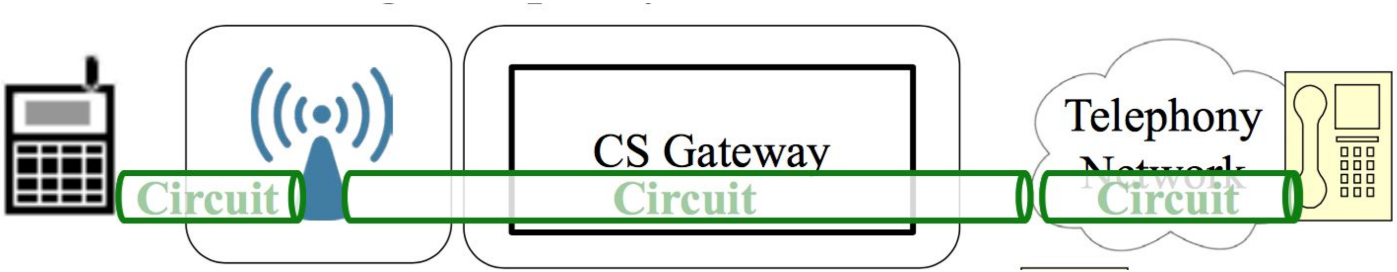
Insecurity of Voice Solution VoLTE in LTE Mobile Networks

Chi-Yu Li, Guan-Hua Tu, Chunyi Peng, Zengwan Yuan, Yuanjie Li, Songwu Lu, Xinbing Wang

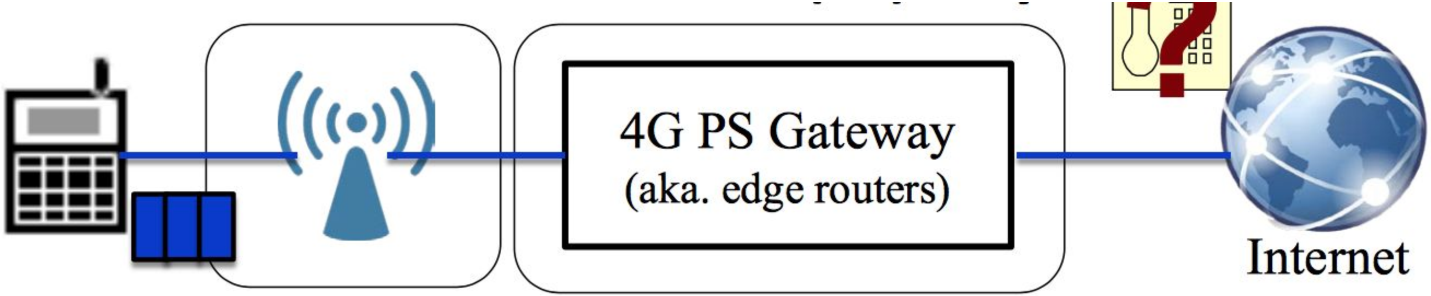
(CCS'15)

Voice Evolution in 4G LTE

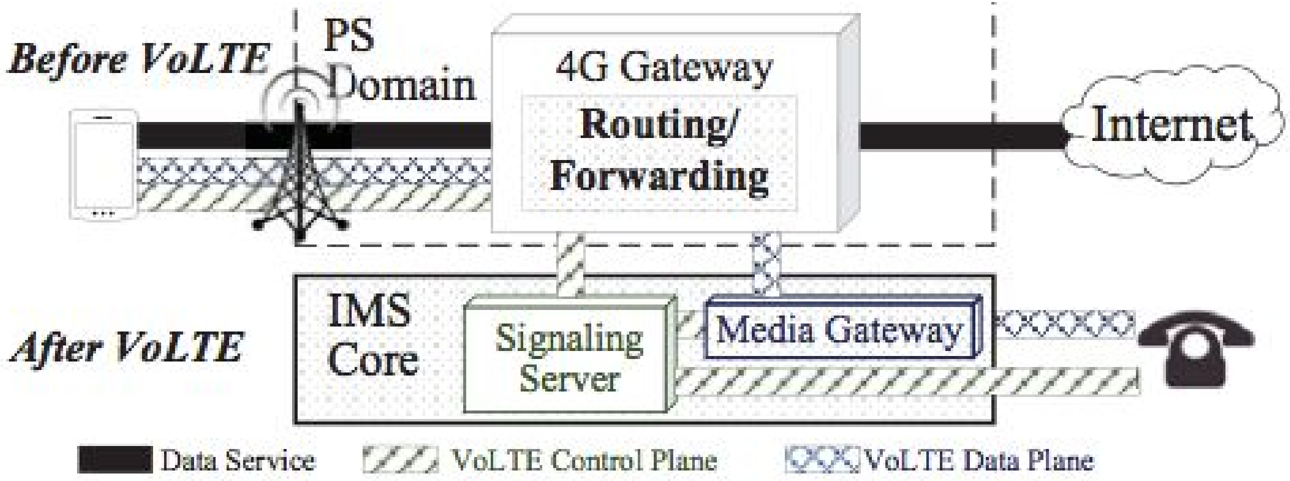
- 2G/3G Solution: Circuit Switched



- 4G LTE Solution: Pack Switched
  - Similar to VoIP over the Internet w/ high priority, quality of service offered by LTE



Voice over LTE (VoLTE): Voice in Packets



- PS delivery: offers PS connectivity, forwards packets, and control utility
- IMS Core: telephony & multimedia service
    - Media: deliver multimedia (voice) to VoLTE users
    - Signal: call control function

How does VoLTE work?

- Control Plane
    - Exchange call signaling messages through session initiation protocol
    - On as long as VoLTE is on
    - Non-guaranteed bit-rate w/ highest priority
- Data Plane
    - Voice packet delivery
    - On demand by control session
    - Guaranteed bit rate class
- All voice traffic and signaling messages are carried in packets
    - 4G gateway route regular data packages but also control and data plane packages
    - Higher priority than data services

Carrying Data in Signaling Bearer

Lack of Access Control at Phone Software & Hardware

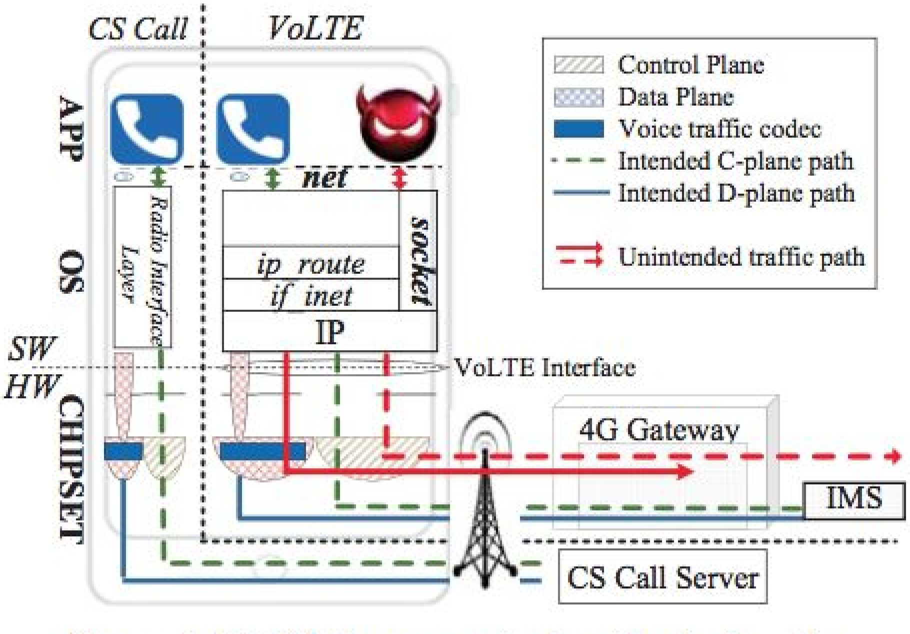


Figure 3: VoLTE Access control on the device side.

- Two Access Control for VoLTE
  - Hardware
  - Software
    - Apps can obtain VoLTE interface information
      - IP and routing information
    - Injecting data packets to signal bearer

Lack of Access Control at Phone Software & Hardware

- Validation
    - App can obtain VoLTE interface
        - learning signal bearer & PS data
            - Check rmnet0 or rmnet1 when disabling VoLTE
            - Then check routing table
    - Inject Non-VoLTE packets into signaling bearer
        - Send packet to signaling server
        - Receives ICMP packet from VoLTE gateway
- Lesson
    - Can’t distinguish Internet data & VoLTE interface
    - Hardware trusts all VoLTE interface traffic

Imprudent Routing and Forwarding in the Network

- Traffic carried through VoLTE is not verified at runtime
  - Non-authentic control packets can be forwarded by network
- Routing Rules in Mobile Networks are abused
  - When routing rule toward each phone exist at gateway, phone can communicate without reaching signaling bearer
  - Mobile to Mobile & Mobile to Internet Communication
- Validation
  - Mobile to Internet: observe messages exchange between phone and external server
  - Mobile to Mobile: send ICMP Echo Request to Mobile
- Lessons
  - Operator does not regulate routing and packet forwarding for the VoLTE bearer

Exploiting VoLTE for Free Data Access

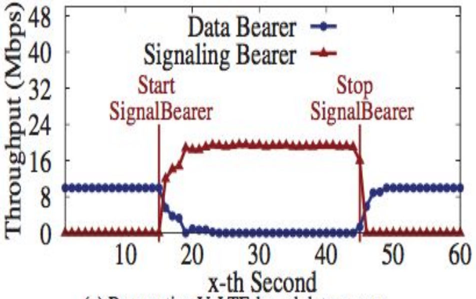
Abusing No Billing of VoLTE Signal

- Billing doesn’t take signaling into account, regardless of destination
    - Only call duration on data plane is collected for billing
    - Control messages is meant for facilitating calle
- Hence, injecting data into signal bearer -> free data
- No way of limiting traffic going through signaling bearer
- Validation
    - Make calls every 15 seconds for 10 hours, 42.4 MB control messages, none charged
    - Fake 5000 ICMP Echo Request and receive 4914 echo replies
- Lessons
    - Exploit free signaling
    - Better access control or no free-of-charge policy

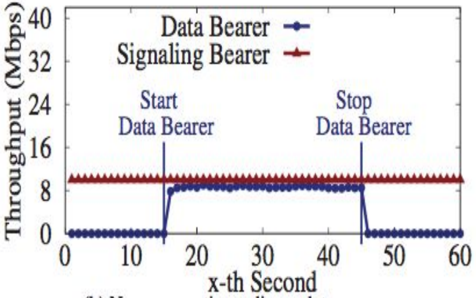
Manipulating Data Access Priority

Abusing High QoS og VoLTE Signaling

- VoLTE suppresses normal PS data
- Validation
    - During downlink session, launch VoLTE exploit data access that’s greater than affordable throughput
    - Swap launch ordering for exploited VoLTE and data session



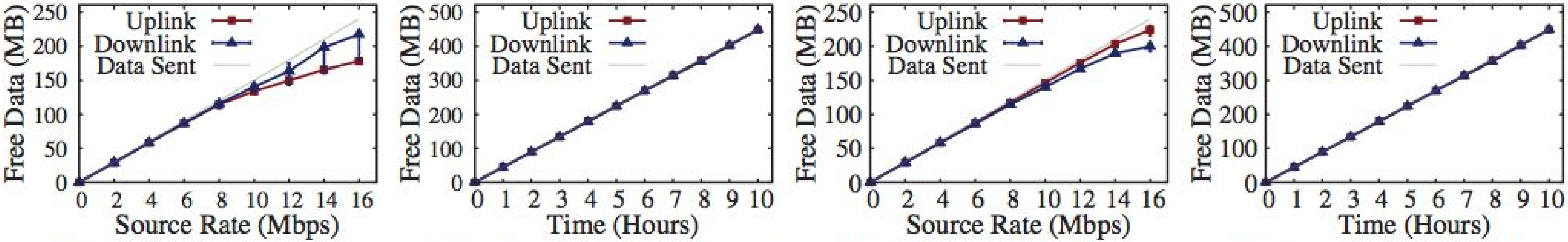
(a) Preemptive VoLTE-based data access



(b) Non-preemptive ordinary data access

Proof Of Concepts Attacks

- Free Data Attack
    - Adversary leverages ICMP tunneling to deliver data through signal bearer
    - Update routing table (only on rooted phone)



(a) Mobile-to-Internet data w.r.t rate (b) Mobile-to-Internet data w.r.t time (c) Mobile-to-mobile data w.r.t rate (d) Mobile-to-mobile data w.r.t time

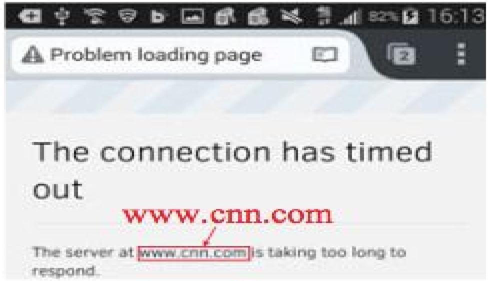
Figure 8: The volume of free data almost linearly increases with regards to (w.r.t) traffic source rate and run time in external (a,b) and internal (c,d) cases.

Proof of Concepts Attacks

- Data DoS Attack
  - Shutdown ongoing services by leveraging priority access
  - Requires malware on victim’s phone to detect data services starts and send adversary IP information
  - Adversary sends high-rate spams to victim’s IP
- Overcharging Attack
  - Similar as the above attack, the adversary sends spams to victim’s IP via data service bearer

Attacks on Real Apps

- Free Skype Service over Mobile Networks
  - ICMP tunnel between phone and external server
  - Modify routing table to tunneling server
  - Run skype app over phone and consume data
- Data DoS on Web Browser and Youtube
  - Data DoS while loading CNN webpage with browser watching Youtube
  - Send 10Mbps of VoLTE spam to phone

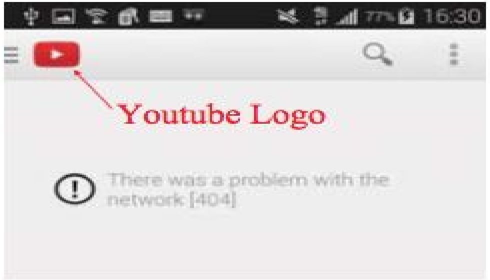


Problem loading page

The connection has timed out

The server at www.cnn.com is taking too long to respond.

(a) Web DoS



There was a problem with the network [404]

(b) Youtube DoS

Muting Voice Through Spams in VoLTE Data Plane

Injecting Voice Into the Voice Bearer

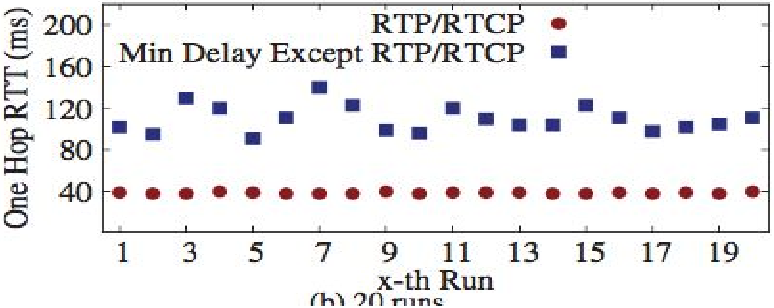
- Voice Bearer
    - Handled by hardware without software intervention
    - Each session identifier is a secret
- However
    - Deliver invalid data packet since
        - Inject data to voice bearer
        - Confidential information can be inferred through salient features

Insufficient Data-Plane Access Defense at Phone

- Voice codec is encoded within hardware
- But, it doesn’t restrict access to authentic VoLTE calls only
  - Accepts other apps injection as long as correction session information
  - Voice bearer can be overflowed
- Validation
  - During an ongoing call, app generates packets with voice session identifier and sends to via VoLTE interface
  - Callee’s voice is muted
- Lessons
  - Doesn’t authenticate origin of app traffic

Side-Channel Leakage of Session Privacy

- Session ID should be secret as carried by the signaling messages of VoLTE application
- Destination IP address can be retrieved from routing table
- VoLTE signal and voice bearer uses the same IP, so one can learn port by sending packets to all the ports because RTP and RTCP has smallest delay
- Validation
    - App scans all port and and delay between ports



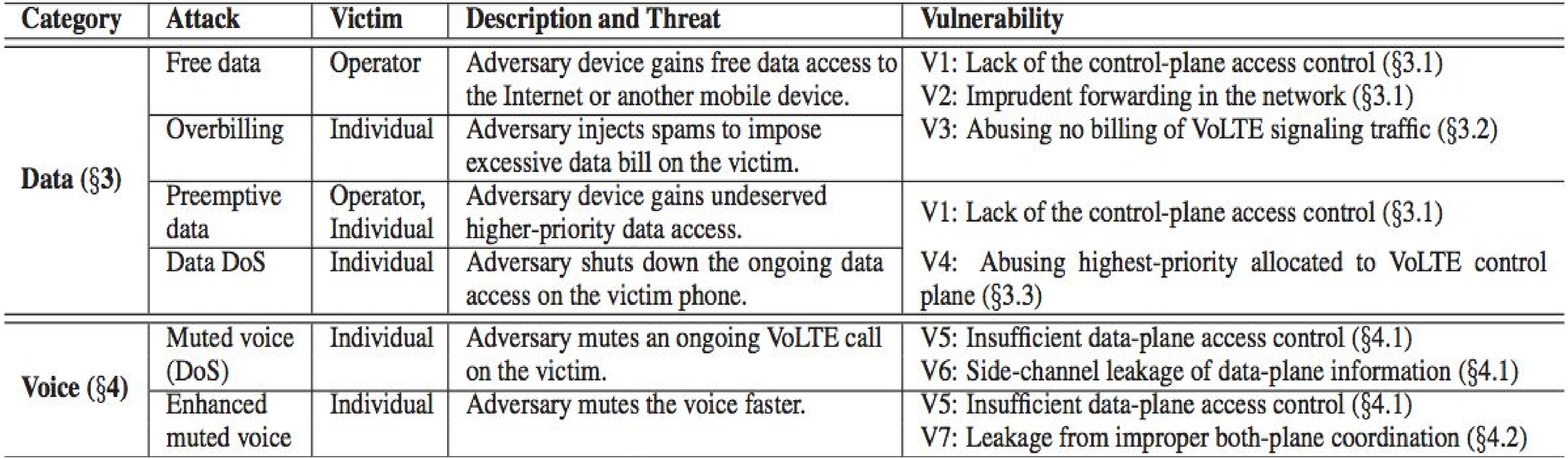
Side-Channeling Leakage by Improper Coordination

- Get Voice session ID
- Voice Bearer during call setup and termination via control signals
- If voice bearer isn’t established, voice packets are sent to control plane
  - Observe voice packet via non-VoLTE apps
- Validation
  - IP packets collected from VoLTE signaling interface and verifies port

Voice Muted DoS Attack

- Call muted on both sides, requires a malware on victim’s phone
- Learn ports of RTP session via side-channeling
- Malware hijack RTP packets with corresponding session ID
- Mute both uplink and downlink

Summary



Category	Attack	Victim	Description and Threat	Vulnerability
Data (§3)	Free data	Operator	Adversary device gains free data access to the Internet or another mobile device.	V1: Lack of the control-plane access control (§3.1) V2: Imprudent forwarding in the network (§3.1) V3: Abusing no billing of VoLTE signaling traffic (§3.2)
	Overbilling	Individual	Adversary injects spams to impose excessive data bill on the victim.	
	Preemptive data	Operator, Individual	Adversary device gains undeserved higher-priority data access.	V1: Lack of the control-plane access control (§3.1) V4: Abusing highest-priority allocated to VoLTE control plane (§3.3)
	Data DoS	Individual	Adversary shuts down the ongoing data access on the victim phone.	
Voice (§4)	Muted voice (DoS)	Individual	Adversary mutes an ongoing VoLTE call on the victim.	V5: Insufficient data-plane access control (§4.1) V6: Side-channel leakage of data-plane information (§4.1)
	Enhanced muted voice	Individual	Adversary mutes the voice faster.	V5: Insufficient data-plane access control (§4.1) V7: Leakage from improper both-plane coordination (§4.2)

Recommended Fixes

- 4G Gateway enforces strict routing regulation for bearer
- Operator stops free-signaling policy and charges signals to data traffic
- Ensure resource allocation to authentic traffic only
- Device
  - Only allow dialer app to access VoLTE interface
  - Chipset verifies traffic source and destination

Discussion

- What are the main contributions to this work?
- What are the limitations of the paper?
- Are the attacks feasible on a large scale?
- Are the mitigations suggested sufficient?