JOHANNES KEPLER UNIVERSITY LINZ | JKU

Univ.-Prof. Dr. Alois FERSCHA
Fachbereich Informatik

Altenberger Straße 69
A-4040 Linz
Tel.: +43 (732) 2468 4762
Fax: +43 (732) 2468 4765

fercha@pervasive.jku.at
http://www.pervasive.jku.at

Univ.-Doz.in DI Dr.in Ingrid Schaumüller-Bichl

Department Sichere Informationssysteme

FH OÖ Fakultät für Informatik, Kommunikation und Medien, Hagenberg

Risikoanalyse für PUFs und PUF-basierte Anwendungen

Die Analyse und Bewertung von Risiken stellt die Basis für alle nachfolgenden Schritte in der Erstellung und Umsetzung von Sicherheitskonzepten dar. Nicht zuletzt aufgrund der zunehmenden Komplexität moderner Informationssysteme erlangt das Thema Risikoanalyse – nach Jahren, in denen man eher den pragmatischen Ansatz von Standardsicherheitsmaßnahmen vorgezogen hat – zunehmende Bedeutung. Verstärkt wird dieser Ansatz durch gesetzliche und regulatorische Anforderungen.

Der Vortrag gibt zunächst einen Überblick über das Big Picture im Bereich Risikoanalyse – von spezifischen Verfahren über das betriebliche Umfeld bis zum Schutz Kritischer Infrastrukturen.

Als aktuelles Beispiel für die Entwicklung spezifischer Risikoanalysemethoden werden die Arbeiten zur Analyse von PUFs und PUF-basierten Anwendungen im Rahmen eines laufenden Forschungsprojektes vorgestellt. PUFs (Physically Uncloneable Functions) gelten aufgrund ihrer Eigenschaften als interessanter neuer Lösungsansatz für eine Reihe von Sicherheitsanwendungen. Diese reichen von gegenseitiger Authentisierung über fälschungssichere elektronische Identitäten und DRM bis zur sicheren Generierung kryptographischer Schlüssel. Einsatzgebiete für PUFs werden insbesondere im industriellen Bereich (Elektronik-, Flugzeug- und Automobilindustrie,...) gesehen, aber auch Anwendungen im High-Security-Bereich werden diskutiert.

Der Vortrag zeigt die besonderen Herausforderungen im Bereich Risikoanalyse für PUFs und PUF-basierte Anwendungen und erste Lösungsansätze auf. Die Ergebnisse der RA-Methodik sollen in weiterer Folge in die Entwicklung von Protection Profiles und Security Targets nach Common Criteria einfließen.

Zeit: Donnerstag, 7. Februar 2013, 08:00 Uhr

Ort: Johannes Kepler Universität Linz
Informatik-Gebäude, SCP 3, HS 19

Kurzbiographie

Univ.-Doz.in DI Dr.in Ingrid Schaumüller-Bichl studierte Technische Mathematik an der Johannes Kepler Universität Linz und promovierte 1982 als erste Frau an der Linzer Universität sub auspiciis präsidentis. 1992 Habilitation im Fach "Angewandte Informatik" an der Universität Klagenfurt. Seit 2006 ist sie Professorin an der FH OÖ, Fakultät für Informatik, Kommunikation und Medien in Hagenberg im Bereich Sichere Informationssysteme. Dr.in Schaumüller-Bichl ist Mitautorin des Österreichischen Informationssicherheitshandbuches, Mitglied der ENISA (European Network and Information Security Agency) WGs on Risk Management sowie der ÖNORM. Weiters Lehrbeauftragte an den Universitäten Linz, Klagenfurt und Krems, Vizepräsidentin der OCG und österreichische Repräsentantin in IFIP TC11 sowie stellvertretende Vorsitzende des Rates für Forschung und Technologie für Oberösterreich (RFT OÖ).