INF-MSc-340: Mobile Security				**BOSS-Nr.** 70990
Englischer Modultitel: Mobile Security				
Studiengänge: Masterstudiengang Informatik, Masterstudiengang Angewandte Informatik, Masterstudiengang Wirtschaftsinformatik				
Turnus: nach Ankündigung	**Dauer:** 1 Semester	**Studienabschnitt:** 2.–3. Semester	**Credits:** 6	**Aufwand:** 180 (60/120)

1 **Modulstruktur**

Nr.	Element / Lehrveranstaltung	Typ	Credits	SWS
1	Mobile Security	Vorlesung	4	2
2	Übung zu Mobile Security	Übung	2	2

2 **Lehrveranstaltungssprache:** englisch

3 **Lehrinhalte**

Diese Vorlesung befasst sich mit verschiedenen, grundlegenden Aspekten mobiler Betriebssysteme und der Anwendungssicherheit; mit einem Schwerpunkt auf dem beliebten Open-Source-Betriebssystem Android. Im Allgemeinen wird das Bewusstsein und Verständnis der Studierenden für Sicherheits- und Datenschutzprobleme in diesem Bereich erhöht. Die Studierenden lernen, aktuelle Sicherheits- und Datenschutzprobleme bei Smartphones aus der Perspektive der verschiedenen Akteure im Smartphone-Ökosystem anzugehen: Endnutzer, App-Entwickler, Systementwickler, und Drittparteien. Konkret werden in diesem Modul die folgenden Themen und Techniken vermittelt:

- Sicherheitskonzepte und Einführung in die Sicherheitsarchitektur von Android
- Zugriffskontrolle und Berechtigungen
- Rolle von Binder IPC in der Sicherheitsarchitektur
- Mandatory Access Control
- Kompartmentalisierung
- TLS und WebViews
- Sicherheitserweiterungen der Anwendungsschicht
- Spezielle Arten des Phishing
- Hardware-basierte Sicherheit der mobilen Plattform

4 **Kompetenzen**

Nach Abschluss der Veranstaltung sind die Studierenden in der Lage

- Bedrohungsmodelle aus der Perspektive verschiedener Akteure zu analysieren und einzuordnen,
- Die grundlegenden Entwurfsmuster sicherer Systeme sowie bewährte Sicherheitspraktiken zu erkennen und deren Umsetzung in Smartphone-Betriebssystemen zu bewerten,
- Die Integration von Hardware-Sicherheitsmechanismen wie Trusted Execution Environments (TEE) und Konzepten des Trusted Computings in moderne Systemdesigns zu erklären und kritisch zu hinterfragen,
- Techniken zur Stärkung der Privatsphäre von Endnutzern zu analysieren und deren Wirksamkeit sowie Benutzbarkeit kritisch zu bewerten.

5 **Prüfungen**

- Modulprüfung: Klausur (90 - 120 Minuten) oder mündliche Prüfung (30 Minuten). BOSS-NR. 70999
- Studienleistung: Halbzeitklausur nach Ankündigung der Veranstaltenden. BOSS-Nr. 70949

Die Studienleistung ist Voraussetzung für die Teilnahme an der Modulprüfung. Details werden zu Beginn der Veranstaltungen bekannt gegeben.

6 **Prüfungsformen und -leistungen**

[x] Modulprüfungen [ ] Teilleistung

7	**Teilnahmevoraussetzungen** • Erfolgreich abgeschlossen: -keine- • Vorausgesetzte Kenntnisse: Basiswissen in Betriebssystemen und der Programmierung in Java.		
8	**Modultyp und Verwendbarkeit des Moduls** • Wahlpflichtmodul im Masterstudiengang Wirtschaftsinformatik • Vertiefungsmodul in den Masterstudiengängen Informatik und Angewandte Informatik • Forschungsbereich: Software, Sicherheit und Verifikation		
9	**Modulbeauftragte/r** Prof. Dr. C. Rossow und Dr. S. Bugiel	**Zuständige Fakultät:** Informatik	**Beschluss Fakultätsrat:** 03.09.2025