TRACK 2

HITB SECCONF
AMSTERDAM - 2021

Insecure Link : Security Analysis and Practical Attacks of LPWAN

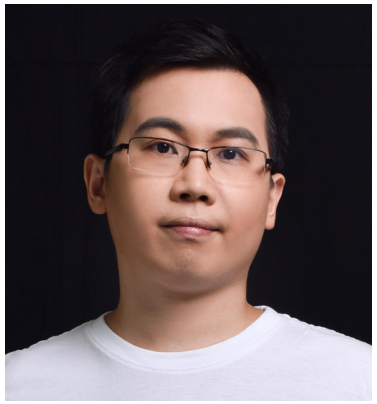
Li YuXiang & Wu HuiYu

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

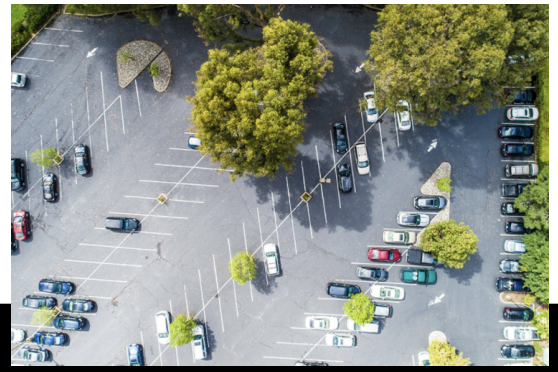
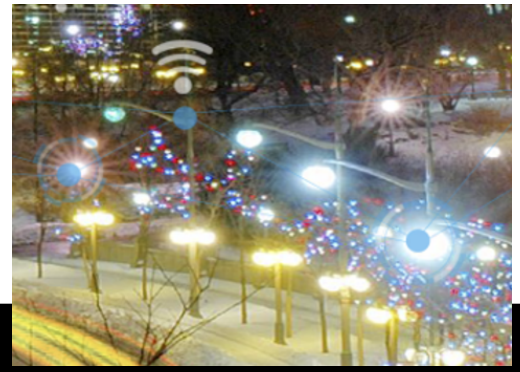
- Introduction to LPWAN Supply Chain
- New Security Risks of LoRaWAN and Our Practice
- Security Internal of NB-IoT
- Security Advice

What is LPWAN

- LPWAN (Low Power Wide Area Network)

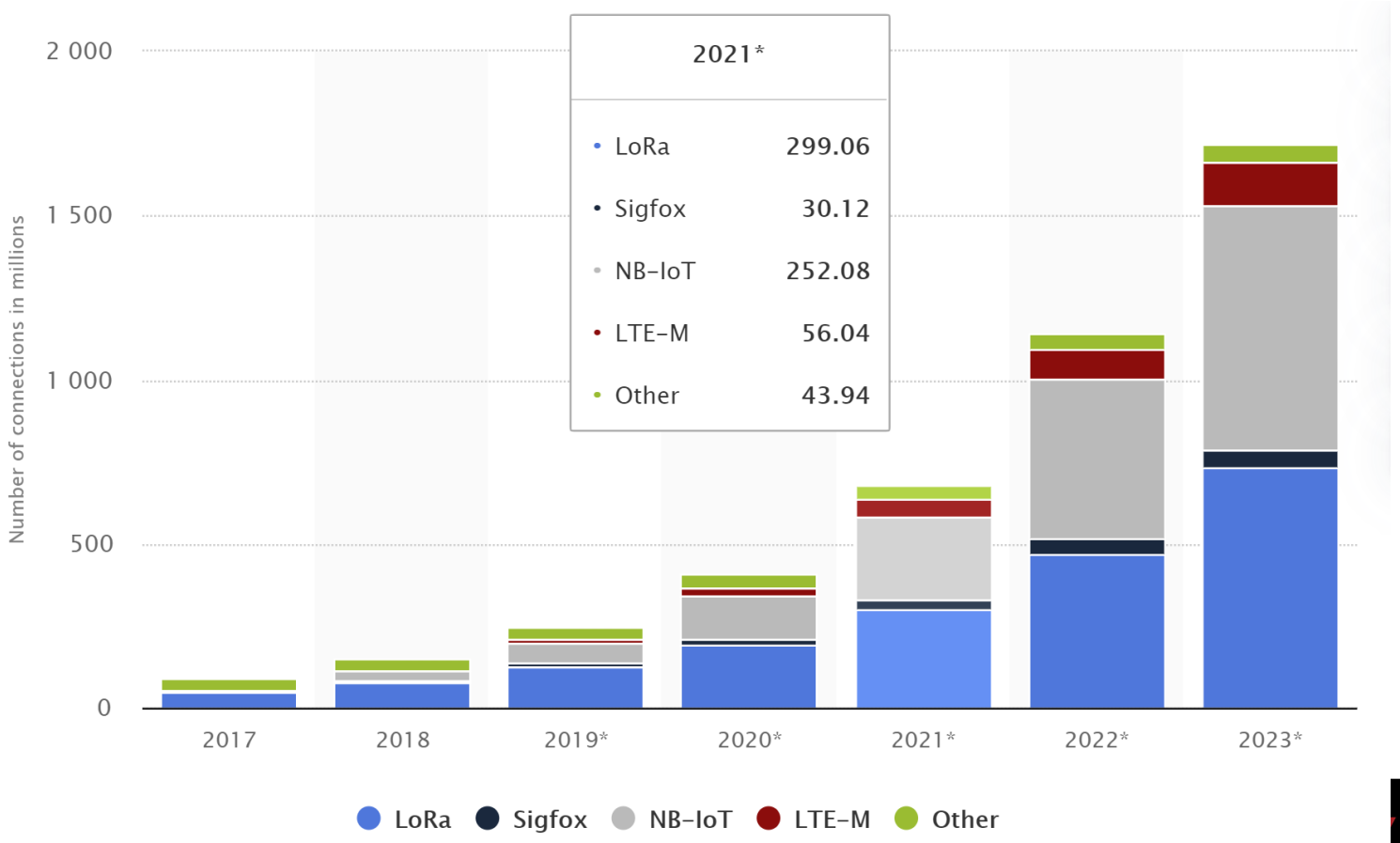
  Low power and low bit rate for long-distance communication.

- Mainstream LPWAN technology
  - LoRa, NB-IoT, sigfox...
- Application Scenarios

The Motivation of Our Work

- LPWAN Market Share Trends



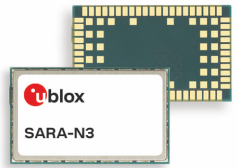
LoRa/LoRaWAN

- 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

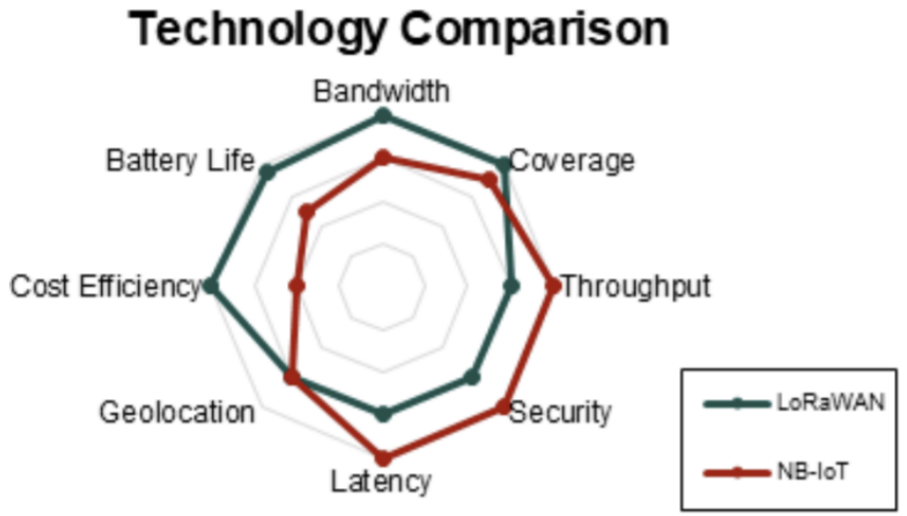
Cloud	THE THINGS NETWORK	ChirpStack	**Telecom Operator**
Product			 
Module			
Chip			 

LoRaWAN vs NB-IoT

- Technical Characteristics

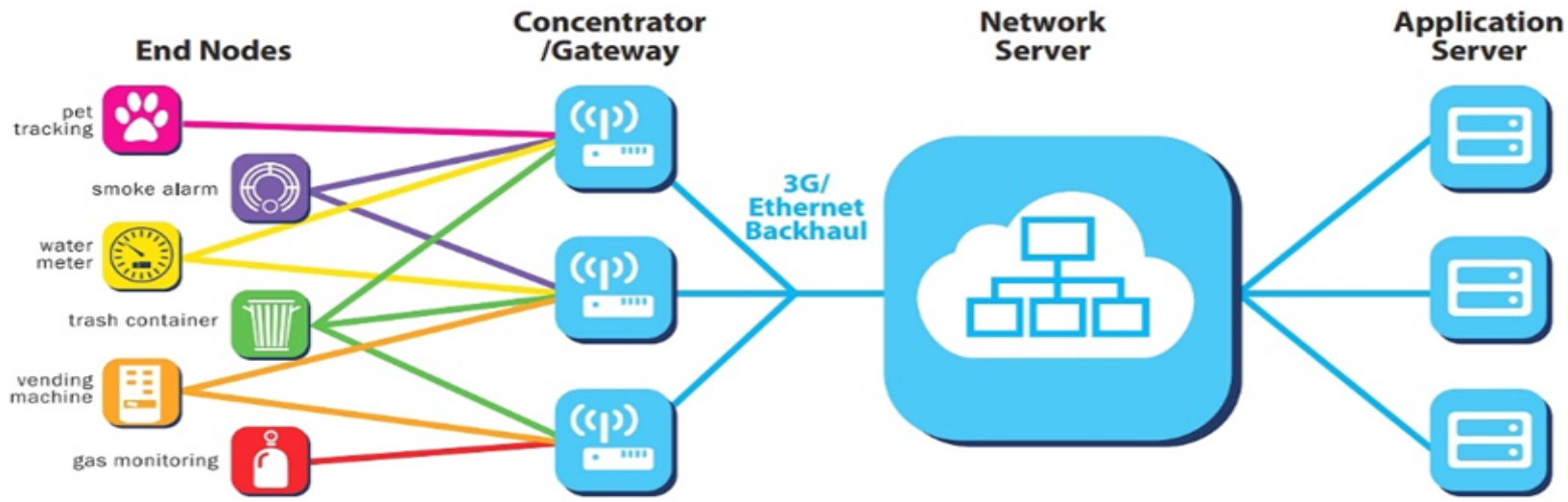
Technology Parameters	LoRaWAN	NB-IoT
Bandwidth	125 kHz	180 kHz
Coverage	165 dB	164 dB
Battery Life	15+ years	10+ years
Peak Current	32 mA	120 mA
Sleep Current	1µA	5µA
Throughput	50 Kbps	60 Kbps
Latency	Device Class Dependent	< 10 s
Security	AES 128 bit	3GPP (128 to 256 bit)
Geolocation	Yes (TDOA)	Yes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

Source: ABI Research

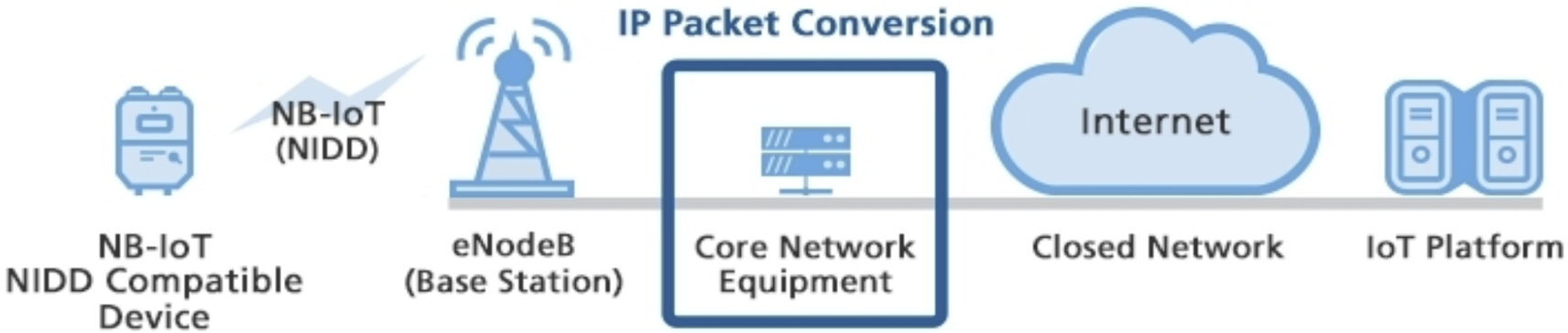


LoRaWAN vs NB-IoT

- Network Architecture

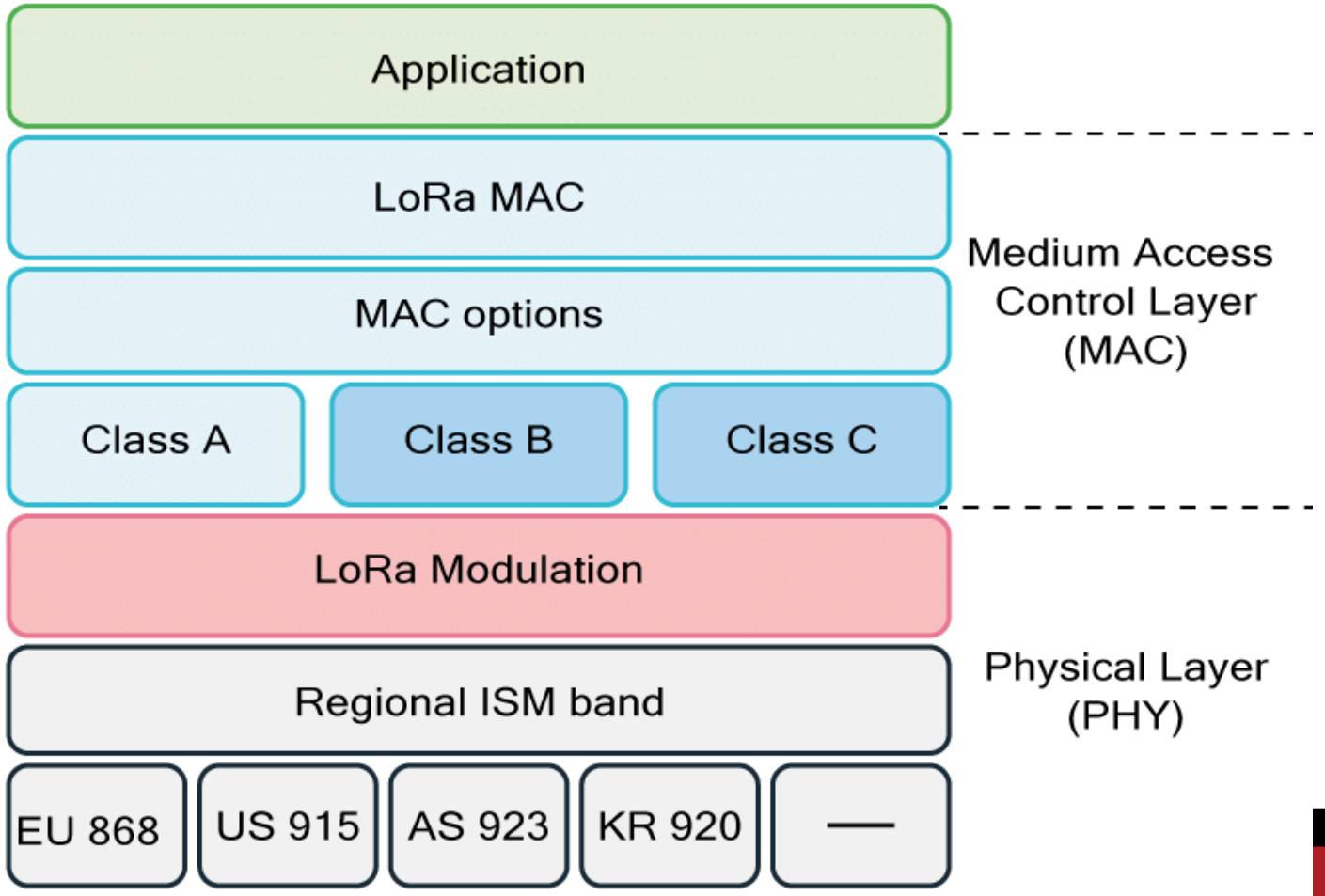


LoRaWAN



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 LoRanWAN 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

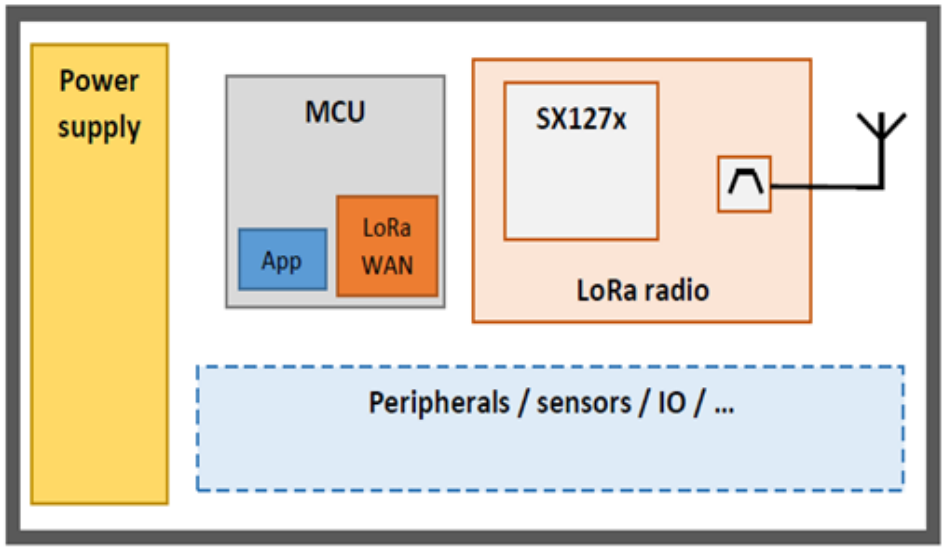
LoRaDawn: New Security Risks of LoRaWAN and Our Practice

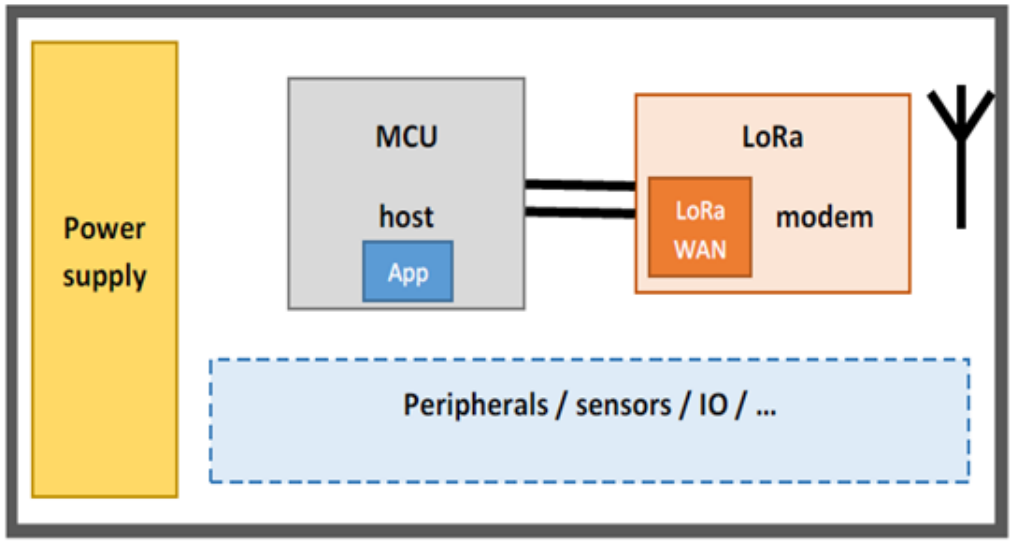
- Technology Implementation in the Real World
- Attack Surface of LoRaWAN Supply Chain
- Our Practice

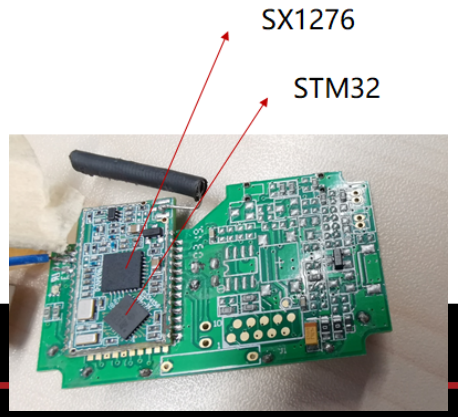
Open Source Implementation in LoRaWAN Supply Chain

- 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

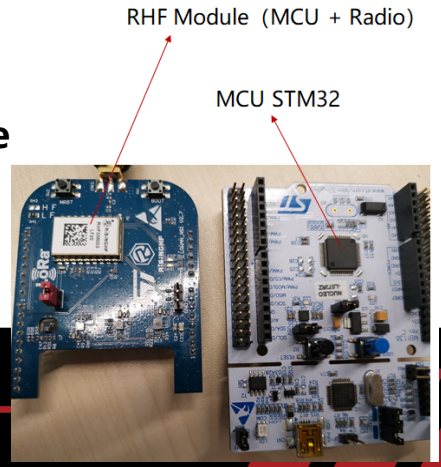
Architecture of LoRaWAN Nodes







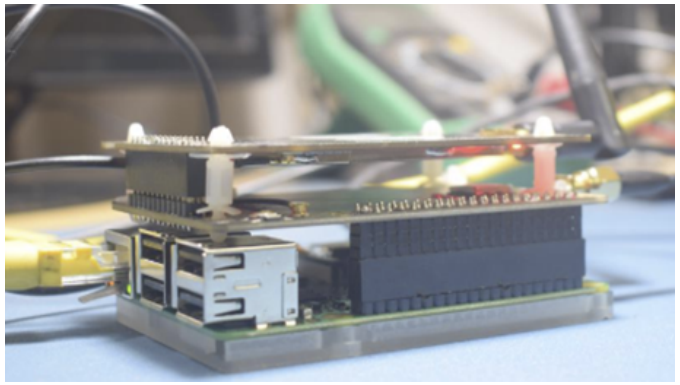
MCU : Application + **LoRaMac-node**
Radio: Modem , SX1276/SX1272

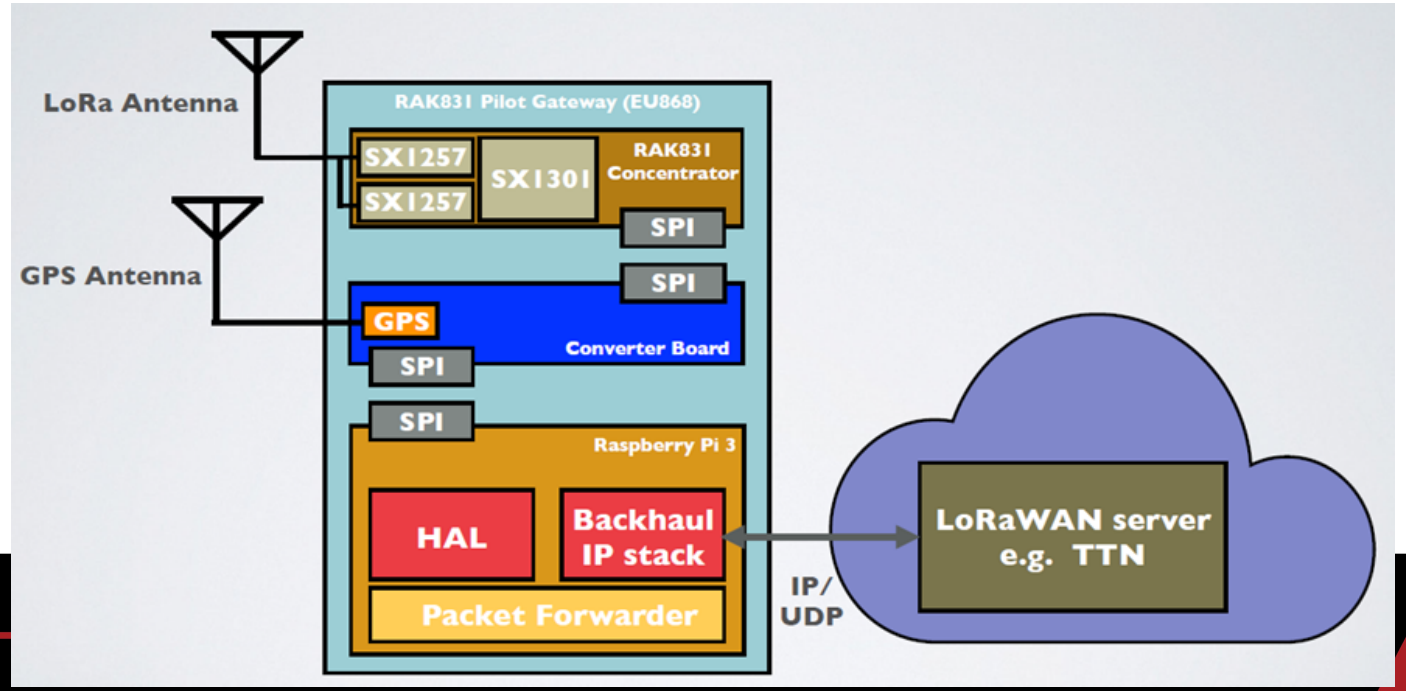


MCU : Application + RTOS/AT library
Module : AT Server + **LoRaMac-node**

Architecture of LoRaWAN Gateways

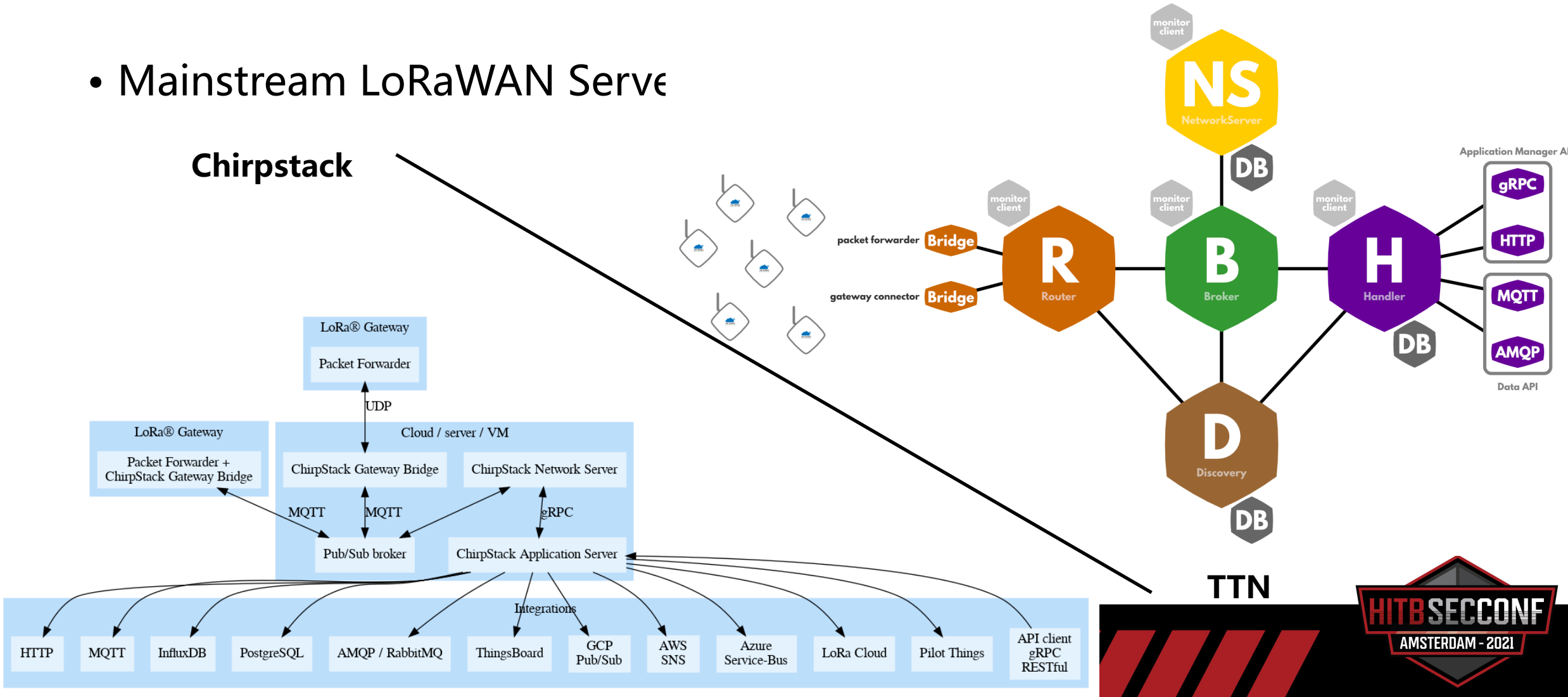
- Packet Forwarder (Bridge between node and server)
  - packet_forwarder,basicstation,mqtt, etc.
- Linux as OS, It's a router





Architecture of LoRaWAN Network Server

- Mainstream LoRaWAN Serve



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.

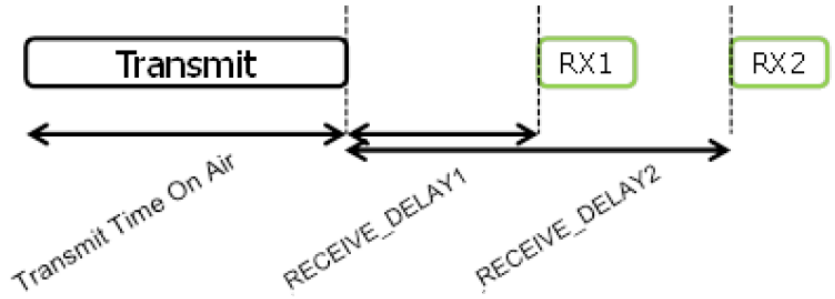
Advantage: No need to know the AppKey

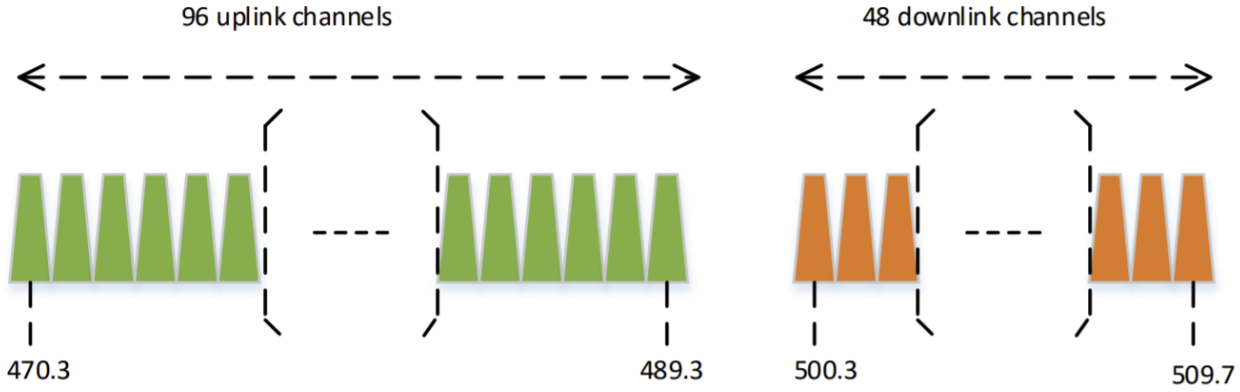
Fixed in version 4.4.4.

```
@@ -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

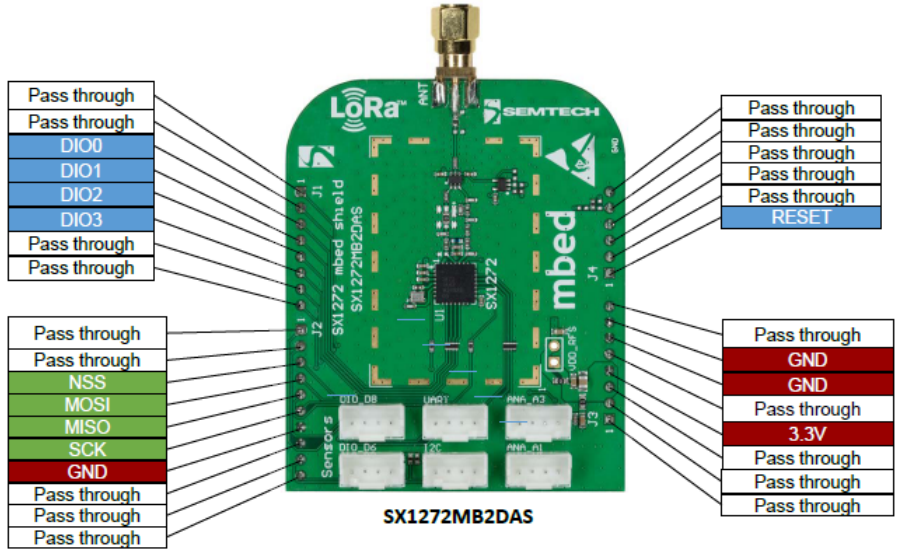
- How to send radio packets to nodes
  - Receive Windows of CLASS-A end-devices – [REVEIVE_DELAY1 = 1, JOIN_DELAY1 = 5]
  - Regional downlink channel - [CN470-RX1 Channel Number = Uplink Channel Number modulo 48]

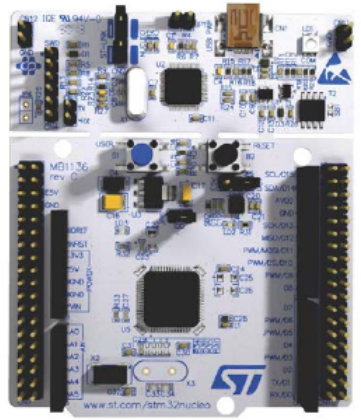




Security Analysis of LoRaMac-node

- 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)

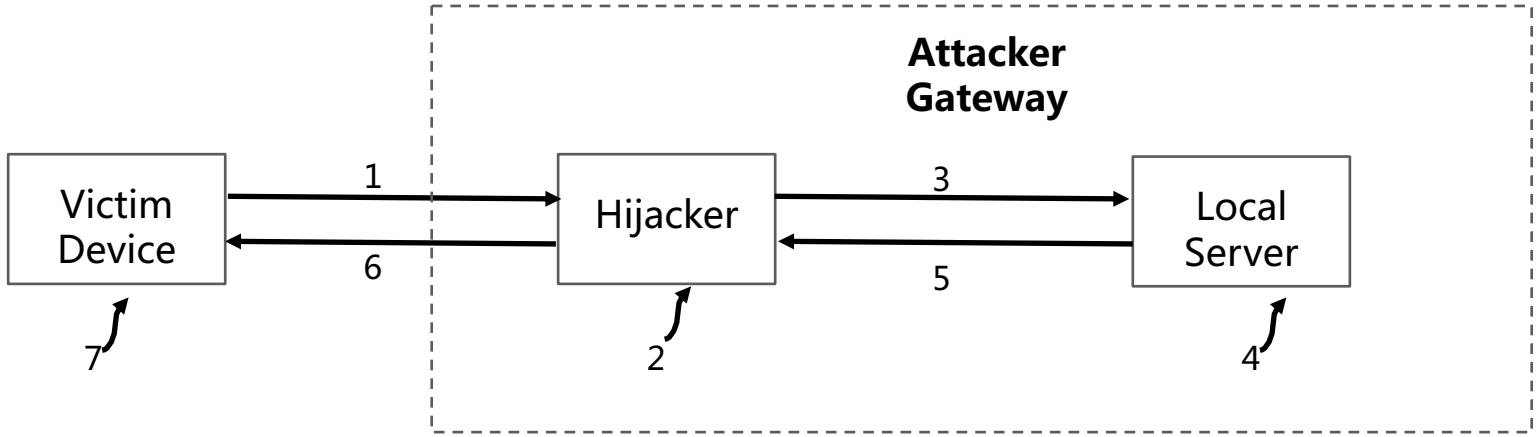




NUCLEO-L073RZ

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.

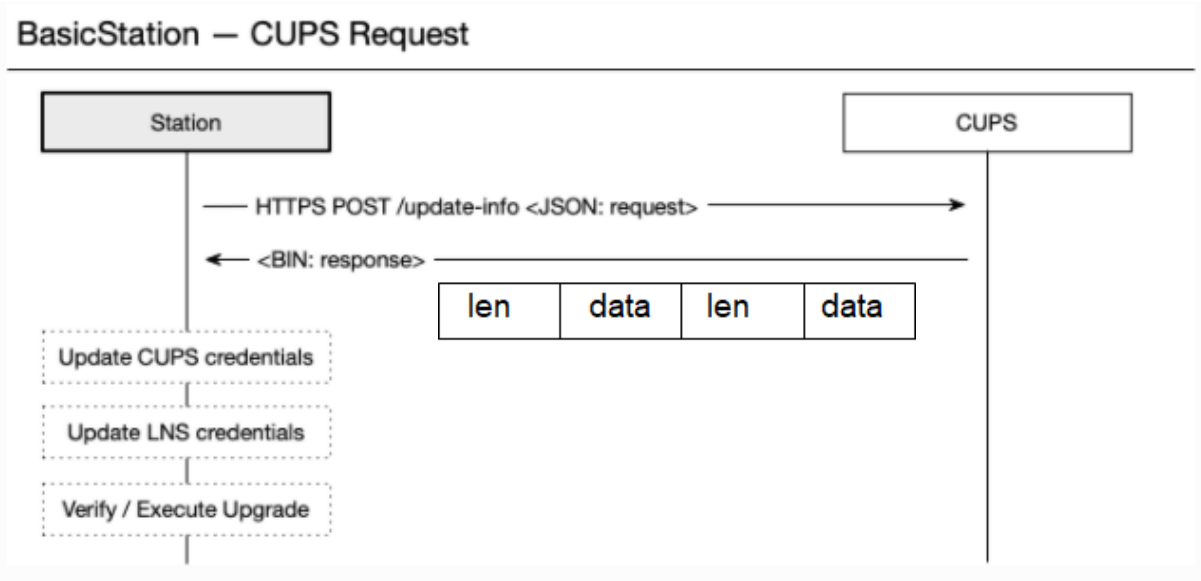
6. Send malicious radio to the victim

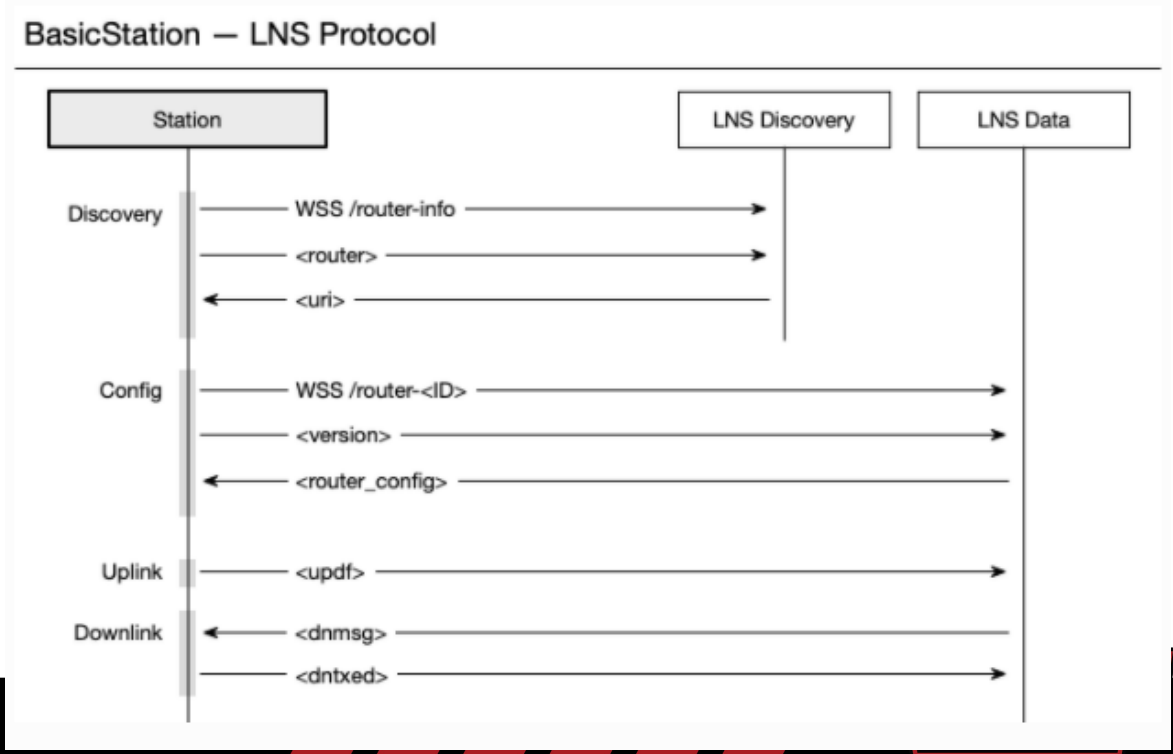
4. Calculate downlink channel and delay

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





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

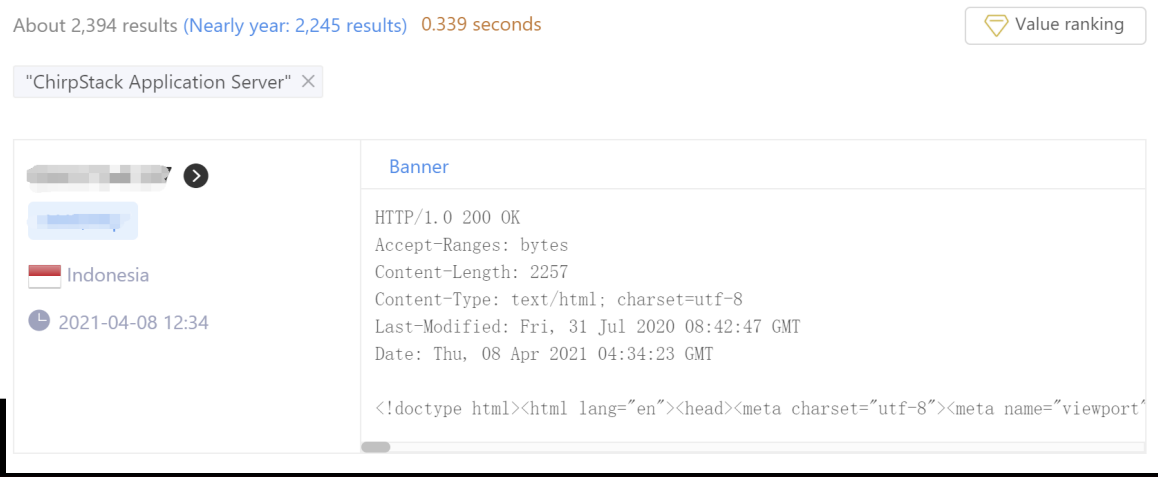
Stations support two mechanisms for running remote commands on the gateway:

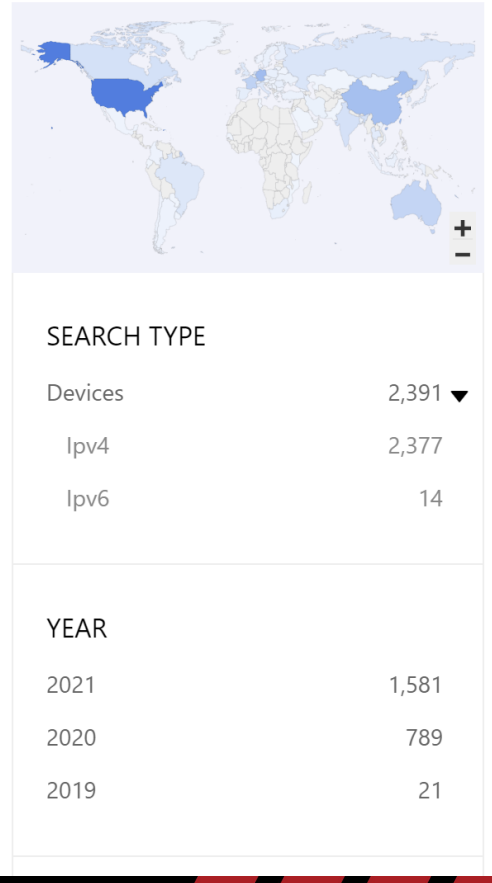
```
{
  "msgtype"  : "runcmd"
  "command"  : STRING,
  "arguments": [ STRING, ... ]
}
```

```
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

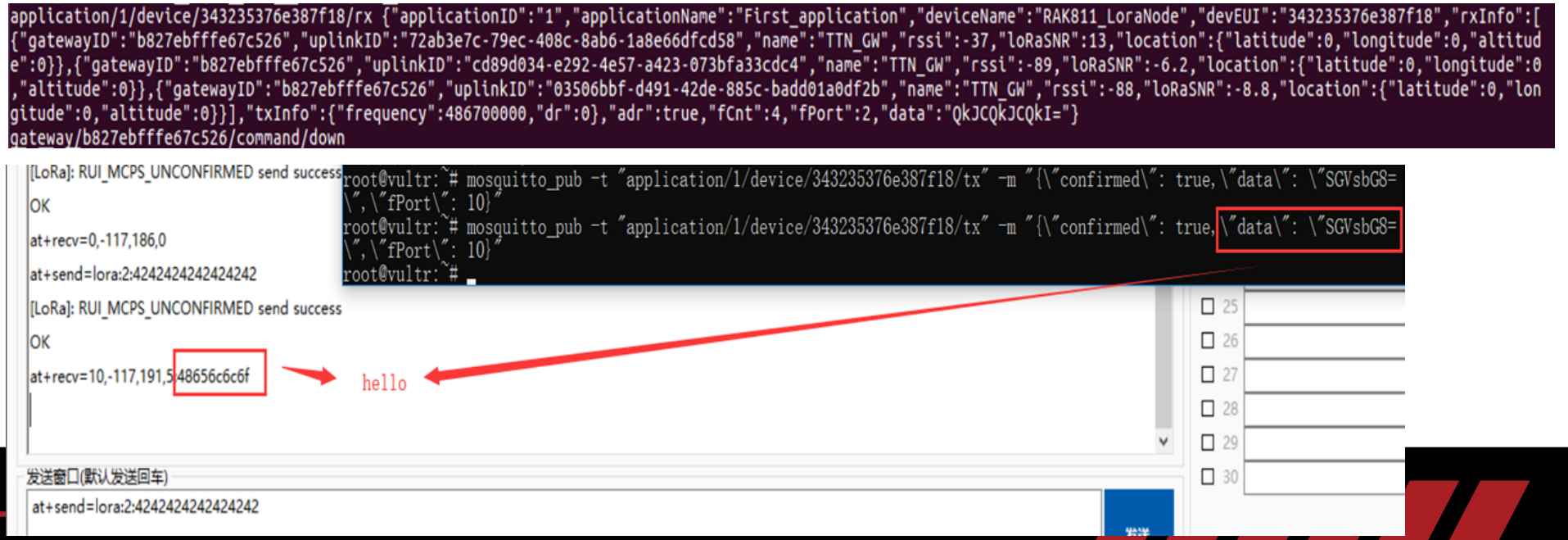
- Default weak password (No mandatory user settings)
  - Database, Application Server WEB
- No authentication by default
  - MQTT, gRPC





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



lorawan-stack：Security issues of open source code

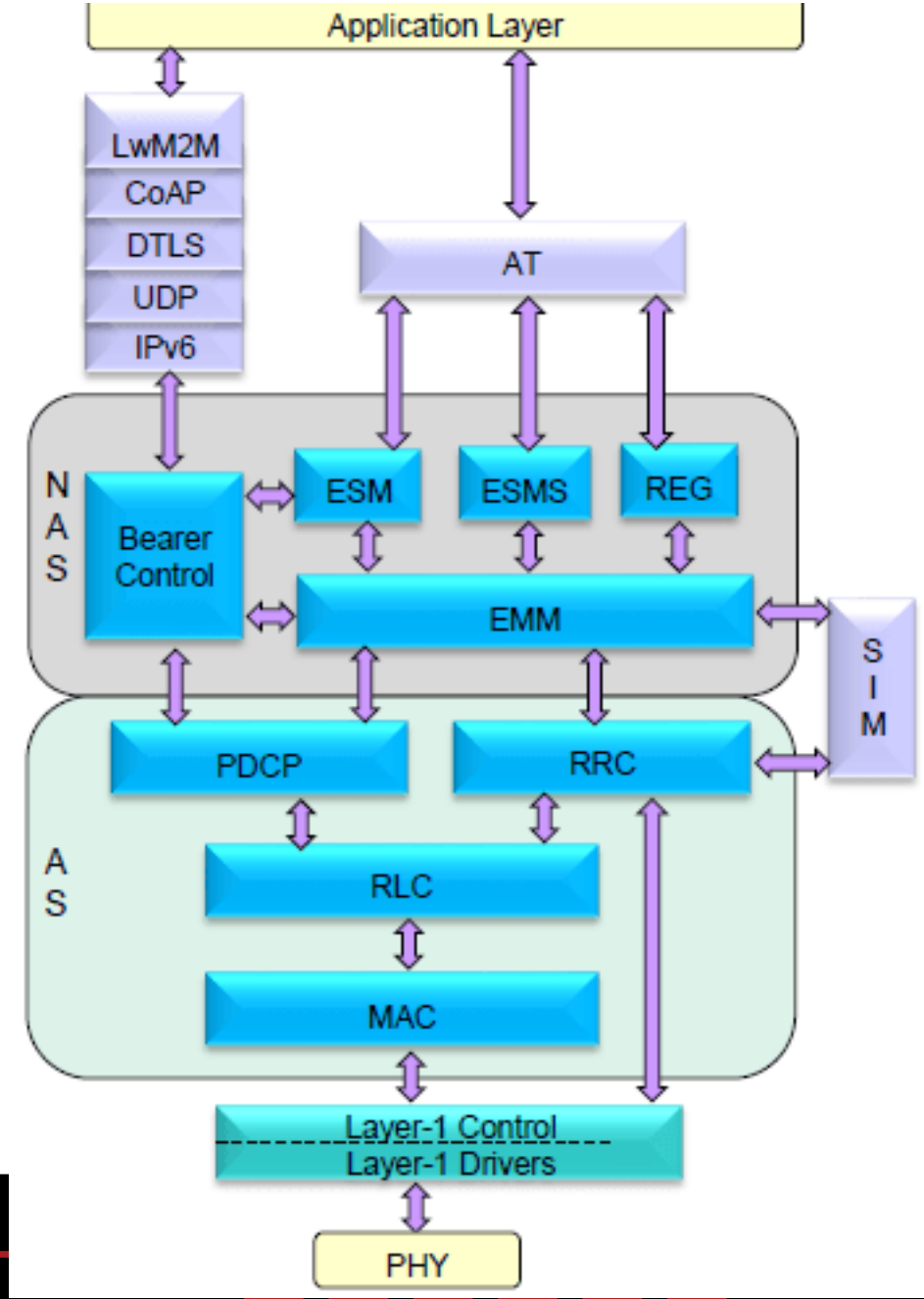
- UDP parsing error
  - nil panic (Sending UDP leads to denial of service)

Security Internal of NB-IoT

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

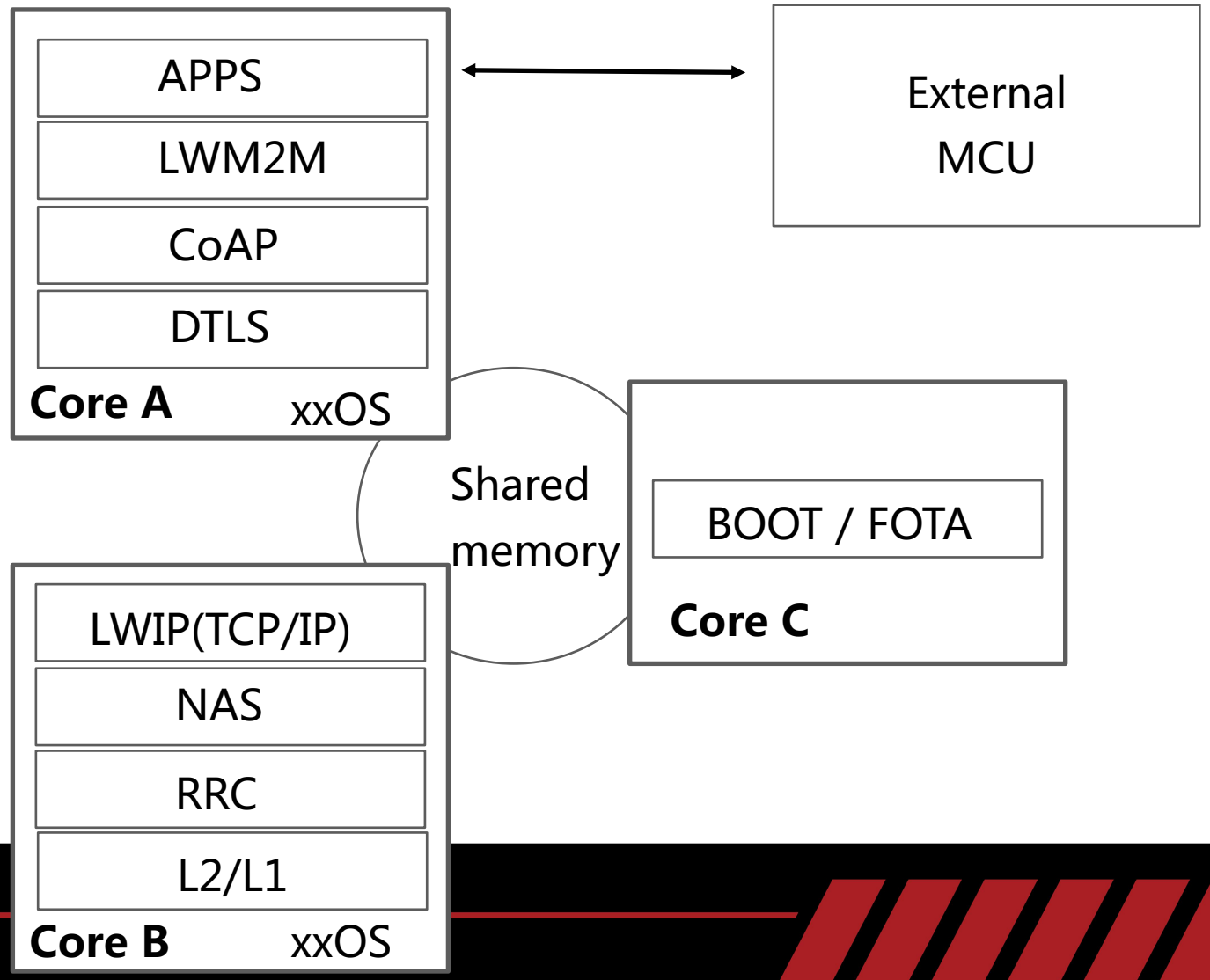
Overview of NB-IoT

- 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



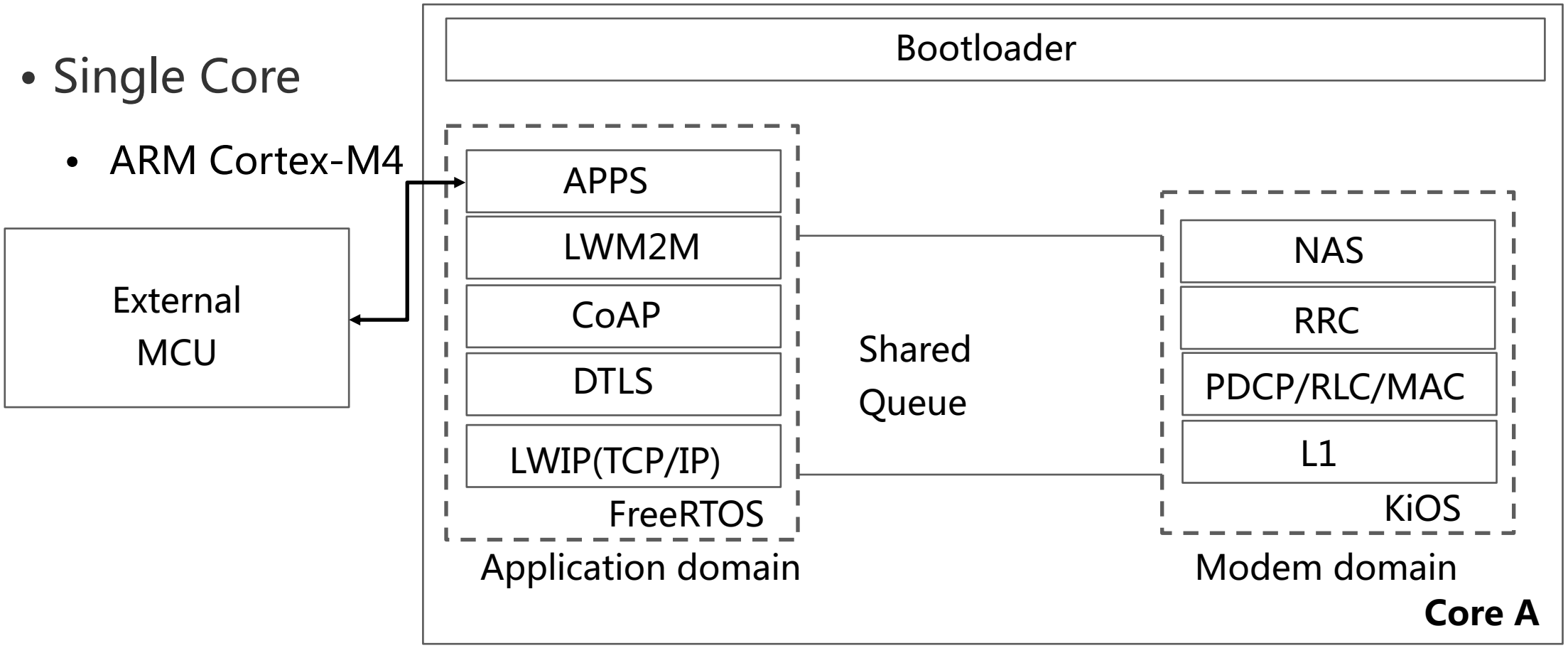
Architecture of NB-IoT Chip (A)

- Multi-Core
  - ARM Cortex-M0



Architecture of NB-IoT Chip (B)

- Single Core
  - ARM Cortex-M4



Attack Surface of NB-IoT Module

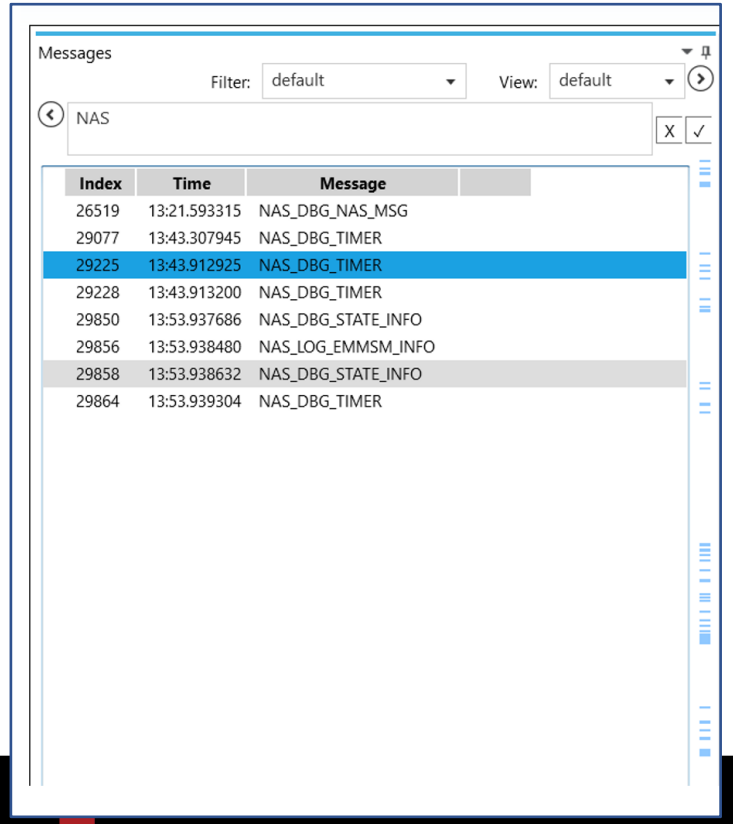
- APPS
  - at_cmd_handler
- LWM2M
  - object_function
- CoAP / MQTT / HTTP?
- TCP/IP
  - lwip .etc

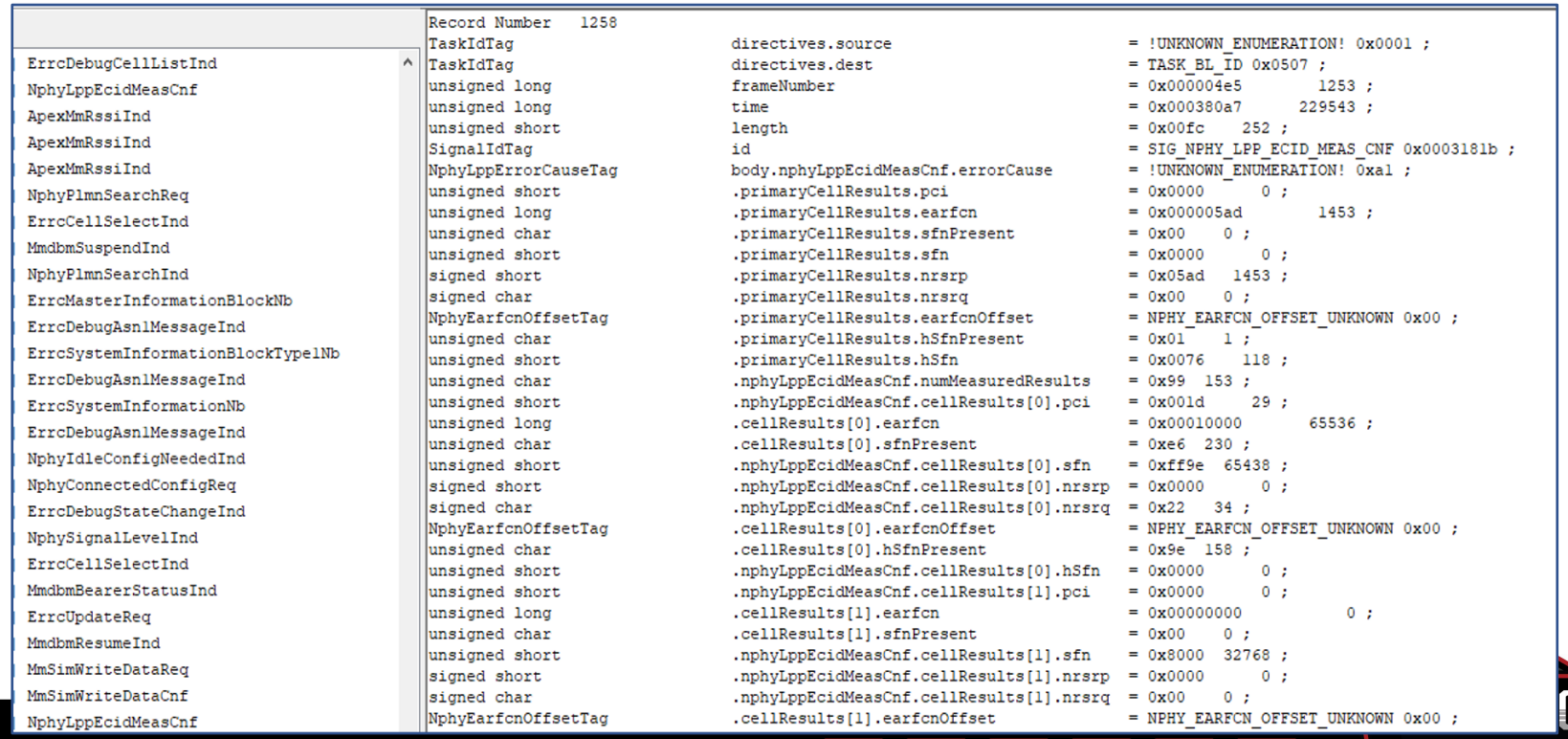
- NAS
  - ESM, EMM
- RRC
  - MIB, SIBx

- Inter-Core Communication

Our Practice

- LOG for debugging





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