64313 Mobile Security

Lehrende/r	Mario Kubek	Modulbeauftragte/r	Mario Kubek

Dauer des Moduls	ECTS	Workload	Häufigkeit
ein Semester	10	300 Stunden	in jedem Semester

Lehrveranstaltung(en)		WS/SS	SWS
01864	Mobile Security		4+2

Detaillierter Zeitaufwand

Kurseinheiten: 150 Stunden
Übungsaufgaben: 75 Stunden
Prüfungsvorbereitung: 75 Stunden

Qualifikationsziele

Die Studierenden haben nach erfolgreicher Bearbeitung fundierte Kenntnisse zu den jeweiligen Sicherheitsarchitekturen und -mechanismen moderner, mobiler Betriebssysteme wie iOS und Android erlangt. Sie kennen typische Bedrohungen, Angriffsszenarien und Gegenmaßnahmen im Kontext mobiler Geräte, Applikationen und Datenübertragung. Die Studierenden sind zudem in der Lage, selbstständig mobile Applikationen auf Sicherheitsprobleme und Schadcode hin zu analysieren und sind mit dem dafür nötigen Vorgehen und gängigen Werkzeugen vertraut. Durch dieses Wissen können die Studierenden den Sicherheitsstatus ihrer Endgeräte und der darauf installierten Applikationen einschätzen und ihn selbst aktiv verbessern.

Inhalte

Der Kurs "Mobile Security" führt in die Sicherheitskonzepte und -mechanismen mobiler Endgeräte wie Smartphones und Tablets sowie der auf ihnen laufenden Betriebssysteme und Applikationen ein. Der Fokus dieser Betrachtungen liegt dabei auf den gängigen Betriebssystemen iOS und insbesondere Android. Konkret befasst sich der Kurs zunächst mit den allgemeinen Bedrohungen und Angriffsszenarien in diesem Kontext sowie den Sicherheitsarchitekturen obiger Plattformen und ihren Prinzipien als Gegenmaßnahmen. Der zweite Schwerpunkt ist den Sicherheitsproblemen und der Einführung in das Penetration Testing mobiler Applikationen gewidmet. Die dazu nötigen Techniken der statischen und dynamischen Analyse werden vorgestellt und voneinander abgegrenzt. In diesem Rahmen wird die Vorgehensweise beim Reversing von Android-Applikationen erklärt, wobei zu diesem Zweck auf ihre Beschaffung, ihre Analyse und die dafür nötigen technischen Umgebungen und Werkzeuge eingegangen wird. Weiterhin werden die wichtigsten Schwachstellen im Code mobiler Applikationen und deren Erkennung sowie die Detektion von Schadcode und gängige Schutzmaßnahmen behandelt. Ebenfalls werden verschiedene Ansätze forensischer Untersuchungen mobiler Endgeräte besprochen. Abschließend gibt der Kurs einen Überblick über eine Reihe von Angriffen auf die Datenübertragung und das dafür nötige Vorgehen.

Inhaltliche Voraussetzung

Modul 63512 "Sicherheit im Internet" (01866/01868)

Lehr- und Betreuungsformen

Kursmaterial

Einsendeaufgaben mit Korrektur und/oder Musterlösung

internetgestütztes Diskussionsforum

Zusatzmaterial

Betreuung und Beratung durch Lehrende

Anmerkung

Der Basistext muss vor Semesterbeginn beschafft werden. Basistext: M. Spreitzenbarth: Mobile Hacking: Ein kompakter Einstieg ins Penetration Testing mobiler Applikationen - iOS, Android und Windows Phone, 2017

Formale Voraussetzung

keine

Verwendung des Moduls	B.Sc. Informatik B.Sc. Mathematisch-technische Softwareentwicklung M.Sc. Informatik M.Sc. Praktische Informatik

Prüfungsformen	Art der Prüfungsleistung	Voraussetzung
Prüfung	bestandene benotete Prüfungsklausur	keine
Stellenwert der Note	1/8	