YOUNG RESEARCHERS' DAY TRIFFT IKT-SICHERHEITSKONFERENZ

16.10.2018
13:00 BIS 16:00 UHR

CONGRESS CENTRUM ALPBACH
Alpbach 246, 6236 Alpbach
Telefon: +43 (0) 5336 600 100

acm Chapter

fh OBERÖSTERREICH

OESTERREICHISCHE COMPUTER GESELLSCHAFT ®
AUSTRIAN COMPUTER SOCIETY

SBA Research

/fh///
st.pölten

YOUNG RESEARCHERS' DAY TRIFFT IKT-SICHERHEITSKONFERENZ

Der Young Resarchers' Day soll den besten Studierenden jeder österreichischen Institution, die einen Security-Lehrgang bzw. Lehrschwerpunkt anbietet, die Möglichkeit geben, ihre eigenen Arbeiten vorzutragen.

Als Grundgedanke hinter diesem Event, welches 2012 ins Leben gerufen wurde, steht der Wunsch, eine „Nachwuchsvernetzung" zu fördern.

Der Young Researchers' Day findet im Rahmen des ACM SIGSAC Chapters Vienna und des OCG-Arbeitskreises IT-Sicherheit statt und wird von SBA Research, der FH Oberösterreich und der FH St. Pölten organisiert.

YOUNG RESEARCHERS' DAY TRIFFT IKT-SICHERHEITSKONFERENZ

16.10.2018

PROGRAMM

13.00 – 13.10
Begrüßungsworte
GenMjr Mag. Rudolf Striedinger, Leiter Abwehramt
Dr. Ingrid Schaumüller-Bichl, FH Oberösterreich

13.10 – 13.25
FALKE-MC: A Neural Network Based Approach to Locate Cryptographic Functions in Machine Code
Alexander Aigner, FH Oberösterreich, Campus Hagenberg

13.25 – 13.40
Lightweight Key Derivation and Authentication for Low-End In-Car Nodes
Sergei Bauer, Universität Klagenfurt

13.40 – 13.55
Enabling Continuous Information Security Management
Michael Brunner, Universität Innsbruck

13.55 – 14.10
Process Behaviour Classification
Sebastian Eresheim, FH St. Pölten

14.10 – 14.30 ***Coffee Break***

14.30 – 14.45
Securing Systems against Machine Learning-driven, Password Guessing Attacks
Georg Knabl, FH Joanneum

14.45 – 15.00
Implementing Attribute-Based Credentials over OAuth 2.0
Dominik Koehle, AIT – Austrian Institute of Technology GmbH, FH Campus Wien

15.00 – 15.15
Designing an effective Auditing Method of Automotive Security for enabling Business Growth
Tobias Millauer, FH Oberösterreich, Campus Hagenberg

15.15 – 16.00 ***Coffee Break and Poster Session***

FALKE-MC: A Neural Network Based Approach to Locate Cryptographic Functions in Machine Code

Alexander Aigner, FH Oberösterreich, Campus Hagenberg

Abstract: Although the localization and classification of cryptographic functions in binary files is a growing challenge in information security, it is still a time consuming and laborious task. In this work, we present FALKE-MC, a novel framework that creates classifiers for arbitrary cryptographic algorithms from sample binaries. Functions are automatically recognized and features as well as constants are extracted. They are used to train a neural network, which can then be applied to classify functions in unknown binary files. The framework is fully automated, from the input of binary files and the creation of a classifier through to the output of classification results. The evaluation shows that our approach offers a high detection rate in combination with a low false positive rate. We are confident that FALKE-MC can simplify and accelerate the localization and classification of cryptographic functions in practice.

Lightweight Key Derivation and Authentication for Low-End In-Car Nodes

Sergei Bauer, Universität Klagenfurt

Abstract: Security features for highly automated vehicles have gained substantial public attention in recent years. Current in-vehicle networks contain sensitive security gaps. Efficiency and cost trigger the need for fast and secure security features that can be included in low-end automotive processing units without introducing extra hardware costs, excessive power consumption or crippling time delays. Using efficient lightweight ciphers combined with a novel key derivation technique a well evaluated cryptographic primitive was used, in order to achieve authenticate commands and components. This solution was validated on a typical automotive ASIC requiring only 10% of the controller’s program code size and available RAM usage for the cryptographic operations, allowing the device to carry out its application task with minimal overhead due to security.

Enabling Continuous Information Security Management

Michael Brunner, Universität Innsbruck

Abstract: Information Security Management Systems (ISMS) aim at ensuring proper protection of information values and information processing systems (i.e. assets). Information Security Risk Management (ISRM) techniques are incorporated to deal with threats and vulnerabilities that impose risks to information security properties of these assets. Accounting for the rapid evolution of businesses enterprises have to efficiently deal with changes to their assets, their risk exposure and the impact of these changes to their ISMS and ISRM activities. Current approaches are not well-suited for enterprises facing information security challenges from continuously evolving systems, diverse requirements regarding information security properties and regular changes to their assets and threat landscape. In our talk, we will present ADAMANT, our tool-based framework providing a continuous risk-driven approach to model and enact workflows in ISMSs. In addition, we will discuss the automation capabilities of our framework and present empirical results from case studies investigating the introduction of ADAMANT in small- and medium-sized enterprises.

Process Behaviour Classification

Sebastian Eresheim, FH St. Pölten

Abstract: Anomaly detection has long been used for detecting attacks on networks and computers. Its basic principle is declaring something as the norm and reporting deviations from it. Detecting such abnormalities in process behaviour is a crucial step for determining whether a computer is compromised or not. However, before abnormal behaviour of a process can be detected, the process needs to be correctly classified, because what might be normal for process A is not necessarily normal for process B. Consequently, the classification can already be a detection of behaviour deviations, for example when process A's behaviour is classified as a behaviour of process C.

In this talk, a statistical approach is proposed in combination with Machine Learning to classify process behaviour and thus build a baseline of behaviour for each process.

Securing Systems against Machine Learning-driven, Password Guessing Attacks

Georg Knabl, FH Joanneum

Abstract: When passwords are attacked by password cracking software like John the Ripper or hashcat, the efficiency of this process is significantly affected by the quality of the password lists that are used. Traditionally, tools like these use rule sets or masks along with dictionaries that include leaked passwords gained by previous successful attacks. However, these pre-identified password creation schemes are chosen and converted to attack patterns either by humans or by static automation algorithms which might miss actual human password patterns. Additionally, these tools have limited capabilities in generating password lists of individuals.

In recent years, machine learning algorithms have evolved that are capable of learning password creation schemes of humans by analyzing password leaks. Additionally, these algorithms can be fed with personal information of an individual to generate tailored password lists. Hence, this technology poses a new threat to password security and needs to be considered when securing systems.

This talk will introduce the problem and point out approaches to harden systems that rely on password security and build a protection layer against machine learning-based attacks.

Implementing Attribute-Based Credentials over OAuth 2.0

Dominik Koehle, AIT – Austrian Institute of Technology GmbH, FH Campus Wien

Abstract: An attribute-based credential (ABC) is a container that holds some of a user's identity information. It allows selective disclosure of some of the identity attributes without actually identifying the user. Current ABC systems (U-Prove and Idemix) all require the user's identity information to be available to the identity provider (IdP) in plaintext form.

CREDENTIAL – an EU-funded research project – addresses this issue by utilizing proxy re-encryption and redactable signatures and so further improves the user's privacy when using a cloud-based IdP for authentication.

This talk will give an overview of the cryptographic techniques as well as the extension of the OAuth 2.0 framework that is used as the basis for the delegated authorization -- which is required for a user-centric IdM sytem. A live demonstration of the implemented system and an outlook of open research questions will conclude the talk.

Designing an effective Auditing Method of Automotive Security for enabling Business Growth

Tobias Millauer, FH Oberösterreich, Campus Hagenberg

Abstract: The goal of this master's thesis is the creation of a framework for auditing automotive security. Our research examines the initial situation of the Original Equipment Manufacturer's (OEM) Corporate Audit department using the Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis and analyses the most common information security and automotive standards. Business growth through information security is illustrated by several models. The research domains of the automotive security framework developed in this thesis covers a wide range of audit topics. The results of our thesis are suitable for use by auditors during interviews as well as Chief Information Security Officers (CISO) for strategy development.