Cellular location tracking attacks using signalling protocols

Siddharth Rao[1], Tuomas Aura[1], Dr. Silke Holtmanns[2], Dr. Ian Oliver[2]
[1] Department of Computer Science, Aalto University
[2] Bell labs - Nokia Networks, Finland

Signaling System no. 7 (SS7)

Signaling System No. 7 (SS7) is one of the mobile communication backend protocols mainly used for establishing the roaming interconnectivity across 2G/GSM mobile network operators. Besides roaming, SS7 has enabled a wide range of facilities such as Short Message Services (SMS), toll-free numbers, televoting and Local Number Portability (LNP). It was built during the time when mobile network operators used to be the trusted network of government-owned organizations and the security of the whole network were provided by denying access to external entities. Being a four decades old protocol, SS7 have the following issues:

- Attackers can gain access to the SS7 based core network using other Internet protocols.
- Once they are inside the core network, they can exploit the routing layer to map the periphery of the network, scan for open ports and send hostile communication messages.
- Since there is no authentication check or any other cryptographic protection within the network, the attackers can impersonate as the network internal nodes and query for subscriber information from other nodes.

Location tracking attacks using SS7

As shown in figure 1, an attacker with SS7 access can track the location of the cellphone users just by having their phone number. The accuracy of the tracked location depends on the cellular service procedure and the core network element queried by the attacker.

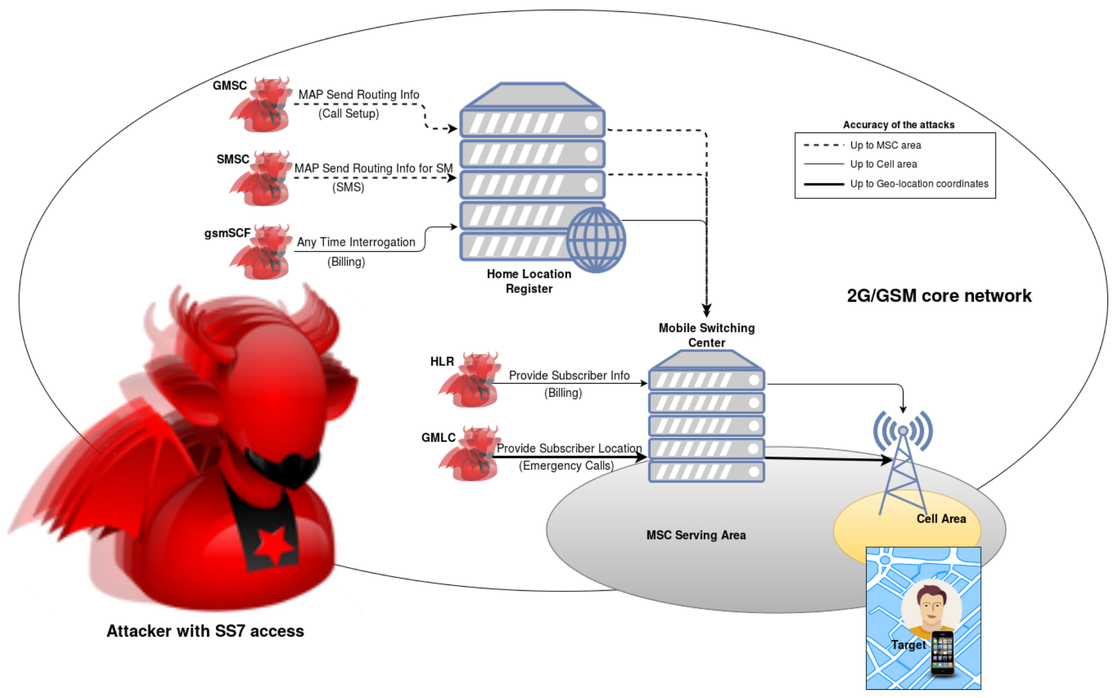

Figure 1: Impersonation of an SS7 attacker as different core network nodes to learn the location of the targeted cellphone user

- **Querying the Home Location Register (HLR):** By impersonating as Global MSC (GMSC) or Short Message Service Center (SMSC), an attacker can initiate either the call set up or SMS delivery procedures to query the HLR for the global title of the MSC and IMSI of the target. The MSC service area indicates the state or county in which the target is currently roaming. The attacker can also learn about the cell area of the target by misusing the billing platform related procedures.
- **Querying the Mobile Switching Center (MSC):** Once the IMSI and global title of the MSC is known, the attacker can query the MSC by impersonating as HLR to know the cell area of the target. It is also possible to misuse the emergency call procedures to track the target to the accuracy of his geographical coordinates.

Note: More details on the location tracking attacks can be found in our survey article [1].

Diameter Protocol

3GPP has standardized the use of Diameter in 4G/LTE core network communication to support mobility, IP Multimedia Subsystem (IMS) and to extend the functionalities of SS7 over an all-IP network. As a relatively new protocol, Diameter has a strong support for Authentication - Authorization - Accounting (AAA), encryption of communication traffic and mechanisms to hide the internal topology. However, the security and privacy considerations of Diameter fall short to guarantee the end-user from being tracked [2].

Exploiting the interoperability between SS7 and Diameter based core networks

Most mobile network operators upgrade their network from GSM to LTE gradually - to avoid service interruption and optimize the return on investment on the infrastructure. Due to this, the current interconnection network contains inhomogeneous set-up of nodes that support either SS7 or Diameter. For interoperability reasons with the partners, the edge nodes often have the ability to translate between Diameter and SS7 protocols, which is done using Interworking Functions (IWF). In such situations, the attacker can exploit the lack of security measures in the interconnections by tracking the location of an LTE cellphone user. Unlike the SS7 based attacks, here the attacker can gain more fine-grained information such as software version, IMEI number, the operating system of their devices along with location tracking up to the granularity of cell area.

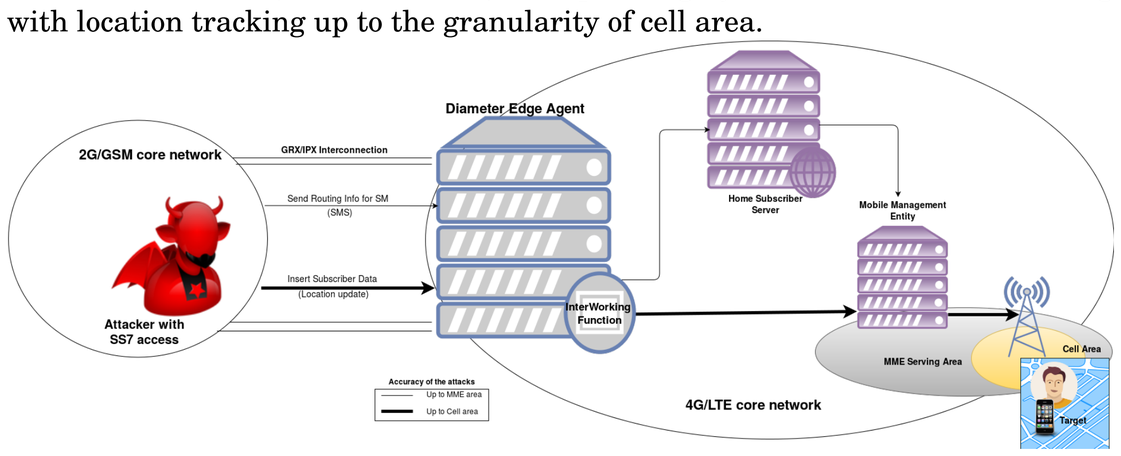

Figure 2: An attacker from SS7 core network can track the LTE user's location using Interworking Functionalities (IWF).

As shown in the figure 2, the IWF provides an easy way for an attacker to translate the SS7 based attacks into Diameter location tracking procedures.

Countermeasures

Deploying the combination of efficient filtering mechanisms and standardized security measures will protect the end user's location privacy against the attacks that exploit the signaling protocols.

- Effective SS7 filter/firewall to consider the contextual location of the users.
- Implementing NDS/IP security over the Diameter Edge Agents.
- Whitelisting the partners and the protocols used by them.
- Regular monitoring and logging of the signaling traffic.

It is important to note that these countermeasures has to be done solely from the mobile network operators and there is no way that an app or mechanism from end-user's side can detect or protect them from such attacks.

Publications

[1] S. P Rao, S. Holtmanns, I. Oliver, T. Aura, "We know where you are! - Utilising the telecom core network for user tracking," *The 8th International Conference on Cyber Conflict - Cycon 2016*. (To appear)

[2] S. Holtmanns, S. P Rao, I. Oliver, "User location tracking in LTE networking using the Interworking Functionality," *The 15th International IFIP TC6 Networking Conference, (NETWORKING 2016)*.

[3] S. P Rao, B. T Kotte, S. Holtmanns, "Privacy in LTE networks - Reviewing the security and privacy considerations in LTE networks", *The 9th EAI International Conference on Mobile Multimedia Communications*. (To appear)

Secure Systems Research Group
Department of Computer Science
School of Science, Aalto University, Finland

Contact information for comments & improvement ideas: Siddharth Rao
Email: siddharth.rao@aalto.fi