# The Communication and Computation Cost of Wireless Security – Extended Abstract

Dave Singelée[†], Stefaan Seys[†], Lejla Batina[‡], Ingrid Verbauwhede[†]

[†] ESAT–COSIC
Katholieke Universiteit Leuven – IBBT
3001 Heverlee-Leuven, Belgium
{f rst.last}@esat.kuleuven.be

[‡] CS Department/Digital Security group
Radboud University
Nijmegen, The Netherlands
lejla@cs.ru.nl

## Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*

## General Terms

Algorithms, Security

## Keywords

**Keywords:** Wireless security, RFID, Authentication, Cryptography, Energy Consumption

## 1. INTRODUCTION

Ambient intelligence, the future internet, smart dust, all lead to the immersion of electronics in the human environment. E-health applications are one example: patients will carry intelligent sensors and actuators which are wireless connected to monitoring devices and health professionals. All these applications carry heavy security and privacy risks. Strong authentication is needed such that the correct medical doses can be administered or that brain stimulants cannot be hacked. On top, these devices have typically an extremely limited power, energy and area budget.

Adding security and privacy to these and similar wireless applications has a cost. Security and privacy relies mostly on cryptographic algorithms and associated protocols. To run these protocols on wireless embedded devices requires energy from the battery, which is limited. Therefore it is important to get insight into the global energy cost of secure wireless communications. The two most important factors contributing to the energy cost are the 'computation' cost and the 'communication' cost.

Some protocols rely on light-weight computations on the device of Alice, but require a lot of communication with the device of Bob, which could be another device, a reader, a server or another terminal. Other protocols require maybe heavy public-key operations but only need a small amount of communication.

The goal of this paper is to get some insight into this com-putation-communication trade-off. It will be illustrated with several well-known authentication schemes for RFID and similar small devices.

The rest of this extended abstract is divided into the following sections. Section 2 defines what we mean with cost and with benefits. In section 3 we illustrate the communication cost of different wireless standards. In section 4 we deal with the platforms and costs of different cryptographic algorithms. The next section describes the four protocols we have chosen for our evaluation. These protocols are secret key, public key, hash and stream-cipher based. Finally, we conclude in section 6.

## 2. COSTS AND BENEFITS

Cost as well as benefits are difficult to measure concepts. There are many aspects to cost. One can measure area, e.g. the number of gates or the number of transistors which is typically done for hardware designs. Software designs will measure the memory footprint. Another measure of cost is the execution time needed for calculating cryptographic primitives. Yet another measure is design time and design effort.

In this presentation we will focus on the energy cost. Energy for wireless security has two main components: communication cost and computation cost. The communication cost is associated with the wireless transmission and reception. It includes all the radio parts, the digital and analog circuits to process, transmit and receive the information bits. Computation cost is associated with the execution of the cryptographic algorithms on the embedded platform.

For communication as well as communication we will need energy from the battery. Our unit of measurement is the amount of energy need to transmit and/or receive one bit of information, expressed typically in nJ/bit.

For each of the wireless standards and for each of the cryptographic algorithms there are many implementation options. E.g. the energy difference between a hardware and a software implementation of the same cryptographic


*WiSec'11,* June 14–17, 2011, Hamburg, Germany.
ACM 978-1-4503-0692-8/11/06.

| | Range | Throughput | Freq. | Power | | Energy/bit | |
|---|---|---|---|---|---|---|---|
| | | | | TX | RX | TX | RX |
| | (m) | (kbps) | (GHz) | (mW) | (mW) | (nJ/bit) | (nJ/bit) |
| 802.11G | 30–100 | 54,000 | 2.4 | 2,300 | 1,900 | 42.59 | 35.19 |
| Zigbee | 75 | 250 | 2.4 | 46.44 | 33.30 | 185.76 | 133.20 |
| NFC/RFID | 0.2 | 424 | 13.56E-3 | 60.00 | 60.00 | 141.51 | 141.51 |
| Bluetooth classic | 30 | 2,100 | 2.4 | 99.90 | 67.50 | 47.57 | 32.14 |
| Bluetooth low energy | 5 | 1,000 | 2.4 | 48.00 | 39.20 | 48.00 | 39.20 |
| Nordic RF | 5 | 1,000 | 2.4 | 21.47 | 25.65 | 10.74 | 12.83 |
| BAN | 5 | 1,000 | 2.4 | 2.60 | 0.73 | 2.60 | 0.73 |

**Figure 1: Comparing wireless standards.**

algorithm can vary over a few orders of magnitude. So, the numbers given in this presentation are used to give an indication of the cost and to provide insight into the alternatives.

# 3. COMMUNICATION COST OF DIFFERENT WIRELESS STANDARDS

As a first exercise we have compared different wireless standards. We choose wireless standards which are currently in use and which are aimed mostly at "low power" applications. The different wireless standards are GSM, Wifi, 802.11, Bluetooth, Zigbee, RFID and a state-of-the-art Body Area Network (BAN). Table 1 shows that the numbers vary substantially for different standards. This fact implies that the background of the schemes i.e. various cryptographic primitives have to be carefully scanned in terms of costs.

# 4. COST OF CRYPTOGRAPHY ON EMBEDDED PLATFORMS

As mentioned above obtaining security and privacy for pervasive applications is a challenging problem, mainly due to the low power/energy budgets. A basic security protocol for almost all RFID security protocols is authentication. Although it can be obtained by means of symmetric-key cryptography, using public-key algorithms for this purpose is also possible. In this way, we obtain not just a tag (or a reader) authentication, but we can also meet some privacy requirements. This issue is especially important for RFID applications as a user often does not want to be known or even linked on the basis of several authentications. Hence, we observe that in literature, a wide variety of authentication and security protocols is described using symmetric key and public key primitives.

A typical platform for a wireless node is an embedded microcontroller. Examples include an 8051, an AVR or an ARM platform. Wireless sensor nodes are typically battery operated devices. Hence the total amount of energy taken from the battery is important. On the other hand, a passive RFID tag consists of a small chip that is powered during the communication with a reader. These two cases are intrinsically different in terms of implementation strategies as well as for the cost issues. Namely, the peak power consumed by a tag is the main concern in the RFID scenario, while it influences the total energy only partially in the wireless node case. Hence, a systematic evaluation of computation and communication costs needs to consider examples of both cases and for both platforms, micro-controller and ASIC based. To complete the cost evaluation an example primitive is selected from each group mentioned above. As a block-cipher algorithm we choose AES that is the main standard for encryption and has been already evaluated in several previous studies [6, 11]. As a public-key primitive Elliptic Curve Cryptography (ECC) has proven to be the best choice for constrained environments ever since it invention in the mid 80's. As a consequence, a majority of research on compact low-power public-key hardware architectures for RFID is dedicated to ECC [10, 5]. To complete the study we also choose one hash function and one stream cipher. For the hash function we look at the SHA3 competition and choose one of the finalists [8]. Unfortunately, as a result of the heavey security requirements from NIST, each of these finalists is quite large and power hungry. As stream cipher we select Trivium, a light weight version of the eStream portfolio, [12].

# 5. SELECTION OF PROTOCOLS

We based our selection of the protocols solely on the cryptographic building blocks that are used. The idea is to compare RFID authentication protocols that are exclusively based on a cryptographic hash function, a symmetric block cipher, a symmetric stream cipher, or an asymmetric cryptographic primitive. It is very important to note that each of these protocols have different security and privacy properties. Some are designed to merely offer tag-to-server authentication, while others also offer mutual authentication, or provide various means of privacy protection. The protocols also differ in terms of scalability and key management complexity.

- *Basic zero-knowledge device authentication protocol of Engbert et al.*: Engberg, Harning and Jensen were one of the first to propose an RFID authentication protocol [3]. They present a modular zero-knowledge protocol which relies exclusively on the use of a cryptographic keyed hash function. The authors also discuss how their protocol can be extended to offer advanced security and privacy protection.

- *ISO 9798-2 mutual entity authentication protocol based on AES*: Most RFID authentication protocols are challenge-response protocols which use symmetric and/or asymmetric cryptographic primitives. Protocols for symmetric challenge-response techniques based on encryption are defined in the ISO/IEC 9798-2 standard [7]. Feldhofer et al. [4] proposed to employ these symmetric challenge-response protocols in the context of RFID networks, using the symmetric block cipher AES.

- *PEPS protocol of Billet et al.*: Billet, Etrog and Gilbert recently proposed the PEPS protocol [1]. This privacy-preserving RFID authentication protocol relies exclusively on the use of a stream cipher. Since the protocol makes use of a symmetric primitive, the reader and RFID tag share a secret key $K$.

- *ECC-based Randomized Schnorr protocol*: Recently, various RFID authentication protocols (such as [9]) have been proposed that rely exclusively on the use of Elliptic Curve Cryptography (ECC), since these offer some interesting security and privacy properties. One of these protocols is the Randomized Schnorr protocol [2], proposed by Bringer, Chabanne and Icart.

The communication- computation cost of these selected protocols will be discussed during the presentation. For communication cost, we look at the number of transfers between Alice and Bob, together with the size of the messages. For computation cost, we look at the cryptographic calculations taking place. As can be seen from Table 1, the distance between Alice and Bob plays an important role in the communication cost. Hence, for very short to short distances, it makes sense to move some of the computation burden to the side with a high energy supply.

## 6. CONCLUSIONS

Future internet means that humans find electronics everywhere in their environment. Body Area networks, sensor nets, RFID, NFC and many more wireless applications will offer novel experiences to the human. All of these applications carry security and privacy risks. Many novel protocols with varying security properties have been proposed. In this presentation, we aim at connecting these security properties with the physical constraints, more specifically with the limited power and energy budgets of many applications. By taking both, communication and computation cost into account, we aim at providing a more holistic insight into the actual cost of security protocols. During our presentation, we will illustrate this with specific examples.

## 7. ACKNOWLEDGEMENTS

This work was supported in part by the IAP Programme P6/26 BCRYPT of the Belgian State, by the European Commission under contract number ICT-2007-216676 E-CRYPT NoE phase II, by EU Project UNIQUE (FP7) and by the K.U. Leuven-GOA TENSE (GOA/11/007).

## 8. REFERENCES

[1] O. Billet, J. Etrog and H. Gilbert. Lightweight Privacy Preserving Authentication for RFID Using a Stream Cipher. In *17th International Workshop on Fast Software Encryption (FSE '10), LNCS*, volume 6147, pages 55–74. Springer-Verlag, 2010.

[2] J. Bringer, H. Chabanne, and T. Icart. Cryptanalysis of EC-RAC, a RFID Identification Protocol. In *International Conference on Cryptology and Network Security (CANS'08), LNCS*, volume 5339, pages 149–161. Springer-Verlag, 2008.

[3] S.J. Engberg, M.B. Harning and C.D. Jensen. Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience. In *Second Annual Conference on Privacy, Security and Trust (PST '04)*, pages 89–101. 2004.

[4] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems using the AES Algorithm. In M. Joye and J. J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems (CHES'04), LNCS*, volume 3156, pages 357–370. Springer-Verlag, 2004.

[5] D. Hein, J. Wolkerstorfer, and N. Felber. ECC is Ready for RFID - A Proof in Silicon. In: R. Avanzi, L. Keliher, F. Sica (eds.) *Selected Areas in Cryptography, Lecture Notes in Computer Science*, volume 5381, pages 401–413. Springer-Verlag, 2009.

[6] A. Hodjat, and I. Verbauwhede. The Energy Cost of Embedded Security for Wireless Sensor Networks. In Sensor Network Operations, G. Griffin, T. La Porta, and S. Phoha (eds.), John Wiley & Sons, pp. 510-522, 2006.

[7] ISO/IEC 9798-2. Information Technology – Security Techniques – Entity Authentication – Part 2: Mechanisms Using Symmetric Encipherment Algorithms, 1999.

[8] M. Knezevic, K. Kobayashi, J. Ikegami, S. Matsuo, A. Satoh, U. Kocabas, J. Fan, T. Katashita, T. Sugawara, K. Sakiyama, I. Verbauwhede, K. Ohta, N. Homma, T. Aoki, "Fair and Consistent Hardware Evaluation of Fourteen Round Two SHA-3 Candidates," to appear in IEEE Transactions on VLSI, 13 pages, 2011.

[9] Y. K. Lee, L. Batina, D. Singelée, and I. Verbauwhede. Low-Cost Untraceable Authentication Protocols for RFID (extended version). In S. Wetzel, C. N. Rotaru, and F. Stajano, editors, *Proceedings of the 3rd ACM Conference on Wireless Network Security (WiSec '10)*, pages 55–64. ACM, 2010.

[10] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede. Elliptic Curve Based Security Processor for RFID. *IEEE Transactions on Computer*, volume 57(11), pages 1514–1527, November 2008.

[11] G. de Meulenaer, F. Gosset, F.-X. Standaert, and O. Pereira. On the Energy Cost of Communications and Cryptography in Wireless Sensor Networks, (extended version). *IEEE Int. Workshop on Security and Privacy in Wireless and Mobile Computing, Networking and Communications (SecPriWiMob'2008)*, pages 580 - 585, October 2008.

[12] The eSTREAM project, end of phase 3, http://www.ecrypt.eu.org/stream/endofphase3.html, 2008.