SS7 Discovery

SS7 is the primary protocol used by telephony devices to route circuit switched phone calls around the world. Simply put, it’s the protocol that nearly all of our phone calls are based upon. It’s a protocol that’s seen a great deal of success, after all, we can place phone calls around the world by simply dialing a number. If a link goes down, the circuit trunks are rerouted automatically and consumers rarely notice an issue has occurred.

Unfortunately, SS7 was not designed for security. The primary mechanism for protecting SS7 is the concept of a ‘walled garden’. This means that we’ll only allow trusted entities to connect to the network. Based on the widespread prevalence of telephony, we know we can no longer trust all of those that are connected to the SS7 network.

Watch the following talk from Tobias Engel <https://www.youtube.com/watch?v=-wu_pO5Z7Pk>

If you’d like to start with a less technical version, in addition to Engel’s, check this out the 60 Minutes version: <https://www.youtube.com/watch?v=O4tUx1W3zLc>

Once you’ve watched Engel’s talk, write a 500-word summary on how the SS7 protocol works.

Signaling System 7, or SS7, is the communications protocol suite used around the world by telecom network operators. Standardized in the 1980s, it was designed at a time when telecom operators, between state and corporate operations, were few. At the time land-lines were the extent of most communications and the telecom operators were able to secure these mediums amongst each other against outside/untrusted entities. The only weak point in this system is that anyone who has been authorized or has acquired access to the network has free reign. This was all possible at the time because the only people with access to the network were the network holders themselves. When mobile phones were released though, they were accompanied by a handful of new protocols, which still had no authentication. Surprisingly getting access to SS7 is laughably easy, being sold by telecom operators.

Once on the network, Information on any subscriber to any operator network can be collected through their cell. Given someone’s phone number, you can access all details of their current signals routing information which means you can pick up a lot of information from them. Common Examples are forwarding calls, tracking approximate geolocation (location of connecting towers). Eventually telecom providers started noticing this as a problem and began filtering traffic to mitigate attacks. Current attacks now require VLR/MSC and the IMSI which must be obtained through some other means.

The US requires that when someone calls 911 the caller must be located accurately (within 300 meters). Location services can use triangulation or request a Latitude and Longitude pair (some even return GPS positions). In order to access this information one must go through the Gateway Mobile Location Center (GMLC), which does require authentication. Unfortunately this authentication can be bypassed with some spoofing.

Through the CAMEL protocol for routing calls through mobile networks, if an attacker modifies information in in a switching center, he can forward calls from specific numbers to any other number (i.e. himself and then to a recording proxy before proceeding to the intended target of the call). This effectively places the attacker as a middle man, listening in on any call from their target. This is similar to the idea used with SMS interception and impersonation.

If you are in the area, close enough to scan for TMSI pages to specific cells, one can identify the IMSI and phone number of the corresponding TMSI.