Sicherheitsanalyse im Mobilfunkbereich

Studiengang: MAS | Vertiefung: MAS Information Technology

Kann mit Hilfe von Open Source Tools eine Sicherheitsanalyse im Mobilfunkbereich durchgeführt werden? Swisscom möchte eine Übersicht möglicher Tools, welche für interne Analysen genutzt werden können.

Ausgangslage

Die Swisscom betreibt das grösste Mobilfunk Netzwerk der Schweiz. Die Anforderungen der Kunden an die Verfügbarkeit und Leistungsfähigkeit der Netze steigt stetig. Deshalb baut und betreibt Swisscom Netze, die sich durch höchste Sicherheit, Verfügbarkeit und Leistungsfähigkeit auszeichnen.
Um die Sicherheit der Mobilfunkinfrastruktur zu gewährleisten, beauftragt die Swisscom regelmässig interne und externe Sicherheitsspezialisten die Infrastruktur auf Schwachstellen/Verwundbarkeiten zu prüfen. Da im Mobilfunkbereich viele proprietäre Protokolle und «Closed Source»-Lösungen verwendet werden, möchte Swisscom eine Übersicht möglicher Open Source Tools, welche für interne Sicherheitsanalysen genutzt werden könnten.

Zielsetzung

Im Rahmen der Master Thesis soll eine technische Sicherheitsanalyse der identifizierten Schwachstellen/Bedrohungen mithilfe von zu evaluierenden Open Source Tools durchgeführt werden.

Vorgehen

In der ersten Phase wurde mit der Durchführung eines «Threat Model» in den Bereichen «Radio Access», «Mobile Core» und «IP Multimedia Subsystem» eine Übersicht möglicher Bedrohungen erstellt. Basierend auf den gesammelten Informationen ist im Anschluss ein technischer, hauptsächlich sicherheitsbezogener, Anforderungskatalog erstellt worden. Dieser Katalog diente zur Evaluation der zu testenden Open Source Tools.
Als Vorbereitung für die technische Machbarkeitsprüfung der evaluierten Tools wurde mit Hilfe von Docker und einem «Universal Software Radio Peripheral» (Ettus USRP B210) eine Laborumgebung aufgebaut. Im darauffolgenden Arbeitsschritt wurde die Nutzung der Tools in einem explorativen Ansatz getestet.

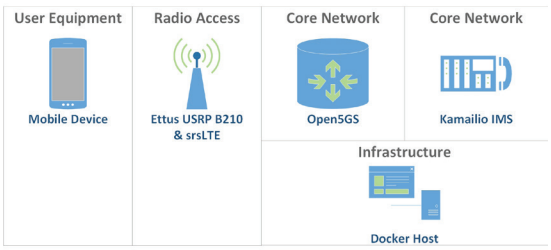
Resultat

Die identifizierten Bedrohungen wurden nach der STRIDE Methode in einem Katalog dokumentiert und dienten als Input für die Evaluation der Open Source Tools. Basierend auf dem Anforderungskatalog konnten über 100 verschiedene Tools und Projekte identifiziert werden. Für die Durchführung der technischen Sicherheitsanalyse wurde eine Mobilfunkinfrastruktur mit Open5GS, srsLTE und Kamailio IMS aufgebaut. Diese Container-basierte Umgebung ermöglicht ein flexibles Testing, welches das produktive Netzwerk und den Betrieb nicht stören oder negativ beeinträchtigen.

Fazit und Ausblick

Die erarbeiteten Resultate dieser Master Thesis ermöglichen die Durchführung interner Sicherheitsanalysen und -tests in einer Laborumgebung. Nach Abschluss der Master Thesis wird die Evaluation der Tools und Projekte sowie der Blueprint der Laborumgebung als Open Source Projekt auf GitHub veröffentlicht. Weitere Infos:
https://github.com/Lofmir/Mobile-Network-Security

Lukas Benninger



Schema Laborumgebung