Dissecting VoLTE: Exploiting Free Data Channels and Security Problems

Hongil Kim, Dongkwan Kim @ SysSec Lab.

32C3

KAIST

Credits:
Minhee Kwon, Hyeongseok Han, Yeongjin Jang, Taesoo Kim, Dongsu Han, Yongdae Kim

SysSec Lab. KAIST

KIM, HONG IL

Ph.D. student at **System Security Lab.** KAIST

Research interest:
- Cellular network system
- Mobile device security
- Internet of Things (IoT) security

KIM, DONG KWAN

M.S. student at **System Security Lab.** KAIST

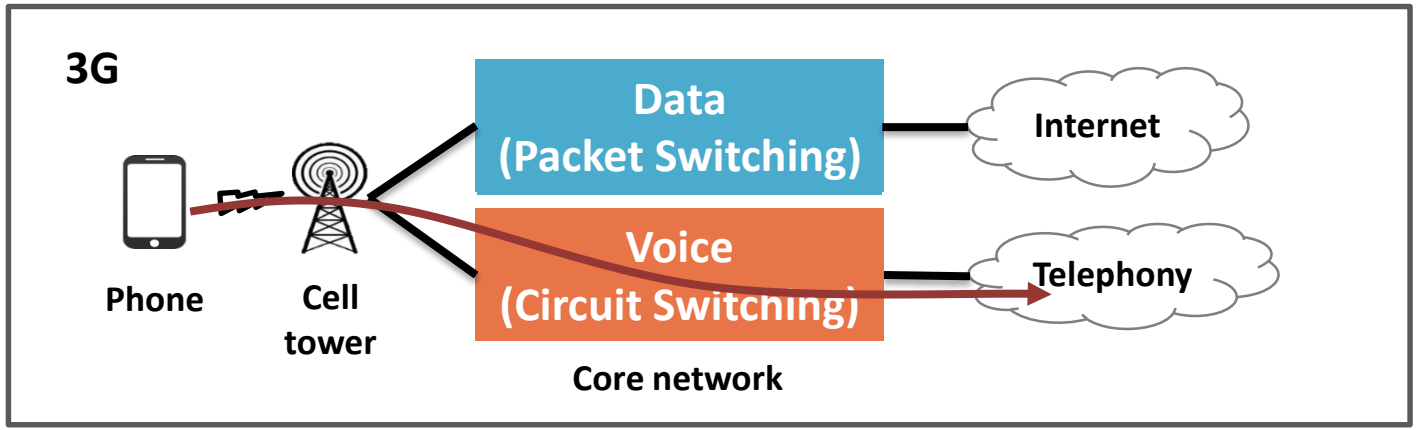
Research interest:
- Cellular Security
- CPS Security
- System Security

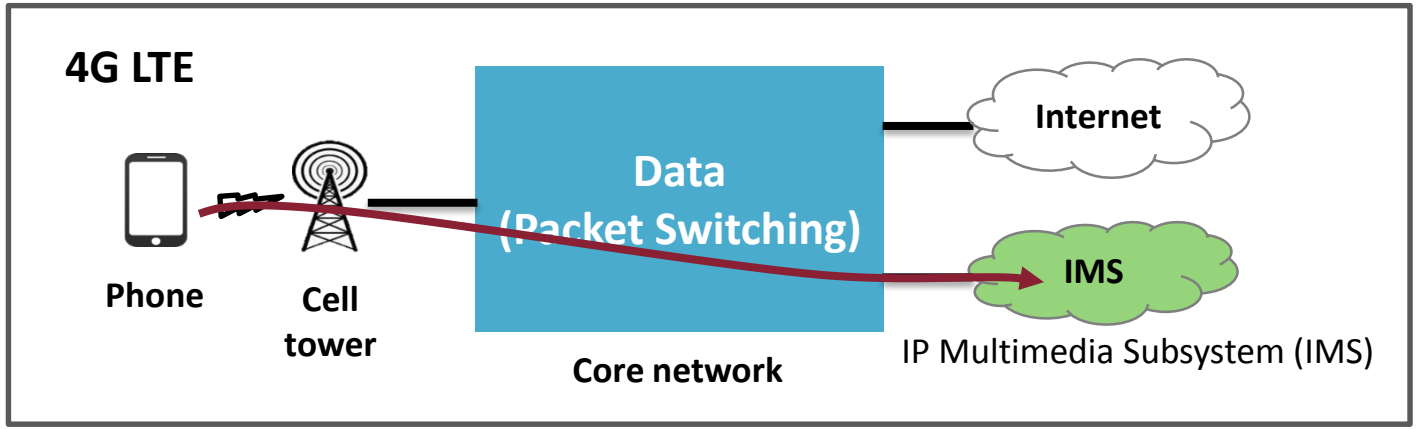
VoLTE = Voice over LTE

- Implementation of VoIP on LTE

- 3G network
  - Data and voice are separated
- 4G LTE network : All-IP based Network
  - Both data and voice are delivered as data-flow

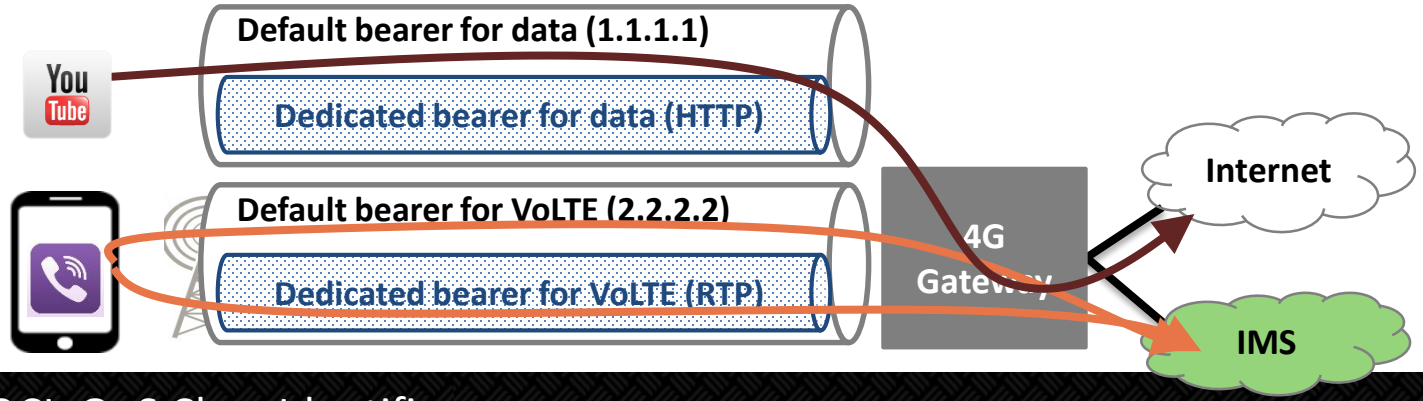
- Advantages on VoLTE
  - **For users**: high voice quality, faster call setup, better battery life.
  - **For operators**: increase usability, reduce cost, rich multimedia services


3G
Data
(Packet Switching)
Internet
Voice
(Circuit Switching)
Telephony
Phone
Cell
tower
Core network


4G LTE
Data
(Packet Switching)
Internet
IMS
Phone
Cell
tower
Core network
IP Multimedia Subsystem (IMS)

Each service is delivered by bearer

- In LTE, all services are delivered data channels, called “bearers”
  - Data, Voice, Video, …
- **Bearer**: a virtual channel with below properties
  - Based on **QCI*** value, it determines bandwidth, loss rate, latency (QoS)
  - **Default bearer**: Non Guaranteed Bit rate
  - **Dedicated bearer**: Guaranteed Bit rate



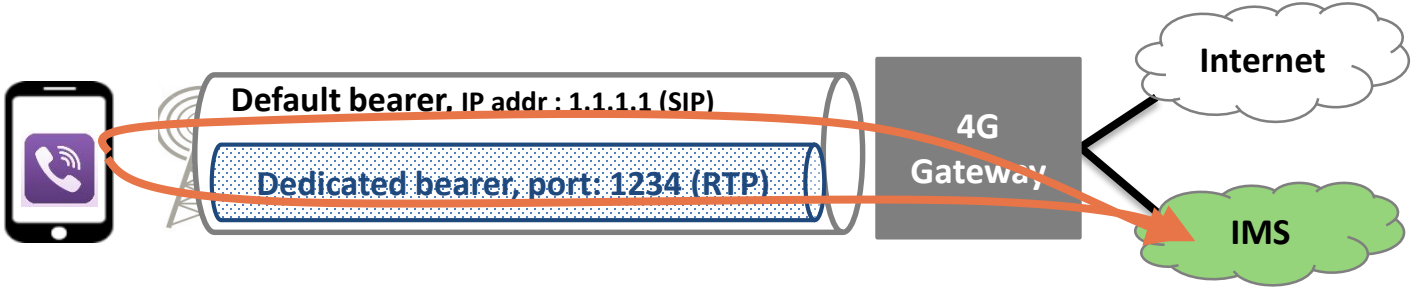
*QCI: QoS Class Identifier

Each service is delivered by bearer

QCI	Bearer Type	Priority	Packet Delay	Packet Loss	Usage
1		2	100 ms	10^{-2}	Voice data (VoLTE)
2	Gauranteed Bit rate	4	150 ms	10^{-3}	Video data
3		3	50 ms		Real-time gaming
4		5	300 ms		Buffered streaming
5		1	100 ms	10^{-6}	IMS signaling (VoLTE signaling)
6	Non Gauranteed Bit rate	6	300 ms		Buffered streaming, TCP based services
7		7	100 ms	10^{-3}	Live streaming, Interactive Gaming
8		8	300 ms	10^{-6}	TCP based services e.g. email, ftp, chat etc.
9		9			

Voice delivery in LTE

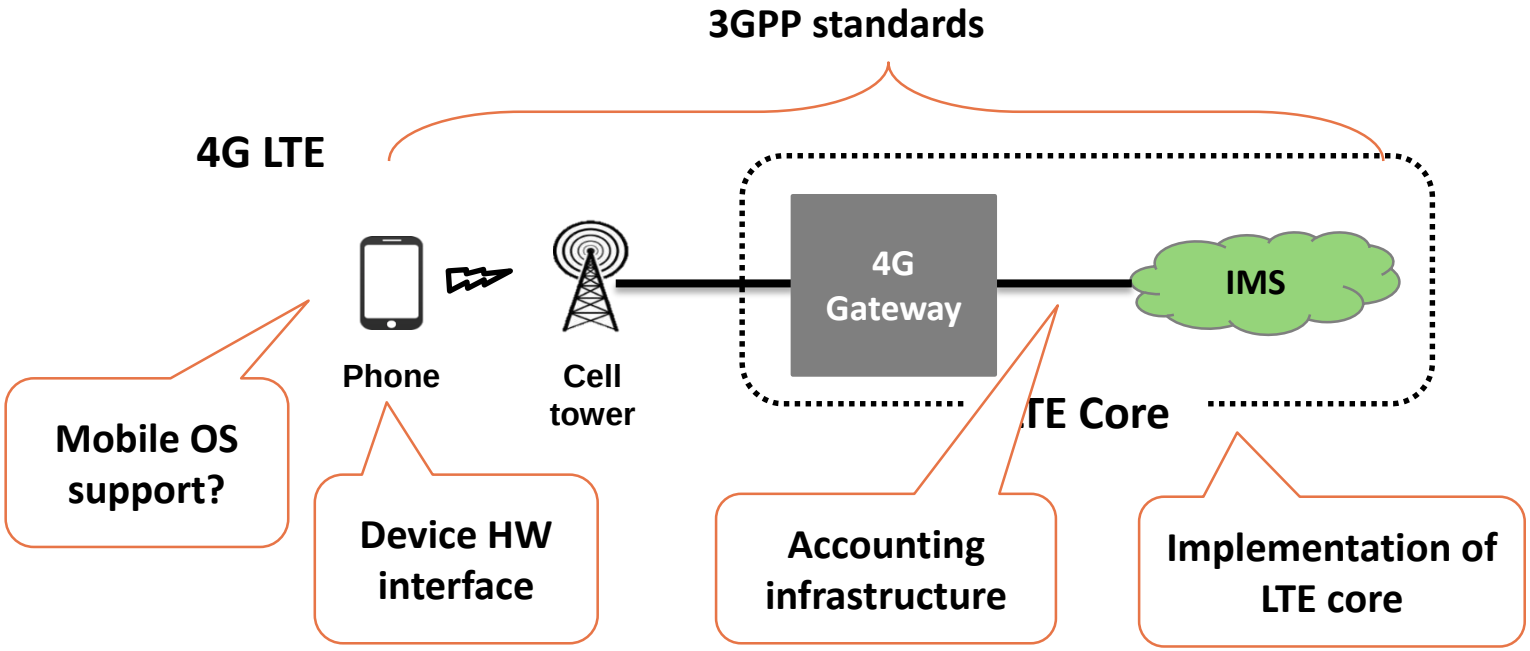
- Voice is delivered through two bearers
- For VoLTE service,
  1. Default bearer: call signaling (control-plane), *SIP
  2. Dedicated bearer: voice data (data-plane), *RTP



*SIP: Session Initiation Protocol, *RTP: Real-time Transport Protocol

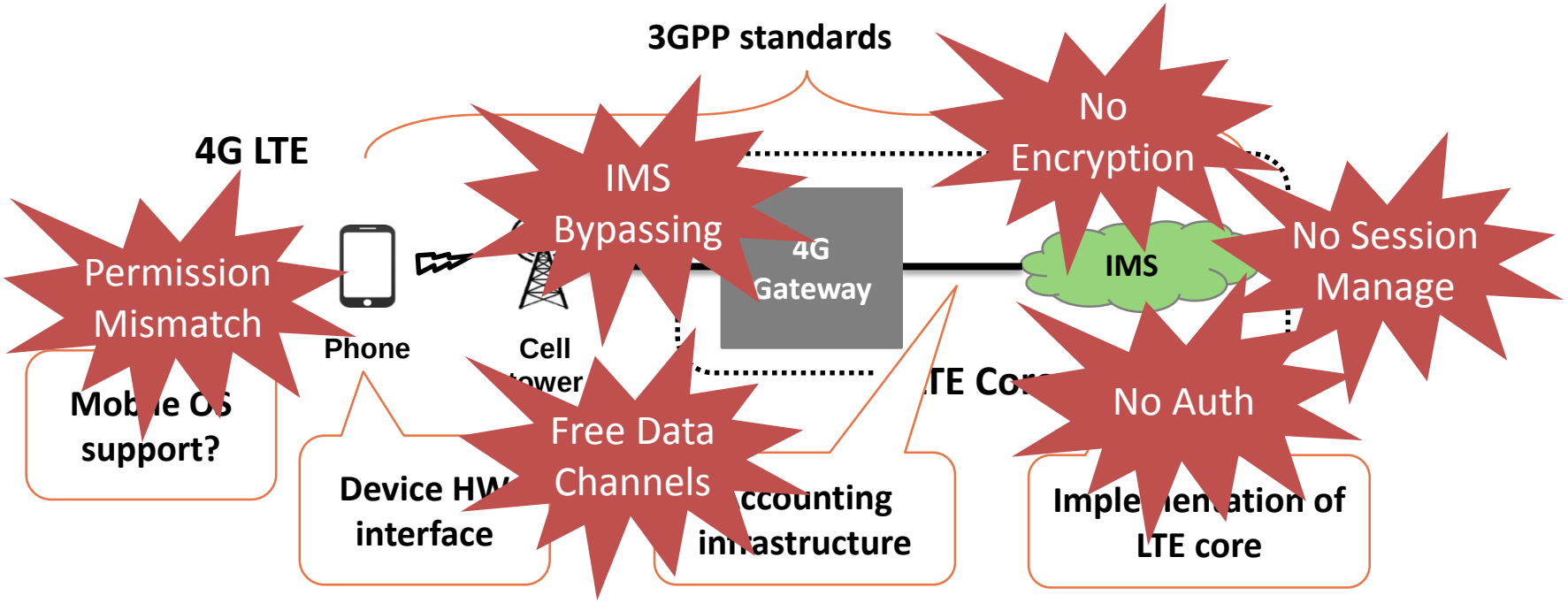
VoLTE makes cellular network more complex

- Let's check potential attack vectors newly introduced in VoLTE



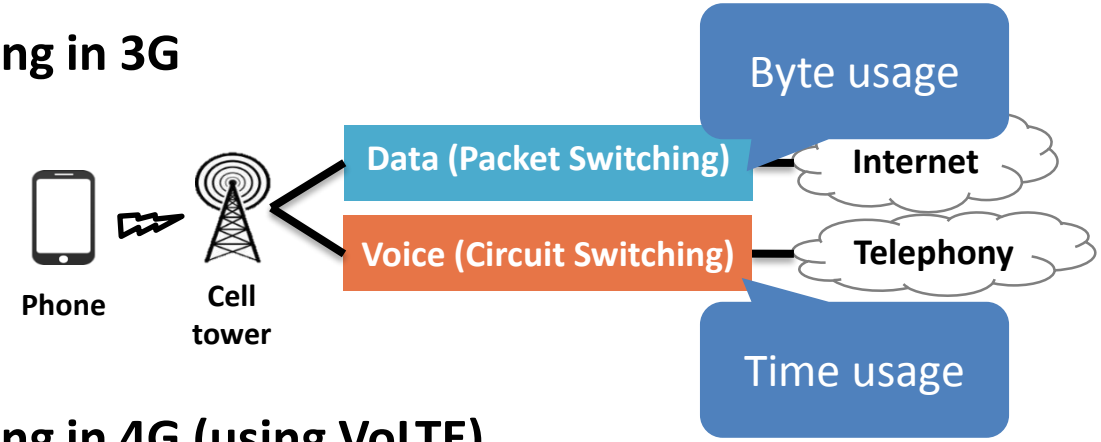
VoLTE makes cellular network more complex

- Let's check potential attack vectors newly introduced in VoLTE

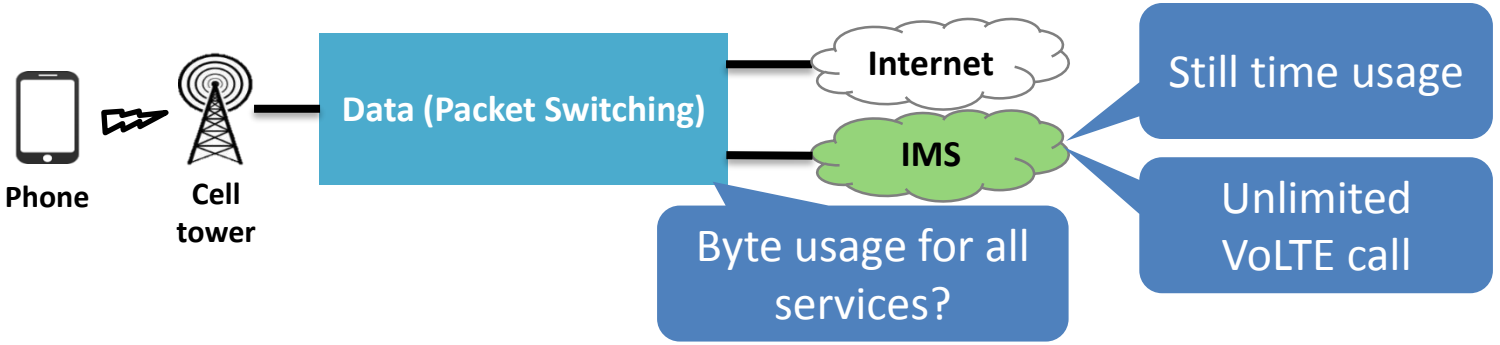


#1: VoLTE Accounting

❖ **Accounting in 3G**

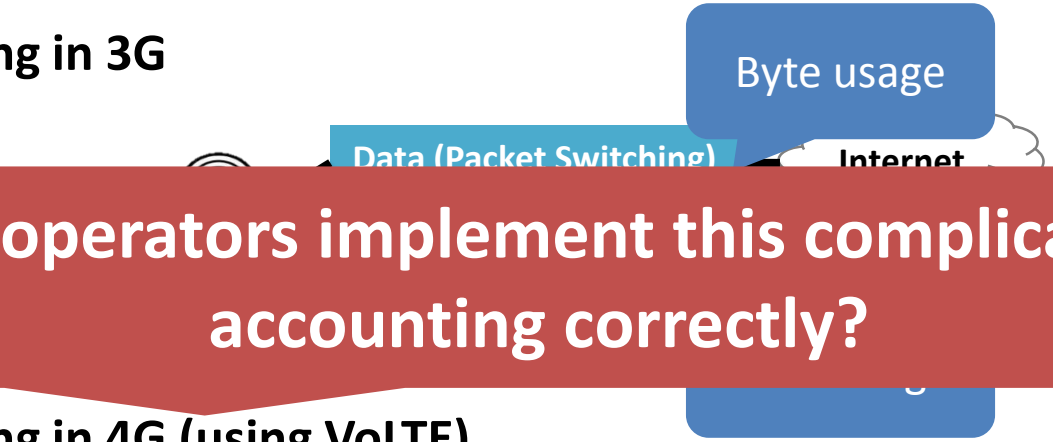


❖ **Accounting in 4G (using VoLTE)**

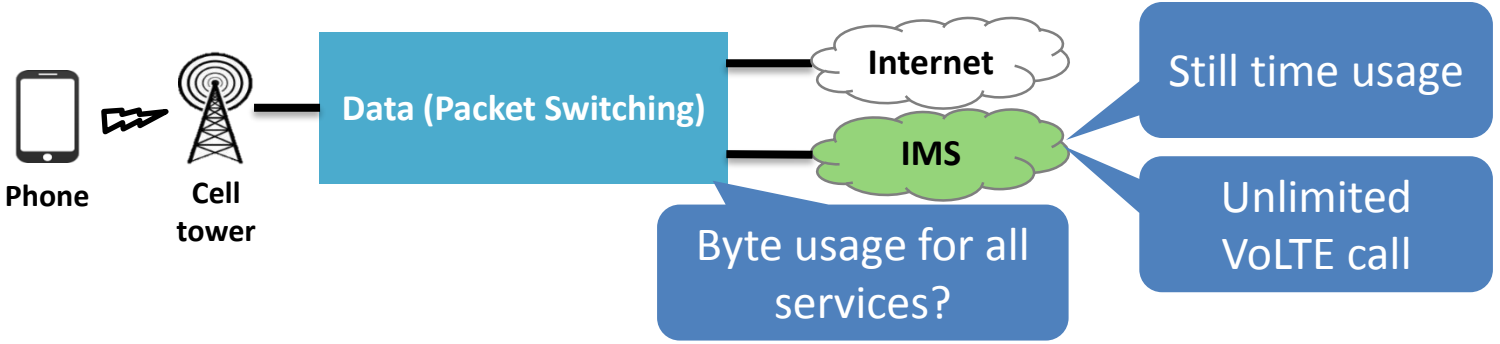


#1: VoLTE Accounting

- Accounting in 3G

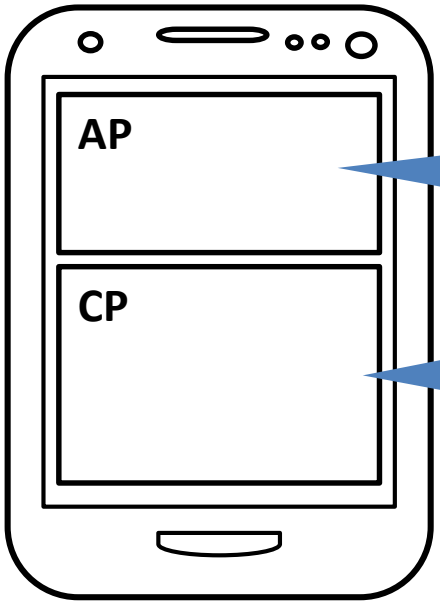


- Accounting in 4G (using VoLTE)



Anatomy of smartphone

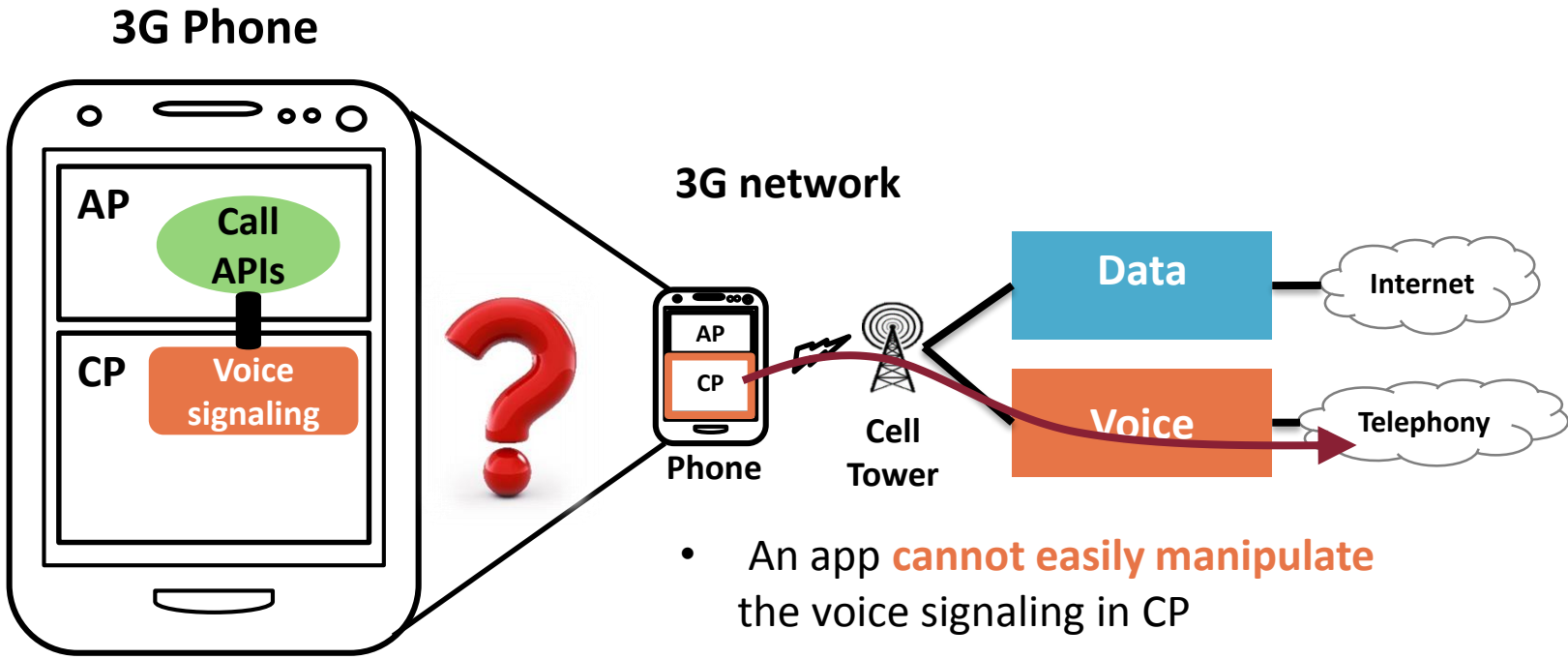
- Smartphone has two processors



Application processor (AP)
- Running mobile OS (Android)
- Running User application

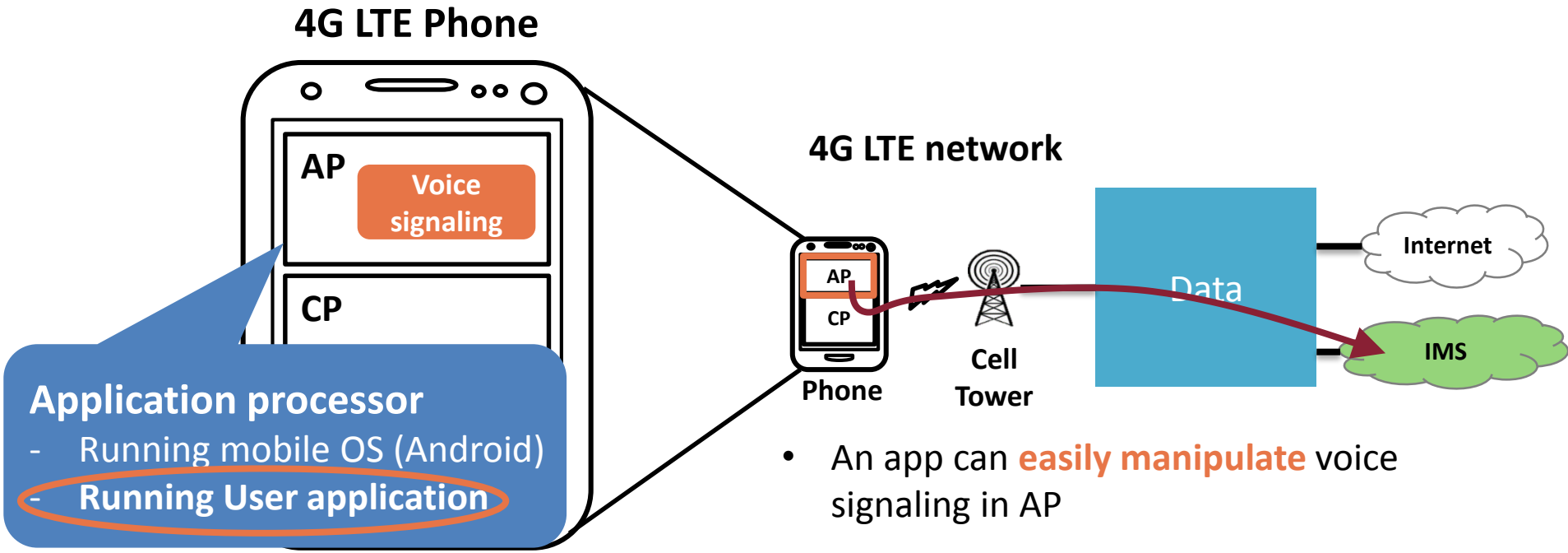
Communication processor (CP)
- Telephony Processor (modem)
- Digital Signal Processing (DSP)

#2 Voice solution in device, 3G case



- An app **cannot easily manipulate** the voice signaling in CP
- An app needs **"CALL_PHONE" permission** for calling

#2: Voice solution in device, LTE



- An app can **easily manipulate** voice signaling in AP

#2: Voice solution in device, LTE

```
busybox netstat -an | grep "5060"
tcp        0      0 100.105.226.218:5060    0.0.0.0:*               LISTEN

udp        0      0 100.105.226.218:5060    0.0.0.0:*
```

4G LTE network

```
rmnet0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:100.105.226.218  Mask:255.255.255.252
          UP RUNNING  MTU:1440  Metric:1
          RX packets:197 errors:0 dropped:0 overruns:0 frame:0
          TX packets:203 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:76194 (74.4 KiB)  TX bytes:110360 (107.7 KiB)

rmnet1    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.108.252.73  Mask:255.255.255.252
          UP RUNNING  MTU:1440  Metric:1
          RX packets:29380 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22312 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28737559 (27.4 MiB)  TX bytes:2720188 (2.5 MiB)
```

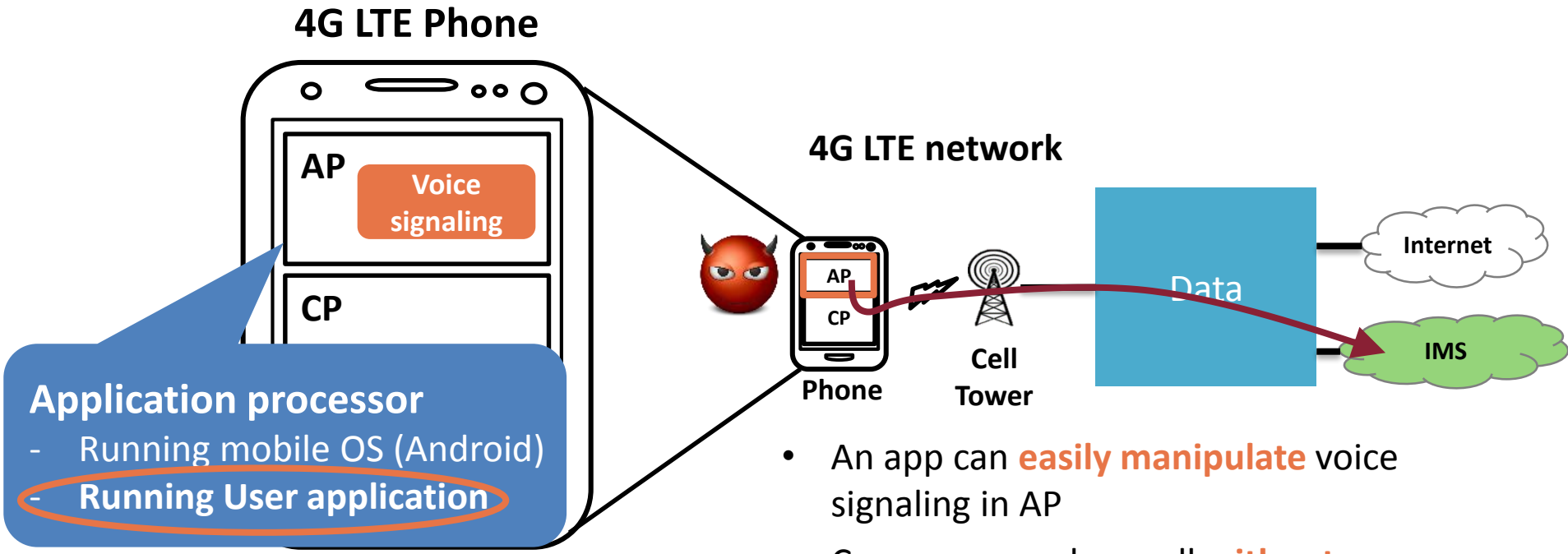
Internet

IMS

Applicatio
- Running
- **Running**

e voice

#2: Voice solution in device, LTE



- An app can **easily manipulate** voice signaling in AP
- Can an app make a call **without "CALL_PHONE" permission?**

Two findings in VoLTE

1. A complex accounting infrastructure

2. Delegating voice signaling (previously done by CP) to AP

Our approach to attack two findings

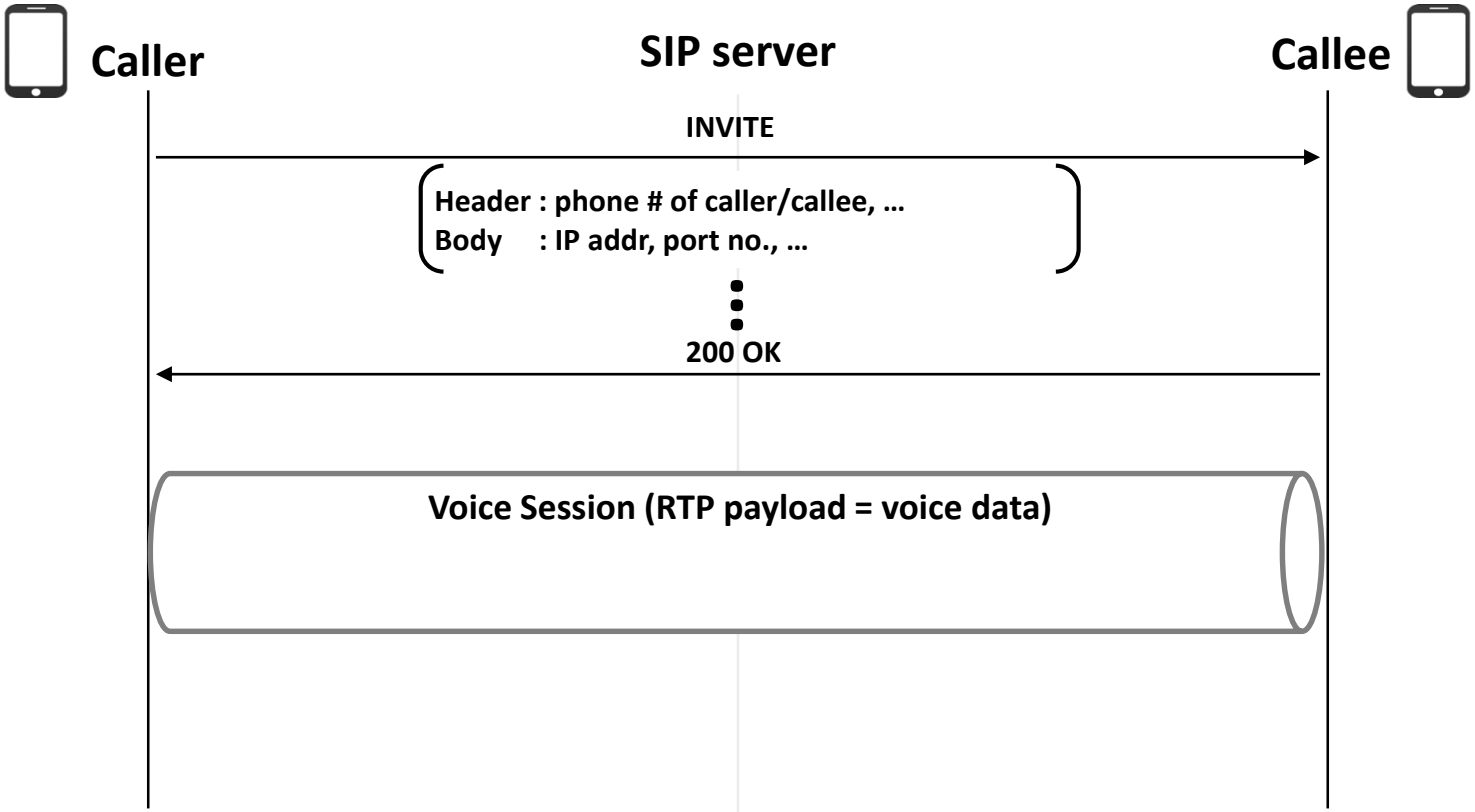
- Analyze 3GPP standards related with VoLTE service
  - Leave detail implementation to operators, chipset vendors, …
- Make a checklist of potential vulnerable points in the VoLTE feature
  - About 60 items for both control and data plane
- Perform an analysis in 5 major operational networks
  - 2 U.S. operators and 3 South Korea operators

Quick summary of results

- **Four free data channels**
  - **Using VoLTE protocol** (for all operators)
    - SIP tunneling
    - Media tunneling
  - **Direct communication** (for some operators)
    - Phone-to-Internet
    - Phone-to-Phone

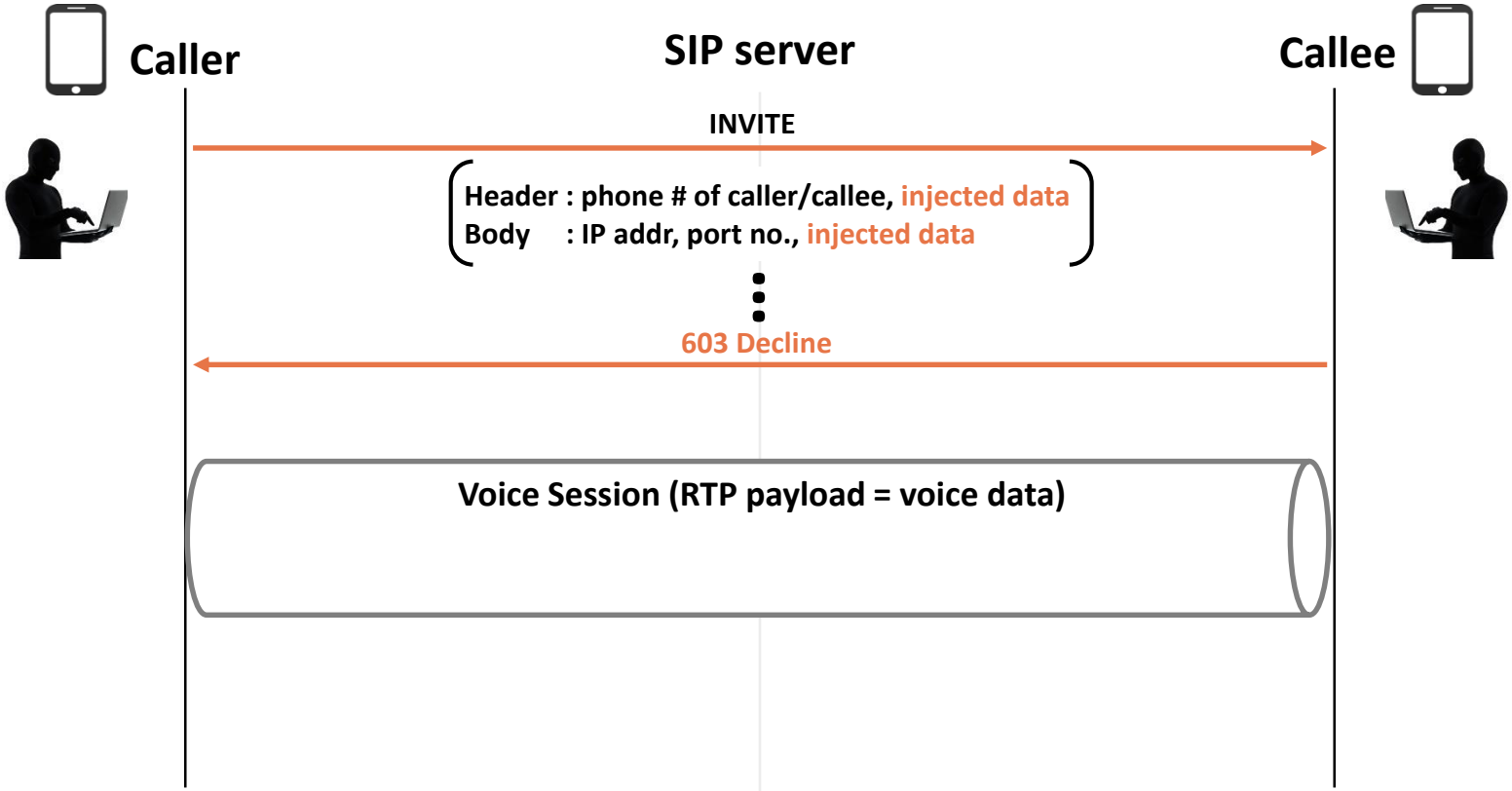
- **Five security issues**
  - **No encryption** of voice packets
  - **No authentication** of signaling
  - **No call session management** (DoS on the cellular infrastructure)
  - **IMS bypassing**
  - **Permission model mismatch** (VoLTE call without “CALL_PHONE” permission)

VoLTE Call Procedure



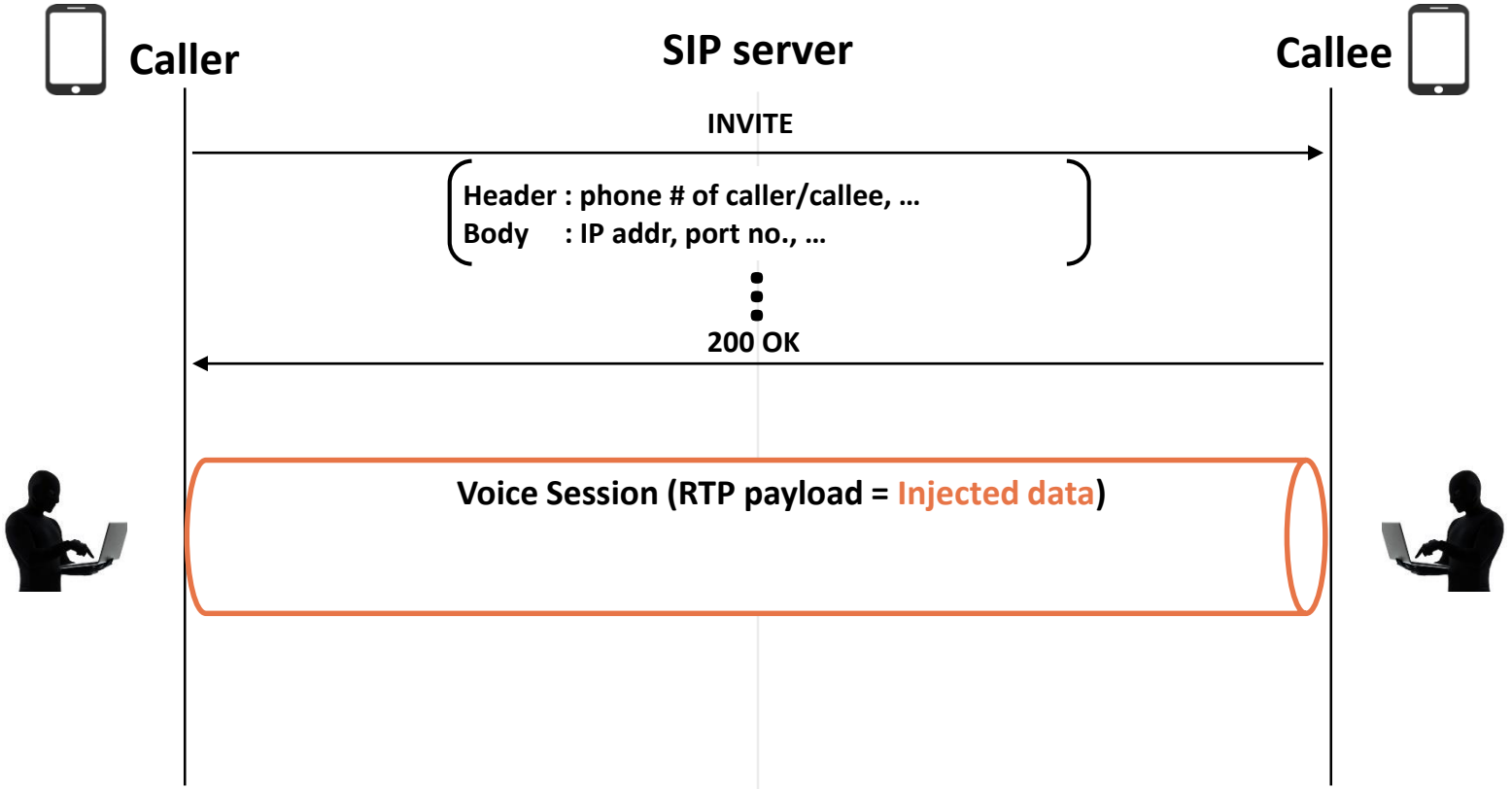
*SIP: Session Initiation Protocol, *RTP: Real-time Transport Protocol

Free Channel: SIP Tunneling



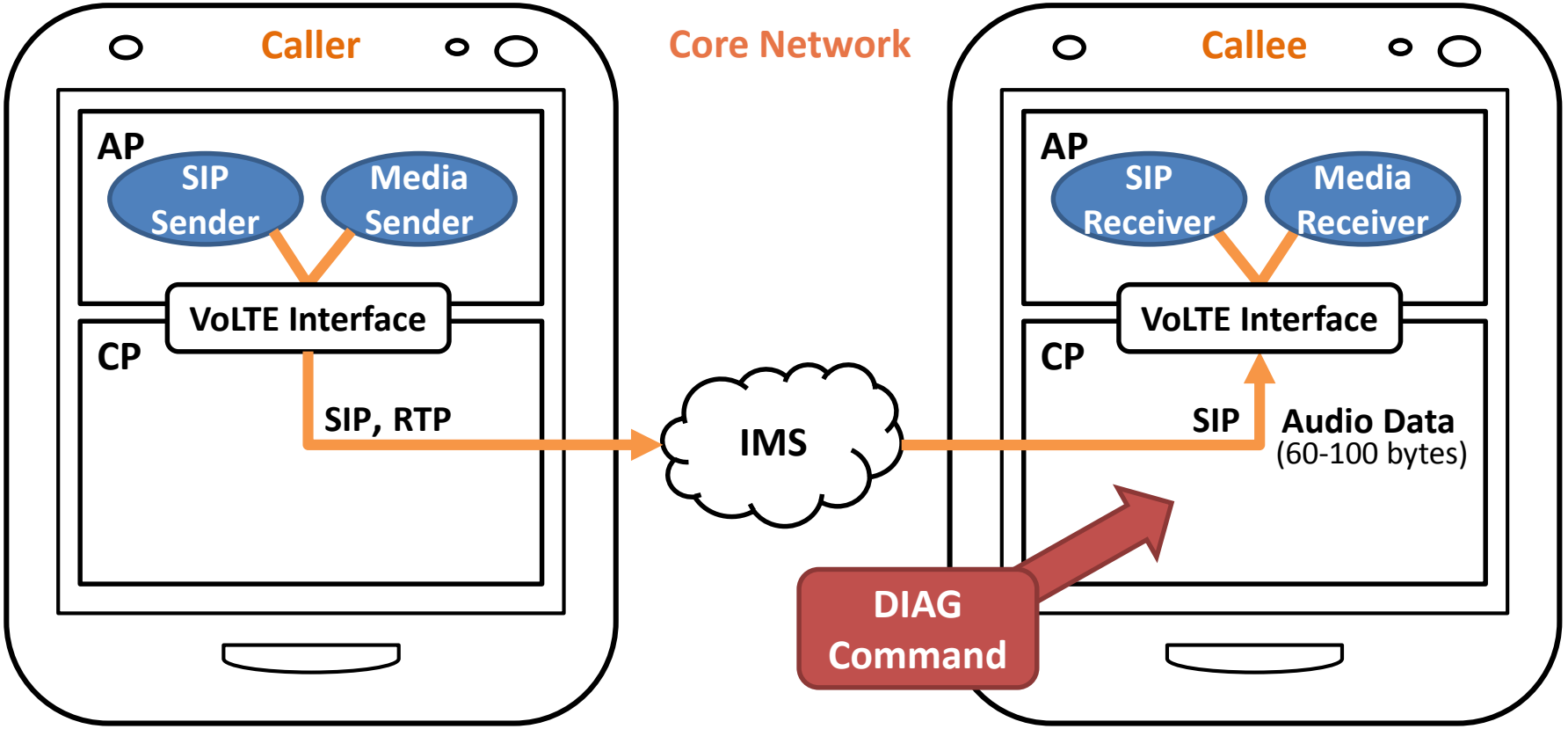
*SIP: Session Initiation Protocol, *RTP: Real-time Transport Protocol

Free Channel: Media Tunneling



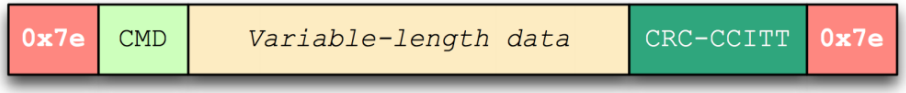
*SIP: Session Initiation Protocol, *RTP: Real-time Transport Protocol

Attack Implementation in Detail



Diagnostic Protocol (DIAG)

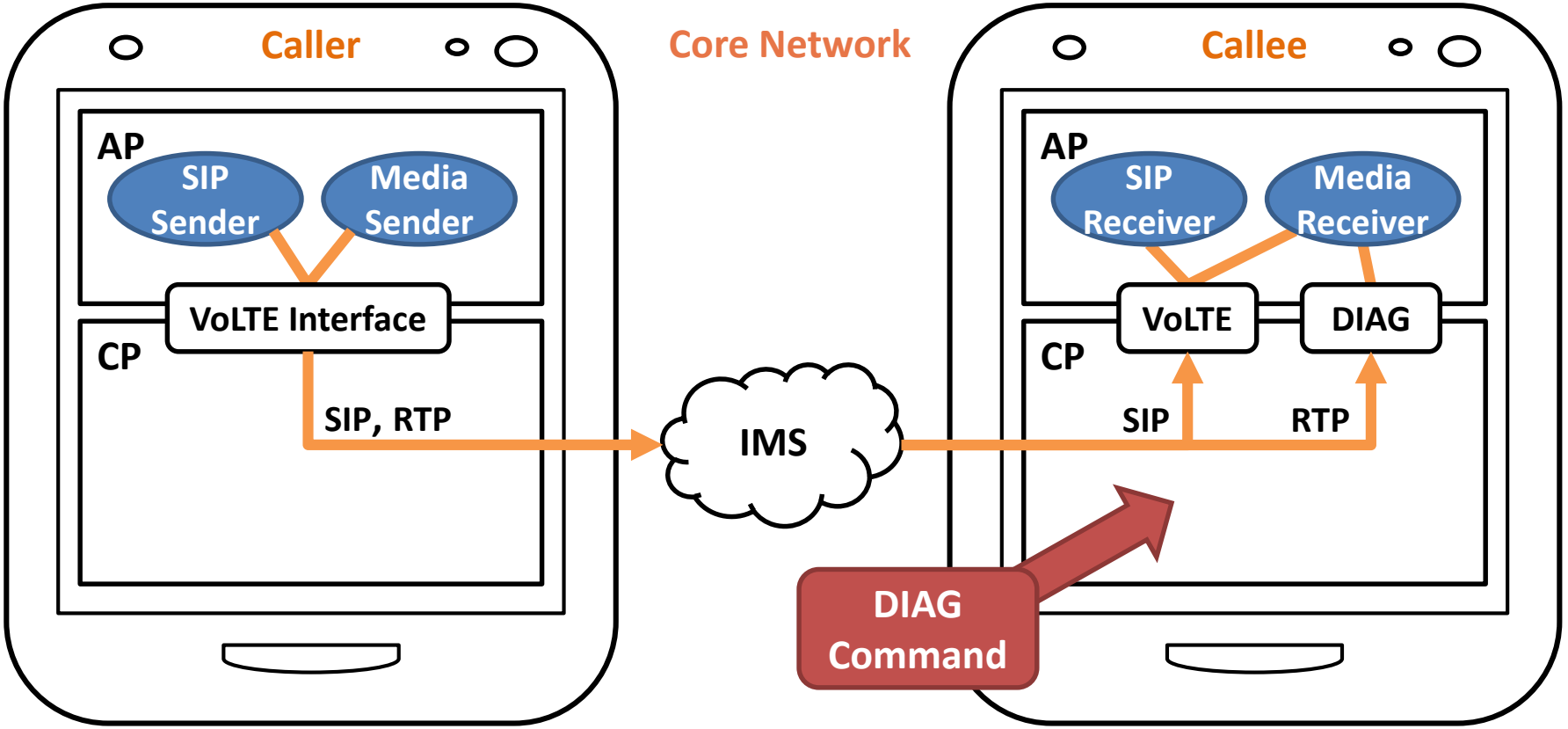
- Proprietary protocol by QualComm
- Several functions (memory read/write, SMS read/write, signaling dump, ...)
- Real-time data logging for RF diagnosis (Diagnostic Monitor)



Command	Opcode
MEMORY READ/WRITE	17, 18, ...
PASSWORD	70, ...
SMS READ/WRITE	83, 84, ...
LOG	15, 16, ...

* Delugre, “Reverse Engineering a Qualcomm Baseband”, 28C3

Attack Implementation in Detail



Outline

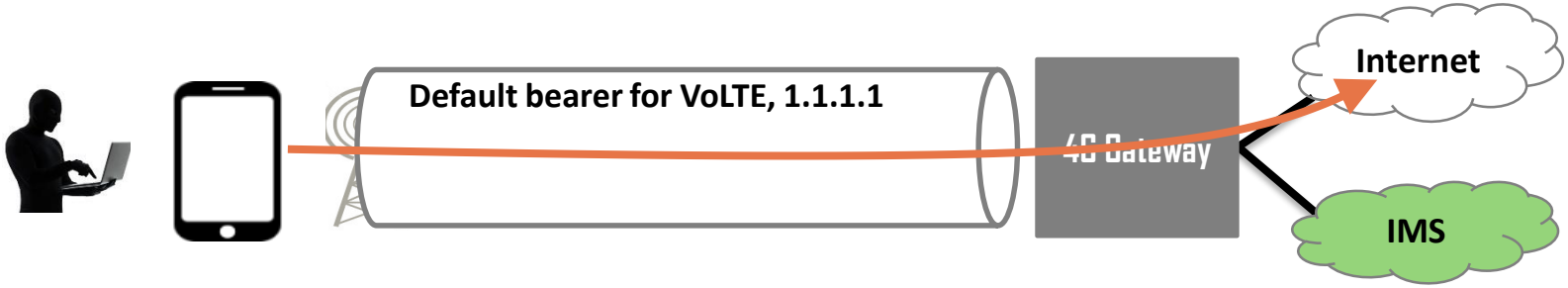
- **Four free data channels**
  - **Using VoLTE protocol** (for all operators)
    - SIP tunneling
    - Media tunneling
  - **Direct communication** (for some operators)
    - Phone-to-Internet
    - Phone-to-Phone

- **Five security issues**
  - **No encryption** of voice packets
  - **No authentication** of signaling
  - **No call session management** (DoS on the cellular infrastructure)
  - **IMS bypassing**
  - **Permission model mismatch** (VoLTE call without “CALL_PHONE” permission)

Free Channel: Direct communication

- **Phone-to-Internet**
  - Open a TCP/UDP socket with **voice IP**
  - Send data to the **Internet**

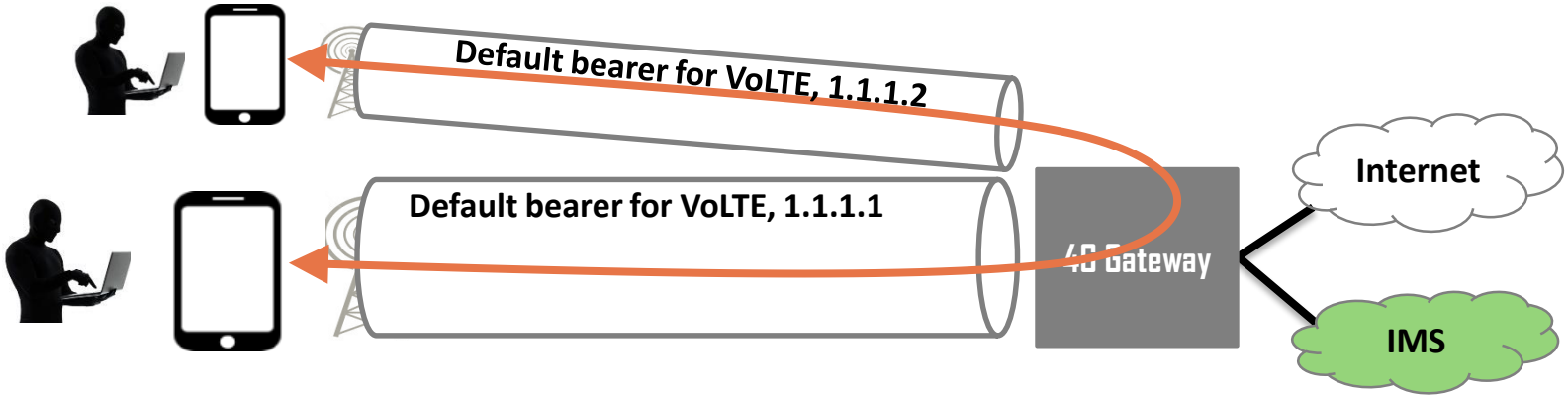
  E.g. TCP/UDP Socket (Src: voice IP/port, Dst: youtube.com/port)



Free Channel: Direct communication

- **Phone-to-Phone**
  - Open a TCP/UDP socket with **voice IP**
  - Send data to **callee**

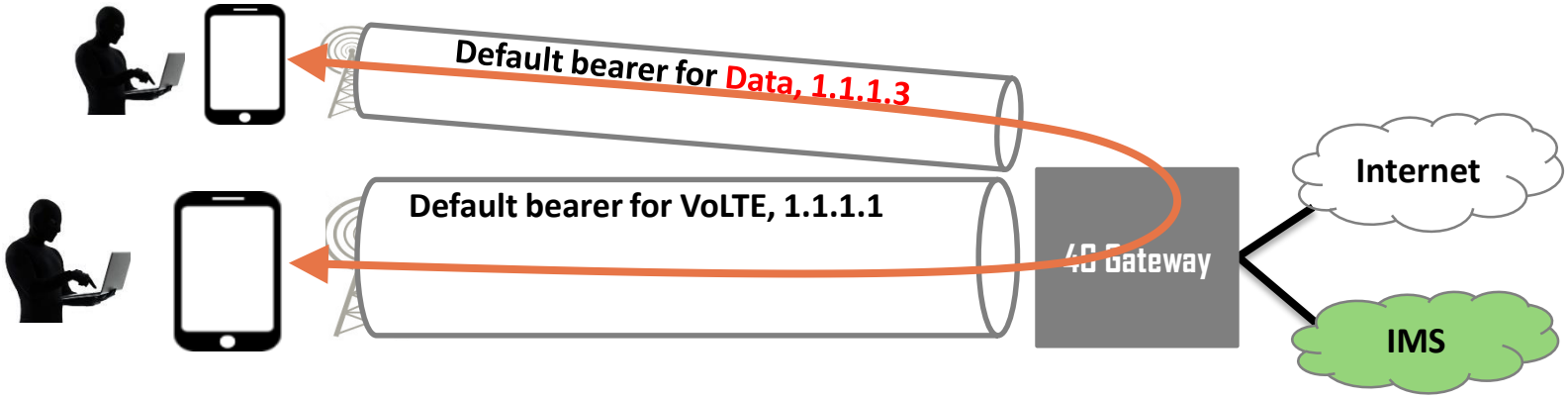
E.g. TCP/UDP Socket (Src: voice IP/port, Dst: callee's voice IP/port)



Overbilling with Direct Communication?

- **Phone-to-Phone**
  - Open a TCP/UDP socket with **voice IP**
  - Send data to **callee**

E.g. TCP/UDP Socket (Src: voice IP/port, Dst: callee's data IP/port)



Evaluation Result: Accounting Bypass

	Free Channel	US-1	US-2	KR-1	KR-2	KR-3
Using VoLTE Protocol	SIP Tunneling	✓	✓	✓	✓	✓
	Media Tunneling	✓	✓	✓	✓	✓
Direct Communication	Phone to Phone	✓	✗	✓	✗	✗
	Phone to Internet	✗	✓	✓	✗	IPv4:✓ IPv6:✗

Last update: 20th April, 2015

✓: vulnerable/not charged, x: secure

Evaluation Result: Accounting Bypass

	Free Channel	US-1	US-2	KR-1	KR-2	KR-3
Using VoLTE Protocol	SIP Tunneling	✓	✓	✓	✓	✓
	Media Tunneling	✓	✓	✓	✓	✓
Direct Communication	Phone to Phone	✓	✗	✗	✗	✗
	Phone to Internet	✗	✓	✗	✗	IPv4:✓ IPv6:✗

Last update: 30th Nov., 2015

✓: vulnerable/not charged, x: secure

Evaluation Result: Accounting Bypass

	Free Channel	US-1	US-2	KR-1	KR-2	KR-3
Using VoLTE Protocol	SIP Tunneling	X				
	Media Tunneling	42 Kbps				
Direct Communication	Phone to Phone	16.8 Mbps				
	Phone to Internet	21.5 Mbps				

Last update: 20th April, 2015

✓: vulnerable/not charged, x: secure

Outline

- **Four free data channels**
  - **Using VoLTE protocol** (for all operators)
    - SIP tunneling
    - Media tunneling
  - **Direct communication** (for some operators)
    - Phone-to-Internet
    - Phone-to-Phone

- **Five security issues**
  - **No encryption** of voice packets
  - **No authentication** of signaling
  - **No call session management** (DoS on the cellular infrastructure)
  - **IMS bypassing**
  - **Permission model mismatch** (VoLTE call without “CALL_PHONE” permission)

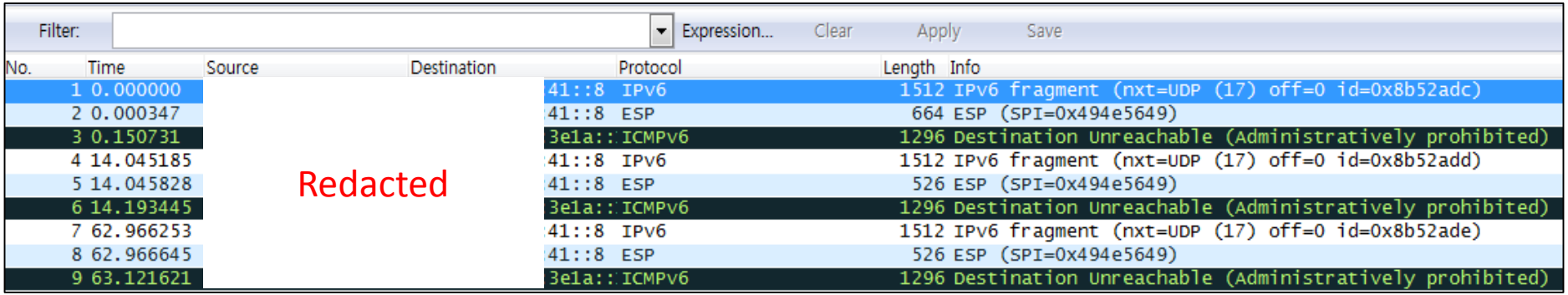
No Encryption for Voice Packets

- For voice signaling,
  - only one operator was using IPsec
  - An attacker can easily manipulate VoLTE call flow
- For voice data,
  - no one encrypted voice data
  - An attacker might wiretap the outgoing voice data

Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
IMS	No SIP Encryption						Message manipulation
	No Voice Data Encryption						Wiretapping

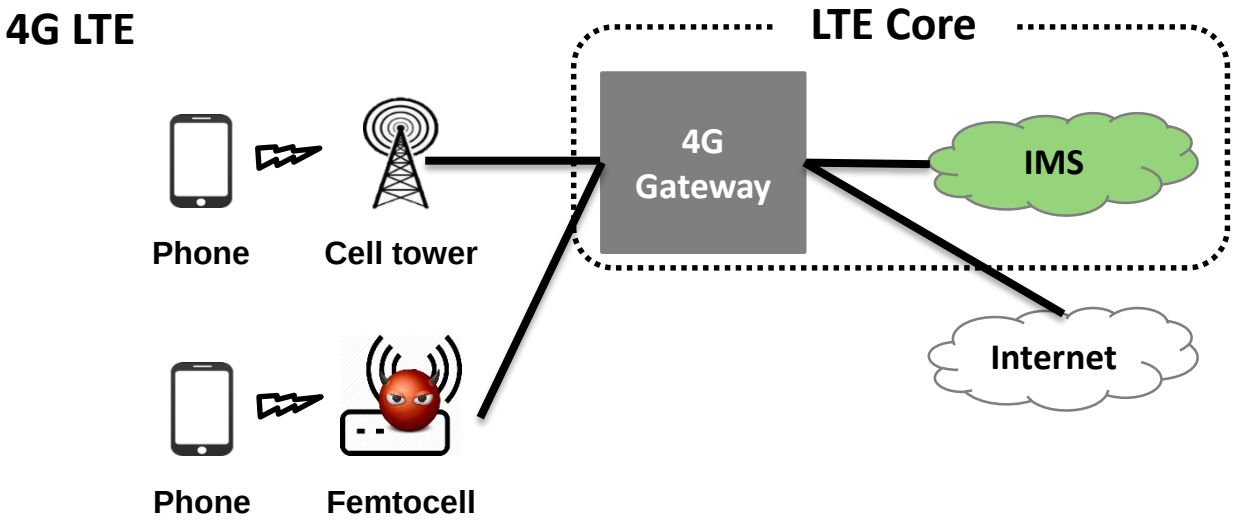
 : Vulnerable  : Secure

No Encryption for Voice Packets



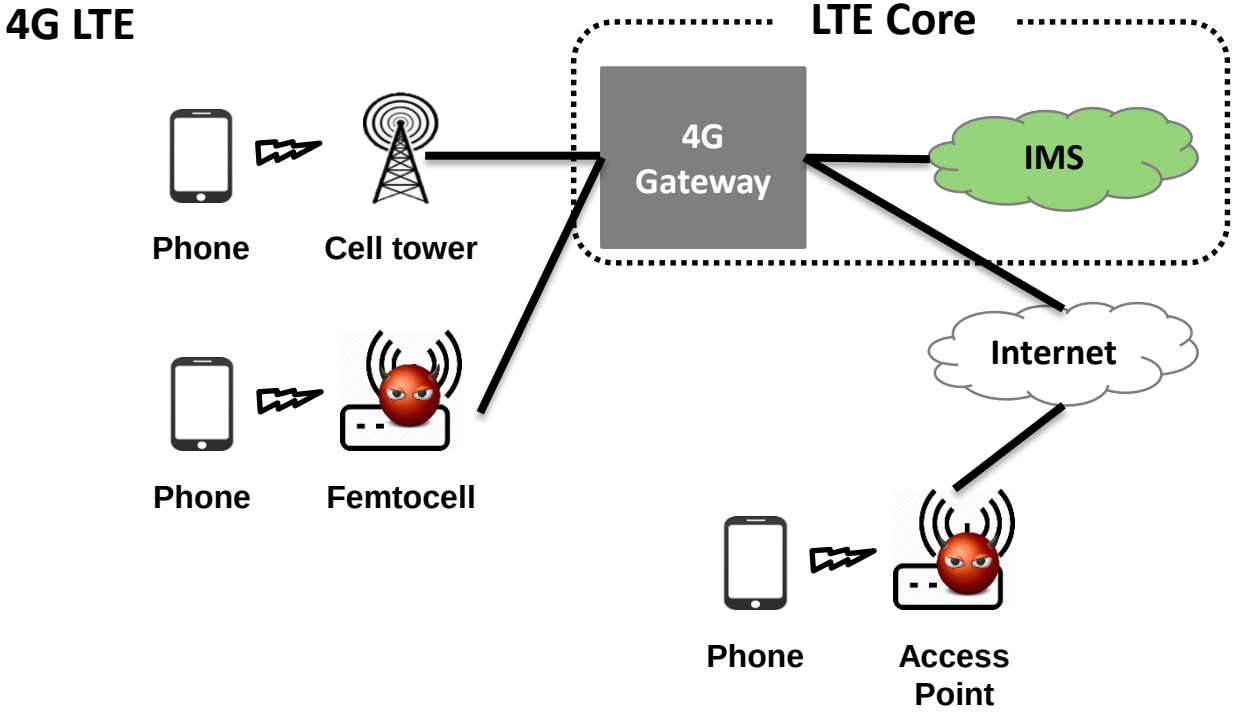
	US-1	US-2	KR-1	KR-2	KR-3
Network protocol	**IPv6**	**IPv6 + IPsec**	**IPv4**	**IPv4**	**IPv6**
Transport protocol for SIP	**TCP & UDP**	**TCP & UDP**	**UDP**	**UDP**	**UDP**
Encryption algorithm for IPsec	**-**	**AES**	**-**	**-**	**-**

Is Wiretapping Possible?



Wiretapping Is Possible!

- Even some operators are providing Wi-Fi calling without encryption!



No Encryption for Voice Packets

- For voice signaling,
  - only one operator was using IPsec
  - An attacker can easily manipulate VoLTE call flow
- For voice data,
  - no one encrypted voice data
  - An attacker might wiretap the outgoing voice data

Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
IMS	No SIP Encryption						Message manipulation
	No Voice Data Encryption						Wiretapping

 : Vulnerable  : Secure

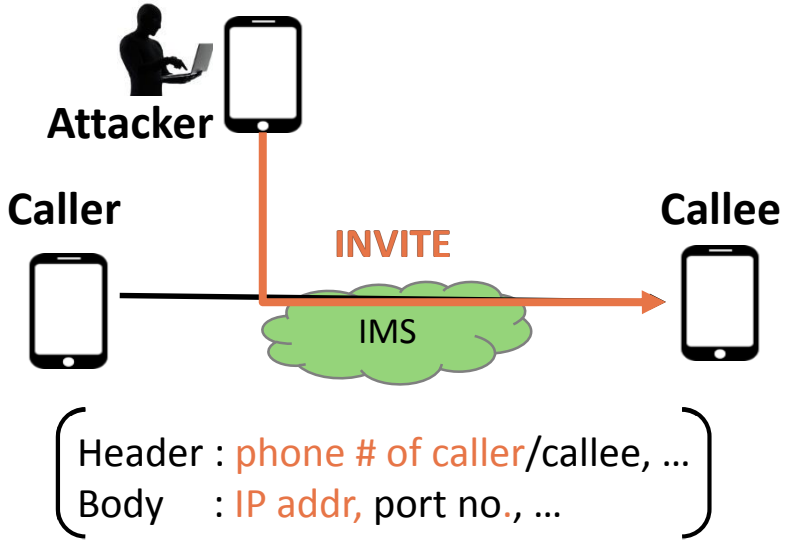
No Authentication/Session Management

- No authentication
  - Make a call with a fake number
- No session management
  - Send multiple INVITE messages
    - Several call sessions are established
  - **In a normal call, one user can call to only one person**
    - For each call session, high-cost bearer is established
  - Even one sender can deplete resources of the core network

Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
IMS	No Authentication						Caller Spoofing
	No Session Management						Denial of Service on Core Network

 : Vulnerable  : Secure

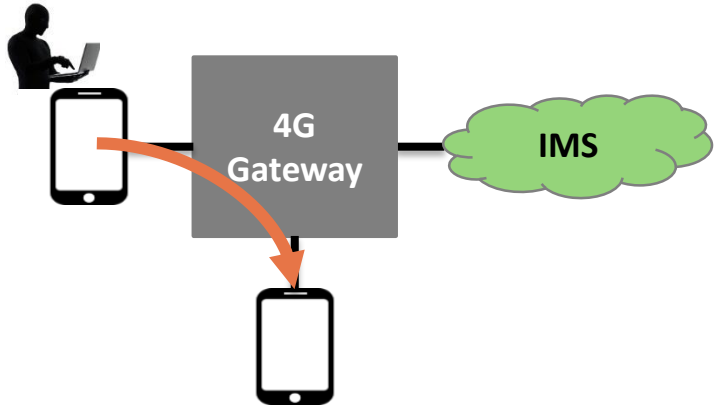
Caller Spoofing Scenario




vim (vim) ⌘1
..dia tunneling (zsh) ⌘2
adb (adb)
do_phishing = True
send_GangnamStyle = True
caller_ip = ".100.196"
caller_phone_no = "0606"
to_whom = "7183"
NORMAL BR: master | sip_client_spoof.py <os | utf-8 | python 11% LN 67:1
ATTACKER
11:26 PM
Tap to add current location
11:26 PM
Tue, Sep 29
Welcome to Smart Notice!
Getting started... Please wait.
Google
CALLEE
11:26 PM
YouTube
Phone
Messages
Contacts
Internet
Apps
CALLER
Phone
TALK

IMS Bypassing

- All voice packets should pass IMS, but
- An attacker can bypass SIP servers in IMS
  - IMS vulnerabilities are also possible
    e.g. Make a call with a fake number



Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
4G-GW	IMS Bypassing	😈	🙂	😈	🙂	🙂	Caller Spoofing

😈 : Vulnerable 🙂 : Secure

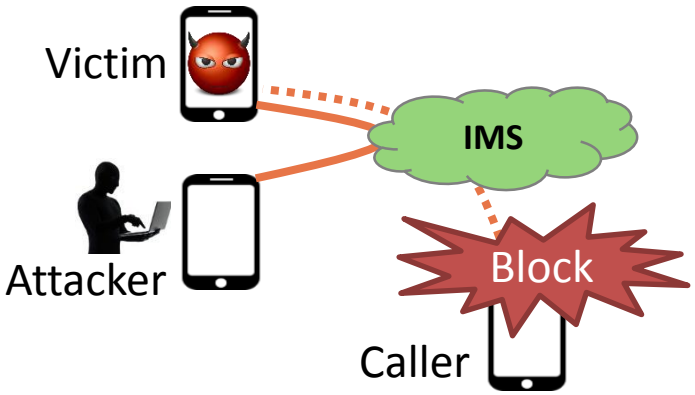
Android Permission Model Mismatch

- No distinction between a phone call and a normal data socket
  - An app needs "*android.permission.CALL_PHONE*"
  - In VoLTE, we found that an app can call with "*android.permission.INTERNET*"
- A malicious app **only with Internet permission** can perform
  - Denial of service attack on call
  - Overbilling attack by making an expensive video call

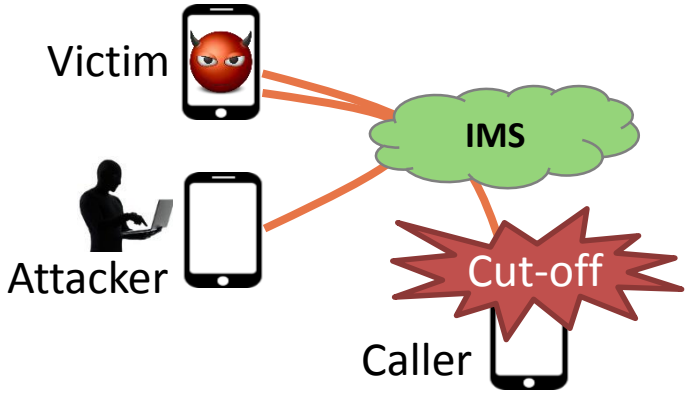
Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
Phone	Permission Mismatch	Vulnerable for all Android					Denial of Service on Call, Overbilling

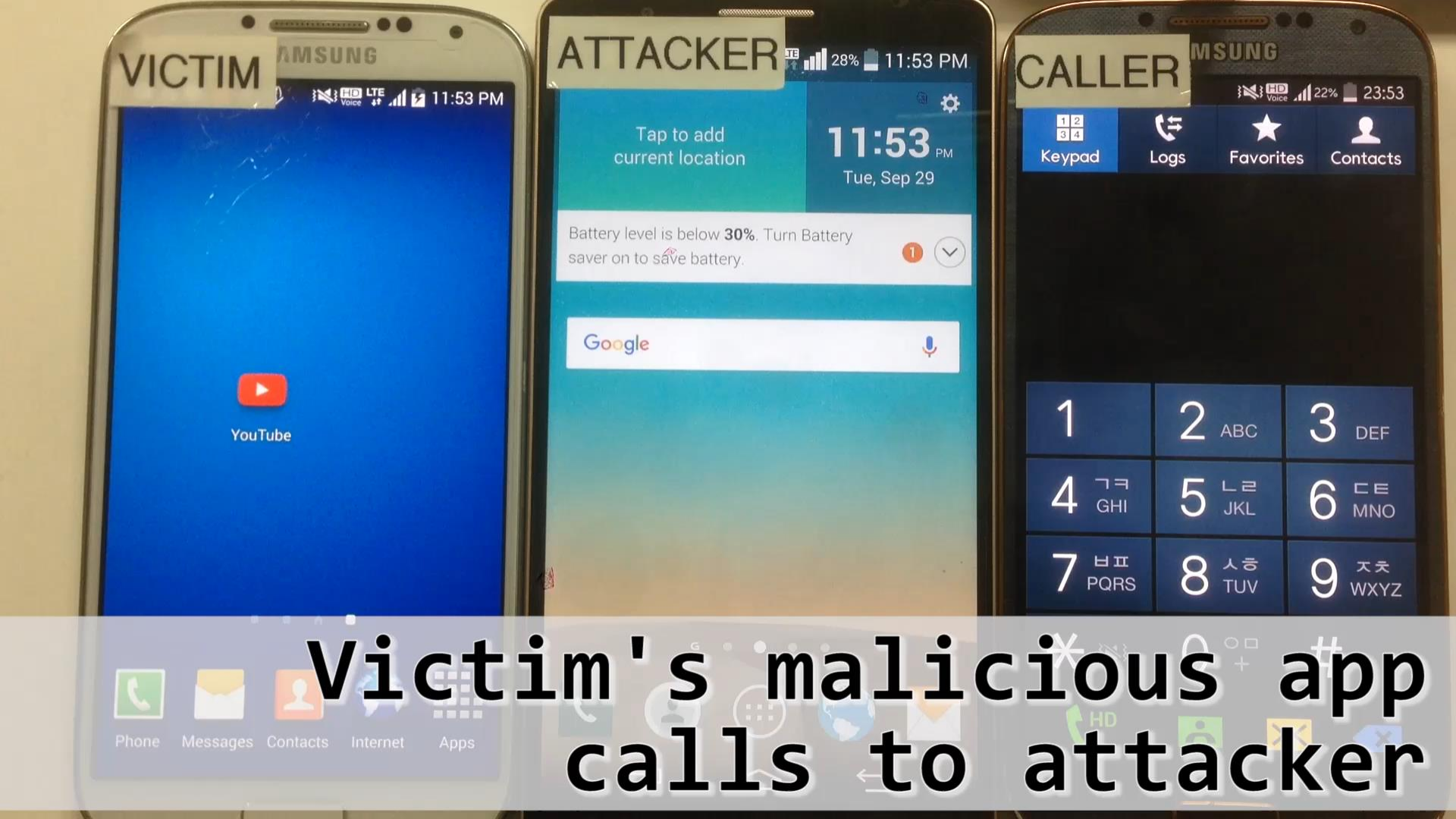
Denial of Service on Call Scenario

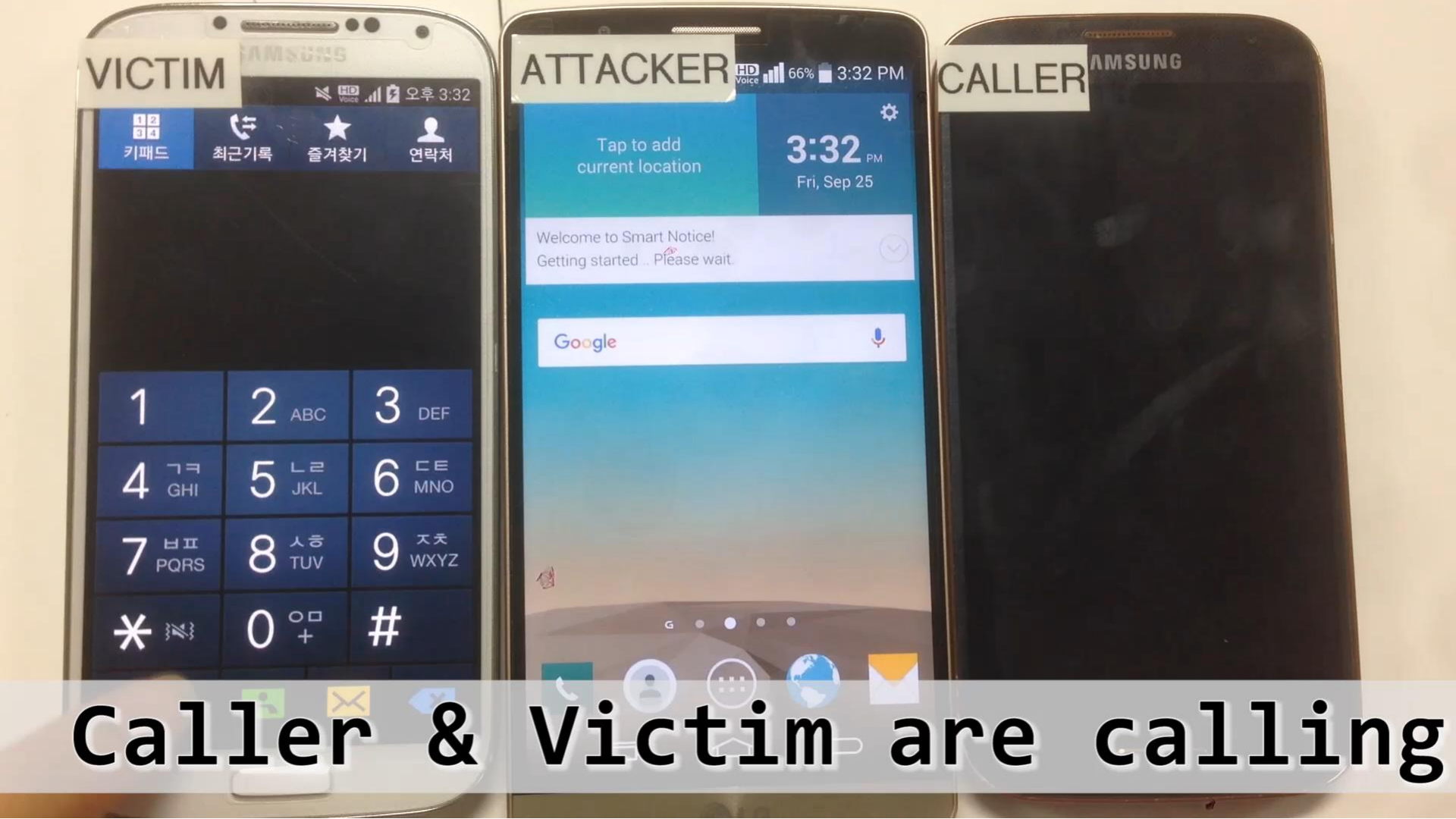
- Blocking an incoming call



- Cutting off an ongoing call




VICTIM
11:53 PM
YouTube
Phone
Messages
Contacts
Internet
Apps
ATTACKER
28% 11:53 PM
Tap to add current location
11:53 PM
Tue, Sep 29
Battery level is below 30%. Turn Battery saver on to save battery.
Google
CALLER
22% 23:53
Keypad
Logs
Favorites
Contacts
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
Victim's malicious app calls to attacker


VICTIM
오후 3:32
키패드
최근기록
즐겨찾기
연락처
ATTACKER
66% 3:32 PM
Tap to add current location
3:32 PM
Fri, Sep 25
Welcome to Smart Notice!
Getting started ... Please wait.
Google
CALLER
Caller & Victim are calling

Free Data Channels	Free Channel	US-1	US-2	KR-1	KR-2	KR-3
Using VoLTE Protocol	SIP Tunneling	✓	✓	✓	✓	✓
	Media Tunneling	✓	✓	✓	✓	✓
Direct Communication	Phone to Phone	✓	✗	✓	✗	✗
	Phone to Internet	✗	✓	✓	✗	✗

Weak Point	Vulnerability	US-1	US-2	KR-1	KR-2	KR-3	Possible Attack
IMS	No SIP Encryption						Message manipulation
	No Voice Data Encryption						Wiretapping
	No Authentication						Caller Spoofing
	No Session Management						Denial of Service on Core Network
4G-GW	IMS Bypassing						Caller Spoofing
Phone	Permission Mismatch	Vulnerable for all Android					Denial of Service on Call, Overbilling

 : Vulnerable  : Secure

Mitigation

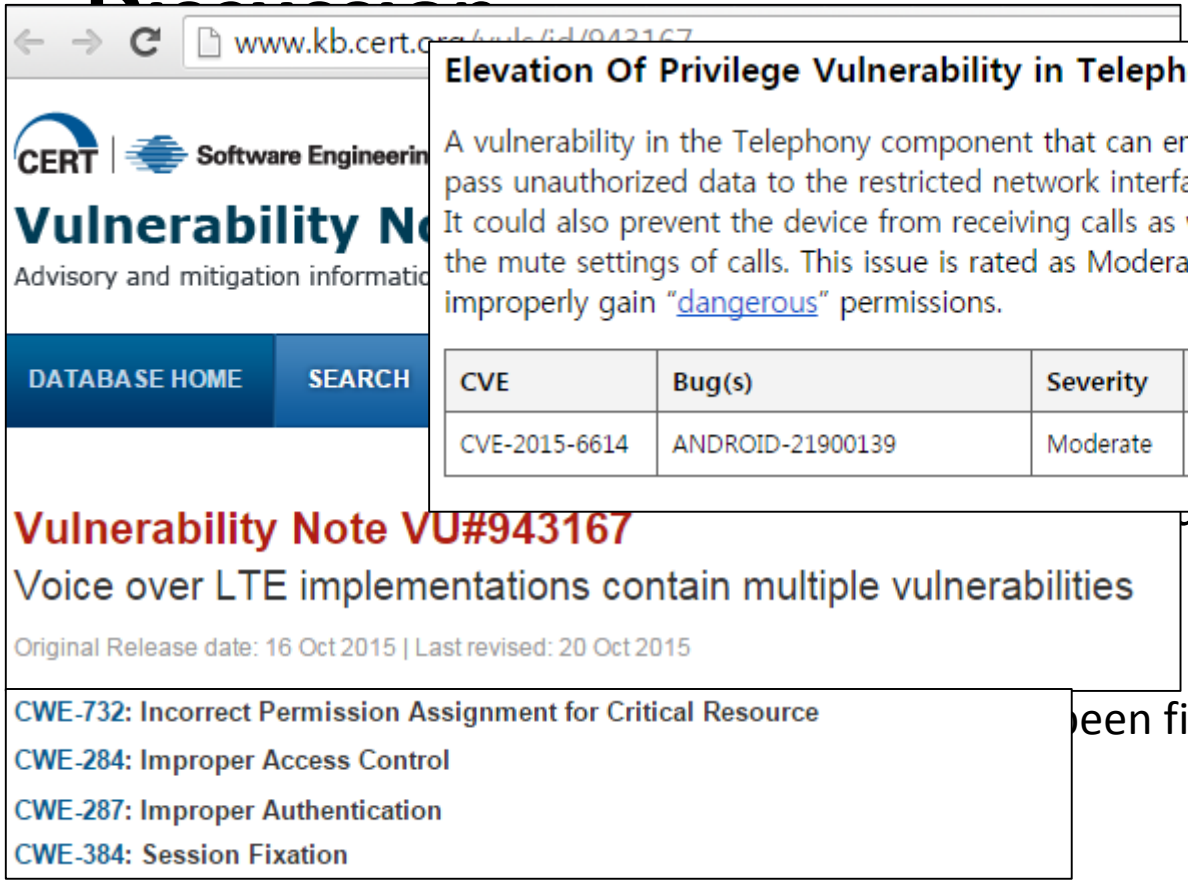
Point	Vulnerability	Mitigation	Responsible Entity
IMS	No Security Mechanisms	IPsec/TLS + SRTP	Operators IMS provider
	No Authentication	Cross-validation of all headers (IP/TCP/SIP)	
	No Session Management	Regulation on call sessions	
4G-GW	Direct Communication	Regulation on direct communication	Operators
Phone	Permission Mismatch	Strictly binding sockets to data interface	Mobile OS (Android)
	SIP/Media tunneling	Regulation on packet routing Deep packet inspection (DPI)	Mobile OS (Android) Operators

How to resolve media tunneling? **Not easy! Maybe byte-usage accounting?**

Discussion

- Some parts of 3GPP specifications are left to operators
  - Several misunderstandings of the operators
  - Different implementations and security problems
  - **Even important security features are only recommendations, not requirement**

- We reported vulnerabilities to US/KR CERTs, and Google in May
  - Google replied “moderate severity”
  - All two U.S. operators ACK’ed, but no follow-ups
  - Only two among three KR operators have been fixing with us



Elevation Of Privilege Vulnerability in Telephony

A vulnerability in the Telephony component that can enable a local malicious application to pass unauthorized data to the restricted network interfaces, potentially impacting data charges. It could also prevent the device from receiving calls as well as allowing an attacker to control the mute settings of calls. This issue is rated as Moderate severity because it can be used to improperly gain "dangerous" permissions.

CVE	Bug(s)	Severity	Affected versions	Date reported
CVE-2015-6614	ANDROID-21900139	Moderate	5.0, 5.1	Jun 8, 2015

ent

Google in May

been fixing with us

Discussion

www.kb.cert.org/vuls/id/943167

CERT | Software Engineering

Vulnerability No

Advisory

DATABA

Vulne

Voice

Original R

CWE-732

CWE-284

CWE-287

CWE-384

Elevation Of Privilege Vulnerability in Telephony

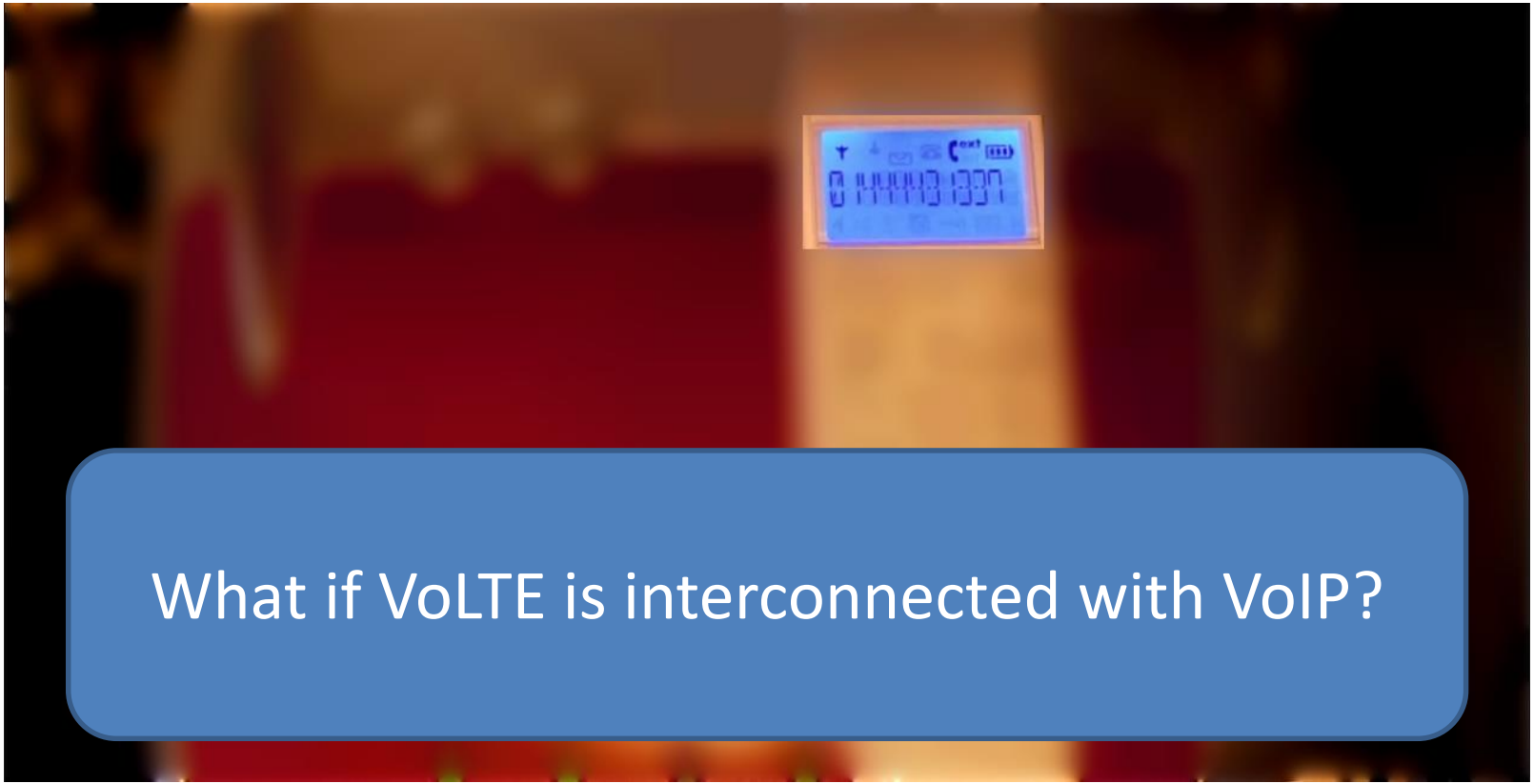
A vulnerability in the Telephony component that can enable a local malicious application to pass unauthorized data to the restricted network interfaces, potentially impacting data charges. It could also prevent the device from receiving calls as well as allowing an attacker to control

Acknowledgements

We would like to thank these researchers for their contributions:

- Abhishek Arya, Oliver Chang and Martin Barbella, Google Chrome Security Team: CVE-2015-6608
- Daniel Micay (daniel.micay@copperhead.co) at Copperhead Security: CVE-2015-6609
- Dongkwan Kim of System Security Lab, KAIST (dkay@kaist.ac.kr): CVE-2015-6614
- Hongil Kim of System Security Lab, KAIST (hongilk@kaist.ac.kr): CVE-2015-6614
- Jack Tang of Trend Micro (@jacktang310): CVE-2015-6611
- Peter Pi of Trend Micro: CVE-2015-6611
- Natalie Silvanovich of Google Project Zero: CVE-2015-6608
- Qidan He (@flanker_hqd) and Wen Xu (@antlr7) from KeenTeam (@K33nTeam, http://k33nteam.org/): CVE-2015-6612
- Seven Shen of Trend Micro: CVE-2015-6610

Is VoIP Secure Enough?



Conclusion

- Newly adopted VoLTE has
  - A complex (legacy time-based) accounting
  - Delegated voice signal (previously done by CP) to AP
- We analyzed the security of VoLTE for 5 operators, and found
  - Four free data channels
  - Five security problems
- All related parties have problems
  - 3GPP, telcos, IMS providers, mobile OSes, and device vendors
- More and more reliance on cellular technology
  - Automobiles, power grid, traffic signal, ...

Holistic re-evaluation of security for VoLTE?

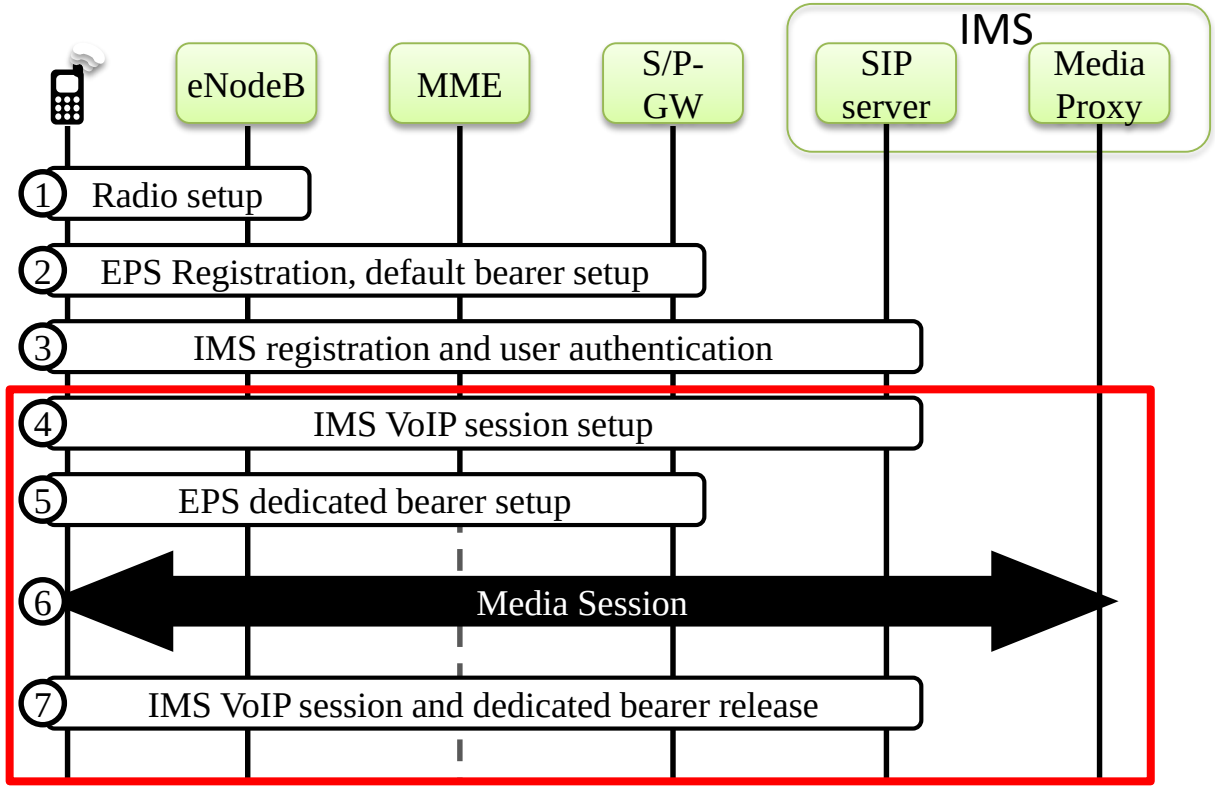
Thank You!

Any questions?

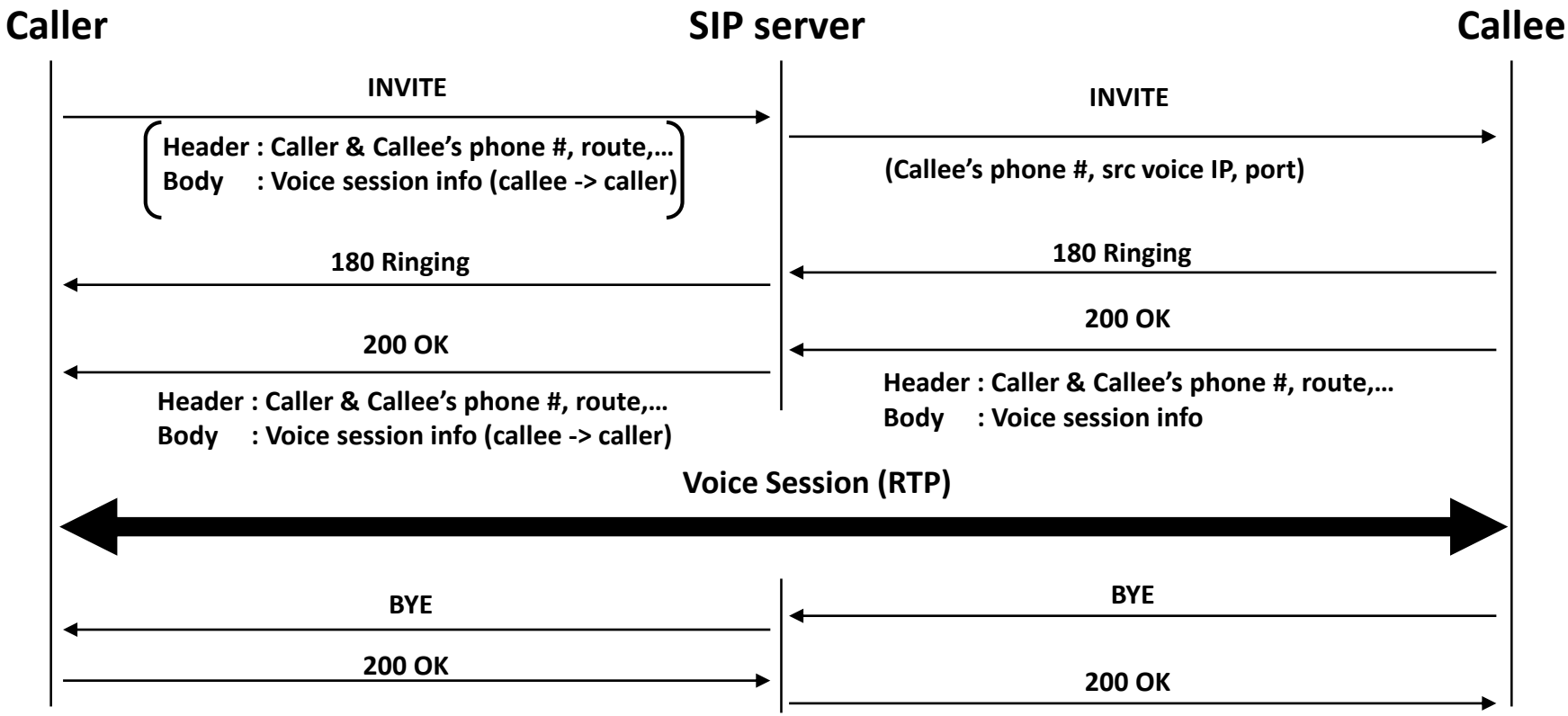
dkay@kaist.ac.kr
hongilk@kaist.ac.kr

APPENDIX

VoLTE procedure



SIP Signaling Procedure



Empirical Analysis

	US-1	US-2	KR-1	KR-2	KR-3
Network protocol	IPv6	IPv6 + IPsec	IPv4	IPv4	IPv6
Transport protocol for SIP	TCP & UDP	TCP & UDP	UDP	UDP	UDP
Encryption algorithm for IPsec	-	AES	-	-	-
Capability of changing SIP source port	✓	✘	✓	✓	✓
Existence of a media proxy	✘	✓	✘	✓	✓
Sending random data through media session	✓	✓	✓	✓	✓
Free use of audio channel	✓	✓	✓	✓	✓

Detailed Results of Media Tunneling

- Media channel characteristics from the control plane messages

	US-1	US-2	KR-1	KR-2	KR-3
QoS Param. (Kbps)	38	49	41	41	49
Bandwidth (Kbps)	38/49	49	65	65	65
Latency (sec)	0.1	0.1	0.1	0.1	0.1
Loss rate (%)	1	1	1	1	1

- Actual measurement results (**trade-offs** between throughput and loss rate)

	US-1	US-2	KR-1	KR-2	KR-3
Throughput (Kbps)	37.90	36.93	45.76	39	50.48
Latency (sec)	0.52	0.02	0.10	0.32	0.30
Loss rate (%)	1.44	1.74	0.77	0.65	0.73