YOUNG RESEARCHERS' DAY
TRIFFT **IKT-SICHERHEITSKONFERENZ**

26.09.2017
13:00 BIS 16:00 UHR

CONGRESS CENTER VILLACH
Europaplatz 1, 9500 Villach
Telefon: +43 (0) 4242 22522 5804

acm Chapters
FH OBERÖSTERREICH
OESTERREICHISCHE COMPUTER GESELLSCHAFT
AUSTRIAN COMPUTER SOCIETY
SBA Research

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 und der FH Oberösterreich organisiert.

YOUNG RESEARCHERS' DAY TRIFFT IKT-SICHERHEITSKONFERENZ

26.09.2017

PROGAMM

13.00-13.15

Begrüßung
Ingrid Schaumüller-Bichl, FH OÖ
Edgar Weippl, SBA Research

Begrüßungsworte
GenMjr Mag. Rudolf Striedinger, Leiter Abwehramt

13.15-13.35

Extensibility in a Privacy-preserving eID:
Towards a Mobile eID System for Real-world Identification and Offline Verification
Michael Hölzl, JKU Linz

13.35-13.55

Influence of Emotions on the Spread of Information in Social Networks
Ema Kusen, WU Wien

14.00-14.20

Integrating Shared Cyber Threat Intelligence into Information Security Risk Management
Clemens Sauerwein, Universität Innsbruck

14.20-14.40

Graphs and their use in Binary Malware Analysis
Patrick Kochberger, FH St. Pölten

14.45-15.05

Physically Unclonable Functions as security anchors – an objective review
Martin Deutschmann, Technikon

15.05-15.25

Detecting Fraud and Attacks in Business Process Executions
Kristof Böhmer, Universität Wien

15.25-16.00

Coffee Break and Poster Session

Extensibility in a Privacy-preserving eID: Towards a Mobile eID System for Real-world Identification and Offline Verification

Michael Hölzl, JKU Linz

Abstract: There are many systems that provide users with an electronic identity (eID) to sign documents or authenticate to online services (e.g. governmental eIDs, OpenID). However, current solutions lack in providing proper techniques to use them as regular ID cards that digitally authenticate their holders to another physical person in the real world. We envision a fully mobile eID which provides such functionality in a privacy-preserving manner, fulfills requirements for governmental identities with high security demands (such as driver's licenses, or passports) and can be used in the private domain (e.g. as loyalty cards). In this presentation, we discuss potential use cases and difficulties as well as present a general architecture for such a flexible and privacy-preserving mobile eID.

Influence of Emotions on the Spread of Information in Social Networks

Ema Kusen, WU Wien

Abstract: In online social networks (OSNs), news travel fast and reach a large number of users within a short period of time. Although having a great potential to do good for society, OSNs have also been recognized as a convenient tool to influence people. One important influential factor that is in the focus of our work are *emotions* conveyed in the OSN messages.

While expressing emotions publicly over social media (*social sharing of emotions*) has become a common way of communication in the 21st century, studies also found that social sharing of emotions is contagious and may steer emotional reactions in a user, leading to malicious consequences (e.g. inducing feelings of pain, humiliation, and rage over injustice portrayed in a message and potentially leading to online radicalization). Thus, understanding how people express emotions, under which circumstances, and how they behave once they encounter a particular emotion has become a research topic of a growing body of recent studies. To this end, however, studies have largely contributed to the field by focusing on the impact of sentiment polarities on user behavior. Yet, two emotions belonging to the same affective valence may trigger distinct user reactions.

Given this context, the goal of our work is to examine how users react to emotionally-charged OSN messages in terms of emotions conveyed in their replies, as well as the number of likes, shares, and temporal features (e.g. time stamps of OSN user's reaction). We approach our study by 1) extracting over 5 million messages from three widely popular OSNs – Twitter, Facebook, and YouTube, 2) implementing and validating an NLP-based R-script for emotion extraction, 3) identifying sentiments and basic emotions according to Plutchik's wheel conveyed in the messages, and 4) obtaining behavioral patterns with respect to user reactions. We show that there is a distinct behavioral pattern when OSN users encounter specific emotions.

Integrating Shared Cyber Threat Intelligence into Information Security Risk Management

Clemens Sauerwein, Universität Innsbruck

Abstract: In the last couples of years, the complexity and interconnectedness of information systems, and the number of security related incidents increased significantly. In order to guarantee confidentiality, integrity and availability of these information systems an appropriate information security risk management must be in place. The timely acquisition and processing of information regarding vulnerabilities, threats, and available countermeasures represents a big challenge for a reliable and executive information security risk management. In order to address this challenge a multitude of shared cyber threat intelligence sources can be identified, ranging from public available threat intelligence sources (e.g. vulnerability databases, mailing lists, expert blogs,. . .) to cyber threat intelligence sharing communities that exchange the needed information among each other. However, little is known about the added value and use of shared cyber threat intelligence for information security risk management in organisations. In order to address this issue we conducted several empirical studies with security experts in the field followed by data analysis of public available shared cyber threat intelligence sources. In doing so we briefly analyzed how shared cyber threat intelligence can be integrated into information security risk management processes.

Graphs and their use in Binary Malware Analysis

Patrick Kochberger, FH St. Pölten

Abstract: The increasing number of Malware every day makes signature-based approaches more and more ineffective, therefore behavioral analysis is becoming a key component in the study and detection of Malware. To identify harmful behavior inside a binary the machine code has to be converted into a searchable format that can be used for the analysis. One way to achieve that is to generate flow graphs. This talk will explain what different approaches like CFG, DFG or PDG look like and what they can be used for.

Physically Unclonable Functions as security anchors – an objective review

Martin Deutschmann, Technikon

Abstract: Hardware entangled security mechanisms for ICT systems are gaining steadily in importance, as pure software solutions have clear limitations in terms of achievable security level. A potential alternative are so-called Physically Unclonable Functions (PUFs), an intensively debated topic in the crypto community since a couple of years. Beside those who praise PUFs as an indispensable security solution, there are also critics, who do not believe in the concept and who regularly publish successful attacks on PUFs. Whether PUFs can provide an added value depends on the way how they are used and implemented. In my talk I would therefore like to present practical aspects for the proper use of PUFs. I would like to reflect which structures are appropriate for being used as a PUF source and which quality parameters are significant in this context.

Detecting Fraud and Attacks in Business Process Executions

Kristof Böhmer, Universität Wien

Abstract: In recent years business process definitions have emerged from documentation to execution. Hence, instead of only describing inter-organizational connections or internal practices and operations business processes are directly implementing and executing them. So, business processes are not only deeply integrated into core IT systems, span organizational borders, and handle confidential information but also became an valuable target for internal and external attackers, fraud, and misuse.
Despite this situation established IT security mechanisms concentrate mainly on classic network and software security, leaving the attack vector „business process“ unprotected. However, failing at the detection of malicious process executions can result in the loss of private/confidential information, substantial fines, lost in trust, or even rendering an organization nonoperational. So we see it as a necessity that business processes are not left behind at the current trend and development towards security and will outline related challenges and solutions.