Einladung zum

3rd Young Researcher's Day 2013

Nach zwei erfolgreichen Young Researcher's Days starten wir kurz vor dem Sommer in Runde drei.
Frau Ingrid Schaumüller-Bichl und Herr Edgar Weippl laden ganz herzlich zum **3rd Young Researcher's Day** ein, der im Rahmen des ACM SIGSAC Chapters Vienna und des OCG-Arbeitskreises *IT-Sicherheit* am

25.06.2013 von 09.30 – 12.30 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:

09:30-09:40	Begrüßung Ingrid Schaumüller-Bichl (FH Hagenberg), Edgar Weippl (TU Wien, SBA Research)
09:40-10:10	*Structural Definition of Malware Behavior* Robert Luh (FH St. Pölten)
10:10-10:40	*Covert Computation - Hiding Code in Code for Obfuscation Purposes* Sebastian Schrittwieser (TU Wien)
10:40-11:10	*Scenario-driven Testing of Security-related Domain-specific Language Models* Bernhard Hoisl (WU Wien)
11:10-11:30	Frühstücks-Pause
11:30-12:00	*Integrating Passive RFID Devices into the Internet of Things* Johannes Samhaber (TU Graz)
12:00-12:30	*Practical Privacy-Preserving Video Surveillance* Andreas Unterweger (FH Salzburg)

Der Young Researcher's Day findet in den Räumen der OCG statt (Wollzeile 1, 1010 Wien). Wir ersuchen um eine Anmeldung bis zum 21.06.2013 an Yvonne Poul (ypoul@sba-research.org).

Wir freuen uns über Ihr Kommen und auf einen spannenden **3rd Young Researcher's Day 2013!**

Ingrid Schaumüller-Bichl
FH Hagenberg

Edgar Weippl
SBA Research

Structural Definition of Malware Behavior

Robert Luh – FH St. Pölten

Each month, hundreds of thousands of new malware variants are discovered and need to be tediously analyzed by antivirus companies in order to understand and counteract the threat these malicious programs pose to our global IT infrastructure. The project introduced here addresses the challenge by providing a method to generalize malicious behavior through structural definitions.

We present a schema that can be used to map malicious behavior beginning at its general goal down to the individual API calls used to execute specific system tasks. The application of this schema is illustrated by an example.

Furthermore, we discuss preliminary findings in the area of Windows API/system call behavior hinting at conclusive malicious – or benign – software activities discovered through dynamic (run-time monitoring) analysis.

Covert Computation - Hiding Code in Code for Obfuscation Purposes

Sebastian Schrittwieser – TU Wien

As malicious software gets increasingly sophisticated and resilient to detection, new concepts for the identification of malicious behavior are developed by academia and industry alike. While today's malware detectors primarily focus on syntactical analysis (i.e., signatures of malware samples), the concept of semantic-aware malware detection has recently been proposed. Here, the classification is based on models that represent the underlying machine and map the effects of instructions on the hardware. In this talk, we demonstrate the incompleteness of these models and highlight the threat of malware, which exploits the gap between model and machine to stay undetectable. To this end, we introduce a novel concept we call covert computation, which implements functionality in side effects of microprocessors. For instance, the flags register can be used to calculate basic arithmetical and logical operations. This talk shows how this technique could be used by malware authors to hide malicious code in a harmless-looking program. Furthermore, we demonstrate the resilience of covert computation against semantic-aware malware scanners.

Scenario-driven Testing of Security-related Domain-specific Language Models

Bernhard Hoisl – WU Wien

In this talk, we present an approach for the scenario-based testing of security-related DSML language models. The DSML language model is a crucial artifact in DSML development, because it captures all relevant domain abstractions and specifies the relations between these abstractions. In software engineering, scenarios are used to explore and to define system behavior as well as to specify user requirements. The different steps in a requirements-level scenario can then be refined through detailed scenarios. In our approach, we specify security properties via the DSML language model and provide for a scenario-based testing procedure for an integration case of two DSMLs. These refinements of high-level scenarios into executable test scenarios allow for a close cooperation of the security expert and the DSML engineer.

Integrating Passive RFID Devices into the Internet of Things

Johannes Samhaber – TU Graz

The Internet of Things (IoT) is understood as a concept where numerous items are able to acquire and store data as well as communicate over the Internet. This talk presents the realization of the last step towards the Internet of Things: Integrating passive RFID tags into the Internet.

A secure Internet layer based on IPsec and IKEv2 is established upon the RFID-communication layer, which allows for secure end-to-end connection between tags and clients. The IKEv2 protocol requires an elliptic curve Diffie-Hellman (ECDH) key exchange. For this purpose, we present a fast and area efficient ECC core implementation in hardware, using the NIST curve P-192 over the prime field F(p192).

Practical Privacy-Preserving Video Surveillance

Andreas Unterweger – FH Salzburg

In order to preserve people's privacy, videos captured with surveillance cameras are often encrypted -- either as a whole or in parts. While partial encryption, e.g., limited to facial regions, has many advantages, state-of-the art approaches are often computationally expensive. To overcome this limitation, a new encryption approach for the commonly used Motion JPEG format is presented, which operates on a bit stream level, requiring no expensive re-encoding operations, while being completely format compliant. The prototypical encryption framework is capable of encrypting VGA-sized Motion JPEG video streams at 25 frames per second, i.e., in real-time.