RISE SICS and LTH

presents

ÖØresund Security Day Spring 2018

June 4, 2018

09.30 – 16.00

***Location**: Room 2311, E-huset, LTH, Lund*
John Erikssons väg 4

Program

Sponsored by: SICS South

09:30-09:50	Arrival & breakfast	
09.50-10.00	Introduction/Welcome	Thomas Carnehult, RISE SICS
10.00-10.25	A privacy preserving model and protection scheme for real-time cloud based production data analytics	Christian Gehrmann, LTH
10:25-10:30	Question & Discussion	
10.30-10.55	Standardizing IoT Transport Layer Security: Lessons Learned from Formally Verifying EDHOC	Theis Grønbech Petersen, ITU & Thorvald Sahl Jørgensen, ITU
10:55-11:00	Questions & Discussion	
11.00-11.15	*Break*	
11:15-11:40	Attacks on Industrial Control Systems (ICS)	Ludwig Seitz, RISE SICS
11:40-11:45	Questions & Discussion	
11.45-13.00	*Lunch (Ideon Krydhyllan)*	
13.00-13.25	A Security Analysis of the Ticket Inspection Ceremony in Denmark	Rosario Giustolisi, ITU
13.25-13.30	Questions & Discussion	
13.30-13.55	Post-quantum Cryptanalysis	Erik Mårtensson, LTH
13.55-14.00	Questions & Discussion	
14.00-14:15	*Break*	
14.15-14.40	Compositional Reasoning for Information-Flow Control	Willard Rafnsson, ITU
14.40-14.45	Questions & Discussion	
14.45-15.10	How we accidentally did sequential composition	Sebastian Alexander Mödersheim, DTU
15.10-15.15	Questions & Discussion	
15.15-15.20	*Mini break*	
15.20-15.45	Encryption and Reversible Computations	Ken Friis Larsen, DIKU Michael Kirkedal Thomsen, DIKU
15.45-15.50	Questions & Discussion	
15.50-16.00	Closure & Next Event	Christian Gehrmann (LTH) & All

Sponsored by: SICS South

Presentation abstracts

A privacy preserving model and protection scheme for real-time cloud based production data analytics

This presentation describes data item protection scheme and corresponding key management scheme that allows large scale, privacy and confidentiality protected, cloud based data analytics. We describe the general security model, the key management scheme and the protected item format in our solution.

Christian Gehrmann, LTH

Standardizing IoT Transport Layer Security: Lessons Learned from Formally Verifying EDHOC

Ephemeral Diffie-Hellman over COSE (EDHOC for short), is a protocol that aims to replace TLS for resource constrained IoT devices using a selection of lightweight ciphers and formats. It is inspired by the newest internet standard of TLS 1.3, and includes the famous reduced round-trip modes of the protocol. However, unlike TLS, it does not suffer from the complexities of supporting its non-existent legacy, nor it gains from the long life of a protocol that has received huge attention from the research community and security professionals. How well does it stack up to its big brother? In this work, we collaborated closely with the original authors of EDHOC to produce a formal analysis of the protocol, contribution that is necessary for its standardization within IETF. We discovered interesting and non-trivial properties about the security of the reduced round-trip mode: namely that the first and second payloads in the protocol are guaranteed integrity and secrecy (respectively) only conditionally to the protocol completion, and a similar result of conditional security with regards to the claims of perfect-forward-secrecy. These are rather complex properties, and in fact dangerous if the decision for an implementation is left to programmers who might misunderstand their guarantees. The input of our study, which we present in this talk, will be used to improve the next iteration of the EDHOC standard draft.

Authors: Theis Grønbech Petersen, Thorvald Sahl Jørgensen, Alessandro Bruni, Carsten Schürmann

A Security Analysis of the Ticket Inspection Ceremony in Denmark

We examine the inspection ceremony for the mobile transport ticket in Denmark. We discuss three potential security weaknesses that are ascribable to both human and computer components of the ceremony. The main vulnerabilities are due to the design choices of how the visual inspection ceremony is organised and the lack of information that is stored in the ticket barcode. Those vulnerabilities are significant as attacks can be automated, and rather modest skills are necessary to break the inspection ceremony. We state four principles that aim at strengthening the security of inspection ceremonies and propose an alternative ceremony whose design is driven by the stated principles.

Rosario Giustolisi, ITU

Post-quantum Cryptanalysis

Using large-scale quantum computers Shor's algorithm solves both the integer factoring problem and the discrete logarithm problem in polynomial time. To prepare for the future new public-key cryptosystems, based on the difficulty of other mathematical problems, such as the Learning With Errors problem (LWE) and the problem of decoding a random linear code, have been created. The difficulty of these systems is not as well understood. Thus, it is vital for cryptanalysts to develop techniques to try to break them. This presentation will introduce recent work in this area from our research group.

Erik Mårtensson, LTH

Sponsored by: SICS South

Compositional Reasoning for Information-Flow Control
I will briefly outline the state-of-the-art for proving that programs satisfy information-flow security properties. I demonstrate that the properties enforced by these approaches fall victim to a caveat: they are (generally) not preserved under composition. Thus, these approaches do not scale to large programs. Finally, I will outline my ongoing research on addressing this situation: I show properties that can be preserved under composition (and highlight how these properties dodge the above-mentioned caveat), show that these properties can be enforced at compile-time and at run-time, give examples of composition operators (which include concurrency and state) that preserve these properties, and show how these operators can be used to implement an enforcement (Secure Multi-Execution, which becomes sound by construction).
Willard Rafnsson, ITU

How we accidentally did sequential composition
The aim of compositional reasoning for security is to verify the security of components in isolation and then use a composition theorem to show that the composed system is also secure. The simplest form is parallel composition: running several security protocols over the same communication medium, where these protocols have nothing to do with each other except maybe sharing a fixed infrastructure of keys. So far, the results in this area concern simple protocols without a global state. More complicated is sequential composition where one protocol establishes a new session key and another protocol uses that key. So far, the results in this area support only simple protocols without a global state and with a clearly defined point of interaction, namely the session key that has to be authenticated and confidential. Our work concerns more complicated protocols that have a global state in form of sets of messages. An example is a database of a keyserver that maintains for each user a database of valid and of revoked public keys. Users may generate new keys and register them with the server or update them, revoking an old key. The databases may be shared between several protocols, e.g., we may have several protocols that involve the server to make updates to the database. The databases may also be shared between different users to model shared storage. This is a generalization of previous parallel composition results in that it allows the interaction between the protocols through shared sets. An important contribution is a general and declarative way to reason about this interaction: when verifying the individual protocols, we have to take into account that they run in an environment they may make changes to the shared sets, leading to an assume-guarantee-style reasoning. The core of the result is formalized in the Isabelle theorem prover. While our focus was entirely on parallel composition, this actually also covers most of sequential composition: we can see this as a special case where one protocol negotiates new session keys and puts them into a set and another protocol consumes them from this set. The assume-guarantee on this set is then that only authentic and secret keys are entered into this set and that no key may be leaked while it is in the set. This generalizes how the sequential protocols interact with each other (in fact, it does not need to be sequential) and it also simplifies the conditions and reasoning about the interaction (and thus the proofs of the compositionality theorems).
Sebastian Alexander Mödersheim, DTU

Encryption and Reversible Computations
Encryption is a special case of conditional loss-less transformation and is, thus, interesting to study from the perspective of reversible computations. We show some of the advantages of implementing encryption algorithms in a reversible language; here exemplified with implementing in Janus several symmetric lightweight encryption algorithms. We not only get both encryption and decryption programs with less implementation time, but also sketch how to translate the Janus program to a low-level program, which is then intended to be used to formally show the absence of state information leakage. This shows a way to use reversible programming to increase resilience to some side-channel attacks and give prospects for writing more secure algorithms in the future.
Authors: Dominik Taborsky, Ken Friis Larsen, Michael Kirkedal Thomsen

Sponsored by: SICS South