5th International Symposium on

Foundations & Practice of Security

École de technologie supérieure (ÉTS)
1100, rue Notre-Dame Ouest
Montreal (Quebec)
Canada

FIELDS

ÉTS

RYERSON UNIVERSITY
FACULTY OF SCIENCE

MINES TELECOM
INSTITUT
Mines-Télécom

Lab-STICC

Universitat Oberta de Catalunya

IN3

ARES
Advanced Research on Information Security and Privacy

IEEE
Montréal

Welcome

Welcome Message from the General Chairs

On behalf of the Organizing Committee, we would like to welcome you to the fifth annual Foundations & Practice of Security (FPS) symposium held at ETS (École de technologie supérieure), in Montréal, Canada. The objective of the FPS symposium is to present and discuss international research in different areas of theoretical and practical security solutions. Topics covered this year include security in social networks, intrusion detection, wireless network security, privacy and trust, policy-based security architectures, cryptography and cryptanalysis, security of mobile applications, testing techniques for security validation, and information theoretic security. This year's symposium received 62 submissions from 28 countries, out of which 23 papers were selected for regular oral presentation, and 3 for short presentations. All submissions went through a careful anonymous review process (3 or more reviews per submission) aided by 52 Technical Program Committee members and 32 external sub-reviews. This year's program includes two keynote addresses by Douglas Stinson (University of Waterloo, Canada) and Ana Rosa Cavalli (TELECOM & Management SudParis, France). We would like to thank everyone who has given his or her time, energy and ideas to assist in organizing this event, including all the members of the organizing committee, the TPC Co-Chairs, TPC members and all the reviewers, and our two distinguished keynote speakers, Dr. Stinson and Dr. Cavalli Boucher who have agreed to address the symposium attendees. In particular, we would like to highlight and acknowledge the tremendous efforts of Dr. Joaquin Garcia-Alfaro (TPC Co-chair) and Dr. Chamseddine Talhi (Local Arrangements Chair) who worked tirelessly on various symposium related tasks. We also wish to thank all of our sponsors who have made this event possible. It is through the collective efforts of these individuals and organizations that we are able to bring you a great event!

We are delighted to have you here and we hope you find this symposium to be a rewarding learning and partnership experience. We also hope that you will get a chance to enjoy your visit to Montréal.

Ali Miri
General Chair for FPS 2012

Frédéric Cuppens
General Co-Chair for FPS 2012

General Information

Registration

Participants may register on:

- Thursday, October 25: 8:15 AM to 3:00 PM
- Friday, October 26: 9:00 AM to 3:00 PM

Locations

- Conference building : B (please ask the security office)
- Conference room : B-4410
- Lunch and coffee breaks room : B-4502
- Social event (Banquet) About 7 minutes walking distance from ETS:
  - http://www.roselina.ca/
  - 1000, de La Gauchetière Ouest, Montréal, QC

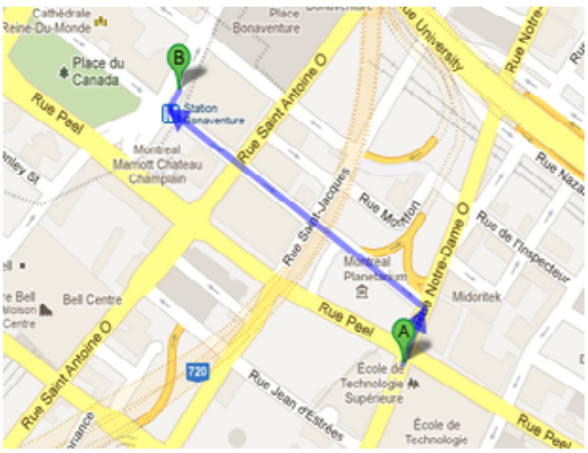
Wireless Internet Access

- Network name: ETS-Public
- Username: wifi-Workshop@etsmtl.ca
- Password: October.25-2012

Maps

From Bonaventure metro station to ÉTS

From ÉTS to Roselina Restaurant

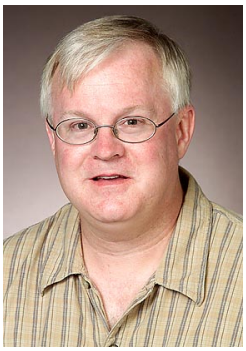


Program at a glance

Time	Thursday, October 25
8:45 AM	Welcome and Opening Remarks
9:00 AM	Keynote: *A coding theory approach to unconditionally secure proof-of-retrievability schemes for cloud storage*
10:00 AM	Coffee Break
10:30 AM	Session 1: Cryptography and Attack Modeling
12:15 PM	Lunch
1:45 PM	Session 2: Key Management and Cryptographic Protocols
3:00 PM	Coffee Break
3:30 PM	Session 3: Privacy and Trust
6:30 PM	Banquet

Time	Friday, October 26
9:00 AM	Keynote: *How to use testing techniques for security validation*
10:00 AM	Coffee Break
10:30 AM	Session 4: Policies and Application Security
12:15 PM	Lunch
1:45 PM	Session 5: Network Security I
3:00 PM	Coffee Break
3:30 PM	Session 6: Network Security II
4:50 PM	Farewell

Keynote Speakers



Dr. Douglas Stinson

Professor, PhD, University of Waterloo, Canada

Title: *A coding theory approach to unconditionally secure proof-of-retrievability schemes for cloud storage*

Abstract

There has been considerable recent interest in cloud storage wherein a user asks a server to store a large file. One issue is whether the user can verify that the server is actually storing the file, and typically a challenge-response protocol is employed to convince the user that the file is indeed being stored correctly. The security of these schemes is phrased in terms of an extractor which will recover or retrieve the file, given any proving algorithm that has a sufficiently high success probability. We investigate proof-of-retrievability (POR) schemes in the model of unconditional security, where an adversary has unlimited computational power. In this case retrievability of the file can be modelled as error-correction in a certain code. We provide a general analytical framework for such schemes that yields exact (non-asymptotic) reductions that precisely quantify conditions for extraction to succeed as a function of the success probability of a proving algorithm, and we apply this analysis to several archetypal schemes. In addition, we provide a new methodology for the analysis of keyed (unbounded-use) POR schemes in an unconditionally secure setting, and use it to prove the security of a modified version of a scheme due to Shacham and Waters under a slightly restricted attack model, thus providing the first example of a keyed POR scheme with unconditional security. This talk is based on joint work with Maura Paterson and Jalaj Upadhyay.

Bio

Douglas Stinson received the B.Math. degree from the University of Waterloo, in 1978, the M.Sc. degree from the Ohio State University in 1980, and the Ph.D. degree in combinatorics and optimization from the University of Waterloo in 1981. His research interests include cryptography and computer security, combinatorics and coding theory, and applications of discrete mathematics in computer science. He is the author of over 300 research publications as well as mathematics-based cryptography textbooks. He has held academic positions at the University of Manitoba, where he was an NSERC University Research Fellow, and the University of Nebraska-Lincoln. Currently he holds the position of Professor in the David R. Cheriton School of Computer Science at the University of Waterloo. He held the NSERC/Certicom Industrial Research Chair in Cryptography from 1998 to 2003. He held a Mathematics Faculty Fellowship from 2001-2004 and a University Research Chair from 2005-2011. He was elected as a Fellow of the Royal Society of Canada in 2011.

Keynote Speakers (cont.)

Dr. Ana Rosa Cavalli

Professor, PhD, Institut Mines-Telecom,
TELECOM & Management SudParis, France

Title: *How to use testing techniques for security validation*

Abstract

Testing techniques are used to check if a given system implementation satisfies its specification or some predefined properties. These testing techniques can be active, based on the execution of specific test sequences against the implementation under test, or passive, based on the observation of the exchange of messages (input and output events) of the implementation under test during run-time. In the last years, important research initiatives have taken place dealing with the application of testing techniques to check security properties; in particular, to check the correctness of security policy implementations and also to define intrusion detection techniques. In this talk, we will present some of these approaches and their application to real case studies as well as some ideas of how to specify security policies.

Bio

Ana Rosa Cavalli received her Doctorat d'Etat (*Mathematics Science and Informatics*), from the University of Paris VII, in 1984. In 1981, she integrated the LITP (*Laboratoire d'Informatique Theorique et Programmation*), CNRS, Paris, where she worked on proof methods for temporal logics and their application to communication protocols. From 1985 to 1990, she was a researcher in the department Languages and Switch Systems, at CNET (*Centre National d'Etudes des Telecommunications*), where she worked on software engineering and formal methods. She is Full Professor at TELECOM & Management SudParis (ex *Institut National des Telecommunications*) since 1990. She is the director of the Software for Networks department. She is also responsible of the research team Verification and test of services and protocols and the AVERSE team, in the CNRS research laboratory SAMOVAR. Her research interests are on specification and verification, testing methodologies for conformance and interoperability testing, active testing and monitoring techniques, the validation of security properties and their application to services and protocols. She is the leader of the European Marie Curie network TAROT (*Training and Research on Testing*) and participates to several national and international projects.

Thursday, October 25, 2012

9:00 – 10:00 AM

Room: B-4410

Keynote: *A coding theory approach to unconditionally secure proof-of-retrievability schemes for cloud storage*

Speaker: Douglas Stinson

Chair: Ali Miri (Ryerson University, Canada)

10:30 AM - 12:15 PM

Session 1: Cryptography and Attack Modeling

Room: B-4410

Chair: Wahab Hamou-Lhadj (Concordia University, Canada)

MaD2: An Ultra-Performance Stream Cipher for Pervasive Data Encryption

Jie Li and Jianliang Zheng (City University of New York, USA)

MaD2 is an ultra-performance stream cipher that runs into one clock cycle per byte on a typical personal computer. With an encryption/decryption rate significantly higher than the disk data transfer rate, it can be employed to secure data at rest with almost no user observable performance degradation. The cipher resists various known cryptanalytic attacks. It also demonstrates good statistical feature and clears all the NIST statistical tests, the new Diehard battery of tests, and the TestU01 batteries of tests.

Proofs of Retrievability via Fountain

Sumanta Sarkar and Reihaneh Safavi-Naini (University of Calgary, Canada)

Proofs of Retrievability (PoR) allows a verifier to check the integrity of its data stored at some remote untrusted cloud storage through an interactive challenge-response protocol with the storage (prover). An unbounded-use PoR scheme allows to run unbounded number of challenge-response interactions. Constructions of PoR scheme aim to minimize the communication complexity in the challenge-response protocol, the storage overhead and computation of responses. The security of a PoR scheme is formalized by showing the existence of an extractor which retrieves the file from an erasing adversary that can pass the challenge-response protocol with some reasonable probability. The extractor decodes the file by collecting the correct responses from the prover. In this paper, we modify the unbounded-use PoR scheme of Shacham and Waters (2008) to have faster computation of responses which uses XORing of data blocks. In our scheme, responses are the encoded symbols of a Fountain code and they are verified by using homomorphic linear authenticators. The number of data blocks that are challenged is probabilistic, which is O(log l) on the average case and O(l) in the worst case, where l is the security parameter. Response computation becomes faster if the number of challenged blocks is small.

MARC: Modified ARC4

Jianliang Zheng and Jie Li (City University of New York, USA)

RC4, often referred to as Alleged RC4 (ARC4) in open literature due to trademark issue, was and probably still is the most popular stream cipher. Although some weaknesses in its key scheduling algorithm have been reported and new faster and claimed secure stream ciphers have been proposed, ARC4 is likely to remain as a big player in cryptographic applications. In this paper, we propose a new variant of ARC4, called Modified ARC4 (MARC), which enhances the security of ARC4 by modifying its key scheculing algorithm and improves the performance by modifying its pseudo-random generation algorithm. MARC retains the simplicity of ARC4 and is faster than all the software-efficient finalists of eStream except HC-128.

Detection of HTTP-GET Attack with Clustering and Information Theoretic Measurements

Pawel Chwalinski, Roman Belavkin and Xiaochun Cheng (Middlesex University, London, UK)

One of the attacks observed against HTTP protocol is HTTP-GET attack using sequences of requests to limit accessibility of web-servers. This attack has been researched in this report, and a novel clustering technique has been developed to tackle it. In general, the technique uses entropy-based clustering and application of information theoretical measurements to distinguish among legitimate and attacking sequences. It has been presented that the introduced method allows for formation of recent patterns of behaviours observed at a web-server, that remain unknown for the attackers. Subsequently, statistical and information theoretical metrics are introduced to measure difference between a sequence of requests, and legitimate patterns of behaviour. The method recognises more than 80% of legitimate and attacking sequences, regardless of strategies chosen by attackers. This result is rea sonably good, comparing to other techniques that do not rely on the instances of known attacks.

Towards Modelling Adaptive Attacker's Behaviour (Short Paper)

Leanid Krautsevich (University of Pisa, Italy); Fabio Martinelli and Artsiom Yautsiukhin (Consiglio Nazionale delle Ricerche, Italy)

Most of the current models of an attacker for a computer system assume that the adversary has a complete knowledge of a system. Although, such vision is helpful for searching for weak places in the defence of the security of the system, such model does not describe the reality well enough. In practice, attackers have very limited amount of knowledge about a system and often do mistakes while attacking it. Therefore, such models cannot be used for assessment of the real security risks and should be updated. We aim at the model for the behaviour of an attacker. The model takes into account the uncertain knowledge of the attacker about the system. In addition, the attacker in our model tries different attack paths in case of a failure. Our mathematical model is based on Markov Decision Processes theory which allows to predict attacker's decisions.

1:45 - 3:00 PM

Session 2: Key Management and Cryptographic Protocols

Room: B-4410

Chair: Nadia Tawbi (Université Laval, Québec)

A Generic Algebraic Model for the Analysis of Cryptographic-Key Assignment Schemes

Khair Eddin Sabri (University of Jordan, Jordan) and Ridha Khedri (McMaster University, Canada)

One of the means to implement information flow policies is by using a cryptographic approach commonly referred to as key assignment schemes. In this approach, information is made publicly available to users but in an encrypted form. Then, keys are assigned to users such that each key reveals a specified part of the information. Usually the distribution of keys follows a predefined scheme that specifies the ability of users to reveal information. In this paper, we present an algebraic approach based on idempotent commutative semirings to define, specify, and analyse key assignment schemes. Then we illustrate its usage on two key assignment schemes selected from the literature. Also, we propose amendments to the studied schemes to extend their scopes. The proposed generic algebraic approach enables the assessment of the secrecy of key assignment schemes through algebraic calculations, which can be automated using Prover9.

Message Transmission and Key Establishment: Conditions for Equality of Weak and Strong Capacities

Hadi Ahmadi and Reihaneh Safavi-Naini (University of Calgary, Canada)

Secure communication using noisy resources was first studied in the two contexts of secure message transmission (SMT) by Wyner as well as Csiszar-and-Korner, and secret key establishment (SKE) by Ahlswede-and-Csiszar as well as Maurer. The work defines secrecy (resp. secret-key (SK)) capacity as the highest achievable rate at which a secure message can be sent (resp. a shared key can be established). Maurer and Wolf later focused on

SKE and noticed that the secrecy requirement in the SK capacity definition was weak as it required only the ratio between the adversary's information and the key length to be negligible. They suggested a stronger definition of the SK capacity where secrecy requires absolute amount of adversary's information about the key to be negligible. Additionally, they provided an interesting approach to prove the equality of the two SK capacities for the above communication scenarios (setups). Followup work has since studied several setups for SKE by considering the weak notion of SK capacity without discussing whether the results also hold for the strong definition. In this paper, we pose the question whether Maurer-and-Wolf's approach is applicable to those SKE setups studied thereafter, and more importantly, whether the equality of weak and strong SK capacities can be derived in general for all discrete memoryless communication setups. We also extend this study to message transmission and investigate the equality of weak and strong secrecy capacities. We provide a formal treatment of these questions considering in a general description of a communication setup. We show that weak and strong SK capacities are equal for any setup that allows reliable transmission in any direction. For message transmission, we show that the secrecy capacities are equal when the setup allows the sender to use randomness.

COMPASS: Authenticated Group Key Agreement from Signcryption

Nicholas Mailloux (University of Ottawa, Canada); Ali Miri (Ryerson University & University of Ottawa, Canada); and Monica Nevins (University of Ottawa, Canada)

One of the means to implement information flow policies is by using a cryptographic approach commonly referred to as key assignment schemes. In this approach, information is made publicly available to users but in an encrypted form. Then, keys are assigned to users such that each key reveals a specified part of the information. Usually the distribution of keys follows a predefined scheme that specifies the ability of users to reveal information. In this paper, we present an algebraic approach based on idempotent commutative semirings to define, specify, and analyse key assignment schemes. Then we illustrate its usage on two key assignment schemes selected from the literature. Also, we propose amendments to the studied schemes to extend their scopes. The proposed generic algebraic approach enables the assessment of the secrecy of key assignment schemes through algebraic calculations, which can be automated using Prover9.

Scalable Deniable Group Key Establishment (Short Paper)

Kashi Neupane (Atlanta Metropolitan State College, USA); Rainer Steinwandt and Adriana Suarez Corona (Florida Atlantic University, USA)

The popular Katz-Yung compiler from CRYPTO 2003 can be used to transform unauthenticated group key establishment protocols into authenticated ones. In this paper we present a modification of Katz and Yung' construction which maintains the round complexity of their compiler, but for typical unauthenticated group key establishments adds authentication in such a way that deniability is achieved as well. As an application, a deniable authenticated group key establishment with three rounds of communication can be constructed.

3:30 - 4:25 PM

Session 3: Privacy and Trust

Room: B-4410

Chair: Esma Aïmeur (Université de Montréal, Canada)

Classifying Online Social Network Users Through the Social Graph

Cristina Pérez-Solà (Universitat Autònoma de Barcelona, Spain) and Jordi Herrera-Joancomartí (Universitat Autònoma de Barcelona & Internet Interdisciplinary Institute, Spain)

In this paper, we address the problem of classifying online social network users using a naively anonymized version of a social graph. We use two main user attributes defined by the graph structure to build an initial classifier, node degree and clustering coefficient, and then exploit user relationships to build a second classifier.

We describe how to combine these two classifiers to build an OSN user classifier and then we evaluate the performance of our architecture by trying to solve two different classification problems (a binary and a multiclass problem) using data extracted from Twitter. Results show that the proposed classifier is sound and that both classification problems are feasible to solve by an attacker who is able to obtain a naively anonymized version of a social graph.

A Formal Derivation of Composite Trust

Tim Muller and Patrick Schweitzer (University of Luxembourg, Luxembourg)

Trust appears in asymmetric interactions, where one party (the active party) can easily betray a stakeholder (the passive party). Over the Internet, the amount of information that a passive party can use to determine the integrity of an active party, is often limited. The scenario where there is only one passive party and one active party is well studied, and has been solved under specific assumptions. We generalize the setting to allow for more parties. In particular, the paper contains a formal derivation of conjunction and disjunction of trust opinions.

IPv6 Stateless Address Autoconfiguration: Balancing Between Security, Privacy and Usability

Ahmad Alsa'deh, Hosnieh Rafiee and Christoph Meinel (University of Potsdam, Germany)

Included in the IPv6 suite is a method for devices to automatically configure their own addresses in a secure manner. This technique is called Cryptographically Generated Addresses (CGAs). CGA provides the ownership proof necessary for an IPv6 address without relying on any trust authority. However, the CGA computation is very high, especially for a high security level defined by the security parameter (Sec). Therefore, the high cost of address generation may keep hosts that use a high Sec value from frequently changing their addresses. Consequently, the result is that hosts using CGAs are still susceptible to privacy related attacks. This paper proposes some modifica-tions to the standard CGA in order to make it more usable and configurable security approach while protecting the users' privacy. We make CGA more privacy-conscious by changing the addresses over time to protect users from being tracked. We propose to reduce the CGA granularity of the security level from 16 to 8. We believe that the granularity 8 is more reasonable for most applica-tions and scenarios. We implement and evaluate these extensions to the stand-ard CGA.

Information-theoretic foundations of differential privacy (Short Paper)

Darakhshan J. Mir (Rutgers University, USA)

We examine the information-theoretic foundations of the increasingly popular notion of differential privacy. We establish a connection between differential private mechanisms and the rate-distortion framework. Additionally, we also show how differentially private distributions arise out of the application of the Maximum Entropy Principle. This helps us locate differential privacy within the wider framework of information-theory and helps formalize some intuitive aspects of our understanding of differential privacy.

Friday, October 26, 2012

9:00 – 10:00 AM

Keynote: *How to use testing techniques for security validation*
Speaker: Ana Rosa Cavalli
Room: B-4410
Chair: Nora Cuppens-Boulahia (Télécom Bretagne, France)

10:30 AM - 12:15 PM

Session 4: Policies and Application Security

Chair: Frédéric Cuppens (Télécom Bretagne, France)

Policy Administration in Tag-Based Authorization

Sandro Etalle (Eindhoven University of Technology & University of Twente, The Netherlands); Timothy L. Hinrichs (University of Illinois at Chicago, USA); Adam J. Lee (University of Pittsburgh, USA); Daniel Trivellato and Nicola Zannone (Eindhoven University of Technology, The Netherlands)

Tag-Based Authorization (TBA) is a hybrid access control model that combines the ease of use of extensional access control models with the expressivity of logic-based formalisms.The main limitation of TBA is that it lacks support for policy administration. More precisely, it does not allow policy-writers to specify administrative policies that constrain the tags that users can assign, and to verify the compliance of assigned tags with these policies. In this paper we introduce TBA^2 (Tag-Based Authorization & Administration), an extension of TBA that enables policy administration in distributed systems. We show that TBA^2 is more expressive than TBA and than two reference administrative models proposed in the literature, namely HRU and ARBAC97.

Enabling dynamic security policy in the Java security manager

Fabien Autrel, Nora Cuppens-Boulahia and Frederic Cuppens (Télécom Bretagne, France)

The Java execution environment includes several security mechanisms. They are found in the language itself, in the class loader, in the class verifier and in the sandbox in which bytecode is executed. The sandbox isolates the executed bytecode from the host on which the Java virtual machine is executed. The security policy enforced by the sandbox can be configured depending on who runs a program and the origin of the program and offers fine-grained mechanisms to control resource access. However, the security policy language offers no higher-level paradigms, such as the abstraction of users into roles, to enable the management of java security policies into large infrastructures. Moreover those policies are static and cannot change depending on the state of the environment into which they are deployed. We propose in this article an approach to use of the OrBAC model to configure the sandbox security policy, allowing the use of an implementation-independent policy language which offers facilities to manage large sets of JVMs, enables the expression of dynamic security policies and offers an advanced administration model..

A Novel Obfuscation: Class Hierarchy Flattening

Christophe Foket, Bjorn De Sutter, Bart Coppens and Koen De Bosschere (Ghent University, Belgium)

This paper presents class hierarchy flattening, a novel obfuscation technique for programs written in object-oriented, managed programming languages. Class hierarchy flattening strives for maximally removing the inheritance relations from object-oriented programs, thus hiding the overall design of the program from reverse engineers and other attackers. We evaluate the potential of class hierarchy flattening by means of a fully automated prototype tool for Java bytecode. For real-life programs from the DaCapo benchmark suite, we demonstrate that the transformation effectively hinders both human and tool analyses, and that it does so at limited overheads.

RESource: A Framework for Online Matching of Assembly with Open Source Code

Ashkan Rahimian (Concordia University, Canada); Philippe Charland (Defence R&D Canada, Canada); Stere Preda and Mourad Debbabi (Concordia University, Canada)

Software reverse engineering is a fastidious task demanding a strong expertise in assembly coding. Various existing tools may help analyze the functionality of a binary file without executing it and an interesting step would naturally be the search for the original source files. Our tool called RESource considers the extraction of some features in the assembly code so that queries can be triggered to a source repository in a reliable way: either (1) the result is a set of references to the original project files provided they are hosted on the repository or (2) at

least some functionalities of the binary file are unleashed. Such an approach is very promising given its proved performances in real assembly code applications.

Touchjacking Attacks on Web in Android, iOS, and Windows Phone

Tongbo Luo, Xing Jin, Ajai Ananthanarayanan and Wenliang Du (Syracuse University, USA)

To make it easy for applications to interact with the Web, most mobile platforms, including Android, iOS, and Windows Phone, provide a mechanism that allows applications to embed a small but powerful browser component inside. This mechanism is called WebView in Android (it is called dierent names in other platforms). WebView implements a number of APIs that can be used by applications to interact with the web contents inside WebView. It has been pointed out by the previous work that malicious applications can use these APIs to attack the web contents inside WebView. Proposals are made by the previous work to x the problems of those APIs. We have discovered that by xing those APIs, WebView is still not secure. This is because the previous work only focuses on the APIs specifically designed for WebView; they have overlooked the APIs that WebView inherits from its super classes. These APIs are designed for the general-purposed user interface (UI) components, and they seem to pose no risk to those components; however, the combination of these APIs with the Web has led to new risks. We have identied several attacks based on these APIs. Our attacks are called Touchjacking attacks. They treat WebView as a blackbox, i.e., they do not use the APIs that are designed specically for WebView; instead, they only use the inherited APIs. Through these APIs, malicious applications can attack the web contents inside WebView.

1:45 - 3:00 PM

Session 5: Network Security I

Room: B-4410

Chair: Ana Rosa Cavalli (Télécom SudParis, France)

Short-term Linkable Group Signatures with Categorized Batch Verification

Lukas Malina (Brno University of Technology, Czech Republic); Jordi Castella-Roca, Arnau Vives-Guasch (Universitat Rovira i Virgili, Spain); and Jan Hajny (Brno University of Technology, Czech Republic)

In ad hoc wireless networks like Vehicular ad hoc Network (VANETs) or Wireless Sensor Networks (WSN), data confidentiality is usually a minor requirement contrary to data authenticity and integrity. Messages broadcasted from a node to other nodes should be authentic but also keep user's privacy in plenty scenarios working with personal data. Group signatures (GS) are used to provide privacy and authenticity to the users. Moreover, GS with batch verification can be efficient. Nevertheless, the current solutions have practical drawbacks like using an expensive tamper-proof hardware, the computation bottlenecks of the verification and revocation phases, complicated certificate distribution/revocation or omitting important properties like short-term linkability which is demanded in several applications, e.g. change lanes of vehicles in VANETs. To our best knowledge, our solution employs the short group signature with short-term linkability and categorized batch verification for the first time. Our solution provides more efficient signing and verification than compared schemes. Moreover, the solution allows secure and practical registration and revocation of users. The usage of proposed scheme protects the honest users who can now join and securely communicate without losing their privacy.

GHUMVEE: efficient, effective and flexible replication

Stijn Volckaert, Bjorn De Sutter, Tim De Baets and Koen De Bosschere (Ghent University, Belgium)

We present GHUMVEE, a multi-variant execution engine for software intrusion detection. GHUMVEE transparently executes and monitors diversified replicae of processes to thwart attacks relying on a predictable, single data layout. Unlike existing tools, GHUMVEE's interventions in the process' execution are not limited to system call invocations. Because of that design decision, GHUMVEE can handle complex, multi-threaded real-life programs that display non-deterministic behavior as a result of non-deterministic thread scheduling and as a result of pointer-value dependent behavior. This capability is demonstrated on GUI programs from the Gnome and KDE desktop environments.

Extracting Attack Scenarios Using Intrusion Semantics

Sherif Saad and Issa Traore (University of Victoria, Canada)

Building the attack scenario is the first step to understand an attack and extract useful attack intelligence. Existing attack scenario reconstruction approaches, however, suffer from several limitations that weaken the elicitation of the attack scenarios and decrease the quality of the generated attack scenarios. In this paper, we discuss the limitations of the existing attack scenario reconstruction approaches and propose a novel hybrid approach using semantic analysis and intrusion ontology. Our approach can reconstruct known and unknown attack scenarios and correlate alerts generated in multi-sensor IDS environment. Our experimental results show the potential of our approach and its advantages over previous approaches.

On Securely Manipulating XML Data

Houari Mahfoud and Abdessamade Imine (University of Nancy, France)

Over the past years several works have proposed access control models for XML data where only read-access rights over non-recursive DTDs are considered. A small number of works have studied the access rights for updates. In this paper, we present a general model for specifying access control on XML data in the presence of the update operations of W3C XQuery Update Facility. Our approach for enforcing such update specification is based on the notion of query rewriting. A major issue is that query rewriting for recursive DTDs is still an open problem. We show that this limitation can be avoided using only the expressive power of the standard XPath, and we propose a linear algorithm to rewrite each update operation defined over an arbitrary DTD (recursive or not) into a safe one in order to be evaluated only over the XML data which can be updated by the user. This paper represents the first effort for securely XML updating in the presence of arbitrary DTDs (recursive or not) and a rich fragment of XPath.

3:30 - 4:30 PM

Session 6: Network Security II

Chair: Joaquin Garcia-Alfaro (Télécom Bretagne, France)

Mitigating Collaborative Blackhole Attacks on DSR-Based Mobile Ad Hoc Networks

Isaac Woungang (Ryerson University, Canada); Sanjay Kumar Dhurandher (University of Delhi, India); Rajender Dheeraj Peddi (Ryerson University, Canada); and Issa Traore (University of Victoria, Canada)

A Mobile ad hoc network (MANET) is a collection of mobile nodes that rely on co-operation amongst devices that route packets to each other. From a security design perspective, MANETs have no clear line of defense.. This lack of security leads the network accessible to both legitimate network users and malicious attackers. A blackhole attack is a severe attack that can be employed against data routing in MANETs. A blackhole is a malicious node that can falsely reply for any route requests without having an active route to a specified destination and drop all the receiving data packets. The attack may even lead to more devastating damage if two or more blackhole nodes cooperate with each other to launch an attack. This type of attack is known as collaborative blackhole attack. In this paper, a novel scheme (so-called DCBA) for detecting collaborative blackhole attacks in MANETs is introduced. Simulation results are provided, showing that the DCBA outperforms DSR in terms of packet delivery ratio and network throughput, chosen as performance metrics, when collaborative blackhole nodes are present in the network.

QoS Aware Adaptive Security Scheme for Video Streaming in MANETs

Tahsin Reza and Michel Barbeau (Carleton University, Canada)

Real-time video streaming is delay sensitive and has minimum bandwidth and QoS requirements. Achieving target QoS for video streaming is challenging in a decentralized and self-organized MANET. Cryptography algorithms offer confidentiality of shared data, but they have computation cost. Our work addresses the issue of

delay overhead caused by the introduction of cryptography that directly affects video streaming performance. Our proposal is motivated by possibilities of adaptive security and multimedia service. We make an effort to identify why, when and how to deploy adaptation. We propose QaASs (QoS aware Adaptive Security scheme), an adaptive mechanism that counters the effect of delay overhead by adapting cryptography and multimedia properties, providing QoS while maintaining a required level of security. We evaluate our proposal through implementation and analysis of simulation results.

A Case Study of Side-Channel Analysis using Decoupling Capacitor Power Measurement with the OpenADC

Colin O'Flynn and Zhizhang Chen (Dalhousie University, Canada)

When capturing power measurements for processing with side-channel analysis, there are many options around both how the measurement is taken, and also how that measurement is digitized. This work concentrates on a new technique which measures the current through a decoupling capacitor, with a probe that can easily be built in any electronics lab. In addition an open-source digitizer board is presented, which is specifically designed to measure the signals required for side-channel analysis. The techniques presented in this work facilitate sharing of repeatable measurement techniques: the measurement environment presented can easily be duplicated at a very low cost.