

TRACK 2

HITBSECCONF

AMSTERDAM - 2021

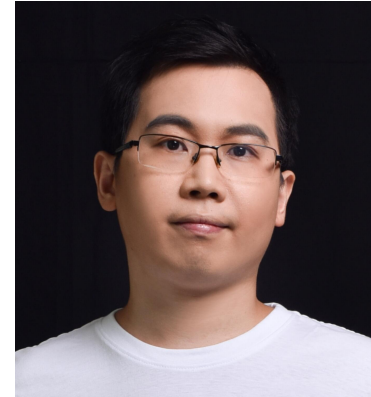
Insecure Link : Security Analysis and Practical Attacks of LPWAN

Li YuXiang & Wu HuiYu
Tencent Blade Team

About US

Li YuXiang (@Xbalien29)

Senior security researcher at Tencent Blade Team. Focusing on mobile security and IoT security. Reported multiple vulnerabilities of Chrome & Android. Speaker of BlackHat USA, DEFCON 27, CanSecWest, HITB AMS 2018.



Wu HuiYu (@NickyWu_)

Senior security researcher at Tencent Blade Team. Mainly focusing on AIoT security research. Bug hunter, Winner of GeekPwn 2015 & 2020, and speaker of Black Hat USA, DEFCON, HITB, CanSecWest and POC.



About Tencent Blade Team

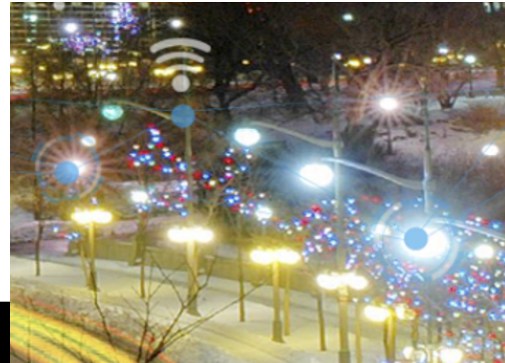
- Founded by Tencent Security Platform Department in 2017
- Focus on security research in the areas of AIoT and Cloud virtualization
- Report 200+ vulnerabilities to vendors such as Google, Apple, Microsoft, Amazon
- More about us : <https://blade.tencent.com>

Agenda

- Introduction to LPWAN Supply Chain
- New Security Risks of LoRaWAN and Our Practice
- Security Internal of NB-IoT
- Security Advice

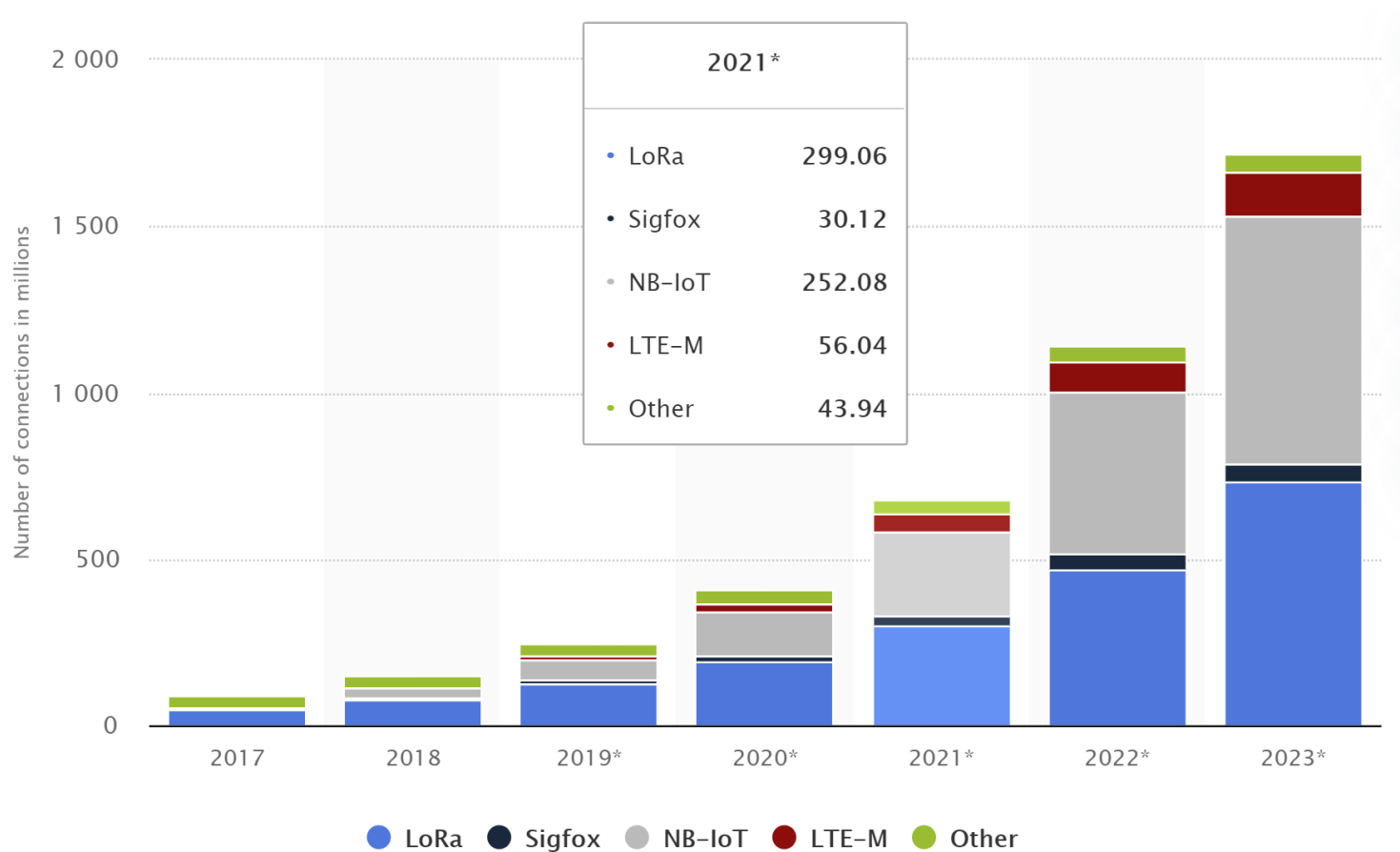
What is LPWAN

- LPWAN (Low Power Wide Area Network)
 - Low power and low bit rate for long-distance communication.
- Mainstream LPWAN technology
 - LoRa, NB-IoT, sigfox...
- Application Scenarios



The Motivation of Our Work

- LPWAN Market Share Trends



LoRa/LoRaWAN

- LoRa (Long Range) is a proprietary low-power wide-area network modulation technique. It is based on spread spectrum modulation techniques derived from chirp spread spectrum (CSS) technology
- It use unlicensed frequency bands, such as 470, 868, 915 MHz, which can independently build gateways and core networks
- LoRaWAN is a cloud-based medium access control (MAC) layer protocol but acts mainly as a network layer protocol for managing communication between LPWAN gateways and end-node devices as a routing protocol, maintained by the LoRa Alliance.

NB-IoT

- NB-IoT is a new IoT technology set up by 3GPP as a part of Release 13. Although it is integrated into the LTE standard, it can be regarded as a new air interface.
- It uses the licensed frequency bands, which are the same frequency numbers used in LTE, and employs QPSK modulation.
- There are different frequency band deployments, which are stand-alone, guard-band, and in-band deployment

LPWAN Supply Chain

Cloud



Telecom Operator

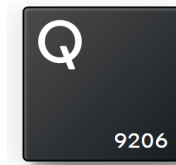
Product



Module



Chip

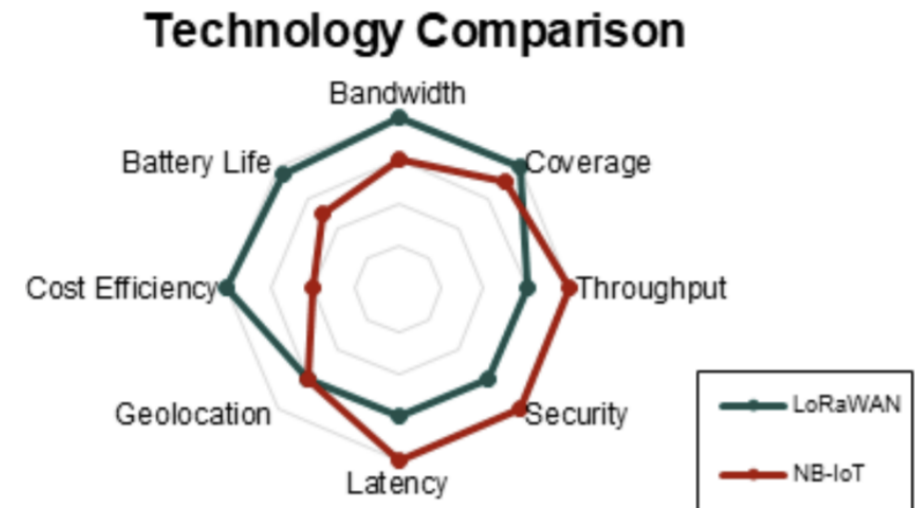


LoRaWAN vs NB-IoT

- Technical Characteristics

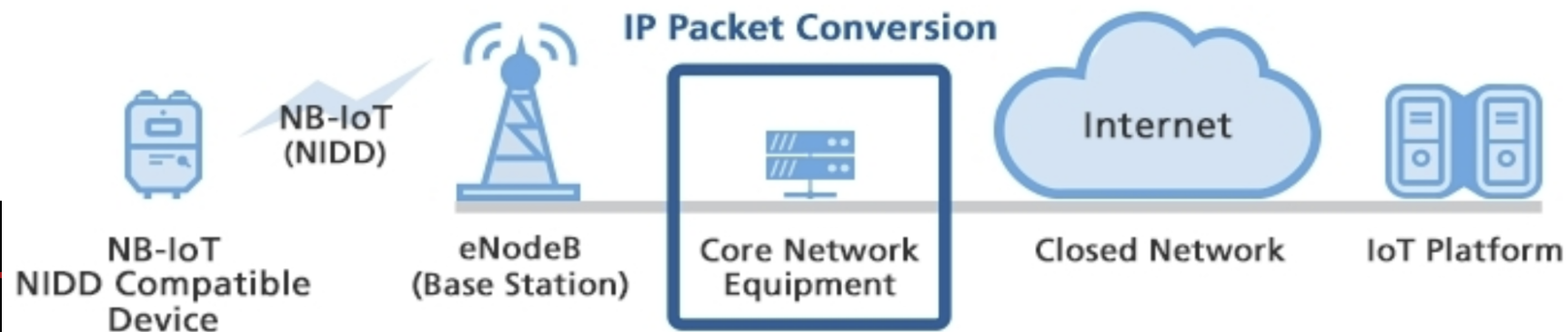
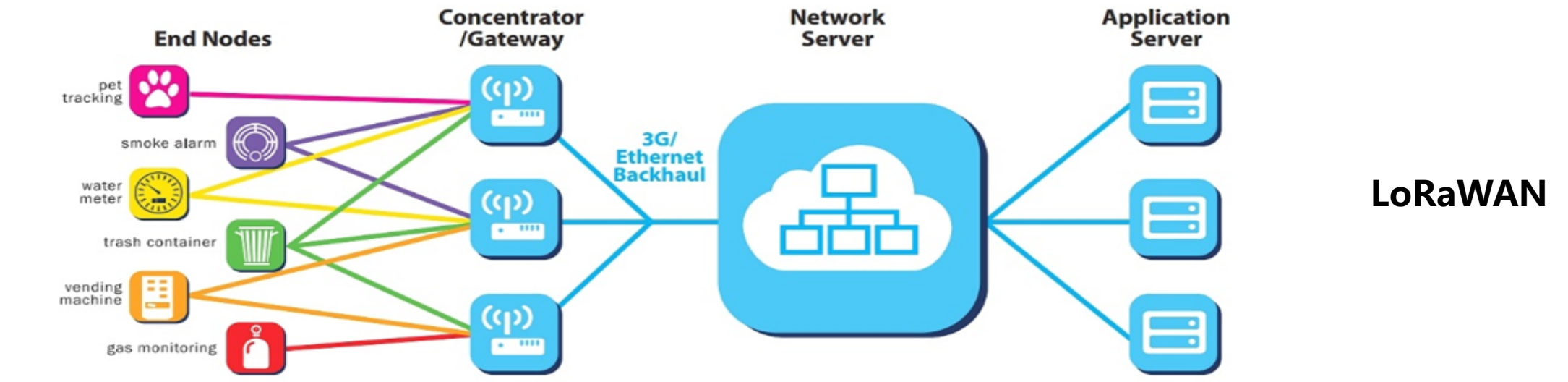
Technology Parameters	LoRaWAN	NB-IoT
Bandwidth	125 kHz	180 kHz
Coverage	165 dB	164 dB
Battery Life	15+ years	10+ years
Peak Current	32 mA	120 mA
Sleep Current	1µA	5µA
Throughput	50 Kbps	60 Kbps
Latency	Device Class Dependent	< 10 s
Security	AES 128 bit	3GPP (128 to 256 bit)
Geolocation	Yes (TDOA)	Yes (in 3GPP Rel 14)
Cost Efficiency (Device and Network)	High	Medium

Source: ABI Research



LoRaWAN vs NB-IoT

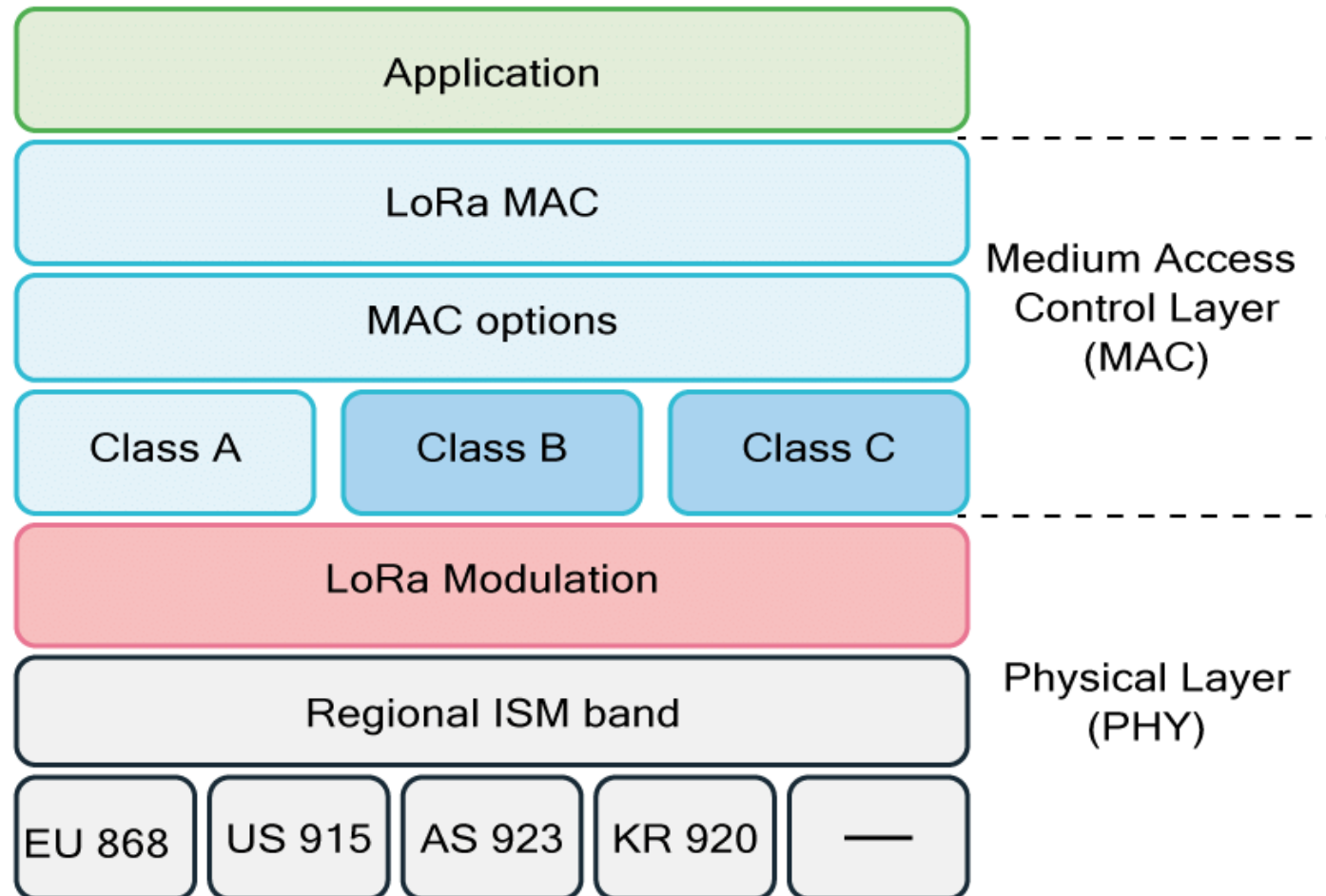
- Network Architecture



NB-IoT



LoRaWAN Protocol v1.0.3



The Key to the LoRaWAN Protocol v1.0.3

- The security basis of the protocol: AES (encryption, integrity)
 - AppKey : stored in the node and server, used to generate the session key
 - NwkSKey/AppSKey : Session key, used for encryption, decryption and MIC verification
- End-Device Activation
 - ABP : Node and server settings NwkSKey, AppSKey (will not change during the life cycle)
 - OTAA : Key negotiation process in which the session key is generated by AppKey

Previous Security Research

- LoRaWAN
 - Security issues of the specification (v1.0.3) > Fixed by v1.1 of the specification
 - Security risks of LoRaWAN deployment > Improve Vendors's security awareness
- NB-IoT
 - There are few studies, most of which is survey or theory

Security Risks of LoRaWAN Devices in the Real World

- Some vendors have security solutions
 - Random key / one-machine-one-key
 - Security specification for hardware
- Another part of vendors has weak security awareness
 - Use the same AppKey or a well-known AppKey
 - The AppKey is easy to guess or displayed on the device shell
 - The debug port is exposed or the firmware can be read

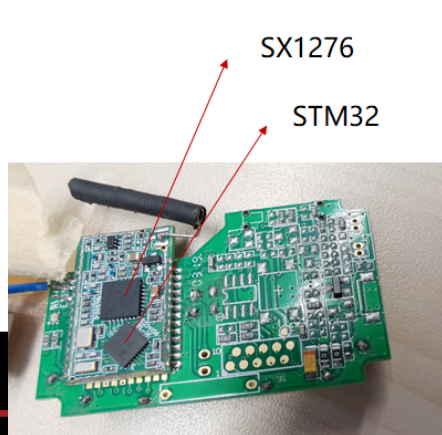
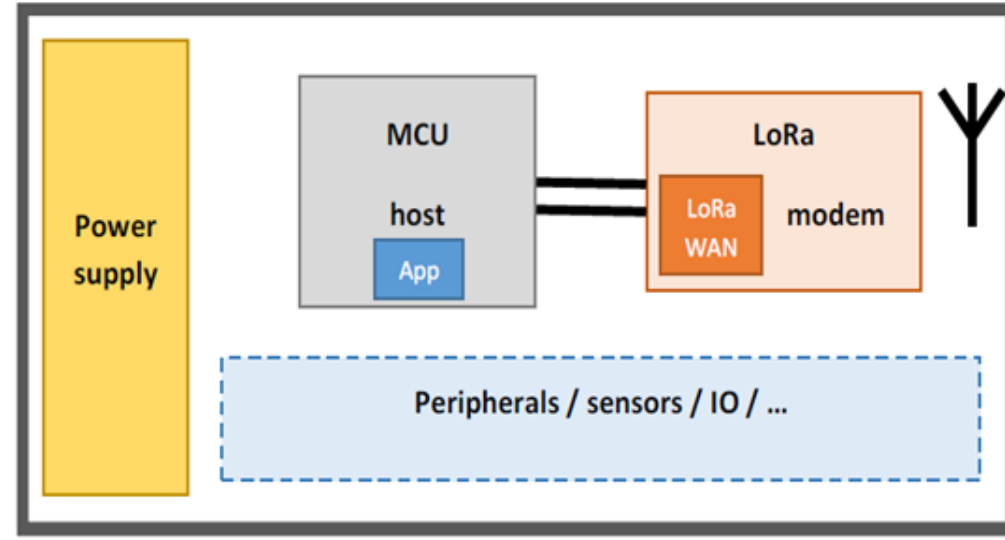
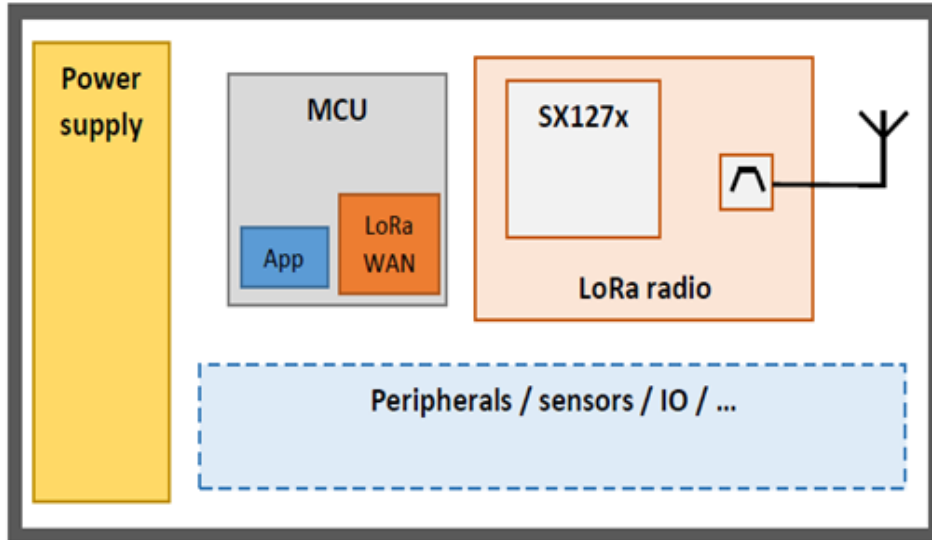
LoRaDawn: New Security Risks of LoRaWAN and Our Practice

- Technology Implementation in the Real World
- Attack Surface of LoRaWAN Supply Chain
- Our Practice

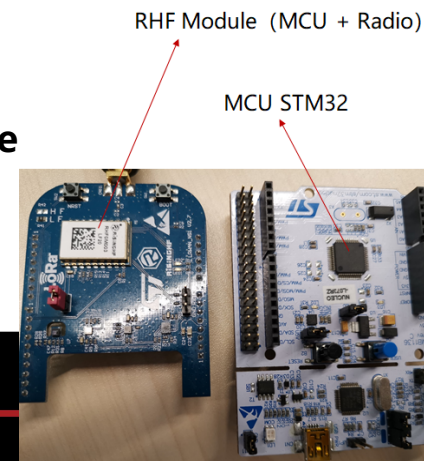
Open Source Implementation in LoRaWAN Supply Chain

- LoRaWAN Nodes
 - LoRaMac-node: <https://github.com/Lora-net/LoRaMac-node>
- LoRaWAN Gateways
 - Packet_forwarder: https://github.com/Lora-net/packet_forwarder
 - Basicstation: <https://github.com/lorabasics/basicstation>
- LoRaWAN Servers
 - Chirpstack: <https://github.com/brocaar>
 - TTN: <https://github.com/TheThingsNetwork/lorawan-stack>

Architecture of LoRaWAN Nodes



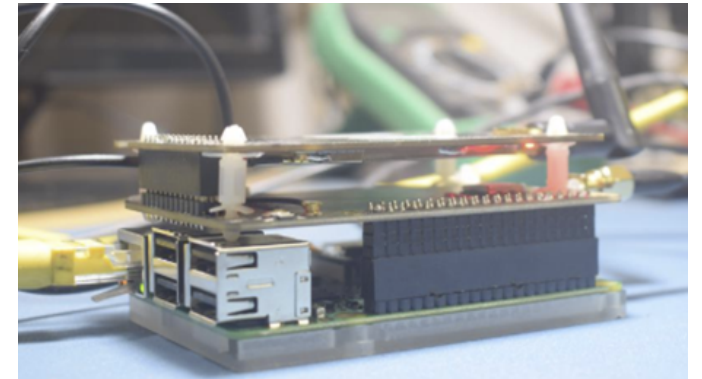
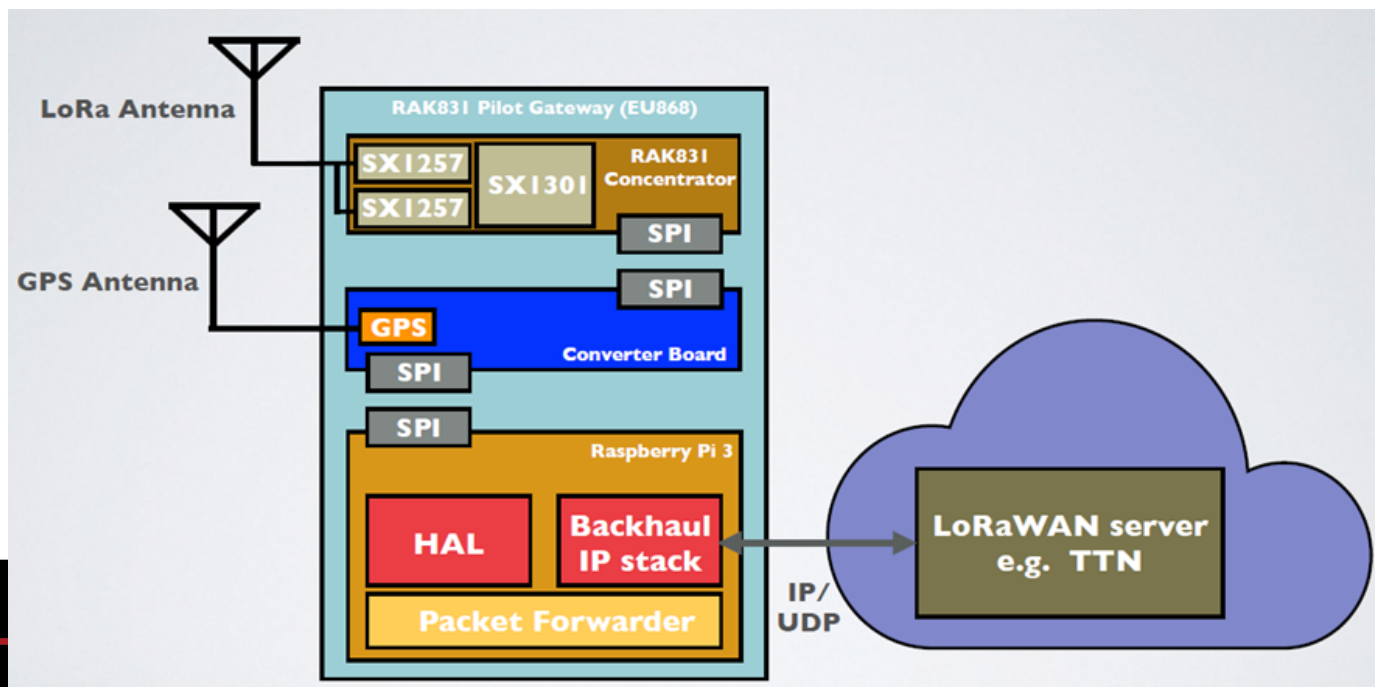
MCU : Application + **LoRaMac-node**
Radio: Modem , SX1276/SX1272



MCU : Application + RTOS/AT library
Module : AT Server + **LoRaMac-node**

Architecture of LoRaWAN Gateways

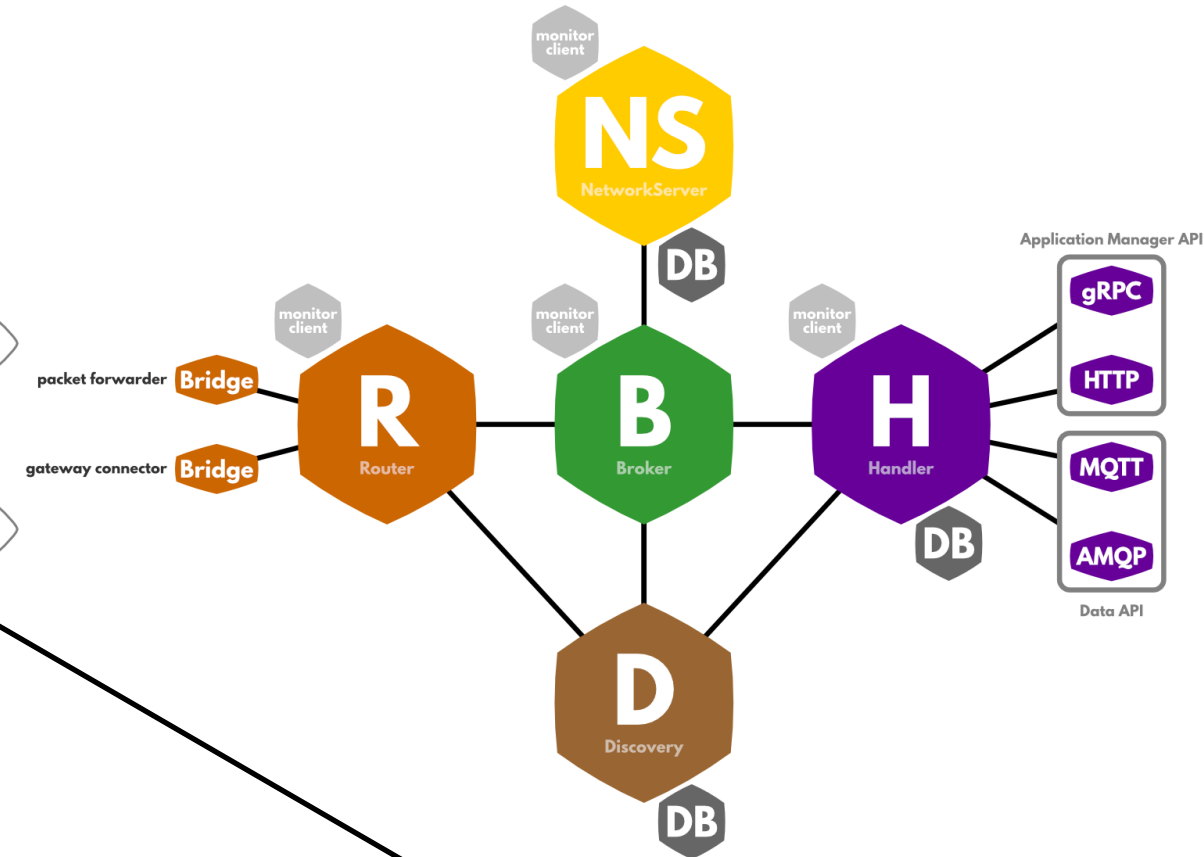
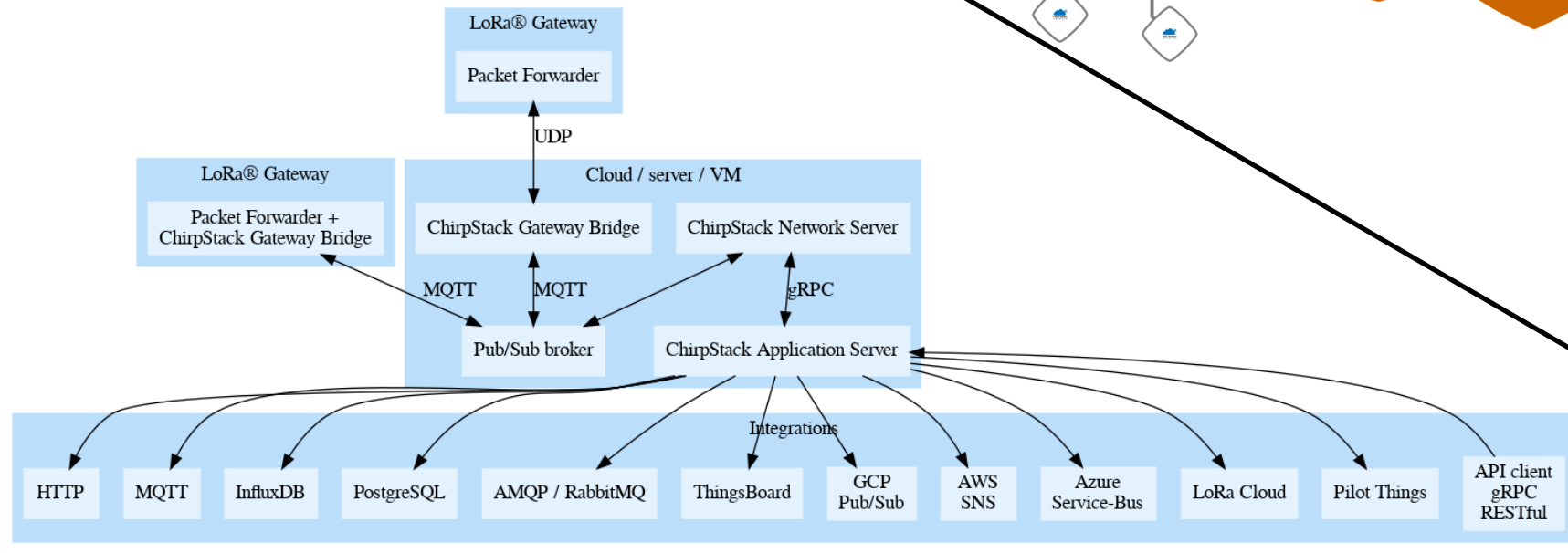
- Packet Forwarder (Bridge between node and server)
 - packet_forwarder, basicstation, mqtt, etc.
- Linux as OS, It's a router



Architecture of LoRaWAN Network Server

- Mainstream LoRaWAN Server

Chirpstack



TTN



Attack Surface of LoRaWAN Supply Chain

- Nodes
 - Vulnerabilities in the LoRaMac-Node, affecting a wide range of.
- Gateways
 - Security risks of different Packet Forwarder.
- Servers
 - Risk of abusing the default configuration.
 - Security issues of open source code.

Security Analysis of LoRaMac-node

- LoRaWAN end-device stack implementation released by Semtech
- CVE-2020-11068
 - The vulnerability exists in the process of OTAA, which can cause harm to the devices that are joining the network.
 - For deployed projects, it is necessary to rejoin the network, which needs to be combined with other attack methods.

Advantage: No need to know the AppKey

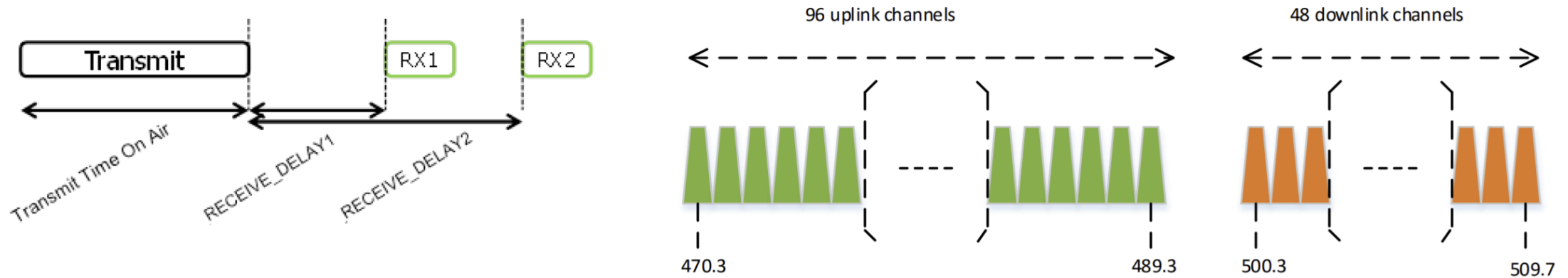
Fixed in version 4.4.4.

```
@@ -997,6 +997,13 @@ static void ProcessRadioRxDone( void )
997     switch( macHdr.Bits.MType )
998     {
999         case FRAME_TYPE_JOIN_ACCEPT:
1000 +         // Check if the received frame size is valid
1001 +         if( size < LORAMAC_JOIN_ACCEPT_FRAME_MIN_SIZE )
1002 +         {
1003 +             MacCtx.McpsIndication.Status = LORAMAC_EVENT_INFO_STATUS_ERROR;
1004 +             PrepareRxDoneAbort( );
1005 +             return;
1006 +         }
1007     macMsgJoinAccept.Buffer = payload;
1008     macMsgJoinAccept.BufSize = size;
```



Security Analysis of LoRaMac-node

- How to send radio packets to nodes
 - Receive Windows of CLASS-A end-devices – [REVEIVE_DELAY1 = 1, JOIN_DELAY1 = 5]
 - Regional downlink channel - [CN470-RX1 Channel Number = Uplink Channel Number modulo 48]



Security Analysis of LoRaMac-node

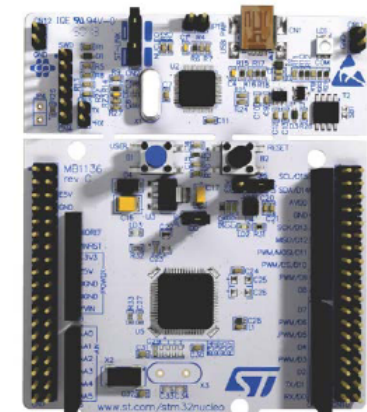
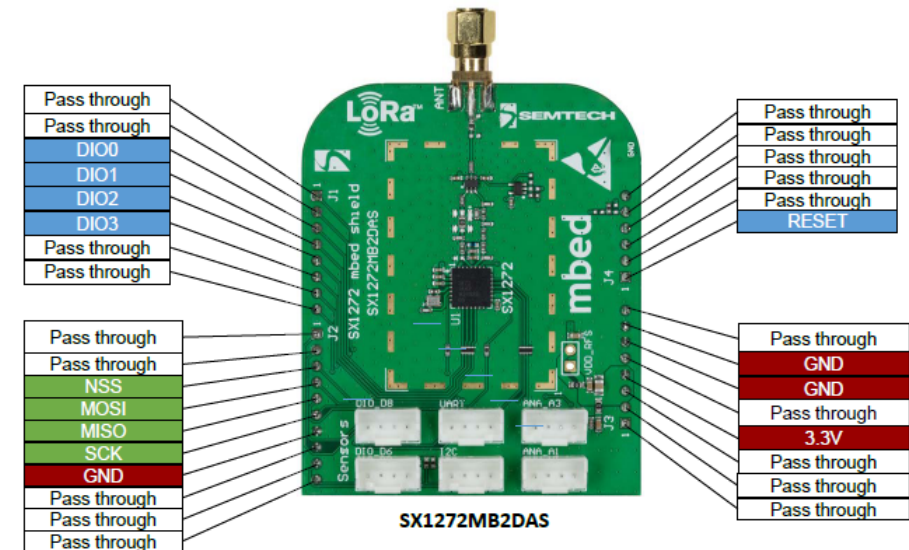
- Debug

- Hardware : P-NUCLEO-LRWAN1

- STLINK-Debugs
 - MCU (LoRaMac-node)
 - Expansion board (SX1272MB2DAS,SX1276MB2DAS

- Software : IMPL + DEBUG Tools

- STM32CubeExpansion+ Keil
 - LoRaMac-Node + (VS CODE + openocd)

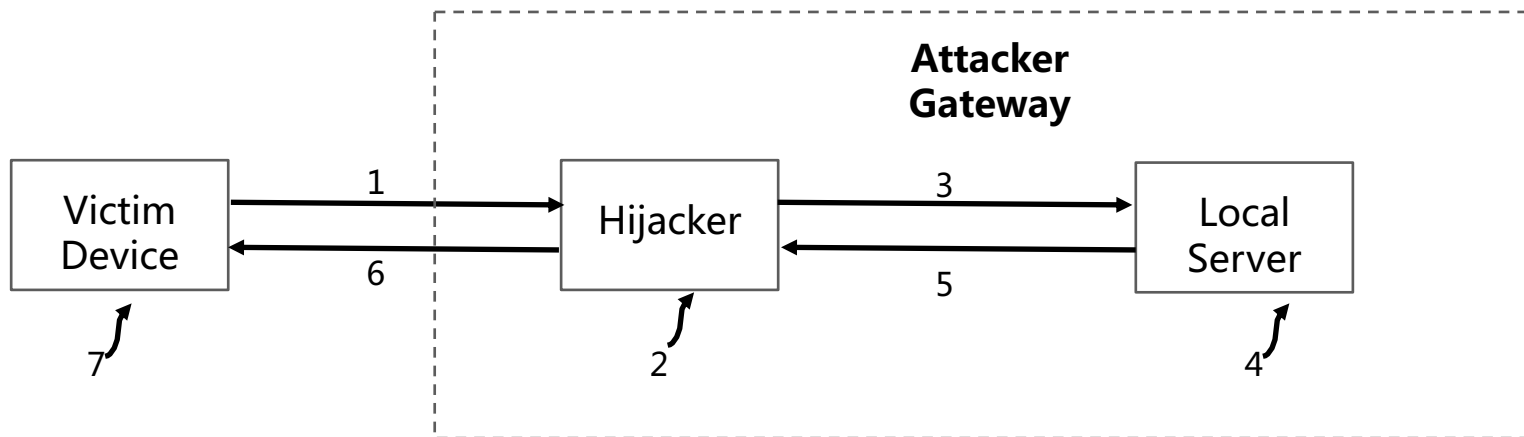


NUCLEO-L073RZ



Security Analysis of LoRaMac-node

- Our Practice



1. The victim sends OTAA packet
7. Device dropped or restarted

2. Sniffing the upstream channel
3. Notify the local server.
6. Send malicious radio to the victim

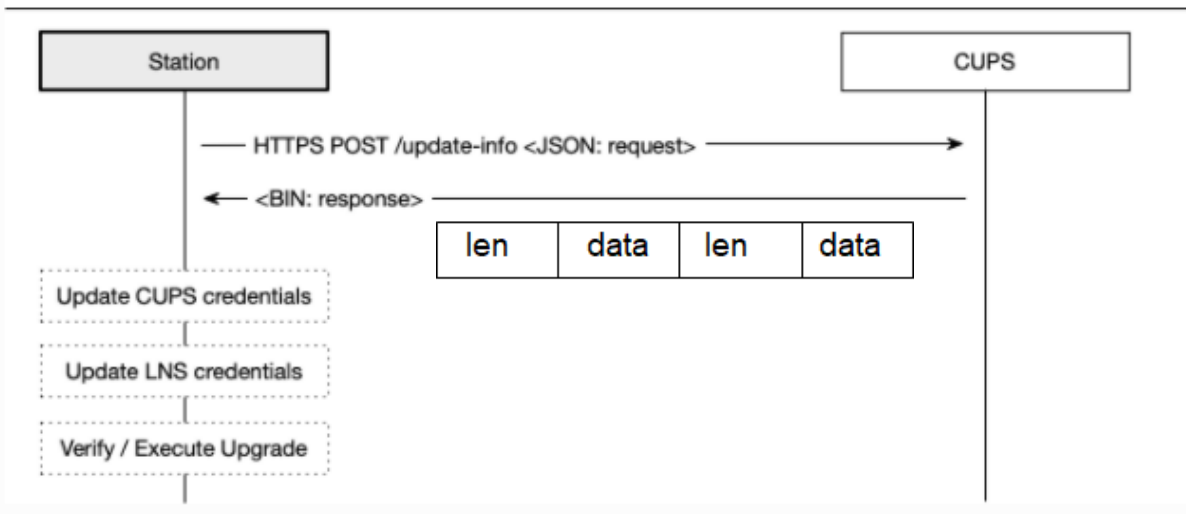
4. Calculate downlink channel and delay
5. Send malicious data to hijacker



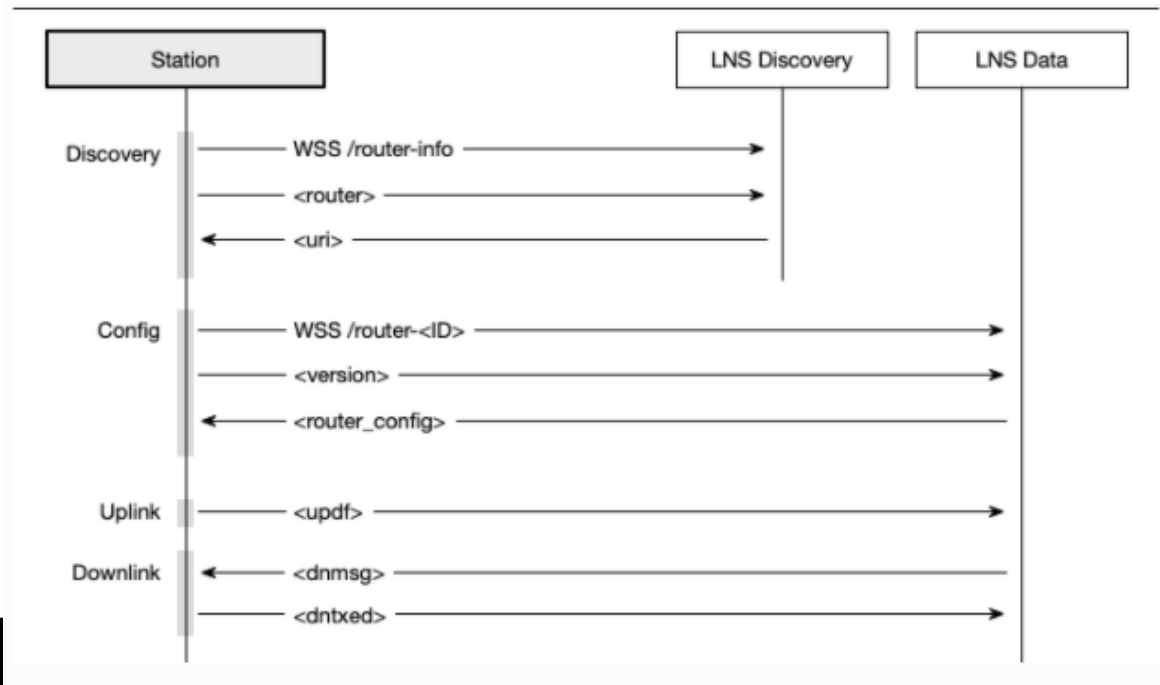
Security Analysis of LoRa Basics™ Station

- New state-of-the-art gateway packet-forwarder
 - CUPS: custom update protocol, LNS: WebSocket + Json to LoRaWAN® Network Server

BasicStation – CUPS Request



BasicStation – LNS Protocol



Security Analysis of LoRa Basics™ Station

- Attack surface [Man-in-the-middle hijacking or malicious server]
 - Does not force the authentication mode to be enabled
 - The risk of LNS capacity abuse: Remote code execution
 - CUPS has memory corruption vulnerability(CVE-2020-4060) and logic vulnerability

Security Analysis of LoRa Basics™ Station

- The risk of LNS capacity abuse

```
client->server ws://x.x.x.x:1234/router-info
{"router":"b827:ebff:fe67:c526"}
```

```
server->client {"router":"b827:ebff:fe67:c526","muxs":"muxs-
::0","uri":"ws://x.x.x.x:1234/traffic/eui-B827EBFFFE67C526"}
```

```
client->server ws://x.x.x.x:1234/traffic/eui-B827EBFFFE67C526
{"msgtype":"version","station":"2.0.3(rpi/std)","firmware":null,"package"
:null,"model":"rpi","protocol":2,"features":"rmtsh"}
```

```
server->client Send downlink data and execute malicious commands.
{"msgtype": "runcmd","command":"touch pwn.txt","arguments":
["pwn.txt"]}
```

Remote Commands

Stations support two mechanisms for running remote commands on the gateway:

```
{
  "msgtype" : "runcmd"
  "command" : STRING,
  "arguments": [ STRING, ... ]
}
```

```
519 int sys_execCommand (ustime_t max_wait, str_t* argv) {
520     int argc = 0;
521     while( argv[argc] ) argc++;
522     if( argc == 0 || (argc==1 && argv[0][0]==0) )
523         return 0;
524     sys_flushLog();
525     pid_t pid1;
526     if( (pid1 = fork()) == 0 ) {
527         pid_t pid2 = 0;
528         if( max_wait!=0 || (pid2 = fork()) == 0 ) {
529             if( access(argv[0], X_OK) != 0 ) {
530                 // Not an executable file
531                 str_t* argv2 = rt_mallocN(str_t, argc+3);
532                 memcpy(&argv2[3], &argv[0], sizeof(argv[0])*(argc+1)); // also copy tr
533                 if( access(argv[0], F_OK) == -1 ) {
534                     // Not even a file - assume shell statements
535                     argv2[0] = "/bin/sh";
536                     argv2[1] = "-c";
537                     argv2[2] = argv[0];
538                     argv = argv2;
```


Chirpstack: Risk of Abusing the Default Configuration


- Default weak password (No mandatory user settings)
 - Database, Application Server WEB
- No authentication by default
 - MQTT, gRPC


About 2,394 results (Nearly year: 2,245 results) 0.339 seconds


Value ranking

"ChirpStack Application Server" X

 >



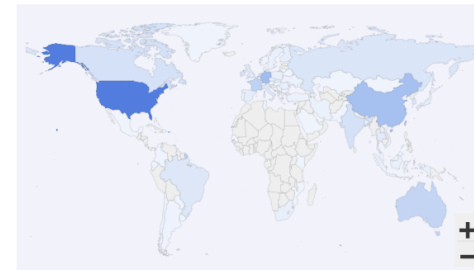
 Indonesia

 2021-04-08 12:34

Banner

```
HTTP/1.0 200 OK
Accept-Ranges: bytes
Content-Length: 2257
Content-Type: text/html; charset=utf-8
Last-Modified: Fri, 31 Jul 2020 08:42:47 GMT
Date: Thu, 08 Apr 2021 04:34:23 GMT

<!doctype html><html lang="en"><head><meta charset="utf-8"><meta name="viewport"
```



SEARCH TYPE

Devices	2,391 ▼
Ipv4	2,377
Ipv6	14

YEAR

2021	1,581
2020	789
2019	21

Chirpstack: Risk of Abusing the Default Configuration

- MQTT integration (User password and ACL optional)
 - Steal the upstream and downstream data of the device
 - Fake scheduling downlink

```
application/1/device/343235376e387f18/rx {"applicationID": "1", "applicationName": "First_application", "deviceName": "RAK811_LoraNode", "devEUI": "343235376e387f18", "rxInfo": [{"gatewayID": "b827ebfffe67c526", "uplinkID": "72ab3e7c-79ec-408c-8ab6-1a8e66dfcd58", "name": "TTN_GW", "rssi": -37, "loRaSNR": 13, "location": {"latitude": 0, "longitude": 0, "altitude": 0}}, {"gatewayID": "b827ebfffe67c526", "uplinkID": "cd89d034-e292-4e57-a423-073bfa33cdc4", "name": "TTN_GW", "rssi": -89, "loRaSNR": -6.2, "location": {"latitude": 0, "longitude": 0, "altitude": 0}}, {"gatewayID": "b827ebfffe67c526", "uplinkID": "03506bbf-d491-42de-885c-badd01a0df2b", "name": "TTN_GW", "rssi": -88, "loRaSNR": -8.8, "location": {"latitude": 0, "longitude": 0, "altitude": 0}}, {"txInfo": {"frequency": 486700000, "dr": 0, "adr": true, "fCnt": 4, "fPort": 2, "data": "QkJCQkJCQkI="}} gateway/b827ebfffe67c526/command/down
```

```
[LoRa]: RUI_MCPS_UNCONFIRMED send success
OK
at+recv=0,-117,186,0
at+send=loras:2:4242424242424242
[LoRa]: RUI_MCPS_UNCONFIRMED send success
OK
at+recv=10,-117,191,548656c6c6f
hello
at+send=loras:2:4242424242424242
```

lorawan-stack : Security issues of open source code

- UDP parsing error
 - nil panic (Sending UDP leads to denial of service)

```
====read udp====
====UnmarshalBinary====&{GatewayAddr:192.168.220.140:42516 ReceivedAt:2020-04-29 04:32:29.19865367
packetType:PushData GatewayEUI:6666666666666666 Data:<nil>}
  INFO Finished unary call                               duration=2.464827ms grpc_method=GetIdentifiersForEU
quest_id=01E72VBACFWWRB6R5EGZVSAR3S
  INFO Finished unary call                               duration=2.781037ms grpc_method=Get grpc_service=tt
CH77EKW4CAWRYEGVWK
  INFO Connected                                       gateway_eui=6666666666666666 gateway_uid=my-admin-g
====handleUp===={GatewayAddr:192.168.220.140:42516 ReceivedAt:2020-04-29 04:32:29.198653675 -0700
e:PushData GatewayEUI:6666666666666666 Data:<nil>}
panic: runtime error: invalid memory address or nil pointer dereference
[signal SIGSEGV: segmentation violation code=0x1 addr=0x8 pc=0x184ebd1]

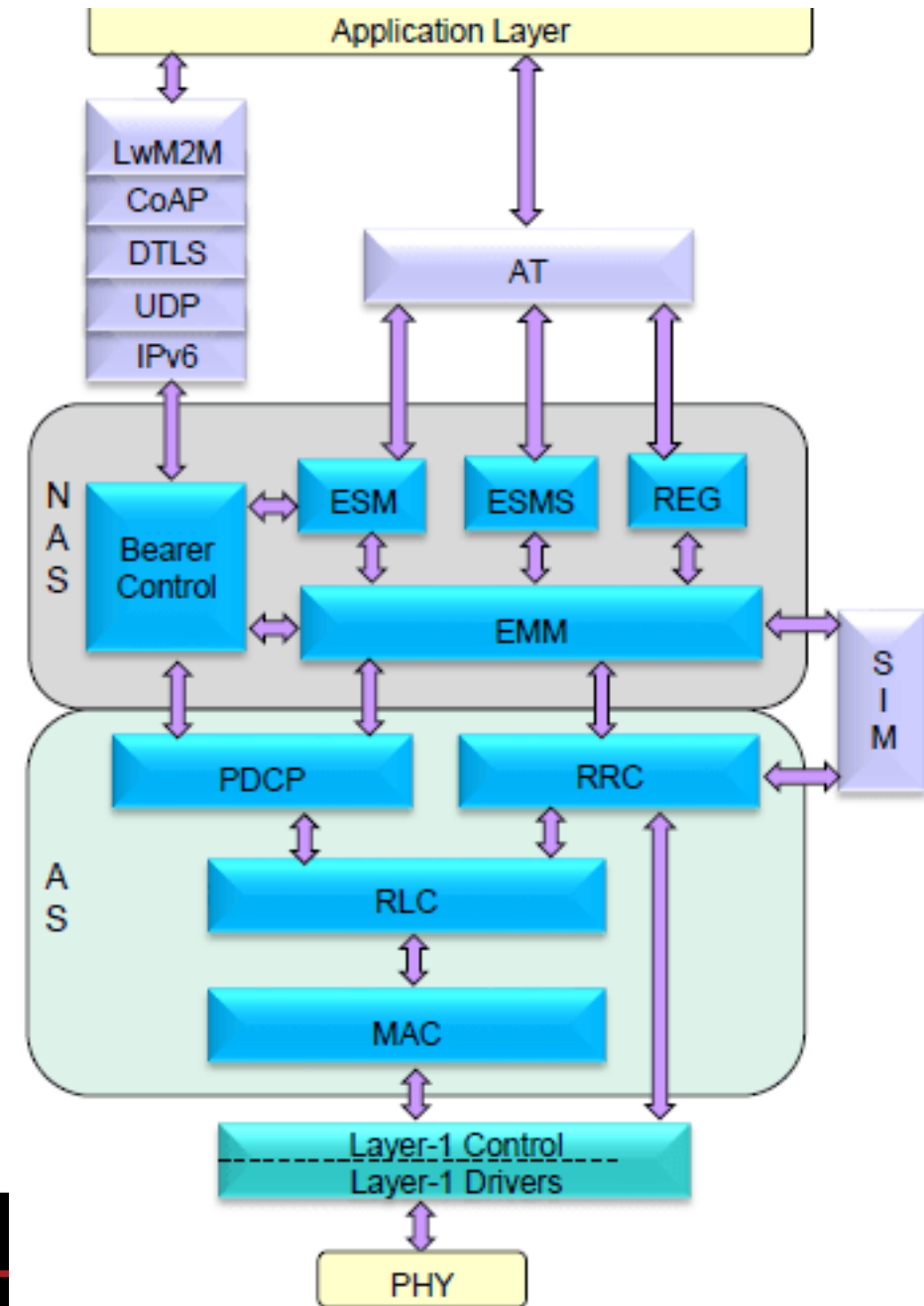
goroutine 130 [running]:
go.thethings.network/lorawan-stack/pkg/gatewayserver/io/udp.(*srv).handleUp(0xc0006ce320, 0x25d3be6
0x27d226ff8c, 0x36e4320, 0x8a6102, 0xc000ca8028, ...)
    /home/yun/lora/lorawan-stack/pkg/gatewayserver/io/udp/udp.go:261 +0x261
go.thethings.network/lorawan-stack/pkg/gatewayserver/io/udp.(*srv).handlePackets(0xc0006ce320)
    /home/yun/lora/lorawan-stack/pkg/gatewayserver/io/udp/udp.go:181 +0x3b1
created by go.thethings.network/lorawan-stack/pkg/gatewayserver/io/udp.Serve
    /home/yun/lora/lorawan-stack/pkg/gatewayserver/io/udp/udp.go:101 +0x203
yun@ubuntu:~/lora/lorawan-stack$
```

Security Internal of NB-IoT

- Technology Implementation in the Real World
- Attack Surface of NB-IoT
- Our Practice

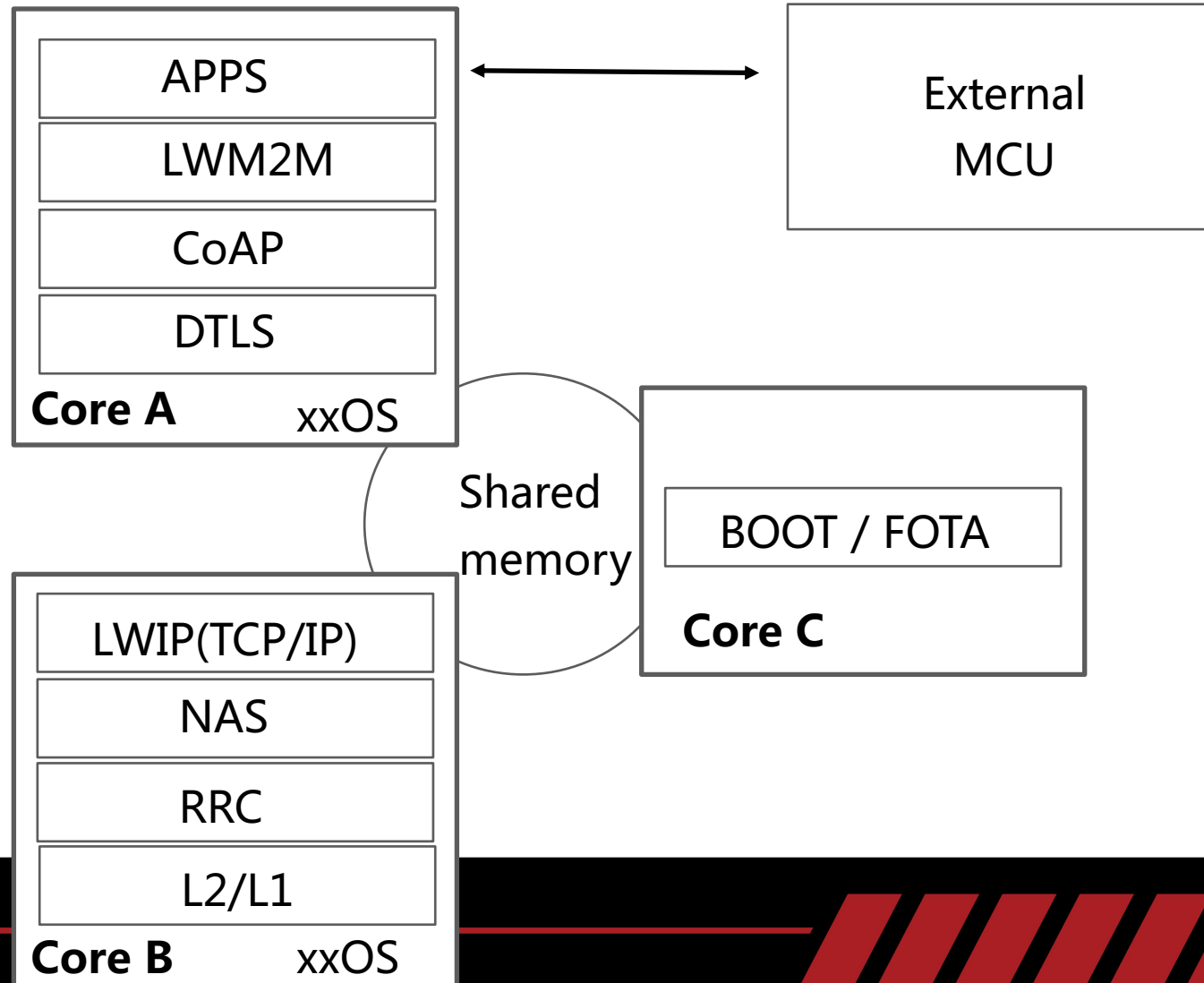
Overview of NB-IoT

- SOC: High Integration
 - Different architectures/ RTOS
- Complex protocol stack
 - NB-IoT PHY + LTE AS/NAS
 - TCP/IP + APPS
- EPC/eNB/IoT Cloud Platform
 - Black box



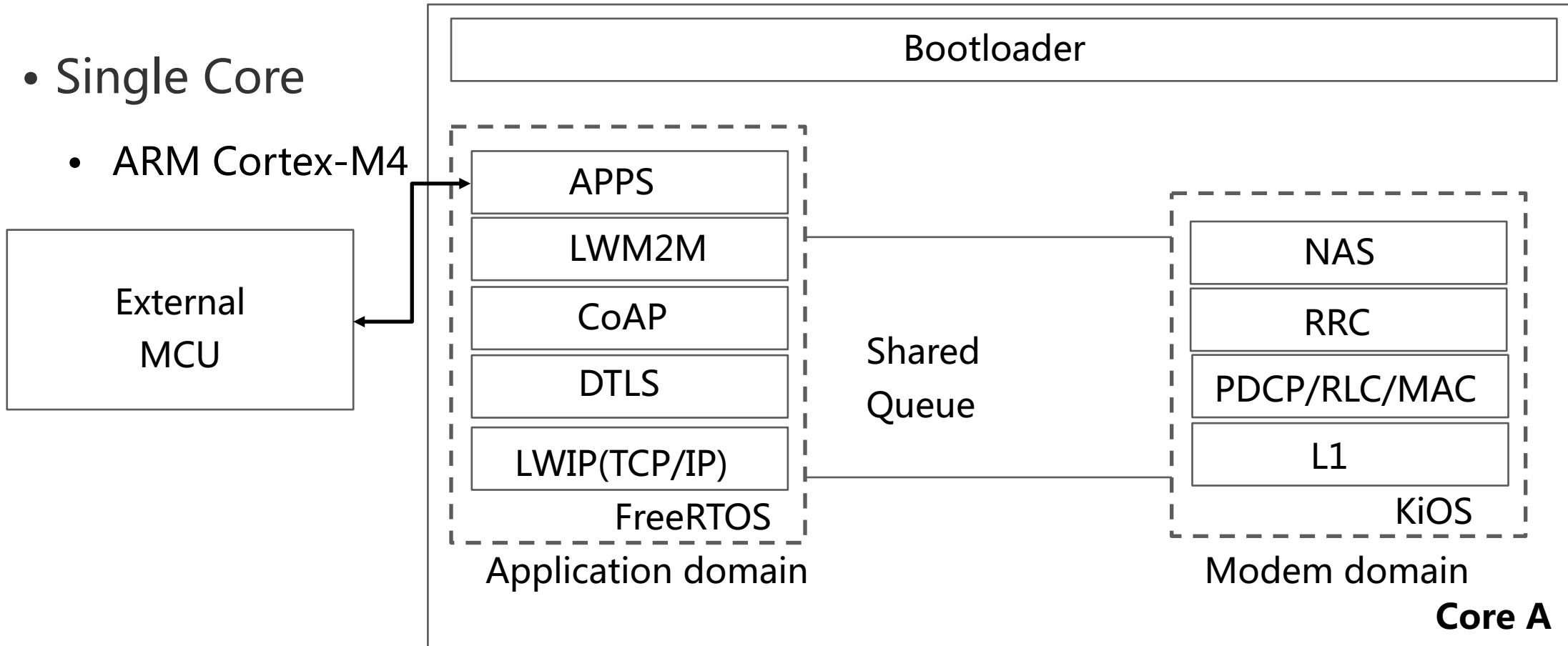
Architecture of NB-IoT Chip (A)

- Multi-Core
 - ARM Cortex-M0



Architecture of NB-IoT Chip (B)

- Single Core
 - ARM Cortex-M4



Attack Surface of NB-IoT Module

- APPS

- at_cmd_handler

- LWM2M

- object_function

- CoAP / MQTT / HTTP?

- TCP/IP

- lwip .etc

- NAS

- ESM, EMM

- RRC

- MIB, SIBx

- Inter-Core Communication

Our Practice

- LOG for debugging

Messages

Filter: default View: default

NAS

Index	Time	Message
26519	13:21.593315	NAS_DBG_NAS_MSG
29077	13:43.307945	NAS_DBG_TIMER
29225	13:43.912925	NAS_DBG_TIMER
29228	13:43.913200	NAS_DBG_TIMER
29850	13:53.937686	NAS_DBG_STATE_INFO
29856	13:53.938480	NAS_LOG_EMMSM_INFO
29858	13:53.938632	NAS_DBG_STATE_INFO
29864	13:53.939304	NAS_DBG_TIMER

```
Record Number 1258
TaskIdTag
TaskIdTag
unsigned long
unsigned long
signed short
SignalIdTag
NphyLppErrorCauseTag
unsigned short
unsigned long
unsigned char
unsigned short
signed short
signed char
NphyEarfcnOffsetTag
unsigned char
unsigned short
unsigned char
unsigned short
unsigned long
unsigned char
unsigned short
signed short
signed char
NphyEarfcnOffsetTag
unsigned char
unsigned short
unsigned short
unsigned long
unsigned char
unsigned short
signed short
signed char
NphyEarfcnOffsetTag
unsigned short
unsigned short
unsigned long
unsigned char
unsigned short
signed short
signed char
NphyEarfcnOffsetTag
directives.source = !UNKNOWN_ENUMERATION! 0x0001 ;
directives.dest = TASK_BL_ID 0x0507 ;
frameNumber = 0x000004e5 1253 ;
time = 0x000380a7 229543 ;
length = 0x00fc 252 ;
id = SIG_NPHY_LPP_ECID_MEAS_CNf 0x0003181b ;
body.nphyLppEcidMeasCnf.errorCause = !UNKNOWN_ENUMERATION! 0x01 ;
.primaryCellResults.pci = 0x0000 0 ;
.primaryCellResults.earfcn = 0x000005ad 1453 ;
.primaryCellResults.sfnPresent = 0x00 0 ;
.primaryCellResults.sfn = 0x0000 0 ;
.primaryCellResults.nrsrp = 0x05ad 1453 ;
.primaryCellResults.nrsrq = 0x00 0 ;
.primaryCellResults.earfcnOffset = NPHY_EARFCN_OFFSET_UNKNOWN 0x00 ;
.primaryCellResults.hSfnPresent = 0x01 1 ;
.primaryCellResults.hSfn = 0x0076 118 ;
.nphyLppEcidMeasCnf.numMeasuredResults = 0x99 153 ;
.nphyLppEcidMeasCnf.cellResults[0].pci = 0x001d 29 ;
.cellResults[0].earfcn = 0x00010000 65536 ;
.cellResults[0].sfnPresent = 0xe6 230 ;
.nphyLppEcidMeasCnf.cellResults[0].sfn = 0xff9e 65438 ;
.nphyLppEcidMeasCnf.cellResults[0].nrsrp = 0x0000 0 ;
.nphyLppEcidMeasCnf.cellResults[0].nrsrq = 0x22 34 ;
.cellResults[0].earfcnOffset = NPHY_EARFCN_OFFSET_UNKNOWN 0x00 ;
.cellResults[0].hSfnPresent = 0x9e 158 ;
.nphyLppEcidMeasCnf.cellResults[0].hSfn = 0x0000 0 ;
.nphyLppEcidMeasCnf.cellResults[1].pci = 0x0000 0 ;
.cellResults[1].earfcn = 0x00000000 0 ;
.cellResults[1].sfnPresent = 0x00 0 ;
.nphyLppEcidMeasCnf.cellResults[1].sfn = 0x8000 32768 ;
.nphyLppEcidMeasCnf.cellResults[1].nrsrp = 0x0000 0 ;
.nphyLppEcidMeasCnf.cellResults[1].nrsrq = 0x00 0 ;
.cellResults[1].earfcnOffset = NPHY_EARFCN_OFFSET_UNKNOWN 0x00 ;
```

Our Practice

- Testing
 - Raspberry Pie + EC20 + IoT SIM
 - USRP + TEST SIM



Security Advise

- LoRaWAN
 - Node: adopt the latest version of the protocol stack
 - Gateway: use authentication or encryption mechanism
 - Server: Clear weak passwords, enable authentication, open ports require data verification

Security Advise

- NB-IoT
 - Node:
 - Update the firmware or third-party library in time
 - Use DTLS or MQTT TLS to communicate with IoT cloud platform
 - EPC: Operators restrict network access policy

Thank You

blade@tencent.com

