1100 - ‘Ghost Telephonist' Impersonates You Through LTE CSFB

Sunday at 11:00 in Track 4
45 minutes | Exploit

Yuwei Zheng*Hacker*

Lin Huang*Hacker*

One vulnerability in CSFB (Circuit Switched Fallback) in 4G LTE network will be presented. In the CSFB procedure, we found the authentication step is missing. This results in that an attacker can hijack the victim's communication. We named this attack as 'Ghost Telephonist'. Several exploitations can be made based on this vulnerability. When the call or SMS is not encrypted, or weakly encrypted, the attacker can impersonate the victim to receive the "Mobile Terminated" calls and messages or to initiate the "Mobile Originated" calls and messages. Furthermore, Telephonist Attack can obtain the victim's phone number and then use the phone number to make advanced attack, e.g. breaking Internet online accounts. These attacks can randomly choose victims, or target a given victim. We verified these attack with our own phones in operators' network in a small controllable scale. The experiments proved the vulnerability really exists. The attack doesn't need fake base station so the attack cost is low. The victim doesn't sense being attacked since no fake base station and no cell re-selection. Now we are collaborating with operators and terminal manufactures to fix this vulnerability.

Yuwei Zheng

Yuwei Zheng is a senior security researcher from Radio Security Research Dept. of 360 Technology. He has rich experiences in embedded systems over 10 years. He reversed blackberry BBM, PIN, BIS push mail protocol, and decrypted the network stream successfully in 2011. He successfully implemented a MITM attack for Blackberry BES based on a modified ECMQV protocol of RIM. He focuses on the security issues of embedded hardware and IOT systems. He was the speaker of DEF CON , HITB etc.

@huanglin_bupt

Lin Huang

Lin HUANG is a wireless security researcher and SDR technology expert, from Radio Security Research Dept. of 360 Technology. Her interests include the security issues in wireless communication, especially the cellular network security. She was the speaker of some security conferences, DEF CON , HITB, POC etc. She is the 3GPP SA3 delegate of 360 Technology.

Contributor Acknowledgement:

The Speakers would like to acknowledge Qing YANG, for his contribution to the presentation. Qing YANG is the founder of UnicornTeam & Radio Security Research Department in 360 Technology. He has rich experiences in information security area. He made presentations at BlackHat, DEF CON , CanSecWest, HITB, Ruxcon, POC, XCon, China ISC etc.

#defcon25/by_track/track4/sunday #defcon25/By_Day/_Sunday