EINLADUNG

Young Researchers' Day trifft IKT-Sicherheitskonferenz

Der Young Researchers' Day ist eine gemeinsame Veranstaltung des ACM SIGSAC Chapters Vienna und des OCG-Arbeitskreises *IT-Sicherheit*. Der nächste Young Researchers' Day findet im Rahmen der IKT-Sicherheitskonferenz in St. Pölten statt. Ingrid Schaumüller-Bichl, FH Oberösterreich, und Edgar Weippl, SBA Research, laden ganz herzlich zum **Young Researchers' Day trifft IKT-Sicherheitskonferenz** ein.

Als Grundgedanke hinter diesem Event steht der Wunsch, dass jede österreichische Institution, die einen Security-Lehrgang bzw. Lehrschwerpunkt anbietet, ihren besten Studierenden die Möglichkeit gibt, die eigenen Arbeiten vorzutragen und so eine „Nachwuchsvernetzung" zu fördern.

Mittwoch, 04. November 2015, 14.00 – 17.00 Uhr
FH St. Pölten, Audimax

Programm:

14.00-14.10	Begrüßung
14.10-14.40	Forschungsbedarf & Berufsmöglichkeiten des Österreichischen Bundesheers AbwA ObstdG Mag. Walter Unger (BMLVS)
14.40-15.10	Static Analysis of Cryptography in Mobile Applications Johannes Feichtner (IAIK TU Graz)
15.10-15.40	Copri, Factoring RSA public keys Martin Wind (FH Joanneum)
15.40-16.10	Pause
16.10-16.40	Smart Meter Intrusion Detection System Matthias Schrattenholzer (FH St. Pölten)
16.40-17.10	Improving the forensic process (Senior Researcher Vortrag) Martin Schmiedecker (SBA Research)
18.00-20.00	Networking Lounge *gemeinsam mit der IKT-Sicherheitskonferenz / Networking Lounge gehostet durch Land NÖ*

Wir freuen uns auf einen spannenden **Young Researcher's Day!**

Ingrid Schaumüller-Bichl
FH Oberösterreich

Edgar Weippl
SBA Research

Anmeldung unter: https://www.sba-research.org/events/young-researchers-day-trifft-ikt-sicherheitskonferenz/

Static Analysis of Cryptography in Mobile Applications
Johannes Feichtner (IAIK TU Graz)

As mobile platforms enjoy great popularity, software vendors use mobile devices also to deploy applications which process sensitive data. Unfortunately, they often provide only little details on how responsibly critical information, such as passwords and encryption keys, are protected. Users can hardly be sure whether programs handle entered credentials accordingly. A wrong application of cryptography or security-critical APIs, however, may expose secrets to unrelated parties and, thereby, undermine the intended security level.

In this talk, we first present our approaches to assess the implementation of sensitive functionality in Android and iOS applications by means of static program analysis. Secondly, we introduce our inspection framework, named CryptoSlice, targeted to automatically identify and analyze security-related code in Android applications. Having applied our tool on a set of real-world programs, we finally provide a practical insight into the prevalence of security-critical misconceptions.

Copri, Factoring RSA public keys
Martin Wind (FH Joanneum)

This talk aims at presenting an efficient implementation to factorize large sets of RSA public keys into coprimes. To achieve nearly linearithmic runtime, the algorithm "Factoring into coprimes in essentially linear time" - as described by Daniel J. Bernstein - is modified to fit a cluster environment. Furthermore, a subset of all used TLS RSA public keys, aggregated by a recent network scan of the IPv4 address space, was analyzed to show weaknesses in currently used RSA keys.

Finally, possible reasons of weak keys and recommendations to generate secure public keys are discussed.

Smart Meter Intrusion Detection System
Matthias Schrattenholzer (FH St. Pölten)

Durch die Richtlinie der EU von 2006 über die Einführung von intelligenten Messgeräten steht die Energiewirtschaft bei der Zählertechnik vor einem großen Wechsel. Die Vernetzung der Messtechnik bringt neue Herausforderungen an die IT Systeme der Energieanbieter mit sich. Um diesen Herausforderungen gerecht zu werden, werden neue Methoden und Anwendungsmöglichkeiten gesucht, um abseits von konventionellen Intrusion Detection Systemen, die richtigen Maßnahmen zur Gewährleistung eines sicheren Betriebes zu ermöglichen.
Die Entwicklung einer Proof-of-Concept Implementierung, die Informationen von verschiedenen Schichten zusammenführt und analysiert sowie Regeln für den korrekten Ablauf von Aktionen beschreibt, ist eines der Ergebnisse dieses Projektes. In einer realen Umgebung beim Projektpartner kann die Implementierung in einem Pilotprojekt getestet werden.

Improving the forensic process (Senior Researcher Vortrag)
Martin Schmiedecker (SBA Research)

The forensic process as used today has severe problems: massive amounts of data to be analysed, semi-manual analysis steps and many heterogenous devices in use, even for single persons.
This talk will give an overview on different approaches that have been proposed recently to mitigate these issues, including fully automatic data extraction & analysis steps, and moving from a single-threaded tool chain to fleet forensics.