Einladung zum

4th Young Researcher's Day 2014

Nach drei erfolgreichen Young Researcher‘s Days starten wir im neuen Jahr in Runde vier.
Frau Ingrid Schaumüller-Bichl und Herr Edgar Weippl laden ganz herzlich zum **4th Young Researcher's Day** ein, der im Rahmen des ACM SIGSAC Chapters Vienna und des OCG-Arbeitskreises *IT-Sicherheit* am

Donnerstag, 23.01.2014 von 14:00 – 17:30 Uhr

stattfinden wird.

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.

Programm:

14:00-14:10	Begrüßung Ingrid Schaumüller-Bichl (FH OÖ, Campus Hagenberg), Edgar Weippl (TU Wien, SBA Research)
14:10-14:40	*Hardware-Software-Codesign of Side-Channel Evaluated Identity-based Encryption* Thomas Unterluggauer (IAIK TU Graz)
14:40-15:10	*Cloudoscopy: services discovery and topology mapping* Johanna Ullrich (TU Wien)
15:10-15:40	*Syntaktische Definition von Malware Verhalten* Hermann Dornhackl (FH St. Pölten)
15:40-16:00	Pause
16:00-16:30	*Praxistaugliche Kommunikationssicherheit in einer Smart Metering Infrastruktur* Christian Peuker (FH Salzburg)
16:30-17:00	*Communication Schemes for Proces Execution Histories to Enforce Entailment Constraints in Process-Driven SOAs* Thomas Quirchmayr (WU Wien)
17:00-17:30	*Towards a Privacy-Preserving Federated Identity as a Service Model* Bernd Zwattendorfer (IAIK TU Graz)
17:30	Ausklang

Der Young Researcher's Day findet in den Räumen der OCG statt (Wollzeile 1, 1010 Wien). Wir ersuchen um eine Anmeldung bis zum 21.01.2014 an Yvonne Poul (ypoul@sba-research.org).

Wir freuen uns über Ihr Kommen und auf einen spannenden **4th Young Researcher's Day 2014!**

Ingrid Schaumüller-Bichl
FH OÖ, Campus Hagenberg

Edgar Weippl
SBA Research

fh OBERÖSTERREICH

OESTERREICHISCHE COMPUTER GESELLSCHAFT
AUSTRIAN COMPUTER SOCIETY

acm Chapter

secure
sba-research.org

Hardware-Software-Codesign of Side-Channel Evaluated Identity-based Encryption

Thomas Unterluggauer (IAIK TU Graz)

Providing sufficient security to embedded applications has become increasingly important. The schemes being used rely on the presence of a key for encryption. Contrary to this approach, the promising concept of identity-based encryption (IBE) enables the encryption of data by just knowing the recipient's identity, avoiding the key exchange problem. This talk discusses identity-based encryption for embedded platforms. Besides computational speed and low resource optimizations for embedded applications, it also focuses on security against side-channel attacks.

Cloudoscopy: services discovery and topology mapping

Johanna Ullrich (TU Wien)

We define and study cloudoscopy, i.e., exposing sensitive information about the location of (victim) cloud services and/or about the internal organisation of the cloud network, in spite of location-hiding efforts by cloud providers. A typical cloudoscopy attack is composed of a number of steps: first expose the internal IP address of a victim instance, then measure its hop-count distance from adversarial cloud instances, and finally test to find a specific instance which is close enough to the victim (e.g., co-resident) to allow (denial of service or side-channel) attacks. We refer to the three steps/modules involved in such cloudoscopy attack by the terms IP address deanonymisation, hop-count measuring, and co-residence testing.

We present specific methods for these three cloudoscopy modules, and report on results of our experimental validation on popular cloud platform providers. Our techniques can be used for attacking (victim) servers, as well as for benign goals, e.g., optimisation of instances placement and communication, or comparing clouds and validating cloud-provider placement guarantees.

Syntaktische Definition von Malware Verhalten

Hermann Dornhackl (FH St. Pölten)

Es wird die Anwendung formaler Methoden zur Modellierung von Malware Verhalten beschrieben. Die Modellierung des Verhaltens erfolgt dabei über syntaktische Strukuren, die bösartiges Verhalten in Execution Traces von Malware abbilden. Dieses bösartige Verhalten wird durch eine formale Grammatik beschrieben, die als Terminalsymbole die API calls enthält; Nicht-Terminale repräsentieren Sequenzen von API calls, die jeweils bestimmte (Teil-)Ziele der Malware beschreiben. Die Kombination verschiedener Nicht-Terminale in sequentiellen und hierarchischen Strukturen ergeben Angriffsvektoren, die von bösartiger Software verwendet werden. Ausgehend von diesen durch die Grammatik definierten syntaktischen Strukturen kann ein Parser generiert werden, mit dessen Hilfe in den Execution Traces einer verdächtigen Software nach bösartigen Verhaltensmustern gesucht werden kann.

Praxistaugliche Kommunikationssicherheit in einer Smart Metering Infrastruktur

Christian Peuker (FH Salzburg)

In today's life the usage of renewable resources for energy production are gaining more and more importance. Reasons are limited fossil fuels as well an increasing will to combat climate change. Based on the European Union's „20-20-20“ climate and energy targets an ambitious roadmap was created to change the existing traditional power grids into future energy networks.

As a first step it is necessary to verify the security and privacy challenges of a smart metering infrastructure and to find solutions how they should be met. The talk is focused on a smart metering gateway and its security relevant demands based on the BSI protection profile. Based on this profile a prototype of a smart metering gateway based on open standards and protocols has been developed. The existing prototype fulfils the majority of the requirements of the protection profile while keeping costs at a minimum.

Communication Schemes for Proces Execution Histories to Enforce Entailment Constraints in Process-Driven SOAs

Thomas Quirchmayr (WU Wien)

A distributed business process is executed in a distributed computing environment. In this context, the service-oriented architecture (SOA) paradigm provides a mature and well understood framework for the integration of software services. Entailment constraints, such as mutual exclusion or binding constraints, are an important means to specify and enforce business processes in a SOA.

Process engines control the process flow and are responsible for the coordination of the services that participate in a distributed business process. Since the enforcement of entailment constraints requires knowledge of the subjects or roles who executed particular task instances, we need to communicate the execution history of the respective tasks and processes between the services and the process engines. However, the inherent concurrency of a distributed system may lead to omission failures. Such failures may impair the enforcement of entailment constraints in a process-driven SOA. In particular, the impact of these failures as well as the corresponding countermeasures depend on the architecture of the respective process engine.

We discuss communication schemes for (distributed) process execution histories in a SOA. In particular, we provide generic procedures for different communication schemes and examine the efficiency of these schemes as well as their characteristics if omission failures occur.

In this context, we especially consider if the respective process engine acts as an orchestration engine or as a choreography engine.

Towards a Privacy-Preserving Federated Identity as a Service Model

Bernd Zwattendorfer (IAIK TU Graz)

Identity management plays a key role in e-Government. Giving the increasing number of cloud applications, also in the field of e-Government, identity management is also vital in the area of cloud computing. Several cloud identity models have already emerged, whereas the so-called "Identity as a Service"-model seems to be the most promising one. Cloud service providers currently implement this model by relying on a central identity broker, acting as a hub between different service and identity providers. While the identity broker model has a couple of advantages, still some disadvantages can be identified. One major drawback of the central identity broker model is that both the user and the service provider must rely on one and the same identity broker for identification and authentication. This heavily decreases flexibility and hinders freedom of choice for selecting other identity broker implementations. We by-pass this issue by proposing a federated identity as a service model, where identity brokers are interconnected. This federated identity as a service model retains the benefits but eliminates the drawbacks of the central cloud identity broker model.