European Cooperation in the field of Scientific and Technical Research
- COST -

Brussels, 15 May 2014

COST 043/14

MEMORANDUM OF UNDERSTANDING

Subject :	Memorandum of Understanding for the implementation of a European Concerted Research Action designated as COST Action IC1403: Cryptanalysis of ubiquitous computing systems (CRYPTACUS)

Delegations will find attached the Memorandum of Understanding for COST Action IC1403 as approved by the COST Committee of Senior Officials (CSO) at its 190th meeting on 14 May 2014.

MEMORANDUM OF UNDERSTANDING
For the implementation of a European Concerted Research Action designated as

COST Action IC1403
CRYPTANALYSIS OF UBIQUITOUS COMPUTING SYSTEMS (CRYPTACUS)

The Parties to this Memorandum of Understanding, declaring their common intention to participate in the concerted Action referred to above and described in the technical Annex to the Memorandum, have reached the following understanding:

1. The Action will be carried out in accordance with the provisions of document COST 4114/13 "COST Action Management" and document COST 4112/13 "Rules for Participation in and Implementation of COST Activities" , or in any new document amending or replacing them, the contents of which the Parties are fully aware of.

2. The main objective of the Action is to improve and adapt the existent cryptanalysis methodologies and tools to the ubiquitous computing framework. Cryptanalysis, which is the assessment of theoretical and practical cryptographic mechanisms designed to ensure security and privacy, will be implemented along four axes: cryptographic models, cryptanalysis of building blocks, hardware and software security engineering, and security assessment of real-world systems.

3. The economic dimension of the activities carried out under the Action has been estimated, on the basis of information available during the planning of the Action, at EUR 48 million in 2014 prices.

4. The Memorandum of Understanding will take effect on being accepted by at least five Parties.

5. The Memorandum of Understanding will remain in force for a period of 4 years, calculated from the date of the first meeting of the Management Committee, unless the duration of the Action is modified according to the provisions of section *2. Changes to a COST Action* in the document COST 4114/13.

A. ABSTRACT AND KEYWORDS

Recent technological advances in hardware and software have irrevocably affected the classical picture of computing systems. Today, these no longer consist only of connected servers, but involve a wide range of pervasive and embedded devices, leading to the concept of "ubiquitous computing systems".
The objective of the Action is to improve and adapt the existent cryptanalysis methodologies and tools to the ubiquitous computing framework. Cryptanalysis, which is the assessment of theoretical and practical cryptographic mechanisms designed to ensure security and privacy, will be implemented along four axes: cryptographic models, cryptanalysis of building blocks, hardware and software security engineering, and security assessment of real-world systems.
Researchers have only recently started to focus on the security of ubiquitous computing systems. Despite the critical flaws found, the required highly-specialized skills and the isolation of the involved disciplines are a true barrier for identifying additional issues. The Action will establish a network of complementary skills, so that expertise in cryptography, information security, privacy, and embedded systems can be put to work together.
The outcome will directly help industry stakeholders and regulatory bodies to increase security and privacy in ubiquitous computing systems, in order to eventually make citizens better protected in their everyday life.
Keywords: Cryptography, Security Assessment, Privacy, Ubiquitous Computing, Embedded Devices

B. BACKGROUND

B.1 General background

Recent technological advances in hardware and software have irrevocably affected the classical picture of computing systems. Today, these systems no longer consist only of connected servers, but involve a wide range of pervasive devices. This new paradigm, where information processing is embedded into everyday objects, has brought the concept of "ubiquitous computing systems". Such pervasive devices perform actions on behalf of their users for access control in mass transportation, payment, building access control, vehicle ignition systems, biometric passports, smart meters, and many others.
Three distinctive characteristics of pervasive devices have a strong impact on their security: (1) they

suffer from low memory and processing capabilities, which make the use of highly secure building blocks difficult, (2) they mostly rely on hardware and embedded software, which causes longer life-cycles and make much harder to integrate up-to-date components, (3) they frequently contain collected personal data, which raises the problem of privacy. As a consequence, security through obscurity is a common malpractice in ubiquitous computing.

Only recently researchers started to focus on the cryptanalysis of ubiquitous computing devices, that is on the security and privacy assessment of the cryptographic mechanisms used to protect the devices and the data. Despite this, they already managed to find critical flaws in several widely deployed devices. For example, Texas Instruments' Digital Signature Transponder was successfully attacked in 2005 (Bono et al., 2005); Mifare Classic was completely "dismantled" by several research teams (Garcia et al., 2008); critical flaws in the KeeLoq ignition car system were revealed (Bogdanov et al., 2006) and later improved between 2006 and 2008; serious weaknesses were found in iClass (Garcia et al., 2012) and Hitag2 (Verdult et al., 2012); DESFire MF3ICD40 suffers from side-channel attacks (Oswald et al., 2011); etc. This enumeration is long and quite worrying. Even applications from which we expect high security are not immune to security problems. For example, a "fatal" flaw in the random number generator of Taiwan's ID cards has very recently been discovered (Bernstein et al., 2013). These ubiquitous devices are not the only source of trouble: the back-end system that collects and stores data may be the target of security and privacy attacks, for example de-anonymisation attacks on geolocated data (Gambs et al., 2013).

The lengthy enumeration provided above hides the fact that most of the attacks have been carried out by small disconnected groups, and required different knowledge and skills to be fully completed. For example, both Mifare Classic and KeeLoq have been attacked by four different academic teams with very different approaches before being completely broken. This demonstrates that knowledge in the field of secure ubiquitous computing systems is highly fragmented.

The Action will directly benefit stakeholders involved in ubiquitous computing systems, in particular manufacturers, integrators, and operators of such systems. They will be able to use the results of this Action to improve their analysis methodologies and consequently the security of their products and services. The European companies leading the market that are Action Participants will obtain an edge over their competitors. Finally, and above all, the citizens will benefit from increased security and privacy in everyday applications and scenarios, especially when personal data is processed.

B.2 Current state of knowledge

In spite of well-known best practices in the field of security engineering, many real-world systems suffer from critical weaknesses. Consider for example the infamous case of the Mifare Classic used in London's Oyster card (Nohl et al., 2008; Garcia et al., 2008, Garcia et al., 2009), DVD copyright protection (Bloom et al., 1999), mobile (Barkan et al., 2008) and satellite (Driessen et al., 2012) phone communications, the security protocols at the basis of our WiFi communications (Tews et al., 2009; Sepehrdad et al., 2013), the EMV protocol (Murdoch et al., 2010) used in bank cards, the NFC (Near Field Communication) (Francis et al., 2010) which is now the basis for contactless payments, or the Medtronic pacemakers and cardiac defibrillators (Halperin et al., 2008) implanted in thousands of patients.

Even though the quoted research seems destructive at first glance, the approach of finding vulnerabilities in real-world systems has given extremely valuable feedback to the security community. In fact, many of the successful attacks have led to much better security designs coming from industry and academia.

A novelty of the Action is to address the security and privacy problems in ubiquitous computing with a cross-layer approach from theory to practice. As detailed in Section D, the Action will indeed consider four layers, so far addressed separately:

- Security and Privacy Models
- Cryptanalysis of Protocols and Primitives
- Hardware and Software Security Engineering
- Security and Privacy Analysis of Real-world Systems

The security and privacy models layer will involve both scientist from the field of cryptography and researchers more focused on privacy. Indeed these two research communities target security and privacy models using different approaches, e.g., (Vaudenay, 2007) and (Domingo, 2007), and the Action will enable them to collaborate to reach more advanced and practical models.

Many lightweight or ultralightweight building blocks have been designed to fit the constrained environments of ubiquitous computing systems. However, the main concerns are the real security and privacy of these primitives, which are often supported only by apparently reasonable and intuitive arguments. Most of these proposals have been broken well before being deployed. The Action will improve the cryptanalysis and design methods by gathering knowledge and skills from different communities. In particular, many lightweight or ultralightweight protocols are developed in the cryptographic community and in the RFID security community without any coordination. The Action Participants will fill the gap between the research communities concerned.

Current applications of side-channel attacks to real-world devices are usually based on standard techniques (DPA, CPA, ...), which already demonstrated their efficacy on practical systems (Eisenbarth et al., 2008; Oswald and Paar, 2011; Moradi et al., 2011; Balasch et al., 2012; Zhou et al., 2013). It raises questions whether advanced attacks (e.g., trading off data complexity for time complexity) or attacks targeting less usual parts of the implementations (e.g., the random number generation), are relevant to practice. The interaction between hardware security issues and software security issues is also a promising and appealing track for investigations, which justifies that they are presented in the same research layer in the Action.

B.3 Reasons for the Action

There is a clear need for a network of experts in the area of cryptanalysis of ubiquitous computing systems. The task of finding and repairing the security weaknesses of ubiquitous real-world complex systems requires a multi-disciplinary approach, which combines expertise in fields as diverse as constrained hardware, secure software development, wireless security, privacy protection, side-channel analysis and lightweight authentication protocols, to name a few. Strong interaction between these different disciplines is not only beneficial but essential. The Mifare Classic case already cited in Section B.1 illustrates the problem, given that four independent academic teams with very different skills were needed to completely break the device.

All Action participants are experts in security of ubiquitous computing systems, but they come from various poorly interconnected fields. Although some of them have already collaborated, many others did not because no opportunity like this one, to work with people from closely-related but different fields, ever arose. This Action is clearly an appropriate way to foster this highly beneficial collaboration. The aforementioned multiple, interrelated yet disconnected, research fields that the Action will bring together for the first time will also greatly benefit from the added value of the networking opportunities offered by the Action. One particular aim of the Action is to put in close contact research groups ascribed to quite different approaches and working methodologies, particularly those dealing with theoretical models and abstractions and those that have a much more practical, hands-on, physical, lab-based expertise.

The focus on cryptanalysis is an original attribute of the Action. Usually, cryptanalysis is a background task of researchers in cryptography and security, and they never stop their design-oriented research to fully devote their time and efforts to cryptanalysis tasks for long periods. As a consequence, cryptanalysis can hardly be funded by conventional national or international funding programmes, and experts in this field do not have opportunities to join their efforts. This clearly

results in suboptimal contributions.
Additionally, mass market applications often suffer from a significant lack of security because it is a hard and very time consuming issue. On the contrary, device manufacturers have incentives to develop new features, to reduce production costs and to gain market shares by shipping products early. There is, therefore, a lack of incentives to improve devices' security. However, in the long term, this lack of security will strongly damage businesses as well as the society as a whole.
It could be said that secure devices (e.g., smart-cards) follow a certification process that requires strict evaluations. However, most devices of the Internet of Things (IoT) are not "secure devices" but we nevertheless rely on them for our daily security and privacy protection. Therefore, this Action will also serve the purpose of developing a framework process for security evaluations for such devices.
Based on these observations, namely (a) experts in cryptanalysis are mostly isolated, (b) cryptanalyzing a system requires many complementary skills, (c) research activities related to cryptanalysis cannot benefit from conventional funding for networking and, (d) manufacturers have no incentive to perform security assessments on most ubiquitous devices, the Proposer strongly believes that COST is the most appropriate funding programme to conduct research in the field of ubiquitous computing systems.
The Action is aimed at European economic and societal needs, for example by working on improved privacy solutions for a better privacy protection of European citizens, but also by speeding up the scientific and technological advances that contribute to the creation of more competitive technology, which is highly beneficial in terms of intellectual property and exportation. Although Europe is still among the world leaders in the design, manufacturing and distribution of ubiquitous systems, it has to face strong competition from both the US and Asia. Thus, this is a critical time for the expertise convened from this Action to play a key role in keeping, or even improving, our international position and the huge benefits that derive from it.
The overall outcome of the Action will be the identification, creation and exploitation of new expertise in the field at an European level, for helping to design new, more secure and privacy-aware ubiquitous systems that will contribute to an international competitive advantage in the medium and long term. Finally, and above all, the citizens will benefit from increased security and privacy in everyday applications and scenarios, especially when personal data is processed.

B.4 Complementarity with other research programmes

There are several initiatives and projects related to security and privacy that have contact points

with this Action.
The Data without Boundaries - DwB - project [DWB] exists to support equal and easy access to official microdata for the European Research Area, within a structured framework where responsibilities and liability are equally shared. The DwB project concentrates on micro data which is a very specific kind of data structure that could be adapted so as to be used in the context of this Action. Other projects share common points with this Action, in particular the INTER-TRUST project [INTERTRUST] whose objective is to develop a dynamic and scalable framework to support trustworthy services and applications in heterogeneous networks and devices. Clearly, trust is related to privacy and interoperability and, in this sense, this project is also related to the uTrustIt project [UTRUSTIT] for internet of things, the Deserec Project "DEpendability and Security by Enhanced REConfigurability" [DESEREC] for critical infrastructures, and FP7 Demons Project - DEcentralized, cooperative and privacy-preserving MONitoring for trustworthinesS [DEMONS]. All those projects address relevant issues related to privacy and security, but they differ significantly from this Action in terms of methodology and context. Indeed, none of them consider a cryptanalytic approach to assess the security and privacy of embedded devices.
FP7 PRESERVE is more cryptography-oriented and addresses Hardware Security Module (HSM) ASIC for Vehicle-2-X communications, with the aim to develop and prototype sufficiently fast HSM for secure key-storage and acceleration of ECC crypto operations. FET UNIQUE addresses the foundations for forgery-resistant security hardware. The project focuses on methods to prevent counterfeiting of hardware blocks, including Physically Unclonable Functions (PUF). CATRENE eGo [EGO] proposes a new way to establish wireless channels between objects or subjects in the future internet of things. The possibility of security attacks is taken into account, but no active investigations are performed in eGo. Although there is no overlap between this Action and PRESERVE, UNIQUE, and EGO, some aspects of these projects are relevant for this Action, and they will highly likely benefit from the network of expertise available through this Action.
Two ongoing COST Actions have also links with this Action: IC1306 and IC1204.
However this Action significantly differs from the goals of COST Action IC1306, where "side-channel attacks" also appear in the scope. While this Action focuses on concrete attacks to identify new threats (and motivate further research in order to better fix them in the future), the Action IC1306 about "secure digital interaction project" focuses on models to capture leakages in general, and add them in the abstract cryptographic models used to prove security. Note also that this Action does not overlap with the activities of Action IC1204, which addresses the manufacturing flows of secure hardware, as well as fault attacks and active disturbances on actual hardware, i.e. ASICs and FPGAs.

C. OBJECTIVES AND BENEFITS

C.1 Aim

The main objective of the Action is to improve the analysis methodologies and tools for assessing the security and privacy of ubiquitous computing systems, ultimately providing recommendations for secure designs.

C.2 Objectives

To achieve the main objective, Action Participants will directly contribute with knowledge and skills to secondary objectives identified below:

- Introduce security and privacy models in ubiquitous computing systems in order to provide a rigorous framework for the cryptanalysis and design contributions.
- Improve the cryptanalysis methods, focusing on primitives and protocols designed for ubiquitous computing systems.
- Develop side-channel attacks methodologies and tools and reverse-engineering techniques suitable to ubiquitous computing systems.
- Analyze the security of real-world systems including privacy issues related to the data collected by these systems.

C.3 How networking within the Action will yield the objectives?

The strength of the Action consists in creating a strong network between researchers with complementary research skills at the forefront of their respective research areas. The Action integrates skills from the fields of cryptography, information security, privacy, reverse-engineering, radio-frequency identification, Internet of things, and physical attacks on microcircuits. To enforce the relationships between the Action Participants, several activities will be organized, as follows:

- Action Participants will collaborate in order to launch national and international research projects within the Action scope.

- Action Participants will jointly organize Training Schools for both young researchers and non-academic stakeholders, as well as research workshops.
- Action Participants will collaborate by producing joint publications (including a book) and open-source software, requiring them to regularly discuss and meet together.
- Mobility of Action Participants will be strongly supported by the Action. Mobility improves skills of young researchers, facilitates the development of Early-Stage Researchers, and disseminates the knowledge and experience of senior researchers. The Action will fund Short Term Scientific Missions (STSMs) and encourage Action Participants to attend conferences and make other international visits, supported where possible by travel grants.
- The Action will also support activities that aim to facilitate long-term mobility of European researchers.

C.4 Potential impact of the Action

Pervasive devices perform actions on behalf of their users for access control in mass transportation, payment, building access control, vehicle ignition systems, biometric passports, smart meters, and many others. Communicating objects no longer belong to science fiction, they are already here and will become the future computing paradigm. Only recently researchers started to focus on the practical security analysis of such devices. Despite this, they already managed to find critical flaws in several widely deployed devices.

The Action will develop new methodologies and tools to perform security analysis of ubiquitous computing systems as well as performing practical attacks. The Action will also allow the scientific community to better understand the limits of the attacks an adversary can perform, and provide recommendations for better implementations, primitives, and protocol designs. Indeed, designing secure building blocks cannot be done without perfectly mastering the attack methodologies.

The Action will consequently benefit the European stakeholders involved in the development of ubiquitous computing systems, including researchers, manufacturers, integrators and operators, helping them to increase their visibility and lead the market. However, and even more importantly, the Action will contribute to make citizens safer while using everyday computing devices that ensure both security and privacy.

C.5 Target groups/end users

The target groups and end-users consist of public and private organizations that have an interest in ubiquitous computing systems:

- International research community in the fields of cryptography, security, privacy, embedded systems, and ubiquitous computing, who will be able to build on the results of the Action.
- International, national and regional industry in the above fields, including (but not limited to) semiconductor companies, systems integrators, banking and telecommunications industry. They will be able to address the weaknesses identified in the Action, and take into account the methodologies and advice provided by the Action in order to improve their ICT solutions. Additionally, the European industry will have the opportunity to hire well trained young scientists, who will promote best practices in the design of real-world ubiquitous computing systems.
- EU Agencies in the related fields, e.g. ENISA, who will be able to benefit from the knowledge and tools developed by the Action.
- National bodies, in particular in the field of security and privacy (e.g. privacy commissioners), and governmental institutions (e.g. ANSSI, BSI, CESG,...). The Action will provide them with the know-how needed to define policies, regulations, and certifications.
- Security evaluation labs, such as CEA-LETI, Riscure, and Brightsight.

The Action Participants are strongly connected with the above-mentioned target groups. Several of them are experts for international and national bodies, e.g., the ENISA, which will make the dissemination of the results of the Action easier and faster.

D. SCIENTIFIC PROGRAMME

D.1 Scientific focus

Security is clearly one of the biggest concerns of today's digital world, with its outsourced and distributed nature, with its plethora of inter-connected devices, all in an ubiquitous computing tandem (Takabi et al, 2010). Three distinctive characteristics of ubiquitous computing systems have

a strong impact on their security: (1) pervasive devices suffer from low memory and processing capabilities, which make the use of highly secure building blocks difficult, (2) they mostly rely on hardware and embedded software, which causes longer life-cycles and make much harder to integrate up-to-date components, (3) they frequently contain collected personal data, which raises the problem of privacy. Privacy is one issue of great social interest, with a multi-lateral dimension, from data privacy to location privacy.
The objective of the Action is to improve the existent cryptanalysis methodologies along with developing new tools for assessing the security of ubiquitous computing systems. Focusing on cryptanalysis is an original attribute of the Action. Cryptanalysis is addressed within the Action across the layers from theory (security and privacy models) to practice (attacks of real-world systems).

D.2 Scientific work plan methods and means

The work plan of the Action is divided into fully complementary layers, organized in four Working Groups (WG) as follows:

- WG1: Security and Privacy Models
- WG2: Cryptanalysis of Protocols and Primitives
- WG3: Hardware and Software Security Engineering
- WG4: Security and Privacy Analysis of Real-world Systems

During the Kick-Off meeting, each WG will be requested to provide within a 6-month period the expected outcomes, milestones, and risks. This assessment will be presented during the first MC meeting, and revised all along the duration of the Action to take into account the arrival of new Action Participants. At this stage, the expected outcomes are the following ones:

- WG1: A security and privacy model for ubiquitous computing systems that could eventually lead to a security and privacy certification.
- WG2: Recommendations and assessment processes for the design of protocols and primitives for different devices.
- WG3: Methodologies in the field of hardware and software engineering to specifically attack embedded devices. These methodologies will come along 3 software tools for side-channel attacks and reverse-engineering.

- WG4: Attacks on real-world systems.

Working Group 1: Security and Privacy Models

Keywords: Cryptography, Models, Proofs, Privacy, Certification.

One of the major concerns of cryptography and more generally information security is to establish proofs of security. Such proofs only make sense if they are done in a well-established model. The field of cryptography dedicated to ubiquitous computing systems, especially focused on Radio Frequency IDentification (RFID), is not yet mature and many topics are currently intensively addressed by the research community, including the design of privacy-friendly protocols.

Although the concept of privacy by design has been supported by the authorities for years, it is undeniable that no means have been provided to the industry to evaluate or design ICT solutions in the spirit of privacy by design. Most of the initiatives on privacy are strongly guided by laws and regulations but the concept of privacy by design cannot rely only on legal and societal questions; it must also consider the technical view of the problem. As stated by Gurses, Troncoso and Diaz (Gurses et al., 2012): "the absence of references to any technical means or principles simply gives no motivation to explore the potentials of translating privacy into systems design."

In the area of RFID, which is a specific form of ubiquitous computing, the formal definitions of security and privacy notions followed a long evolution. For instance, the basic notion of identification protocol with a tag and a reader can be formalized in a 2-party setting, or in a concurrent environment. Also, once we realize that the protocol output (a.k.a. the return channel) gives side information which could help the adversary to mount attacks, the (threat) model is enriched. Sometimes, we also include cross-authentication with identification. Definitions change if we consider symmetric algorithms or public-key cryptography. Later, the privacy notion in identification followed many different variants. Currently, there are two well established models: the one based on simulation - originated in (Vaudenay, 2007), with its latest version appearing in (Ouafi and Vaudenay, 2012) - and the one based on indistinguishability (Hermans et al., 2011).

In addition to the aforementioned privacy models that refer to RFID protocols, it is important to study the data collected in the back-ends of RFID systems and more generally ubiquitous computing systems, which might endanger the privacy of customers in several ways. There is a need for a holistic privacy model that comprises not only protocols but the whole system in which they are deployed. Privacy preserving techniques (e.g., statistical disclosure control, privacy preserving data mining, location privacy, etc.) might be studied to address the privacy issues derived from the wide adoption of ubiquitous computing able to collect data from people almost everywhere.

When the data is stored in databases, it should be kept private but, at the same time, it needs to be useful to researchers and practitioners. Simply encrypting the data is not a solution since, although it is kept private, it cannot be used. There are several privacy models that consider the protection of data privacy from different perspectives. In (Domingo, 2007) data privacy issues are split in three dimensions depending on the main actors involved, namely respondents, users and owners. In this sense, respondents privacy is mainly related to the field of statistical disclosure control, user privacy relates to private information retrieval and owner privacy is closely related to privacy preserving data mining. In (Perez, 2011), the authors address the privacy problem of data with location information and they distinguish three dimensions, like in (Domingo, 2007), but instead of considering the main actors to define the dimensions, they focus on the nature of the data to be protected. Thus, they identify the dimensions of the "Where", i.e. location information, the dimension of the "What", i.e. query information, and the dimension of the "Who", i.e. identification information. The two aforementioned models have been fused in the context of smart cities (Martinez, 2013), in which data collectors such as sensors, mobile phones and RFIDs, among others, are ubiquitous. The resulting model has five dimensions for privacy, namely identity privacy, query privacy, location privacy, footprint privacy and owner privacy. The study of those models and how they apply to ubiquitous computing is paramount for the proper deployment and general acceptance of ubiquitous systems like the ones studied in this Action.

Outcome: the Action will investigate how existing security and privacy models might be extended to consider distributed settings (e.g., authentication server, database) and real-world conditions (e.g., physical noise in the communication channel). A taxonomy of models will be considered and WG1 will also use insights from attacks studied in other WGs. In particular, the Action Participants involved in this WG will consider the possibility to introduce side-channel attacks in the security and privacy models. The outcome of the WG may lead to a privacy certification scheme suited to ubiquitous computing systems.

Working Group 2: Cryptanalysis of protocols and primitives

Keywords: Cryptography, Cryptanalysis methodologies and tools, Protocols and primitives, Proofs.

Many primitives and protocols have been designed to fit the requirements and constrained environments of ubiquitous computing systems, e.g., authentication protocols, distance bounding protocols, ownership transfer protocols, and path checking protocols. However, the main concerns are the real security and privacy of these protocols, which are often supported only by apparently reasonable and intuitive arguments.

For example, ultralightweight authentication protocols suitable for battery-less devices involve

simple bit-wise operations like "and", "or", "exclusive or", modular additions, and cyclic shift operations. They are efficient and fit the hardware constraints. However, most of these proposals have been broken well before being deployed. WG2 will identify the common weaknesses and define the process that should be followed to assess the security of such protocols. A security and privacy sanity check (possibly automated to some extend) would already disqualify most of the candidates.

WG2 will benefit from the knowledge gathered by the different scientific communities represented in the Action. Many protocols are developed in the RFID security community and in the cryptographic community without any coordination. For example the structure of ultralightweight (synchronized) protocols developed in the RFID security community seems to be very close to the structure of stream ciphers developed in the cryptographic community. The cryptanalysis methodologies for stream ciphers might be used against ultralightweight (synchronized) protocols as well. The Action Participants will fill the gap between the concerned research communities in order to share the methodologies and skills.

WG2 will also be strongly linked with WG1 related to security and privacy models. Indeed, when protocols seem secure, cryptanalysis consists of proving it formally, which requires a well-defined model. WG2 will study security proofs whenever possible, but there are still protocols that remain hard to analyze, for instance path-checker protocols for supply chains (Elkhiyaoui et al, 2012), protocols used in the biometric passports, or identity documents in general (Prabhakar et al., 2003), and distance-bounding protocols (Hancke and Kuhn, 2005; Boureanu et al. 2013; Fischlin and Onete, 2013).

Outcome: WG2 will develop recommendations and assessment processes for the design of protocols and primitives for different devices (e.g., passive, active, semi-active RFID tags, sensors) that are usually employed in ubiquitous computing systems. These guidelines will be helpful for practitioners as well as researchers for the subsequent development of reliable and provably secure communication protocols resilient to attacks that have already been identified.

Working Group 3: Hardware and Software Security Engineering

Keywords: Side-channel attacks, Reverse-engineering, Privacy analysis.

Hardware and software security engineering is the study of security and privacy of practical systems. It basically deals with the design of robust systems and the evaluation of the required security and privacy policies. WG3 focuses on the tools, processes, and methods of security and privacy engineering that enable security assessment of ubiquitous computing systems. This requires expertise in many areas such as cryptography, privacy, embedded devices, hardware designs,

software implementations, testing and evaluation processes, tamper resistance, reverse-engineering, side-channel analysis, and fault attacks.

In ubiquitous computing systems, security through obscurity is a common practice where cryptographic mechanisms are kept secret to make attacks harder to perform and to protect manufacturer's innovation. So recovering the details of implemented mechanisms in an embedded system is usually the first step before being able to assess the security of the system. WG3 will exploit well-known reverse-engineering techniques and tools that exist in the field of software security to analyze ubiquitous computing systems, including side-channel analysis based reverse engineering to gain information of the implemented algorithms.

Side-channel attacks are very powerful attacks with frequently devastating effects. They exploit existing flaws in the implementation of algorithms or can extract secret-key dependent information by measuring physical characteristics such as the power consumption or the electromagnetic emanation. Such attacks are highly promising and not sufficiently known by the community of ubiquitous computing. Even more important is the fact that ubiquitous computing devices are so omnipresent and pervasive that an adversary can easily take them from insecure environments and mount attacks at home or open labs.

Analyzing real-world systems remains, to a large extent, an ad-hoc and target-specific task. Part of the research challenge of WG3 will be to formalize this methodology and generalize it in order to make it applicable to new systems. One approach the Action will take is the development and further improvement of three open-source tools:

- **GIAnT** (Generic Implementation Analysis Toolkit) provides a low-cost platform for side-channel analysis, fault-injection attacks (e.g., based on clock or power supply variations), and enables a combination of side-channel attacks with fault injection.
- **Chameleon** enables the emulation of arbitrary contactless cards and other RFIDs. This cost-efficient tool can be flexibly programmed via a USB port, and serve for the security analysis of RFID-based systems.
- **Avatar** enables the security analysis of embedded devices software.

GIAnt and Chameleon exist already on smaller scale and they will both be dramatically enhanced within the Action. GIAnT currently only supports the measurement of a single side-channel and the injection of a single specific fault. GIAnT will be modularized within the Action, which will allow multiple fault sources in parallel, i.e., voltage, clock and EM glitches, as well as capturing multiple side-channels in parallel. The Chameleon shall be improved to operate purely passively powered from the EM field of an RFID reader and to support further types of contactless devices, including

125 kHz RFIDs. Avatar (Zaddach et al, 2014) is a prototype of an event-based arbitration framework that orchestrates the communication between an emulator and a target physical device. Avatar's goal is to enable complex dynamic analysis of embedded firmware in order to assist in a wide range of security-related activities (such as: reverse engineering, malware analysis and vulnerability discovery) without requiring access to the source code or documentation of the device. In addition to the open-source tools, this Working Group will also interact with the logical side-channel analysis. Logical side-channels are, for instance, a different error message, a parity bit or a small bias in the cipher which reveals some information (e.g., about the internal state of the cipher) which helps an attacker to reduce the search space. Having access to a number of protocol sessions allows an attacker to accumulate knowledge that, when combined, allows him to single out the secret key or at least to get a modest-size set of viable candidates.

Another important aspect of WG3 refers to privacy issues related to the data collected by the ubiquitous computing systems. When those systems collect data from individuals, their privacy could be endangered since personal information like habits, health condition, economic status, and the like could be recovered. There are several techniques that aim at protecting the privacy of individuals whose data are collected, but they are mainly focused on census-like data. WG3 will study how to apply those techniques for the specific case of data collected by ubiquitous systems. WG3 will investigate how to extend existing security protocols in privacy-preserving ones regarding context information such as the location of individuals as well as content such as the data (payload) being transmitted. The goal will be to maintain and enhance the reliability and accuracy of existing schemes while at the same time protecting users and individuals from attacks targeting their privacy, i.e., tracking, profiling, compromise of private information that may subsequently lead to identity theft.

Outcome: WG3 will develop methodologies in the field of hardware and software engineering to specifically attack embedded devices in ubiquitous computing systems. These methodologies will come along 3 software tools for side-channel attacks and reverse-engineering. WG3 will also address the privacy question and provide a process framework to extract and exploit personal data leaking from a ubiquitous computing systems. WG3 will eventually serve as an input for the design of new protected mechanisms.

Working Group 4: Security and privacy analysis of real-world systems

Keywords: Real-world applications, Practical attacks, Holistic approach, Citizens' awareness

In spite of well-known good practices in the field of security engineering, many real-world systems suffer from critical weaknesses. Vulnerabilities in real-world systems arise form implementation

mistakes (Garcia et al., 2012), misconfiguration and poor protocol designs (Verdult et al., 2012), weak ciphers and pseudo-random generators (Indesteege et al., 2008; Garcia et al., 2008; Garcia et al., 2010), errors at the logical level (Murdoch et al., 2010) and often, a combination of the above (Garcia et al., 2009). Even though the quoted research seems destructive at first glance, the approach of finding vulnerabilities in real-world systems has given extremely valuable feedback to the security community. In fact, many of the successful attacks have led to much better security designs coming from industry and academia.

The cryptanalysis of real-world systems, including privacy issues related to the data collected by these systems, require an holistic approach. Indeed, even when all the system components are secure in isolation, this does not provide any warranties over the system as a whole. This is a major advantage of this Action in terms of methodology over other projects that do not consider real-world cases. WG4 is a strength of this Action.

WG4 will strongly interact with the other WGs. WG4 will apply the methodologies and tools developed in WG2 and WG3 to real-world systems. The lessons learned from this exercise will in turn enhance the security engineering techniques of WG3. Furthermore, WG4 will map real-world systems to the models proposed in WG1. WG1 will enhance those models when these are unable to map realistic adversarial capabilities.

Note that the activities of WG4 will be guided by a strict deontological ethics. This means that the activities will be performed under legal agreements when needed. The scientific board of the Action will be consulted if in doubt.

Outcome: WG4 will have a short-term and practical impact. In particular, WG4 will (1) provide companies with helpful recommendations for attack mitigation, (2) challenge WG1, WG2, and WG3 with experimental results, in order to make models, tools, and methods better fitted to the real-world, and (3) raise the awareness of citizens, because users themselves can significantly reduce the risks when they are aware of the security and privacy issues.

E. ORGANISATION

E.1 Coordination and organisation

Management

The Action will be coordinated by a Management Committee (MC) that will meet twice a year. The MC will appoint a chair and a vice-chair during the Kick-Off meeting. The MC will also nominate, during the Kick-Off meeting, committees dedicated to coordinate specific aspects of the Action: a Website Committee, a Parity Committee, and a Scientific Board. Finally, the MC will elect a chair

for each of the four Working Groups (WG). The Kick-Off meeting will also be an opportunity to meet non-academic stakeholders concerned by security and privacy in ubiquitous computing systems, and invite them to join the Action.
Each Working Group (WG) will organize a meeting twice a year. All the WG meetings will be scheduled such that Action Participants can attend several WG meetings. The meetings will be co-located with major conferences in cryptography and security to facilitate interaction between the WGs, and to save on travel and organization costs.
The MC will publish progress reports on a yearly basis, and a final report at the end of the Action. The reports will contain the scientific outcomes of each WG, and the significant data related to the Action (events sponsored, funded Short Term Scientific Missions (STSMs), ...). Additionally, a public conference will be organized once the Action is completed, in order to present all the Action contributions in a single venue.
Action Participants are all experts in security of ubiquitous computing systems, but they come from various poorly interconnected fields. Although some of them have already collaborated in the past, many others did not because no opportunity like this one, to work with people from closely-related but different fields, ever arose. This Action is clearly an appropriate way to do so. Once Action Participants will know better the skills and expertise within the consortium, they will be able to launch nationally or internationally funded collaborative projects, e.g., within the H2020 Framework. The capacity of the Action Participants to raise research funds was taken into account to settle the consortium.

Website Committee

A website will be set up and continuously maintained all along the lifetime of the Action. The website will promote the activities and outcomes of the Action (publications, events, ...), and it will also share internal information among the Action Participants (minutes of the MC meetings, reports, ...). The website will be maintained collaboratively. For that, the website committee will be launched during the Kick-Off meeting, consisting of (at least) one representative from each WG. The content of the Action Website is described in Section H.3 (Dissemination Plan).

Parity Committee

Particular attention will be paid to the assignment of responsibilities. Parity regarding gender balance will be openly promoted. The location of the meetings will also be carefully selected in order to ensure fairness between the COST Member Countries, and maximize local impact. Finally, and for maximizing the Action benefits for Early-Stage Researchers, responsibilities will be well-

balanced between junior and senior Action Participants, as this Action includes Action Participants already quite well-established in the scientific community but also promising Early-Stage Researchers; the above-mentioned guidelines have been already taken into account for the invitation of Action Participants.
The mission of the Parity Committee will be to ensure that the Action reaches its target in terms of parity. The Committee will suggest to the MC the actions to be taken in order to enforce gender balance, ensure fairness between the COST Member Countries, and guarantee an adequate share of the Action's responsibilities between junior and senior researchers.
A description of the activities to ensure gender balance and involvement of Early-Stage Researchers is provided in Section E.4.

Scientific Board

The Action will set up a permanent Scientific Board in charge of guaranteeing the scientific quality of the activities supported by the Action. The missions of the Scientific Board include the evaluation of proposals for Short Term Scientific Missions (STSMs), the monitoring of the achieved objectives, and the organization of scientific events. The dissemination activities will be carried out through several channels:

- Organization of workshops and training schools for young researchers and non-academic stakeholders (see the timetable provided in Section F.1).
- Support of researchers' mobility at all steps of their career to improve the skills of PhD students and post-doctoral fellows, to facilitate the development of Early-Stage Researchers, and to spread the knowledge and experience of senior researchers.

The Scientific Board will be requested by the MC to suggest activities to promote excellence (eg, best paper award, prizes,...). In particular, each of the three Workshops (see Section F.1) might start with a keynote talk by the Action Participant who published the best contribution of the year, according to the Scientific Board. The production of high quality outputs must be an objective of the Scientific Board.

E.2 Working Groups

The Action is balanced between theoretical research and practical research, distributed over four Working Groups (WG) focusing on specific topics (listed below from theory to practice).
All the Working Groups target the same major conferences (e.g., ACM CCS, CRYPTO,

EUROCRYPT, IEEE S&P) and journals (e.g., Journal of Cryptology, Journal of Information Security, IEEE Pervasive Computing, Journal of Cryptographic Engineering, IEEE Transactions on Information Forensics and Security), but each of them is also concerned by more specific workshops (e.g., CHES, CARDIS, ESORICS, RFIDsec).

- WG1: Security and privacy models.
- WG2: Cryptanalysis of primitives and protocols.
- WG3: Hardware and software security engineering.
- WG4: Security and privacy analysis of real-world systems.

This division has the great advantage of addressing security of ubiquitous computing systems from theory to practice, such that each Working Group will provide the other ones with open questions and outcomes.

The Working Groups are not defined according to the researchers' communities, but according to their research objectives, in order to facilitate the interaction between different skills and expertise. For example, WG1 that addresses the security and privacy models will involve researchers from the fields of cryptography, security, privacy, and embedded devices. This way to define the Working Groups complies with the spirit of COST Actions, whose aim is to make researchers from different communities work together. Finally, the structure of the Working Groups was thought in such a way that Action Participants can join the activities of more than one Working Group, and they are flexible enough to permit at the implementation stage the inclusion of research activities not foreseen during the preparation of the Action.

Each Working Group will be led by a Chair elected by the MC during the Kick-Off meeting. Each Working Group will also have a representative in the committees and boards (See Part E1).

E.3 Liaison and interaction with other research programmes

The Action is definitely open to interact with other COST Actions and other European and international research programs whose scientific activities or objectives intersect with the cryptanalysis of ubiquitous computing systems. This includes in particular the research projects related to the fields of cryptography, security, privacy, embedded devices, and ubiquitous computing.

The MC will invite representatives of the relevant research projects to give a short talk and present their projects to the Action Participants. Following this meeting, the MC will be able to decide

which interactions are the most appropriate to set up fruitful collaborations. At this stage, the interactions that are conceivable are sharing training schools for young researchers, in order to provide them with a diversity of complementary skills and knowledge, and co-locating or co-organizing scientific workshops and joint publications. The Action has a positive attitude towards interaction with other initiatives in related areas and disciplines such as hardware security, cryptanalysis, wireless security, and privacy enhancing technologies.

E.4 Gender balance and involvement of early-stage researchers

This COST Action will respect an appropriate gender balance in all its activities and the Management Committee will place this as a standard item on all its MC agendas. The Action will also be committed to considerably involve Early-Stage Researchers. This item will also be placed as a standard item on all MC agendas.

The low ratio of women in computing across Europe is a persistent problem that this Action will tackle by taking concrete steps to encourage female participation at all levels:

- At the highest levels (Chair, Vice-Chair, MC members, WG leaders) the MC will actively seek to get and keep a good gender balance with at least a 40% female representation. Female ratios are poor in areas related to computer science, and even poorer in general in leadership positions, so the MC will aim to implement an even stronger policy at the managerial roles within this Action.
- In training schools, e.g., by reserving a quota of stipends for female participants of at least 33%. Workshop panel members, and speakers invited to any organized events will also be subjected to this quota.
- We plan to continue the organization of workshops that promote female researchers like the CrossFyre initiative: http://www.cosic.esat.kuleuven.be/crossfyre/
- Be actively involved and encourage and support participation of Action members in projects like the European Association for Women in Science, Engineering and Technology (WITEC) http://www.witec-eu.net/ and in Networking Networking Women (N2Women) http://committees.comsoc.org/n2women/

The MC will additionally encourage the formation of a Circle for Women in the area covered by this Action, following the best practice recommended by the Anita Borg Institute, to create a supportive environment to help women's careers grow, build up networks, learn from other women

experiences, etc.

Furthermore, this Action will encourage the participation of Early-Stage Researchers in all managerial positions and meetings, aiming at least at a 20% representation among the managerial roles of the Action. The Action Participants believe that to ensure a sustainable development of the field in Europe, it is vital that Early-Stage Researchers take responsibility and gain important experience not only in the scientific progress of the field, but also in its managerial and networking aspects. The MC will facilitate this experience by enforcing a 20% representation.

F. TIMETABLE

The Action will cover a 4-year period, during which the following events will be organized:

- 2 Management Committee (MC) meeting every year, including the 1st MC meeting where Chair, Vice-Chair, MC members, WG leaders will be elected.
- 6 Working Groups (WG) meetings distributed as follows: 1 WG meeting on Year 1 and Year 4; and 2 WG meetings on Year 2 and Year 3
- 3 Workshops (WS) (Year 2, Year 3, and Year 4)
- 1 final conference (CNF) on Year 4
- 2 Training schools (TS) for young researchers and industry, on Year 2 and Year 3

Note that the meetings will be co-located with major conferences in cryptography and security to facilitate interaction between the WGs, and to save on travel and organization costs. Consequently, the timetable could be slightly modified to suit to the schedule of the target conferences.

Year1				Year2				Year3				Year4			
01-03	04-06	07-09	10-12	13-15	16-18	19-21	22-24	25-27	28-30	31-33	34-36	37-39	40-42	43-45	46-48
					WS	TS			WS	TS			WS		CNF
			WG1		WG1		WG1		WG1		WG1		WG1		
			WG2		WG2		WG2		WG2		WG2		WG2		
			WG3		WG3		WG3		WG3		WG3		WG3		
			WG4		WG4		WG4		WG4		WG4		WG4		
MC			MC		MC		MC		MC		MC		MC		MC

G. ECONOMIC DIMENSION

The following COST countries have actively participated in the preparation of the Action or otherwise indicated their interest: AT, BE, CH, DE, ES, FR, IL, IT, NL, SE, TR, UK. On the basis of national estimates, the economic dimension of the activities to be carried out under the Action has been estimated at 48 Million € for the total duration of the Action. This estimate is valid under the assumption that all the countries mentioned above but no other countries will participate in the Action. Any departure from this will change the total cost accordingly.

H. DISSEMINATION PLAN

H.1 Who?

In order to contribute to the framework for European Action "Horizon 2020", the dissemination plan has as one of its main aims the strengthening of the European research. In this way it is intended to stimulate research and advances in new technologies, strengthen European's industrial leadership, contribute to the social challenges posed by the framework "Horizon 2020" (specifically those related to "Secure societies - Protecting freedom and security of Europe and its Citizens") and boost the cooperation between European research centers. The target audience for the dissemination of the results of the Action will include internal audience and external audience. The internal audiences are members and participants in the COST Action. On the other hand, the external audience is composed of all those who directly or indirectly are benefited by the outcome Action. Including:

- International research community (researchers, PhD students, technical staff) in the fields of cryptography, security, privacy, embedded devices, and ubiquitous computing.
- International, national, and regional industry in the above fields, including (but not limited to) semiconductor companies, systems integrators, banking and telecommunication industry.
- EU Agencies in the related fields, e.g., ENISA, and professional and standardization groups (IEEE, ITU).
- National bodies, in particular in the field of security and privacy (e.g., privacy commissioners), and governmental institutions (e.g., ANSSI, BSI, CESG)
- Mass media, which may be interested in spreading information related to Action outcomes related to real-world applications issued by WG4.

H.2 What?

The Action will disseminate information and knowledge to the audience identified in Section H.1. The content of the dissemination is listed below, while the methods and channels used for the dissemination are described in Section H.3.

- A book (or a special issue in an OpenAccess journal) on the security and privacy in ubiquitous computing systems authored or edited by the Action Participants.
- Non technical articles aimed at large-audience in international and national magazines. Publishing large-audience articles written in national languages is important to reach a broader basis, including younger people who are the next generation of researchers.
- Articles in international conferences and journals. The outcomes of each WG should be at least two joint publications every year. In order to be considered as an Action outcome, the publications will need to contain an acknowledgement to COST.
- Proceedings of the workshops organized by the Action.
- Software (GIAnT, Chameleon, and Avatar) developed/extended in the framework of the Action.
- Reports of the progress of the Action, special and final reports, and minutes of the MC meetings.
- Expertise provided to the community, especially to young researchers and non-academic stakeholders through Training Schools.
- Public and private information through the Action Website.
- Short-Term Scientific Missions (STSMs).

H.3 How?

As already stated in Section H.1, the target audience for the dissemination of the results of the Action is twofold: internal audience and external audience.
The website will be the unique portal of the Action for both internal and external audiences. It will contain a restricted area where Participants will be able to upload works in progress and internal documents, and the website will be associated with several mailing lists. The website will contain

general information about the Action (identity of the participants, committees, boards, chairs and contact), schedule of past and future events organized by the Action, and scientific information. The website will also internally share information about national and international project proposals to allow Action Participants to discuss and find partners, and an open board will allow them to announce open positions at any career level, including Master internships, PhD theses, Postdoc and faculty positions.

The events organized by the Action are listed below:

- MC Meetings: 8 meetings, including Kick-Off Meeting and Final Meeting.
- WG Meetings: there are 6 meetings per WG (see Section F.1).
- Workshops: there are 3 public 2-day workshops organized by a WG, or jointly by a few WGs.
- Training Schools: there are 2 training schools, which are events that target young researchers and non-academic stakeholders.
- Conference: there is a final conference that will publicly present the outcomes of the Action.
- Short-Term Scientific Missions: support of researchers' mobility at all steps of their career to improve the skills of PhD students and post-doctoral fellows, to facilitate the development of Early-Stage Researchers, and to spread the knowledge and experience of senior researchers.