

https://dspace.org/

Vulnerabilities of signaling system number 7 (SS7) to cyber attacks and how to mitigate against these vulnerabilities.

Kamwendo, Bob

2016
http://hdl.handle.net/10539/20048

Downloaded from a DSpace repository. https://dspace.org/

Abstract

As the mobile network subscriber base exponentially increases due to some attractive offerings such as anytime anywhere accessibility, seamless roaming, inexpensive handsets with sophisticated applications, and Internet connectivity, the mobile telecommunications network has now become the primary source of communication for not only business and pleasure, but also for the many life and mission critical services. This mass popularisation of telecommunications services has resulted in a heavily loaded Signaling System number 7 (SS7) signaling network which is used in Second and Third Generations (2G and 3G) mobile networks and is needed for call control and services such as caller identity, roaming, and for sending short message servirces. SS7 signaling has enjoyed remarkable popularity for providing acceptable voice quality with negligible connection delays, possibly due to its circuit-switched heritage. However, the traditional SS7 networks are expensive to lease and to expand, hence to cater for the growing signaling demand and to provide the seamless interconnectivity between the SS7 and IP networks a new suite of protocols known as Signaling Transport (SIGTRAN) has been designed to carry SS7 signaling messages over IP.

Due to the intersignaling between the circuit-switched and the packet-switched networks, the mobile networks have now left the "walled garden", which is a privileged, closed and isolated ecosystem under the full control of mobile carriers, using proprietary protocols and has minimal security risks due to restricted user access. Potentially, intersignaling can be exploited from the IP side to disrupt the services provided on the circuit-switched side.

This study demonstrates the vulnerabilities of SS7 messages to cyber-attacks while being transported over IP networks and proposes some solutions based on securing both the IP transport and SCTP layers of the SIGTRAN protocol stack.