



Liaison Statement

Liaison Statement Title:	Impersonation Attacks in 4G Networks
---------------------------------	--------------------------------------

Source Meeting Information		
Meeting Number	Meeting Date	Meeting Location
CVD#24_01	21 May 2019	Conference Call, London

Document Details		
Document Number:	Creation Date:	Document Author:
Doc CVD-2019-0024	22 May 2019	GSMA CVD Governance Team / Samantha Kight, GSMA
Originating GSMA Source:	Deadline for response:	Liaison Statement Contact
GSMA CVD Governance Team	30 June 2019	GSMALiaisons@gsma.com
Security Classification	Non-confidential	

Action	
Recipients: To: 3GPP SA3 and RAN2 Cc: RAN	GSMA would like to ask 3GPP SA3 and RAN2 to take the above into consideration for Impersonation Attacks in 4G Networks.

1 Introduction

GSMA has been made aware through its “Coordinated Vulnerability Disclosure Programme” that a Research Paper concerning impersonation attacks in 4G Networks is due to be published later this year. In order to allow for the telecommunications standards setting community to address the above vulnerability, the authors of the Research Paper have agreed that the summary of the work may be shared with 3GPP.

2 Item for Consideration

2.1 Abstract from the Research Paper

“Mutual authentication is used to confirm the claimed identities of communication parties. In the context of mobile networks, it is an important security aim for the connection between user equipment (e.g., smartphones) and base stations, as the wireless medium is accessible for everyone and identities can be easily forged. Proving the claimed identities with the help of cryptographic protocols prevents attacks in which an attacker impersonates one of the parties. Long Term Evolution (LTE/4G) as the latest deployed mobile network generation establishes mutual authentication with a provably secure Authentication and Key Agreement (AKA) protocol on layer three of the network stack. Unfortunately, recent studies demonstrate the feasibility of impersonation attacks against LTE on layer two that allow to deterministically manipulate user data due to missing integrity protection.

In this paper, we perform a cross-layer analysis considering the layer-two vulnerability combined with layer-three mechanisms. We find that the capability to manipulate user data in combination with packet reflections as default IP stack behavior of operating systems allows an active attacker to impersonate a user towards the network and vice versa; we name these attacks imp4Gt (IMPersonation attacks in 4G neTworks). In particular, we show that an attacker can establish arbitrary TCP/IP connections to the network (on behalf of the victim) or the phone (on behalf of the network). The attacks have severe consequences for both providers and users: providers can no longer rely on mutual authentication for billing, access control, and legal prosecution. On the other side, users are exposed to any incoming IP connection as the attacker can bypass the provider’s firewall. We demonstrate the real-world applicability of the uplink imp4Gt attack and access a website with the victim’s identity in a commercial network. Our analysis demonstrates that the lack of integrity protection in combination with the IP stack behavior of mobile operating systems completely breaks the mutual authentication aim of LTE on the user plane.”

2.2 Observations from GSMA

In their Research Paper the authors describe two attacks which need to be addressed; an uplink impersonation attack and downlink impersonation attack.

The 3GPP specification requires only encryption but not integrity protection for the user plane traffic between the UE and the eNB. A man-in-the-middle attacker on the radio interface can perform a known-plaintext attack for the user plane replacing the contents of whole PDCP frame with attacker’s own IP packets, thus impersonating the victim in uplink direction, or impersonating as an arbitrary TCP server towards the UE in downlink direction.

An essential part of the new attacks is to use ICMP responses from the UE when the attacker needs to learn the LTE network internal information in order to perform the known-plaintext attack. The attacks exploit UE's default IP stack behaviour where the original IP packet, containing LTE network internal addressing information, is included in ICMP Destination Unreachable message. Even if ICMP Destination Unreachable messages would be filtered in LTE network's firewall the attacker is able to change the message type to allowed ICMP messages to bypass firewall. The research paper shows that typically MNOs allow ICMP Echo messages from their LTE networks.

The paper discusses several countermeasures such as DNS over TLS to block the preparation phase of the attack, and changing the mobile OS IP reflection behaviour to prevent the victim's phone being used as an encryption/decryption oracle, but all mentioned countermeasures have significant limitations according to the researchers. In the end the researchers recommend to deploy mandatory full rate integrity protection on the user plane in LTE and in 5G with "urgency".

The authors submitted the paper to a conference to be presented publicly on 11-15 November 2019.

2.3 3GPP Support: SA3 and RAN2

GSMA is requesting SA3 and RAN2 to review what needs to be done to cover this from a standards perspective in order to make sure there is protection for customers. These new attacks also exploit the lack of user plane integrity protection, like the previously known "aLTEr"-attack, which shows that a general solution is needed.

2.4 Deadline

GSMA would appreciate a response from the SA3 meetings on 24-28 June 2019 and implementation accordingly by the next SA3 and RAN2 meetings taking place end of August 2019.

3 Contact

Further questions, can be directed to Samantha Kight at the GSMA (skight@gsma.com)

Annex A Further Information on GSMA CVD

A.1 GSMA CVD

The GSMA coordinated Vulnerability disclose programme invites both private individuals and organisations to report vulnerabilities impacting the mobile industry to the GSMA in a responsible manner. More information may be found at gsma.com/cvd.

A.2 GSMA CVD Governance Team

This team consists of GSMA operator members who are Subject Matter Experts within the GSMA Fraud and Security Group. The team assess and determine the appropriate steps for industry in dealing with each CVD submitted to the GSMA.