KAIST

Syssec

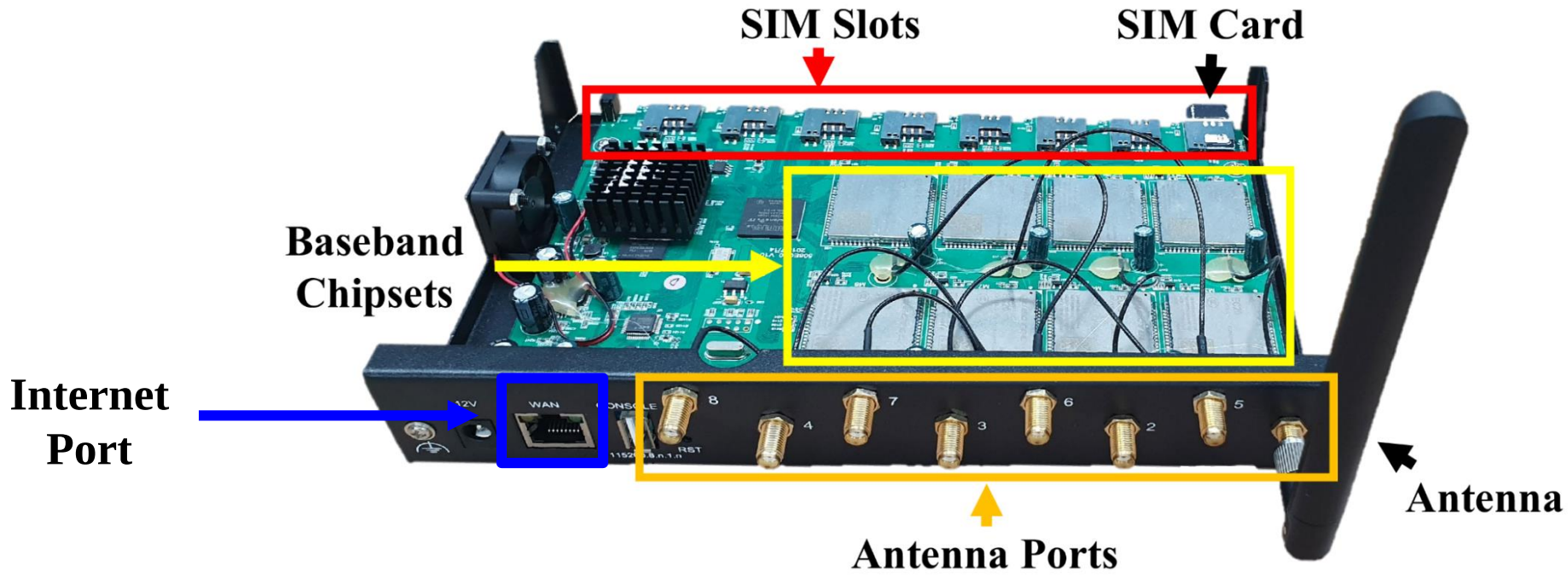
Preventing SIM Box Fraud Using Device Model Fingerprinting

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

KAIST Syssec

SIM Box

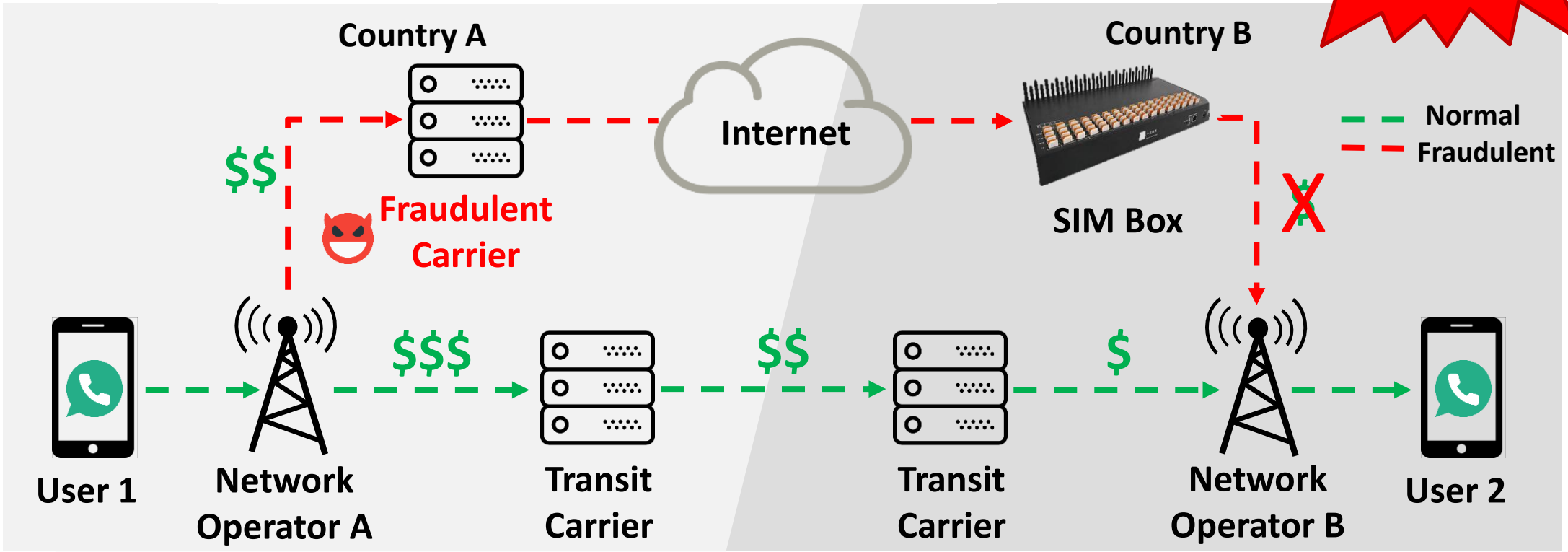
- **What is a SIM Box?**
  - VoIP Gateway converting VoIP call to cellular call and vice versa
  - Contains multiple SIM slots & baseband chipsets & antennas
    - Enables multiple calls with a single device



Illegal Use of SIM Box

- **Interconnect Bypass Fraud**
  - Convert routed international calls to local calls using SIM Boxes
  - Cause revenue loss of Mobile Network Operators

3.11 B USD*

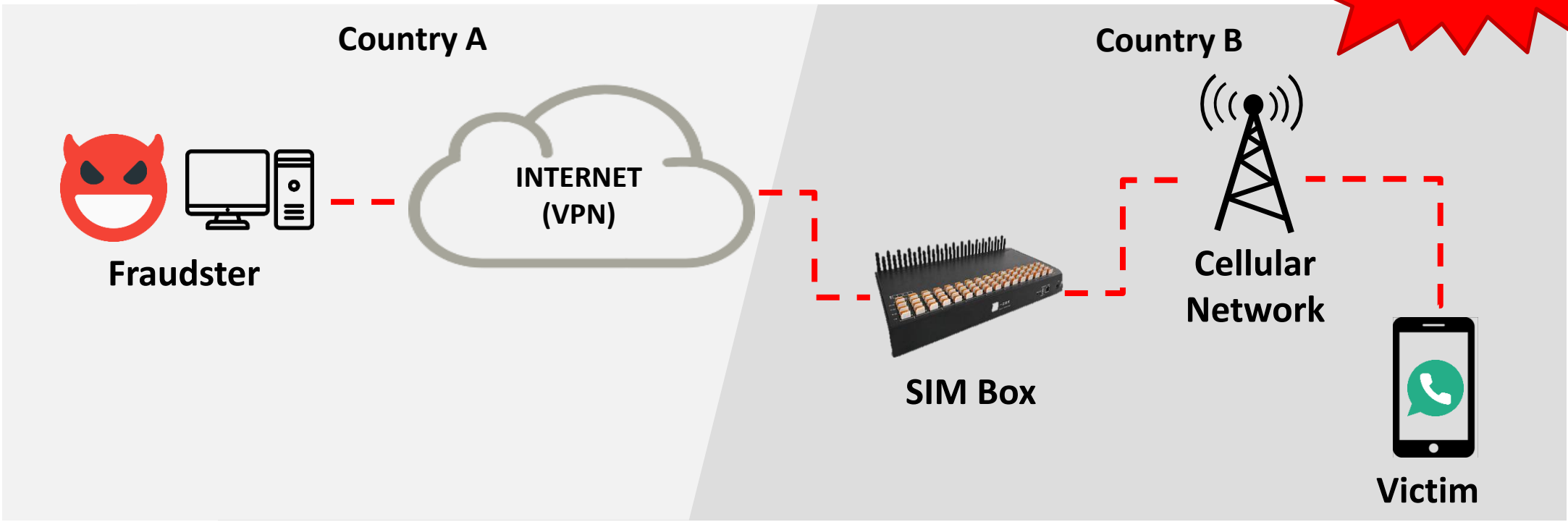


* Fraud Loss Survey Report, 2021

Illegal Use of SIM Box

- **Voice Phishing (Voice Scam Fraud)**
  - Deceive victims for obtaining money or personal information
    - Impersonate close people of victims (e.g. family, colleague)

600 M USD*



* Korea National Office of Investigation, 2021

Related Works

- **SIM box call detection using voice call quality**
  - PinDr0p [1]
  - Boxed Out [2]

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

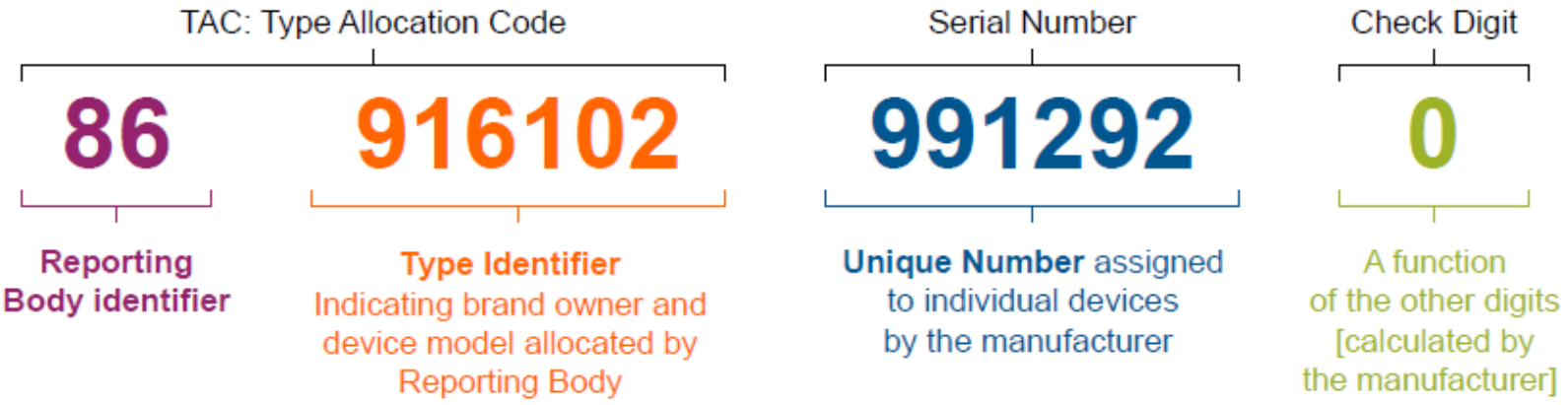
➔ Detected only after calls are made

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

How about IMEI?

- **IMEI (International Mobile Equipment Identity)**
  - 15 digit identifier allocated to every cellular devices
  - Values are unique: enables to identify individual devices
  - Can be used for banning stolen/malicious devices

- **Structure of IMEI**

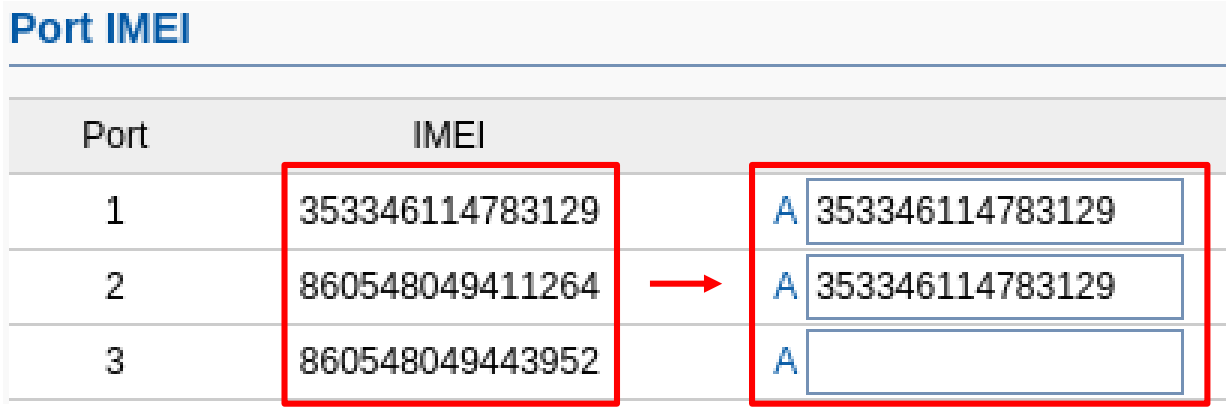


Model	TAC
iPhone 13	35757387
iPhone 6	35207506
Galaxy S10	35480910
Galaxy A12	35413676

Limitations of IMEI

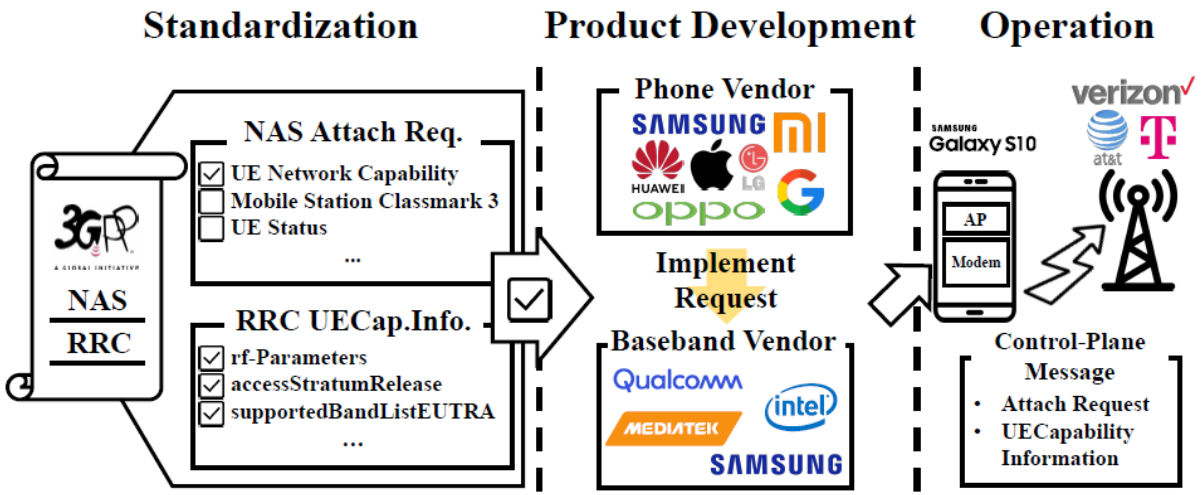
- **Network always trusts reported IMEI**
  - IMEI is a device-reported value
  - Network has no validation process of reported IMEI

- **What if malicious UE reports false IMEI?**
  - Network cannot detect it; malicious UEs cannot be blocked via IMEI
  - SIM boxes support IMEI manipulation



Intuition

Every year…

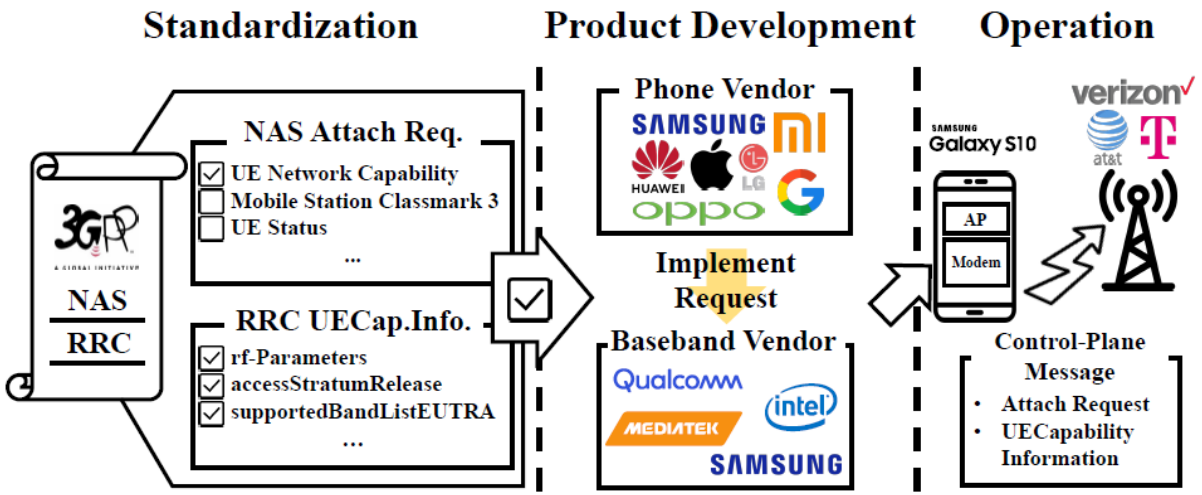


SYSSEC KAIST

Intuition

Every year…

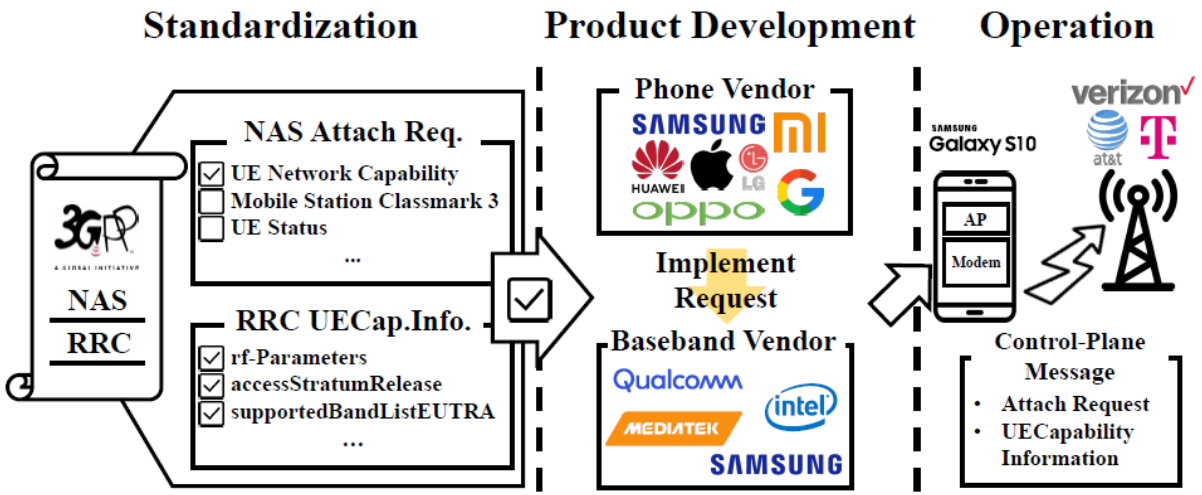
- 3GPP adds **new cellular capabilities** to their specification



Intuition

Every year…

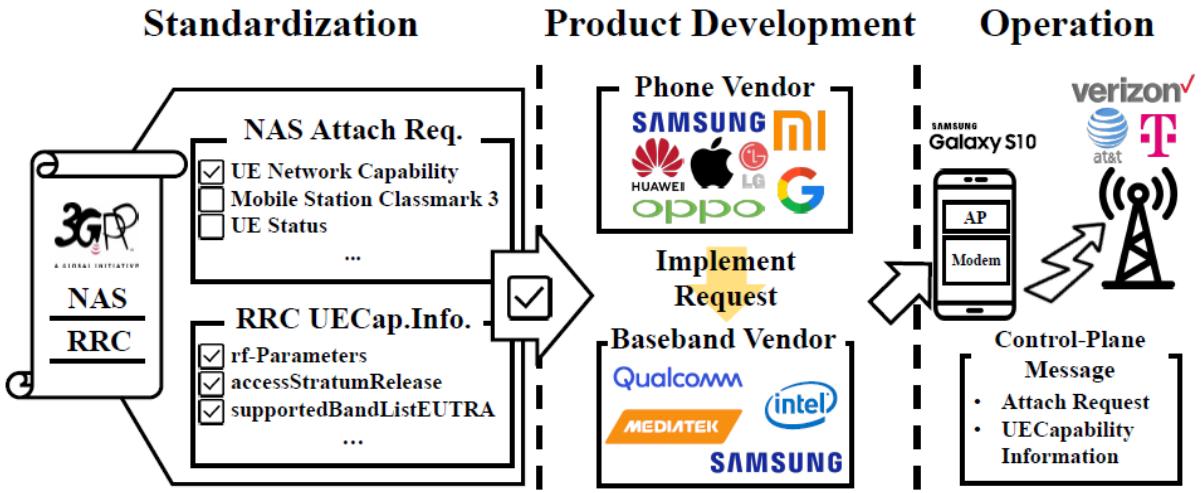
- **3GPP adds new cellular capabilities to their specification**
- **Baseband manufacturers produce new chipsets with new capabilities**



Intuition

Every year…

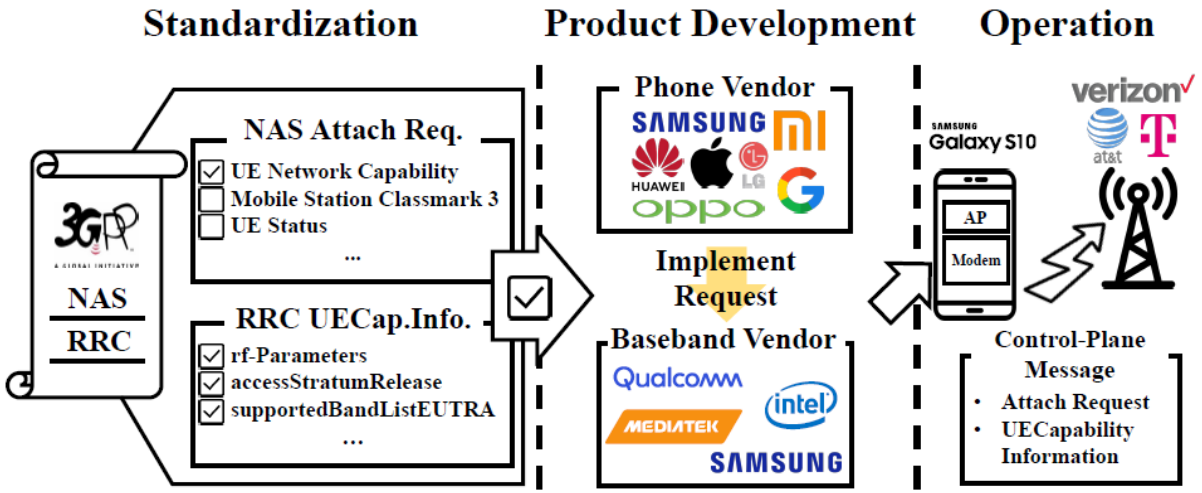
- 3GPP adds new cellular capabilities to their specification
- Baseband manufacturers produce new chipsets with new capabilities
- Smartphone manufacturers produce new smartphones with new capabilities



Intuition

Every year…

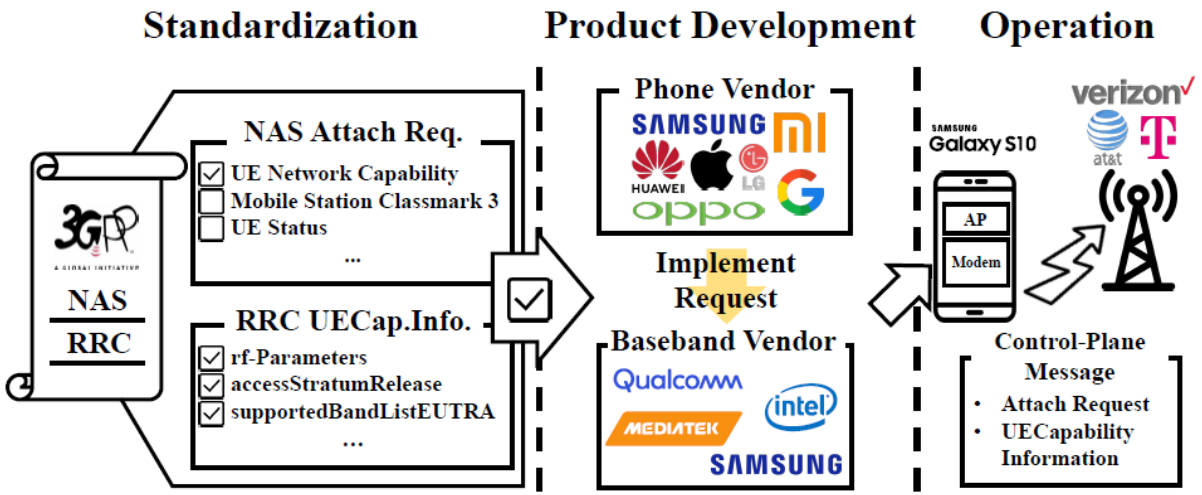
- 3GPP adds new cellular capabilities to their specification
- Baseband manufacturers produce new chipsets with new capabilities
- Smartphone manufacturers produce new smartphones with new capabilities
- Most IoT devices (including SIM box) do not use high-end chipset



Intuition

Every year…

- 3GPP adds new cellular capabilities 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

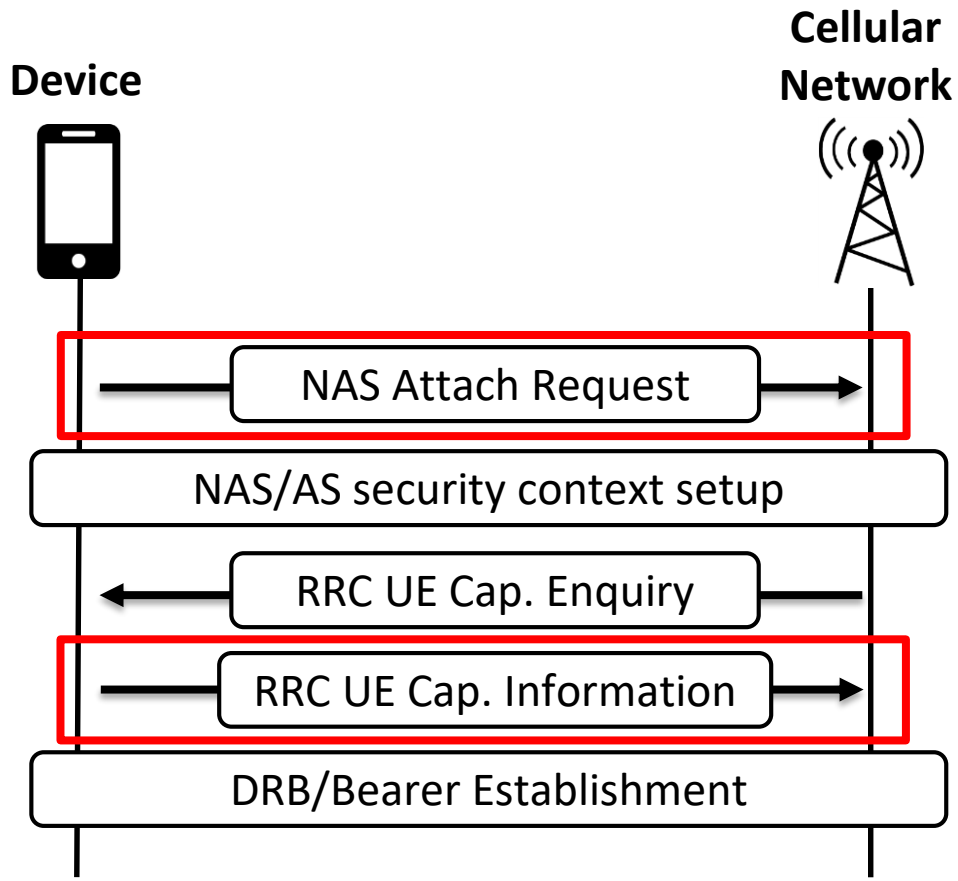


	Galaxy S9	Galaxy S10	SIM Box
Carrier Aggregation	O	O	X
5G	X	O	X

SYSSEC KAIST

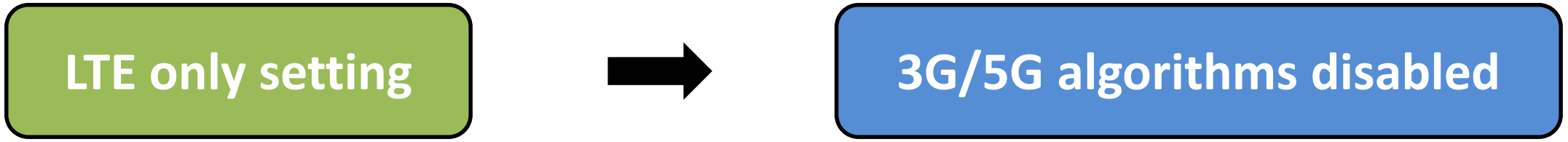
Generating fingerprints

- **Utilized two control-plane messages**
  - Used to report cellular capabilities
  - 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



Consideration 1: End-User Customization

- **End-user customization affect cellular capability**
  - E.g. Changing preferred network

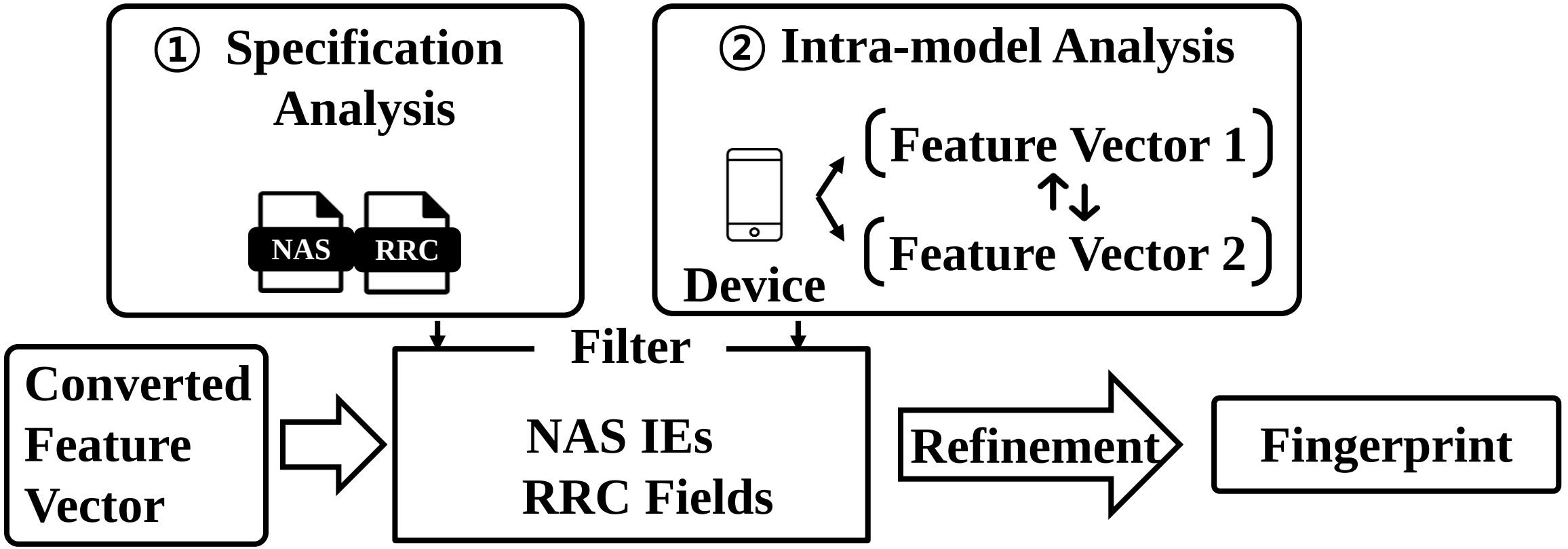


- **Table of the considered configurations**

	Configurations	Options
Setting option	Preferred network	5G-SA, 5G-NSA, or LTE
Engineering mode	Band selection	Automatic / LTE-only / Band (1, 3, 7)
	Service domain	CS/PS, PS only

Consideration 2: Feature Pruning

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



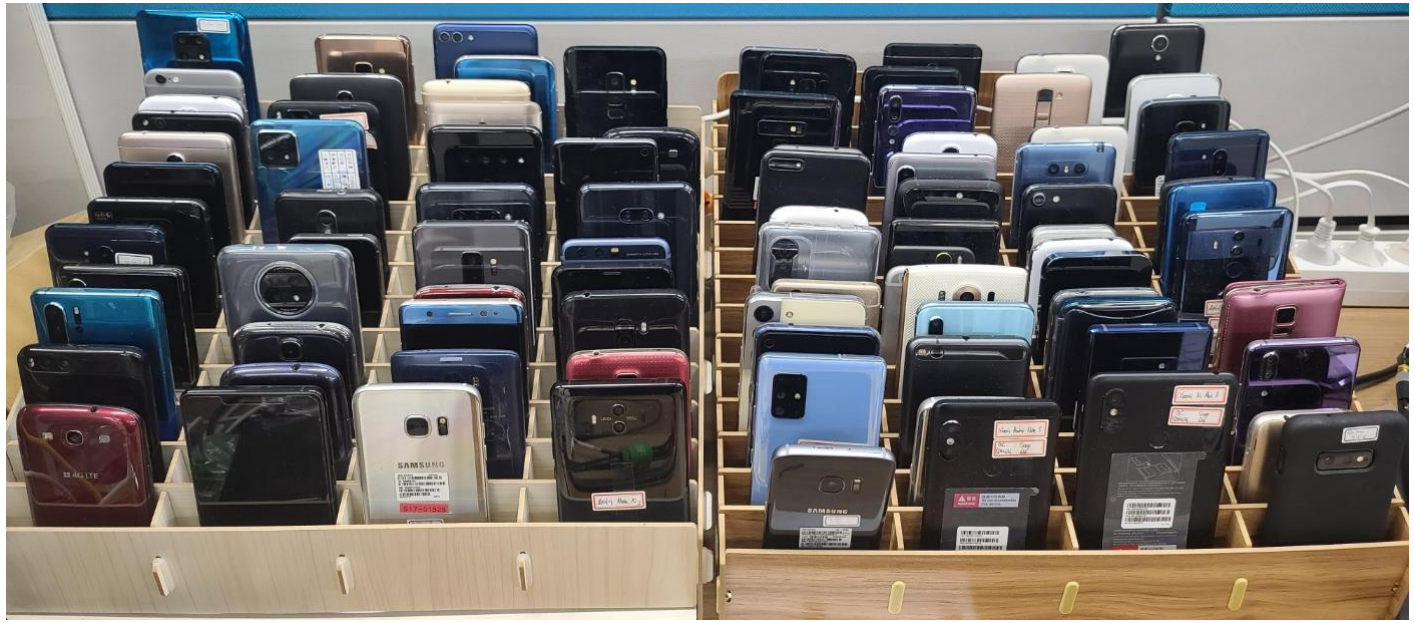
Consideration 2: Feature Pruning

- **Specification analysis**
  - The messages follow specific format in the standard
  - Analyzed 4 cellular specification documents (NAS & RRC) in total
  - Check our homepage and github for full analysis results

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

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**

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**

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

- **Detecting SIM Box using cellular capabilities**
- **Currently in discussion with a tier-1 MNO in Korea for deployment**
- **False positives can be further reduced by using**
  - Call detail records
  - Call patterns
  - SIM card type

- **A large project from Korean police to fight with voice phishing crime**
  - Developing various solutions to reduce the 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

KAIST

Syssec

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

경찰청
KOREAN NATIONAL POLICE AGENCY

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?

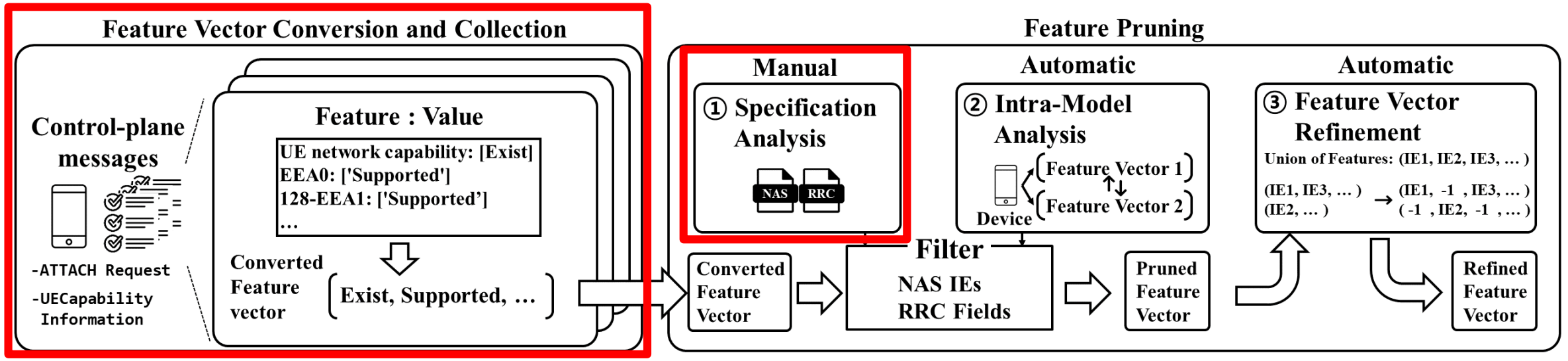
- **Changing SIM box configuration (VIII-A)**
  - SIM box cannot have same fingerprints with phones
  - Made own SIM box for the experiment
  - Sent various AT commands

- **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 / Specification updates



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']]
```