Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

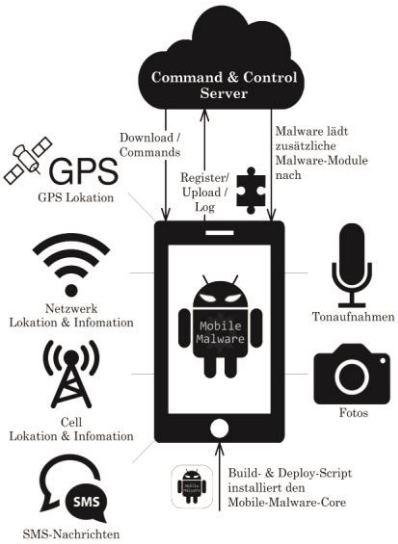
InIT Institut für angewandte
Informationstechnologie

Mobile Malware

Smartphones sind in der heutigen Gesellschaft nicht mehr wegzudenken – mit deren vielseitigen Möglichkeiten sind sie sowohl Teil des beruflichen wie auch des privaten Alltags. Die hohe Verbreitung dieser Geräte macht sie zu einem attraktiven Ziel für Cyberkriminelle. Dabei sind insbesondere Android-Geräte betroffen. Das zeigt sich insbesondere darin, dass über 95 % der mobilen Malware heutzutage für Android entwickelt wird, wobei zunehmend komplexere und ausgereiftere Varianten in Umlauf kommen. Damit man sich auch in Zukunft gegen solche Software verteidigen kann, braucht es gut ausgebildete Fachleute.
Ein Ansatz dafür ist das Lösen von Trainingsaufgaben, bei denen die Teilnehmer mit realistischen Szenarien konfrontiert werden. Ein Beispiel dafür sind die Hacking-Lab-Challenges, die in der Schweiz angeboten werden und sich mit Informationssicherheit befassen. Was jedoch bis jetzt fehlt, sind Szenarien im mobilen Umfeld, solche also, die sich mit Malware auf mobilen Systemen befassen. Um dieses Desiderat zu füllen, wird ein bereits bestehendes Framework des Hacking-Labs um eine Komponente für Android-Geräte ergänzt. Diese Komponente bildet die Basis für den Entwurf und die Integration sechs neuer Trainingsszenarien für den Bereich mobiler Malware im Hacking-Lab.
Die Grundlage für die Entwicklung der Malware und der Szenarien liefert eine Analyse des Verhaltens existierender Malware für Android sowie typischer Angriffsvektoren. Eine Herausforderung bei der Entwicklung ist die Implementierung einer Möglichkeit zum dynamischen Nachladen von Code zur Laufzeit. Dieses Feature sowie das modulare Design der Software ermöglichen eine grosse Flexibilität beim Entwerfen von den Trainingsszenarien.
Endprodukt dieser Bachelorarbeit ist eine voll funktionsfähige Malware, die sich bequem installieren und von einem Command-and-Control-Server aus steuern lässt. Sie erfüllt alle geforderten Funktionen, sodass die ausgearbeiteten Szenarien umgesetzt werden können. Sie ermöglicht unter anderem das Auslesen und Versenden von SMS-Nachrichten, das automatische Schiessen von Fotos sowie die Standortbestimmung über GPS-Koordinaten oder Mobilfunkantennen. Somit ist eine gute Basis für das künftige Training von Fachpersonen zum Thema mobiler Malware gelegt worden.

Diplomierende
Alessandro Monsorno
Moritz Zollinger

Dozent
Bernhard Tellenbach



Ein Android-Mobiltelefon, das mit der entwickelten Malware infiziert wurde, kann SMS-Nachrichten stehlen oder versenden. Weitere Funktionalität kann in Form von Modulen heruntergeladen werden. Dadurch ist es möglich, auf GPS-, Netzwerk- und Mobilfunk-Informationen zuzugreifen, um das Mobiltelefon zu orten. Ebenfalls können via Kamera und Mikrofon unbemerkt Fotos geschossen und Gespräche aufgezeichnet werden. Sämtliche Informationen werden auf einen Command-and-Control-Server übertragen und können dort jederzeit vom Angreifer eingesehen werden.