Bachelor-Arbeit
Exposé

Raphael Brösamle

Institut für Informationssicherheit
Universität Stuttgart
Betreuer: Dr. Kay Schweiger

Das Internet ist ein immer größer werdender Bestandteil des Alltags. Ob zuhause oder unterwegs, eine schnelle und sichere Internetverbindung ist für viele Menschen wichtig. Dafür ist unter anderem das mobile Netz ausschlaggebend. Deshalb wird viel in den Ausbau des Netzes und in neue Technologien investiert. Vor allem die kommende 5G-Technologie spielt dabei eine große Rolle, da sie schnelles und wesentlich sichereres Internet verspricht. Aber ist die Internetverbindung durch die 5G-Technologie tatsächlich sicher?
Dies gilt es in dieser Bachelor-Arbeit herauszufinden. Dafür wird das 5G-AKA-Protokoll unter die Lupe genommen. Im Wesentlichen wird folgendes betrachtet:

- Es wird das 5G-AKA Protokoll beschrieben. Dafür werden die Ziele des Protokolls genannt und es wird dargestellt, wie das 5G-AKA-Protokoll funktioniert.

- Es werden die Unterschiede zwischen den Authentifizierungsmethoden von 5G und 4G aufgezeigt. Dabei werden die Ziele des 4G EPS-AKA-Protokolls genannt und die Verbesserungen des 5G-AKA-Protokolls im Vergleich zum EPS-AKA-Protokoll erklärt.

- Es wird eine bereits bekannte Sicherheitslücke in dem 5G-AKA-Protokoll genannt und beschrieben. Dabei handelt es sich um die Sicherheitslücke, die in *Security vulnerability in 5G-AKA draft*[1] von *Martin Dehnel-Wild and Cas Cremers* erklärt wurde. Des Weiteren wird noch erklärt welche Auswirkungen diese Lücke auf die Sicherheit des Protokolls hat.

- Diese Sicherheitslücke[1] wird implementiert, um dessen Praktikabilität herauszufinden. Die Authentifizierung soll dabei mit Hilfe der Sicherheitslücke umgangen werden.

Literatur

[1] Martin Dehnel-Wild and Cas Cremers. Security vulnerability in 5g-aka draft. *Department of Computer Science, University of Oxford, Tech. Rep*, 2018.