Lecture Notes in Computer Science 9522

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

More information about this series at http://www.springer.com/series/7410

Ion Bica · David Naccache
Emil Simion (Eds.)

Innovative Security Solutions for Information Technology and Communications

8th International Conference, SECITC 2015
Bucharest, Romania, June 11–12, 2015
Revised Selected Papers

Springer

Editors
Ion Bica
Military Technical Academy
Bucharest
Romania

David Naccache
Departement d Informatique
Ecole Normale Superieure
Paris
France

Emil Simion
Advanced Technologies Institute
and University Politehnica of Bucharest
Bucharest
Romania

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-27178-1 ISBN 978-3-319-27179-8 (eBook)
DOI 10.1007/978-3-319-27179-8

Library of Congress Control Number: 2015956125

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by SpringerNature
The registered company is Springer International Publishing AG Switzerland

Foreword

The present volume is the outcome of the 8^{th} International Conference on Security for Information Technology and Communications that comes in a long series of successful events starting in 2008. This conference series was founded to foster novel and exciting research in this area and to help generate new directions for further research and development.

Information and Communications Technologies (ICT) encourage globalization, exchange of information, and the proliferation of cyber space. The advantages of using these technologies are immense but, alongside opportunities, a broad range of issues and drawbacks have limited to some extent the full extraction of benefits from ICT use. One of the main issues with ICT today is ***security***, which has to deal with the flourishing of a myriad electronic attacks, malware, vulnerabilities, and intrusions in the domain of information and communications technologies.

For seven years, SECITC has brought together computer security researchers, cryptographers, industry representatives, and graduate students. One of SECITC's primary goals is to gather researchers from different communities and provide a forum allowing for the informal exchanges necessary for the emergence of new scientific collaborations. Special attention was devoted to young researchers, master and Ph students, with scientific interests in the field of information security, cyber defense, cryptography, and communications and network security.

The initial concept of SECITC arose from a teaching and research collaboration between the two co-founder universities, Military Technical Academy and Bucharest University of Economic Studies, which was meant to highlight the increasing importance of computer and information security. This was followed by discussions with a number of fellow cyber security researchers. Their enthusiastic encouragement persuaded the co-founder universities to move ahead with the daunting task of creating a high-quality conference.

The organization of a conference like SECITC requires the collaboration of many individuals. First of all, we would like to thank the authors and the keynote speakers for graciously accepting our invitation. We express our gratitude to the Program Committee members and external reviewers for their efforts in reviewing the papers, engaging in active online discussion during the selection process, and providing valuable feedback to authors. Last but not least, we would like to thank the two co-chairs of the conference, Prof. David Naccache and Dr. Emil Simion for their special effort to ensure the scientific high quality of our conference.

November 2015 Victor-Valeriu Patriciu

Preface

This volume contains the papers presented at SECITC 2015, the 8th International Conference on Security for Information Technology and Communications (www.secitc.eu), held during June 11–12, 2015, in Bucharest.

There were 34 submissions and each submitted paper was reviewed by at least three Program Committee members. The committee decided to accept 15 papers, and the program also included three invited guest speakers.

For seven years SECITC has been bringing together computer security researchers, cryptographers, industry representatives, and graduate students. The conference focuses on research on any aspect of security and cryptography. The papers present advances in the theory, design, implementation, analysis, verification, or evaluation of secure systems and algorithms.

One of SECITC's primary goals is to bring together researchers belonging to different communities and provide a forum that facilitates the informal exchanges necessary for the emergence of new scientific collaborations. We would like to acknowledge the work of the Program Committee, whose great efforts provided a proper framework for the selection of the papers.

The conference was organised by Advanced Technologies Institute, Bucharest University of Academic Studies and Military Technical Academy.

May 2015

Ion Bica
David Naccache
Emil Simion

Organization

Program Committee

Ludovic Apvrille	Telecom ParisTech, France
Sambit Bakshi	National Institute of Technology Rourkela, India
Paulo Barreto	University of São Paulo, Brazil
Ion Bica	Military Technical Academy, Romania
Catalin Boja	Bucharest Academy of Economic Studies, Romania
Sanjit Chatterjee	Indian Institute of Science, India
Liqun Chen	Hewlett-Packard Laboratories
Xiaofeng Chen	Xidian University, China
Christophe Clavier	Université de Limoges, France
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Joan Daemen	STMicroelectronics
Naccache David	Ecole Normale Superieure, France
Eric Diehl	Sony Pictures
Itai Dinur	Ecole Normale Superieure, France
Bao Feng	HuaWei
Eric Freyssinet	IRCGN
Wang Guilin	IRCGN, Huawei International Pte. Ltd.
Helena Handschuh	Rambus – Cryptography Research
Xinyi Huang	Fujian Normal University, China
Malay Kishore Dutta	Amity School of Engineering and Technology, India
Jean-Louis Lanet	Inria-RBA, France
Tancrede Lepoint	CryptoExperts
Kostas Markantonakis	ISG-Smart Card Centre, Founded by Vodafone, G&D and the Information Security Group of Royal Holloway, University of London, UK
Alfred Menezes	University of Waterloo, Canada
Dan Page	University of Bristol, UK
Victor-Valeriu Patriciu	Military Technical Academy, Romania
Rene Peralta	NIST
Giuseppe Persiano	University of Salerno, Italy
Bart Preneel	Katholieke Universiteit Leuven - COSIC, Belgium
Reyhanitabar Reza	EPFL, Lausanne, Switzerland
Mark Ryan	University of Birmingham, UK
Peter Ryan	University of Luxembourg, Luxembourg

Pierangela Samarati	Università degli Studi di Milano, Italy
Damien Sauveron	XLIM, UMR University of Limoges/CNRS 7252, France
Emil Simion	Advanced Technologies Institute and University Politehnica of Bucharest, Romania
Rainer Steinwandt	Florida Atlantic University, USA
Willy Susilo	University of Wollongong, Australia
Mehdi Tibouchi	NTT Secure Platform Laboratories
Cristian Toma	Bucharest University of Economic Studies, Romania
Michael Tunstall	Rambus – Cryptography Research
Ingrid Verbauwhede	KU Leuven, ESAT/COSIC, Belgium
Qianhong Wu	Beihang University, China
Moti Yung	Google and Columbia University, USA
Lei Zhang	East China Normal University, China

Additional Reviewers

Apvrille, Axelle
Debiao, He
Donida Labati, Ruggero
He, Shuangyu
Lugou, Florian
Singelee, Dave
Sinha Roy, Sujoy
Wang, Ding
Wurcker, Antoine
Zhang, Yuexin

Invited Talks

Authenticated-Encryption: Security Notions, Designs and Applications

Reza Reyhanitabar

EPFL, Switzerland

Abstract. Practical applications of symmetric-key encryption usually aim for two complementary data security properties: confidentiality (privacy) and authenticity (integrity). Yet classical encryption modes such as CBC solely provide confidentiality; hence, are an inadequate tool of a very limited utility unless combined appropriately with an additional cryptographic primitive called a message authentication code (MAC).

An authenticated encryption (AE) scheme simultaneously provides confidentiality and authenticity. The historically popular generic composition paradigm to build an AE scheme by combining two separate primitives, one to ensure confidentiality and another to guarantee authenticity, is neither most efficient nor most robust to implementation errors. This motivated the emergence of dedicated AE designs. AE has been studied for over a decade, yet remains a highly active and interesting area of research as evidenced by the currently running CAESAR competition by the cryptographic community. The competition aims to boost public discussions towards a better understanding of AE designs and to identify a portfolio of next-generation AE schemes by 2017.

In this talk we will explore the historical development of AE as a cryptographic goal and different methods to achieve this goal. I will start by explaining some of the failed attempts to use encryption-with-redundancy mechanisms; for example, the CBCC scheme (CBC encryption with the XOR of the message blocks as the checksum). Then I will talk about the emergence of AE as a formally defined security notion in its own right in 2000. We will explore the generic composition paradigm to achieve the AE goal. I will then look at the evolution of dedicated AE designs, offering better efficiency and usability compared to generic composition, from the introduction of RPC, IAPM, XCBC and OCB in 2001 to the currently running CAESAR competition with 57 algorithms as its first-round submissions.

Importance of useable AE to practice, and to some extent, difficulty of getting it right, is evident from the number of standards in which different AE constructions have been specified (such as IEEE 802.11i, NIST SP 800-38D, ANSI C12.22, and ISO/IEC 19772:2009) as well as widely-deployed standard protocols that employ AE schemes (such as IPsec, SSH, SSL/TLS). Finally, we will look at these standards.

Keywords: Authenticated encryption · Security notions · Provable security · Generic composition · Dedictaed AE designs · CAESAR competition.

New Results on Identity-Based Encryption from Quadratic Residuosity

Ferucio Laurenţiu Ţiplea[1] and Emil Simion[2]

[1] Department of Computer Science, "Al.I.Cuza" University of Iaşi,
700506 Iaşi, Romania
fltiplea@info.uaic.ro
[2] Advanced Technologies Institute, Bucharest, Romania,
ati@dcti.ro

Abstract. This invited talk surveys the results obtained so far in designing identity-based encryption (IBE) schemes based on the quadratic residuosity assumption (QRA). We begin by describing the first such scheme due to Cocks, and then we advance to the novel idea of Boneh, Gentry and Hamburg. Major improvements of the Boneh-Gentry-Hamburg scheme are then recalled. The recently revealed algebraic torus structures of the Cocks scheme allows for a better understanding of this scheme, as well as for new applications of it such as homomorphic and anonymous variants of it.

Identity-based encryption (IBE) was proposed in 1984 by Adi Shamir [10] who formulated its basic principles but he was unable to provide a solution to it, except for an identity-based signature scheme. Sakai, Ohgishi, and Kasahara [9] have proposed in 2000 an identity-based key agreement scheme and, one year later, Cocks [4] and Boneh and Franklin [1] have proposed the first IBE schemes. Cocks' solution is based on quadratic residues. It encrypts a message bit by bit and requires $2\log n$ bits of cipher-text per bit of plain-text. The scheme is quite fast but its main disadvantage is the ciphertext expansion. Boneh and Franklin's solution is based on bilinear maps. Moreover, Boneh and Franklin also proposed a formal security model for IBE, and proved that their scheme is secure under the Bilinear Diffie-Hellman (BDH) assumption.

The Cocks scheme [4] is very elegant and per se revolutionary. It is based on the standard QRA modulo an RSA composite. The scheme encrypts one bit at a time. The bits are considered to be exactly the two values (i.e., -1 and 1) of the Jacobi symbol modulo an RSA modulus n, when applied to an integer non-divisible by n. Thus, if Alice wants to send a bit $b \in \{-1, 1\}$ to Bob, she randomly generates an integer t with the Jacobi symbol b modulo n, hides t into a new message $s = t + at^{-1} \bmod n$ obtained by means of Bob's identity a, and sends s to Bob. The decryption depends on whether a is a quadratic residue or not modulo n. As neither Alice nor Bob knows whether a is a quadratic residue or not, Alice repeats the procedure above with another integer t' whose Jacobi symbol modulo n is b, and sends $s' = t' - at'^{-1} \bmod n$ as well. Now, Bob

Work partially supported by the Romanian National Authority for Scientific Research (CNCS-UEFISCDI) under the project PN-II-PT-PCCA-2013-4-1651.

can easily decrypt by using a private key obtained from the key generator, because either a or $-a$ is a quadratic residue modulo n. It can be shown that the Cocks IBE scheme is IND-ID-CPA secure in the random oracle model under the QRA.

The main disadvantage regarding the efficiency of the Cocks scheme consists of the fact that it encrypts one bit by $2\log n$ bits. A very interesting idea proposed by Boneh, Gentry and Hamburg [2] is to encrypts a stream of bits by multiplying each of them by an Jacobi symbol randomly generated. The generation of these new Jacobi symbols are based on the equation $ax^2 + Sy^2 \equiv 1 \bmod n$. Any solution to this congruential equation leads to two polynomials f and g with the property that $g(s)$ and $f(r)$ have the same Jacobi symbol modulo n, for any square root s of S and any square root r of a. Therefore, g can be used to encrypt one bit, while f can be used to decrypt it. If the solutions of the above congruential equation can be obtained by a deterministic algorithm, then the decryptor knows how to decryt the ciphertext. Therefore, in order to send an ℓ-bit message to Bob, Alice has to solve 2ℓ equations as above (two equations for each bit, one for Bob's identity a and the other one for $-a$), while the decryptor needs to solve only ℓ equations. The ciphertext size is $2\ell + \log n$ bits. Some improvements at the sender side reduces the number of equations to be solved by the encryptor to $\ell + 1$.

An important improvement of the Boneh-Gentry-Hamburg (BGH) scheme was proposed later by Jhanwar and Barua [7]. The improvement works in two directions: improve the time complexity of the algorithm to solve equations $ax^2 + Sy^2 \equiv 1 \bmod n$, and reduce the number of equations to be solved. The first improvement is based on a careful analysis of the solutions of the equation $ax^2 + Sy^2 \equiv 1 \bmod n$. Thus, an efficient probabilist algorithm is developed to randomly generate solutions of such an equation. The second improvement is based on a composition formula according to which two solutions can be combined in some way to obtain a new solution. Therefore, to encrypt an ℓ-bit message, only $2\sqrt{\ell}$ equations need to be solved. Unfortunately, the probabilistic nature of the algorithm by which solutions are obtained leads to a ciphertext larger than in the case of the BGH scheme, namely $2\ell + 2\sqrt{\ell}\log n$ bits. The Jhanwar-Barua (JB) scheme was revisited in [6], where some errors were corrected; unfortunately, the security was not sufficiently argued as it was later remarked in [5]. Moreover, [5] also proposes an improvement by which the number of equations needed to be solved by Alice is reduced to $2\log \ell$. The ciphertext size is also reduced to $2\ell + 2(\log \ell)(\log n)$ bits.

It is well-known that the Cocks scheme is not anonymous [2]. Several researchers tried to extend this scheme to offer identity anonymity; usually, such extensions are based on creating lists of ciphertext so that the identity becomes hidden in the lists. This approach gives rise to very large ciphertexts. It was also a believe that the Cocks scheme does not have homomorphic properties. A very recent result [8] rehabilitates the Cocks scheme with respect to these two weaknesses. Joye [8] identified the algebraic structure of the Cocks ciphertexts: he proved that these are squares in a torus like structure, and form a quasi-group. The underlying group law is the operation needed on ciphertexts to show that the Cocks scheme is homomorphic when the operation on clear messages is the multiplication. Therefore, the Cocks scheme offer homomorphic properties. Another important consequence obtained in [8] is about the anonymity

of the Cocks scheme. It was shown that a different way of computing the ciphertext, without expansion, leads to identity anonymity.

A very interesting question is whether high order Jacobi symbols can be used in the Cocks scheme in order to encrypt more than one bit at a time. A first attempt to do that is the one in [3]. Unfortunately, the only secure scheme proposed in [3] suffers from massive ciphertext expansion.

References

1. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. In: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pp. 213–229. CRYPTO 2001. Springer-Verlag, London, August 2001
2. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption without pairings. In: Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science, pp. 647–657. FOCS 2007. IEEE Computer Society, Washington, DC, USA (2007)
3. Boneh, D., LaVigne, R., Sabin, M.: Identity-based encryption with e^{th} residuosity and its incompressibility. In: Autumn 2013 TRUST Conference. Washington, DC, October 2013. Poster Presentation
4. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Proceedings of the 8th IMA International Conference on Cryptography and Coding, pp. 360–363. Springer-Verlag, London, December 2001
5. Ţiplea, F.L., Simion, E., Teşeleanu, G.: An improvement of Jhanwar-Barua's identity-based encryption scheme. Technical report (2015)
6. Elashry, I., Mu, Y., Susilo, W.: Jhanwar-Barua's identity-based encryption revisited. In: Au, M., Carminati, B., Kuo, C.C. (eds.) Network and System Security. LNCS, vol. 8792, pp. 271–284. Springer International Publishing (2014)
7. Jhanwar, M.P., Barua, R.: A variant of Boneh-Gentry-Hamburg's pairing-free identity-based encryption scheme. In: Inscrypt, pp. 314–331 (2008)
8. Joye, M.: On identity-based cryptosystems from quadratic residuosity (2015)
9. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: Symposium on Cryptography and Information Security. SCIS2000, January 2000
10. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO 84 on Advances in cryptology, pp. 47–53. Springer-Verlag New York, New York (1985)

Efficient Techniques for Extracting Secrets from Electronic Devices

Marios Choudary

University Politehnica of Bucharest
marios.choudary@cs.pub.ro

Summary

Smartcards, such as those provided to their customers by many banks across the world, use a microcontroller to encrypt or decrypt data, in order to authenticate a person (e.g. verify a PIN) or a transaction (e.g. generate an electronic transaction certificate), based on a secret key stored in the microcontroller. However, the physical implementation of a microcontroller *leaks* information via a *side-channel*, such as the power-supply current or electromagnetic emanations. This leakage may allow an attacker to recover the secret key of a microcontroller, and use that to generate valid certificates for unlawful commercial transactions. To reduce this threat, microcontrollers used in the smartcards provided by banks have several layers of countermeasures to limit the amount of side-channel information available to an attacker. But, to develop efficient countermeasures, and to have a correct assessment of the level of security provided by such smartcards, it is important to have a good understanding of the potential of side-channel attacks.

Along the search for better cryptosystems during the two World Wars, to encrypt messages over a particular communication channel, the military discovered the possibility of "listening" to the main communication channel by means of another, unintentional, channel, known as the *side-channel*. As Kuhn [11, Section 1.1.1] and Markettos [12, Section 2.11.1] describe in more detail, there were many such cases during the past century. Among the first known cases, during the First World War, the Germans were able to retrieve the communications of enemy troops, by analysing the earth return-current of the single-wire telegraph system used by those troops [1]. Another important case, this time involving a cryptosystem, was the side-channel analysis performed by British intelligence on the French embassy in London, around 1960–1963 [14]. MI5 and GCHQ scientists used a broad-band radio-frequency tap on the communication line used by the French embassy to transmit information, encrypted using a *low-grade* cipher, in the hope of obtaining partial information of the plaintext, that may *leak* into the channel. It turned out that they were indeed able to retrieve the plaintext of the communication encrypted using the low-grade cipher. Furthermore, they were also able to retrieve a secondary signal, corresponding to the plaintext of a *high-grade* encrypted communication, which leaked somehow (e.g. via electromagnetic cross-talk) into the low-grade channel.

While the previous attacks showed that it was possible to use side-channel leakage, such as the signal recovered by the British intelligence, to recover the plaintext message, the publication of side-channel attacks against the cryptosystem itself, e.g. to

recover the secret key, came much later. Probably the first such publication was the paper by Paul Kocher in 1996 [10], describing the use of timing information to determine the private-key used by the RSA cryptosystem. Kocher's *timing attack* exploited the fact that the time needed to perform the modular multiplication and exponentiation operations, used by the RSA cryptosystem, depended on the value of the private key bits.

Two years later, in 1998, Kocher, Jaffe and Jun published another side-channel attack, known as *Differential Power Analysis* (DPA) [9], which exploited the monitored power consumption of a microcontroller executing DES encryptions, to determine the secret key used with DES. This publication marked a very important point in history, since a cryptosystem such as DES, which was considered secure against all known cryptanalytic attacks, and was even designed to resist the *differential cryptanalysis* attacks discovered by Biham and Shamir [2] after its publication, could be easily broken (i.e. we could recover the secret key), when implemented on a physical device accessible to an attacker. This had important consequences for the pay-TV industry, and later for the banking industry as well, who provided their customers with a microcontroller (in the form of a smartcard), in order to authenticate them, by using their smartcard to perform some encryption using a cryptosystem such as DES. After the publication of DPA, this technique has also been used with the electromagnetic emissions of microcontrollers [8], [13], and was also immediately analysed for the case of AES [3].

In 2002, Suresh Chari, Rao Josyula and Pankaj Rohatgi presented a very powerful method, known as the *Template Attack* [4], to infer secret values processed by a microcontroller, by analysing its power-supply current, generally known as its *side-channel leakage*. This attack uses a profiling step to compute the parameters of a multivariate normal distribution from the leakage of a training device, and an attack step in which these parameters are used to infer a secret value (e.g. cryptographic key) from the leakage of a target device. This has important implications for many industries, such as pay-TV or banking, that use a microcontroller executing a cryptographic algorithm to authenticate their customers.

In this presentation I shall provide an introduction in this interesting field of side-channel attacks, including the Differential Power Analysis and Template attacks. Then, I shall briefly discuss some of my research on obtaining efficient implementations of the Template attack that can push its limits further, by using multivariate statistical analysis techniques to: *a*) determine almost perfectly an 8-bit target value, even when this value is manipulated by a single LOAD instruction [6]; *b*) cope with variability caused by the use of either different devices or different acquisition campaigns [7]; *c*) speed-up the profiling phase of template attacks, resulting in the most efficient kind of template attacks [5].

References

1. Bauer, A.O.: Some aspects of military line communications as deployed by the german armed forces prior to 1945. In: The History of Military Communications, Proceedings of 5th Annual Colloquium (1999)
2. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
3. Chari, S., Charanjit, J., Rao, J., Rohatgi, P.: A cautionary note regarding evaluation of AES candidates on smart-cards. In: NIST AES Round 1 (1999)
4. Chari, S., Rao, J., Rohatgi, P.: Template attacks. In: Cryptographic Hardware and Embedded Systems. CHES 2002. LNCS, vol. 2523, pp. 51–62. Springer, Berlin (2003)
5. Choudary, M.O., Kuhn, M.G.: Efficient stochastic methods: profiled attacks beyond 8 bits. In: CARDIS 2014. LNCS, vol. 8968. Springer, Berlin (2014)
6. Choudary, O., Kuhn, M.G.: Efficient template attacks. In: Smart Card Research and Advanced Applications. CARDIS 2013, pp. 253–270. LNCS, vol. 8419. Springer, Berlin (2013). http://eprint.iacr.org/2013/770/
7. Choudary, O., Kuhn, M.G.: Template attacks on different devices. In: Workshop on Constructive Side Channel Analysis and Secure Design. CODADE 2014, pp. 179–198. LNCS, vol. 8622. Springer, Heidelberg (2014). http://eprint.iacr.org/2014/459/
8. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic analysis: concrete results. In: Cryptographic Hardware and Embedded Systems. CHES 2001, pp. 251–261. LNCS, vol. 2162. Springer, Berlin (2001)
9. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Advances in Cryptology. CRYPTO 1999. LNCS, vol. 1666, pp. 789–789. Springer, Berlin (1999). First published in 1998. http://www.cryptography.com/public/pdf/DPA.pdf
10. Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Advances in Cryptology. CRYPTO 1996, pp. 104–113. LNCS, vol. 1109. Springer, Berlin (1996)
11. Kuhn, M.G.: Compromising emanations: eavesdropping risks of computer displays. Technical Report UCAM-CL-TR-577. University of Cambridge, Computer Laboratory, December 2003. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf
12. Markettos, A.T.: Active electromagnetic attacks on secure hardware. Technical Report UCAM-CL-TR-811. University of Cambridge, Computer Laboratory, December 2011. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-811.pdf
13. Quisquater, J.J., Samyde, D.: ElectroMagnetic Analysis (EMA): measures and counter-measures for smart cards. In: Smart Card Programming and Security, pp. 200–210. LNCS, vol. 2140. Springer, Berlin (2001)
14. Wright, P., Greengrass, P.: Spycatcher: The candid autobiography of a senior intelligence officer. Dell (1988)

Secure and Trusted Application Execution on Embedded Devices

Konstantinos Markantonakis, Raja Naeem Akram,
and Mehari G. Msgna

Information Security Group, Smart Card Centre, Royal Holloway,
University of London, UK
{k.markantonakis,r.n.akram,
mehari.msgna.2011}@rhul.ac.uk

Abstract. Embedded devices have permeated into our daily lives and significant day-to-day mundane tasks involve a number of embedded systems. These include smart cards, sensors in vehicles and industrial automation systems. Satisfying the requirements for trusted, reliable and secure embedded devices is more vital than ever before. This urgency is also strengthened further by the potential advent of the Internet of Things and Cyber-Physical Systems. As our reliance on these devices is increasing, the significance of potential threats should not be underestimated, especially as a number of embedded devices are built to operate in malicious environments, where they might be in the possession of an attacker. The challenge to build secure and trusted embedded devices is paramount. In this paper, we examine the security threats to embedded devices along with the associated prevention mechanisms. We also present a holistic approach to the security and trust of embedded devices, from the hardware design, reliability and trust of the runtime environment to the integrity and trustworthiness of the executing applications. The proposed protection mechanisms provide a high degree of security at a minimal computational cost. Such an agnostic view on the security and trust of the embedded devices can be pivotal in their adoption and trust acquisition from the general public and service providers.

A Number-Theoretic Error-Correcting Code

Eric Brier[1], Jean-Sébastien Coron[2], Rémi Géraud[1,3],
Diana Maimuţ[3], and David Naccache[2,3]

[1] Ingenico
28-32 boulevard de Grenelle, 75015, Paris, France
{eric.brier, remi.geraud}@ingenico.com
[2] Université du Luxembourg
6 rue Richard Coudenhove-Kalergi, 1359 Luxembourg, Luxembourg
{jean-sebastien.coron, david.naccache}@uni.lu
[3] École normale supérieure
Département d'Informatique
45 rue d'Ulm, 75230, Paris Cedex 05, France
{remi.geraud, diana.Maimut, david.naccache}@ens.fr

Abstract. In this paper we describe a new error-correcting code (ECC) inspired by the Naccache-Stern cryptosystem. While by far less efficient than Turbo codes, the proposed ECC happens to be more efficient than some established ECCs for certain sets of parameters.

The new ECC adds an appendix to the message. The appendix is the modular product of small primes representing the message bits. The receiver recomputes the product and detects transmission errors using modular division and lattice reduction.

Contents