Preventing SIM Box Fraud using Device Model Fingerprinting

Beomseok Oh*, Junho Ahn*, Sangwook Bae, Mincheol Son,
Yonghwa Lee, Minsuk Kang, and Yongdae Kim

KAIST Syssec

Introduction

- **Voice phishing (Voice scam fraud)**
  - Deceive victims through voice calls
  - Obtain personal infor. or money from the victims
  - Usually impersonate others
    - Family members, colleague
    - Government officials

Introduction

- ❖ Voice phishing is a big social issue in Korea

5년간 '보이스 피싱' 피해액 1.7조원...지인사칭 급증

[진화하는 보이스피싱] ① 누구든 당할 수 있다···연간 피해 5천억

- ❖ Voice phishing is also a global issue

A New Scam Is Making the Rounds Just in Time for Tax Season

If you haven't heard of "vishing," you may be at risk.

VERONIKA BONDARENKO • JAN 26, 2023 1:03 PM EST

https://www.thestreet.com/banking/what-is-vishing-scam

Introduction

- Criminals use various devices for voice phishing

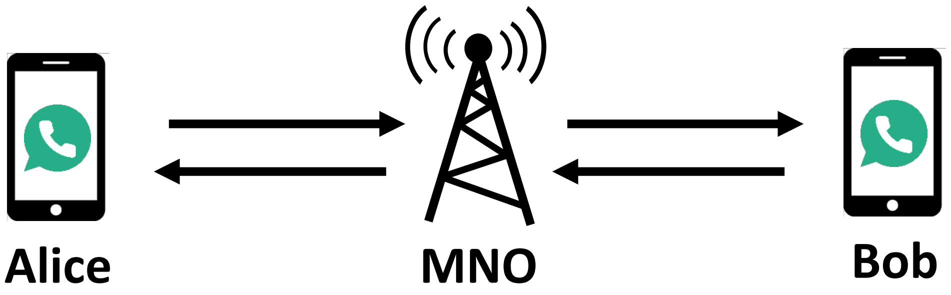
https://www.joongang.co.kr/article/25031604
https://busan.fnnews.com/news/202207071843193672

SIM Box

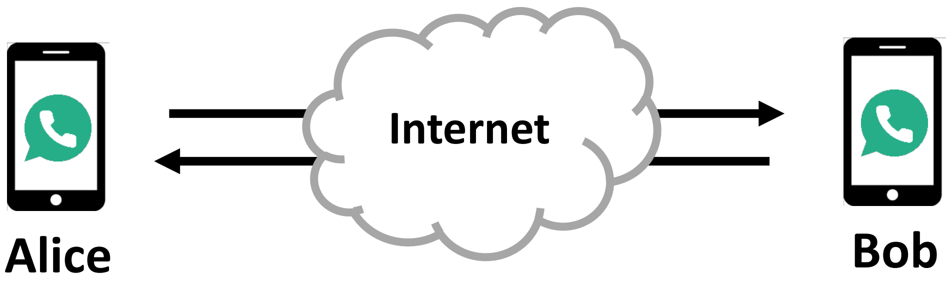
❖ What is a SIM Box?

- VoIP gateway converting cellular call to VoIP call and vice versa
  - Cellular call
    - Voice call through cellular network, routed by MNOs
  - VoIP call
    - Voice traffic converted into IP packets, routed through internet

Cellular call



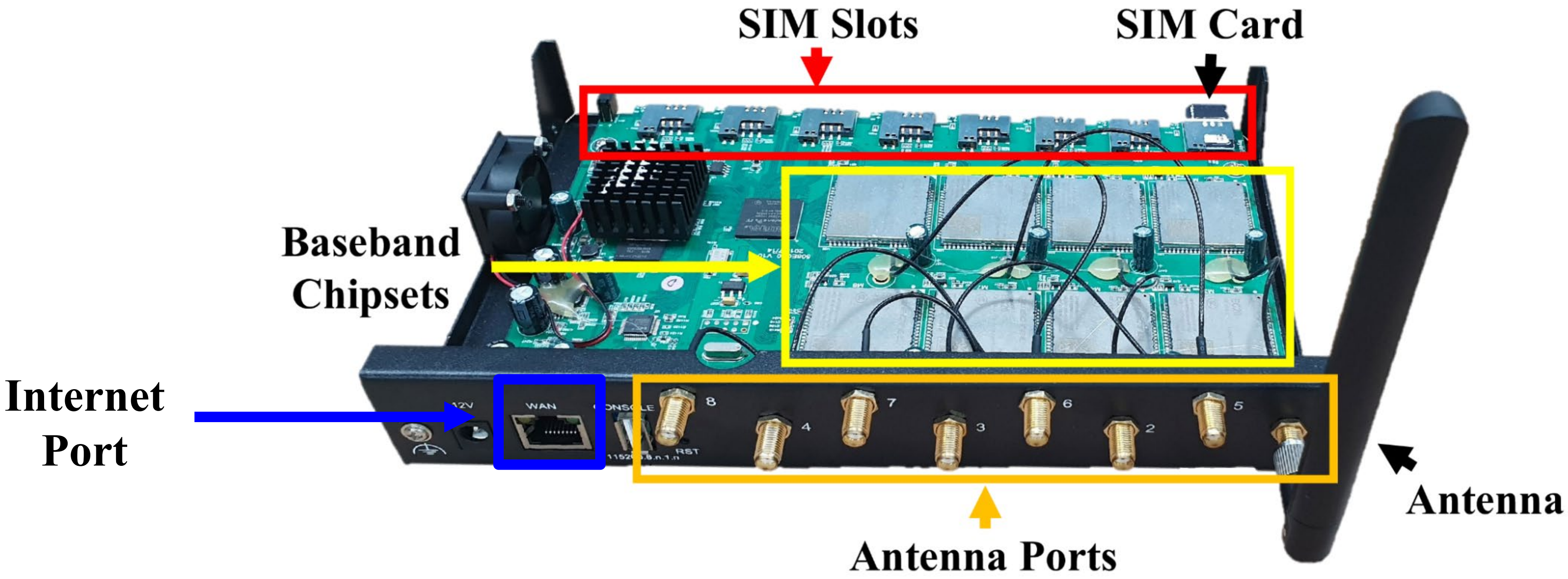
VoIP call



SIM Box

❖ What is a SIM Box?

- VoIP gateway converting cellular call to VoIP call and vice versa
- Contains multiple SIM slots & baseband chipsets & antennas
  - Enables multiple calls with a single device

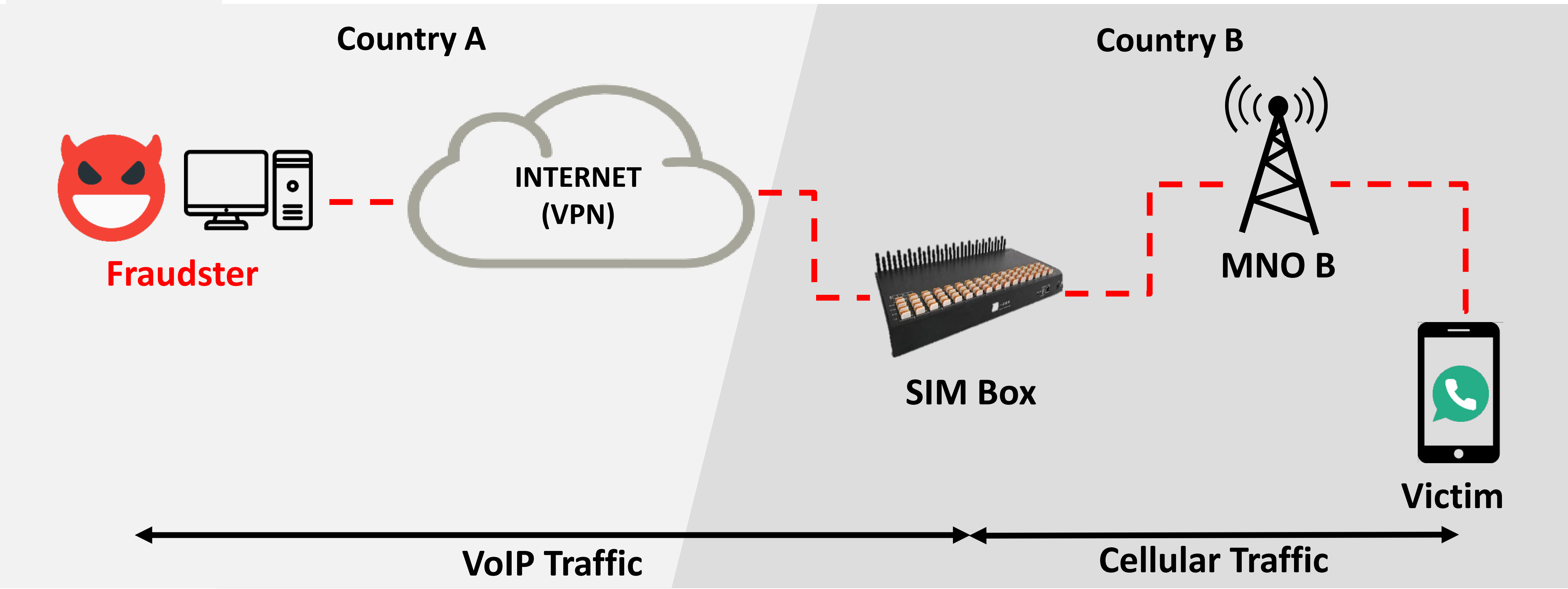


SIM Box Fraud

- **SIM Box fraud includes two types of frauds**
  - Voice phishing (Voice scam fraud)
    - Impersonate close people of victims to obtain personal infor. or money
    - Financial damage to individuals
  - Interconnect bypass fraud
    - Bypass interconnection agreements (roaming) to reduce cost
    - Financial damage to MNOs

Abuse of SIM Box - Voice phishing

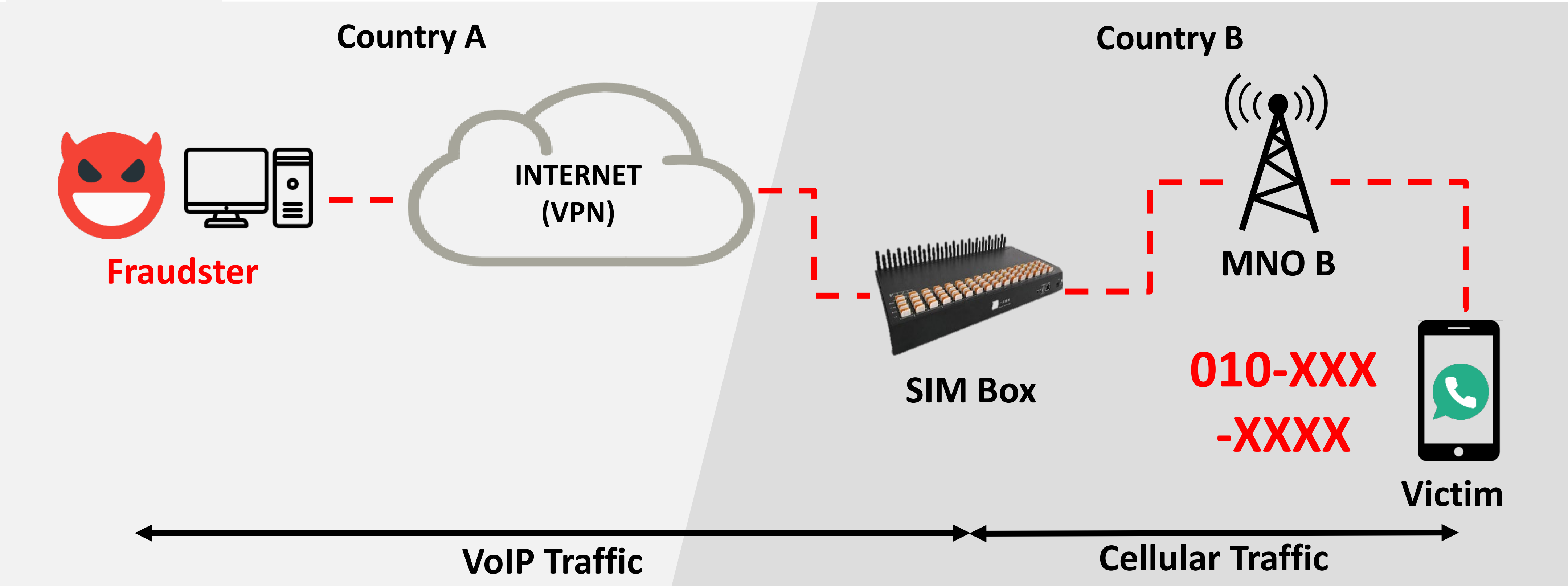
- **Call Flow of Voice Phishing (Voice Scam Fraud)**
  - With SIM Boxes, phishers can call to victim without roaming



* MNO: Mobile Network Operator

Abuse of SIM Box - Voice phishing

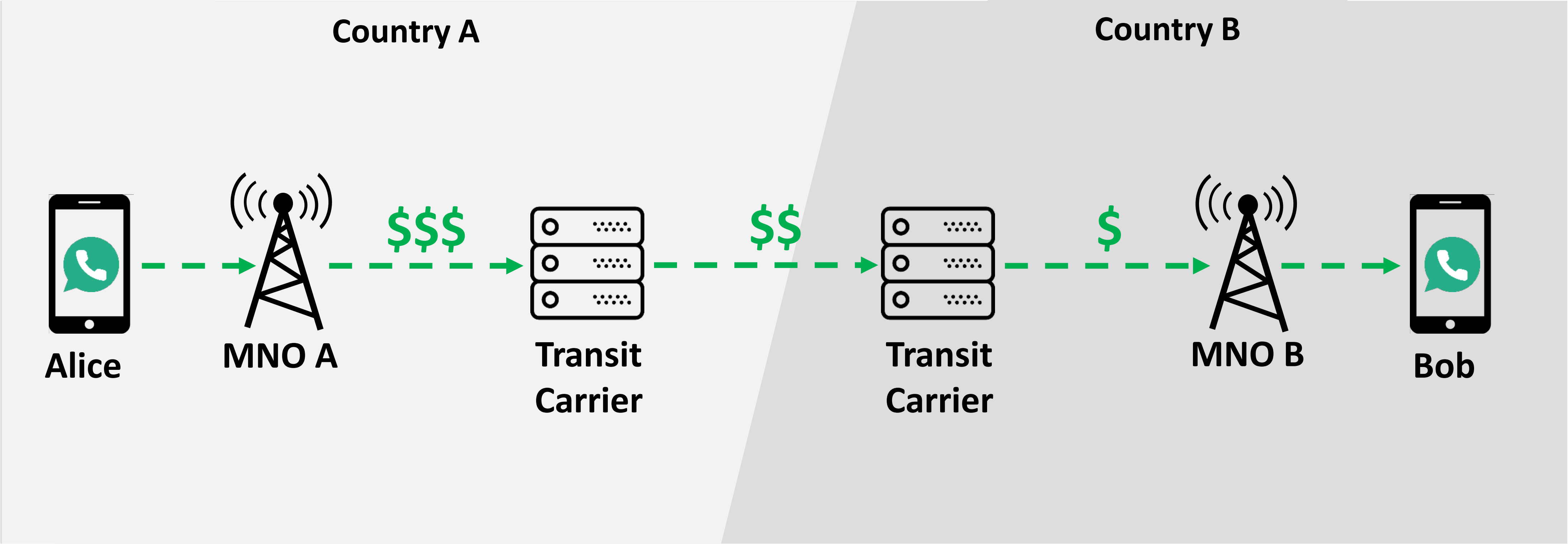
- **Advantages of fraudsters using SIM Boxes**
  - Easy to deceive victims: Local phone number appears on the victim's phone



* MNO: Mobile Network Operator

Abuse of SIM Box – Interconnect Bypass Fraud

- **Call flow of general roaming sceanario**
  - Traffic is routed through transit carriers
  - MNO obtains money from the routed traffic



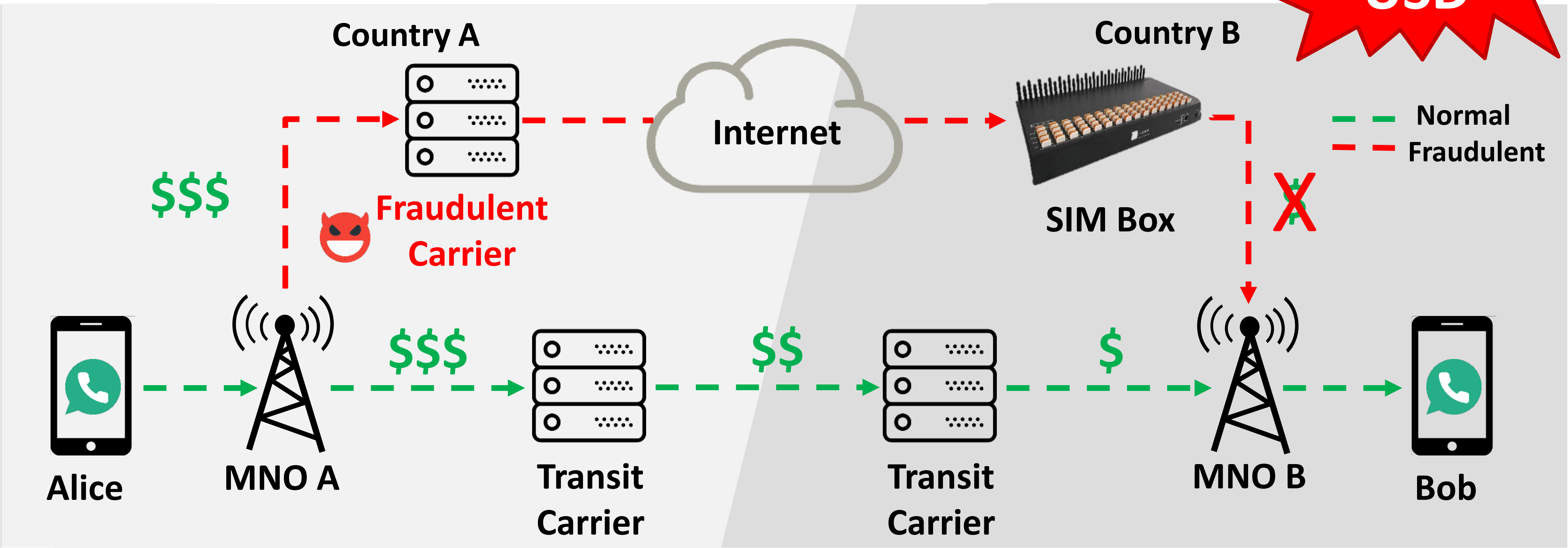
* Fraud Loss Survey Report, 2021

Abuse of SIM Box – Interconnect Bypass Fraud

❖ **Interconnect bypass fraud**

- Fraudulent carrier converts international calls to local calls
- Cause revenue loss of Mobile Network Operators

3.11 B USD*



* Fraud Loss Survey Report, 2021

Previous approaches to detect SIM Box

- **“SIM box call” detection using packet loss**
  - Conversion of packets to different codec cause more packet loss
  - PinDr0p [1], Boxed Out [2]

- **“SIM box” detection using call detail records (CDR)**
  - Detecting SIM Box Fraud Using Neural Network [3]
  - Detecting SIM Box Fraud by Using SVM and ANN [4]

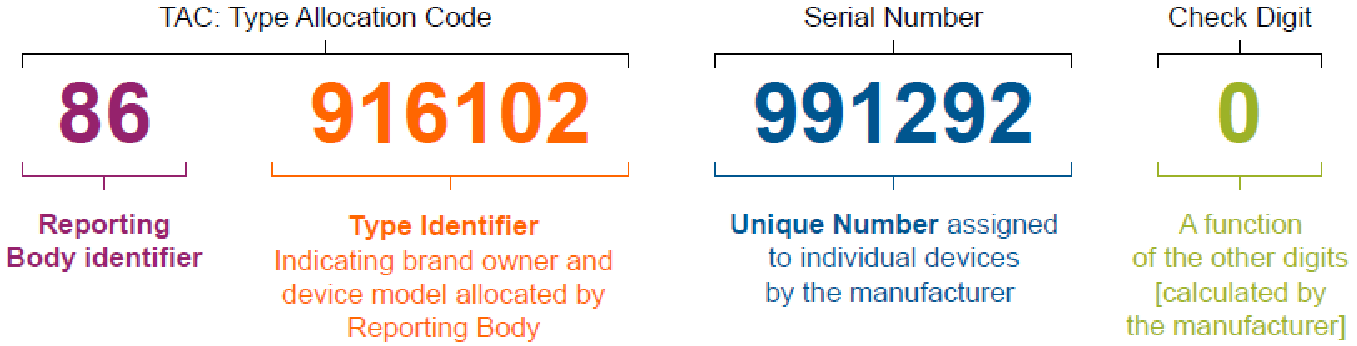
- **Limitation**
  - SIM boxes are only detected after calls are made
  - Frauds **cannot be prevented**

[1] Balasubramaniyan.et.al., CCS’10 [2] B. Reaves et.al., Usenix Sec’15 [3] Ibrahim.et.al., 2012 [4] Sallehuddin.et.al., 2015

Previous approaches to detect SIM Box

- **IMEI (International Mobile Equipment Identity)**
  - 15 digit identifier allocated to every cellular devices
    - Primary design to identify devices individually
  - Currently in use for banning stolen/malicious devices

- **Type allocation code (TAC)**
  - First 8 digits of IMEI
  - Represents device model / baseband model (IoT)

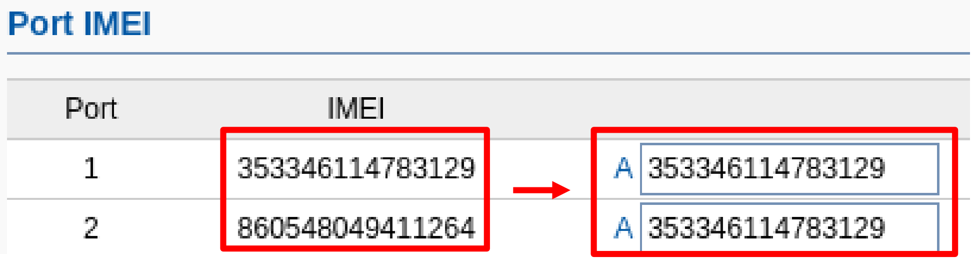

TAC: Type Allocation Code
Serial Number
Check Digit
86
916102
991292
0
Reporting Body identifier
Type Identifier Indicating brand owner and device model allocated by Reporting Body
Unique Number assigned to individual devices by the manufacturer
A function of the other digits [calculated by the manufacturer]

Model	TAC
iPhone 13	35757387
iPhone 6	35207506
Galaxy S10	35480910
EC-25	86483904

Previous approaches to detect SIM Box

- **Limitation of using IMEI**
  - Cellular network has no verification process for IMEI
    - IMEI works as primary key to identify device itself
  - Network cannot detect manipulated IMEI

- **IMEI-based access control would not work for SIM box**
  - SIM boxes support IMEI manipulation



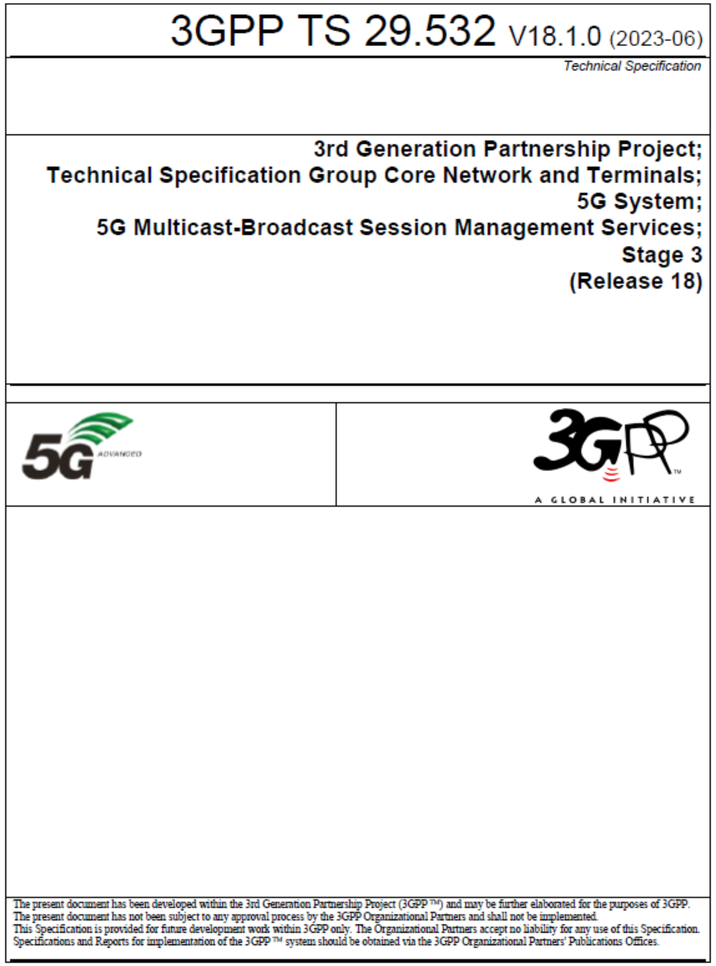
Port IMEI

Port	IMEI		
1	353346114783129	→	A 353346114783129
2	860548049411264		A 353346114783129

Intuition from standards

❖ Cellular Standard

- Defines "almost everything" of cellular
    - Network, device, communications… etc.
    - Suggested behavior in specific scenarios
- Large number of documents & Huge volume for each
- Cellular industry should obey standards
    - MNOs
    - Device manufacturers
- Standards are being kept updated



3GPP TS 29.532 V18.1.0 (2023-06)

Technical Specification

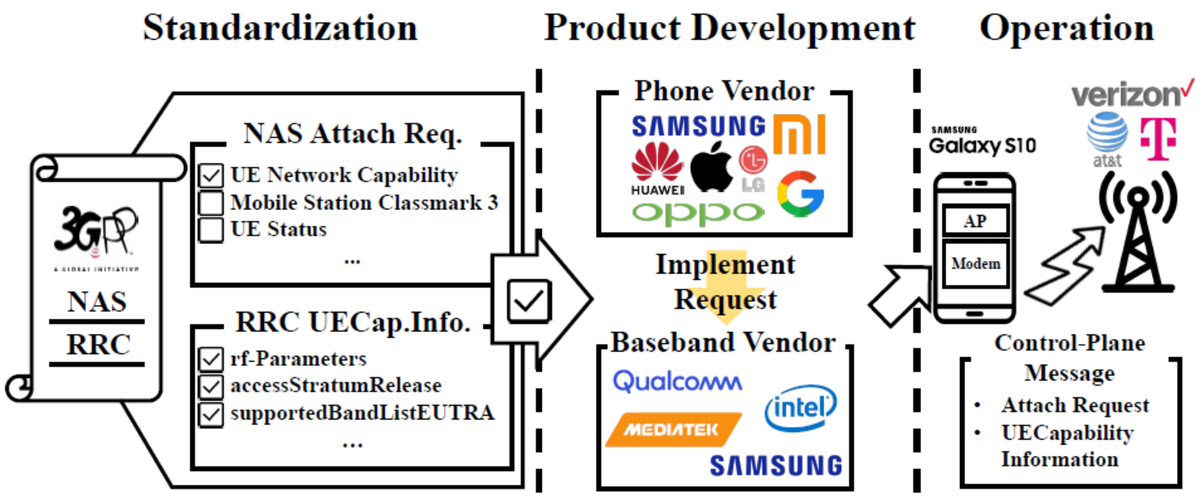
3rd Generation Partnership Project;
Technical Specification Group Core Network and Terminals;
5G System;
5G Multicast-Broadcast Session Management Services;
Stage 3
(Release 18)

The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and Reports for implementation of the 3GPP ™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Intuition from standards

Every year…

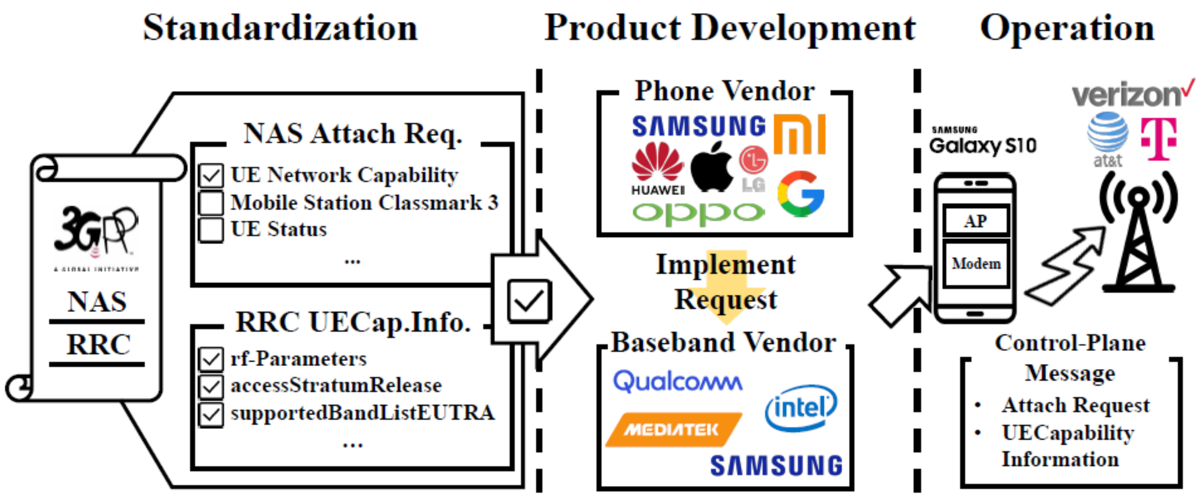
- 3GPP adds new cellular capabilities for devices to their specification



Intuition from standards

Every year…

- 3GPP adds new cellular capabilities for devices to their specification
- Baseband manufacturers produce new chipsets with new capabilities



Standardization

Product Development

Operation

NAS

RRC

NAS Attach Req.

☑ UE Network Capability
□ Mobile Station Classmark 3
□ UE Status
…

RRC UECap.Info.

☑ rf-Parameters
☑ accessStratumRelease
☑ supportedBandListEUTRA
…

Phone Vendor

Implement Request

Baseband Vendor

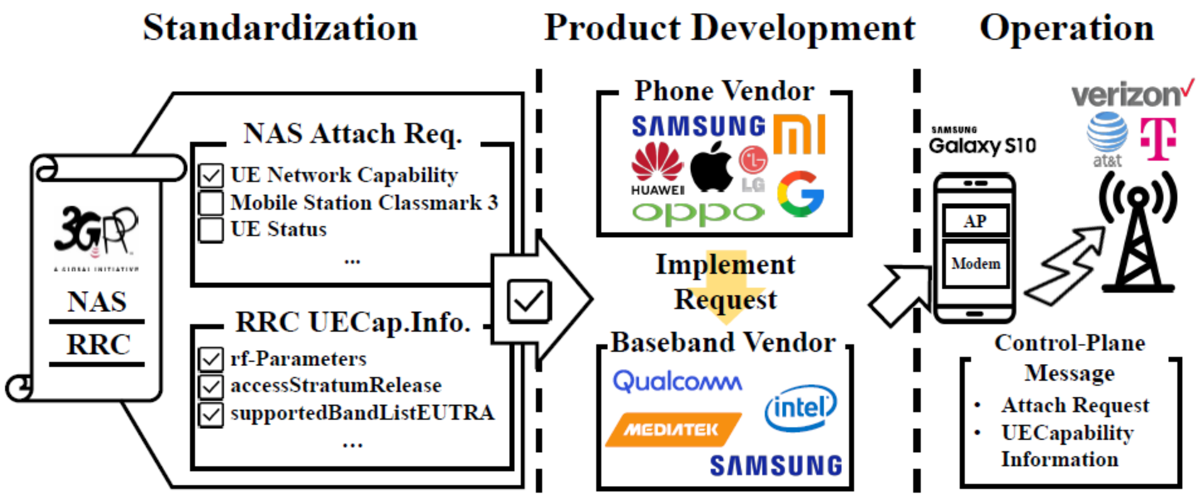
Control-Plane Message

- Attach Request
- UECapability Information

Intuition from standards

Every year…

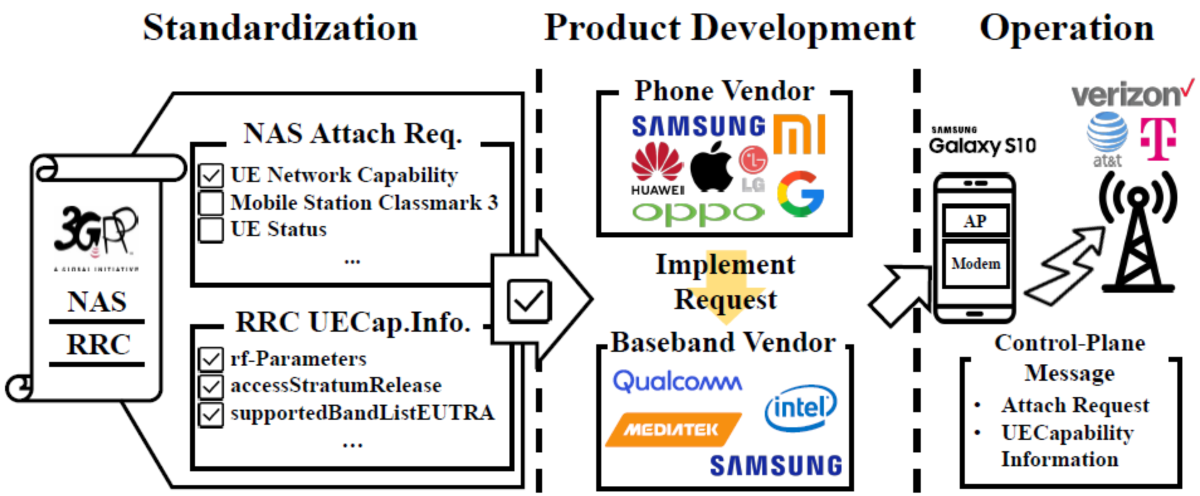
- 3GPP adds new cellular capabilities for devices to their specification
- Baseband manufacturers produce new chipsets with new capabilities
- Smartphone manufacturers produce new smartphones with new capabilities



Intuition from standards

Every year…

- 3GPP adds new cellular capabilities for devices to their specification
- Baseband manufacturers produce new chipsets with new capabilities
- Smartphone manufacturers produce new smartphones with new capabilities
- Most IoT devices (including SIM box) do not use high-end chipset



Intuition from standards

Every year…

- 3GPP adds new cellular capabilities for devices to their specification
- Baseband manufacturers produce new chipsets with new capabilities
- Smartphone manufacturers produce new smartphones with new capabilities
- Most IoT devices (including SIM box) do not use high-end chipset

	Galaxy S22	Galaxy S9	SIM Box
Carrier Aggregation	O	O	X
5G	O	X	X

Intuition from standards

Every year…

- 3GPP adds new cellular capabilities for devices to their specification
- Baseband manufacturers produce new chipsets with new capabilities
- Smartphone manufacturers produce new smartphones with new capabilities
- Most IoT devices (including SIM box) do not use high-end chipset

	Galaxy S22	Galaxy S9	SIM Box
Carrier Aggregation	O	O	X
5G	O	X	X

Intuition from standards

Every year…

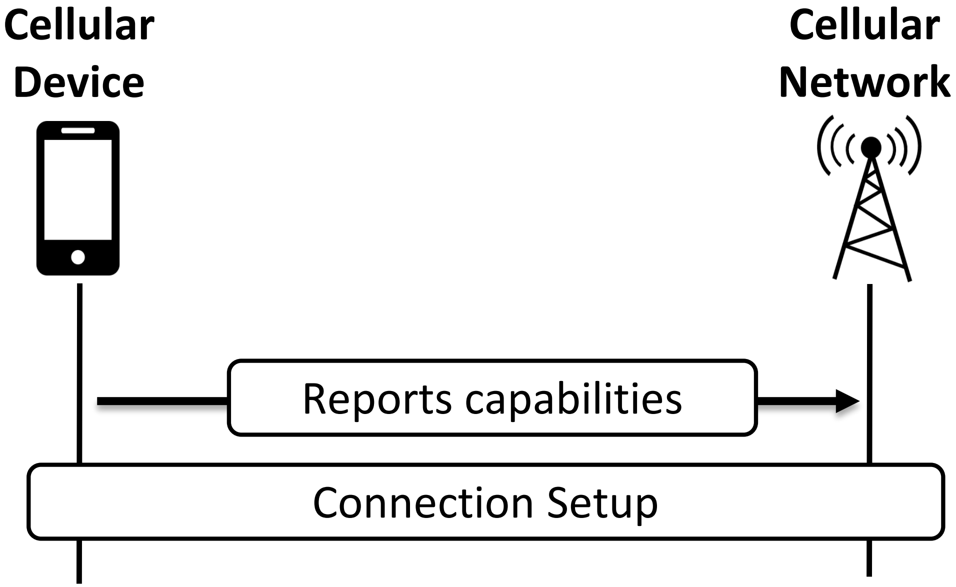
- 3GPP adds new cellular capabilities for devices to their specification
- Baseband manufacturers produce new chipsets with new capabilities
- Smartphone manufacturers produce new smartphones with new capabilities
- Most IoT devices (including SIM box) do not use high-end chipset

	Galaxy S22	Galaxy S9	SIM Box
Carrier Aggregation	O	O	X
5G	O	X	X

Fingerprints

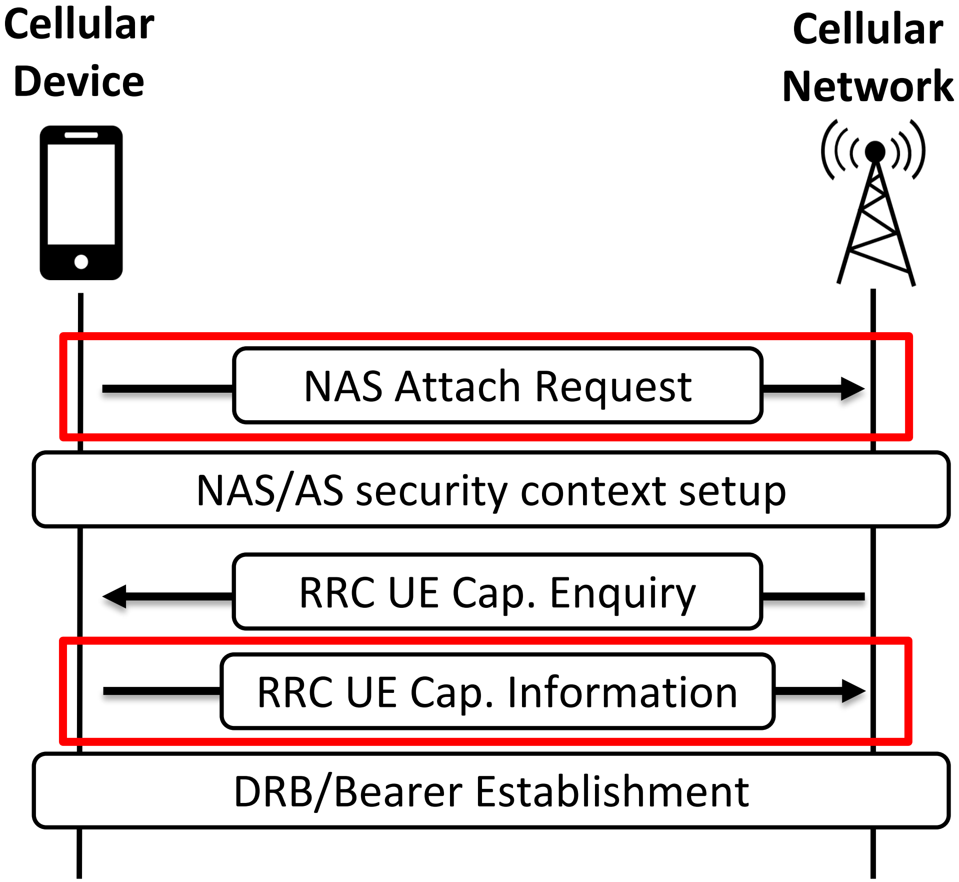
Collecting Device Capabilities

- **Network can collect device capabilities**
  - All cellular devices report own cellular capabilities to the network during attach
    - Capability information helps network to optimize & setup connection



Generating fingerprints

- **Utilized two control-plane messages**
  - NAS Attach Request
  - RRC UE Capability Information
- **The messages contain various features**
  - NAS Attach Request
    - Security algorithms: EIA/EEA 0/1/2
    - Network technologies: handover support
  - RRC UE Capability Information
    - Radio connection information: band support



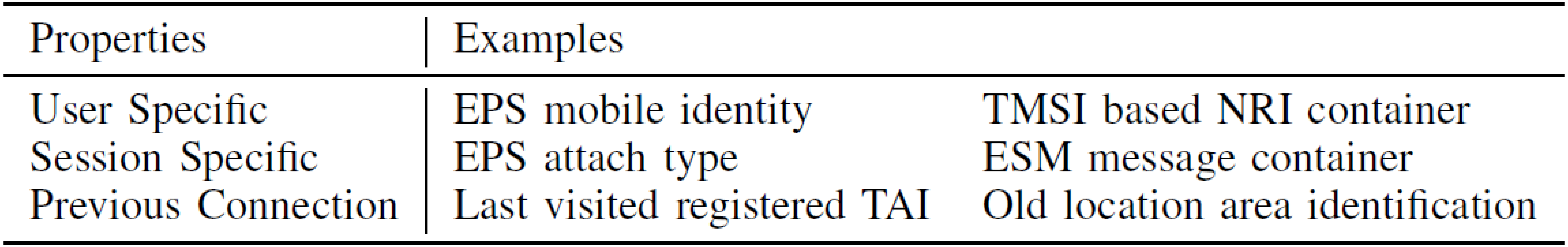
Considerations for “fingerprinting”

- **C1: Are all features helpful to represent device model?**
  - Some features may be affected by other factors
  - Performed additional analysis to prune the feature in the messages

Considerations for “fingerprinting”

- **C1: Are all features helpful to represent device model?**
  - Some features may be affected by other factors
  - Performed additional analysis to prune the feature in the messages

- **Cellular standard analysis**
  - The messages follow specific format in the standard
  - Analyzed 4 cellular standard documents (NAS & RRC) in total



Properties	Examples	
User Specific	EPS mobile identity	TMSI based NRI container
Session Specific	EPS attach type	ESM message container
Previous Connection	Last visited registered TAI	Old location area identification

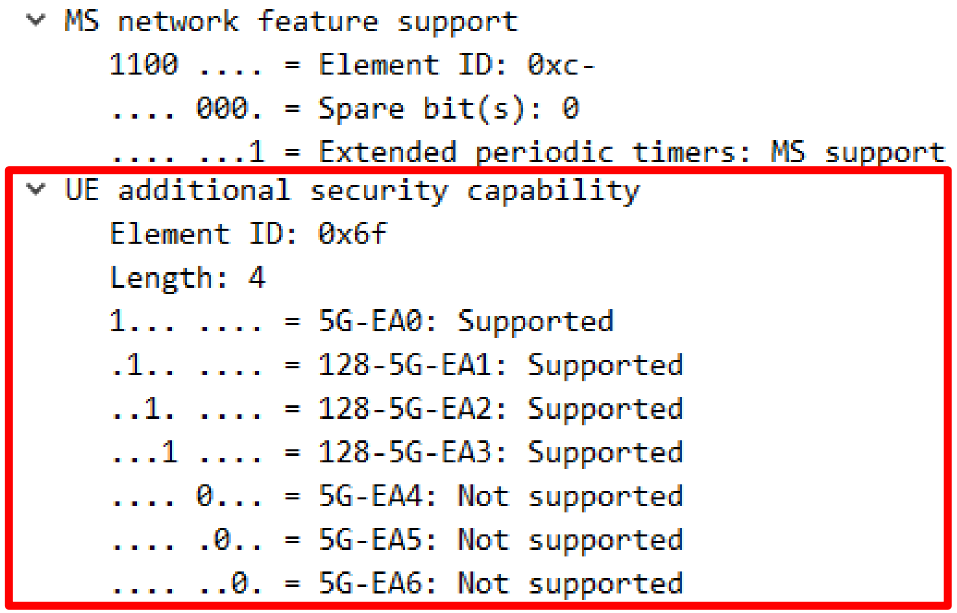
Considerations for “fingerprinting”

- **C2: Do different devices sharing same model report the same capabilities?**
  - E.g. Note20 from Alice, Note20 from Bob
  - Observed that most capabilities are same, but some can differ by device
    - Due to user’s custom device settings

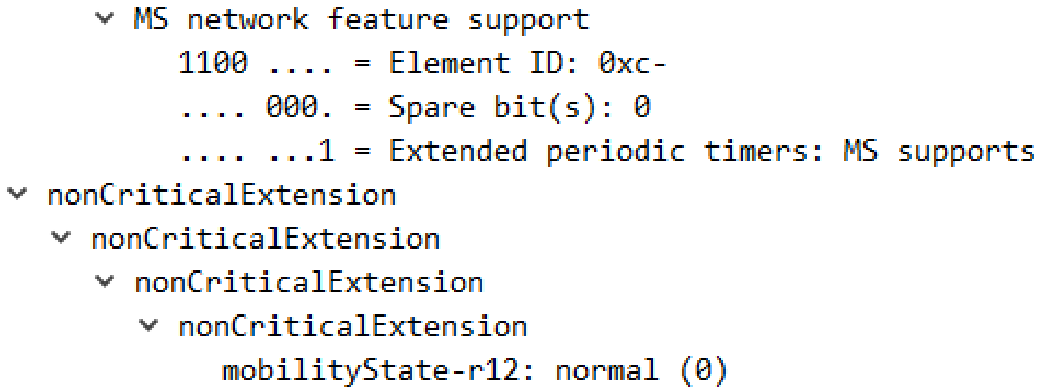
Considerations for “fingerprinting”

- **C2: Do different devices sharing same model report the same capabilities?**
  - Observed that supported capabilities can differ by device
    - Due to user’s custom device settings

“Default” setting → **LTE only setting**



```
⌄ MS network feature support
    1100 .... = Element ID: 0xc-
    .... 000. = Spare bit(s): 0
    .... ...1 = Extended periodic timers: MS support
⌄ UE additional security capability
    Element ID: 0x6f
    Length: 4
    1... .... = 5G-EA0: Supported
    .1.. .... = 128-5G-EA1: Supported
    ..1. .... = 128-5G-EA2: Supported
    ...1 .... = 128-5G-EA3: Supported
    .... 0... = 5G-EA4: Not supported
    .... .0.. = 5G-EA5: Not supported
    .... ..0. = 5G-EA6: Not supported
```

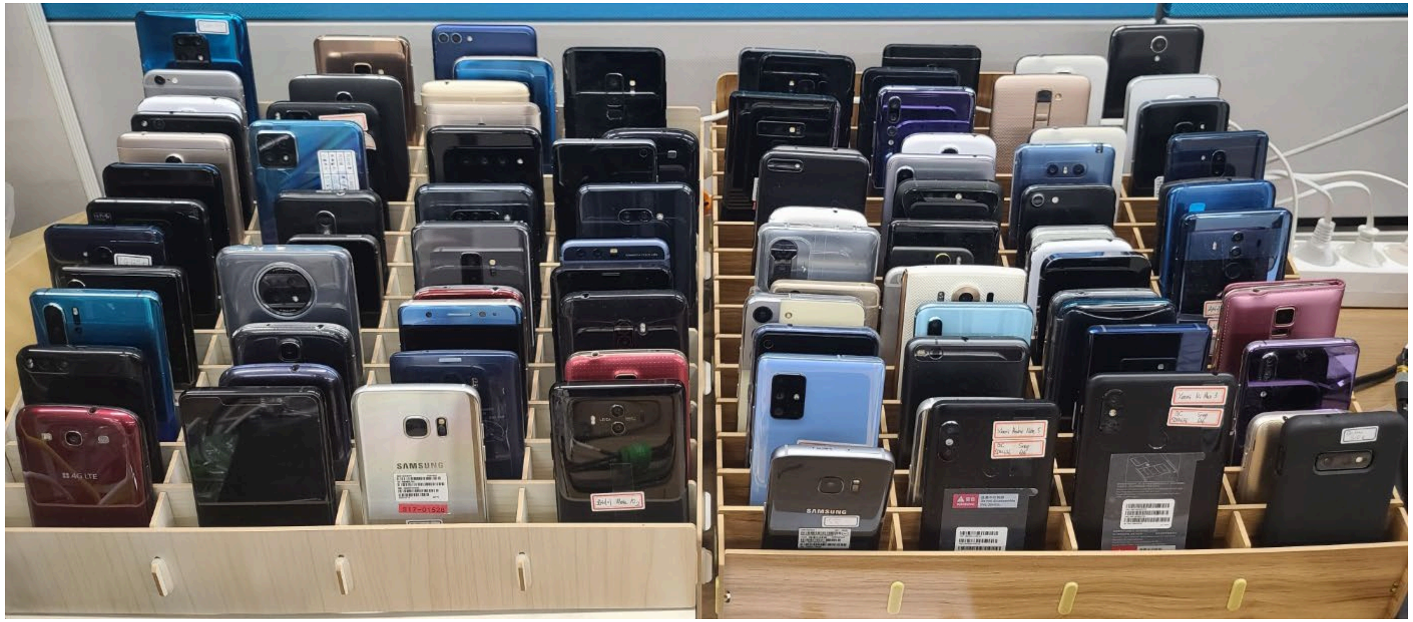


```
    ⌄ MS network feature support
        1100 .... = Element ID: 0xc-
        .... 000. = Spare bit(s): 0
        .... ...1 = Extended periodic timers: MS supports
⌄ nonCriticalExtension
    ⌄ nonCriticalExtension
        ⌄ nonCriticalExtension
            ⌄ nonCriticalExtension
                mobilityState-r12: normal (0)
```

→ No 5G-related security capabilities

Test Devices

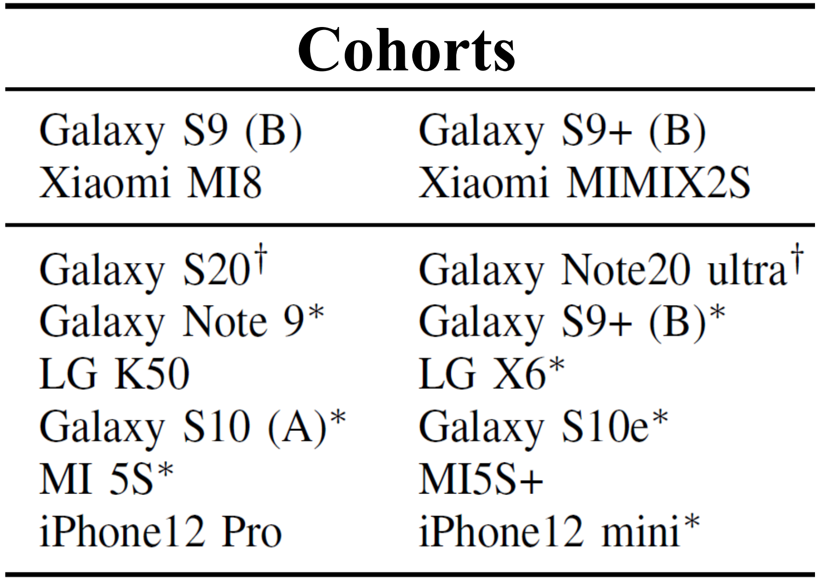
- **102 individual cellular device models**
  - 85 smartphones, 11 IoT devices, 6 SIM Boxes



Empirical Study on Fingerprints

- **Most smartphones have unique fingerprints**
  - Under default configuration, 83 out of 85 smartphones have unique fingerprints
  - Considering all configurations, only 8 pairs have overlapping fingerprints

- **Exceptions: Cohorts**
  - Some models have same fingerprints
    - Same baseband model
    - Same manufacturer
    - Similar release date (< 6 months)
  - Can be considered as same device model



Cohorts	
Galaxy S9 (B)	Galaxy S9+ (B)
Xiaomi MI8	Xiaomi MIMIX2S
Galaxy S20†	Galaxy Note20 ultra†
Galaxy Note 9*	Galaxy S9+ (B)*
LG K50	LG X6*
Galaxy S10 (A)*	Galaxy S10e*
MI 5S*	MI5S+
iPhone12 Pro	iPhone12 mini*

→ **Fingerprints can be used to distinguish smartphone models**

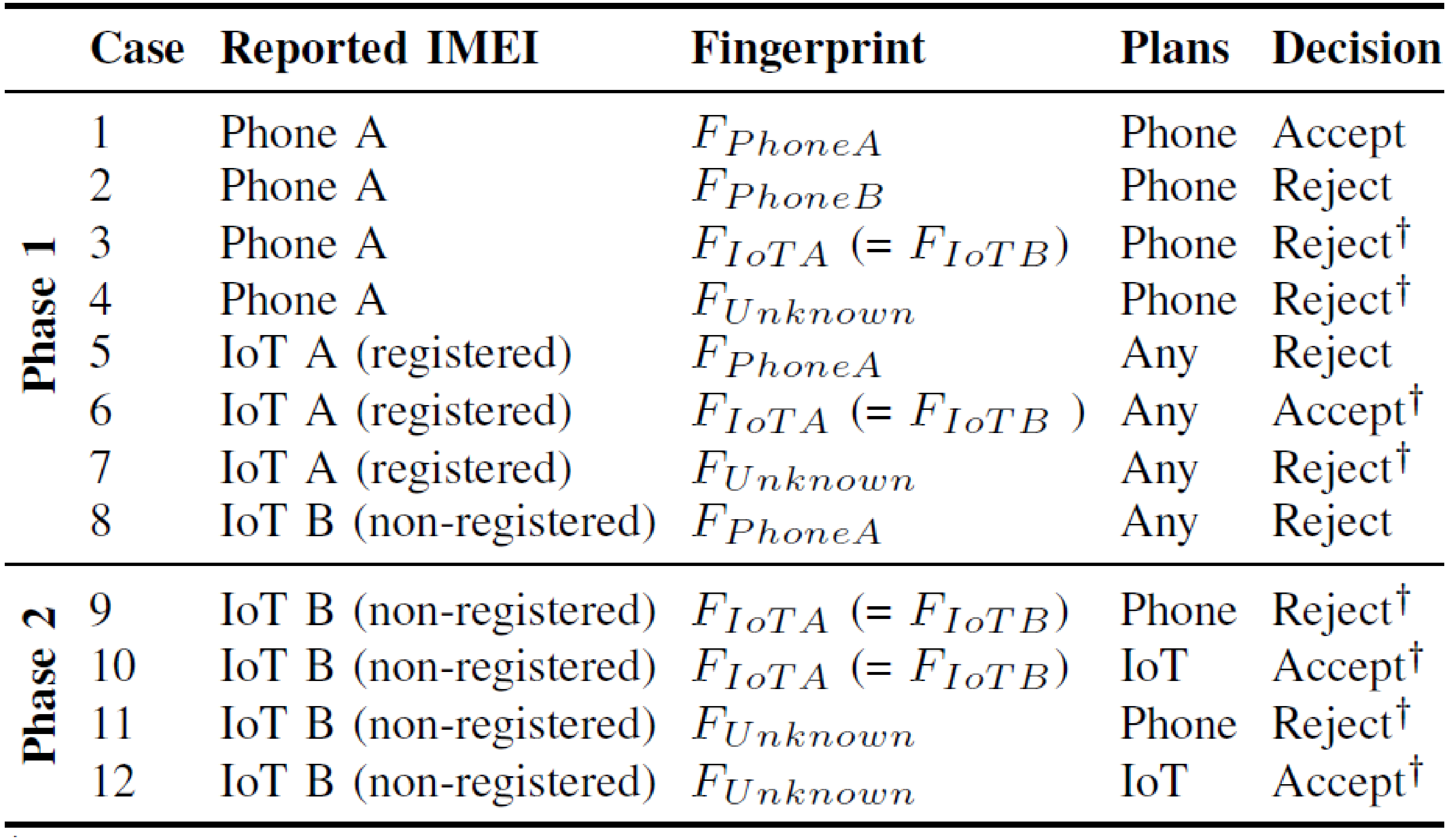
Empirical Study on Fingerprints

- **Smartphones and SIM boxes have different fingerprints**
  - Carrier aggregation (CA) related features
    - SIM boxes do not support CA as they only have single antenna for each chipset
  - Difference on baseband chipsets
    - SIM boxes use low-cost baseband chipsets; supporting protocol versions are lower

- **IoT devices and SIM boxes might have overlapping fingerprints**
  - Fingerprint of IoT devices are highly affected by baseband chipsets
  - If IoT devices contains same baseband chipsets, might have same fingerprints

Suggested Network Behavior

- Access Control List (ACL)



	Case	Reported IMEI	Fingerprint	Plans	Decision
Phase 1	1	Phone A	F_{PhoneA}	Phone	Accept
	2	Phone A	F_{PhoneB}	Phone	Reject
	3	Phone A	F_{IoTA} (= F_{IoTB})	Phone	Reject†
	4	Phone A	$F_{Unknown}$	Phone	Reject†
	5	IoT A (registered)	F_{PhoneA}	Any	Reject
	6	IoT A (registered)	F_{IoTA} (= F_{IoTB})	Any	Accept†
	7	IoT A (registered)	$F_{Unknown}$	Any	Reject†
	8	IoT B (non-registered)	F_{PhoneA}	Any	Reject
Phase 2	9	IoT B (non-registered)	F_{IoTA} (= F_{IoTB})	Phone	Reject†
	10	IoT B (non-registered)	F_{IoTA} (= F_{IoTB})	IoT	Accept†
	11	IoT B (non-registered)	$F_{Unknown}$	Phone	Reject†
	12	IoT B (non-registered)	$F_{Unknown}$	IoT	Accept†

Conclusion

- **Proposed network-level SIM box detection using device capabilities**
  - SIM Boxes can be distinguished from smartphones via fingerprints
    - Some IoT devices may have overlapping fingerprints with SIM Boxes
  - Robust against IMEI manipulation
  - Enables to prevent SIM Boxes from making calls in cellular network

- **Currently in discussion with a tier-1 MNO in Korea for deployment**

- **A large project from Korean police to fight with voice phishing crime**
  - This research was supported and funded by the Korean National Police Agency*

* Project Name: Tracking and identifying devices and call traffic in voice phishing ecosystem / Project Number: PR10-03-020-22

Q&A: Good questions

- [허현] This paper uses the fingerprinting technique as a defense mechanism. However, device fingerprinting is an attack mechanism in web security or privacy areas. Doesn't this mitigation raise privacy concerns?

- [정수환] Even if the network employs this paper's fingerprinting technology to block specific SIM boxes' SIM data, considering there are multiple SIMs within one SIM Box, would it be feasible to block all SIMs within that specific SIM Box once a single SIM is fingerprinted?

Q&A: Good questions

- [김광민] Can you successfully distinguish an attacker who spoofs a message with the same capabilities as a commercial device?

- [박승민] When creating an ACL using a fingerprint database, is there an overhead in storing / updating / searching the database?

- [Valentin] Can the system adapt to entirely new smartphone models or significant changes in smartphone technology?
- [Valentin] Because the network can falsely reject smartphones if the network doesn't have comprehensive smartphone fingerprints, (how) can the system adapt to different network sizes / natures?

Thank You. Questions?

- You can reach us
  - Beomseok Oh (beomseoko@kaist.ac.kr)
  - Junho Ahn (dwg226@kaist.ac.kr)
  - https://sites.google.com/view/devicefingerprinting

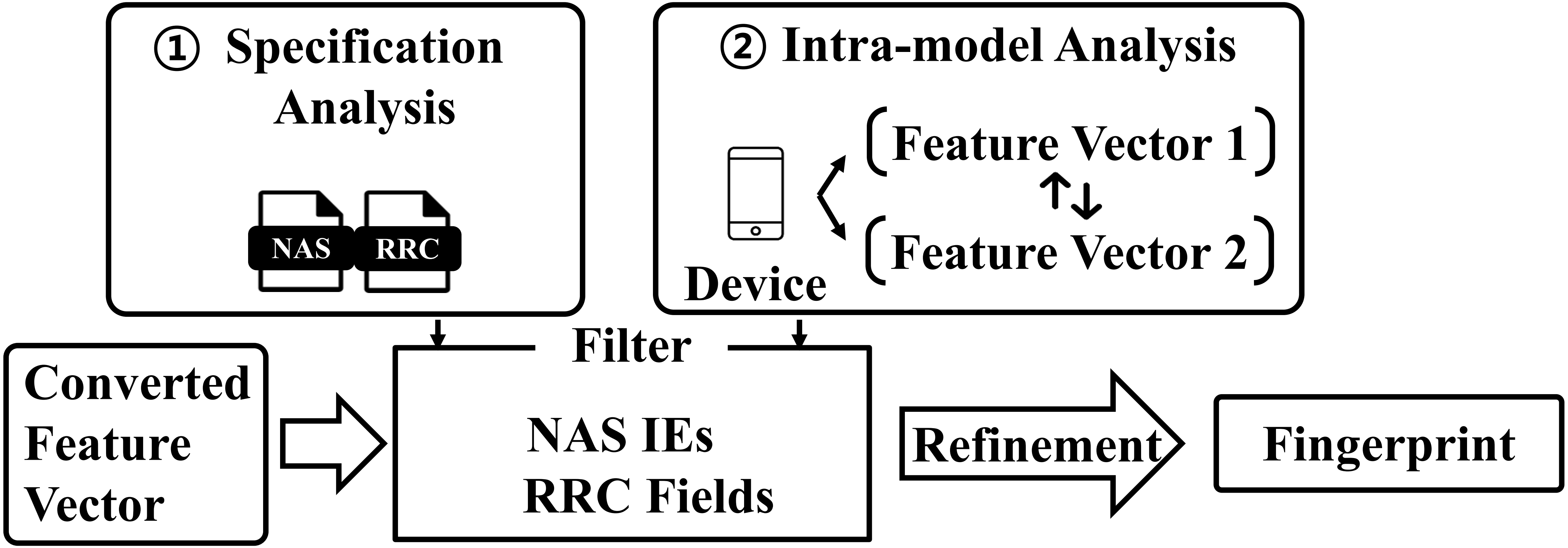
What make fingerprints unique?

- **Baseband vendors**
  - Vendors employ unique configurations for several technologies
    - Use different configuration on battery saving technology (DRX)
    - Support of positioning technology (OTDOA)
- **Phone vendors**
  - Vendors choose to support several capabilities
    - Security algorithms: EIA3, EEA3

→ **Different baseband vendors & phone vendors make unique fingerprints**

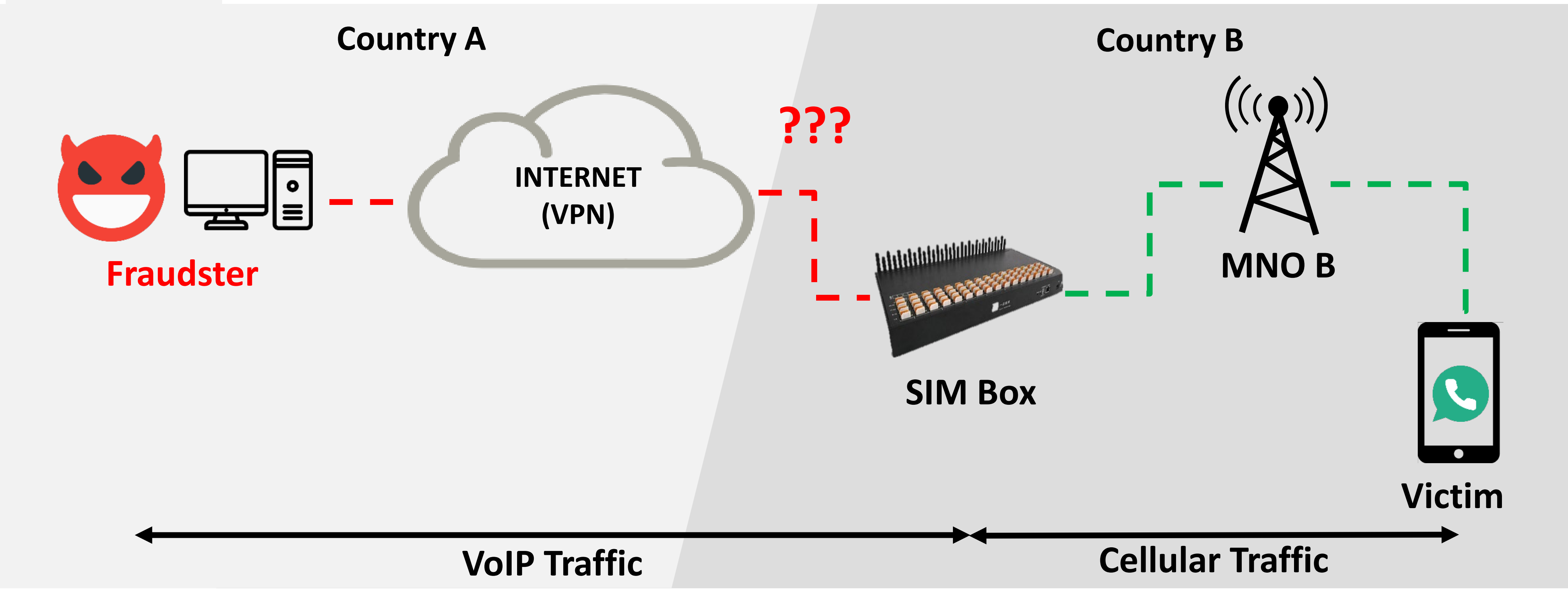
Consideration 2: Feature Pruning

- Not all features are device-model-specific
- Additional analysis are performed to prune the feature



Abuse of SIM Box - Voice phishing

- **Advantages of fraudsters using SIM Boxes**
  - Hard to track fraudsters



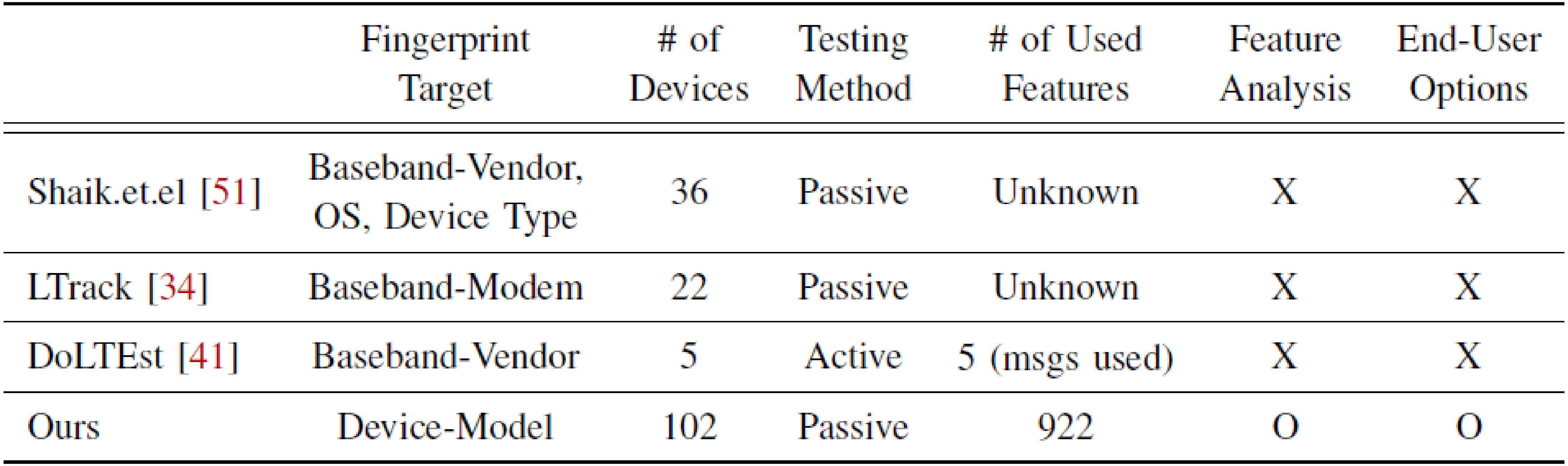
* MNO: Mobile Network Operator

Abuse of SIM Box - Voice phishing

- **Advantages of fraudsters using SIM Boxes**
  - Location of SIM Boxes are also hard to track

https://v.daum.net/v/20230515141119663
http://www.adinews.co.kr/news/articleView.html?idxno=61379

Comparison with previous works



	Fingerprint Target	# of Devices	Testing Method	# of Used Features	Feature Analysis	End-User Options
Shaik.et.el [51]	Baseband-Vendor, OS, Device Type	36	Passive	Unknown	X	X
LTrack [34]	Baseband-Modem	22	Passive	Unknown	X	X
DoLTEst [41]	Baseband-Vendor	5	Active	5 (msgs used)	X	X
Ours	Device-Model	102	Passive	922	O	O

Open-world Evaluation

Questions to answer

- Is unknown device classified as unknown?
- Is known device classified as known?

Evaluation

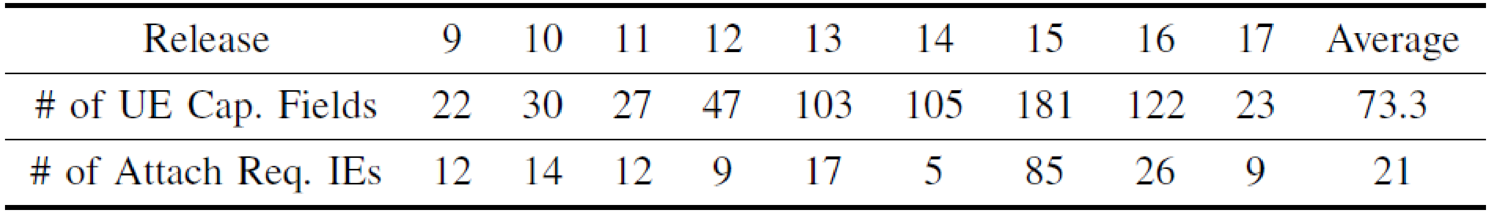
- Constructed new fingerprint dataset with 30 devices
  - Consisting of 15 known device models and 15 unknown device models
- Matched with original dataset (with 102 devices)

Results

- Unknown devices are classified as unknown (15/15)
- Most known device are classified as known (12/15): Due to the configuration

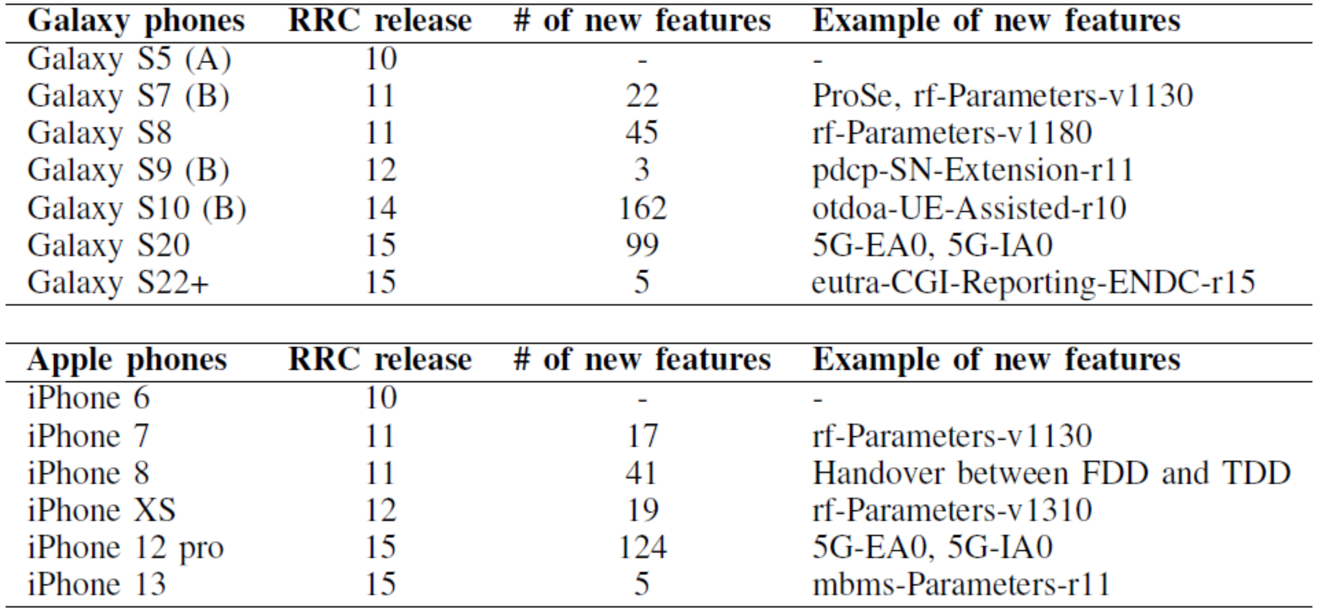
Will new device have new fingerprints?

- New capabilities are keep added to the standards



Release	9	10	11	12	13	14	15	16	17	Average
# of UE Cap. Fields	22	30	27	47	103	105	181	122	23	73.3
# of Attach Req. IEs	12	14	12	9	17	5	85	26	9	21

- New devices follow new standards, thus contain new features

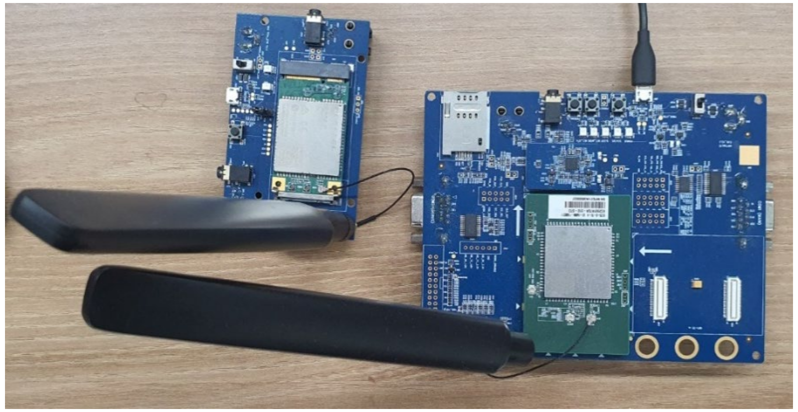


Galaxy phones	RRC release	# of new features	Example of new features
Galaxy S5 (A)	10	-	-
Galaxy S7 (B)	11	22	ProSe, rf-Parameters-v1130
Galaxy S8	11	45	rf-Parameters-v1180
Galaxy S9 (B)	12	3	pdcp-SN-Extension-r11
Galaxy S10 (B)	14	162	otdoa-UE-Assisted-r10
Galaxy S20	15	99	5G-EA0, 5G-IA0
Galaxy S22+	15	5	eutra-CGI-Reporting-ENDC-r15

Apple phones	RRC release	# of new features	Example of new features
iPhone 6	10	-	-
iPhone 7	11	17	rf-Parameters-v1130
iPhone 8	11	41	Handover between FDD and TDD
iPhone XS	12	19	rf-Parameters-v1310
iPhone 12 pro	15	124	5G-EA0, 5G-IA0
iPhone 13	15	5	mbms-Parameters-r11

Can fraudsters bypass our system?

- **Changing SIM box configuration (VIII-A)**
  - SIM box cannot have same fingerprints with phones
  - Made own SIM box for the experiment
  - Sent various AT commands



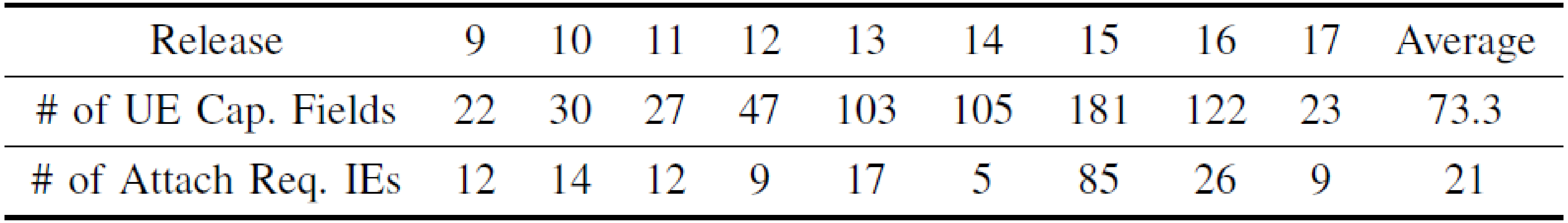
- **Using MitM scheme (VIII-B)**
  - Message can be encrypted; fraudsters cannot modify freely

- **Implementing software SIM box (VIII-C)**
  - Too costly; even state-of-the-art SDR requires to implement lots of functions
  - We showed that several functions (e.g. VoLTE, 3G redirection) are needed

Overhead of the system

- **Feature Vector Conversion and Collection**
  - Leverage semi-automated procedure

- **Specification Analysis**
  - Bootstrap
    - About 6 hours
  - Specification Updates
    - Specifications are not written from scratch; expansion of previous versions

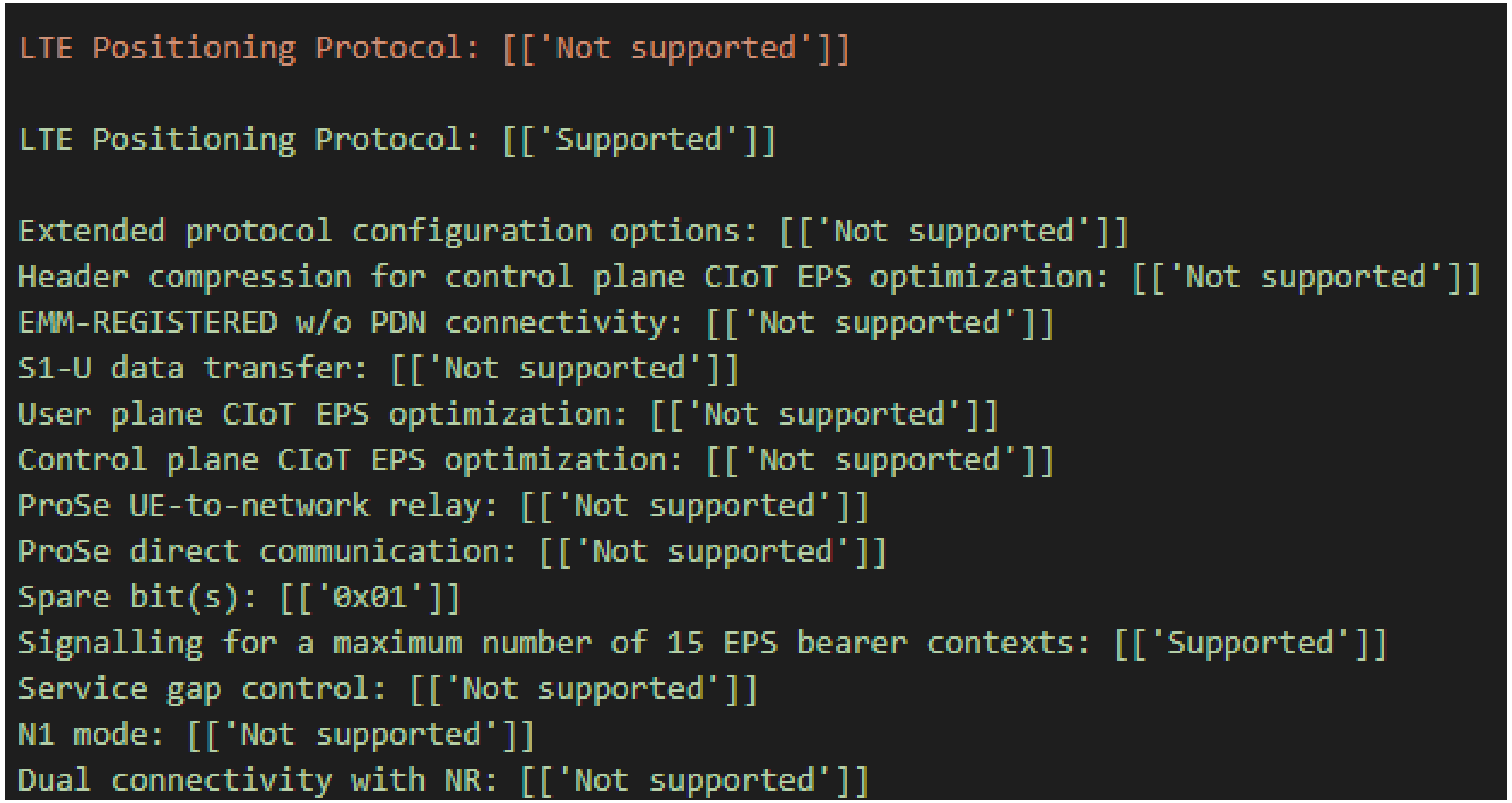


Release	9	10	11	12	13	14	15	16	17	Average
# of UE Cap. Fields	22	30	27	47	103	105	181	122	23	73.3
# of Attach Req. IEs	12	14	12	9	17	5	85	26	9	21

# of new features in each specification version

Analysis Result – SIM Box Detection

- **SIM boxes have different fingerprint with smartphones**
  - Ejoin SIM box vs Galaxy S20 (Qualcomm)



```
LTE Positioning Protocol: [['Not supported']]

LTE Positioning Protocol: [['Supported']]

Extended protocol configuration options: [['Not supported']]
Header compression for control plane CIoT EPS optimization: [['Not supported']]
EMM-REGISTERED w/o PDN connectivity: [['Not supported']]
S1-U data transfer: [['Not supported']]
User plane CIoT EPS optimization: [['Not supported']]
Control plane CIoT EPS optimization: [['Not supported']]
ProSe UE-to-network relay: [['Not supported']]
ProSe direct communication: [['Not supported']]
Spare bit(s): [['0x01']]
Signalling for a maximum number of 15 EPS bearer contexts: [['Supported']]
Service gap control: [['Not supported']]
N1 mode: [['Not supported']]
Dual connectivity with NR: [['Not supported']]
```