COST Cryptanalysis of Ubiquitous Computing Systems (CRYPTACUS) Workshop
March 14-15, 2017, Sutomore, Montenegro
https://www.cryptacus.eu/

BOOKLET OF ABSTRACTS

COST is supported by the EU
Framework Programme Horizon 2020

PREFACE

This Booklet of Abstracts comes as a results of a very successful first Cryptacus' workshop, organized in one of the COST Member countries - Montenegro.
For this workshop 14 presentation proposals were accepted and Cryptacus has funded speakers who came to Montenegro from Finland, France, Greece, Italy, Luxembourg, Serbia, Turkey, and the United Kingdom.
We hope that the Cryptacus audience will find this Booklet of Abstracts useful and interresting.

Gildas Avoine
Julio Hernandez-Castro
Milena Djukanovic

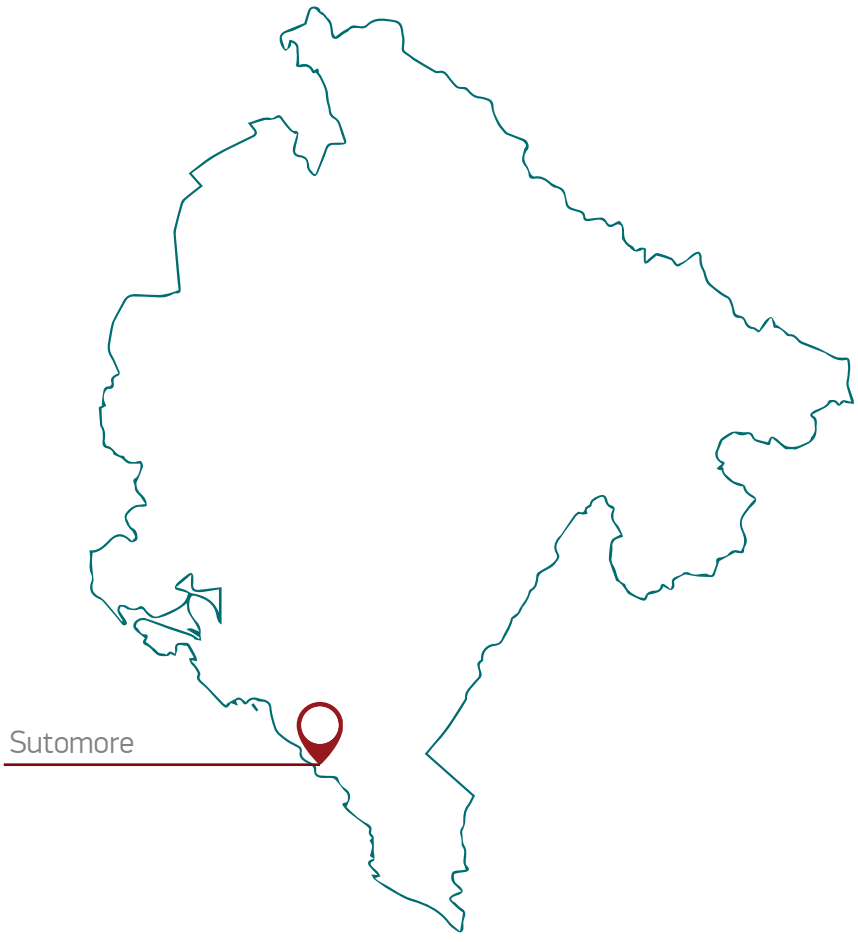

TABLE OF CONTENTS

Template Attacks Exploiting Static Power And Application To CMOS Lightweight Crypto-Hardware

Davide Bellizia[1], Milena Djukanovic[2], Giuseppe Scotti[1], and Alessandro Trifiletti[1]

[1] Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni, University of Rome, La Sapienza, Rome, Italy
{bellizia,scotti,trifiletti}@diet.uniroma1.it,
[2] Faculty of Electrical Engineering, University of Montenegro, Podgorica, Montenegro
milenadj@ac.me

In 2007, Giorgetti et al. demonstrated the possibility to use the static current as source of information leakage. Attack exploiting static power relies on the physical fact that subthreshold currents in CMOS technology are strongly dependent on the input vectors. In the context of Side-Channel Attacks, profiled attacks have been proved as one of the strongest attack procedures. The Template Attack Exploiting Static Power (TAESP) [1] uses static currents to recover the relevant information from a cryptographic device, taking advantage of the temperature dependence of static currents. The TAESP procedure can be summarized as follows: a profiling phase is used to profile the clone devices static power consumption, while executing the target operation at N different temperatures. Gaussian templates are then built on those profiles. After that, during the attacking phase, experiments are performed on the device under attack at the same N working temperatures, collecting static power samples to be compared with templates from the previous stage. Finally, the posteriori probability is computed for each template, and the maximum likelihood principle is used to choose the template (e.g. the key) with the highest probability. In order to evaluate the effectiveness of the proposed TAESP procedure, and to consider effects of process variations, 100 Monte Carlo generated sample circuits of a 40nm CMOS 4-bit crypto-core based on the PRESENT-80 block cipher have been used to perform TAESP. Furthermore, also a complete implementation of the PRESENT-80 has been attacked, considering three different corners of the technology. Comparing a univariate versus a multivariate TAESP on the 4-bit crypto-core, the number of successful attacked chips can be increased of more than 50% using more than one temperature. Considering the complete implementation, the upper bounds probability of the multivariate TAESP can be increased x3.3 times in the worst-case (SS), respect to the univariate approach.

References

1. Bellizia, D., Djukanovic, M., Scotti, G., and Trifiletti, A.: Template attacks exploiting static power and application to CMOS lightweight crypto-hardware. Int. J. Circ. Theor. Appl., 45: 229241. doi: 10.1002/cta.2286. (2017)

A Tale of Cache-Timing Attacks in OpenSSL: Constant-Time Callees with Variable-Time Callers

Cesar Pereida García and Billy Bob Brumley

Laboratory of Pervasive Computing
Tampere University of Technology, Finland
cesar.pereidagarcia@tut.fi,
billy.brumley@tut.fi

Abstract. Side-channel attacks are a serious threat to security-critical software. OpenSSL is a prime security attack target due to the library's ubiquitous real world applications, therefore, the history of cache-timing attacks against OpenSSL is varied and rich. The presentation includes a brief history of cache-timing attacks in OpenSSL. To mitigate remote timing and cache-timing attacks, many ubiquitous cryptography software libraries such as OpenSSL and LibreSSL feature constant-time implementations of cryptographic primitives. Unfortunately, software defects in these libraries only provide temporary security as new side-channel techniques are developed. The result is vulnerable code that leaks confidential information and that can be exploited to recover private keys using state-of-the-art side-channel techniques.

Adding a new chapter to OpenSSL rich history, this presentation features a concrete example of a new cache-timing attack exploiting a software defect in OpenSSL. We disclose a vulnerability in OpenSSL 1.0.1u that recovers ECDSA private keys for the standardized elliptic curve P-256 despite the library featuring both constant-time curve operations and modular inversion with microarchitecture attack mitigations. Exploiting this defect, we target the errant modular inversion code path with a cache-timing and improved performance degradation attack, recovering the inversion state sequence. The improved performance degradation attack allow us to accurately recover the inversion state sequence despite the speed of this operation compared to the scalar multiplication.

We propose a new approach of extracting a variable number of nonce bits from these sequences, and improve upon the best theoretical result to recover private keys in a lattice attack with as few as 50 signatures and corresponding traces. As far as we are aware, this is the first timing attack against OpenSSL ECDSA that does not target scalar multiplication, and furthermore the first side-channel attack on cryptosystems leveraging P-256 constant-time scalar multiplication.

Moreover, we demonstrate a cache-based key recovery attack against two ubiquitous security protocols (SSH and TLS) linked against OpenSSL to perform ECDSA signature operations. We extract P-256 ECDSA keys from an OpenSSH server for the SSH scenario and from an stunnel server for the TLS scenario.

Enhancing the Honeywords System: Mitigating Active Adversaries and Increasing Typo-safety of Honeywords

Ziya Alper Genc
University of Luxembourg
ziya.genc@uni.lu

Suleyman Kardas
Batman University
skardas@gmail.com

Mehmet Sabir Kiraz
TUBITAK BILGEM
mehmet.kiraz@tubitak.gov.tr

Abstract

Security enhancements for Honeywords system [1] against active attackers will be discussed. The Honeywords system provides resistance against offline dictionary attacks and allows to detect password database breaches. However, the original Honeywords protocol is not robust against malicious code modifications, where the adversary alters the code running on either the login server or the honeychecker. In addition, users could be mistakenly submit honeywords to the login server that would falsely trigger the alarm. We will begin with describing the original Honeywords protocol of Juels and Rivest. Next, security improvements to mitigate code modification attacks will be explained [2]. We will continue with illustrating our method for increasing the typo-safety of honeywords. Finally, we will discuss the challenges in securing the passwords against adversaries which observe the submissions to the login server. Participants will be able to list different adversary models in password based authentication schemes and identify the strong and weak points of Honeywords system in each of them.

Keywords

passwords, cracking, honeywords, authentication, typo safe, password sniffing

References

[1] Ari Juels and Ronald L Rivest. Honeywords: Making password-cracking detectable. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 145–160. ACM, 2013.

[2] Ziya Alper Genc, Süleyman Kardas, and Mehmet Sabir Kiraz. Examination of a new defense mechanism: Honeywords. http://eprint.iacr.org/2013/696.pdf, 2013.

Security Evaluation of Symmetric Key Primitives using CP

David Gérault, LIMOS, University Clermont Auvergne, France

Ubiquitous computing systems heavily rely on efficient symmetric key cryptographic primitive. Designing and evaluating the security of such primitives is a very challenging task. Proving the security of a cipher for each of these threats basically requires implementing the search for each kind of distinguisher, $e.g.$ differential characteristics with a good probability or integral distinguishers.

Automatic methods, aiming at making the life of designers easier, appeared in the past few years. In particular, Mixed Integer Linear Programming (MILP) was used to analyze several block ciphers. Despite its efficiency, it has some limitations. For instance, modelling the non linear components of the cipher (the S boxes) requires building a very large set of linear inequations, which are barelly readable for humans and only scale up for small S boxes.

We present a new approach for automatic cryptanalysis of block ciphers using Constraint Programming (CP). CP is a declarative programming paradigm in which the problems to solve are modelled as a Constraint Satisfying Problem (CSP). While SAT is limited to boolean variables, and MILP to linear constraints, CP allows constraints and variables of any kind and generalizes these approaches. In addition, CP models are typically very natural and easy to read and understand, which limits the risk for human mistakes. For instance, it allows us to model the S boxes by simply giving the table to the solver. To demonstrate the potential of CP for automatic evaluation of symmetric key primitives, we present three results: The first one [4], revisits the search for related key differential characteristics on AES 128. Not only is the CP approach faster than the previously existing algorithms [1] [2], but it also finds solution that had been missed by these works. The second one [3] studies the related key security of a lightweight block cipher, Midori. In essence, using CP, we were able to mount practical related key differential attacks on this cipher. Finally, in [5], yet to be presented at FSE 2017, we broaden the field of application of constraint programming by studying other properties, such as related tweakey impossible differential attacks on SKINNY, integral distinguishers on PRESENT, and impossible differential attacks on HIGHT.

References

[1] A. Biryukov and I. Nikolic. Automatic search for related-key differential characteristics in byte-oriented block ciphers: Application to aes, camellia, khazad and others. In *EUROCRYPT 2010*.

[2] P. Fouque, J. Jean, and T. Peyrin. Structural evaluation of AES and chosen-key distinguisher of 9-round AES-128. In *Advances in Cryptology - CRYPTO 2013*.

[3] D. Gérault and P. Lafourcade. Related-key cryptanalysis of midori. In *Progress in Cryptology - INDOCRYPT 2016*, volume 10095 of *Lecture Notes in Computer Science*, pages 287–304, 2016.

[4] D. Gerault, M. Minier, and C. Solnon. Constraint programming models for chosen key differential cryptanalysis. In *Principles and Practice of Constraint Programming - CP 2016*.

[5] S. Sun, D. Gerault, P. Lafourcade, Q. Yang, Y. Todo, K. Qiao, and L. Hu. Analysis of aes, skinny, and others with constraint programming. In *FSE*, 2017.

Memory carving in ubiquitous devices

Thomas Gougeon[1], Morgan Barbier[1], Patrick Lacharme[1], Gildas Avoine[2,3], and Christophe Rosenberger[1]

[1] Normandie Universite; ENSICAEN-UNICAEN-CNRS, GREYC UMR 6072, F-14032 Caen, France
[2] INSA Rennes, IRISA UMR 6074
[3] Institut Universitaire de France

Ubiquitous devices usually gather and store personal data, possibly related to the behaviour of their holder. They are typically low-cost devices including (but not limited to) credit cards, mass transportation passes, electronic passports, keyless entry and start systems, and ski passes. For example, a mass transportation pass may store information about the last trips of the traveller, an EMV card records information about the last dozens of payments done by the customer, a car ignition key in recent vehicles contains plenty of information about the car and the behaviour of the driver. In most cases, the personal data contained in these devices are accessible without requiring any authentication.

Interpreting the meaning of the captured raw data is difficult and time-consuming when neither the data structure nor the data encoding are known. The task becomes tedious if the number of devices to be analysed is large. In spite of that, such a task is important when investigations must be carried out. It can be to find digital evidence in connection with criminal investigations – when information related to a suspect is stored in a device – , to collect some information related to a missing person or to verify that a system complies with the claims of the manufacturers or authorities.

Almost all existing contributions on the memory carving problem for ubiquitous devices consider ad-hoc, hand-made analyses. An exception is the work of Ton Van Deursen et al. [2], who investigated the memory carving problem for sets of memory dumps, and applied it to public transportation cards. They propose to automatically locate where the information can be stored on the dump. Another work is due to Gougeon et al. [1], who investigated an automatic distinction of cryptographic material in dumps of ubiquitous devices in order to eliminate areas of the memory where there is no information to decode. Nevertheless, none of these works provide an automatic interpretation of the data.

Stored information are usually mixed in the dump memory, including textual information, dates, cryptographic data, serial numbers, etc. possibly encoded with different functions. Considering that the encoding functions used in a given dump are unknown, the decoding process needs to exhaustively test all possible functions at all possible location. Unfortunately, no oracle can efficiently determine whether the decoding of the information is correct leading to a huge number of false positives.

This talk introduces a method to efficiently eliminate the false positives generated by the decoding of textual information. A false positive appears when

a bit sequence in a dump is decoded with a function that is different from the one used to encode it. After decoding textual information, strings need to be separated in two categories, those which make sense and those which not make sense. An analysis of the n-grams frequencies of the tested string is performed. These frequencies are then compared to those of a dictionary corpus containing words, cities, and names to take the decision. For example, this method retrieves holder names in transport cards, bank cards and passports with a success rate of 99% while keeping the false positive rate as low as 3%.

References

[1] Thomas Gougeon, Morgan Barbier, Patrick Lacharme, Gildas Avoine, and Christophe Rosenberger. Memory carving in embedded devices: separate the wheat from the chaff. In *Applied Cryptography and Network Security*, volume 9696, pages 592–608, 2016.

[2] Ton Van Deursen, Sjouke Mauw, and Sasa Radomirovic. mCarve: Carving attributed dump sets. In *USENIX Security Symposium*, pages 107–121, 2011.

On the Hardware Trojans and Confidentiality

Eleni Isa, Nicolas Sklavos

SKYTALE Research Group,
Computer Engineering & Informatics Department,
University of Patras, Hellas
e-mail: {isa, nsklavos}@ceid.upatras.gr

The whole process of making an integrated circuit, starts from describing the system's specifications and ends with the final packaging and testing of the chip. During this process, there are many different stages. Some of these, hide many dangers which can influence the final function of the system. The above field has grown into a major research need. This happens because a trust device has to do with the assurance, that the circuit which is made is the same circuit with the designed one. Two of the most important reasons for developing trusted hardware field, was firstly the economic burden of making new correct chips, and secondly the need of fully functional circuits. This work is centered to the hardware security prospect, and especially to the main enemy of every circuit, which is called hardware trojans. These are small scale integrated circuits which are inserted in the initial circuit usually from an adversary. A hardware trojan can have two impacts on the circuit's functionality. Either it changes its functionality and forces it to do something different, or it allows the circuit works properly and it just transmits details to the adversary. It is understandable that both functions are undesirable.

Due to the importance of the matter, during the last years, many different ways for detecting trojans have developed. The two basic categories are the destructive and non-destructive methods. The first one, as its name indicates, uses a sample of the manufactured circuits and examines it using chemical analysis. However, this process is expensive and time consuming. The second-wide category, concludes the non-destructive methods. It could be classified again under two main heads: non-invasive and invasive techniques. The first ones conclude run-time tests. The selected integrated circuits are tested in real-time action and the results are compared with the desirable ones. On the other hand, there is test-time methods which they conclude logic and side-channel tests. Logic tests use test vectors to detect all possible trojans. Side-channel techniques measures data such as power consumption or path delay and they compare them with the results of a testified correct circuit called "golden". Nevertheless, there are also many different kinds of trojans. Most of the times, trojans are classified based on the activation mechanism. The two basic categories are triggers and payloads. Both of them can be digital or analog. Trigger trojan can be activated from an event like a specific value, for digital trojans, or a special event of a sensor, for analog trojans. Furthermore, payload Trojan can affect the output of the circuit for a specific combination of input values. All the above can destruct the function of a circuit and thus the whole system functionality. So, trusted devices with crucial meaning and purpose, probably have more possibilities to be hacked.

References

1. Sklavos N, Chaves R, Di Natale G, Regazzoni F (2017) Hardware Security and Trust, Springer.
2. M. Tehranipoor, C. Wang, Introduction to Hardware Security and Trust, Springer, 2012.
3. Xuan Thuy Ngo, Jean-Luc Danger, Sylvain Guilley "Hardware property checker for run-time Hardware Trojan detection", 2015 European Conference on Circuit Theory and Design (ECCTD), 24-26 August, 2015.

Analysis of Keystream Generators With KUF

Orhun Kara[1] and Muhammed F. Esgin[2]

[1] TÜBİTAK BİLGEM UEKAE, Gebze, Kocaeli, Turkey
orhun.kara@tubitak.gov.tr
[2] Faculty of Information Technology, Monash University, Clayton, Australia
muhammed.esgin@monash.edu

Extended Abstract

We have seen several examples of lightweight block ciphers in the literature in the last decade such as PRESENT, KATAN/KTANTAN, LED, Piccolo and SIMON/SPECK. On the other hand, there is almost no modern ultra lightweight stream cipher (say, having area less than 1000 GE). One exceptional example is the proposal by Armknecht and Mikhalev at FSE 2015 which they call keystream generators (KSGs) with Keyed Update Function (KUF), using the key in the state update. Armknecht and Mikhalev describe a design which they call Sprout. Sprout may be considered as the first modern ultra lightweight stream cipher with its hardware area cost less than 1000 GEs.

There have been several attacks on Sprout. All of them are dedicated analysis and mounted on Sprout itself. In this work, we study the security of keystream generators with keyed update functions in a generic setting. We mount a generic attack to a specific family of keystream generators with KUF, which we call *clockwise shifted keystream generators with KUF*. We define a concept of weak internal states. Roughly, a weak state is a state that can produce output up to some degree without the key. The attack is successful if a weak internal state occurs during the keystream generation.

We simply exploit the biased incorporation of key bits into the feedback function during the update of the internal states. We call the advantage in guessing a feedback value given the corresponding internal state as its *guess capacity*. The generic attack works on the shift registers with their average guess capacities larger than one half. First of all, weak states are determined and loaded in a table with their output pieces that they can produce without the key, and the table is sorted with respect to the outputs. Then, any weak state is examined during the online phase of the attack. Its feedback values up to several clocks are guessed and evaluated to check if the weak state examined is the correct state. It is possible to recover the correct internal state without knowing the key if one clocks the register enough number of times during each test, thanks to the guess capacity. The exact feedback values are determined after recovering the internal state. The last step is solving the system of the equations generated by the outputs of the feedback functions in order to recover the key.

Let s be the internal state size of a clockwise shifted KSG with KUF. Assume there are 2^{s_d} weak states. Then, the memory complexity is also around 2^{s_d}. We need roughly 2^{s-s_d} bits of keystream so that a weak state occurs with high probability. We run a test to check if a state is correct. The time complexity is proportional to $2^{s-\mu}$ where a weak state can produce μ bits of output without knowing the key. Actually, $2^{s-\mu}$ is approximately the number of the test. Assume each test costs roughly α_{ter} clocks. We provide a lower bound for α_{ter} for a satisfactory success rate and prove that it is inversely proportional to the correlation of the guess capacity.

One concrete example of our generic method is the attack mounted on Sprout. We treat Sprout as a clockwise shifted KSG with KUF. Sprout contains many weak states. Indeed, there are roughly 2^{s_d} states that can produce $83 - s_d$ bit outputs without the key. Its average guess capacity is very high and is equal to 0.75. More interestingly, the guess capacity is one for half of the states. It is possible to mount the generic attack on Sprout in practical limits.

An Improved Man-in-the-Middle Attack Against HB$^{\#}$ Authentication Protocols

Miodrag J. Mihaljević, Siniša Tomović and Milica Knežević
Mathematical Institute, Serbian Academy of Sciences and Arts, Belgrade

HB$^{\#}$ and Random-HB$^{\#}$ reported in [1] are important members of a family of HB-authentication protocols. In HB$^{\#}$ and Random-HB$^{\#}$, the response $\mathbf{z}$ based on which the verifier accept or reject authenticity of a prover is specified as the following: $\mathbf{z} = \mathbf{aX} \oplus \mathbf{bY} \oplus \mathbf{e}$ where all matrices and vectors are binary and $\mathbf{X}$, $\mathbf{Y}$ have dimensions $k_X \times m$ and $k_Y \times m$, respectively, and $\mathbf{a}$, $\mathbf{b}$, $\mathbf{z}$ have dimensions k_X, k_X and m respectively. The matrices $\mathbf{X}$ and $\mathbf{Y}$ are the secret ones determined by the secret keys of dimension $k_X + k_Y + 2m - 2$ and $(k_X + k_Y)m$ for HB$^{\#}$ and Random-HB$^{\#}$, respectively. MIM attack against HB$^{\#}$ reported in [2] enforces that the verifier decides on acceptance/rejection based on the following: $||\mathbf{aX} \oplus (\mathbf{b} \oplus \bar{\mathbf{b}})\mathbf{Y} \oplus (\mathbf{z} \oplus \bar{\mathbf{z}})||$ where $\mathbf{z} = (\mathbf{a} \oplus \bar{\mathbf{a}})\mathbf{X} \oplus \mathbf{bY} \oplus \mathbf{e}$ and $(\bar{\mathbf{a}}, \bar{\mathbf{b}}, \bar{\mathbf{z}})$ is a suitable triplet wiretapped from an authentication session between a legitimate prover and verifier where $\bar{\mathbf{z}} = \bar{\mathbf{a}}\mathbf{X} \oplus \bar{\mathbf{b}}\mathbf{Y} \oplus \bar{\mathbf{e}}$. The MIM attack proposed in [2] consists of the following main steps: (i) estimation the weight of $\bar{\mathbf{e}}$ based on the acceptance rate after number of modified authentication sessions; (ii) recovering i-th bit of $\bar{\mathbf{e}}$ based on the estimated weight of $\bar{\mathbf{e}}$ and the acceptance rate after an additional number of modified authentication sessions where i-th position of $\bar{\mathbf{e}}$ is flipped, $i = 1, 2, ..., m$; (iii) construction and solving a system of linear equations where unknowns are the secret key bits.

In this talk we show that all three steps (i)-(iii) could be improved resulting in a significantly reduced complexity of the secret key recovery. The main underlying ideas for improvement of the attack are the following ones. As a motivation for our consideration of the advanced MIM attacks, we point out to the following issue: The only input for estimation of the noise bits is the acceptance rate - All other operations employed in [2] are basically just certain deterministic manipulations of the acceptance rate. Accordingly, a natural question is the following one: Is it possible to directly evaluate the noise bits based on the acceptance rate. A preliminary answer is "Yes" but under condition that we know the relevant probability distributions. Consequently we focus on the following approach:
- consider numbers of successful authentications c and c' as realizations of the integer random variables C and C', respectively;
- based on the probability distributions of C and recorded c estimate the weight of $\bar{\mathbf{e}} = [\bar{\mathbf{e}}_\mathbf{i}]_{\mathbf{i=1}}^{\mathbf{m}}$;
- introduce the conditional probability distributions $\{\Pr(C' = x|H_i)\}_{x=0}^{n}$, $i = 0, 1$, where H_0 and H_1 correspond to the hypotheses that $\bar{e}_i$ is equal 0 and 1, respectively, $i = 1, 2, ..., m$;
- assuming that $\bar{e}_i$ is a realization of a random variable E such that $\Pr(E = 1) = p < 1/2$, and $\Pr(E = 1) = 1 - p$, after experimentally obtained c'_i, estimate e_i as follows: $\bar{e}_i = 0$ if $\frac{(1-p)\Pr(C'=c'_i|H_0)}{p\Pr(C'=c'_i|H_1)} > 1$, otherwise, $\bar{e}_i = 1$.

The steps (i) and (ii) of the MIM attack reported in [2] have been improved employing the above underlying ideas, and the step (iii) has been improved through a more efficient approach for solving the system of equations.

Complexity of the proposed improved MIM attack has been evaluated theoretically and experimentally, and the experiments confirm the theoretically obtained results. The obtained experimental results on complexity of the improved MIM attack are compared with the ones claimed in [2] in Table 1 which shows that a significant improvement has been obtained.

	Random HB$^{\#}$	HB$^{\#}$
claimed complexity of the MIM attack reported in [2]	$2^{30.1}$	$2^{21.7}$
complexity of the proposed improved MIM attack	$2^{25.3}$	$2^{16.9}$

Table 1: Table 1. Comparison of the complexities of the secret key recovery when $k_X = 80$, $k_Y = 512$, $m = 441$ and $\tau = 0.125$ (claimed complexity of the MIM attack reported in [2] has been corrected for the missing factor 4).

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.

Univariate Power Analysis Attacks Exploiting Static Dissipation of Nanometer CMOS VLSI Circuits for Cryptographic Applications

D. Bellizia, S. Bongiovanni, P. Monsurrò, G. Scotti, A. Trifiletti[1]

[1] University of Rome Sapienza, Dpt. of Information, Electronics and Telecom. Engineering

Side-Channel Attacks (SCAs) attempt to recover secret data – such as cryptographic keys – exploiting the information leaked by the digital hardware during its operation. Power Analysis Attacks (PAAs) use the dependence of power consumption on the processed data as a source of information. We here exploit static power consumption, arising because of parasitic diode currents and sub-threshold conduction in advanced CMOS processes. Device scaling make information leakage larger, because device variability and sub-threshold leakage worsen: this is particularly true for ultra-constrained devices, meant to operate in low-voltage low-power conditions. Information theory can provide concepts to extract information leaking from digital processing of the cryptographic keys. The mutual information $I(X;L)$ between two random processes X and L (where X are the keys, and L is static power consumption) is the difference between the entropy $H(X)$ of X and the conditional entropy of X given L, $H(X|L)$. If L has no relation to X, mutual information is zero; if the leakage current carries information about the secret key, mutual information is positive. The ideal digital implementation of a cryptographic algorithm with no leakage would show no mutual information between the key and the static current. By computing $I(X;L)$ it is possible to evaluate the information leaked through the side-channel in the ideal case of an attacker which can measure the actual device and create a full template model. These ideas are here used for Attacks Exploiting Static Power (AESP). It is shown that many logic families designed to be robust against dynamic power attacks are more vulnerable to AESP attacks than conventional CMOS gates: WDDL (wave dynamic differential logic) and MDPL (masked dual-rail pre-charged logic) devices show higher mutual information than conventional CMOS, whereas only SABL (sense-amplifier based logic) devices show lower leakage. A potential effective solution to information leakage through static power may come from another logic style, the time-enclosed logic (TEL). TEL gates code information as relative delays between two paths. The steady-state of TEL gates is independent on the processed data, as all the processing is performed during the transient. This means that integrating static power consumption data yields close to no information on the internal state of the circuit.

References

1. D. Bellizia, S. Bongiovanni, P. Monsurrò, G. Scotti, and A. Trifiletti: Univariate Power Analysis Attacks Exploiting Static Dissipation of Nanometer CMOS VLSI Circuits for Cryptographic Applications. IEEE Trans. Emerg. Topics in Comp. (In Press)

UI deception at its finest: The Android case

Constantinos Patsakis, Efthimios Alepis

Department of Informatics, University of Piraeus
80, Karaoli & Dimitriou, 18534, Piraeus, Greece

Mobile interfaces due to the lack of space have to squeeze a lot of UI components and information in a rather limited environment. Therefore, while the UI seems rather simple, it is infact rather complex. Moreover, since all applications share the same small screen, they end up stacking on top of each other, which becomes more complex as applications which work on the background may pop up on top of others. This increases the complexity further because as our work illustrates, users cannot always accurately determine to which application does a foreground component belong.

While *clickjacking* techniques were firstly introduced to browsers, they soon became popular in mobile environments and transformed into what we call *tapjacking* where users are tricked into clicking/tapping on seemingly benign objects in applications, which are far from being what they appear to be. As a result, they may greatly expose themselves.

The goal of this presentation is to showcase some attacks which can be launched against Android, but most importantly against Marshmallow and Nougat, the two latest and significantly hardened versions. More presicely, we discuss how Android permission model allows applications without dangerous permissions to sniff the users' PIN/pattern and perform a range of other dangerous and unauthorised tasks. The use of the zero permission model highlights the significance of our attacks since not only users do not see any potential harmful permission to grant, but the permissions are automatically granted and cannot be revoked, providing both stealthness and persistence to the malicious application.

Certifying the Uncertifiable: A Critique of Common Criteria EAL4+ using the DESFire EV1 TRNG

Darren Hurley-Smith and Julio Hernandez-Castro
University of Kent

Abstract

Common Criteria is a set of internationally standardised security guidelines that have been in effect since 1999. A component of these standards is the Evaluation Assurance level, or EAL. These levels (1 through 7) represent increasing requirements of the manufacturer, to acquire Common Criteria certification of a product. EAL4+, for example, indicates that a product is manufactured with what are described as 'good' security practices. This does not require Common Criteria oversight during manufacture, it is a retroactive certification based on inspections and testing. EAL testing is solicited by the manufacturer. Examples of EAL4+ certified products are: Red Hat Enterprise Linux 5, Windows 7, FreeBSD, and the DESFire EV1 smart card.

The Bundesamt fur Sichterheit in der Informationstechnik (BSI) has published results of NXP's DESFire EV1 assessment [2]. Through examination of this report, it is apparent that significant testing is performed against cryptographic algorithms. The level of security is evaluated as sufficient to meet the EAL4+ standard. However, the nonces used during authentication and cryptographic processes are tested under BSI standard AIS 31 [3]. This document suggests testing deterministic RNGs (pseudo and true generators) for entropy, NIST800-60 compliance and uniformity of output.

Our research, has shown that testing only for entropy, uniformity and bit-level chi-square goodness of fit is insufficient [4]. Many existing batteries, such as Dieharder and NIST STS, do not detect any significant issues with DESFire EV1 TRNG output. However, it has been proven that there are clear and consistent biases in the output of this particular TRNG, that were not detected by the EAL4+ testing process (and by extension BSI AIS 31). We propose that although the Common Criteria system is fit for its stated purpose and remains within its stated bounds, additional testing is required to pick upon errors that may occur due to post-processing of output, such as whitening functions.

This hypothesis is founded on similar observations made by Oswald and Paar when reporting on their side-channel attacks on the DESFire smart card [5]; reliance on mathematical principles of cryptographic security as a basis for testing is insufficient to guarantee security. Bernstein et al provide a noteworthy example in their work: Re-factoring RSA Keys from Certified Smart Cards [1]. In their work, they demonstrate that FIPS140-2 is only sufficient to outline the basic security functionality of a device, not enforce standards sufficient to prevent tampering or derivation of security data.

Building on published work and confirmation of our findings by NXP after responsible disclosure, we have conducted a test of 100 DESFire EV1 cards, to determine whether our initial results were isolated to particularly bad hardware. This has been found to not be the case, with over 68% of cards demonstrating very poor byte-level chi-square goodness of fit for only 1 MB of TRNG output. These results match our previously reported bias, demonstrating an issue that has eluded Common Criteria testing, and which may present a potential attack vector that is not considered in the DESFire EV1 EAL4+ compliance report.

Our discussion will focus on the limitations, both stated and unstated, of the Common Criteria EAL4+ in the context of the DESFire EV1. We will demonstrate that current test batteries are founded on well-known fundamental principles, but do not account for the implementation choices of manufacturers. We will close by discussing future work, in which we will explore the possibility of a more collaborative post-implementation test methodology for TRNGs.

References

1. Bernstein, D. J., Chang, Y.-A., Cheng, C.-M., Chou, L.-P., Heninger, N., Lange, T., and Van Someren, N. (2013). Factoring rsa keys from certified smart cards: Coppersmith in the wild. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 341–360. Springer.
2. for Information Security, F. O. (2016). Bsi-dsz-cc-0955-2016 for nxp secure smart card controller p6021y vb including ic dedicated software from nxp semiconductors germany gmbh. Technical report, Federal Office for Information Security.
3. fur Sichterheit in der Informationstechnik, B. (2013). Evaluation of random number generators version 0.10. Technical report, Bundesamt fur Sichterheit in der Informationstechnik.
4. Hurley-Smith, D. and Hernandez-Castro, J. (2016). Bias in the mifare desfire ev1 trng. In *Radio Frequency Identification: 12th International Workshop, RFIDsec 2016, Hong Kong, China, November 30-December 2, 2016*. Springer International Publishing.
5. Oswald, D. and Paar, C. (2011). Breaking mifare desfire mf3icd40: power analysis and templates in the real world. In *Int. Workshop on Cryptographic Hardware and Embedded Systems*, pages 207–222. Springer.

Measuring the Distance: Reverse Engineering the DESFire EV2 Distance Bounding Protocol

Darren Hurley-Smith and Julio Hernandez-Castro
University of Kent

Abstract

Radio Frequency Identification (RFID), is used in a countless range of applications. Access control, personal identification, transport and retail all make use of such systems in the name of expediency and convenience. As the criminal element has targeted these devices, a steady increase in the security capabilities of such devices has been observed. The Mifare Classic provides a sterling example of a platform that was compromised by analysis of its crypto-systems and hardware, with a practical attack demonstrated by de Konig Gans in 2008 [1]. This has resulted in the widespread adoption of open cryptographic algorithms, including AES-128, as a standard across multiple platforms (Mifare DESFire, Mifare PLUS X, FeliCa, etc.) [2]

However, cryptographic attacks are not the only threat faced by modern RFID implementations. Usurpation of communication sessions, by means of relay attacks, is a valid concern. Though authentication may protect the content of an RFID card against casual decryption and analysis, it does not protect it from attacks that seek to manipulate an RFID device into a vulnerable state, by injecting commands at critical moments in the communication between card and reader [3].

A class of security algorithms knows as distance bounding protocols were proposed in the early 1990's, though the physical limitations of RF communication and computer technology prevented their use in the crowded, confined environments in which modern RFID usage often takes place. Brands and Chaum discuss the theoretical characteristics of early distance bounding protocols, suggesting their potential as a means to provide security to RFID communication under threat form relay attacks [4]. The theoretical development of distance bounding protocols has continued alongside efforts to implement workable interpretations of such theory in practical applications. This has led to the introduction of some of the first commercially available RFID cards that boast distance bounding features.

The Mifare DESFire EV2 is one such example. Designed as a multi-application card, supporting third-party after market application initialisation and authentication, it is marketed as a highly secure (Common Criteria EAL5+) RFID card. There is not yet an evaluation of its distance bounding protocol, and as such, we undertake an examination of its distance bounding protocol from a consumer perspective. The distance bounding protocol used is not documented in publicly available literature, requiring reverse engineering in software, with an analysis of the timing characteristics and random number generator used as elements of its security system.

We present our reverse engineering methodology, findings, timings and a security evaluation. The theoretical resilience of the derived protocol is investigated, with attention given to mafia, distance and terrorist frauds [5, 6]. Future work is also discussed, with a focus on potential attacks and current unknowns regarding the potential countermeasures implemented on the EV2. A good example of this is the potential for fast-phase replay attacks, which our results suggest are possible without strict verifier rules.

References

1. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D Garcia. A practical attack on the mifare classic. In *Int. Conference on Smart Card Research and Advanced Applications*, pages 267–282. Springer, 2008.
2. NXP Semiconductors Ltd. *The Success of Mifare*. NXP Semiconductors. Retrieved from: https://www.mifare.net/en/ 17:00 05/10/2016.
3. Jason Reid, Juan M Gonzalez Nieto, Tee Tang, and Bouchra Senadji. Detecting relay attacks with timing-based protocols. In *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pages 204–213. ACM, 2007.
4. Stefan Brands and David Chaum. Distance-bounding protocols. In *Advances in Cryptology-EUROCRYP93*, pages 344–359. Springer, 1994.
5. Jolyon Clulow, Gerhard P Hancke, Markus G Kuhn, and Tyler Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In *Security and Privacy in Ad-Hoc and Sensor Networks*, pages 83–97. Springer, 2006.
6. Cas Cremers, Kasper B Rasmussen, Benedikt Schmidt, and Srdjan Capkun. Distance hijacking attacks on distance bounding protocols. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 113–127. IEEE, 2012.

The Success Rate Reconsideration of the MIM Attack Against HB# Authentication Protocols

Siniša Tomović, Milica Knežević and Miodrag J. Mihaljević *

HB family of authentication protocols has attracted a lot of attention because of their simple implementations and the provable security based on the well-known hard problem - learning parity with noise (LPN). Prominent representatives of this family are Random-HB# and HB#. Their authentication procedure consists of the following steps: first, the tag sends a blinding vector $\mathbf{b}$ to the reader and the reader responds with challenge vector $\mathbf{a}$ to the tag. Then tag sends $\mathbf{z} = \mathbf{aX} \oplus \mathbf{bY} \oplus \mathbf{e}$ to the reader, where $\mathbf{e}$ is a noise vector whose bits independently follow Bernoulli distribution with coefficient τ, and $\mathbf{X} \in \mathbb{Z}_2^{k_X \times m}, \mathbf{Y} \in \mathbb{Z}_2^{k_Y \times m}$ are the secret keys (random matrices for Random-HB# and so-called Toeplitz matrices for HB#). The reader validates the tag, ie. accepts its response if the weight $\|\mathbf{aX} \oplus \mathbf{bY} \oplus \mathbf{z}\|$ falls under a certain threshold value.

Random-HB# and HB# are formally proven to be secure in a specific GRS man-in-the-middle attack scenario [1], where the adversary is able to modify only the challenge vectors sent from the reader. In [2] Ouafi, Overback and Vaudenay have proposed an efficient and general man-in-the-middle (MIM) attack where the adversary modifies all messages during communication session (the OOV attack). The main idea behind the OOV attack is that the secret values can be extracted from the reader's acceptance rate after repeating specific MIM protocol modifications. Namely, the adversary first eavesdrops a protocol session to obtain a triplet of exchanged messages $(\bar{\mathbf{a}}, \bar{\mathbf{b}}, \bar{\mathbf{z}} = \bar{\mathbf{a}}\mathbf{X} + \bar{\mathbf{b}}\mathbf{Y} + \bar{\mathbf{e}})$. Then he modifies n consecutive protocol sessions by replacing current $\mathbf{a}, \mathbf{b}, \mathbf{z}$ with $\hat{\mathbf{a}} = \mathbf{a} \oplus \bar{\mathbf{a}}, \hat{\mathbf{b}} = \mathbf{b} \oplus \bar{\mathbf{b}}, \hat{\mathbf{z}} = \mathbf{z} \oplus \bar{\mathbf{z}}$, respectively, and counts the number c of succesfull authentications after those replacements. The authors have claimed that the acceptance rate c/n follows binomial distribution, and use the normal distribution cummulative function as its approximation ie. $c/n \approx \Phi(\frac{thr-(m-\|\bar{e}\|)\tau-\|\bar{e}\|(1-\tau)}{\sqrt{m\tau(1-\tau)}})$ to estimate the weight $\|\bar{\mathbf{e}}\|$ of the noise vector $\bar{\mathbf{e}} = \bar{\mathbf{a}}\mathbf{X} + \bar{\mathbf{b}}\mathbf{Y} + \bar{\mathbf{z}}$, for the sample size n large enough. Then they recover $\bar{\mathbf{e}}$ by flipping its bits and measuring its changed weight, obtaining the linear combination $\bar{\mathbf{a}}\mathbf{X} + \bar{\mathbf{b}}\mathbf{Y}$. The secret keys are found as the solution of the linear system made of enough of these linear combinations for different triplets $(\bar{\mathbf{a}}, \bar{\mathbf{b}}, \bar{\mathbf{z}})$.

We have experimentally evaluated the OOV attack and it appears significantly less successful in comparison what has been claimed in [2] for the specified sample size n. We have found that, although the main idea of the attack is correct, the lower rate of success appears as a consequence of employment of inadequate approximation of the real probability distribution of the acceptance rate. More precisely, the acceptance rate of the employed modifications actually follows the so-called Poisson-Binomial distribution and it has been inadequately (for the claimed sample size) approximated by the normal distribution, resulting in an increased probability of incorrect estimation of the noise vector and accordingly construction of an incorrect system of linear equations. We point out that the probability of the acceptance, as a function of the parameters $m, \tau, \|\bar{\mathbf{e}}\|, thr$, can be expressed as:

$$pb(\|\bar{\mathbf{e}}\|, thr) = \sum_{i=0}^{thr} \sum_{j=0}^{\min\{i,\|\bar{\mathbf{e}}\|\}} \binom{\|\bar{\mathbf{e}}\|}{j} \binom{m - \|\bar{\mathbf{e}}\|}{i-j} \tau^{\|\bar{\mathbf{e}}\|+i-2j} (1-\tau)^{m-(\|\bar{\mathbf{e}}\|+i-2j)} .$$

After replacement the approximation with the above exact probability distribution we have obtained the experimentally verified significantly better success rate of the attack.

References

[1] Gilbert, H., Robshaw, M.J.B., Seurin, Y. *HB#*:Increasing *the Security and Efficiency of HB+*, Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 361–378. Springer, Heidelberg (2008)

[2] Ouafi, K., Overbeck, R., Vaudenay, S.: *On the Security of HB# against a Man-in-the- Middle Attack*. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 108-124. Springer, Heidelberg (2008)

*M. Mihaljević, S. Tomović and M. Knežević are with Serbian Academy of Sciences and Arts, Belgrade, Serbia.

Pushing elliptic curve speed limits in OpenSSL

Nicola Tuveri[*], Billy Bob Brumley[*], and Patrick Longa[**]

[*]Department of Pervasive Computing, Tampere University of Technology
[**]Microsoft Research, USA

Public key, or asymmetric, cryptography represents a major revolution in modern cryptography and the enabling factor in most modern digital communications and many other technologies based on online and offline authentication and authorization schemes.

One of the main disadvantages of asymmetric cryptography over symmetric cryptography is the cost in terms of computation and memory required; elliptic curve cryptography (ECC), suggested independently by Miller [7] and Koblitz [4] since 1985, has seen increasingly wide adoption due to the vast improvements on both cost factors while providing the same level of security of "traditional" public key cryptography.

Nonetheless, asymmetric cryptography continues to be computationally expensive: new curves have been recently proposed to further improve ECC performances, and we focus our research on Curve25519 [2] and Four$\mathbb{Q}$ [3]. These two curves attain considerable performance improvements by taking into account hardware and implementation factors in the mathematical design of the curves, addressing the optimization of the underlying field operations and reducing the number of group operations involved in scalar multiplications.

During our research we focus on OpenSSL, a popular software library widely adopted to provide cryptographic security, and measure the performance of the implementation of Curve25519 included in OpenSSL 1.1.0. Finding that it does not meet the expected speed, we propose and benchmark the integration of an alternative implementation by A. Langley [6]. We also benchmark and propose the integration of the reference implementation of the Four$\mathbb{Q}$ curve [1, 5].

For the integration we use the *engine API* exposed by OpenSSL, which provides a way to opt, at runtime, for alternative implementations of the cryptosystems defined in the library at compile-time.

The results show considerable speed improvements over the previous implementations and set unprecedented speed records.

References

[1] Tolga Acar, Patrick Longa, Karen Easterbrook, Craig Costello, and Brian LaMacchia. FourQlib, 2015. URL https://www.microsoft.com/en-us/research/project/fourqlib/.

[2] Daniel J Bernstein. Curve25519: new Diffie-Hellman speed records. In *International Workshop on Public Key Cryptography*, pages 207–228. Springer, 2006. URL https://cr.yp.to/ecdh/curve25519-20060209.pdf.

[3] Craig Costello and Patrick Longa. *Four$\mathbb{Q}$: Four-Dimensional Decompositions on a $\mathbb{Q}$-curve over the Mersenne Prime*, pages 214–235. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015. ISBN 978-3-662-48797-6. URL http://eprint.iacr.org/2015/565.

[4] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177): 203–203, 1987. doi: 10.1090/s0025-5718-1987-0866109-5. URL http://dx.doi.org/10.1090/S0025-5718-1987-0866109-5.

[5] Watson Ladd, Patrick Longa, and Richard Barnes. Curve4Q. Internet-Draft draft-ladd-cfrg-4q-00, IETF Secretariat, September 2016. URL http://www.ietf.org/internet-drafts/draft-ladd-cfrg-4q-00.txt.

[6] Adam Langley. curve25519-donna, 2008. URL https://code.google.com/archive/p/curve25519-donna/.

[7] Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 417–426. Springer, 1985.