



> ESD America

> web: esdoversight.com

> twitter: [@esdoversight](https://twitter.com/esdoversight)

ESD OVERSIGHT

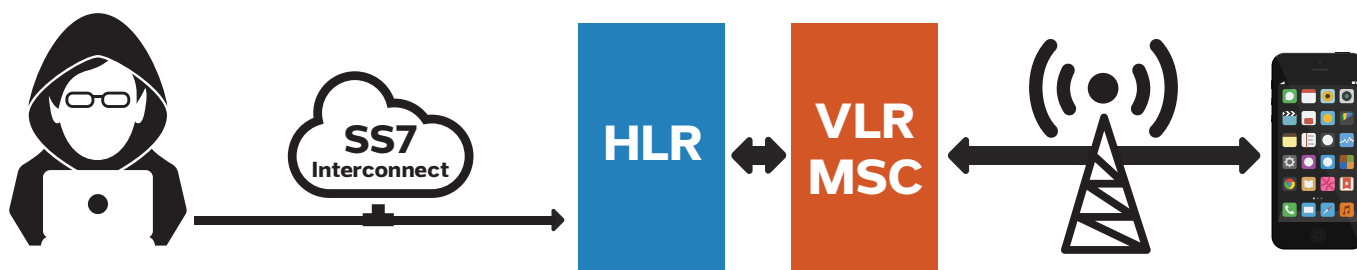
The first cellular network firewall

Our multi-year research has identified a number of severe vulnerabilities in the Signaling System #7 core infrastructure protocols for voice networks.

Our multi-year research has identified a number of severe vulnerabilities in the Signaling System #7 core infrastructure protocols for voice networks

Based on our research results, the SS7 core infrastructure can no longer be trusted, and advanced countermeasures are required to combat this potent threat.

- In cities, it is possible to track subscribers down to street level
- The same approach can also be used to retrieve IMEI and subscriber state
- Modification of subscriber data offers a vast opportunity for billing fraud
- Prepaid contract becomes postpaid, number barring (ODB) can be deleted
- USSD codes can be executed for other subscribers
- Re-routing of bank authentication SMS messages
- Remote interception of telephone calls
- SS7 allows decryption of 2G/GSM as well as 3G/UMTS calls
- Completely passive attack, no active IMSI catcher required



The Solution

To this end, we have two products that represent the world's first comprehensive solution against SS7 attacks: *ESD Oversight Protect* & *ESD Oversight Detect*. SS7 Network Penetration testing is also available to carriers around the world who recognise the need to ensure their networks and their subscribers are protected from the potential damaged these vulnerabilities expose.

Les Goldsmith
Chief Executive Officer
les@esdamerica.com



Trent Smith
Comsec Solutions Manager
trent@esdamerica.com