



RISIKEN VON ANDROID APPS EINSCHÄTZEN

PENTESTING MOBILE APPLICATIONS

Die Herausforderung: Android-Anwendungen statisch und dynamisch analysieren. Mehr und mehr Unternehmen setzen für sicherheitskritische Aufgaben Apps ein. Von diesen gehen aber zunehmend größere Gefahren aus. Dieses Seminar hilft Ihnen dabei, Risikopotenziale zu erkennen und abzuwehren. Erlernen Sie verschiedene Techniken anhand von Praxisbeispielen, die Ihnen die Funktionalität sowie Sicherheitsprobleme aufzeigen. Sie profitieren sowohl von statischen als auch dynamischen Analyseverfahren und deren Anwendungstools.

Inhalte des Seminars

Bestandteile einer Android App

- Welche Bestandteile sind für die Analyse wichtig, und wie kann man diese (tool-unterstützt) untersuchen?

Sicherheitsmodell Android

- Welche Eigenschaften des Android OS helfen bei der Analyse und machen im Ganzen sicher?

Typische Probleme von Android Apps

- Wie sehen Fehler in Apps aus?
- Einzelne Probleme im Detail, kategorisiert anhand der OWASP Mobile Top 10

Analysetechniken

- Welche statischen und dynamischen Techniken sind prinzipiell möglich?
- Wo liegen die Grenzen einzelner Verfahren?

Umgang mit ausgewählten Tools anhand von Beispielen

- APKTool
- ARM Disassembler
- Frida
- mitmproxy

Ihr Nutzen

- » Nach dem Seminar können Sie Risiken von Android Apps einschätzen.
- » Sie können Schwachstellen analysieren und aktuelle Gefahren von Android Apps aufzeigen.
- » Sie verstehen unterschiedliche Analyseverfahren und können diese gezielt nach Anwendungsfall einsetzen.

INFORMATIONEN IM ÜBERBLICK

- Grundkenntnisse Programmierung Java/C++, Basiswissen Android Anwendungen (Komponenten, manifest, Permission)

- Architekten/innen, Entwickler/innen sowie Pentester/innen von eingebetteten Systemen

- 1 Tag Präsenz

- 600,-

- Garching bei München, inhouse

Veranstaltet durch



Referent:



Dr. Dennis Titze,
wiss. Mitarbeiter
Fraunhofer AISEC



Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/pentesting-mobile-applications