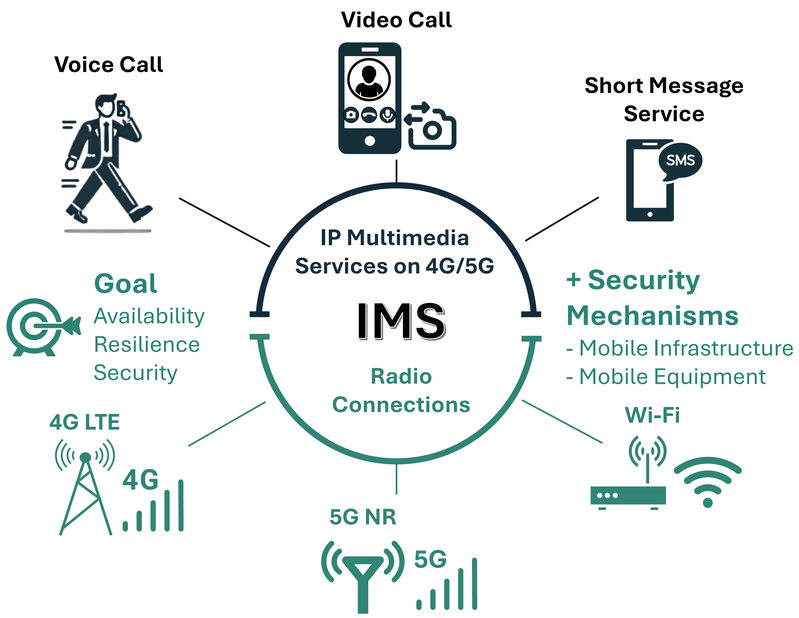
IMS is Not That Secure on Your 5G/4G Phones

Jingwen Shi[1], Sihan Wang[1], Min-Yue Chen[1], Guan-Hua Tu[1], Tian Xie[2], Man-Hsin Chen[3], Yiwen Hu[1], Chi-Yu Li[3], Chunyi Peng[4]
[1] Michigan State University [2] Utah State University [3] National Yang Ming Chiao Tung University [4] Purdue University

SNMS Research
Security, Networking, and Mobile System

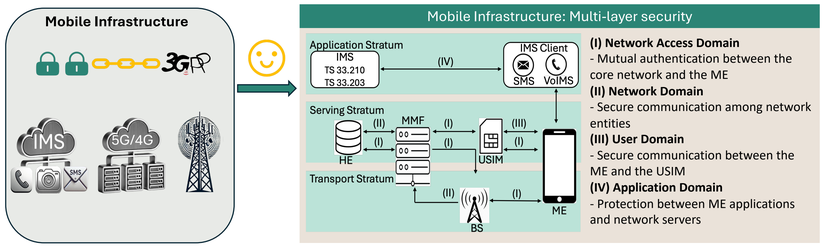
What Is IMS ?



What Is Our Motivation?

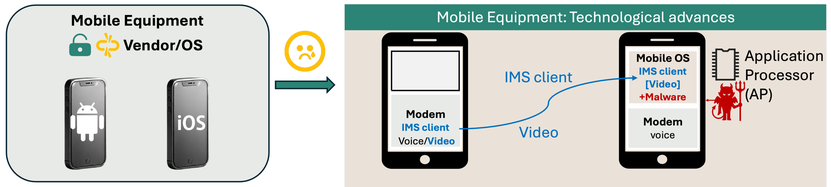
Motivation: Security of mobile equipment (ME) lags behind that of the network architecture.

Mobile infrastructure employs multi-layered security across four domains.



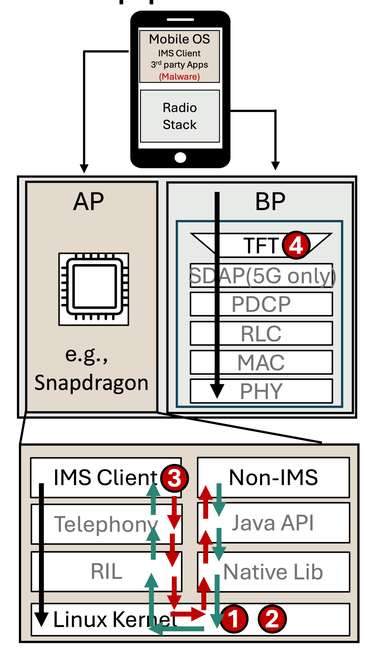
Mobile equipment security has remained unchanged over the past decades !

It also failed to keep pace with technological advances.



Our Findings

Mobile Equipment Architecture



Four insecure designs:

V1. Unprotected IMS signaling routing [**Intercept**]

V2. Unrestricted IMS signaling source [**Inject**]

V3. Unprotected video data delivery [**Hijack**]

V4. Unrestricted source for IMS video delivery [**Hijack**]

Three attacks:

A1. Block IMS services

A2. Spoof SMS with arbitrary display name

A3. Hijack video session

Validation:

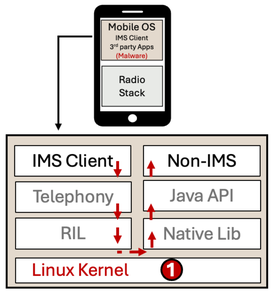
Ten phone models [Samsung, LG, TCL, Google Pixel]

Five Carriers

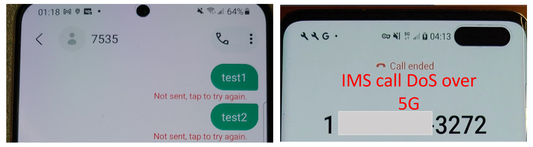
Two countries

A1. DoS-ALL Attack

Mobile Equipment Architecture

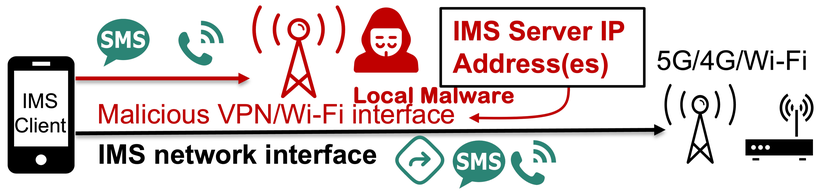


Damage: A novel DoS attack that prevents IMS clients from using **all** access networks over Wi-Fi, 4G LTE, 5G NR.



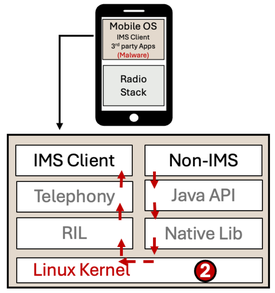
Challenge: The conventional VPN/Wi-Fi interface **cannot** prevent users from accessing IMS services.

Solution: Adversary can assign the IMS server IP address to a malicious VPN/Wi-Fi interface, bypassing the restriction. [V1]

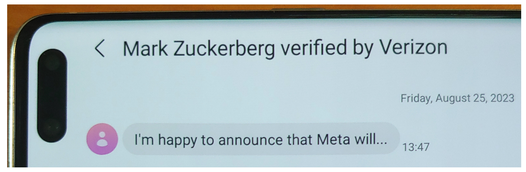


A2. NameSpoofing Attack

Mobile Equipment Architecture

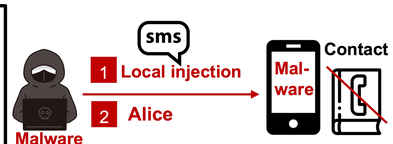


Damage: The SMS sender's display name can be arbitrarily specified.



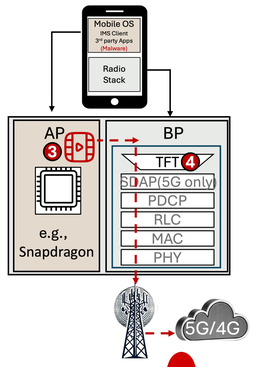
Challenge: The conventional method of spoofing a display name is **not** practical: Pass 5G/4G network -> Exist in contact

Solution: Fabricate SMS by the 3GPP2 standard (ASCII).
The ME may adopt a *pass-through* policy for IMS signaling fall outside of IPsec protection.



A3. ViIMS-ANY Attack

Mobile Equipment Architecture

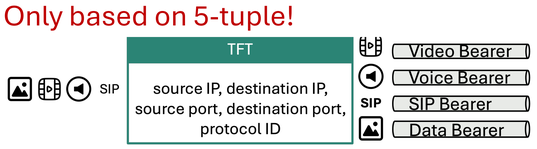


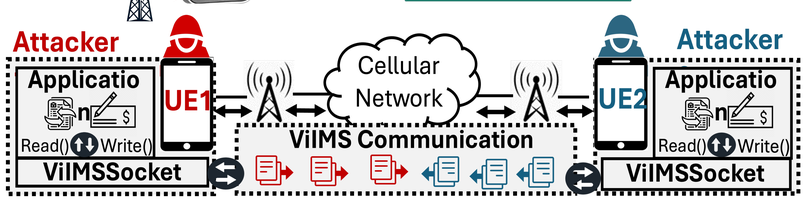
Damage: An attack that abuses ViIMS as a covert communication channel between two malicious MEs, bypassing operator policies.

V3: No encryption or authentication for media data.

V4: TFT (Traffic Flow Template)

Only based on 5-tuple!





Google Security Vulnerabilities Report Assessment:
High severity and High quality

© 2024 SNMS Research Lab, Michigan State University. Presented at MobiCom 2024. All rights reserved.
Contact: Jingwen Shi, shijingw@msu.edu ; Sihan Wang, wangsih3@msu.edu