Einladung zum

1st Young Researcher's Day 2012

Frau Ingrid Schaumüller-Bichl und Herr Edgar Weippl laden ganz herzlich zum **1st Young Researcher's Day** ein, der im Rahmen des OCG-Arbeitskreises *IT-Sicherheit* am 01.03.2012 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.

Es erwartet Sie folgendes Programm:

Uhrzeit	Vortragender	Institution	Titel
13:00	Begrüßung		
13:10-13:40	Stefan Kölbl	IAIK Graz	Cryptanalysis of a SHA-3 Candidate
13:40-14:10	Hubert Eigner	FH Campus Wien	Token-based authentication for Smartphones
14:10-14:40	Michael Oggolder Eva Freihofner Christoph Meinhart	FH Hagenberg	The principal-agent problem in the context of cross-company business processes
14:40-15:10	Marion Marschalek	FH St. Pölten	Dynamic Malware Analysis: Automated Classification of unknown Executables using Data Mining Algorithms
15:10-15:50	Pause		
15:50-16:20	Christian Praher	Uni Linz	Working Set Based Model for Approximation of Least User Access
16:20-16:50	Martin Mulazzani	TU Wien	Reliable Browser Fingerprinting
16:50-17:20	Anne Baumgraß	WU Wien	Bridging the Gap between Mining and Engineering of RBAC Models
17:20	Ausklang		

Der Young Researcher's Day findet in den Räumen der OCG statt (Dampfschiffstraße 4, 1030 Wien).

Wir ersuchen um eine Anmeldung bis zum 27.02.2012 an Yvonne Poul (ypoul@sba-research.org).

Wir freuen uns über Ihr Kommen und auf einen erfolgreichen **1st Young Researcher's Day 2012!**

Ingrid Schaumüller-Bichl
FH Hagenberg

Edgar Weippl
SBA Research

secure sba-research.org

FH OBERÖSTERREICH

OESTERREICHISCHE COMPUTER GESELLSCHAFT
AUSTRIAN COMPUTER SOCIETY

Cryptanalysis of a SHA-3 Candidate

Stefan Kölbl - IAIK TU Graz

Abstract:

Cryptographic hash functions are a versatile and essential building block for security applications. They map an input of arbitrary length to a short fixed size output. Hash functions have a broad range of practical applications and are used for message integrity, storing passwords, random number generation or message authentication codes. In the last few years, the cryptanalysis of hash functions has made a huge leap forward. Weaknesses have been found for many hash functions widely used. MD5 is completely broken and the SHA-1 standard is not considered to be secure anymore. In 2007, NIST launched a public competition to select a new hash algorithm as a future SHA-3. From 64 submissions, five finalists are left to become the new standard in 2012.

In this master thesis, the finalist Keccak is analyzed regarding its security. Different cryptanalysis methods are applied to find possible weaknesses of round-reduced versions.

Token-based authentication for Smartphones

Hubert Eigner – FH Campus Wien

Abstract:

Secure authentication techniques available on modern smartphones often suffer from the problem of lacking usability. Password authentication for example is able to prevent unauthorized access, but on the other hand it requires a time consuming action each time the device is unlocked. Due to short but frequent sessions of smartphone usage, usability of authentication mechanisms has a big impact on the user acceptance.

This work should provide a user-friendly alternative to these authentication methods, which can be realized on current smartphones. The mechanism described uses a hardware-token to authenticate the user. If the token is within range of the smartphone, the user will have no additional effort to unlock the mobile device. If the token is out of range, the user has to provide a password to authenticate. The mechanism is based on an authentication protocol, which meets the requirements on energy efficiency and limited resources by optimizing the communication effort as well as using a hash based challenge-response technique.

A prototype was implemented on an Android Smartphone and a MSP430 based MCU. As Bluetooth was the most appropriate choice out of the available technologies, it was chosen for communication. It was possible to implement the service on smartphone side by using only the official API functions. The token allows fast authentication without a need of additional user action but an extra piece of hardware has to be carried by the user. The prototype proved that secure and user-friendly authentication methods can be implemented on currently available hardware.

The principal-agent problem in the context of cross-company business processes

Michael Oggolder, Eva Freihofner, Christoph Meinhart – FH Hagenberg

Abstract:

The so-called principal-agent problem occurs when trust boundaries are exceeded. In a principal-agent situation the principal is the party that assigns the other party (the agent) to act on their behalf.

The cause of the principal-agent problem lies in the conflict of interest of the parties involved. If the agent is able to act autonomously, the agent might act to their own advantage instead of the principal's. A principal-agent problem exists if this risk cannot be entirely compensated for.

A further aspect is the information asymmetry, which makes it more difficult to control the agent. To mitigate the principal-agent problem preventive and reactive controls can be applied, which counteract the different causes of the problem.
In praxis, these controls are most interesting concerning cross-company business processes, since the principal-agent problem occurs there frequently.

Dynamic Malware Analysis

Automated Classification of unknown Executables using Data Mining Algorithms

Marion Marschalek – FH St. Pölten

Abstract:

This paper proposes a method, which allows automated validation of unknown software based on behavioral structures. The automatic classification was accomplished by application of Data Mining algorithms.

For training and testing of classification techniques 1100 samples were used, retrieved from a relational database of behavior-based software analysis. This papers objective was the evaluation of a fast and simple approach of automated appraisal of the given dataset. Assuming the two classes Virus='yes' and Virus='no' the classification was performed, depending on the behavior of a given sample.

The data was split into categories of behavior and each category was subject of an analysis. Named categories summed the activities concerning Files, Registry Keys, Registry Values, Processes, Services, loaded DLLs and Network Communication. The data was analyzed with single-instance algorithms, relating to the single activities of the samples. Furthermore multi-instance methods were applied to focus on the samples as a whole.
Best results were achieved using the multi-instance techniques, especially on the dataset of loaded DLLs per sample. Generally the output of multi-instance methods was of higher quality. A significant problem during analysis phase was the data composition. Number and expressiveness of harmless samples were too low. Therefor the categories Registry Key, Processes, Services and Network Communication were not suitable for automated analysis by Data Mining techniques.

Working Set Based Model for Approximation of Least User Access

Christian Praher – JKU Linz

Abstract:

Amongst others the "Principle of Least Privilege PoLP" is one of the major design goals of modern access control systems. PoLP states that a user should have activated only those permissions that are needed to complete the current task/job.
Contemporary access control models like e.g. Role Based Access Control (RBAC) and Domain and Type Enforcement (DTE) already incorporate mechanisms to enforce least privilege. However in practice this principle is very hard to achieve as it either requires extensive user participation and/or highly complex and tight security policies.

We propose a novel model for operating system access control that continuously monitors the users past access control usage and automatically creates least privilege "working sets". In the style of virtual memory systems, our working sets are a dynamic concept that go along with the current access control usage of a user. The contents of these working sets are "application roles" that characterize the most important resource usages of an application, like e.g. opened handles, imported DLLs or network activity. Working sets are created at the granularity level of sessions and first evaluations of real world user data have shown that already after only a small number of learning sessions our model should be able to considerably limit the otherwise unrestricted permission space of user logon session.

Reliable Browser Fingerprinting

Martin Mulazzani – TU Wien

Abstract:

With the web browser becoming more and more important, the reliable detection if a client is using a specific browser is still hard. So far the UserAgent is used, which is a self-reported string provided by the client. It is not a security feature, and can be changed arbitrarily.

In this paper we propose a new method for identifying web browsers, based on the underlying Javascript engine. We instrument a Javascript conformance test, test262, with more than 10,000 test cases to calculate the minimal fingerprint for each browser. We collected data for more than 150 browser and operating system combinations, and present algorithms to calculate a minimal fingerprint for each of a given set of browser. Our method is up to 3 orders of magnitude faster than previous work, and can be implemented in just a few lines of Javascript. We evaluate the feasibility of our method with a survey, and discuss the consequences for user privacy and security. In the future, this technique could be used to enhance state of the art session management, as session hijacking can be made considerably harder.

Bridging the Gap between Mining and Engineering of RBAC Models

Anne Baumgraß – WU Wien

Abstract:

In information systems and organizations permissions need to be tailored, both to allow legitimate users to perform their specific tasks and to avoid fraud and abuse. Role-based access control (RBAC) is a de facto standard to model and specify access control policies.

Mining approaches, such as role mining or organizational mining, can be applied to derive RBAC models from a system's configuration or from log files that result from executing the usual business processes. Mining techniques document the current state of a system and produce current-state RBAC models. However, current-state RBAC models mostly follow from structures that have evolved over time and are not the result of a systematic rights management procedure. In contrast, role engineering models are applied to define a tailored RBAC model for a certain organization or information system. They produce a target-state RBAC model that is customized for the business processes which are supported via the respective information system. The migration from a current-state RBAC model to a tailored target-state RBAC model is, however, a non-trivial task.

This talk presents approaches to derive current-state RBAC models and facilitate the definition of target-state RBAC models. On this basis, a systematic approach to migrate current-state RBAC models to target-state RBAC models is presented.