Inhaltsverzeichnis

1 Motivation **1**

2 Gesellschaftlicher Kontext **3**

2.1 Bedrohung durch private Akteure 3

2.2 Bedrohung durch staatliche Organisationen 3

2.3 Verhaltensänderung 4

2.4 Thematisierung in der Schule 5

3 Ziele **7**

3.1 Übersicht der Angriffsvektoren 7

4 Low Layer Angriffe **13**

4.1 Sicherheitsrisiko der GSM-Luftschnittstelle 13

4.1.1 GSM Architektur 14

4.1.2 Aufbau eines Anrufs 16

4.1.3 Sniffing: GSM-Verschlüsselung 19

4.1.4 Brechen von A5/1 21

4.1.5 Tracking 22

4.1.6 Zusammenhang mit der Silent-SMS 24

4.1.7 Man-in-the-middle: IMSI-Catcher 25

4.1.8 Schutzmaßnahmen: Erkennung und Visualisierung 30

4.2 Die Java Card - Risikofaktoren der SMS 42

4.2.1 Architektur einer SIM-Karte 43

4.2.2 Funktion der Java Card 44

4.2.3 Programmierung von Java-Karten 48

4.2.4 Funktion des Short Message Service 52

4.2.5 Kommunikation des Providers mit der SIM-Karte 61

4.2.6 Angriffsvektor Signatur 63

4.2.7 Konsequenzen eines Angriffs 66

4.2.8 Schutzmaßnahmen: Erkennung und Visualisierung 68

5 High Layer Angriffe 73
5.1 Definition Smartphone 73
5.2 Problematik proprietärer Software 73
5.2.1 Risiko von proprietären Chat-Protokollen 74
5.2.2 Risiko von proprietären Chat-Apps 74
5.2.3 Alternative Chat-Protokolle und Clients 76
5.2.4 Alternative Betriebssysteme 79
5.2.5 Schutzmaßnahmen 83

6 Schnittstellenübersicht eines Smartphones 85
6.1 Bluetooth 86
6.2 WLAN 88
6.3 Kamera 90
6.4 USB 90
6.5 GPS 92

7 Fazit 93

Literaturverzeichnis 95

Sachregister 98

http://www.springer.com/978-3-658-12611-7

Sicherheitsaspekte von Mobiltelefonen
Erkennung und Visualisierung von Angriffsvektoren
Gewald, P.
2016, XIII, 98 S. 53 Abb., Softcover
ISBN: 978-3-658-12611-7