VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kansliets noteringar Kod	Dnr
2014-48128-116647-16	2014-4845

2014
Project Grant Junior Researchers

Area of science
Natural and Engineering Sciences

Announced grants
Research grants NT April 9, 2014

Total amount for which applied (kSEK)

2015	2016	2017	2018	2019
1043	1075	1103	1123	1209

APPLICANT

Name(Last name, First name)
Mitrokotsa, Aikaterini

Date of birth
781008-3662

Gender
Female

Email address
aikmitr@chalmers.se

Academic title
PhD

Position
Assistant Professor

Phone
+46 31 772 10 40

Doctoral degree awarded (yyyy-mm-dd)
2007-11-12

WORKING ADDRESS

University/corresponding, Department, Section/Unit, Address, etc.
Chalmers tekniska högskola
Institutionen för data-och informationsteknik
Nätverk och System
Rännvägen 6B
41296 Göteborg, Sweden

ADMINISTRATING ORGANISATION

Administrating Organisation
Chalmers tekniska högskola

DESCRIPTIVE DATA

Project title, Swedish (max 200 char)
PRECIS: Integritet och säkerhet i bärbara datorprylar

Project title, English (max 200 char)
PRECIS: Privacy and security in wearable computing devices

Abstract (max 1500 char)
Wearable and ubiquitous computing will create a wave of adoption similar to smartphones, enabling new applications in areas such as smart homes and healthcare. They collect unique information about each individual and offer transparent authentication. However they have weak security and scatter our digital fingerprints across different services.

PRECIS has the ambitious goal to address this challenge and to introduce a unifying framework for authentication in wearable computing that provides: i) accurate and transparent authentication, ii) rigorous privacy guarantees, even if multiple wearable devices are involved in the authentication. Existing solutions address information leakage at a local level; although the functionality of a single wearable device can be privacy-preserving, collectively they unwittingly compromise our privacy. Our novel idea is to guarantee privacy collectively, by considering all information leakage if an adversary has access to multiple services related to different wearable devices. This is a significant research challenge that we will address through cross-disciplinary advances in cryptography, decision-making and machine learning. We shall employ multi-factor and cross-layer authentication protocols, secure multi-party computation and differential privacy, fields that have been studied mostly in isolation. PRECIS shall lead to breakthroughs in secure and private wireless communications and will prepare us for the future of wearable computing.

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-48128-116647-16

Name of Applicant
Mitrokotsa, Aikaterini

Date of birth
781008-3662

Abstract language
English

Keywords
privacy, security, authentication, wearable computing, ubiquitous computing

Review panel
NT-2, NT-14

Project also includes other research area

Classification codes (SCB) in order of priority
10201, 20203, 20204

Aspects

Continuation grant
Application concerns: New grant
Registration Number:

Application is also submitted to

similar to: **identical to:**

ANIMAL STUDIES

Animal studies
No animal experiments

ENCLOSED APPENDICES

A, B, C, N, S

APPLIED FUNDING: THIS APPLICATION

Funding period (planned start and end date)
2015-01-01 -- 2019-12-31

Staff/ salaries (kSEK)

Main applicant	% of full time in the project	2015	2016	2017	2018	2019
Aikaterini Mitrokotsa	25	285	295	305	315	326
Other staff						
PhD student	80	616	636	657	680	703
Total, salaries (kSEK):		901	931	962	995	1029

Other project related costs (kSEK)	2015	2016	2017	2018	2019
laptops/PCs	20	20			
travel costs	60	60	60	60	60
lic and disputation costs			15		50
Premesis	49	51	53	54	56
Direct IT costs	13	13	13	14	14
Total, other costs (kSEK):	142	144	141	128	180

Total amount for which applied (kSEK)

2015	2016	2017	2018	2019
1043	1075	1103	1123	1209

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-48128-116647-16

Name of Applicant
Mitrokotsa, Aikaterini

Date of birth
781008-3662

ALL FUNDING

Other VR-projects (granted and applied) by the applicant and co-workers, if applic. (kSEK)

Funds received by the applicant from other funding sources, incl ALF-grant (kSEK)

Funding source	Total	Proj.period	Applied	2015
EU	900	2013-2016		

Project title
BEAT: Biometric Evaluation and Testing

Applicant
Aikaterini Mitrokotsa

Funding source	Total	Proj.period	Applied	2015
STINT	150	2014-2015		

Project title
Cross-layer authentication for wireless networks

Applicant
Aikaterini Mitrokotsa

POPULAR SCIENCE DESCRIPTION

Popularscience heading and description (max 4500 char)

Bärbar och allestädes närvarande datorisering är en kommande teknologi som förväntas ge en våg av förändringar likt den med dagens smartphones. Dessa små bärbara småprylar - "gadgets" - (t.ex. FitBit, GoogleGlass, och SmartWatch) har gått från att vara science fiction till vardagsteknik. De samlar unik information om varje individ och möjliggör även förenklad autentisering. De ger också möjlighet till många nya tillämpningar inom områden såsom smarta hem, distansövervakning, nyckellös öppning av bilar och trådlösa betalningar, samt hemtjänst och sjukvård, som kräver både hög säkerhet och integritet.

Enligt Ciscos Visual Networking Index var det 2013 nästan 22 miljoner gadgets globalt som genererade 1,7 petabytes med datatrafik per månad. ABI research spår att den globala marknaden för gadgets kan nå 170 miljoner enheter år 2017 och i en marknadsundersökning förväntas marknaden för dessa enheter överstiga 8 miljarder US dollar år 2018.

Problemet är att dessa gadgets har svag säkerhet och att våra digitala fotspår sprids i olika tjänster. Flera sentida studier har visat att trådlös autentisering kan knäckas. De senaste avslöjanden om massövervakning av Internet bekräftar också att bärbara gadgets och smarta hem som återrapporterar allt som görs är inte längre en fiction. Google har redan börjat investera i automatiserade hem genom att förvärva företaget NEST, som utvecklar enheter för smarta hem. Även om integriteten i varje enskild tjänst är tillräcklig, kan en angripare med tillgång till många system fortfarande knäcka integritetsskyddet.

PRECIS har som mål att anta dessa nya utmaningar och introducera ett enhetligt ramverk för autentisering i samband med bärbar databehandling som erbjuder: i) korrekt och transparent autentisering, ii) stark integritet även om flera enheter används vid autentisering.

PRECIS skall skapa korrekta, tillförlitliga och integritetsskyddande autentiseringsmekanismer som förbereder oss för användandet av nästa generations gadgets. Detta är ett lämpligt tillfälle att studera lämplig metodik för att lösa dessa problem och därmed förbereda oss för en framtid med än mer bärbar databehandling.

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-48128-116647-16

Name of applicant
Mitrokotsa, Aikaterini

Date of birth
781008-3662

Title of research programme
PRECIS: Privacy and security in wearable computing devices

Appendix A

Research programme

Vetenskapsrådet, Box 1035, SE-101 38 Stockholm, tel. +46 (0)8 546 44 000, vetenskapsradet@vr.se

Appendix A

PRECIS: Privacy and Security in Wearable Computing Devices

Aikaterini Mitrokotsa

1 Purpose and Aims

Wireless Communication & Wearable Devices

Wearable computing technology is the next big thing in consumer electronics and computing industry. It is expected to create a wave of adoption similar to that of smartphones. Wearable devices have moved from the realm of science fiction to everyday consumer technology (*e.g.* FitBit, GoogleGlass, SmartWatch). They often collect unique information about each individual (*e.g.* cardiac rhythm) and have emerged as a new means of authentication. They enable many new applications in areas such as smart homes, remote home monitoring, keyless entry in automobiles, NFC (Near Field Communication)/Wi-Fi payments, assisted living and hospital settings, which require strong security and privacy guarantees. Fig. 1 depicts some of the applications of wearable devices such as home care, traffic alerts, activity tracking, home security, energy management.

ABI research states that the global market for wearables could reach 170 million devices by 2017, while a market research report states that wearable computing products market is expected to cross $8 billion in 2018. Wearable computing devices offer a transparent login procedure in a nomadic applications environment (*e.g.* the same wearable device used to authenticate in automobile and building access control, login to computer or mobile devices). Furthermore, the new generation of Implantable Medical Devices (IMDs) enable home monitoring of patients and wireless collection of data from IMDs. This data is relayed to a database, scattering sensitive data to third parties. However, as wireless communication increases it becomes a more attractive target for criminal activity and state surveillance. The goal of PRECIS is to provide accurate and privacy-preserving authentication mechanisms for wearable devices and IMDs, and prepare us for the future of wearable computing.

Figure 1: *Applications of wearable devices.*

Main Challenges

Although the use of wearable devices is becoming the new norm, some important challenges need to be addressed.

Security Threats Numerous recent studies have shown that authentication systems in wireless communications can be (easily) broken. In automobile access control, an adversary (*man-in-the-middle*) may unlock and even start an RFID-enabled car even if the car key is located very far [20]. Similar attacks have also been mounted against bankcards [16], proximity cards, NFC-enabled mobile phones [21] and IMDs. Impersonation attacks against IMDs may lead to life-threatening situations. PRECIS shall safeguard wearable devices against unauthorised access.

Privacy Threats The *privacy implications* of wearable computing devices can lead to oppressive electronic data surveillance. Wearable devices can often be read without authorisation and without leaving a trace. A constellation of wearable and smart home devices reporting back to someone everything we do, does not seem as a fiction story anymore. Google has already started investing in the home automation industry by buying a company called NEST that develops smart-home automated appliances. Ensuring compliance with EU privacy statues cannot begin if we do not understand and cannot measure the effects on privacy of these new technologies. PRECIS has the ambitious goal to provide strong privacy guarantees for authentication in wearable computing.

Imperfect Information Many wearable devices rely on uniquely identifying individuals based on biometric information that is inherently noisy (due to natural variability). Furthermore, in some cases noise in the communication channel may lead to transmission errors, since wearable and implantable devices often operate in an inherently noisy environment. Thus, the development of accurate authentication mechanisms for wearable computing becomes more challenging.

Objectives

These are significant research challenges that we will address using advances from *cross-disciplinary* fields including cryptography, decision-making and machine learning and focus on the design of *privacy-preserving* and *accurate* authentication protocols. The main questions that PRECIS will address are:

– *How do we establish a foundation for security and privacy in wearable computing?*
– *Can privacy-preserving protocols co-exist with authentication protocols in wearable computing?*

PRECIS has the ambitious goal to address these challenges and to introduce a unifying framework for authentication in wearable computing that provides:
a) accurate transparent authentication with high usability, and
b) privacy guarantees even if multiple wearable devices are involved in the authentication process.

Existing solutions provide weak security guarantees something that can be easily demonstrated by the number of attacks against these systems. Furthermore, they address information leakage at a local level; although the functionality of a single wearable device can be privacy-preserving, collectively they unwittingly compromise our privacy. Our novel idea is that privacy should be guaranteed collectively by considering all information leakage if an adversary has access to multiple services related to different wearable devices. Based on our framework we propose to design and evaluate a better seamless authentication process, which solves fundamental security and privacy challenges. In more detail, our plan involves the following aspects of the problem:

i) Multiple devices need to participate in the authentication process. PRECIS shall employ efficient multi-factor authentication protocols where multiple wearable devices are linked to function as a "team" and thus, provide stronger guarantees, increase the certainty and accuracy of user authentication.

ii) The authentication process is performed in the *wireless medium* which facilitates eavesdropping and involves *untrusted* databases where sensitive and private information are stored. PRECIS shall employ secure multi-party computation techniques to guarantee that sensitive information will not be transferred "in the clear" and allow computations with encrypted data shared between untrusted parties.

iii) We need to verify *location proximity* since often the authentication process depends on the proximity to a location. PRECIS shall employ cross-layer authentication protocols to provide strong guarantees regarding the physical proximity of a wearable device to a verifier (authenticator) and safeguard against relay attacks.

iv) We need to answer the fundamental question of privacy-preservation when multiple devices are involved in the authentication and avoid linkability. Existing solutions address information leakage in a local level; although functionality of a single wearable device is privacy-preserving, collectively they compromise our privacy. PRECIS shall answer this question by correlating all the different sources of data related to different wearable devices. This shall be achieved by employing differential privacy and secure-multi party computation.

PRECIS shall provide a unifying framework to tackle all these challenges at the same time by using multi-factor and cross-layer authentication protocols, secure multi-party computation and differential privacy. These fields have been studied mostly in isolation. For instance, differential private mechanisms have been studied in the context of databases and machine learning, but their relation to authentication has not been examined before. Similarly cross-layer authentication in

combination with multi-factor authentication and secure multi-party computation has not been investigated before. PRECIS is sure to lead to breakthroughs in *securing wireless communications* and providing *privacy-guarantees* that are necessary to prepare us for the future of wearable computing.

2 Survey of the field

Wearable Devices & Authentication

Wearable devices often collect unique information about each individual (*e.g.* cardiac rhythm) and have emerged as a new means of authentication. They offer transparent authentication in a nomadic applications environment (*i.e.* mobile devices, computers, cars). A company called *Bionym* has recently launched a device for this purpose which is based on the electrocardiogram (ECG) [1]. However, existing authentication mechanisms [37] dedicated to wearable computing devices are not yet mature.

Authentication & Distance-bounding Authentication in wearable devices often depends on the proximity to a location. For instance, an RFID-enabled car key has to be close enough to the car to unlock it. Other systems such as contactless payment cards, transport tickets work on similar principles. In all these cases, proximity is guaranteed through the perceived operating range of the authentication party (*i.e.* signal attenuation). This creates a significant security vulnerability, since an adversary (*man-in-the-middle*) can perform a simple relay attack to circumvent this assumption on proximity. Verifying the proximity of a protocol participant is very challenging from a protocol design perspective. *Distance-bounding* (DB) protocols are cross-layer authentication protocols based on the round-trip time of carefully defined cryptographic challenge-response exchanges that can be employed to guarantee physical proximity. Numerous DB protocols were proposed [11; 30; 44] and many attacks against them have been published [5; 6; 18]. Part of these protocols are performed under *noisy conditions*. Recently, the PI has proposed the first family of provably secure DB protocols called SKI [7; 8]. Another provably secure protocol attaining quite strong relay attack resistance requirements has been recently published in [19]. However, the security of DB protocols is dependent on the underlying communication channel. It remains an open question the employment of DB protocols in conventional channels similar to those used in NFC.

Authentication & Decision-making Wearable devices, being in constant contact with our bodies, collect information that could be integrated with biometric authentication. However, this information presents a natural variability. The data collecting process has a high degree of variability (*i.e.* fresh biometric trait and stored template). For instance, two different scans of the same fingerprint would result to different captured data (*i.e.* due to the difference in finger pressure during the fingerprint scanning). Many approaches have been proposed to solve this problem [15; 29; 47] but many of them have also been shown to be vulnerable to multiple attacks and lack of a formal proof of correctness. The same problem applies when noise in the communication channel leads to transmission errors. We will approach the authentication problem as a *decision making* problem where we need to decide whether or not to accept the credentials of an identity-carrying entity; a very challenging decision under noisy conditions. This *decision making* process of authentication can be modeled using *game theory* [4]. The authentication problem is formulated as a two-player game between the authentication system (verifier) and the prover. Nevertheless, existing approaches [4] are based on unrealistic assumptions such as knowing the adversary's payoff.

Multi-factor Authentication Relying on just one wearable device might not be enough to achieve accurate authentication. The inherent noise of biometric information (*e.g.* heart rate,

temperature) might lead to false rejection of legitimate users and conversely to false acceptance of unauthorised users. *Grouping-proof* protocols can be employed to guarantee that multiple devices are present at the same time. They have been introduced by Juels [28] in order to provide evidence that two RFID tags are simultaneously present. Subsequently, many *grouping-proof* protocols [40] have been proposed based on rather informal models. Burmester *et al.* [10] have provided a provably secure grouping-proof protocol for RFID tags which has been subsequently proven to be vulnerable to attacks. Hermans and Peeters [27] have introduced a private grouping proof protocol with a provable construction. It remains an open question how to efficiently combine grouping-proof and distance-bounding protocols especially in the setting of wearable computing devices.

Wearable Devices & Privacy-preservation

Wearable devices provide important benefits but they are also accompanied with the threat of ubiquitous electronic surveillance. In many cases, wearable devices could be read by unauthorised individuals without giving any indication about that to their owners. Adversaries could collect personal information ranging from the identity, the location, habits or even medical data which might further lead to discrimination (*i.e.* social stigma for medical conditions, reveal information to health insurances). For instance, wearable devices produce traces that can subsequently be used to track individuals. Although data traces might be sanitised and anonymised to avoid privacy threats, they can still reveal information that could be employed for the generation of user profiles. Location and identity can also be leaked in wireless communications, not only by eavesdropping transmitted messages, but also by measuring signal strength and messages' arrival times in the physical layer.

The problem of privacy-preservation in wireless communication has already received a lot of attention in the literature. Location privacy in the context of distance-bounding, was introduced by Rasmussen and Čapkun [43], who noted that DB protocols may leak further location-related information than just the proximity of the verifier to the prover. To combat this, they proposed a privacy-preserving DB protocol [43] (RČ protocol). However, the RČ protocol has been shown to be vulnerable to attacks [3; 35]. The PI [35] has proposed a new DB protocol that improves the basic construction of the RČ protocol and renders it secure against the latter attacks. Additionally, the PI has proven [36] that location privacy is information-theoretically impossible for omniscient adversaries. However, for limited adversaries, carefully chosen parameters enable computational, provable location privacy in practice.

A survey of privacy preservation in wireless sensor networks is presented in [31], while currently there are two main provably secure models for privacy-preservation in RFID systems: one based on simulation [48] and one on indistinguishability [26]. However, the problem is far more general and there is a need for holistic security models that comprises not only protocols but the whole system in which they are deployed.

3 Project Description

PRECIS' Novel Approaches to Target the Challenges

This section connects PRECIS' approach with the state-of-the-art and outlines how we shall address the critical research problems associated with the challenges. Unlike earlier approaches, PRECIS attempts to boldly take an innovative approach that spans privacy-preservation and accurate authentication by employing cross-disciplinary fields including cryptography, decision making and machine learning.

Among the important questions that we want to investigate are:

i) How can we achieve accurate and robust authentication with wearable computing devices?

ii) How can we guarantee privacy-preservation when multiple wearable devices are involved?

iii) How can we efficiently use multi-factor authentication and inter-communication between heterogeneous wearable computing devices?

Two parallel research directions will be followed. **Track A** shall focus on the employment of cryptographic primitives for authentication and privacy preservation. **Track B** will focus on the employment of decision making and machine learning approaches including differential privacy. Both research tracks will aim at solving the authentication problem in wearable computing devices while maintaining privacy-preservation.

Our work will be organised around three core axes. Firstly, PRECIS shall provide *efficient authentication mechanisms* for wearable device. Secondly, we shall introduce multi-factor authentication and inter-communication for heterogeneous wearable devices. Finally, PRECIS shall provide *privacy-preservation guarantees* for the authentication process via wearable devices. The principal investigator (Katerina Mitrokotsa) has recently joined Chalmers (Aug. 2013) as assistant professor. She was recruited through a very competitive process (1 out of ∼70 candidates world-wide in ICT subjects) from a program for ICT Areas of Advance[1] that Chalmers uses to recruit international top talent. She has a strategic position that Chalmers provides in order to invest in promising research directions.

Even though the financial request for the PI is 25% (for 5 years) she will be able to spend more time on being actively involved in the project. Additionally, one PhD student will be employed throughout the project (80%) while 20% will be spent on teaching activities. Progress will be made in a number of 6-month cycles alternating theoretical and practical work. Implementation of new algorithms-protocols usually takes 1-3 weeks, depending on the complexity. Below we give more details on the research methodology. The research is carried out in three work packages that are all grounded in a common methodological framework.

WP 1 - Wearable devices & Authentication

PRECIS will address the authentication problem in wearable devices based on three approaches: distance-bounding, efficient decision making and multi-factor authentication.

Task 1.1 - Distance-bounding (Track A) PRECIS shall investigate the development of efficient authentication protocols to verify the proximity of wearable computing devices to the authenticator. It remains an open question the employment of DB protocols in conventional channels similar to those used in NFC. PRECIS shall design novel cross-layer authentication protocols that offer distance bounding transparently. We shall do so by leveraging the ideas behind modern DB protocols (which rely on the physical layer) and provide an interface to the network and application layer. This will guarantee the transmission of messages with a certain delay and within a certain probability of error.

A first extension of distance bounding to group settings has been introduced by [49]. Furthermore, a DB protocol for IMDs has been introduced by Rasmussen *et al.* [42] based on ultrasonic. However, there are still many open issues regarding security and privacy of group DB protocols and DB protocols in IMDs. PRECIS will investigate how we may achieve provably secure and privacy-preserving group DB protocols and how grouping-proof protocols [40] may be employed to provide stronger guarantees of accurate authentication.

Task 1.2 - Decision-making (Track B) We will approach the authentication problem as a decision making problem where we need to decide whether or not to accept the credentials of an identity-carrying entity; a very challenging decision under noisy conditions. The goal is to minimise the loss of the authenticator and to increase the accuracy of the authentication system. The PI has already provided an *expected loss* framework for DB protocols [13]. PRECIS will build on this recent work by the PI and investigate its extension to wearable computing technologies. We shall examine what is the loss regarding the resources we need to spend, to increase the accuracy of the authentication and how many bits of private information might be revealed without compromising the security of the system. We shall specify a budget or cost for resource use, privacy leakage and for the authentication errors.

[1] `http://www.chalmers.se/en/areas-of-advance/ict/`

Task 1.3 - Multi-factor authentication (Tracks A & B) PRECIS shall investigate the use of multiple wearable devices in order to achieve accurate authentication. This is quite challenging considering the inherent noise of biometric information collected by multiple wearable devices for the authentication purposes. PRECIS shall investigate how to efficiently combine *grouping-proof* (GP) protocols and *distance-bounding* (DB) protocols for multiple wearable devices in the context of multi-factor authentication (including multi-modal biometrics). Authentication protocols dedicated to wearable computing devices are not yet mature [45]. Existing solutions use rather informal models, are poorly grounded in theory and do not take into consideration realistic assumptions in order to achieve the alleged security. PRECIS shall examine the efficient deployment of multi-modal biometrics (*i.e.* behavioral, physiological traits). Efficient classification methods shall be employed to guarantee the accuracy of the authentication (*i.e.* Support Vector Machines, Gaussian Mixture Models). PRECIS shall build on efficient multi-modal authentication and efficient combination of GP and DB protocols to provide provably secure and accurate authentication protocols.

WP 2 - Wearable devices & Privacy

PRECIS will investigate the problem of privacy preservation in wearable computing devices based on two main approaches: privacy-preservation based on cryptographic primitives and privacy-preservation based on machine learning and differential privacy.

Task 2.1 - Privacy-preservation & cryptographic primitives (Track A) Guaranteeing privacy preservation and safeguarding against information leakage is very challenging when multiple devices and consequently multiple third party service providers are involved in the process. Even if each transition has been anonymised or encrypted, collectively they unwittingly compromise our privacy. It remains an open question how to address this problem in a collective way. PRECIS shall investigate how to achieve accurate authentication without violating the privacy rights of the users and preserve both *content* information (*i.e.* transmitted data) as well as *context* data (*i.e.* location). Due to the nature of the problem in order to achieve privacy-preservation in a collective way we need to build upon a number of techniques.

We shall investigate secure multiparty computation schemes such as *homomorphic* encryption techniques [23; 39] and *oblivious transfer* [32] to guarantee that sensitive information will not be transferred "in the clear" and allow computations with encrypted data. Special attention will be paid on the employment of these homomorphic techniques since Bringer *et al.* [46] have shown that bit-by-bit encryption may lead to serious threats (*i.e. hill climbing* [33]). Since fully homomorphic encryption is computationally expensive we shall focus on the employment of partial homomorphic techniques and investigate the employment of recently proposed schemes [9; 22] that show promise regarding the computational cost. Furthermore, we shall investigate the employment of *zero-knowledge proofs* [24] and *undeniable signatures* [12] in a distributed setting. These effectively give control over who can verify one's identity and can be very important tools for *privacy-preservation. Private information retrieval (PIR)* techniques [38] will be employed to recover private information stored in a database (*i.e.* biometric templates). The main challenge we want to tackle is to develop lightweight techniques for resource-constrained devices where the trade-off between privacy and computation can be tuned according to the target application.

Task 2.2 - Machine learning & differential privacy (Track B) *Privacy-preservation* has been studied by research communities in machine learning and statistics. Recently, the strands of this work have begun to merge, with the formalism of *differential privacy* [17]. Consider the problem of learning from a database that contains private information and then communicating the statistical findings to an untrusted party. The goal is to convey useful information to any queries, but also strive to minimise what is revealed about the original data, as it can contain sensitive information, *e.g.* whether a particular person suffers from a disease. *Differential privacy* [17] offers a formal framework that can be used to bound the amount of info that an

adversary can discover. For instance, recent IMDs provide home monitoring via wireless base stations that subsequently relay data to doctors with web access to a database [25] (Fig. 2). If we consider that an unauthorized party (*i.e.* health insurance) would like to have access to the database to get statistical information about the monitored patients, differential privacy could be employed to protect sensitive information. PRECIS shall employ differential private mechanisms to safeguard sensitive information. Recently, it has been shown that differentially private mechanisms also enforce truthfulness and are resistant to coalitions [34]. An interesting open question will be to apply such methods to dynamic problems, such as those faced in wearable computing technology and to address the question of how to implement such mechanisms when the service provider is not fully trusted. Furthermore, we shall build on private similarity testing [2] to guarantee that our authentication mechanisms are private-preserving (*i.e.* via appropriate similarity metrics).

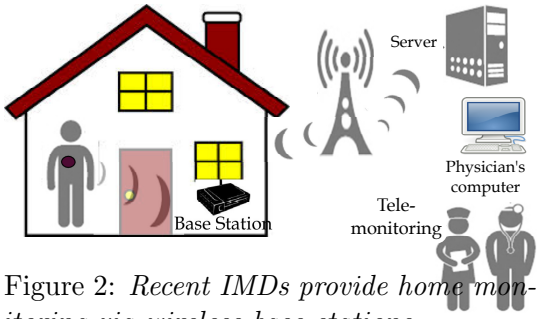

Figure 2: *Recent IMDs provide home monitoring via wireless base stations.*

WP 3 - Evaluation of the developed framework in different settings

We will use input from the unified framework developed in WP 1 and WP 2 to create evaluation scenarios. Two example scenarios will be authentication and privacy-preservation in *smart-home appliances* and *healthcare applications*. We will then simulate these scenarios in order to evaluate the developed framework.

For the first scenario, we shall investigate how accurate and privacy-preserving authentication could be implemented based on one or multiple wearable devices in a *smart-home setting*. We shall consider that wearable computing devices shall be used to offer transparent authentication in a nomadic applications environment; this includes a single wearable device used for authentication to login in PCs, mobile devices (*i.e.* iPads, iPods, mobile phones), access control (*e.g.* cars, buildings) and e-payment transactions. We shall investigate privacy-preservation for content information (*i.e.* transmitted messages) as well as context information (*i.e.* location) privacy. We shall answer the question: *Is it still possible to identify individuals if their activity is collected from multiple sources (*i.e. *NFC payments, access control, coffee-shop wifi access)?*

For the second scenario, we shall consider accurate authentication and privacy-preservation for wearable devices employed in healthcare monitoring wearable devices as well as IMDs. Currently, wearable devices and IMDs employed in healthcare applications provide limited or no security and privacy guarantees. For instance, today's IMDs store detailed medical information (*i.e.* patient's identity, medical history) that can be easily read by passively listening to radio communication. PRECIS shall guarantee data integrity and combat unauthorised reading and modification of sensitive information stored in wearable devices and IMDs. Regarding privacy, we shall consider both the bearer's identity privacy as well as the measurements (recorded logs) privacy.

4 Significance

Scientific Significance

PRECIS shall provide a unifying framework for accurate and privacy-preserving authentication mechanisms and prepare us for the next generation of wearable computing technology; something that is missing from the current state-of-the-art. Existing solutions address information leakage at a local level; although the functionality of a single wearable device can be privacy-preserving, collectively they unwittingly compromise our privacy. PRECIS' novel idea is to guarantee privacy in a collective way by considering all information leakage if an adversary has access to multiple services related to different wearable devices while at the same time provide transparent and accurate authentication. The time has come to embark on this new track and establish a foundation for security and privacy in wearable computing. PRECIS will enable innovation in the core of

wireless communications and will extend opportunities offered by recent advances in the field of cryptography, decision-making and machine learning that show considerable promise. This seems to be the ideal moment to investigate the use of such methods to solve the problem of *reliable* and *privacy-preserving* authentication mechanisms and prepare us for the future of wearable computing. Boosting research in security and privacy for wearable computing technology will allow Sweden to lead secure and privacy-preserving communications in the research community.

Societal Significance

Supporting research in securing wearable computing technology gives Sweden an important advantage in the long-term competitiveness in both research and development. PRECIS fits perfectly to Sweden's objectives and strategy for sustainable cities. VR's support is vital for leveraging PRECIS' high potential in a strategic area that is lacking in Sweden. More precisely, the proposed project shall definitely contribute to the Swedish excellence and competitiveness in the following sectors:

Healthcare Wearable computing technologies have many applications in healthcare and well-being and shall have a substantial impact on fostering good heath in ageing Europe. They can enhance inpatient safety and facilitate patient home monitoring and support the shift from hospital care to citizen-centered care. Accurate and privacy-preserving authentication in such applications is urgent considering the serious implications if wearable devices storing critical information (*e.g.* medical history) are compromised.

Vehicles & transport Modern vehicles are already using wearable devices in their access control system (*e.g.* RFID enabled automobiles) and communicate wirelessly with other cars (*i.e.* info about traffic), on-road signs, toll-collection systems and repair shops. RFID tags are also used in public transit systems and are already under attack (*e.g.* Dutch OV-chip card). Wearable technology will soon replace transport cards and can help make transport more sustainable, efficient and smarter.

Wireless & Mobile Technologies Wearable computing technologies will soon be used in supply chain management, inventory control and environmental monitoring. PRECIS focuses on improving the reliability of these technologies. The research results may also be used to improve the authentication mechanisms for secure and accurate transactions.

Energy efficiency Smart home appliances have already arrived and wearable devices are used to adjust environmental control systems (*e.g.* central heating) in an energy efficient way. Wireless communications in smart grids enable both utilities and customers to transfer, monitor, predict and manage energy usage effectively. Accurate and privacy-preserving authentication for wearable devices may only have positive impact on energy efficient systems.

5 Preliminary Results

The PI has all the required expertise to tackle the multi-dimensional problem of privacy-preserving and accurate authentication in wearable computing. A problem that requires expertise in cryptographic primitives, decision making and machine learning and is very rare to find in one person. Our preliminary results [7; 8; 14; 36; 41] have already made impact in the security community. As already mentioned in section 1, recently the PI has proposed the first family of provably secure distance-bounding protocols [7; 8] and is experienced in all aspects of protocol design and security analysis. Furthermore, the PI has investigated the use of wearable devices in a hospital setting [41] in order to enhance inpatient medication safety and more precisely to facilitate the medication administration process and reduce medication errors. The proposed scheme is based on the use of RFID tags and grouping-proof protocols to make sure that correct medication is administered to the corresponding patient. Additionally, the PI has investigated the problem of location privacy in distance-bounding protocols [36] and has proven that location privacy is

information-theoretically impossible for adversaries that are able to see the signal strengths of the transmissions and the sending and receiving time of transmitted messages. However, the PI has shown that for limited adversaries, carefully chosen parameters enable computational, provable location privacy in practice. Furthermore, the PI has recently generalised the concept of differential privacy to arbitrary dataset distances [14].

6 National and International Collaboration

The PI had the chance to work in four academic institutes in four different European countries (*i.e.* Switzerland, The Netherlands, Greece, Sweden) and thus, to establish a strong scientific network of top scientists who operate at the forefront of many disciplines related to this proposal.

National Collaborations Nationally, we will collaborate in the topic of wireless communications and secure communications with Prof. Gunnar Karlsson and Prof. Panos Papadimitratos at KTH correspondingly. Additionally, we will collaborate with Prof. Andrei Sabelfeld and his group at Chalmers who brings know-how in web and information security as well as Dr. Christos Dimitrakakis who is well known for his work in optimal decision making.

EU Collaborations The EU FP7 project BEAT (Biometric Evaluation and Testing) in which the PI is involved focusing on privacy-preserving biometric authentication will create important synergies with existing collaborators and partners in the domain of biometric authentication and cryptography (SAFRAN-Morpho, Auton. Univ. of Madrid (UAM), KU Leuven). Furthermore, we have a strong collaboration with Prof. Jan van der Lubbe in TU Delft in the Netherlands as well as with Dr. Pedro Peris-Lopez at Madrid Carlos III Univ. of Madrid in Spain in RFID security and privacy. Moreover, we have a good collaboration with the information security group and the smart card centre at Royal Holloway headed by Prof. Konstantinos Markantonakis.

Non-EU Collaborations We will collaborate with Prof. Kanta Matsuura and his group at University of Tokyo on provable security. A collaboration is already established via research visits that we have recently started. We will also collaborate with Prof. Gerhard Hancke at City University of Hong Kong with whom we have recently launched a collaboration on cross-layer authentication via a STINT project. The PI has a good and long-lasting collaboration with Dr. Tom Karygiannis and his group at NIST and Prof. Berhnard Plattner and his group at ETHZ as well as with Prof. Serge Vaudenay at EPFL.

A *Dagstuhl Seminar on Security and Privacy in Wearable Computing*, with some of our collaborators, will be organized to disseminate the results of PRECIS.

7 Other Grants

The project *DecentLP: Robust Decentralized Location Privacy* headed by Prof. Andrei Sabelfeld is submitted as VR project grant in April 2014. Katerina Mitrokotsa is a co-applicant in the *DecentLP* project and shall devote 5% of her time. Additionally, we should make clear that the two projects *DecentLP* and PRECIS have *no overlap*. More precisely, *DecentLP* is focusing on providing privacy-preserving techniques for location-based services. On the contrary, PRECIS focuses on the development of a unifying framework for accurate and privacy-preserving authentication in wearable computing. Although the two projects do not overlap they create useful synergies. Theoretical results developed in PRECIS could be applicable to *DecentLP*.

References

[1] F. Agrafioti, F. M. Bui, and D. Hatzinakos. Secure telemedicine: Biometrics for remote and continuous patient verification. *Journal Comp. Netw. and Communic.*, 2012(924791), 2012.

[2] M. Alaggan, S. Gambs, and A.-M. Kermarrec. Private similarity computation in distributed systems: From cryptography to differential privacy. In *Principles of Distributed Systems*, pages 357–377. 2011.

[3] J.-P. Aumasson, A. Mitrokotsa, and P. Peris-Lopez. A Note on a Privacy-preserving Distance Bounding Protocol. In *Proc. of ICICS*. 2011.

[4] M. Barni. A game theoretic approach to source identification with known statistics. In *Proc. of ICASSP*, 2012.

[5] A. Bay, I. Boureanu, A. Mitrokotsa, I. Spulber, and S. Vaudenay. The Bussard-Bagga and Other Distance Bounding Protocols under Man-in-the-Middle Attacks. In *Proc. of Inscrypt*, 2012.

[6] I. Boureanu, A. Mitrokotsa, and S. Vaudenay. On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols - PRF-ness alone Does Not Stop the Frauds! In *Proc. of LATINCRYPT*, 2012.

[7] I. Boureanu, A. Mitrokotsa, and S. Vaudenay. Practical and Provably Secure Distance-Bounding. In *Proc. of ISC*, 2013.

[8] I. Boureanu, A. Mitrokotsa, and S. Vaudenay. Secure & Lightweight Distance-Bounding. In *Proc. of LightSec*, 2013.

[9] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In *Proc. of TCS*, 2012.

[10] M. Burmester, B. de Medeiros, and R. Motta. Provably secure grouping-proofs for RFID tags. In *Proc. of CARDIS'08*.

[11] L. Bussard and W. Bagga. Distance-Bounding Proof of Knowledge Protocols to Avoid Terrorist Fraud Attacks. Technical Report RR-04-109, EURECOM, 2004.

[12] D. Chaum. Zero-knowledge undeniable signatures. In *Proc. of EUROCRYPT*, 1990.

[13] C. Dimitrakakis, A. Mitrokotsa, and S. Vaudenay. Expected Loss Bounds for Authentication in Constrained Channels. In *Proc. of INFOCOM*, 2012.

[14] C. Dimitrakakis, B. Nelson, A. Mitrokotsa, and B. I. P. Rubinstein. Robust, secure and private bayesian inference. *Arxiv*, abs/1306.1066, 2013.

[15] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*, 38(1):97–139, Mar. 2008.

[16] S. Drimer and S. J. Murdoch. Keep your enemies close: distance bounding against smartcard relay attacks. In *Proc. of USENIX*, 2007.

[17] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Proc. of TCC*, 2006.

[18] M. Fischlin and C. Onete. Subtle kinks in distance-bounding: an analysis of prominent protocols. In *Proc. of WiSec*, 2013.

[19] M. Fischlin and C. Onete. Terrorism in distance bounding: Modeling terrorist fraud resistance. In *Proc. of ACNS*, 2013.

[20] A. Francillon, B. Danev, and S. Čapkun. Relay attacks on passive keyless entry and start systems in modern cars. In *Proc. of NDSS*, 2011.

[21] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis. Practical NFC peer-to-peer relay attack using mobile phones. In *Proc. of RFIDSec*, 2010.

[22] C. Gentry, A. Sahai, and B. Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Proc. of CRYPTO*, 2013.

[23] S. Goldwasser and S. Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In *Proc. of STOC*, 1982.

[24] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, 18(1):186–208, 1989.

[25] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing*, 7(1):30–39, 2008.

[26] J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel. A new RFID privacy model. In *Proc. of ESORICS*, 2011.

[27] J. Hermans and R. Peeters. Private yoking proofs: Attacks, models and new provable constructions. In *RFIDSec*, 2012.

[28] A. Juels. "Yoking-proofs" for RFID tags. In *Proc. of PERCOMW*, 2004.

[29] A. Juels and M. Sudan. A fuzzy vault scheme. *Jrnl Designs, Codes & Cryptography*, 38(2):237–257, February 2006.

[30] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira. The Swiss-Knife RFID Distance Bounding Protocol. In *Proc. of ICISC*, volume 5461 of *LNCS*, pages 98–115, 2008.

[31] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham. Privacy preservation in wireless sensor networks: A state-of-the-art survey. *Ad Hoc Networks*, 7(8):1501–1514, Nov. 2009.

[32] H. Lipmaa. An oblivious transfer protocol with log-squared communication. In *Proc. of ISC*, 2005.

[33] M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fern, J. Ortega-Garcia, and J. A. Siguenza. Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification. In *Proc. of ICCST*, 2006.

[34] F. McSherry and K. Talwar. Mechanism design via differential privacy. In *Proc. of FOCS*, 2007.

[35] A. Mitrokotsa, C. Onete, and S. Vaudenay. Mafia Fraud Attack against the RČ Distance-Bounding Protocol. In *Proc. of IEEE RFID T-A*, 2012.

[36] A. Mitrokotsa, C. Onete, and S. Vaudenay. Location leakage in distance bounding: Why location privacy does not work. *Computers & Security*, To Appear 2014.

[37] S. Ojala, J. Keinanen, and J. Skytta. Wearable authentication device for transparent login in nomadic applications environment. In *Proc. of SCS*, 2008.

[38] R. Ostrovsky and W. E. Skeith. A survey of single-database private information retrieval: techniques and applications. In *Proc. of PKC*, 2007.

[39] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Proc. of EUROCRYPT*, 1999.

[40] P. Peris-Lopez, A. Orfila, J. C. Hernandez-Castro, and J. C. A. van der Lubbe. Flaws on RFID grouping-proofs. Guidelines for future sound protocols. *J. Network & Computer Applications*, 34(3):833–845, 2011.

[41] P. Peris-Lopez, A. Orfila, A. Mitrokotsa, and J. C. A. van der Lubbe. A comprehensive RFID solution to enhance inpatient medication safety. *I. J. Medical Informatics*, 80(1):13–24, 2011.

[42] K. B. Rasmussen, C. Castelluccia, T. Heydt-benjamin, and S. Čapkun. Proximity-based access control for implantable medical devices. In *Proc. of CCS*, 2009.

[43] K. B. Rasmussen and S. Čapkun. Location Privacy of Distance Bounding. In *Proc. CCS'08*, pages 149–160. ACM, 2008.

[44] J. Reid, J. M. Gonzalez Nieto, T. Tang, and B. Senadji. Detecting Relay Attacks with Timing-based Protocols. In *Proc. of ASIACCS*. ACM, March 2007.

[45] N. Sarier. Practical multi-factor biometric remote authentication. In *Proc. of BTAS*, Sept. 2010.

[46] K. Simoens, J. Bringer, H. Chabanne, and S. Seys. A framework for analyzing template security and privacy in biometric authentication systems. *IEEE Trans. Inform. Forens. & Sec.*, 7(2):833–841, 2012.

[47] P. Sukarno, M. Phu, N. Bhattacharjee, and B. Srinivasan. Increasing error tolerance in biometric systems. In *Proc. MoMM'10*, pages 50–55, New York, NY, USA, 2010. ACM.

[48] S. Vaudenay. On privacy models for RFID. In *Proc. of ASIACRYPT*, 2007.

[49] S. Čapkun, K. M. E. Defrawy, and G. Tsudik. Group distance bounding protocols. In *Proc. of TRUST*, 2011.

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-48128-116647-16

Name of applicant
Mitrokotsa, Aikaterini

Date of birth
781008-3662

Title of research programme
PRECIS: Privacy and security in wearable computing devices

Appendix B

Curriculum vitae

Vetenskapsrådet, Box 1035, SE-101 38 Stockholm, tel. +46 (0)8 546 44 000, vetenskapsradet@vr.se

Personal Information

Mitrokotsa, Aikaterini, 781008-3662
ORCID: 0000-0002-7073-0258, Web site: `http://www.cse.chalmers.se/~aikmitr/`

Higher Education Qualifications

2002-2007: **PhD in Computer Science**, University of Piraeus, Greece, On the Subject: **"Intrusion Detection in Computer Networks Using Machine Learning Algorithms"**, Supervisor: Prof. Christos Douligeris, with highest distinction, **PhD Award date:** 12/11/2007.

1997-2001: **B.Sc. Degree in Computer Science**, University of Piraeus, GPA: 8.4/10.

Employment

08.2013-Today: Assistant Professor, Department of Compute Science & Engineering, **Chalmers University of Technology**, Sweden (80% research, 20% teaching).

09.2012-08.2013: Professor Univ. of Applied Sciences Western Switzerland (HES-SO), Geneva.

07.2010-12.2012: Research Associate-**Marie Curie Fellow**, **EPFL**, Switzerland.

10.2008-04.2010: Research Associate-**NWO Rubicon Fellow**, **TU Delft**, The Netherlands.

09.2007-09.2008: Visitor Assistant Professor, **Vrije Universiteit**, The Netherlands.

02.2002-09.2007: Research assistant, University of Piraeus, Greece.

06.2002-07.2007: Visiting Faculty, Technological Education Institute (TEI) of Chalkida, Greece.

01.2004-03.2004: Research assistant, Hellenic Authority for the Information and Communication Security and Privacy (ADAE), Greece.

01.2002-05.2002: Consultant of Information Security for the Company Encode S.A., Greece.

Qualification required for appointment as docent

Applied in Jan. 2014 expected result April 2014

Fellowships and Awards

2013-2014: **STINT Initiation Grant**, Project: *"Cross-layer Authentication Protocols for Wireless Networks"* (∼150.000 SEK - 2 partners).

2013-2017: **Chalmers ICT Areas of Advance** funding of research for 4 years (including funding for 1 PhD student) (∼900.000 €). Very competitive (1 selected from ∼70).

2012-2016 **STREP (FP7)**, Project: *"BEAT: Biometrics Evaluation & Testing"* (∼3.5 millions €-10 partners). Project number: 284989.

2010-2012: **Marie Curie IEF (FP7):** Project: *"PPIDR: Privacy-Preserving Intrusion Detection and Response in Wireless Communications"* (∼166.000 €). Project number: 252323.

2009-2010: **ICT Talent Grant** awarded by the TU Delft. Project: *"Intrusion Detection & Response in Wireless Communication"*. (∼35.000 €).

2008-2009: **NWO Rubicon Grant**. Project: *"Intrusion Detection in Ubiquitous Computing Technologies"* (55.000 €).

2002-2005: Scholarship by the **Foundation of Bodossaki** for PhD studies.

2001: Led the graduation oath for the **highest GPA among all students** of the Department.

1998-2000: Award by the **University of Piraeus** for best performance for undergraduate studies.

1997-1999: Best Student Award & Scholarship by the **National Scholarship Foundation**, GR.

Conference Organisation

– **Publication Chair:** *AfricaCrypt* 2012
– **Program Chair:** *ACM Workshop on Artificial Intelligence and Security (AISec 2014)*, *ECML/PKDD Workshop on Privacy & Security Issues in Data Mining & Secure Machine Learning* 2010, *International Workshop on RFID Technology* 2009-2010.

Selected service in Program Committees

IEEE INFOCOM 2015-2014, IEEE Conference on Communications & Network Security (**IEEE CNS 2013-2014**), Intern. Conference on Applied Cryptography & Network Security (**ACNS 2014**) International Conference on Availability, Reliability & Security (**ARES 2013-2014**), **NordSec 2014**, Workshop on RFID Security & Privacy (**RFIDsec 2013**), **Indocrypt 2013**, **Africacrypt 2012**.

Supervised Post-doctoral Researchers
– Dr. Aysajan Abidin, 2014-Today, Topic: *"Privacy-preserving biometric authentication"*, Chalmers.

Supervised PhD Students
– Asli Bay, EPFL 2011-2012, Topic: *"Attacks in Authentication Protocols"*.
– Sergio Pastrana, Carlos III University of Madrid 2009-2010, Topic: *"Intrusion Detection in MANET.*
– Michael Beye, TU Delft 2009-2010, Topic: *"RFID Security & Privacy"*.

Supervised Master Students
– Erica Löfström, MSc. Thesis: *"Diversification in a white-box environment"*, Chalmers 2014.
– Christoffer Karlsson, MSc. Thesis: *"Distance-bounding protocols"*, Chalmers, 2014.
– Daniel Olausson, MSc. Thesis: *"Privacy-preserving biometrics"*, Chalmers, 2014.
– André Malm, MSc. Thesis: *"Obfuscation in a white-box environment"*, Chalmers 2014.
– Iosif Spulber, MSc. Project: *"Solving the Hidden Number problem"*, EPFL, 2012.
– Tamas Nagy, MSc. Thesis: *"Intrusion Detection in RFID systems"*, Vrije Universiteit, 2008.
– Despo Galataki, MSc. Project: *"Intrusion Detection within a building"*, Vrije Universiteit, 2008.
– Atul Mehta, MSc.Project: *"Intrusion Detection for Integrated WSN & RFID"*,Vrije Universiteit, 2008.
– Manolis Tsagkaris, MSc. Thesis: *"Intrusion detection in MANETs"*, Univ. of Piraeus, 2007.

Institutional Responsibilities
– **Director** of the *Master of Advanced Studies* Program: *Information Security Management Systems*, University of Applied Science Western Switzerland (HES-SO) (2012-2013).
– **PhD Thesis examiner-reviewer:** ▪ J. Magazinius, Chalmers, Topic: *"Dynamic Enforcement of decentralized security policies"* 2013, ▪ L. Mirowski, Univ. of Tasmania, Topic: *"A whole of system approach of security analysis in RFID systems using an integrated layered reference model"* 2011.
– *MSc. Thesis examiner* for Z. Chen, EPFL, Topic: *"The LPN Problem & algebraic methods"* 2013.

Commissions of Trust
– **Editorial Board:**
▪ IEEE Communications Letters (2013-today).
▪ Computers & Security, Elsevier (2013-today).
▪ KSII Transactions on Internet & Information Systems (2013-today).
▪ Information Security Journal (Taylor & Francis) (2012-today).
– **Guest editor:**
▪ Special Issue in IEEE Transactions on Dependable & Secure Computing.
▪ Special Issue in Journal of Personal & Ubiquitous Computing, Springer.
▪ Special Issue in Journal of Networks & Computer Applications.
– **Reviewer:**
▪ National Science Foundation (NSF) CAREER Proposals.
▪ Research Council for Natural Sciences & Engineering at the Academy of Finland.
▪ Discovery Grants Natural Sciences & Engineering Research, Canada.
– **Groups of experts:**
▪ ENISA Permanent Stakeholders Group (PSG) (2012-2015).
▪ ENISA's expert group PROCENT-EG (2009-2010).
▪ Network & Information Security (NIS) platform for the Working Group (WG 3) Secure ICT Research & Innovation.

Selected Teaching Experience
– Operating Systems, Chalmers, Winter semester, 2013.
– Security Protocols & Applications, EPFL, Spring semester 2011, 2012.
– Cryptography & Security, TU Delft, 2010.
– Computers & Network Security, Vrije Universiteit, Spring semester, 2008.
– Advanced Topics in Network Security, Vrije Universiteit, Winter semester 2007.

Memberships of Scientific Societies
▪ **ERCIM** Working Group in Security & Trust Management, ▪ **Sys-Sec** (NoE FP7) Associate Member, ▪ **IEEE** member, ▪ **ACM** member, ▪ **IACR** member, ▪ Member of **European Association for Biometrics**, ▪ Award co-chair for ACM Networking Networking **N2Women** (ACM SIGMOBILE).

Major Collaborations
▪ **University of Tokyo**, Prof. Kanta Matsuura (Research visits) Topic: *"Authentication protocols"*.
▪ **City University of Hong Kong**, Prof. Gerhard Hancke, Collaboration in STINT project.
▪ **EPFL**, Prof. Serge Vaudenay, Topic: *"Provable Security"*.
▪ **ETHZ**, Prof. Bernhard Pattner, Topic: *"Intrusion Response"*.
▪ **Carlos III Univ. of Madrid**, Prof. Pedro Peris Lopez, Topic: *"RFID Security & Privacy"*.

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-48128-116647-16

Name of applicant
Mitrokotsa, Aikaterini

Date of birth
781008-3662

Title of research programme
PRECIS: Privacy and security in wearable computing devices

Appendix C

List of publications

Vetenskapsrådet, Box 1035, SE-101 38 Stockholm, tel. +46 (0)8 546 44 000, vetenskapsradet@vr.se

Appendix C: Publication List[*†]

Aikaterini Mitrokotsa

I have written more than 40 scientific publications in international journals, books, and conference proceedings and my work has been cited more than 700 times while my *h-index* is 12 and my *i10-index* is 14 (according to *Google Scholar*). I have participated in the organization of workshops, served as reviewer for 20 journals and multiple conferences, and have served as guest editor for three special issues focusing on secure communications and the RFID technology (Journal of Networks and Computer Applications (Elsevier), IEEE Transactions on Dependable and Secure Computing, Personal and Ubiquitous Computing (Springer)). Currently, among others I serve as associate editor for the *IEEE Communications Letters* and the *Computers & Security* journal (Elsevier). I have also been invited to give lectures on subjects related to my expertise by a number of institutions (International Telecommunication Union (ITU), European Patent Office (EPO)).

Peer-reviewed original articles in International Journals

[J1*] A.Mitrokotsa, C. Onete, S. Vaudenay, "Location Leakage in Distance-Bounding: Why Location Privacy does not Work", *Computers & Security*, Elsevier, To Appear 2014.

[J2] A. Mitrokotsa, P. Peris-Lopez, C. Dimitrakakis, S. Vaudenay. "On selecting the nonce length in distance-bounding protocols", *Computer Journal (Oxford)* 56(10): 1216-1227, (2013) doi: 10.1093/comjnl/bxt033.

[J3] A. Mitrokotsa, C. Dimitrakakis, "Intrusion Detection in MANET using Classification Algorithms: The Effects of Cost and Model Selection", *Ad hoc Networks*, Elsevier, doi: 10.1016/j.adhoc.2012.05.006, 11(1): 226–237, Jan. 2013.

[J4] S. Pastrana, A. Mitrokotsa, A. Orfila, P. Peris-Lopez. "Evaluation of Classification Algorithms for Intrusion Detection in MANETs". Knowledge-Based Systems, Elsevier, doi: 10.1016/j.knosys.2012.06.016, Vol. 36, Dec. 2012, pages 217–225.

[J5*] P. Peris-Lopez, A. Orfila, A. Mitrokotsa, J.C.A. van der Lubbe, "A Comprehensive RFID solution to enhance inpatient medication safety", *International Journal of Medical Informatics*, 80(1): 13–24, Jan. 2011.

[J6] A. Mitrokotsa, C. Dimitrakakis, P. Peris-Lopez, J.C. Hernandez-Castro. "Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels". *IEEE Communications Letters*, Feb. 2010, 14(2):121–123, Feb. 2010.

[J7] A. Mitrokotsa, N. Komninos, and C. Douligeris. "Protection of an Intrusion Detection Engine with Watermarking in Ad Hoc Networks". *International Journal of Network Security*, 10(2): 93–106, March 2010.

[*] This publication list corresponds to the last eight years. The full publication list can be found in `http://www.cse.chalmers.se/~aikmitr/Publications.html`

[†] Selected relevant publications are denoted by * and bold letters.

[J8] A. Mitrokotsa, M.R. Rieback, and A.S. Tanenbaum. "Classifying RFID Attacks and Defenses". *Special Issue on Advances in RFID Technology, Information Systems Frontiers, Springer*, LLC 2009, 12(5):491–505, 2010.

[J9] A. Mitrokotsa, N. Komninos, C. Douligeris, (2007), "Intrusion Detection and Response in Ad hoc Networks", *International Journal on Computer Research, Special Issue on Advances in Ad Hoc Network Security*, Nova Science Publishing Inc., Vol. 15, Issue 1, pages 23–55, 2007.

Peer-reviewed Conference Contributions

[C1*] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Practical & Provably Secure Distance-Bounding", In *Proceedings of the 16th Information Security Conference*, Dallas, Texas, USA, Nov. 2013.

[C2*] C. Dimitrakakis, A. Mitrokotsa, and S. Vaudenay, "Expected loss bounds for authentication in constrained channels", In *Proceedings of INFOCOM 2012*, Orlando Florida 2012, March 2012.

[C3] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Secure & Lightweight Distance-Bounding", In Proceedings of the 2nd International Workshop on Lightweight Cryptography for Security & Privacy (LightSec 2013), May 2013, Gebze, Turkey.

[C4] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "On the Need for Secure Distance-Bounding", Extended abstract, In Proceedings of the Early Symmetric Crypto (ESC 2013), Jan. 2013, Mondorf-les Bains, Luxembourg.

[C5] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Towards Secure Distance Bounding", In Proceedings of the 20th International Workshop on Fast Software Encryption (FSE 2013), March 2013, Singapour.

[C6*] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols - PRF-ness alone Does Not Stop the Frauds!", In *Proceedings of LATINCRYPT 2012, 2nd International Conference on Cryptology and Information Security in Latin America*, Santiago, Chile, Oct. 2012, pp. 100-120, LNCS 7533 Springer 2012.

[C7] A. Bay, I. Boureanu, A. Mitrokotsa, I. Spulber, S. Vaudenay, "The Bussard-Bagga and Other Distance Bounding Protocols under Man-in-the-Middle Attacks", In *Proceedings of Inscrypt'2012, 8th China International Conference on Information Security and Cryptology*, Nov. 2012, Beijing, China.

[C8] C. Dimitrakakis, A. Mitrokotsa, "Near-Optimal Node Blacklisting in Adversarial Networks", 2012 Conference on Decision and Game Theory for Security (GameSec 2012), Poster Session, Budapest, Hungary, Nov. 2012.

[C9] A. Mitrokotsa, C. Onete and S. Vaudenay, "Mafia Fraud Attack against the RC distance-Bounding Protocol", In *Proceedings of the 2012 IEEE RFID Technology and Applications (IEEE RFID T-A)*, Nov. 2012, Nice, France, pages 74-79, IEEE Press.

[C10] M. Safkhani, N. Bagheri, A. Mitrokotsa, P. Peris-Lopez, "On the Traceability of Tags in SUAP RFID Authentication Protocols", In *Proceedings of the 2012 IEEE RFID Technology and Applications (IEEE RFID T-A)*, Nov. 2012, Nice, France, pages 80-84, IEEE Press.

[C11] M. Safkhani, N. Bagheri, P. Peris-Lopez, A. Mitrokotsa, J.C. Hernandez-Castro, "Weaknesses in another Gen2-Based RFID Authentication Protocol", In *Proceedings of the 2012 IEEE RFID Technology and Applications (IEEE RFID T-A)*, Nov. 2012, Nice, France, pages 292-296, IEEE Press.

[C12] J.-P. Aumasson, A. Mitrokotsa, P. Peris-Lopez, "A Note on a Privacy-Preserving Distance Bounding Protocol", In *Proceedings of the 13th International Conference on Information and Communication Security (ICICS 2011)*, Nov., Beijng China. Springer Vol. 7043, pp. 78-92.

[C13] P. Darcy, B. Stantic, A. Mitrokotsa, A. Sattar, "Detecting Intrusions within RFID Systems through Non-Monotonic Reasoning Cleaning", In *Proceedings of the 6th International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, Dec. 2010, Brisbane, Australia.

[C14] C. Dimitrakakis and A. Mitrokotsa. "Statistical Decision Making for Authentication and Intrusion Detection", In *Proceedings of the 8th IEEE International Conference on Machine Learning and Applications (ICMLA 2009)*, Miami, FL, USA, Dec. 2009, pp. 409-414, IEEE Computer Society.

[C15] A. Mitrokotsa, M.R. Rieback, and A.S. Tanenbaum. "Classification of RFID Attacks". In *Proceedings of the 2nd International Workshop on RFID Technology - Concepts, Applications, Challenges (IWRT 2008), in conjunction 10th International Conference on Enterprise Information Systems*, pages 73–86, Barcelona, Spain, June 2008. INSTICC Press, Portugal.

[C16] A. Mitrokotsa, M. Tsagkaris, and C. Douligeris. "Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms". In *Proceedings of the Seventh Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2008) - Advances in Ad Hoc Networking*, Computer Science, pages 133–144, Palma de Mallorca, Spain, June 2008. Springer.

[C17] A. Mitrokotsa, C. Dimitrakakis, and C. Douligeris. "Intrusion Detection Using Cost-Sensitive Classification". In *Proceedings of the 3rd European Conference on Computer Network Defense (EC2ND 2007)*, LNEE, pages 35–46, Heraklion, Crete, Greece, Oct. 2007. Springer-Verlag.

[C18] A. Mitrokotsa, N. Komninos, and C. Douligeris. "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET". In *Proceedings of IEEE International Conference on Pervasive Services 2007 (ICPS 2007)*, pages 118–127, Instabul, Turkey, July 2007.

[C19] A. Mitrokotsa, N. Komninos, and C. Douligeris. "Towards an Effective Intrusion Response Engine Combined with Intrusion Detection in Ad Hoc Networks". In *Proceedings of the 6th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2007)*, pages 137–144, Corfu, Greece, June 2007.

[C20] A. Mitrokotsa, R. Mavropodi, and C. Douligeris. "Detecting Packet Dropping Attacks Using Emergent Self-Organizing Maps in Mobile Ad Hoc Networks". In *Proceedings of International Conference on Intelligent Systems and Computing: Theory and Applications*, pages 111–118, Ayia Napa, Cyprus, July 2006.

[C21] A. Mitrokotsa and C. Douligeris. "Intrusion Detection Using Emergent Self-Organizing Maps". In G. Antoniou et al., editor, *SETN 2006*, volume 3955 of *Lecture Notes in Artificial Intelligence*, pages 559–562, Heraklion, Greece, May 2006, Springer-Verlag.

Edited Books

[EB1] A. Mitrokotsa, S. Vaudenay, *Progress in Cryptology - Africacrypt 2012, Proceedings of the 5th International Conference on Cryptology in Africa*, Ifrane, Morocco, July 10-12, 2012, Lecture Notes in Computer Science, Vol. 7374.

[EB2] C. Dimitrakakis, A. Gkoulalas-Divanis, A. Mitrokotsa, V.S. Verykios, Y. Saygin, *Proceedings of the 1st International ECML/PKDD Workshop on Privacy and Security Issues in Data Mining and Machine Learning (PSDML 2010)*, Vol. 6549, Lecture Notes in Artificial Intelligence, Subseries of LNCS Springer.

[EB3] Q.Z. Sheng, A. Mitrokotsa, S. Zeadally, Z. Maamar, *Proceedings of the 4th International Workshop on RFID Technology - Concepts, Applications, Challenges IWRT 2010*, in conjunction with ICEIS 2010, Funchal, Madeira - Portugal, 8 - 12 June 2010, SciTePress Portugal, ISBN:978-989-8425-11-9.

[EB4] Q.Z. Sheng, A. Mitrokotsa, S. Zeadally, Z. Maamar, *Proceedings of the 3rd International Workshop on RFID Technology - Concepts, Applications, Challenges IWRT 2009*, in conjunction with ICEIS 2009, Milan, Italy, May 2009, INSTICC Press Portugal, ISBN: 978-989-8111-94-4.

Peer Reviewed Chapters in Books

[CB1] A. Mitrokotsa, M. Beye, P. Peris-Lopez, Chapter: "Threats to Networked RFID Systems". In Book: Unique Radio Innovation for the 21st Century: Building Scalable and Global RFID Networks. Eds. D. Ranasinghe, M. Sheng, S. Zeadally. Springer-Verlag., 2011, ISBN: 978-3-642-03461-9.

[CB2] A. Mitrokotsa and C. Douligeris. Chapter: "Integrated RFID and Sensor Networks: Architectures and Applications", In Book: *RFID and Sensor Networks: Architectures, Protocols, Security and Integrations*. Wireless Networks and Mobile Communication Series, pages 511–535. Auerbach Publications, CRC Press, Taylor and Francis Group, LLC 2010, ISBN: 978-1-4200-4288-7.

[CB3] A. Mitrokotsa and T. Karygiannis. Chapter: "Intrusion Detection Techniques in Sensor Networks", In Book: *Wireless Sensor Network Security*, pages 251–272. Cryptology and Information Security Series. IOS Press, 2008.

[CB4] A. Mitrokotsa and C. Douligeris. Chapter: "Denial of Service Attacks" In Book: *Network Security: Current Status and Future Directions*, pages 117–134. John Wiley and Sons. John Wiley and Sons, June 2007.

[CB5] A. Mitrokotsa and C. Douligeris. Chapter: "DoS Attacks and E-Government", In Book: *Secure eGovernment Web Services*, pages 124–142. Idea Group Publishing, Hershey PA, USA, 2007.

reprinted in:

Information Security and Ethics: Concepts, Methodologies, Tools, and Applications, Information Science Reference, 2008, IGI Global.

Thesis

[T1] A. Mitrokotsa. *Intrusion Detection in Computer Networks Using Machine Learning Algorithms*. PhD thesis, Department of Informatics, University of Piraeus, Greece, 2007.

Technical Reports

[R1] C. Dimitrakakis and A. Mitrokotsa, "Statistical Decision Making for Authentication and Intrusion Detection", *IAS Technical Report IAS-UVA-09-03*, April 2009.

[R2] C. Dimitrakakis, B. Nelson, A. Mitrokotsa and B. I.P. Rubinstein, "Robust, Secure and Private Bayesian Inference", *CoRR abs/1306.1066*, 2013.

[R3] I. Boureanu, A. Mitrokotsa and S. Vaudenay, "Practical & Provably Secure Distance-Bounding", *IACR Cryptology ePrint Archive 2013: 465 (2013)*.

Popular science articles - Other publications

[O1] A. Årnes, J. Aguado, E. Boschi, R. Benito Cortiñas, F. Gaudino, G. Hobgen, T. Karagiannis, A. Mitrokotsa, I. Naumann, P. Papadimitratos, M. Papadopouli, G. Roussos, and K. Tsakona, "Mobile Identity Management", *ENISA Position Paper*, 13 April 2010.

[O2] I. Askoxylakis, P. Belimpasakis, M. Broda, L. Buttyan, S. Gorniak, S. Hoemstra de Grot, S. Ioannidis, P. Kijewski, A. Merle, A. Mitrokotsa, A. Munro, O. Popov, C.W. Probst M. Rohr, L. Romano, C. Siaterlis, C. Vishik, S. Zanero, "Priorities of Research on Current & Emerging Network Technologies", *ENISA Position Paper*, 20 April 2010.

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-48128-116647-16

Name of applicant
Mitrokotsa, Aikaterini

Date of birth
781008-3662

Title of research programme

Appendix N

Budget and research resources

Vetenskapsrådet, Box 1035, SE-101 38 Stockholm, tel. +46 (0)8 546 44 000, vetenskapsradet@vr.se

Appendix N: Budget and Research resources

Aikaterini Mitrokotsa

1 Budget summary

With the current exchange rates and salary requirements at Chalmers, the project shall finance part of the salary for the PI as well as the salary for one PhD student. The PI will be employed at 25% on the project and will supervise the PhD student. The PhD student will be employed for 5 years at 80% on the project. The remaining 20% will be spent on teaching assistance and supervising master students. Furthermore, the budget covers the cost for 2 PC/laptops computers for the PhD student and one owned by the PI. The costs also include travel expenses for trips to conferences as well as the licentiate and disputation costs for the PhD student.

Year	2015	2016	2017	2018	2019	**Total**
Direct costs						
Salary Aikaterini Mitrokotsa	211	218	225	233	241	
Salary PhD Student	455	470	485	502	519	
Operating costs	93	93	88	74	124	473
Equipment	0	0	0	0	0	0
Premises	49	51	53	54	56	263
Total direct costs	808	831	851	863	940	4,293
Indirect costs	236	243	251	260	269	1,259
Total project costs	1,043	1,074	1,103	1,123	1,209	5,552

Table 1: Total project costs (SEK thousand)

2 Other research grants

The table 2 summarizes other available grants available at the moment. More precisely and EU grant where the PI is focusing on privacy-preserving biometric authentication and a STINT initiation research grant which funds research visits among the PI and the City University of Hong Kong.

Type of grant	**Applied or granted**	**Funding source**	**Grant holder/ Project leader**	**Grant period**	**Total amount in thousands**
Project research grant	Granted	EU BEAT: Biometric evaluation & testing	Aikaterini Mitrokotsa	2013-2016	894
Project research grant	Granted	STINT Initiation grant	Aikaterini Mitrokotsa	2014-2015	150

Table 2: Available grants

VETENSKAPSRÅDET
THE SWEDISH RESEARCH COUNCIL

Kod
2014-48128-116647-16

Dnr
2014 -

Name of applicant
Mitrokotsa, Aikaterini

Date of birth
781008-3662

Reg date
2014-04-09 16:35:14

Project title
PRECIS: Privacy and security in wearable computing devices

NT

NT-2, NT-14

Research grants NT April 9, 2014
Project Grant Junior Researchers
*Övrigt generellt
Chalmers tekniska högskola

Appendix S

Signatures

2015	2016	2017	2018	2019	
1043	1075	1103	1123	1209	2015-01-01 -- 2019-12-31

Applicant | **Date**

Head of department at host University | **Clarifi cation of signature** | **Telephone**

A signature on the application is required not only from the applicant but also from the authorised representative of the administrating organisation/institution or equivalent (normally the head of the department or establishment where the research is to be conducted). The signature confirms that the department can accommodate the proposed research, position or equipment; that the costing in the application is approved for the department's part, that any proposed experimentation on human or animal subjects has been reported, and that the applicant has reported any secondary occupations and commercial ties (s)he may have, and nothing inconsistent with good research practice has thereby emerged. The applicant must have discussed these conditions with the representative of the administrating organisation/institution or equivalent before the latter approves and signs the application.

NOTE the exceptions!
Please note that a different procedure applies for the following types of grants:

- Infrastructure- Operation Grants
- Infrastructure- Grants for Expensive Equipment
- Infrastructure- Grants for Large Databases
- Framework Grant SIMSAM
- International Recruitment

For these types of grants the vice-chancellor, instead of the head of department, must sign Appendix S. Thereby (s)he confirms the commitments of the administrative organization. The details are specified in the Call for Proposals, published at www.vr.se.

Vetenskapsrådets noteringar
Kod

2014-48128-116647-16

Vetenskapsrådet, Box 1035, SE-101 38 Stockholm, tel. +46 (0)8 546 44 000, vetenskapsradet@vr.se