Cryptanalysis of Ubiquitous Computing Systems
(CRYPTACUS)
COST ACTION IC1403

2nd CRYPTACUS Workshop

16-18 November 2017
Radboud University, Nijmegen
The Netherlands
(https://cryptacus.cs.ru.nl)

Booklet compiled by Veelasha Moonsamy (email@veelasha.org)

Contents

Invited Talks

"Current state of high-precision EM side-channels and implications on FPGA-based cryptography", Johann Heyszl

High-precision measurement setups for the near-field magnetic field of integrated circuits at close distance allow for very precise evaluations, and attacks, on cryptographic implementations. In a sequence of publications based on FPGA implementations, we have shown the significant impact on different directions. For example, such measurements allow for dedicated attacks on asymmetric cryptographic algorithm implementations by exploiting location-properties or storage cells. Also, such measurements significantly increase the efficiency of attacks against symmetric cryptographic algorithms. While countermeasures such as dual-rail implementations seem invalidated by such side-channel analyses, leakage-resilient constructions retain a (small) protection level. Future work will show whether new such constructions will provide sufficient protection, even against such high-precision measurements

"Cache attacks: From side channels to fault attacks", Clémentine Maurice

Hardware is usually represented as an abstract layer, executing instructions and producing a result. However, hardware can pave the way to vulnerabilities at the software layer, by creating side effects on computations. Microarchitectural side-channel attacks exploit microarchitectural properties of IT systems in order to reveal secret values that are processed by the systems, without any physical access to the device. The CPU cache is a component of choice for an attacker to launch side-channel attacks, as the last-level cache is shared across cores of the same CPU in modern processors. In this presentation, we start by detailing state-of-the-art cache attacks such as Flush+Reload and Prime+Probe. Some of these attacks are rendered difficult by the fact that the last-level cache addressing function and the replacement policy is undocumented in modern Intel processors. We detail these challenges and how we solve them, as well as how we use this knowledge to perform a fault attack on the DRAM, known as Rowhammer, from JavaScript

"State of the Art in Lightweight Symmetric Cryptography", **Léo Perrin**

Lightweight cryptography has been one of the "hot topics" in symmetric cryptography in the recent years. A huge number of lightweight algorithms have been published, standardized and/or used in commercial products. In this talk, we present different "lightweight" algorithms corresponding to different niches of the design space and present some lessons we can learn from them.

First, A5-GCM1 and A5-GCM-2 illustrate what should not be done when designing such a primitive. Both are proprietary algorithms used in competing standards for satellite phone communication. Though initially secret, they were reverse-engineered and, quickly thereafter, attacked with practical complexity. Many other proprietary algorithms are used in contexts where performances play a crucial role and, unfortunately, most of them do not offer a security level comparable to that of, say, the AES.

Then, we turn our attention to Plantlet and LEA. Both are specialized algorithms optimized with a clear target in mind. Plantlet is a stream cipher designed to minimize its area requirement in hardware as much as possible. On the other hand, LEA is one of the most efficient block cipher on micro-controllers, due in part to its use of the ARX paradigm. This optimization influences both the choice of the primitive (for example, a stream cipher like Plantlet can only provide privacy) and the choice of its internal components (ARX primitives are easy to implement efficiently in software).

Finally, we look at a do-it-all algorithm, GIMLI. Its versatility can be seen both at the functional level—it is a sponge permutation, meaning that it can easily provide encryption, authentication, a PRNG, etc—and at the implementation level: its round function is intended to provide a compromise allowing an efficient implementation on all platforms at once. However, an attack targeting 22.5 out of 24 of its rounds was found shortly after its publication. It reminds us that, even for algorithms published after peer review, external cryptanalysis is a necessity. In fact, several lightweight block ciphers from academia have been broken such as Klein or Zorro.

"Towards Low Energy Block Ciphers", **Francesco Regazzoni**

In the last decade, several lightweight block ciphers and hash functions have been proposed. Different metrics have been used to evaluate their performances, including area, power consumption, and energy. Among them, energy is certainly the one which received least attention. Energy, however, is a crucial parameter for for battery operated devices, and will certainly be much more relevant in the near future, when billions of IoT devices will be deployed everywhere and connected to the network.

This talk presents several approaches that can be applied to block ciphers for minimizing their energy consumption. Firstly, we will present advances of technological libraries and design tools, and we discuss if and how they could be useful for reducing the energy consumption of cryptographic functions. Secondly, we will see how energy minimization could be tackled at architectural level, discussing energy efficient implementations of block ciphers.

The final idea we discuss consists in designing new block ciphers, having low energy in mind since the beginning. To this end, the talks will present the reasoning behind the design of Midori, the first block cipher designed to optimize the energy consumed per bit in encryption or decryption operation. The work presented in the talk was mainly carried out by Subhadeep Banik, Andrey Bogdanov, and Francesco Regazzoni.

Session I: Distance-bounding and RFID security protocols

"An optimal distance bounding protocol based on pre-computation", Sjouke Mauw, Jorge Toro-Pozo and Rolando Trujillo-Rasua

Distance bounding protocols use the round trip time of a challenge-response cycle to provide an upper bound on the distance between prover and verifier. In order to obtain an accurate upper bound, the computation time at the prover's side should be minimum, which can be achieved by precomputing the responses and storing them in a lookup table. However, such lookup-based distance bounding protocols suffer from a trade-off between security and the size of the lookup table. For instance, the Tree-based protocol by Avoine and Tchamkerten provides an optimal mafia-fraud security level of $\frac{1}{2n}\ (1+\frac{n}{2})$ (where n is the number of rounds) at the cost of an exponential amount of memory. In the context of resource constrained systems this may not be the most appropriate protocol. In this talk, we will analyse this security-memory trade-off, and show a novel protocol that strikes optimal resistance to mafia fraud given a bound on the size of the protocol.

"Performance Evaluation of an Advanced Man-in-the-Middle Attack Against Certain HB Authentication Protocols", Miodrag J. Mihaljević, Siniša Tomović and Milica Kneević

We consider Man-in-the-Middle (MIM) attacks against certain HB authentication protocols [1] which consists of the following three phases proposed in [2]: (i) estimation the weight of the error vector based on the rejection rate after number of modified authentication sessions; (ii) recovering i-th bit of the error vector based on the estimated weight of and the rejection rate after an additional number of modified authentication sessions where i-th position of the error vector is flipped, i = 1, 2, ..., m; (iii) construction and solving a system of linear equations where unknowns are the secret key bits. The MIM attack reported in [2], we call OOV MIM attack, and the considered advanced one have the same phase (i). Phase (ii) of OOV MIM attack is based on an approximation and employment inversion of the Gaussian function. Phase (ii) of the considered advanced MIM attack is based on employment of optimal Bayesian decision which minimizes the probability of error. Phase (iii) of OOV MIM attack employs a straightforward solving of the system of equations, and this phase of the advanced MIM attack is based on dedicated part-by-part solving the system of equations. The phase (iii) of advanced approach is based on the following: Entire system of equations could be split into subsystems, and each subsystem could be solved and checked independently: Independent solving and checking the solutions provides that higher probability of error in estimation of bits in the vector of noise is tolerated and consequently opens door for reduction of the attack complexity.

This talk provides performance evaluation of the advanced MIM attack and its comparison with OOV MIM attack.

References

[1] H. Gilbert, M. J. B. Robshaw, and Y. Seurin, *HB#: increasing the security and efficiency of HB+*, in Advances in Cryptology - EUROCRYPT 2008, N. Smart, Ed., vol. 4965 of Lecture Notes in Computer Science, pp. 361–378, Springer, Heidelberg, Germany, 2008.

[2] K. Ouafi, R. Overbeck, and S. Vaudenay, *On the security of HB# against a man-in-the- middle attack*, in Advances in Cryptology - ASIACRYPT 2008, J. Pieprzyk, Ed., vol. 5350 of Lecture Notes in Computer Science, pp. 108–124, Springer, Heidelberg, Germany, 2008.

"IoT HoneyBot: a novel approach to detection and handling of IoT-based DDoS attacks", Haris Šemić and Sasa Mrdovic

This presentation shows a novel, work-in-progress implementation of a system, which employs multiple honeypots and a command server that utilizes machine learning to detect new attack types or possible large-scale DDoS attacks in their early phase, called the "IoT HoneyBot". The implementation is continuation on an already completed master thesis project that involved constructing a honeypot system to mimic IoT devices with the goal of coping with manual and Mirai-based telnet attacks.

Description: Current implementation consists of `Node.js` front-end, which interacts with attackers, and Python back-end which reports and stores logs. Two scripts, essentially two honeypots, comprise the front-end. The first one is tasked with handling manually created malicious traffic, e.g. a human attacker who manually connects to our honeypot using the telnet command.

The manual component gives the attacker a fictitious terminal that includes fake login banner, command responses and file system. It uses a complementary file which defines these aspects of emulation. If emulation of another device is required, one needs only to run this component with dedicated file for that device; no code modifications are needed. The second script handles Mirai traffic through recon and infect phases. It faithfully recreates responses that Mirai expects in each phase, making the Mirai bot conclude that it is connected to a valid device.

The back-end is a Python script which receives log data from the front-end, decrypts it, transforms it into readable form, reports it to the user and stores it permanently. It also contains the list of username-password combinations which it uses to validate login attempts. We stationed this component behind a firewall to enhance the data protection, but other deployment strategies are possible. All communication between front-end and back-end is encrypted using AES-256.

Based on this approach, we propose an idea for future upgrade of said master thesis honeypot project, which would be called "IoT HoneyBot". The system would be organized in a similar way to malicious client-server botnets; there would be one protected command server and a large number of deployed front-end components. Each front-end component would handle incoming traffic and report it to the central server, operate with at least SSH and telnet protocols, and would use configuration attained from the command server to define which IoT device/OS that component should emulate. The command server would also receive and handle log data. Encryption would be used to secure the communication between honeypot bots and the server.

The main upgrade regarding the system behavior is usage of machine learning techniques to identify new types of attacks. Whenever unknown data is received, not attributable to a known attack type, a response from a database of already known attacks would be picked, based on the input or randomly, and sent to the attacker. Wrong response would result in an interrupted session, since attack would most likely be cancelled by the attacker. Thus, cooperation of multiple honeypot bots would speed up the learning process in case of an attack involving multiple targets. Connections between bots would be allowed to study how certain malware propagates. All received data would be collected for further analysis by the user.

After learning process is done and new attack added to the database, the configuration files

would be updated to allow for handling of this new type of attack. The new, updated configuration files would be usable by every honeypot bot, depending on which bot the user wishes to emulate which device. This process would allow for future capturing/detection capabilities towards larger collection of malicious traffic.

Another important functionality of the IoT HoneyBot would be prevention/detection of an incoming DDoS attack. Based on received traffic and how many honeypot bots are affected by it in a certain period of time, an analysis could be conducted to determine whether there is an impending danger of a DDoS attack in the near future and what could be its possible targets. Successful analysis would enable us to prevent any further damage.

The specific maximum number of supported honeypot bots would depend mainly on hardware used for HoneyBot deployment. Our current implementation already operates using threads, which enables handling multiple connections at the same time. Data from multiple connections is distinctly separated and easily readable, even when multiple connections are established from the same IP address. Current logging model consists of a separate log file for each unique IP address, allowing for access to entire history of attacks originating from one common source. This model would be expanded with a module solely dedicated to storing command-response pairs for easier analysis of new attack types.

Deploying a large group of honeypot nodes in this fashion would allow for much more detailed analysis of large-scale threats that target multiple IoT devices and use them for malicious purposes. It would enable us to determine propagation paths of various malwares, vulnerabilities of specific devices to any specific malware, intercommunication of infected IoT devices and learn to cope with new attacks faster. We believe that this system would contribute towards improvement of global Internet security.

"On symbolic verification of distance-bounding protocols", Sjouke Mauw, Zach Smith, Jorge Toro-Pozo and Rolando Trujillo-Rasua

Contactless systems are gaining more and more popularity nowadays. An increasing number of applications, including ticketing, access control, e-passports, tracking services, and mobile payments, make use of contactless communication technologies such as RFID and NFC. However, contactless communication is known to be vulnerable to *relay attacks* [6]: a man-in-the-middle attack where an adversary relays the verbatim messages that are being exchanged through the network.

To face relay attacks, Desmedt et al. [2, 3] introduced the notion of *distance- bounding protocols*. These are cryptographic protocols that securely establish an upper bound on the physical distance between a verifier and one or more provers.

Existing symbolic verification frameworks for distance-bounding protocols consider the agents' actions occurrence time and the agents' *location*. One of these frameworks is the one proposed by Basin et al. [1, 9] whose implementation is written in an adapted version of the higher-order theorem-proving tool Isabelle/HOL [8].

On the basis of Basin et al's approach, we introduce a definition of secure distance-bounding that discards the notions of time and location. Instead, it considers the causal ordering of events. This allows us to verify the correctness of distance-bounding protocols with standard protocol verification tools such as Tamarin [7], ProVerif [4] and Scyther [5]. That is to say, we provide the first *fully automated* verification framework for distance-bounding protocols. By using our framework, we confirmed known vulnerabilities in a number of protocols and discovered unreported attacks against two recently published protocols.

References

[1] D. A. Basin, S. Capkun, P. Schaller, and B. Schmidt, *Let's get physical: Models and methods for real-world security protocols*, in TPHOLs'09, pages 1–22, 2009.

[2] S. Bengio, G. Brassard, Y. Desmedt, C. Goutier, and J.- J. Quisquater, *Secure implementations of identification systems*, in Journal of Cryptology, 4(3):175–183, 1991.

[3] T. Beth and Y. Desmedt, *Identification tokens - or: Solving the chess grandmaster problem*, in CRYPTO'90, pages 169–177, 1990.

[4] B. Blanchet, *An Efficient Cryptographic Protocol Verifier Based on Prolog Rules*, in CSFW'01, pages 82–96, 2001.

[5] C, J. F. Cremers, *The Scyther tool: Verification, falsification, and analysis of security protocols*, in CAV'08, pages 414–418, 2008.

[6] Y. Desmedt, C. Goutier, and S. Bengio, *Special uses and abuses of the fiat-shamir passport protocol*, in CRYPTO'87, pages 21–39, 1987.

[7] S. Meier, B. Schmidt, C. Cremers, and D. A. Basin, *The TAMARIN prover for the symbolic analysis of security protocols*, in CAV'13, pages 696–701, 2013.

[8] T. Nipkow, L. C. Paulson, and M. Wenzel, *Isabelle/HOL - A Proof Assistant for Higher-Order Logic*, volume 2283 of LNCS. Springer, 2002.

[9] P. Schaller, B. Schmidt, D. A. Basin, and S. Capkun, *Modeling and verifying physical properties of security protocols for wireless networks*, in CSF'09, pages 109–123, 2009.

"Confusion and Diffusion in Recent Ultralightweight RFID Authentication Protocols", Paolo D'Arco and Roberto De Prisco

Secure authentication is a well-established research area in cryptography and several good solutions are available and used every day. Unfortunately, for low-cost inexpensive computing elements, like RFID tags, it is a quite challenging problem. The hardware imposes very strong constraints on the computing capabilities of the small elements. Hence, standardized techniques based on public key cryptography or on symmetric key primitives cannot be employed in the design.

Due to the above constraints, there are two choices: either to give up because it is difficult (if not even impossible) to achieve the security standard we get in other levels of our digital infrastructure, or to try to achieve a *reasonable* security level also in applications using these cheap computing elements. Indeed, it is redundant to say that they are becoming a crucial end point of smart automated solutions within the so-called "Internet of Things".

The current state of knowledge is quite poor: we do not have any impossibility result within a model for such ultralightweight protocols but, at the same time, all ultralightweight authentication protocols, designed according to some ad-hoc approach, proposed in the last years, have been analyzed and weaknesses of different significance and impact have been quickly found and used to break the protocols.

In some papers many warnings have been rised against such ad hoc solutions. In [2] a full analysis of one of the most representative ultralightweight authentication protocol at that time was provided, and in general the limits of such an ad hoc approach, not based on sound security arguments, were stressed. Moreover recently, in [1], a full guide to the common pitfalls which are usually present in the design of ultralightweight authentication protocols has been provided to designers and practitioners. Nevertheless, ad-hoc protocols with informal security analyses continue to be presented at a considerable rate and they are broken quickly after publication.

Compared to the first protocol proposals of the last years, the *new feature* which almost all of them exhibit is that some *more involved* transforms of the data stored in the tag memory are used in order to construct the messages the Reader and the Tag send to each other to be confident of the reciprocal identities. However, as before, also for these sort of generation 2.0 ultralightweight authentication protocols, the informal security analyses are based solely on the following, questionable and very weak, conclusion: since the transforms are complex, only the legal parts who share the secret keys can produce the correct messages required by the authentication protocol; for the same reason, no adversarial entity, without the secret keys, can be successful with non negligible probability, that is, the best attack that can be applied is to guess the secret keys, which belong to an exponentially large set. In other words the entire security proof, in most cases, reduces to the *alleged complexity* of the transforms.

Contribution: We analyze some of the most recent ultralightweight authentication protocols which uses such transforms, and we show that all of them have some weaknesses which can be used to mount very efficient attacks. We also point out that the crucial point is that such transforms achieve *poor confusion and diffusion*. And an adversary can build ad hoc attacks to reduce from exponential to constant the number of trials needed to break a target authentication protocol.

Transforms analysis and attacks. Lightweight protocols use bit manipulation operations to protect the secret values used for computing the messages the parties send to each other. We review the transforms used in various protocols and provide results that can be used for attacks. More specifically, we describe and analyze the following transforms: the pseudo-Kasami code transform `Kc`, used in [4], the recursive hash transform `Rh`, used in [5, 6], the conversion transform `Con`, used in [3], and a transform based on a Feistel cipher [7]. We show that all of them present some weaknesses which can be used to efficiently defeat the protocols.

- **KMAP.** The protocol KMAP, introduced in [4], is a mutual authentication protocol. According to the authors, "KMAP avoids unbalanced logical operations (or, and) and introduces a new ultralightweight primitive, the pseudo-Kasami code, which enhances the diffusion properties of the protocol messages and makes the Hamming weight of the secrets unpredictable and irreversible". We exploit the weaknesses in the pseudo-Kasami transform and provide efficient attacks against some of the security properties of the protocol.

- **RCIA.** The protocol RCIA, introduced in [5], is a mutual authentication protocol. In RCIA, tags use only three main operations, the bitwise and, or, and bit rotation, and a non-triangular recursive hash transform. We exploit the insights on the recursive hash function transform and we provide an efficient impersonation attack.

- **SASI$^+$.** The protocol SASI$^+$, introduced in [6], is a mutual authentication protocol. It incorporates only bitwise operations, xor, rotation and, like RCIA, the recursive hash transform. We show how to mount an impersonation attack leveraging on RCIA weaknesses.

- **SLAP.** The protocol SLAP, introduced in [3], uses only bitwise operations like xor and rotation and a conversion transform. The authors stress that the conversion transform is the main security component of the system "with properties such as irreversibility, sensibility, full confusion and low complexity", with better performance compared to previous protocols if they are not absent at all. Also for this protocol we exploit the weaknesses of the transform and provide an efficient impersonation attack.

- **FCS-based Protocol.** Very recently, in [7], the authors have proposed a lightweight transform based on the structure of a Feistel Cipher. The approach is quite interesting because it suggests in the design of an ultralightweight protocol the use in a light form of well-known techniques in the standard symmetric key setting. Unfortunately, the specific choices in the design of the round function in the FCS-based transform, produce a weak transform. In particular, the transform is not pseudorandom in a cryptographic sense: an efficient distinguisher can take apart it from a truly random function. Again, the distinguisher leverages on the poor confusion and diffusion achieved by the transform.

Acknowledgement. We thank Domenico Desiato and Giovanni Ciampi for implementing in C language the attacks during their thesis work, providing us useful experimental data and insights.

References

[1] G. Avoine, X. Carpenter and J. Hernandez-Castro. Pitfalls in Ultralightweight Authentication Protocol Designs. *IEEE Transactions on Mobile Computing*. DOI 10.1109/TMC.2015.2492553

[2] P. D'Arco and A. De Santis. On Ultralightweight Rfid Authentication Protocols. *IEEE Transactions on Dependable and Secure Computing*. Vol. 8, No. 4, pp. 548–563, 2011.

[3] H. Luo, G. Wen, J. Su, Z. Huang. SLAP: Succint and Lightweight Authentication Protocol for Low-Cost RFID System. *Wireless Netw*, DOI 10.1007/s11276-016-1323-y, Springer, 2016.

[4] U. Mujahid, M. Najam-ul-Islam, S. Sarwar. A New Ultrlightweight RFID Authentication Protocol for Passive Low Cost Tags: KMAP. *Wireless Personal Communication*, Springer, 2016.

[5] U. Mujahid, M. Najam-ul-Islam, M. Ali Shami. RCIA: A New Ultralightweight RFID Authentication Protocol Using Recursive Hash. *International Journal of Distributed Sensor Networks*, Hindawi, 2015.

[6] U. Mujahid, M. Najam-ul-Islam, A. Raza Jafri, Qurat-ulAin, M. Ali Shami. A New Ultralightweight RFID Mutual Authentication Protocol: SASI Using Recursive Hash. *International Journal of Distributed Sensor Networks*, Hindawi, 2016.

[7] B. Mustapha, M. Djeddou and K. Drouiche. An ultralightweight RFID authentication protocol based on Feistel cipher structure. *Security and Communication Networks*, John Wiley & son, 2017, DOI: 10.1002/sec.1754

[8] M. Safkhani and N. Bagheri. Generalized Desynchronization Attack on UMAP: Application to RCIA, KMAP, SLAP and SASI$^+$ Protocols. Available on the eprint archive, September 2016.

Session II: Other lightweight protocols

"Rescuing LoRaWAN 1.0", Gildas Avoine and Loic Ferreira

In parallel with the coming up of the Internet of Things, several communication protocols have been proposed, which technical specifics differ depending on the intended use case. For instance the Bluetooth wireless protocol allows only short distance communication (several meters). Technologies such as ZigBee or Z-Wave afford medium range distance communication (roughly a hundred meters) and aim at reducing the energy needed by the nodes to set up and maintain a mesh network.

As for long range distance communication (several kilometers), proposals have been made, such as LoRa. LoRa, developed by Semtech company, aims to set up a Low-Power Wide-Area Network (LPWAN), based on a long range, low rate, wireless technology. It is somewhat similar to a cellular technology (2G/3G/4G mobile systems) but optimised for IoT/M2M. LoRa does not require a spectrum license since it uses free (but regulated) radio spectrum (*e.g.*, 863-870 MHz in Europe, 902-928 MHz in the USA, 779-787 MHz in China). A LoRa device, with an autonomous power-supply, is supposed to communicate through several kilometers in an urban area, and to have a lifespan up to eight or ten years. LoRaWAN is a protocol aiming at securing the Medium Access Control layer of a LoRa network. It is designed by the LoRa Alliance, an association gathering more than 400 members (telecom operators, semiconductor manufacturers, digital security companies, hardware manufacturers, network suppliers, etc.).

Public and private LoRaWAN networks are deployed in more than 50 countries worldwide by telecom operators (SK Telecom, FastNet, ZTE, KPN, Orange, Proximus, etc.), private providers (*e.g.*, LORIOT.io), and private initiatives (*e.g.*, The Things Network). Several nationwide networks are already deployed in Europe (France, Netherlands), Asia (South Korea), Africa (South Africa), Oceania (New Zealand), providing coverage to at least half of the population. Trials are launched in Japan, the USA (starting with a hundred cities), China (the expected coverage extend to 100 million homes and 300 million people), India (the first phase network aims to cover 400 million people across the country). The version 1.0.1 followed by version 1.0.2 of the LoRaWAN specification have been released in 2016. In this paper we focus on this last version which is the released 1.0 version currently worldwide deployed.

Our contribution is twofold. Firstly we provide an extensive analysis of the protocol and show it suffers from several weaknesses. Then we describe how attacks, not only theoretical but also practical, based on the protocol flaws may be performed. Secondly we provide several recommendations aiming at mitigating the attacks while at the same time keeping the interoperability between a patched equipment and a non modified one. Our results show that all the attacks we describe may be thwarted if the recommended corrections are applied to the NS and the devices.

We emphasise that the aforementioned attacks, due to the protocol weaknesses, do not lean on potential implementation or hardware bugs, and are likely to be successful against any equipment implementing LoRaWAN 1.0. Likewise the attacks do not entail a physical access to the targeted equipment and are independent from the means used to protect secret values (*e.g.*, using a tamper resistant module such as a Secure Element). Thus our attacker, standing between a LoRaWAN device and the NS, needs only to act on the air interface: she needs to eavesdrop on data exchanged between the device and the server, and to send data to these equipment. In particular the attacker do not need to get a physical access to the targeted device (or server).

We think that the countermeasures we propose represent straightforward changes to be implemented. We present new attacks against LoRaWAN 1.0, and for each of them we provide a precise description of its goal, its implementation, the technical means used, and the tangible consequences. Moreover our attacks do not lean on strong assumptions such as the ability to get a physical access to, and to monitor a device or the NS. In addition we describe attacks targeting either a device or the NS. The attacks and their precise description, the adversary model (which does not imply a physical access to any equipment, in particular the device), and the two kinds of targeted equipment (device and server) are the main aspects

that differentiate our work compared to previous works.

Session III: Hardware and software security engineering

"Cryptographic Hardware from Untrusted Components", Vasilios Mavroudis, Andrea Cerulli, Petr Svenda, Dan Cvrcek, Dusan Klinec and George Danezis

The semiconductor industry is fully globalized, and integrated circuits (ICs) are commonly defined, designed and fabricated in different premises across the world. This reduces production costs, but also exposes ICs to supply chain attacks, where insiders introduce malicious circuitry into the final products. As a result, the security of critical systems that rely on such ICs for cryptographic operations is jeopardized. Existing detection and prevention techniques are brittle, as new threats are able to circumvent them quickly or come with unrealistically high manufacturing costs and complexity.This work follows a different approach and introduces a novel high-level architecture that enables cryptographic devices to maintain their security properties in the presence of malicious hardware components.

Unlike prior mitigation efforts that focused on detecting or preventing errors, our work proposes Myst, an architecture that utilizes cryptographic schemes to distribute trust between multiple ICs, sourced from different supply chains. This ensures that unless an adversary manages to breach all these supply chains, the device remains secure. Our architecture is directly applicable in many critical systems with high-security needs that use secure crypto-processors to carry out sensitive tasks (e.g., key generation and storage, digital signing) or to maintain a protective layer against cyber-attacks and security breaches. For instance, banking infrastructure, military equipment and even space stations that utilize crypto-processors embedded into Hardware Security Modules, Trusted Platform Modules and Cryptographic Accelerators.

Our key insight is that by combining established privacy enhancing technologies (PETs), with mature fault-tolerant system architectures, we can distribute trust between multiple components originating from non-crossing supply chains, thus reducing the likelihood of compromises. To achieve this, we deploy cryptographic schemes on top of an N-variant system architecture, and build a trusted platform that supports a wide-range of commonly used cryptographic operations (e.g., random number and key generation, decryption, signing). However, unlike N-variant systems, instead of replicating the computations on all processing units, Myst uses multi-party cryptographic schemes so that each IC holds only a share of each secret (and not the whole secret itself). Hence, as long as one of the components remains honest, the secret cannot be reconstructed or leaked.

Our proposed architecture is of particular interest for two distinct categories of hardware vendors:

- Design houses that outsource the fabrication of their ICs.
- Manufacturers that rely on commercial off-the-shelf components to build their high-assurance hardware.

Design houses have much better control over the IC fabrication and the supply chain, and this allows them to take full advantage of our architecture. In particular, they can combine existing detection and prevention techniques with our proposed design, to reduce the likelihood of compromises for individual components. On the other hand, commercial off-the-shelf vendors have less control as they have limited visibility in the fabrication process and the supply chain. However, they can still mitigate risk by using ICs from sources, known to run their own fabrication facilities. To our knowledge, this is the first work that combines cryptographic schemes with an N-variant design, to build and evaluate a hardware module architecture that is tolerant to multiple components carrying trojans or errors. To achieve that, we introduce a distributed variant of Schnorr blind signatures that enables Myst to remain competitive in terms of performance compared to single-IC systems. For our evaluation, we build a custom board featuring 120 highly tamper-resistant ICs, and use it to benchmark the performance and reliability of the system in random number and key generation, public key decryption and signing.

"Scalable Key Rank Estimation and Key Enumeration Algorithm for Large Keys",
Vincent Grosso

Evaluation of security margins after a side-channel attack is an important step of side-channel resistance evaluation. The security margin indicates the brute force effort needed to recover the key given the leakages. In the recent years, several solutions for key rank estimation algorithms have been proposed. All these solutions give an interesting trade-off between the tightness of the result and the time complexity for symmetric key. Unfortunately, none of them has a linear complexity in the number of subkeys, that make these solutions slow for large (asymmetric) keys. In this paper, we present a solution to obtain a key rank estimation algorithm with a reasonable trade-off between the efficiency and the tightness that is suitable for large keys. Moreover , by applying backtracking we obtain a parallel key enumeration algorithm.

Side-channel attacks are powerful attacks against cryptographic implementations. To perform a side-channel attack, an attacker needs to be able to measure some physical properties (e.g. power consumption, electromagnetic radiation) of the device while it is computing some operations. With this additional information, some attacks can be performed against cryptographic implementations. This kind of attack has been used to mount some attack against real devices [1]. Hence, having secure implementations for cryptographic algorithms is required.

To defeat side-channel attacks, cryptographic implementations should embed appropriate countermeasures. The security margins that the countermeasures offer should be tested. For that evaluation lab generally launch some popular attacks to evaluate if an adversary can break an implementation by performing, for example, a key recovery attack. This is adapted since the leakage of an implementation highly dependents on the device. Hence, the security obtained by the implementation is highly dependent on the underlying device.

Most of state of the art side-channel attacks follows a divide-and-conquer strategy, where the master key is split into several pieces, called subkeys. The attacker/evaluator mounts an independent attack for each of these subkeys. A security evaluation only based on a success or failure of a key recovery attack is limited by the computational power of the evaluator. To get rid of this limitation a solution is to compute the rank of the key instead of performing a key recovery attack. The rank corresponds to the number of keys needed to be tested before recovering the actual key. Recently, several papers study how to evaluate the security by evaluating the computational power required after a side-channel attack [2, 3, 4, 5]. These papers compute an estimation of the rank of the key after a side-channel attack, without being limited by the evaluator computational power. All these papers focus on symmetric key size. In [3] the authors managed to evaluate ranks for 1024-bit keys, but for larger keys this solution could have some limitations.

Our contributions. We study the cost of the solution of Glowacz et al. for large keys. Next, we present a variation of this key rank estimation algorithm. This variation allows us to obtain a linear complexity of the algorithm in the number of subkeys. To the best of our knowledge it is the first efficient key ranking algorithm to offer such complexity. We then derive some tighter bound for our construction. These tight bounds allow us to have an efficient and tight solution for key rank estimation for large keys (size greater than 1024 bits). Remark our method offers a trade-off between efficiency and tightness of the result. That is a new feature for large key evaluation as the only efficient solution of Choudary and Popescu [6] can not tighten the bounds provide.

Finally by applying similar idea as Poussier et.al [7], we show that our key rank algorithm can be transformed to a key enumeration algorithm.

References

[1] Junrong Liu, Yu Yu, François-Xavier Standaert, Zheng Guo, Dawu Gu, Wei Sun, Yijie Ge, and Xinjun Xie, *Small tweaks do not help: Differential power analysis of MILENAGE implementations in 3G/4G USIM cards*, in Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I, volume 9326 of Lecture Notes in Computer Science, pages 468?480. Springer, 2015.

[2] Daniel J. Bernstein, Tanja Lange, and Christine van Vredendaal, *Tighter, faster, simpler side-channel security evaluations beyond computing power* in IACR Cryptology ePrint Archive, 2015:221, 2015.

[3] Cezary Glowacz, Vincent Grosso, Romain Poussier, Joachim Schüth, and François-Xavier Standaert, *Simpler and more efficient rank estimation for side-channel security assessment*, in Gregor Leander, editor, Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers, volume 9054 of Lecture Notes in Computer Science, pages 117?129. Springer, 2015.

[4] Daniel P. Martin, Jonathan F. O'Connell, Elisabeth Oswald, and Martijn Stam, *Counting keys in parallel after a side channel attack*, in Tetsu Iwata and Jung Hee Cheon, editors, Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II, volume 9453 of Lecture Notes in Computer Science, pages 313?337. Springer, 2015.

[5] Nicolas Veyrat-Charvillon, Benoît Gérard, and François-Xavier Standaert, *Security evaluations beyond computing power*, in Thomas Johansson and Phong Q. Nguyen, editors, Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, volume 7881 of Lecture Notes in Computer Science, pages 126?141. Springer, 2013.

[6] Marios O. Choudary and P. G. Popescu, *Back to massey: Impressively fast, scalable and tight security evaluation tools*, in Wieland Fischer and Naofumi Homma, editors, Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings, volume 10529 of Lecture Notes in Computer Science, pages 367?386. Springer, 2017.

[7] Romain Poussier, François-Xavier Standaert, and Vincent Grosso, *Simple key enumeration (and rank estimation) using histograms: An integrated approach*, in Benedikt Gierlichs and Axel Y. Poschmann, editors, Cryptographic Hardware and Embedded Systems - CHES 2016 - 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings, volume 9813 of Lecture Notes in Computer Science, pages 61?81. Springer, 2016.

"A Leakage Trace Collection Approach for Arbitrary Cryptographic IP Cores",

Athanassios Moschos, Apostolos Fournaris and Nicolas Sklavos

As the need for security in ubiquitous computing systems becomes evident, many such devices are equipped with hardware security tokens featuring cryptographic IP cores. Such tokens and their IP core tend to leak sensitive information that if collected can reveal such information using Side Channel Analysis Attacks (SCAs). To evaluate such systems against SCAs and overall leakage, security engineers must collect a considerable amount of DUT leakage traces, to grade the applicability of popular SCAs like Differential Power Analysis (DPA), Correlation DPA [1] or Mutual Information Analysis (MIA) [2], as well as perform information theoretic leakage/vulnerability tests (mutual information tests or leakage statistic order t-tests/Welch t-tests).

The highly-specialized skills required for the evaluation of ubiquitous computing system device security components become a true barrier for the identification of additional security issues. This obstacle is strengthened by the lack of an overall platform that would enable the estimation of information leakage from different devices. While in theory, the testing approach as well as the employed trace collection tool-set can be designed exclusively for a specific cryptographic implementation (e.g. AES, RSA etc.), in practice, experienced SCA analysts require a generic and flexible tool-set and DUT leakage evaluator (e.g. test vector leakage assessment, TVLA, [3, 4] and its variations [5, 6]), that needs to be easily adapted to the DUT they are currently evaluating [7] and still be able to collect huge amount of traces in a reasonably fast way.

There exists a restricted number of trace collection platforms to be used for testing DUTs either for specific SCAs or overall leakage. Open source SCA setups that are widely used by the research community [8, 9] have either very primitive software/hardware support or they are built on low-cost equipment that cannot endure very sophisticated attacks without having considerable custom software code developed by an attacker. To collect huge amounts of traces (e.g. leakage assessment requires millions of traces [5]) in reasonable time, custom hardware control mechanisms on a platform are developed specifically for the respective DUT's cryptographic algorithm implementation, to provide the appropriate DUT test vector inputs. This considerably increases the development time of the control mechanism (a different control implementation for each crypto-algorithm on test) and restricts its re-usability. Industrial SCA evaluation players offer their own proprietary equipment (Riscure [10], CRI [11]) partially addressing the above problem but at a cost that only high budget security labs can afford. The above trace collection approaches issues (flexibility, cost, ease-of-use, speed) highlight the need for a generic, cheap and easy, practical toolset capable of supporting the latest leakage assessment approaches, providing inputs and collecting outputs to/from a DUT in a unified way regardless of the cryptographic algorithm at hand (whether symmetric or asymmetric).

In an attempt to adapt and improve the existing leakage assessment based cryptanalytic methodologies and tools for the hardware security components to the ubiquitous computing frame work, we designed a mechanism that enables the security assessment of real-world cryptographic IP implementations, regardless of their algorithm implemented internally. We propose an architecture and a mechanism that addresses the above issues by migrating test vector generation and data transmission to the DUT, from the PC software level to the embedded system level. Our proposed system adopts the two FPGA chips isolation approach (a Control FPGA and a cryptography FPGA on a trace collection platform). We propose an embedded system architecture inside the control FPGA consisting of a fully programmable soft-core microprocessor using a reconfigurable peripheral interface that handles communication with the DUT (realized in the Cryptographic FPGA) as well as a customizable hardware interface on the cryptographic FPGA capable of translating our FPGA-to-FPGA custom protocol, to DUT inputs/outputs and commands. Using the proposed approach, the user is provided with a simple-to-use software Application Programming Interface (API) on the microprocessor which can be used to define the DUT inputs/outputs number, byte length and type (random or specific) so as to program leakage assessment and SCAs scenarios and execute them directly on embedded system thus by-passing the slow PC based run-time communication to the DUT. The proposed system can be used regardless of the DUT (supporting up to 4048 bit inputs) thus offering flexibility, reconfigurability, high scalability, fast trace collection and ease of use.

As a reference hardware board, on which to structure and implement the above described proposed architecture, the widely accepted and respected for its low noise trace collection capabilities Sakura-X board, was chosen. This board adopts the isolation between control device and DUT and features 2 FPGA chips, a Spartan 6 acting as the Control FPGA and a Kintex 7 playing the role of the victim hardware implementation. For the proposed implementation, the soft-core Xilinx Microblaze microprocessor was used, due to its broad support by Xilinx in all the firm?s FPGA chips, including SAKURA-X Xilinx Spartan-6 Control FPGA. Nevertheless, there exist various soft-core processors in the open source community or as commercial products (Leon 2/3, openSPARC, ALTERA Nios, RISK V, openRISC etc.) that can be used in the proposed architecture making this architecture applicable to a broad range of FPGA chips (any non-Xilinx Control FPGA).

Using our mechanism with various cryptographic components, the following benefits could be identified compared to the existing competition:

- The attacker is now able to practically realize the multi-encryption trace capture scenario with constant, random or chosen/fixed data sets [12].
- The realization of the multi-encryption scenario leads to large sums of captured waveforms in minimum time.
- The duration of the attack can be greatly reduced because of the ability to use in practice multi-encryption with averaging and hence use fewer traces during an attack execution [12, p.11].
- The effect of various environmental parameters on the trace capturing is minimized since massive trace acquisition can be performed in negligible time (e.g. DPA contest v2 data case [13]).
- Various attack types can be tested on the same target because the amount of time for trace collection is small and manageable. This is valuable in attack approaches that in order to be successful, they require considerable number and diverse types of traces to be collected to overcome a DUT's SCA countermeasures.
- A DUT does not need to be modified by the user to support repetition of cryptographic procedures and trace capturing. The DUT is just connected as is on the Cryptographic FPGA and repetition of cryptographic procedures is undertaken solely by the proposed interfaces.

References

[1] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards* in Advances in Information Security, Feb 2007.

[2] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, *Mutual Information Analysis* in Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 426–442.

[3] B. J. Gilbert Goodwill, J. Jaffe, and P. Rohatgi, *A Testing Methodology for Side-Channel Resistance Validation*, 2011.

[4] G. Becker, J. Cooper, E. DeMulder, G. Goodwill, J. Jaffe, G. Kenworthy, T. Kouzminov, A. Leiserson, M. Marson, P. Rohatgi et al., *Test vector leakage assessment (tvla) methodology in practice*, in International Cryptographic Module Conference, vol. 1001, 2013, p. 13.

[5] T. Schneider and A. Moradi, *Leakage assessment methodology* in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2015, pp. 495–513.

[6] F.-X. Standaert, *How (not) to use welch?s t-test in side-channel security evaluations*, in IACR Cryptology ePrint Archive, vol. 2017, p. 138, 2017.

[7] I. Kizhvatov and M. Witteman, *Academic vs. industrial perspective on SCA, and an industrial innovation*, 2013.

[8] S. Labs and M. Tech, *Sasebo/sakura project*, `http://satoh.cs.uec.ac.jp/SAKURA/index.html`

[9] C. O'Flynn and Z. D. Chen *ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research.*

[10] Riscure, *Inspector: The side channel test tool*, `https://www.riscure.com/archive/Inspector brochure.pdf`

[11] Rambus, *Dpa workstation testing platform*, `http://info.rambus.com/hubfs/rambus.com/Gated-Content/Cryptography/DPA-Workstation-Product-Brief.pdf`

[12] I. Kizhatov and M. Witteman, *Fast acquisition: Exploring the potential of a standard side channel measurement setup*, `https://www.riscure.com/documents/fastacq wp.pdf`

[13] A. Heuser, *A New Difference Method for Side-Channel Analysis with High-Dimensional Leakage Models*, CT-RSA 2012, 2012.

"FPGA Performance Optimization for CAESAR Authentication Ciphers",

Maria Katsaiti, Nicolas Sklavos and Apostolos Fournaris

Moving towards the announcement of the final CAESAR cipher, is making suspense escalate. More and more studies are focusing on comparing and contrasting the candidates that made it to the third round, while they are trying to jump to an accurate prediction of the winners. The finalists are, currently, 15 out of 57, that initially participated in 2013; their submissions have all been described in an HDL language and implemented under a common hardware API, referred as CAESAR Hardware API. Meanwhile, they ensure that they retain the three virtues every encryption algorithms guarantees; integrity, confidentiality and authenticity. This study particularly focuses on the work done by three out of fifteen finalists and how their performance can be boosted, and their speed accelerated; the candidates under examination are AES-OTR, Deoxys and OCB. Following to an introduction of the CAESAR contest and a quick overview of the ciphers individually, results and remarks are discussed in the last section of this work. As it is presented, when pipelining technique is applied on the authenticated ciphers implemented on a Virtex 6 FPGA device, an enhancement of throughput is observed universally.

Session IV: Security and privacy of real-world systems

"DECAP-Distributed Extensible Cloud Authentication Protocol", Andrea Huszti and Norbert Oláh

Cloud computing is becoming more and more important in the field of information technology, which faces many security challenges. One of the most important issues is to achieve secure users' authentication. Vulnerability of an authentication protocol results in successful attacks against confidentiality and integrity of user data stored and processed in the cloud.

In scientific papers, one-factor and two-factor authentication solutions are being used in general. In case of one-factor authentication, the user is only protected by a password that is stored in a verification table, many attacks exist against such systems. In 2000, Hwang and Li suggested a new remote user authentication scheme [5], which is based on smart cards. Instead of a password verification table they applied the ElGamal encryption scheme, but an impersonation attack was found. In 2002, Chien, Jan and Tsien proposed a password-based authentication [2], which does not use a verification table and the passwords were chosen freely. Ku and Chen proved that Chien et al's scheme was vulnerable to several attacks [6]. In 2011, Choudhury et al's showed a two-step authentication protocol [3] for cloud computing where one of the factors is the smart card and the other one is the password. They applied an out of band channel. Later, Chen and Jiang detected an impersonation attack in Choudhury et al's scheme and proposed a new authentication framework which did not use the out of band channel [1]. In practice, OpenStack is one of the most popular cloud computing software. The OpenStack Identity service supports multiple methods of authentication, including user name and password, LDAP, and external authentication methods e.g. Kerberos. There are fears about Kerberos, the so-called Golden Ticket Attack [9, 10] presented on the 2015 RSA Conference slide deck. User authentication is based on secret keys stored on the Kerberos KDC server. If an adversary has a domain or local admin access on an Active Directory domain, he might be able to get the secret key for the KDC server, a golden-ticket, and this way he can manipulate Kerberos tickets to get unauthorized access.

In our protocol called DECAP [4] a person uses a static password and a one-time password for identity verification. The main idea of DECAP is to provide shared responsibility of handling the one-time password, i.e. the one-time password is stored and shared among the cloud servers distributed. We apply a Merkle tree or hash tree for verifying the correctness of the one-time password. A Merkle tree is a binary tree where each non-leaf node is labeled with the hash value of the concatenation of its two children's labels.The protocol is formalized in the Proverif framework. With Proverif events and injective queries, we have proved that DECAP is secure against external adversaries. We show that DECAP fulfills the typical security requirements of a key exchange protocol, i.e. authentication of the participants, key secrecy, key freshness and confirmation that both parties know the new key in the Dolev-Yao model. By having avoided the asymmetric cryptography, we have achieved good efficiency results in our system.

There are three different participants in the scheme. Users ask for services from the cloud service provider. The cloud service provider consists of several cloud servers and a certificated authentication server. A cloud server which is chosen randomly performs the user authentication. The authentication server is managing the cloud servers. The protocol contains three stages: Registration, Authentication and Synchronization. During the registration phase, each user has to register for the cloud service with his smart card. The static password chosen by the user and the seed of the one-time passwords are exchanged. Since we can generate infinitely many one-time passwords, this phase is rarely executed. It is run when the static password is set and modified. In the authentication phase users verify themselves with the help of their one-time passwords and static password. The cloud server authenticates itself, as well. The MAC key is also exchanged after the mutual authentication. Only a cloudserver chosen randomly and the user participate during this phase. This phase is run a lot of times, hence it should be very efficient. By avoiding asymmetric cryptographic primitives, only hash and MAC calculations are applied for minimizing the computational overhead. There are only three interactions between the cloud server and the user. Three is the minimum

number of interactions for accomplishing the typical security requirements. The synchronization phase which is the last phase is responsible for resetting the one-time password and the hash value that verifies it. During this phase, besides the user and the cloud server chosen randomly in the previous phase, the other cloud servers and the authentication server also participate. There is no interaction between the servers and the user during this phase. The user proceeds his synchronization himself. On server side the authentication server manages the process by communicating with all cloud servers. During the phase of synchronization, due to the Merkle-tree structure the new one-time password is set efficiently, the new root node value is calculated in n steps.

References

[1] N. Chen, R. Jiang, *Security Analysis and Improvement of User Authentication Framework for Cloud Computing* in Journal of Networks, 9(1), (2014), pp. 198–203.

[2] H. Y. Chien, J. K. Jan, Y. M. Tseng, *An efficient and practical solution to remote authentication smart card* in Computers & Security, 21(4), (2002), pp. 372–375.

[3] A. J. Choudhury, P. Kumar, M. Sain, *A Strong User Authentication Framework for Cloud Computing* in Proceedings of IEEE Asia-Pacific Services Computing Conference,(2011), pp. 110–115.

[4] A. Huszti, N. Olah, *A simple authentication scheme for clouds* in Proceedings of IEEE Conference on Communications and Network Security (CNS), (2016), Pages: 565–569.

[5] M. S. Hwang, L. H. Li, *A new remote user authentication scheme using smart cards* in IEEE Transactions on Consumer Electronics, 46(1), (2000), pp. 28–30.

[6] W. C. Ku, S. M. Chen, *Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards* in IEEE Transactions on Consumer Electronics, 50(1), (2004), pp. 204–207.

[7] George Kurtz, Dmitri Alperovitch, Elia Zaitsev, *Hacking exposed: Beyond the Malware*, RSA 2015 (slide deck), `https://www.rsaconference.com/writable/presentations/file_upload/exp-t10_hackingexposedbeyondthemalware.pdf`, (2015).

[8] Miguel Soria-Machado, Didzis Abolins, Ciprian Boldea, Krzysztof Socha, *Kerberos Golden Ticket Protection, Mitigating Pass-the-Ticket on Active Directory*, CERT-EU Security Whitepaper 2014-007, (2016).

"How private is your mobile health advisor? Free popular m-Health apps under review",

Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou, Efthimios Alepis, Agusti Solanas and Constantinos Patsaki

The use of smartphones, wearables and embedded portable devices, which enable other devices to become "smarter", are continuously gaining interest and market share, and they have become ubiquitous in people's daily activities. Mobile apps have experienced a significant growth either as health promoters for fitness and health prevention, or as health calendars and advisors. Developers and publishers are providing health or medical related content and services to support and engage their users.

These emerging apps, which could be classified within the field of mobile health (m-Health) [1], create a highly sensitive ecosystem for personal data process, storage and sharing [3, 4, 5]. Moreover, due to smartphones numerous embedded sensors and advanced processing capabilities, most apps often store and process not only health-related data but other sensitive information as well, such as the user's location, his/her list of contacts and photographs, etc.

In this talk, we report our investigations on the exposure of m-health apps' users, as their core data is very sensitive and the developers of most widely used apps are expected to have integrated many protection mechanisms. Therefore, we have selected 20 of the most popular free m-Health apps in Google Play Store, based on a set of strict content, quality and installation criteria and we have performed an in-depth analysis of their behavior and sharing practices regarding the secure and private transmission of their users? data.

The major questions we have posed in our study are the following:

1. What data are shared?
2. Which entities can access users' data?
3. What data are shared with each entity?
4. Are these data transmitted securely?
5. How do developers respond to bug reports?
6. How much time do security/privacy issues take to be fixed?
7. How well prepared are we for the General Data Privacy Regulation (GDPR) enforcement?

To evaluate the apps, we have developed an assessment methodology and we have performed two rounds of tests from February 2016 to August 2017. After reporting our first results to the app vendors and we checked how many of the apps have fixed the reported issues. In addition, during our second round of assessment we checked a set of critical functional or non-functional requirements regarding the compliance with the upcoming GDPR [2] by the 19 remaining apps in Google Play Store.

Summary of main findings

Health data sharing. We have collected health-related transmitted keywords and/or phrases related to the health status or the medical condition of the user. Our experiments show that 80% (N=16) of the analyzed apps transmit users' health related data, while 20% (N=4) store them locally on the device. In terms of security, only 50% (N=8) of those apps transmit the health data over an encrypted channel.

Location privacy exposure. Our analysis shows that 7 out of the 20 apps transmit the user location. Moreover, 4 of those apps send their users' location to 5 distinct third party domains, while 3 of those transmit the location over plain HTTP. Especially, in one of the apps, which did not offer any special geolocated service to their users, two of its third parties advertisement services asked for the user's geolocation at a rate of almost one request each 3 seconds within a timeframe of approximately 12 minutes.

Passwords transmission. While 8 out of the 11 apps that ask for a password use HTTPS connections to transmit their users' passwords, we cannot conclude that all of them fully protect their users. Our findings show that many of the SSL/TLS connections that we captured have weaknesses and could not be considered fully secure. In addition, we have identified apps that transmit the passwords via GET requests even over HTTP connections.

GDPR readiness. Our study indicates that most of the apps do not comply with GDPR [2] requirements. For example, only 7 out of the 19 apps provide users with an option to withdraw their consent and, thus, they unable the erasure of any previously consented information. Additionally, only 8 out of 19 apps notify their users in advance, even before their registration, that they are sharing data with third parties.

Our results indicate that most of the applications do not follow well-known practices and guidelines, exposing, thus, the privacy of millions of users to severe privacy risks. The transmission of data in plain text, the use of GET instead of POST requests for sensitive data transmission (exposing information in URLs) and insecure software practices and decisions, are some of the major open issues for developers to solve towards enhanced privacy when building m-health apps. User profiling, either for advertising and marketing purposes or for user behavior monitoring, are also a growing concern. Finally, our results show that the upcoming GDPR enforcement requires a lot of effort by app developers and publisher towards their successful compliance.

References

[1] Agusti Solanas, Constantinos Patsakis, Mauro Conti, Ioannis S. Vlachos, Victoria Ramos, Francisco Falcone, Octavian Postolache, Pablo A. Pérez-Martínez, Roberto Di Pietro, Despina N. Perrea, Antoni Martnez-Ballesté, *Smart health: A context-aware health paradigm within smart cities* in IEEE Communications Magazine 52(8): 74-81 (2014)

[2] Home Page of EU GDPR, `http://www.eugdpr.org/`

[3] Tobias Dehling, Fangjian Gao, Stephan Schneider, and Ali Sunyaev, *Exploring the far side of mobile health: information security and privacy of mobile health apps on ios and android* in JMIR mHealth and uHealth, 3(1):e8, 2015.

[4] Sascha Fahl, Marian Harbach, Thomas Muders, Lars Baumgärtner, Bernd Freisleben, and Matthew Smith, *Why eve and mallory love android: An analysis of android ssl (in) security*, in Proceedings of the 2012 ACM conference on Computer and communications security, pages 5061. ACM, 2012.

[5] Konstantin Knorr and David Aspinall, *Security testing for android mhealth apps*, in Software Testing, Verification and Validation Workshops (ICSTW), 2015 IEEE Eighth International Conference on, pages 1-8. IEEE, 2015.

"Privacy-Preserving Process Mining: Towards the new European General Data Protection Regulation", Edgar Batista de Frutos and Agusti Solanas Gomez

A growing number of companies and organizations have to deal with multiple kinds of information systems (*e.g.*, management information systems, decision support systems, data warehouses, enterprise resource planning, and geographical information systems, among others) to store as much information as possible in order to extract added-value knowledge and make better operational and strategical decisions. Particularly, they can obtain huge benefits by defining, executing, controlling and efficiently managing their business processes.

Business processes consist in a set of activities aiming at accomplishing certain organizational goals (*i.e*, products or services) for their customers. For instance, by monitoring organizational business processes, organizations can optimize their resources, identify bottlenecks, detect inefficiencies or hidden dependencies, and make better decisions for future improvements. However, these tasks are not easy due to the large and concurrent amounts of processes that organizations have in place.

Most techniques to monitor the execution of business processes are based on events (*i.e.*, atomic pieces of information). For each business process, the activity, resources, time-stamp, identifiers and other details are registered in event log files (*i.e*, each entry in the log file is an event). The analysis of those events, stored in log files, helps to determine the real behavior of the studied processes and supports their alignment with their expected behavior (*i.e.,* their conformance). Thus, exploiting such event data meaningfully is a promising way to obtain knowledge about the organizational business processes. These techniques have been grouped under the new research field of **process mining**.

Process mining is a relative young research discipline that embraces, on the one hand, machine learning and data mining techniques and, on the other hand, process modeling and analysis. The main idea of process mining is to discover, monitor and improve real processes by extracting knowledge from event logs readily available in today's information systems. With the information of event log files, three types of process mining techniques can be applied: (i) **discovery**, a technique that produces process models from event logs without any *a priori* information, (ii) **conformance**, involving the comparison of an existing process model with an event log of the same process (to verify the degree of alignment), and (iii) **enhancement**, in order to extend or improve existing process models using the information about the processes recorded in the event log files. [1, 2] (*cf.* Figure 1).

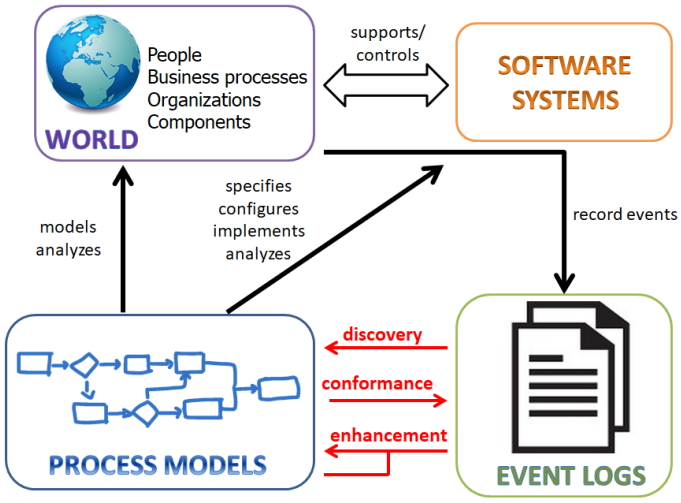

Figure 1: Process mining overview

Process mining techniques rely on the quality of log files. Dealing with noisy and incomplete files is a main challenge that process mining algorithms must face. However, event log files might contain sensitive data (*e.g.,* in hospitals: individual health conditions and treatments) that must be carefully managed to guarantee individuals privacy. Specially in situations in which process mining techniques are externalized (*i.e.,* subcontracted to third parties) it is necessary to put in place the proper measures to avert re-identification and other privacy violations. In such cases, data distortion could be used to prevent the disclosure of sensitive data.

Despite the sensitiveness and particularities (*e.g.,* healthcare-related processes have particular characteristics such as high degree of context dynamism, complexity and multi-disciplinary nature [3]) of the healthcare domain, process mining has been applied [4, 5, 6] with the promise to improve the quality of service, optimize resources and reduce costs.

Research on process mining applied to healthcare focuses on the use of raw data stored in the medical/hospital information system, which contains private information. This makes sense since the goal is to obtain accurate and realistic views of the healthcare processes. However, due to the high sensitivity of medical data, these analyses might not conform with new EU privacy regulations (especially, when these studies are externalized). To mitigate this problem, we study the use of process mining techniques on protected datasets (*i.e.,* properly anonymized). This is an unexplored research direction that opens the door to new challenges and opportunities. By applying privacy-preserving techniques (*e.g.,* micro-aggregation) to event log files containing sensitive data, current process mining techniques might reduce their effectiveness. Thus, it is interesting to study how process models differ when they are generated from raw events or privacy-preserved events (*cf.* Figure 2).

Our study has special relevance when personal data are considered from the legal point of view, with the enforcement of the new European General Data Protection Regulation (GDPR) in May 2018 [7], which strengthens the protection of personal data, specially those referring to sensitive data, for all individuals within the European Union. In the near future, the correct management of sensitive personal data will be in the focus of the European Union, implying the appearance of new forms of data analysis (*e.g.* privacy-preserving process mining) complying with such requirements.

In this talk, we will revisit the concept of process mining and its relation with the healthcare sector,

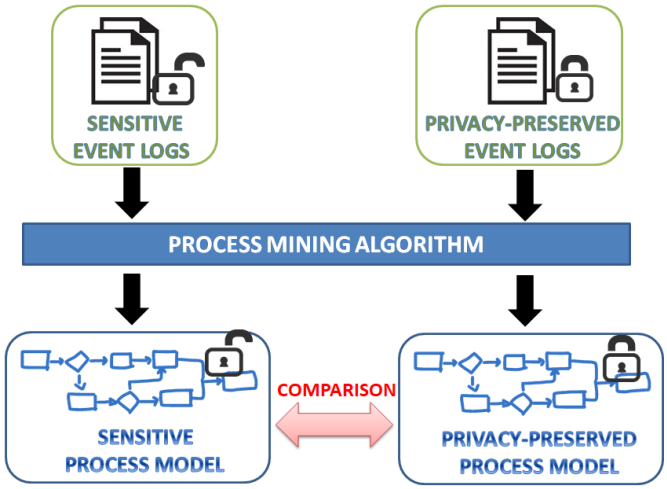

Figure 2: Proposed methodology

which encompass sensitive personal data. Also, we will discuss the main challenges and opportunities for the unexplored field of **privacy-preserving process mining** in the context of the enforcement of the incoming European GDPR.

References

[1] W.M.P.vanderAalst, *ProcessMining:Discovery,Conformance and Enhancement of Business Processes*, in Springer, 2011.

[2] W. M. P. van der Aalst, A. Adriansyah, A. K. A. De Medeiros, F. Arcieri, T. Baier, T. Blickle, J. C. Bose, P. van den Brand, R. Brandtjen, J. Buijs et al., *Process Mining Manifesto*, in International Conference on Business Process Management Workshops (BPM). Springer, 2011, pp. 169–194.

[3] Á. Rebuge and D. R. Ferreira, *Business Process Analysis in Healthcare Environments: A Methodology based on Process Mining*, Information Systems, vol. 37, no. 2, pp. 99–116, 2012.

[4] R. S. Mans, H. Schonenberg, M. Song, W. M. P. van der Aalst, and P. J. M. Bakker, *Application of Process Mining in Health- care A Case Study in a Dutch Hospital*, Proceedings of the 1st International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC), vol. 25, pp. 425–438, 2008.

[5] R. S. Mans, H. Schonenberg, G. Leonardi, S. Panzarasa, A. Cavallini, S. Quaglini, and W. M. P. van der Aalst, *Process mining techniques: An application to stroke care* in Studies in Health Technology and Informatics, vol. 136, pp. 573–578, 2008.

[6] U. Kaymak, R. S. Mans, T. van de Steeg, and M. Dierks, *On Process Mining in Health Care* in Proceedings of the International Conference on Systems, Man and Cybernetics (SMC), 2012, pp. 1859–1864.

[7] Home Page of EU GDPR, `http://www.eugdpr.org/`

"Statistical Disclosure Control meets Recommender Systems: A practical approach",
Fran Casino and Augusti Solanas

Our society lives in an age where the eagerness for information has resulted in problems such as *infobesity*, especially after the arrival of *Web 2.0*. In this context, automatic systems such as recommenders are increasing their relevance, since they help to distinguish useful information from noise. Nowadays, recommender systems (RS) [1] play an active role in the Internet through the advances in data mining and artificial intelligence. Collaborative Filtering (CF) [2] is a kind of recommender system that comprises a large family of recommendation methods. The aim of CF is to suggest/recommend items (e.g. books, films or routes) based on the preferences of users (U) that have already acquired and/or rated some of those items.

The widespread use of CF on the Internet provides great opportunities and benefits for both companies and users, but there is a major drawback: **the lack of users' privacy**. Careless management of personal information, besides being against the legislation in most countries, could lead to serious consequences for both users, whose information is stored, as well as companies. Current legislation requires service providers to properly handle data and ensure users' privacy. However, there are many examples of errors that have led to the disclosure of private information and, hence, it is apparent that legislation alone cannot solve the problem. Consequently, the task of finding and repairing the security and privacy weaknesses of ubiquitous real-world recommender systems is a must. This requires of a multi-disciplinary approach, which combines expertise in fields as diverse as privacy protection, recommender systems, data mining, location privacy, etc. Strong interaction between these different disciplines is not only beneficial but essential. Privacy preserving techniques (e.g., statistical disclosure control, privacy preserving data mining, location privacy, etc.) might be studied to address the privacy issues derived from the wide adoption of ubiquitous computing, which is able to collect data from people almost everywhere at any time.

In the CF field, we need to tackle specific issues related to privacy. For instance, customers, who believe that their preferences/profiles may be exposed, could not give their rating on an item or, give it incorrectly or distorted [3]. This user behaviour, derived from the feeling of lack of privacy, results in a reduction of both the number of ratings as well as their quality. Another drawback is that companies can acquire data about the preferences of many users in a specific domain/market and obtain a big advantage over new competitors if they decide to expand to other markets. Moreover, the existence of large monopolies on the Internet (e.g., Google, Amazon) is another clear disadvantage, so users' data could be transferred amongst different parties, which are managed by the same large companies, without the users' awareness. All this is exacerbated in the recommender systems field, where sparse, high-dimensional datasets need to be processed. In the long term, this lack of security and privacy will strongly damage businesses as well as the society as a whole. As a conclusion, **we need to deal with a trade-off between privacy, recommendation?s accuracy and computational time**. In order to address the privacy issues raised by the systematic collection of private information, which is required for the proper use of CF, current research focuses on Privacy Preserving Collaborative Filtering (PPCF) methods [5].

The aim of this talk is to provide the audience with a comprehensive overview of CF and its lack of privacy. We will point out the existing trade-off between accuracy and privacy. Moreover, we will show the results of comparing three PPCF methods based on well-known SDC techniques such as noise addition [6] and microaggregation [4, 6], in order to demonstrate that it is possible to meet two (apparently) contradictory goals: privacy preservation and recommendation accuracy.

This work is directly related with COST Action IC1403, specifically with WG4: Security and Privacy Analysis of Real-World Systems.

References

[1] P. Resnick and H. Varian. *Recommender systems* in Communications of the ACM, 40(3), 5658. (1997).

[2] D. Goldberg, D. Nichols, B. M. Oki and D. Terry. *Using collaborative filtering to weave an information tapestry* in Communications of the ACM, 35(12), 61–70. (1992).

[3] L.F. Cranor, J. Reagle, and M.S. Ackerman. *Beyond concern: Understanding net users? attitudes about online privacy* in Technical report, The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy, 2000

[4] A. Solanas and A. Martínez-Ballesté, *V-MDAV : A Multivariate Microaggregation With Variable Group Size* in Seventh COMPSTAT Symposium of the IASC, 2006.

[5] F. Casino, C. Patsakis, D. Puig, and A. Solanas, *On privacy preserving collaborative filtering: Current trends, open problems, and new issues* in ICEBE, pp. 244–249. (2013).

[6] F. Casino, J. Domingo-Ferrer, C. Patsakis, D. Puig, and A. Solanas, *A k-anonymous approach to privacy preserving collaborative filtering* in Journal of Computer and System Sciences, Vol. 81, Issue 6, pp. 1000–1011. (2015).

Session V: Cryptanalysis of primitives

"Distinguishing iterated encryption", Eran Lambooij

Suppose that Alice and Bob want to increase their security while communicating with each other. They decide to use a block cipher and encrypt their messages twice with the same key instead of once. It is obvious that this does not increase their security, but will it decrease their security? In this presentation an answer is given to this question, and a more generalized version of it.

A block cipher can be described as a family of permutations indexed by a secret key. The size of this family of permutations almost always is significantly smaller than the set of all possible permutations given the block size of the cipher. This is always the case when the block size and the key size of the cipher are roughly equal. Nevertheless, distinguishing a cipher from a random function generating permutations is hard in the general case when given a limited number of queries.

When a cipher can be decomposed into repeated iterations of the same permutation it can be viewed as a squared (or higher power) permutation. This paper studies the structures introduced by ciphers generating squared (or higher power) permutations. By using these structures it is shown that the cipher can be distinghuished from a random family of permutations.

Several new distinguishers are introduced and these distinguishers are experimentally verified. After that the expected number of chosen plaintext ciphertext pairs needed for the distinguishers to work is proven. The distinguishers can be used to break schemes such as 8K+1 DES. Moreover, the work in this paper can be extended to functions generating random functions, which at this moment is work in progress.

In the presentation the results from the paper will be presented. The paper is joint work with Orr Dunkelman, Tanja Lange and Nathan Keller and is still work in progress. The results are mainly described in my master's thesis (chapter 6).

"On Security Enhancement of Lightweight Encryption Employing Error Correction Coding and Simulators of Channels with Synchronization Errors", Miodrag J. Mihajević

A number of approaches have been reported on employment of results from coding theory for design of symmetric-key encryption schemes. Mainly, security of these coding based encryption proposals has not been properly proven, and some of the proposals have been broken. For example the coding based crypto system proposed in [1] has been broken as reported in [2]. On the other, different approaches of employment coding theory for design secure encryption (in certain evaluation scenarios) have been discussed in [3, 4, 5]: These approaches are focused towards security enhancement of lightweight encryption schemes. According to the reported results two main paradigms for coding based security enhancement have been shown in Figure 3.

It is important to note that the both paradigm, I & II, can be employed for security enhancement of stream ciphers, but only paradigm II can be employed for security enhancement of block ciphers. Figure 4 displays a particular instantiation of the paradigm II. This talk discusses security and the implementation issues of the scheme displayed in Figure 4. Regarding the implementation issues, employment of the raptor codes [6, 7], is considered.

References

[1] M. Esmaeili and T. A. Gulliver, *A secure code based cryptosystem via random insertions, deletions, and errors* in IEEE Common. Lett., vol. 20, no. 5, pp. 870–873, May 2016.

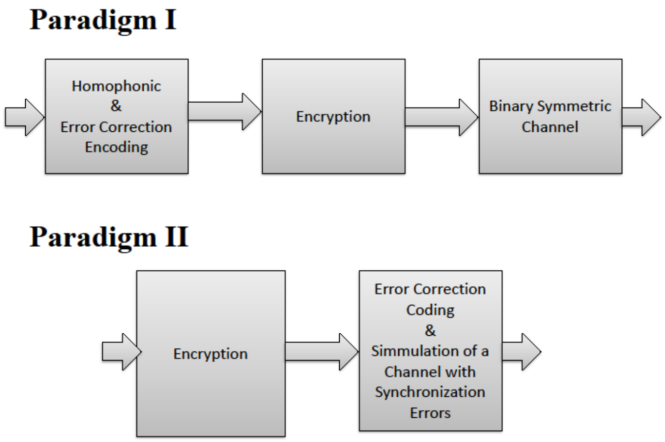

Figure 3: Paradigms for the security enhancement.

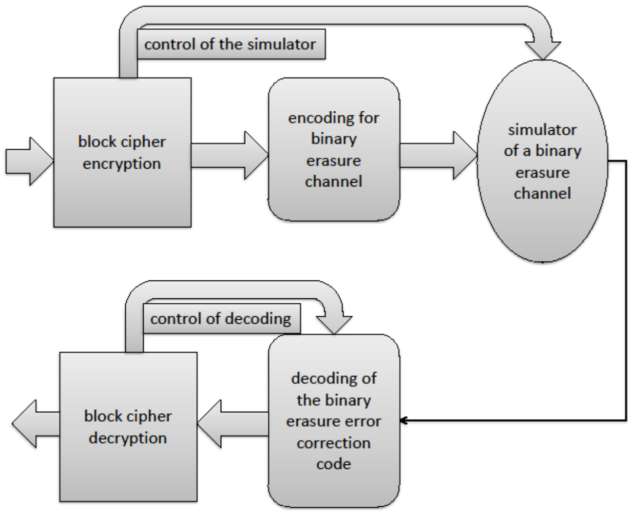

Figure 4: A particular security enhancement.

[2] Y. Lee, Y.-S. Kim and J.-S. No, *Ciphertext-Only Attack on Linear Feedback Shift Register- Based Esmaeili-Gulliver Cryptosystem* in IEEE Common. Lett., vol. 21, no. 5, pp. 971–974, May 2017.

[3] F. Oggier and M.J. Mihaljevic, *An Information-Theoretic Security Evaluation of a Class of Randomized Encryption Schemes* in IEEE Transactions on Information Forensics and Security, vol. 9, no. 2, pp. 158–168, Feb. 2014.

[4] M.J. Mihaljevic, A. Kavcic and K. Matsuura, *An Encryption Technique for Provably Secure Transmission from a High Performance Computing Entity to a Tiny One* in Mathematical Problems in Engineering, vol. 2016, Article ID 7920495, 10 pages, May 2016. doi:10.1155/2016/7920495.

[5] A. Kavcic, M.J. Mihaljevic and K. Matsuura, *Light-Weight Secrecy System Using Channels with Insertion Errors: Cryptographic Implications* in IEEE Information Theory Workshop 2015, Jeju Island, Korea, 11-15 Oct. 2015, Proceedings, pp. 257–261, 2015.

[6] A. Shokrollahi, *Raptor codes* in IEEE Trans. Inform. Theory, vol. 52, no. 6, pp. 2551–2567, June 2006.

[7] A. Shokrollahi and M. Luby, *Raptor codes* in Foundations and Trends in Commun. and Inf. Theory, vol. 6, no. 3-4, pp. 213–322, 2011.

"An Improved Cryptanalsis of Lightweight Stream Cipher Grain-v1", Miodrag J. Mihaljević, Nishant Sinha, Sugata Gangopadhyay, Subhamoy Maitra, Goutam Paul and Kanta Matsuura

Grain-v1 has attracted significant attention and a number of results on its security evaluation has been reported (see for example [1, 2, 3, 4, 5]).

This talk provides additional insights on Grain-v1 security based on its sampling resistance and proposes dedicated time-memory-data trade-off (TMD-TO) approaches for the internal state recovering which employs the guess-and-determine paradigm. Dedicated approaches are proposed for constructing algebraic equations which provide recovering l bits of an internal state of Grain-v1 when l-bits keystream segment is given and remaining 160-l bits of internal state are assumed. The filter function of Grain-v1 provides that fixing relatively a few input variables reduces it to either a quadratic or a linear function so that suitable equations can be constructed. A conditional TMD-TO approach built over the decimated sample with segments beginning with the same prefix, and its generalization based on employment of multiple patterns for the sampling are proposed and employed for the internal state recovery.

Generally speaking, our basic idea is as follows. Consider that the state size is L. We try to observe a few bits (say a of the keystream, and consider that certain bits (say b) of the internal state are fixed to a specific pattern. Then with this information, we try to obtain some more bits (say c) of the internal state. The rest of the bits in the internal state $d = L - b - c$ are either exhaustively searched or may be obtained by suitable TMD-TO attack. This is some kind of "glimpse" of the internal state of Grain-v1.

The talk shows that dedicated guess-and-determine approach, sampling and employment of multiple sample patterns provides additional gains in comparison with a straightforward employment of the traditional TMD-TO techniques and BSW sampling based ones.

Two generic approaches for cryptanalysis employing guess-and-determine and dedicated TMD- TO based attacks are pointed out and analyzed: The first approach employees dedicated guess- and-determine and a conditional TMD-TO with BSW sampling, and the second one is its generalization where the sampling points correspond to multiple patterns, i.e. different prefixes of the sample segments. The second approach provides additional flexibility for setting the trade- off options and provides success of the attack when the available sample is too short for performing the first approach. We propose techniques for recovering a part of Grain-v1 internal state based on assumption of the remaining one and given prefix of the corresponding output, i.e. employing a guess-and- determine paradigm. First, a dedicated TMD-TO based cryptanalysis employing a single-prefix pattern is proposed and discussed, and its generalization when multiple-prefixes patterns are employed is presented later on. Finally, a comparative discussion and the conclusions are given.

References

[1] L. Jiao, B. Zhang and M. Wang, *Two Generic Methods of Analyzing Stream Ciphers* in J. Lopez and C.J. Mitchell (Eds.): ISC 2015, LNCS 9290, pp. 379–396, 2015.

[2] M. J. Mihaljevic, S. Gangopadhyay, G. Paul and H. Imai, *Internal state recovery of Grain-v1 employing normality order of the filter function* in IET Information Security, vol. 6, Iss. 2, pp. 55–64, 2012.

[3] M. Rahimi, M. Barmshory, M.H. Mansouri, M.R. Aref, *Dynamic cube attack on Grain-v1* in IET Information Security, vol. 10, no. 4, pp. 165–172, 2016.

[4] S. Sarkar, S. Banik, S. Maitra, *Differential Fault Attack against Grain Family with Very Few Faults and Minimal Assumptions* in IEEE Transactions on Computers, Year: 2015, Volume: 64, Issue: 6, Pages: 1647–1657, DOI: 10.1109/TC.2014.2339854

[5] B. Zhang and X. Gong, *Another Tradeoff Attack on Sprout-Like Stream Ciphers* in T. Iwata and J.H. Cheon (Eds.): ASIACRYPT 2015, Part II, LNCS 9453, pp. 561–585, 2015.

Session VI: Cryptanalysis of protocols

"Loophole: Timing Attacks on SharedEvent Loops in Chrome", Pepe Vila and Boris Köpf

Event-driven programming (EDP) is the prevalent paradigm for graphical user interfaces, web clients, and it is rapidly gaining importance for server-side and network programming. Central components of EDP are *event loops*, which act as FIFO queues that are used by processes to store and dispatch messages received from other processes.

In this paper we demonstrate that shared event loops are vulnerable to side-channel attacks, where a spy process monitors the loop usage pattern of other processes by enqueueing events and measuring the time it takes for them to be dispatched. Specifically, we exhibit attacks against the two central event loops in Google's Chrome web browser: that of the I/O thread of the host process, which multiplexes all network events and user actions, and that of the main thread of the renderer processes, which handles rendering and Javascript tasks.

For each of these loops, we show how the usage pattern can be monitored with high resolution and low overhead, and how this can be abused for malicious purposes, such as web page identification, user behavior detection, and covert communication.

"How (not) to use TLS between 3 parties", Karthikeyan Bhargavan, Ioana Boureanu, Pierre-Alain Fouque, Cristina Onete and Benjamin Richard

The Transport Layer Security (TLS) protocol is designed to allow two parties, a client and a server, to communicate securely over an insecure network. However, when TLS connections are proxied through an intermediate "middlebox", like a Content Delivery Network (CDN), it does not follow that the standard end-to-end security guarantees of the protocol would necessarily apply. Moreover, the formal models in which authenticated key-exchange protocols, like TLS, have been analysed, also take into consideration just the 2-party setting and do not trivially extend to the case of more than two-parties being legitimately involved in the same execution.

In this talk, we will develop on the security guarantees of Keyless SSL, a CDN architecture currently deployed by CloudFlare that composes two TLS 1.2 handshakes to obtain one proxied TLS connection – which therefore has 3 active parties involved within: a client, an end-server and a proxying CDN. We will demonstrate several attacks onto Keyless SSL; we will see that these attacks apply unfortunately to all versions proposed for Keyless SSL, that is when Keyless SSL is running mainly TLS 1.2 in RSA-mode, but also when it is based on TLS 1.2 in DHE-mode. Some attacks can be seen as forward-secrecy attacks which become possible only when the 2-party TLS-setting is extended to this 3-party CDN-driven setting, others are cross-protocol attacks due to the minimal visibility that the end-server has into what the CDN is actually querying for, in Keyless SSL. In any case, we will show that Keyless SSL fails to meet even its very intended security goals.

We will discuss our proposed adaptation of the Keyless-SSL design, which we can proven secure. We will argue that handshakes in proxied TLS/authenticated key-exchange require a new, stronger, 3-party security model and a set of additional security requirements too. We will give some glimpse into our new security model: i.e., 3(S)ACCE, a generalization of the 2-party ACCE model that has been used in several previous proofs for TLS. Our modified versions of Keyless SSL for TLS 1.2, as well as our proposed, new version of Keyless SSL based on TLS 1.3, are proven secure in this new 3(S)ACCE model.

Our discussion will indicate that proxied TLS architectures, as currently used by a number of CDNs, may be vulnerable to subtle attacks (against channel-security and not only), and therefore deserve close attention. This is all the more relevant, since architectures like Keyless SSL are being IETF-standardised as we speak: `https://tools.ietf.org/html/draft-mglt-lurk-tls-use-cases-02`.

"Quam Bene Non Quantum: Analysing the Randomness of a Quantum Random Number Generator and the Costs of Postprocessing", Darren Hurley-Smith and Julio Hernandez-Castro

Random number generation is critical to many security applications. Trustworthy, and reliable generation of random numbers is essential to the integrity of crypto-systems and authentication protocols. Innovation in this field is constant, and has led to the development of many different entropy harvesting and random number generation methods. A specific class of hardware random number generators, optical Quantum Random Number Generators (QRNG), has been the focus of our current research. The devices we have studied include Quantis 16M pci-e, Quantis 4M pci-e, and Quantis USB, all produced by ID Quantique.

Quantum random number generation is of interest, due to the inherent and theoretically inviolable unpredictability of quantum phenomena [1]. Optical QRNG relies on the inherent quantum properties of photons as a source of randomness [2]. Single photons are emitted, towards a semitransparent element. This element (a polarising beam splitter) has an approximately 50% chance of reflecting the photon towards one single photon detector or allowing it to pass through, towards another detector. These detectors can be interpreted as the values 0 and 1, with detections triggering the appropriate bit value. Theoretically, this should provide a random bit-stream that benefits from the inherent randomness of this quantum phenomenon.

The reality, as highlighted by Frauchiger, Renner and Troyer, is not so simple. They state that an *imperfect* device may be subject to influence from its environment, physical characteristics and other factors [3]. So-called *side-information* may introduce bias into the ostensibly random output of an imperfect device. Such information may be known to observers due to its presence in the environment or device. We observe such biases in our work and identify a variety of statistical tests that the raw output stream performs exceedingly poorly on.

Post-processing of the output, using algorithms keyed to the *side-information* most likely to affect a given device, is suggested as a means to extract randomness from the raw bit-stream. Improvements were observed, but some interesting statistical flaws were observed in some samples. Serial correlation tests for a small set of samples reported weak or very weak results despite post-processing. Our research is ongoing, with the study of larger post-processed files a priority. Inspired by previous research by Dodis et al. concerning the impossibility of cryptography with imperfect randomness [4], we hypothesise that the post-processing algorithm can only mitigate the inherent bias of the raw stream, not remove it entirely.

Post-processing is computation and memory intensive. It is possible to harvest a post-processed stream directly from a Quantis device, but this reduces the listed speed by 75%, far below the advertised *high-speed randomness* claimed in the online marketing material and paraphernalia shipped with each device. It is also post-processed off-device: data is collected raw, then post-processed in software (non-AIS31 Quantis hardware does not provide this by default).

SK Telecom announced, July 2017, that they are in the late stage of producing IoT-scale QRNG devices. Although they use LED photon-emission counting (Quantum Shot Noise) instead of polarisation as a method for harvesting entropy, the points made by Frauchiger et al. stand. Our own observations of Quantis devices have shown that the raw stream fails many key tests of true randomness.

Without the appropriate implementation of hardware post-processing, it is likely that a small-scale QRNG will suffer similar issues. There are strong suggestions that quantum random number generation is not trustworthy in its raw state, and that IoT platforms may suffer from a lack of resources for robust post-processing techniques. IoT-scale QRNG must be subject to stringent design guidelines and testing, which we seek to inform through our analysis of raw and post-processed data. Furthermore, we posit that the advertised speed of hardware RNG should be based on their post-processed output speed, instead of the frequently flawed raw device output.

References

[1] Rarity, J. G., P. C. M. Owens, and P. R. Tapster, *Quantum random-number generation and key sharing* in Journal of Modern Optics 41.12 (1994): 2435–2444.

[2] Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L., and Zbinden, H. (2000), *Optical quantum random number generator* in Journal of Modern Optics, 47(4), 595–598.

[3] Frauchiger, D., Renner, R., and Troyer, M. (2013), *True randomness from realistic quantum devices* in arXiv preprint arXiv:1311.4547.

[4] Dodis, Y., Ong, S. J., Prabhakaran, M., and Sahai, A. (2004), *On the (im) possibility of cryptography with imperfect randomness*, 45th Annual IEEE Symposium on Foundations of Computer Science, 2004 (pp. 196–205).

Special session: Tools

"Open-source tooling for differential power analysis", Cees-Bart Breunesse and Ilya Kizhvatov

Differential power analysis and related techniques have been a subject of public research for almost twenty years. This research field is rich in methods and techniques, but not in publicly available state-of-the-art tools. We would like to discuss this issue and present an experimental high performance open-source toolkit for DPA, along with a basic comparison of the tools.

"Backdoor Detection Tools for the Working Analyst", Sam Thomas

Complex embedded devices are becoming ever prevalent in our everyday lives, yet only a very small amount of people consider the potential security and privacy implications of attaching such a device to our home, business and government networks. As demonstrated through recent publications from academia and blog posts from numerous industry figures, these devices are plagued by poor design choices with regard to end-user security. What's even more worrying are reports of manufacturers inserting backdoor-like functionality into the production firmware of those devices.

Suppose your employer tasks you with assessing the security of such a device. Suppose you're given only a few hours to complete that assessment. With no formal specification of functionality, no access to program source code and limited time, what can you do? In this talk, we deal with that very scenario. We describe two tools we've developed to perform lightweight analysis of Linux-based embedded device firmware. We demonstrate their effectiveness in finding undocumented functionality and backdoors in a number of consumer devices and show how they perform in a lightweight manner with respect to execution time – whilst lessening the expertise required to perform analysis of embedded device firmware.

"Avatar^2 - Enhancing Binary Firmware Security Analysis with Dynamic Multi-Target Orchestration", Marius Muench

Avatar^2 is an open source framework for dynamic analysis of binary firmware. At its core, it utilizes dynamic multi-target orchestration to enable a shared and synchronized analysis of firmware inside multiple tools, such as GDB, OpenOCD, Qemu, PANDA or angr.

This talk highlights the challenges for binary firmware analysis, presents the general architecture and benefits of the Avatar^2 framework, and provides a practical example for the tool's usage.