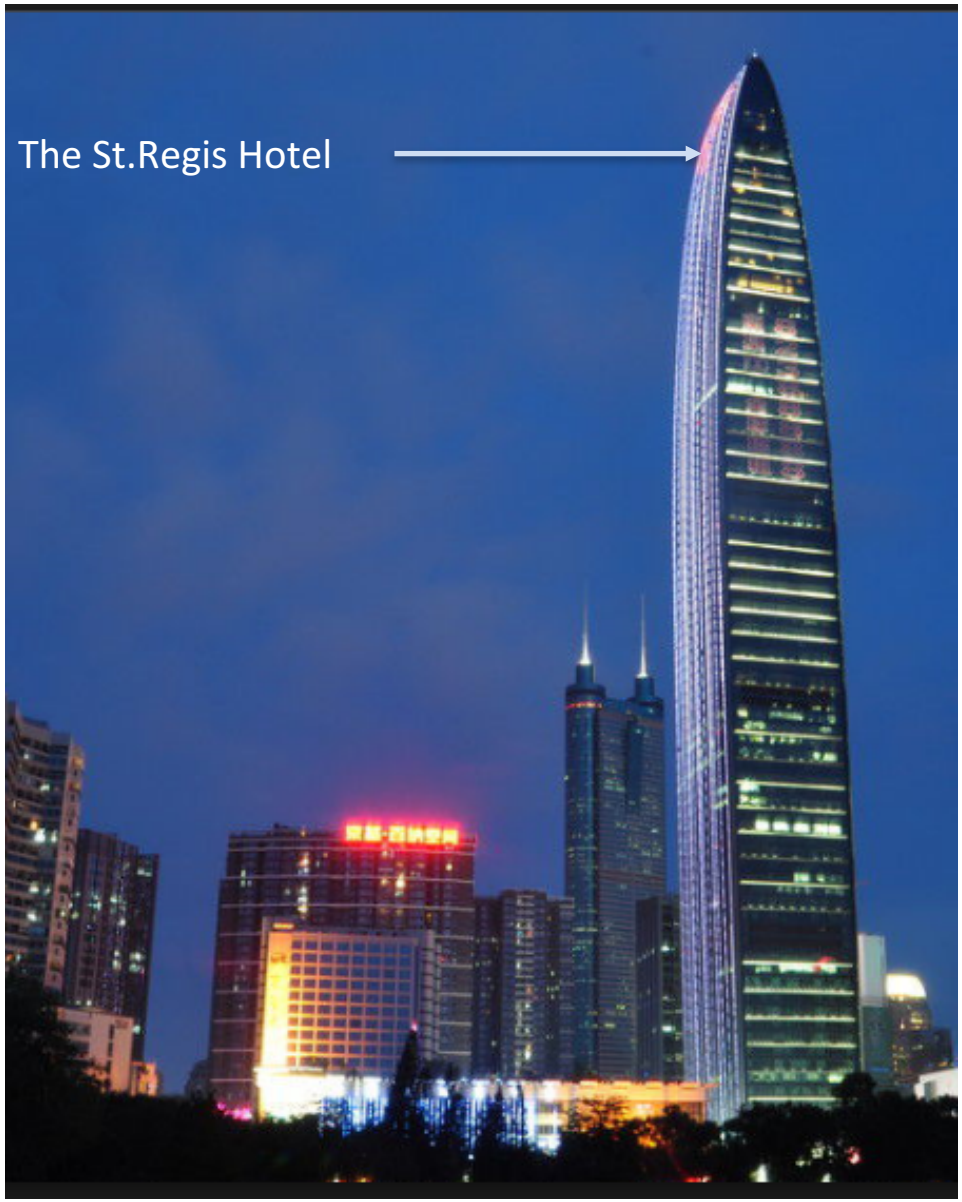



```
C:\Users\lulu\knxmap-master>python main.py apci 10.118.16.102 1.2.2 Progmode
Programming mode disabled

C:\Users\lulu\knxmap-master>python main.py apci 10.118.16.102 1.2.2 Memory_Read
--memory-address 0x0060
b'2e'

C:\Users\lulu\knxmap-master>python main.py apci 10.118.16.102 1.2.2 Restart

C:\Users\lulu\knxmap-master>python main.py apci 10.118.16.102 1.2.2 Memory_Write
 --memory-address 0x0060 --memory-data af
```

Tencent Security Platform Dpt.

Attack KNX Network via KNXnetIP

In DefCon 22, a security researcher showed how to hack the lighting control system in the St.Regis Hotel via the hotel's WIFI network.



If Ethernet is isolated ?

Maybe.. Attack KNX network via KNX TP.

Real-world attack?

Attack KNX Network via KNX TP

Marriott Hotel

- 340 rooms
- 300 meters
- Ocean view

Tencent Security
Platform Dpt.

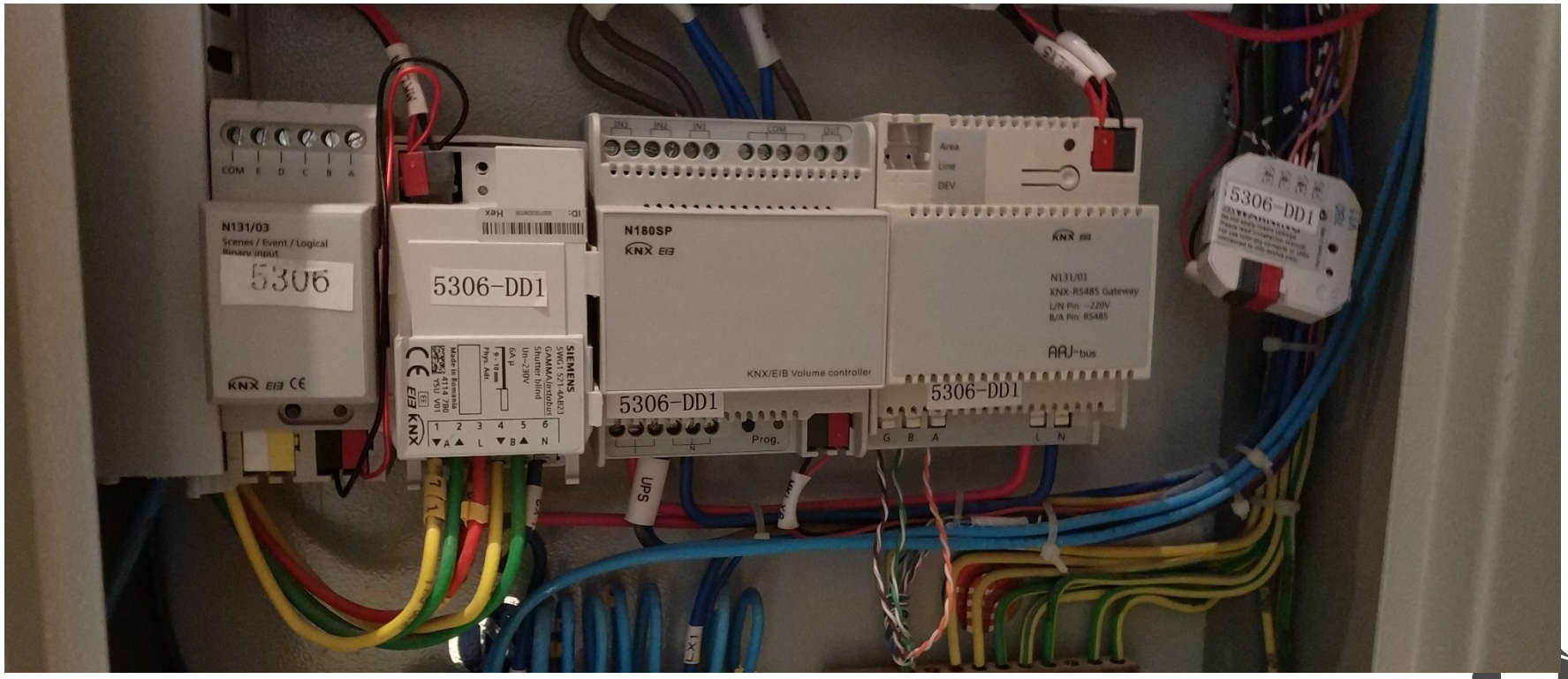
Attack KNX Network via KNX TP

You can use KNX smart panel control in your room, including features such as :

- Light switch with brightness
- Air conditioning temperature
- TV switch
- Music switch
- Curtain switch
- But, Ethernet is isolated

Attack KNX Network via KNX TP

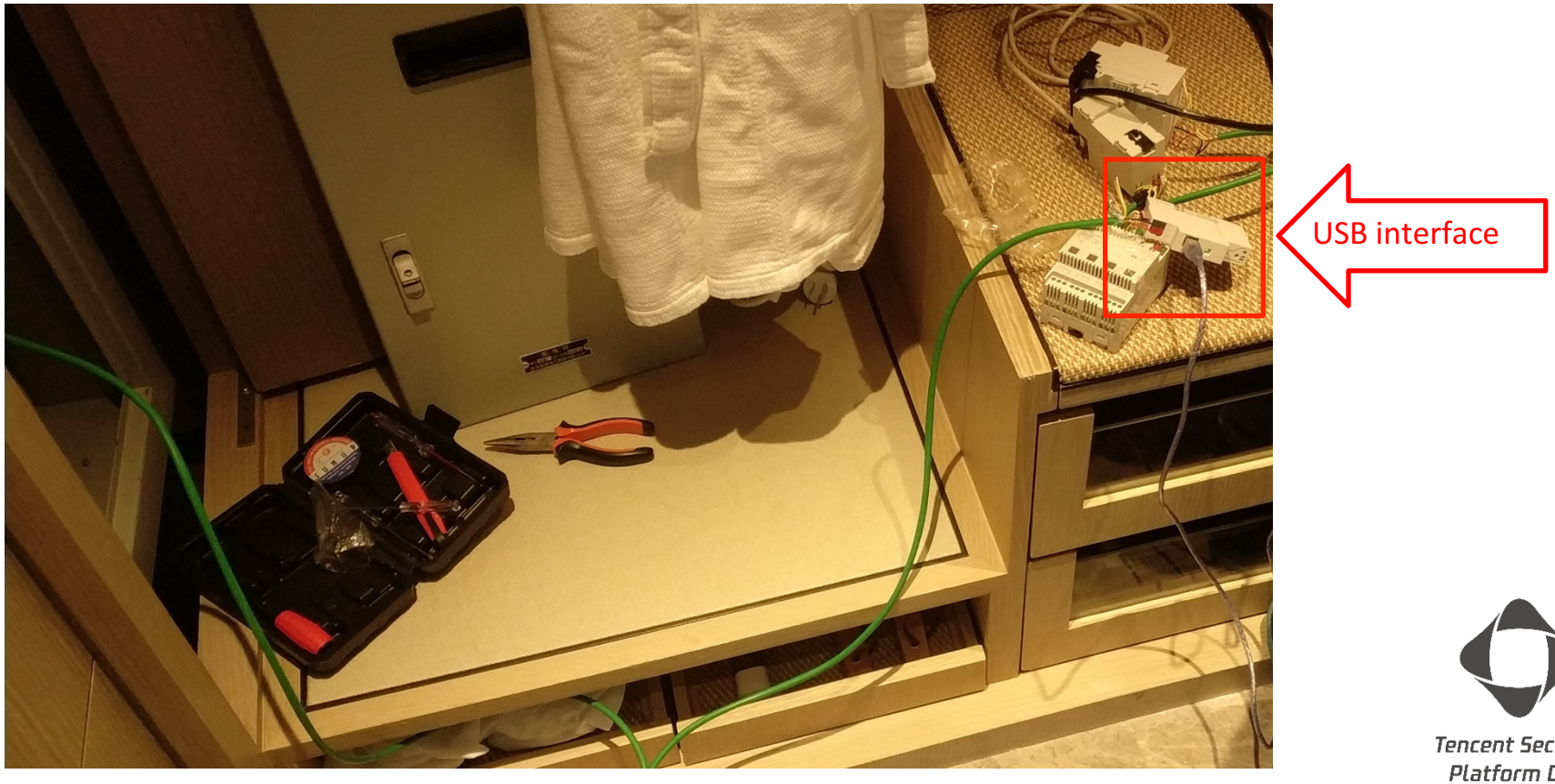
- Step1: Enter the BUS where KNX is located
  - Look for KNX devices in the room



Tencent Security
Platform Dpt.

Attack KNX Network via KNX TP

- Step1: Enter the Bus where KNX is located
  - Look for KNX devices in the room
  - Access KNX network via TP and USB Interface



Tencent Security
Platform Dpt.

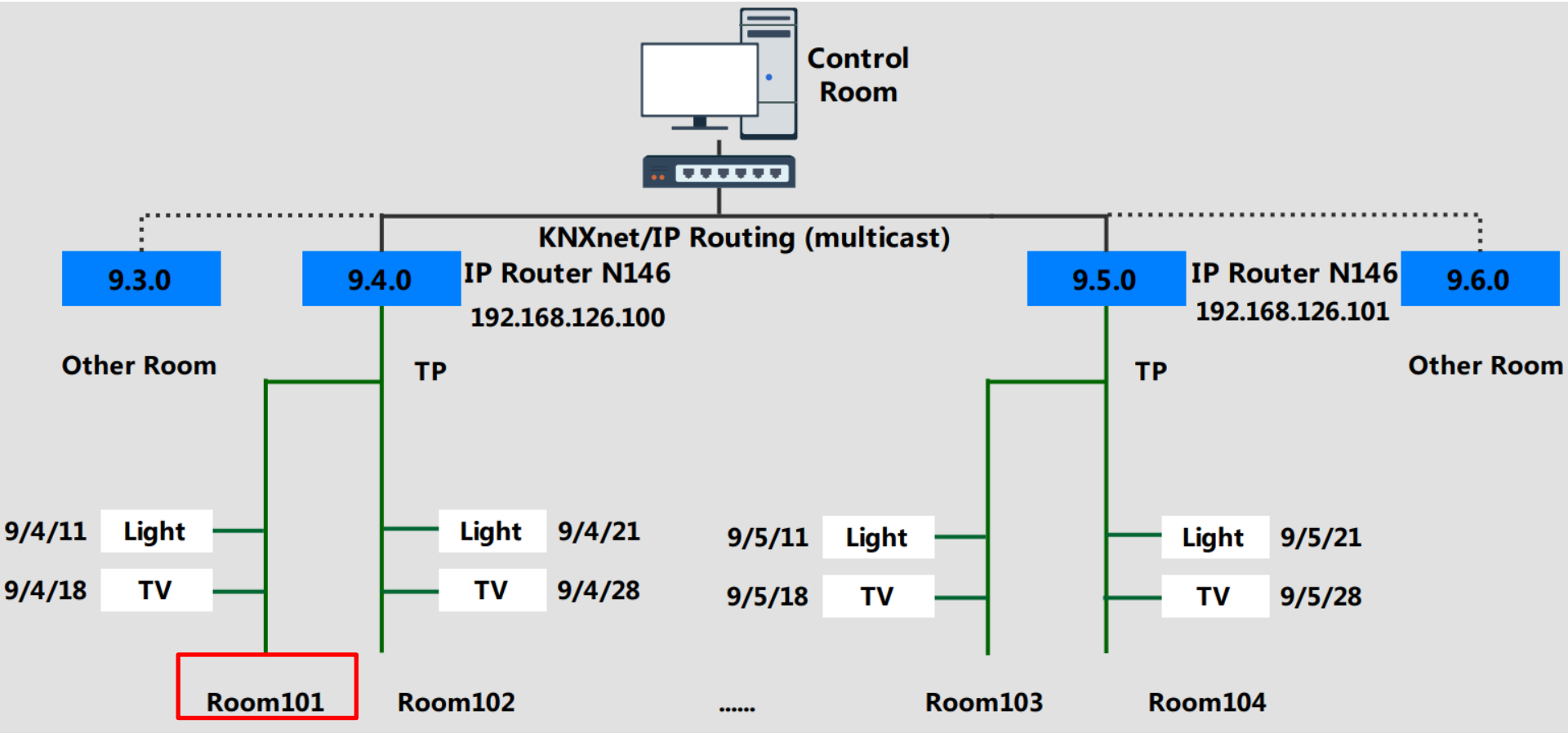
Attack KNX Network via KNX TP

- Step2: Discover devices and build topology
  - Monitor group telegram or bus data
  - Scan the device on Line
  - Get the coupler's detail

Name	Value
KNXnet/IP server	9.4.0
name	IP Router N146
Supported IP assignment methods	manual, DHCP, Auto IP
Enabled IP assignment methods	manual
Current IP assignment method	manual
Routing capabilities	queue overflow statistics, transmitted telegrams statistics,
Configured IP address	192.168.126.100
Configured subnet mask	255.255.255.0
Current IP address	192.168.126.100
Current subnet mask	255.255.255.0
Configured default gateway	192.168.126.254
Current default gateway	192.168.126.254
DHCP/BootP server	0.0.0.0
Routing multicast	224.0.23.12

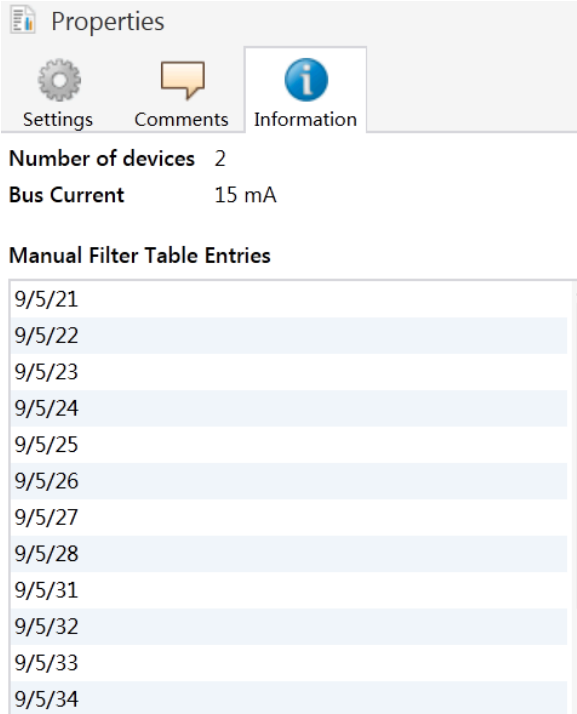
Attack KNX Network via KNX TP

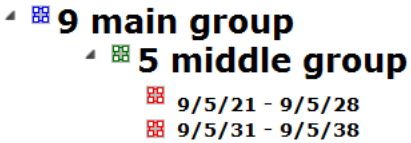
- Step2: Discover devices and build topology
  - IP Router as coupler and share with two rooms
  - Guess the group address in the other rooms



Attack KNX Network via KNX TP

- Step3: Modify group filter tables
  - Brute-force cracking authentication key (the default is 0xFFFFFFFF)
  - Send APCI data to enable program mode
  - Use ETS to configure group filter tables on each Line

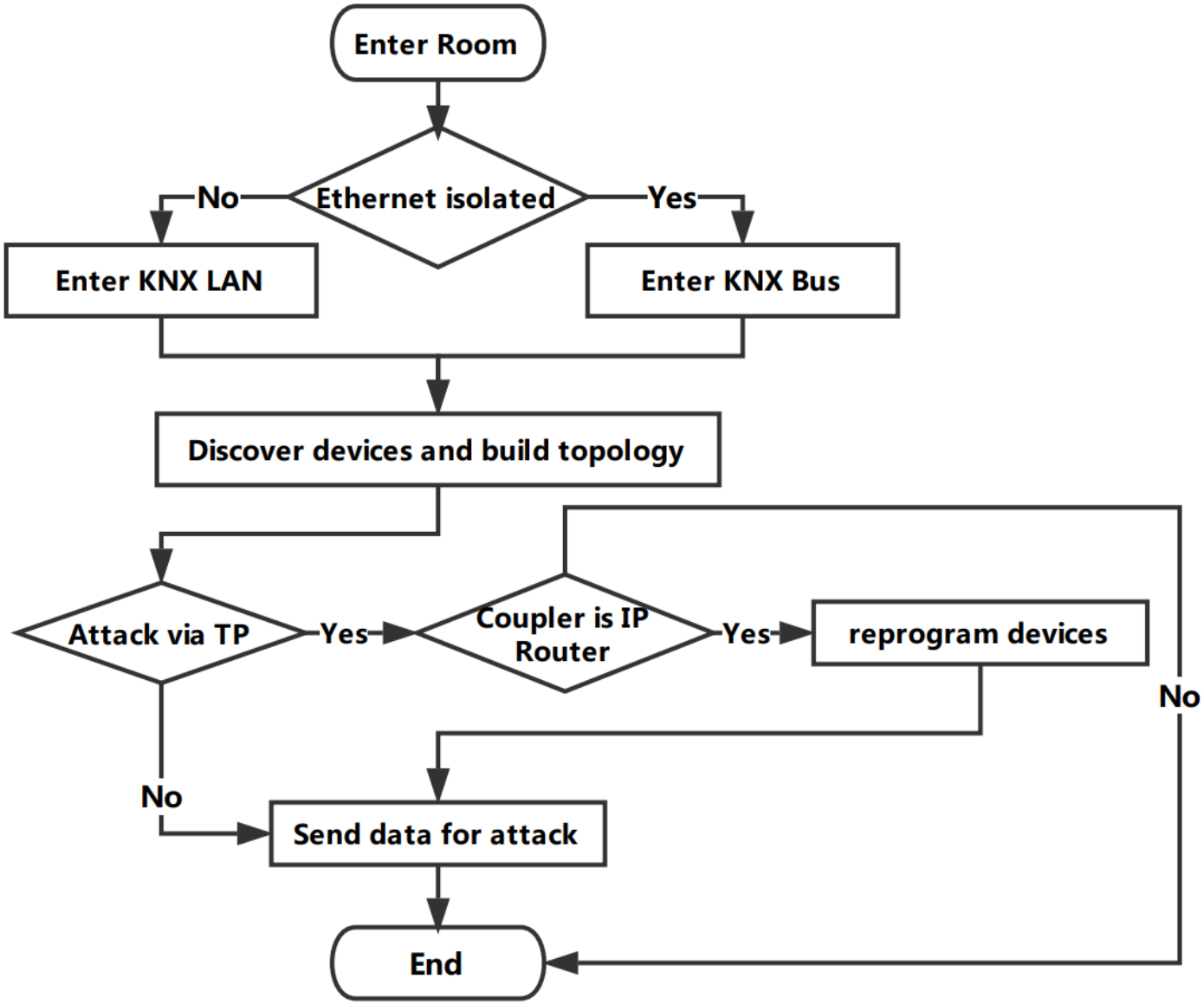




Attack KNX Network via KNX TP

- Step4: Send malicious data for attack
  - Traversing all devices and send data
  - Send group telegram to control devices on the other line
  - Send APCI data to devices

Attack KNX Network



Tencent Security Platform Dpt.

Security Advice

- ZigBee Security Advice
- KNX Security Advice

ZigBee Security Advice

- Update network keys regularly.
- Don’t use any well-known security key.
- Implement custom secure encryption in the application layer (If do not need to be compatible with other devices).

KNX Security Advice

- Don't expose KNX gateways on public networks.
- Make sure each room is isolated .
- Ensure network security including WiFi and switches.
- Use new devices and the latest version of ETS to implement KNX secure.

Tencent Security
Platform Dpt.

Thank You

blade@tencent.com

Tencent Security
Platform Dpt.

Reference

KNX Basics
http://www.knx.org/media/docs/Flyers/KNX-Basics/KNX-Basics_en.pdf

EMI FT12 Message Format
http://www.dehof.de/eib/pdfs/EMI-FT12-Message-Format.pdf

Using KNX Secure in ETS5
http://www.knx.it/download/DOCUMENTAZIONE_KNX/07_M.Vettorato_-_KNX_Secure_-_Use_in_ETS5.pdf

KNX Secure Position Paper_en.pdf
https://www.knx.org/knx-en/Landing-Pages/KNX-Secure/Useful-Material/KNX-Secure-Position-Paper_en.pdf

A Practical Attack Against a KNX-based Building Automation System
https://ewic.bcs.org/upload/pdf/ewic_icscsr14_paper7.pdf

DEFCON-22-Jesus-Molina-Learn-how-to-control-every-room.pdf
https://www.defcon.org/images/defcon-22/dc-22-presentations/Molina/DEFCON-22-Jesus-Molina-Learn-how-to-control-every-room.pdf

Security in KNX or how to steal a skyscraper
http://2015.zeronights.org/assets/files/20-Litvinov.pdf

Building management systems for providing security in existing KNX projects: Organizational measures and device monitoring
https://www.netxautomation.com/netx/images/downloads/Pr%C3%A4sentationen/EN/KNX%20Secure%20EN.pdf

How to Solve It: Manually Adding Group Addresses to the Filter Table
http://knxtoday.com/2015/01/5286/how-to-solve-it-manually-adding-group-addresses-to-the-filter-table.html

Security Analysis of Zigbee
https://courses.csail.mit.edu/6.857/2017/project/17.pdf

zigbee: Securing the Wireless IoT
http://www.zigbee.org/download/new-white-paper-zigbee-securing-the-wireless-iot/

MAXIMIZING SECURITY IN ZigBee NETWORKS
https://www.nxp.com/docs/en/supporting-information/MAXSECZBNETART.pdf

ZIGBEE EXPLOITED - The good, the bad and the ugly
https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf

What's New in ZigBee 3.0
http://processors.wiki.ti.com/index.php/What's_New_in_ZigBee_3.0

Insecure to the Touch: A acking ZigBee 3.0 via Touchlink Commissioning
https://www1.cs.fau.de/filepool/publications/wisec2017_touchlink.pdf