INTEGRACIÓN DE IDEMIX EN ENTORNOS DE IOT

JOSÉ LUIS CÁNOVAS SÁNCHEZ

Tutores
ANTONIO FERNANDO SKARMETA GÓMEZ
JORGE BERNAL BERNABÉ

Facultad de Ingeniería Informática
Universidad de Murcia

José Luis Cánovas Sánchez: *Integración de Idemix en entornos de IoT*

Junio 2017

Ohana means family.
Family means nobody gets left behind, or forgotten.

— Lilo & Stitch

Dedicated to the loving memory of Rudolf Miede.

1939 – 2005

ABSTRACT

Short summary of the contents in English... a great guide by Kent Beck how to write good abstracts can be found here:

https://plg.uwaterloo.ca/~migod/research/beckOOPSLA.html

We have seen that computer programming is an art,
because it applies accumulated knowledge to the world,
because it requires skill and ingenuity, and especially
because it produces objects of beauty.

— Donald E. Knuth [6]

ACKNOWLEDGMENTS

Put your acknowledgments here.

Many thanks to everybody who already sent me a postcard!

Regarding the typography and other help, many thanks go to Marco Kuhlmann, Philipp Lehman, Lothar Schlesier, Jim Young, Lorenzo Pantieri and Enrico Gregorio[1], Jörg Sommer, Joachim Köstler, Daniel Gottschlag, Denis Aydin, Paride Legovini, Steffen Prochnow, Nicolas Repp, Hinrich Harms, Roland Winkler, Jörg Weber, Henri Menke, Claus Lahiri, Clemens Niederberger, Stefano Bragaglia, Jörn Hees, and the whole LaTeX-community for support, ideas and some great software.

Regarding LyX: The LyX port was intially done by *Nicholas Mariette* in March 2009 and continued by *Ivo Pletikosić* in 2011. Thank you very much for your work and for the contributions to the original style.

1 Members of GuIT (Gruppo Italiano Utilizzatori di TeX e LaTeX)

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LISTINGS

ACRONYMS

IoT Internet of Things

ZKP Zero-Knowledge Proof

P2ABCE Privacy-Preserving Attribute-Based Credentials Engine

PoC Proof of Concept

1 INTRODUCTION

In recent years some new concepts have appeared in common people's vocabulary, like *machine learning*, *big data*, *artificial intelligence*, *automation*, etc., but there are two in particular that we are going to focus and try to combine: Internet of Things (IoT) and Internet Security & Privacy.

The IoT is a term with a wide range of interpretations [2], but a breaf definition could be the set of devices, mainly resource constrained, that are interconnected between them in order to achieve a goal. This includes from lampposts with proximity sensors that talk to each other in order to light up part of the street when a passerby walks by, to a sensor on your clothes that tells the washing machine how much detergent to use.

Security & Privacy, thanks to organizations like WikiLeaks, are now taken in consideration by any technology consumer, not only professionals. People are conscious about what their data can be used for, demanding more control over it.

And IoT has proved to not address neither security nor privacy, with recent events like the Mirai botnet DDoS attack on October 2016, considered the biggest DDoS in history [9], or like the multiple vulnerabilities affecting baby monitors [13].

A recent approach to address the problem of privacy is the *strong anonymity*, that conceals our personal details while letting us continue to operate online as a clearly defined individual [4]. One very promising way to achieve this is using Zero-Knowledge Proofs (ZKPs) , cryptographic methods that allows to proof knowledge of data without disclosing it. Furthermore, IBM has been developing a cryptographic protocol suite for privacy-preserving authentication and transfer of certified attributes based on ZKP, called Identity Mixer, Idemix for short [5].

To read more about ZKP aside the introduction done in this thesis, you can read my Mathematics thesis [14].

The goal of this project is to integrate Idemix with the IoT. It will be done using the ABC4Trust's Privacy-Preserving Attribute-Based Credentials Engine (P2ABCE), a framework that defines common architecture, policy language and data artifacts, but based on either IBM's Idemix or Microsoft's U-Prove [12]. This gives us a standardized language to exchange Idemix's messages between IoT devices and usual PCs.

1.1 MOTIVATION

1.2 CHALLENGES

1.3 GOALS

1.4 OUTLINE OF THIS THESIS

2 STATE OF THE ART

In this chapter we present the two dimensions of this project: the IoT development state and an introduction to IBM's privacy-preserving solution, Idemix.

2.1 INTERNET OF THINGS

The development for Internet of Things depends heavily on each target device. We can differentiate two big groups: those with enough processing power to act like an usual computer, and those constrained devices that can't perform arbitrary tasks, sometimes called *embedded*.

We can consider in the first category powerful ARM devices like Raspberry Pi 3, with a 64-bit architecture, 4 CPU cores, 1GB of RAM, which can even compile its own binaries, run the *Java Virtual Machine*, etc., working in practice like any other computer. These kind of devices do not present any major difficulty in terms of research.

What we will consider to be a more *pure* IoT device will be the constrained ones, where it's not trivial to develop any algorithm and run it successfully.

Very known devices fall into this category, like Arduino, powered by Atmel's AVR ATmega328 8-bit microprocessors, with 32KB of program flash memory, 2KB of SRAM, 16MHz of CPU [1]. It seems clear that memory and computation power are a very big issue to deal with when developing to this devices.

A step above in power we can find ESP8266, the most famous Espressif's microcontroller, with built-in WiFi antenna, a Tensilica 16bit RISC microcontroller at 80MHz, 50Kb of RAM, and 1MB flash memory [3]. The possibility of direct WiFi connectivity is its best selling point, putting the *Internet* in Internet of Things.

In another level of power we have microcontrollers usually found in routers, but used in many other applications, like the On-Board Units (OBU) used in Vehicular ad hoc networks (VANET). Characteristics in this range vary around a single core 32-bit CPU, at some hundreds MHz, with tens or hundreds MB of RAM and flash memory, which places them near the first IoT mentioned category.

Although one can code in assembly language for these microcontrollers, there exist C compilers, and many frameworks to build firmware binaries: Arduino Core, Contiki, propietary SDKs, Mongoose OS, ThreadX OS (Real-Time OS), OpenWrt, LEDE, etc. Each firmware targets specific ranges of devices, depending on processing power and memory limitations. For example, Arduino and Contiki aim for microcontrollers like Atmel's ATmega and TI's MSP430, but can also be used in ESP8266, a more powerful microcontroller.

In particular OpenWrt and LEDE (a fork of OpenWrt) are based on Linux, with optimized library binaries, providing many packages through *opkg* [10]. To compile C/C++ code, build the firmware or packages, a complete build system and cross-compiler toolchain can be installed in a x86 host, and using Makefiles select the target hardware [11].

Devices running OpenWRT and other Linux distros are in the limit between IoT categories, but the need of a cross-compiler marks that they belong to the second category.

Starting a big project development for IoT aiming the most constrained devices may not be a good idea. The lack of usual operative system tools (like POSIX), I/O, or even threads can make debugging a tedious task. With good programming practices one can start from the top and slowly end at the bottom with reliable code.

For this reason the current Proof of Concept (PoC) is developed on LEDE, Linux Embedded Development Environment [7], using the Onion Omega2 development board, a Mediatek MT688 microcontroller [8] with a 32-bit MIPS 24KEc CPU at 580MHz, 64MB of RAM and 16MB of flash and built-in WiFi. This development board uses LEDE as its firmware, but its CPU is also listed as compatible with ThreadX OS [15], a Real-Time Operative System for embedded devices.

The PoC will take advantage of the Linux system using files and sockets like in any other Linux desktop distribution, so we can focus on the project itself rather than the specific platform APIs for storage and connectivity.

2.2 IDEMIX

3 MATH TEST CHAPTER

Ei choro aeterno antiopam mea, labitur bonorum pri no. His no decore nemore graecis. In eos meis nominavi, liber soluta vim cu. Sea commune suavitate interpretaris eu, vix eu libris efficiantur.

3.1 SOME FORMULAS

Due to the statistical nature of ionisation energy loss, large fluctuations can occur in the amount of energy deposited by a particle traversing an absorber element[1]. Continuous processes such as multiple scattering and energy loss play a relevant role in the longitudinal and lateral development of electromagnetic and hadronic showers, and in the case of sampling calorimeters the measured resolution can be significantly affected by such fluctuations in their active layers. The description of ionisation fluctuations is characterised by the significance parameter κ, which is proportional to the ratio of mean energy loss to the maximum allowed energy transfer in a single collision with an atomic electron:

You might get unexpected results using math in chapter or section heads. Consider the `pdfspacing` option.

$$\kappa = \frac{\xi}{E_{max}} \tag{1}$$

E_{max} is the maximum transferable energy in a single collision with an atomic electron.

$$E_{max} = \frac{2m_e\beta^2\gamma^2}{1 + 2\gamma m_e/m_x + (m_e/m_x)^2} \,,$$

where $\gamma = E/m_x$, E is energy and m_x the mass of the incident particle, $\beta^2 = 1 - 1/\gamma^2$ and m_e is the electron mass. ξ comes from the Rutherford scattering cross section and is defined as:

$$\xi = \frac{2\pi z^2 e^4 N_{Av} Z\rho\delta x}{m_e\beta^2 c^2 A} = 153.4\frac{z^2}{\beta^2}\frac{Z}{A}\rho\delta x \quad \text{keV},$$

where

z	charge of the incident particle
N_{Av}	Avogadro's number
Z	atomic number of the material
A	atomic weight of the material
ρ	density
δx	thickness of the material

1 Examples taken from Walter Schmidt's great gallery:
http://home.vrweb.de/~was/mathfonts.html

κ measures the contribution of the collisions with energy transfer close to E_{max}. For a given absorber, κ tends towards large values if δx is large and/or if β is small. Likewise, κ tends towards zero if δx is small and/or if β approaches 1.

The value of κ distinguishes two regimes which occur in the description of ionisation fluctuations:

1. A large number of collisions involving the loss of all or most of the incident particle energy during the traversal of an absorber.

   As the total energy transfer is composed of a multitude of small energy losses, we can apply the central limit theorem and describe the fluctuations by a Gaussian distribution. This case is applicable to non-relativistic particles and is described by the inequality $\kappa > 10$ (i. e., when the mean energy loss in the absorber is greater than the maximum energy transfer in a single collision).

2. Particles traversing thin counters and incident electrons under any conditions.

   The relevant inequalities and distributions are $0.01 < \kappa < 10$, Vavilov distribution, and $\kappa < 0.01$, Landau distribution.

3.2 VARIOUS MATHEMATICAL EXAMPLES

If $n > 2$, the identity

$$t[u_1, \dots, u_n] = t\big[t[u_1, \dots, u_{n_1}], t[u_2, \dots, u_n]\big]$$

defines $t[u_1, \dots, u_n]$ recursively, and it can be shown that the alternative definition

$$t[u_1, \dots, u_n] = t\big[t[u_1, u_2], \dots, t[u_{n-1}, u_n]\big]$$

gives the same result.

APPENDIX

A

APPENDIX TEST

Lorem ipsum at nusquam appellantur his, ut eos erant homero concludaturque. Albucius appellantur deterruisset id eam, vivendum partiendo dissentiet ei ius. Vis melius facilisis ea, sea id convenire referrentur, takimata adolescens ex duo. Ei harum argumentum per. Eam vidit exerci appetere ad, ut vel zzril intellegam interpretaris.

More dummy text.

A.1 APPENDIX SECTION TEST

Test: Table 1 (This reference should have a lowercase, small caps A if the option `floatperchapter` is activated, just as in the table itself → however, this does not work at the moment.)

LABITUR BONORUM PRI NO	QUE VISTA	HUMAN
fastidii ea ius	germano	demonstratea
suscipit instructior	titulo	personas
quaestio philosophia	facto	demonstrated

Table 1: Autem usu id.

A.2 ANOTHER APPENDIX SECTION TEST

Equidem detraxit cu nam, vix eu delenit periculis. Eos ut vero constituto, no vidit propriae complectitur sea. Diceret nonummy in has, no qui eligendi recteque consetetur. Mel eu dictas suscipiantur, et sed placerat oporteat. At ipsum electram mei, ad aeque atomorum mea. There is also a useless Pascal listing below: Listing 1.

Listing 1: A floating example (`listings` manual)

```
for i:=maxint downto 0 do
begin
{ do nothing }
end;
```

BIBLIOGRAPHY

[1] *ATmega328 Datasheet*. http://www.atmel.com/Images/Atmel-42735-8-bit-AVR-Microcontroller-ATmega328-328P_Datasheet.pdf.

[2] Luigi Atzori, Antonio Iera, and Giacomo Morabito. "The Internet of Things: A survey." In: *Computer Networks* 54.15 (2010), pp. 2787 –2805. ISSN: 1389-1286. DOI: http://dx.doi.org/10.1016/j.comnet.2010.05.010. URL: http://www.sciencedirect.com/science/article/pii/S1389128610001568.

[3] *Espressif ESP8266 Datasheet*. https://espressif.com/en/products/hardware/esp8266ex/resources.

[4] Tom Henriksson. "How 'strong anonymity' will finally fix the privacy problem." In: *VentureBeat* (2016). https://venturebeat.com/2016/10/08/how-strong-anonymity-will-finally-fix-the-privacy-problem/.

[5] *Identity Mixer*. https://www.research.ibm.com/labs/zurich/idemix/.

[6] Donald E. Knuth. "Computer Programming as an Art." In: *Communications of the ACM* 17.12 (1974), pp. 667–673.

[7] *Linux Embedded Development Environment*.

[8] *MediaTek MT7688 Datasheet*. https://goo.gl/kqD2gF.

[9] R. Thandeeswaran N. Jeyanthi. *Security Breaches and Threat Prevention in the Internet of Things*. IGI Global, 2017.

[10] *OPKG Package Manager*. https://wiki.openwrt.org/doc/techref/opkg.

[11] *OpenWrt's build system*. https://wiki.openwrt.org/about/toolchain.

[12] *P2ABCEngine*. https://github.com/p2abcengine/p2abcengine.

[13] Mark Stanislav and Tod Beardsley. *HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities*. Tech. rep. Rapid7, 2015.

[14] José Luis Cánovas Sánchez. "Pruebas de Conocimiento Cero y sus Aplicaciones."

[15] *THREADX OS Real-Time OS*.

DECLARATION

Put your declaration here.

, Junio 2017

José Luis Cánovas Sánchez

COLOPHON

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede. The style was inspired by Robert Bringhurst's seminal book on typography "*The Elements of Typographic Style*". `classicthesis` is available for both LaTeX and LyX:

https://bitbucket.org/amiede/classicthesis/

Happy users of `classicthesis` usually send a real postcard to the author, a collection of postcards received so far is featured here:

http://postcards.miede.de/

Final Version as of April 5, 2017 (`classicthesis`).