Security Day

Young Researchers' Day trifft Kryptostammtisch

Nach vier erfolgreichen Young Researcher's Days starten wir im Herbst 2014 in Runde 5 – und dies in einem neuen Format.

Ingrid Schaumüller-Bichl, Edgar Weippl und Stefan Mangard laden ganz herzlich zum **Security Day – Young Researchers' Day trifft Kryptostammtisch** ein, der im Rahmen des ACM SIGSAC Chapters Vienna, des OCG-Arbeitskreises IT-Sicherheit und des ENISA European Cyber Security Month stattfinden wird.

Der Security Day findet gemeinsam mit dem Kryptostammtisch des IAIK TU Graz statt und bietet Vorträge von Young und Senior Researchers im Bereich IT Security.

Freitag, 10.10.2014 von 11.00 – 16.00 Uhr
IAIK TU Graz, Inffeldgasse 16a, A-8010 Graz

Programm:

11.00-11.10	Begrüßung Stefan Mangard (IAIK TU Graz), Ingrid Schaumüller-Bichl (FH OÖ, Campus Hagenberg), Edgar Weippl (TU Wien, SBA Research),
11.10-11.35	Crypto Talk I *Proofs of Space* Krzysztof Pietrzak (IST Austria)
11.35-12.15	*Usable Security and Privacy in Mobile and Wearable Computing* Katharina Krombholz (SBA Research)
	Red-Teaming als praktischer Ansatz zur Überprüfung der ISO/IEC 27001 Controls Erik Rusek (FH OÖ, Campus Hagenberg)
12.15-13.25	Mittagspause
13.25-13.50	Crypto Talk II *Malicious SHA-1* Florian Mendel (TU Graz)
13.50-14.30	*Measuring and Improving Quality of Security Requirements in Information Systems Security Risk Management Processes* Christian Sillaber (Universität Innsbruck)
	Creation, Authentication and Recovery of Passwords Christian Kreuzberger (Universität Klagenfurt)
14.30-15.00	Pause
15.00-16.00	*Control-Flow Integrity: Compiler Assisted Signature Monitoring* Mario Werner (TU Graz)
	The Journey of a Malicious HTTP Request Malihe Mansouri (FH Joanneum)
	Konzeptionierung, Entwicklung und Erprobung eines SSL-Zertifikatsfuzzers zur Prüfung von Zertifikatsvalidierungschecks Christian Stoiber (FH St. Pölten)

Wir freuen uns auf einen spannenden **Security Day!**

Ingrid Schaumüller-Bichl
FH OÖ, Campus Hagenberg

Stefan Mangard
IAIK TU Graz

Edgar Weippl
SBA Research

Proofs of Space

Krzysztof Pietrzak (IST Austria)

Proofs of work (PoW) have been suggested by Dwork and Naor (Crypto'92) as protection to a shared resource. The basic idea is to ask the service requestor to dedicate some non-trivial amount of computational work to every request. The original applications included prevention of spam and protection against denial of service attacks. More recently, PoWs have been used to prevent double spending in the Bitcoin digital currency system.

In this talk I will present a new concept called proofs of space (PoS), where a service requestor must dedicate a significant amount of disk space (as opposed to computation as in PoWs). We construct secure PoS schemes in the random oracle model, using graphs with high "pebbling complexity" and Merkle hash-trees.

Joint work with Stefan Dziembowski, Sebastian Faust and Vladimir Kolmogorov.

Usable Security and Privacy in Mobile and Wearable Computing

Katharina Krombholz (SBA Research)

In general, the security of an information system is determined by the security capabilities of the weakest link in the chain. In many cases, the weakest link in the chain is the user. Therefore, an integration of human-computer-interaction aspects into security research is necessary in order to prevent systems from being compromised. Computers have become an essential part of our everyday lives. At this time, not only devices such as desktop computers but also mobile and wearable devices are connected to the Internet and collecting data of their users and surroundings. This implies distinct security, privacy and usability challenges. In the course of this talk, I want to discuss how human-computer interaction methods can be used to design secure and usable systems for mobile and wearable computers. Concerning mobile app development I will use the example of QR codes to illustrate how better usability reduces the susceptibility to phishing attacks. Furthermore, I will address privacy implications on bystanders of augmented reality glasses and how privacy mediating technologies can be designed to tackle the consequential challenges.

Red-Teaming als praktischer Ansatz zur Überprüfung der ISO/IEC 27001 Controls

Erik Rusek (FH OÖ, Campus Hagenberg)

Es werden die beiden Informationssicherheitsüberprüfungen, die Zertifizierung nach ISO/IEC 27001:2013 sowie das Red-Team-Assessment, vorgestellt und auf mögliche Ergänzungen eigegangen. Speziell werden weitere technische Prüfungstätigkeiten, im Rahmen des Red-Team-Assessments, für die ISO-Norm beleuchtet.

Malicious SHA-1

Florian Mendel (TU Graz)

However NSA most likely knows "zero-day" SHA-1 collisions, given its compute power and cryptanalysis skills (as demonstrated with Flame's MD5 collision). Custom versions of common crypto algorithms are common in certain closed systems, where obscurity does contribute to security: pay-TV systems, media platforms, commercial and military encryption gear, etc. and aim to differentiate crypto components across customers or services. Most applications of SHA-1 are integrity checks of files, programs, file systems, etc. For example many secure boot systems use SHA-1 to authenticate the code executed.

By leveraging state-of-the-art differential cryptanalysis techniques, we designed a generator of malicious SHA-1 instances, whose only difference with the original SHA-1 are about 40 bits of the "magic constants". We show how to construct valid executables that collide for such a malicious SHA-1 (that is, that hash to the same value, and thus yield identical digital signatures): examples are given of colliding shell scripts, master boot records, COM executables, and RAR archives. For each file type, we can fully control the 2 payloads: for example the colliding executables can be any 2 arbitrary programs (for example: legit application vs. malware plus legit application). This proof of-concept demonstrates the feasibility of a "crypto implant" that is as strong as the original SHA-1 except for the original designer.

This is a joint project with
- Ange Albertini (Corkami, Germany)
- Jean-Philippe Aumasson (Kudelski Security, Switzerland)
- Maria Eichlseder (TU Graz, Austria)
- Martin Schläffer (TU Graz, Austria)

project-webpage: http://malicioussha1.github.io/

Measuring and Improving Quality of Security Requirements in Information Systems Security Risk Management Processes (ongoing PhD research)

Christian Sillaber (Universität Innsbruck)

Nowadays, security sensitive data is distributed across all kind of devices. Attacks targeting this data are an ubiquitous threat. Embedded systems like smart cards are especially endangered given that they often play central roles in the security concept of bigger systems. A typical smart card consists of a processor and secured cryptographic hardware modules. These components are vulnerable to fault attacks. Previous research mostly focused on securing the cryptographic primitives. However, a system is only as strong as its weakest link. An adversary who mounts fault attacks against an unprotected processor can alter the control flow of the software. This compromises the security of the whole system and has to be prevented. Control-Flow Integrity (CFI) techniques can potentially provide protection. In this thesis, we present a CFI scheme called Derived Signature Monitoring using Assertions (DSMA). The scheme is based on the Continuous-Signature Monitoring (CSM) scheme from Wilken and Shen and has been designed with embedded applications in mind. DSMA uses a hybrid architecture and protects the control flow on the instruction-stream level. This permits the detection of control-flow errors induced by logical as well as by physical attacks. Implementing the scheme requires both hardware and software modifications. We implemented DSMA for the lightweight ARM Cortex-M0+ compatible Xetroc-M0+ processor. The DSMA monitor introduces only a 4.6% overhead on the microprocessor core.

Software instrumentation for DSMA is performed using a modified compiler in combination with a special post-processing tool. The advantage of this concept is its user friendliness.
Protecting a program with DSMA is as simple as compiling it. The modified compiler and the post-processing tool have been built upon the LLVM compiler infrastructure.

Overhead on the software side largely depends on the actual program code. Hardening an assembler optimized implementation of Elliptic Curve Cryptography (ECC) introduces a 2.5% runtime and a 55.7% program memory overhead. Protecting a C version of the Advanced Encryption Standard (AES) on the other hand leads to an 8% runtime and a 4.5% program memory overhead.

This thesis lays the foundation for future research. Further contributions in the field of compiler assisted control-flow integrity can be expected.

Creation, Authentication and Recovery of Passwords

Christian Kreuzberger (Universität Klagenfurt)

Accessing Personal Computers, Mobile Phones, E-Mails or services such as Online Banking require us to authenticate, e.g., by using a username and a password or a PIN code. While the concept of passwords seems to be self-explanatory, several problems can arise, e.g., when creating, storing or recovering passwords. The consequences of those problems are profound: identity theft, espionage, loss of money, and last but not least, inconvenience (e.g., your E-Mail account is hacked and you lose access to your address book and all your E-Mails).

This talk discusses the general idea of creating (secure) passwords, as well as some of the mentioned problems by looking at the tools and implementations used in Operating Systems, Web Browsers and Websites. In addition, simple examples of attacks are provided, demonstrating the necessity of strong cryptographic methods as well as sophisticated recovery schemes

Control-Flow Integrity: Compiler Assisted Signature Monitoring

Mario Werner (IAIK TU Graz)

Nowadays, security sensitive data is distributed across all kind of devices. Attacks targeting this data are an ubiquitous threat. Embedded systems like smart cards are especially endangered given that they often play central roles in the security concept of bigger systems. A typical smart card consists of a processor and secured cryptographic hardware modules. These components are vulnerable to fault attacks. Previous research mostly focused on securing the cryptographic primitives. However, a system is only as strong as its weakest link. An adversary who mounts fault attacks against an unprotected processor can alter the control flow of the software. This compromises the security of the whole system and has to be prevented. Control-Flow Integrity (CFI) techniques can potentially provide protection. In this thesis, we present a CFI scheme called Derived Signature Monitoring using Assertions (DSMA). The scheme is based on the Continuous-Signature Monitoring (CSM) scheme from Wilken and Shen and has been designed with embedded applications in mind. DSMA uses a hybrid architecture and protects the control flow on the instruction-stream level. This permits the detection of control-flow errors induced by logical as well as by physical attacks. Implementing the scheme requires both hardware and software modifications. We implemented DSMA for the lightweight ARM Cortex-M0+ compatible Xetroc-M0+ processor. The DSMA monitor introduces only a 4.6% overhead on the microprocessor core.

Software instrumentation for DSMA is performed using a modified compiler in combination with a special post-processing tool. The advantage of this concept is its user friendliness.
Protecting a program with DSMA is as simple as compiling it. The modified compiler and the post-processing tool have been built upon the LLVM compiler infrastructure.

Overhead on the software side largely depends on the actual program code. Hardening an assembler optimized implementation of Elliptic Curve Cryptography (ECC) introduces a 2.5% runtime and a 55.7% program memory overhead. Protecting a C version of the Advanced Encryption Standard (AES) on the other hand leads to an 8% runtime and a 4.5% program memory overhead.

This thesis lays the foundation for future research. Further contributions in the field of compiler assisted control-flow integrity can be expected.

The Journey of a Malicious HTTP Request

Malihe Mansouri (FH Joanneum)

SQL injection on Web applications is a very popular kind of attack. There are mechanisms such as intrusion detection systems in order to detect this attack. These strategies often rely on techniques implemented at high layers of the application but do not consider the low level of system calls. The problem of only considering the high level perspective is that an attacker can circumvent the detection tools using certain techniques such as URL encoding. One technique currently used for detecting low-level attacks on privileged processes is the tracing of system calls. System calls act as a single gate to the Operating System (OS) kernel; they allow catching the critical data at an appropriate level of detail. Our basic assumption is that any type of application, be it a system service, utility program or Web application, “speaks” the language of system calls when having a conversation with the OS kernel. At this level we can see the actual attack while it is happening. We conduct an experiment in order to demonstrate the suitability of system call analysis for detecting SQL injection. We are able to detect the attack. Therefore we conclude that system calls are not only powerful in detecting low-level attacks but that they also enable us to detect high-level attacks such as SQL injection.

Konzeptionierung, Entwicklung und Erprobung eines SSL-Zertifikatsfuzzers zur Prüfung von Zertifikatsvalidierungschecks

Christian Stoiber (FH St. Pölten)

SSL-Verschlüsselung ist heutzutage eine weit verbreitete Sicherheitstechnologie im Internet. Viele Dienstanbieterinnen und Dienstanbieter schützen durch den Einsatz von Verschlüsselung die Privatsphäre und die teilweise hochsensiblen Daten ihrer Nutzerinnen und Nutzer. Da SSL mit Zertifikaten arbeitet, hat die Endverbraucherin oder der Endverbraucher die Möglichkeit, die Identität der Dienstanbieterin oder des Dienstanbieters zu verifizieren. In der Regel übernimmt die Zertifikatsüberprüfung ein Programmteil - in Form von SSL-Bibliotheken, der in den modernen Browsern und mobilen Applikationen fix integriert ist. Im Frühjahr 2014 veröffentlichte Schwachstellen in SSL-Bibliotheken und im Umgang mit Verschlüsselung bestärken allerdings die Vermutung, dass eine korrekte Zertifikatsprüfung die Ausnahme und nicht die Regel ist.

In dieser Arbeit wird die fehlerfreie Funktion der Zertifikatsüberprüfung, durch zu Hilfenahme eines SSL-Zertifikatsfuzzers, analysiert. Der Fuzzer erzeugt mutwillig veränderte Zertifikate, die bei einer korrekten Zertifikatsüberprüfung abgelehnt werden sollten. Eine umfassende Sicherheitsanalyse ausgewählter mobile Banking Applikationen wird durchgeführt. Die Ergebnisse der Test liefern Informationen über das Sicherheitsniveau von Netbanking auf mobilen Endgeräten.