Anatomy of Commercial IMSI Catchers and Detectors

Shinjo Park
Technische Universität Berlin

Altaf Shaik
Technische Universität Berlin

Ravishankar Borgaonkar
SINTEF Digital

Jean-Pierre Seifert
Technische Universität Berlin

29th Crypto Day, 17/18 October 2019

IMSI catcher is a device to identify and track cellular phone subscribers, traced back to the 1990s with devices such as StingRay from Harris Corporation and GA 900 from Rohde & Schwarz. IMSI catchers threaten the privacy of mobile phone users by identifying and tracking them (Strobel (2007)). Commercial IMSI catcher products exploit vulnerabilities in cellular network security standards to lure nearby mobile devices. Commercial IMSI catcher's technical capabilities and operational details are still kept as a secret and unclearly presented due to the lack of access to these products from the research perspective.

On the other hand, there are several solutions to detect such IMSI catchers to protect the privacy of mobile subscribers. There are smartphone apps such as SnoopSnitch and AIMSICD, dedicated sensor network such as GSMK Overwatch, and network operator assisted method for detecting IMSI catcher activities. These IMSI catcher detectors mainly operate by gathering cellular information, analyzing them for anomalies and warning the user/operator about the presence of an IMSI catcher. However, detecting IMSI catchers effectively on commercial smartphones is still a challenge due to limited information provided by a smartphone and partial implementation of detection parameters.

In this talk, I present a systematic study of commercial IMSI catchers, based on publicly available product brochures and international patents. From these information, I present the technical capabilities and inner-workings of commercial IMSI cathcers and vulnerabilities exploited in cellular networks (2G, 3G, and 4G). Following this, I present a survey on IMSI catcher detection methodologies proposed by various research studies and commercial products. Finally, I provide insights that we believe help guide the development of more effective and efficient IMSI catcher detection techniques.

References

Daehyun Strobel (2007). IMSI-Catcher. *Seminararbeit Ruhr-Universität Bochum* .

crypto day matters 31 (2019)
Beiträge vom 31. Kryptotag, 17.-18.10.2019, Qualcomm, Berlin.
doi:10.18420/cdm-2019-31-23