Received 21 March 2016
Revised 21 March 2016
Accepted 4 April 2016

A decade of security research in ubiquitous computing: results of a systematic literature review

Ema Kusen and Mark Strembeck
Institute for Information Systems and New Media, Vienna University of Economics and Business (WU Vienna), Vienna, Austria

Abstract

Purpose – Ever since Mark Weiser coined the term "ubiquitous computing" (ubicomp) in 1988, there has been a general interest in proposing various solutions that would support his vision. However, attacks targeting devices and services of a ubicomp environment have demonstrated not only different privacy issues, but also a risk of endangering user's life (e.g. by modifying medical sensor readings). Thus, the aim of this paper is to provide a comprehensive overview of security challenges of ubicomp environments and the corresponding countermeasures proposed over the past decade.

Design/methodology/approach – The results of this paper are based on a literature review method originally used in evidence-based medicine called systematic literature review (SLR), which identifies, filters, classifies and summarizes the findings.

Findings – Starting from the bibliometric results that clearly show an increasing interest in the topic of ubicomp security worldwide, the findings reveal specific types of attacks and vulnerabilities that have motivated the research over the past decade. This review describes most commonly proposed countermeasures – context-aware access control and authentication mechanisms, cryptographic protocols that account for device's resource constraints, privacy-preserving mechanisms, and trust mechanisms for wireless *ad hoc* and sensor networks.

Originality/value – To the best of our knowledge, this is the first SLR on security challenges in ubicomp. The findings should serve as a reference to an extensive list of scientific contributions, as well as a guiding point for the researchers' novel to the security research in ubicomp.

Keywords Security, Ubiquitous computing

Paper type General review

1. Introduction

Ever since the invention of the first computer, the computing paradigm has been constantly evolving and has gone through significant changes over the past decades – progressing from Microsoft's slogan *a computer on every desk* to a *multiple devices per user* paradigm. In recent years, this has led to the development of standards and technologies for wireless communication such as wireless local area network (WLAN), long-term evolution (LTE), radio-frequency identification (RFID), near field communication (NFC), as well as all types of mobile, wearable and embedded devices (Dragoni *et al.*, 2009; Pietro and Mancini, 2003; Yau *et al.*, 2006; Zhu *et al.*, 2006a). As a result, the vision of ubiquitous computing (ubicomp) (Weiser, 1991) is about to become reality. Commercially available devices such as smartphones, tablets or smart watches, as well as research prototypes such as smart glasses, smart contact lenses or smart implantable medical devices, provide an omnipresent access to different types of information. However, together with the emergence of new technologies and devices, a number of novel security challenges arise. In ubicomp, security is particularly

International Journal of Pervasive Computing and Communications
Vol. 12 No. 2, 2016
pp. 216-259

1742-7371
DOI 10.1108/IJPCC-03-2016-0018

important because today more people than ever before are using software-based devices as part of their everyday life. Contemporary mobile devices are used for private and for professional communication and host a wide variety of sensitive information, ranging from private text messages or photos, over financial information managed by homebanking apps, to company-internal business secrets that a company's employees access with mobile devices.

1.1 State of the art

The heterogeneous nature of today's computing devices accompanied by corresponding services, applications and user interactions result in novel requirements for designing security mechanisms for protecting ubicomp environments. Some of those requirements are inherited from traditional (stationary) distributed systems and include security goals, such as access control, authentication, data integrity and availability of services, to name a few (Bacon and Moody, 2002). However, the scientific contributions analyzed and presented in this paper highlight the need to adapt traditional security mechanisms to the specific characteristics of ubiquitous computing.

For example, a considerable number of studies have argued that traditional access control and authentication mechanisms are not suitable for the dynamic and mobile nature of a ubicomp environments because of their non-adaptivity to context (Corradi *et al.*, 2004; Hengartner and Steenkiste, 2005; Wang *et al.*, 2008). Among other things, this paper reports on the analysis of the authentication mechanisms proposed in the scientific literature. As expected, biometric techniques evolved significantly over the past decade, proposing mobility patterns and other behavioral characteristics in addition to physiological characteristics such as fingerprint and retina scans. In terms of access control mechanisms, various extensions to role-based access control (RBAC) have been proposed which integrate contextual information into standard RBAC models (see Section 3.3).

In addition to adapting to the device's context, security mechanisms for ubicomp environments face another challenge. In particular, computing devices participating in a ubicomp environment, such as small sensor-enhanced handheld devices, are limited with respect to their computing power, storage and communication range (Cheng *et al.*, 2008; Tan, 2012; Want, 2014), which leads to difficulties in designing security mechanisms that rely on complex computations (Lam *et al.*, 2003; Qiu *et al.*, 2013). Therefore, when designing novel security means for such devices, the focus is often put on lightweight solutions which balance between the strength of the respective security mechanism and the computation overhead. More closely, this paper examines cryptographic protocols and identifies the ones described by their authors as "lightweight" to find out which cryptographic algorithms have been favored over the past decade by the research community.

Apart from the computation overhead, another security-related challenge arises from an *ad hoc* nature of interactions between mobile nodes that have no prior knowledge of each other's behavior or intention. Over the past years, in addition to risk assessment, the human notion of trust has been recognized as an important factor in designing secure ubiquitous environments (Ahamed *et al.*, 2008). As a part of our review, information about different approaches to trust computation has been extracted and mapped to the corresponding phase in a trust lifecycle.

Furthermore, while using ubiquitous services, various threats to user privacy arise (Ren *et al.*, 2006) that are novel to ubiquitous computing, such as tracking and recording

a user's whereabouts without his/her consent or notification. To mitigate these threats, several privacy-preserving mechanisms have been proposed over the past decade that generally rely on hiding and progressively revealing parts of information, storing data in a distributed manner, as well as other techniques (see also Section 3.3).

Our initial search procedure resulted in as many as 12,705 papers on security in ubicomp. By applying a number of carefully selected inclusion criteria and quality assessments, 282 quality papers were systematically included in our review and each was manually analyzed in detail over the course of two years. The information extracted revealed a number of threats, vulnerabilities and attacks that arise in ubicomp and that are reported in this paper. Moreover, a closer look is taken on the related security mechanisms along with their corresponding properties that were adapted for context-awareness and the dynamics of ubicomp environments. This paper also reflects and discusses about the differences related to security goals of distributed computing in general and ubicomp by analyzing the relationship between both computing paradigms.

Apart from our review, security-related topics have also been addressed in other systematic review papers. Nguyen *et al.* (2013) review approaches for model-driven security engineering. A review of security in process-aware information systems is reported by Leitner and Rinderle-Ma (2014). Alemán *et al.* (2013) give an overview of security and privacy for electronic health records. The goal of achieving a secure software system in a software development process has been addressed in the study by Mellado *et al.*, 2010. However, to the best of our knowledge, no systematic study exists that provides an extensive review of the security challenges in ubicomp.

1.2 Contribution

The objective of this systematic literature review (SLR) is to identify the existing body of knowledge, and to analyze the relevant literature that addresses security-related research in ubicomp. The review contributes to the body of knowledge in the field of security in ubicomp in four ways:

(1) by reviewing security threats, vulnerabilities and attacks as the main motivating factors for research;

(2) by summarizing the countermeasures proposed in the papers;

(3) by comparing security goals of ubicomp with those in distributed systems in general; and

(4) by identifying directions for future research.

The remainder of this review is structured as follows. Section 2 describes the method of the SLR. Results are presented in Section 3. In Section 4, a discussion on the results and validity threats is provided. Section 5 concludes the paper and discusses future work.

2. Research method

The results of this review are obtained by carefully following the guidelines (Kitchenham and Charters, 2007) for an SLR, as well as the examples of other SLR papers (Afzal *et al.*, 2009; Leitner and Rinderle-Ma, 2014; Mellado *et al.*, 2010; Nguyen *et al.*, 2013; Radjenović *et al.*, 2013). Typically, an SLR consists of three main phases: planning a review, conducting a review and reporting a review.

In the first phase and as recommended for SLRs (Kitchenham and Charters, 2007), an SLR research protocol[1] was designed to document the procedures used to conduct our SLR. The following details have been included in the protocol: research questions, search strategy, paper selection criteria, quality assessment, data extraction and data synthesis procedures. The systematic review was conducted in the second phase, based on the steps defined in the protocol. The third and final phase encompassed aggregation and elaboration of the collected data. Overall, the SLR has proven to be a lengthy process (it began in December 2013 and was completed in January 2016).

2.1 Search strategy

To provide a comprehensive overview of security-related topics in ubicomp, three main research questions and their corresponding refinements were used to guide the review, as shown below:

RQ1. Demographic data and trends. Identify active researchers (countries) and the distribution of papers over years.

RQ2. Which security-related topics have been addressed in ubicomp research papers?

RQ2.1. Which security issues have been reported on? Identify vulnerabilities, threats and attacks that motivated the research.

RQ2.2. Which countermeasures have been presented? Identify techniques, algorithms and methods proposed to address security-related issues.

RQ2.3. Which security goals have been addressed in the papers?

RQ3. Is there a difference in addressing security in distributed systems in general in comparison to ubiquitous computing? Investigate and determine which security requirements are novel to ubicomp.

Prior to conducting the search for papers, the list of keywords was carefully chosen by following two procedures:

(1) select general and well-established terms including "pervasive computing" and "ubiquitous computing", as well as a list of typical security goals for software-based systems (Strembeck and Rinderle-Ma, 2013); and

(2) to ensure consistency in the terminology used, examine the keywords commonly used in the research community by manually screening through abstracts, keywords and titles of papers published in four well-accepted publication venues for ubicomp research[2].

The final list of keywords was created as a union of the keywords found in both procedures and includes the following:

- *a list related to ubiquitous computing (T1)*: Ubiquitous, pervasive computing, wearable, body area network, mobile computing, context-aware and context-sensitive; and
- *a list related to security (T2)*: Security, confidentiality, authentication, access control, non-repudiation, audit, integrity, authenticity of data, availability, privacy and trust.

Based on the identified key terms, the search string was built in the following way:

$$(T1_1 \vee T1_2 \vee \ldots \vee T1_n) \wedge (T2_1 \vee T2_2 \vee \ldots \vee T2_n) \quad \textit{where}$$
$$T1_{1\ldots n} \in T1 \wedge T2_{1\ldots n} \in T2$$

Because of the specific limitations of each search engine, our SLR was conducted by using in total seven search strings (Table I). The search was conducted over five scientific databases. In specific, Science Direct, IEEEXplore, ACM Digital Library, Wiley Digital Library and Springer Link. During the search and collection process, we used Mendeley reference manager[3] to automatically collect general information about the papers (in total 12,705), such as abstracts, authors, publication venue, publication year and a link to the corresponding source.

2.2 Paper selection

The papers were carefully filtered by following the inclusion and exclusion criteria (EC).

2.2.1 Exclusion criteria. Following are the EC:

- summaries of workshops and tutorials, title pages, editorials and extended abstracts, as they do not provide sufficient information with respect to the objective of our SLR;
- workshop papers, as they report on early stages of a research endeavor;
- posters, as they do not provide enough information for the purpose of this review;
- double entries. If an extended journal paper was found, it was chosen over the conference paper. If a more recent paper was found, it was chosen over its preceding paper;
- papers whose focus was not put on security in ubicomp, i.e. papers that only mention security in their abstracts as one of the issues;
- pure opinion and discussion papers that do not propose a countermeasure or demonstrate a security threat;

String	Form
S1	(ubiquitous *OR* "pervasive computing" *OR* "mobile computing" *OR* wearable *OR* "body area network") *AND* (security *OR* confidentiality *OR* "access control" *OR* authentication)
S2	(ubiquitous *OR* "pervasive computing" *OR* "mobile computing" *OR* wearable *OR* "body area network") *AND* (privacy *OR* integrity *OR* "authenticity of data" *OR* availability)
S3	(ubiquitous *OR* "pervasive computing" *OR* "mobile computing" *OR* wearable *OR* "body area network") *AND* ("non-repudiation" *OR* audit *OR* accountability)
S4	(ubiquitous *OR* "pervasive computing" *OR* "mobile computing" *OR* wearable *OR* "body area network") *AND* (trust)
S5	("context-aware" *OR* "context-sensitive") *AND* (security *OR* confidentiality *OR* "access control" *OR* authentication)
S6	("context-aware" *OR* "context-sensitive") *AND* (privacy *OR* integrity *OR* "authenticity of data" *OR* availability)
S7	("context-aware" *OR* "context-sensitive") *AND* ("non-repudiation" *OR* audit *OR* accountability *OR* trust)

Table I.
Search strings

- any paper whose full text is not accessible;
- any paper that is not written in English; and
- papers published before 2003[4].

Starting from 12,705 initial papers and after applying the above-mentioned EC, the pool included 2,426 potentially relevant papers. Therefore, two additional criteria were introduced to keep the selection process manageable:

(1) papers published in journals with a Scimago Journal Ranking [5] where h-index $\geq$ 35 or SJR $\geq$ 0.8; and

(2) papers published in conference proceedings with a rank A+ or A based on Computer Science Conference Rankings[6].

The latter criterion was also used in other literature studies (Webster and Watson, 2002) where it was indicated that researchers should examine conference proceedings with a reputation for quality.

Figure 1 summarizes the number of papers after applying each exclusion criterion.

It is important to note that both authors participated in the selection process to minimize personal bias, as recommended by García-Borgoñóna *et al.* (2013), Kitchenham and Brereton (2013) and Radjenović *et al.* (2013).

2.3 Quality assessment

After identifying the potentially relevant papers, a quality assessment was conducted based on the suggestions in the studies by Afzal *et al.* (2009), Dybå and Dingsøyr (2008), García-Borgoñóna *et al.* (2013), Kitchenham and Brereton (2013) and Santiago *et al.* (2012)). In particular, our quality assessment consisted of seven questions and a corresponding three-point answer scale with *Yes* (1), *No* (0) and *To some extent* (0.5) as possible answers, as shown below:

- Is the paper based on research?
- Is there a clear statement of the aim?
- Is there an adequate description of the context in which the research was carried out?
- Does the paper review the related research of the topic?

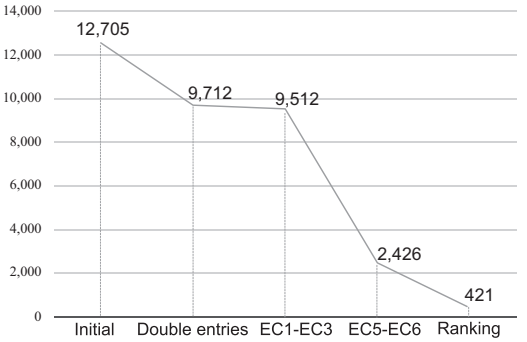


Figure 1.
Number of papers resulting after each stage of applying EC

- Is the research method described adequately?
- Is there a clear statement of the findings?
- Does the paper discuss future work?

Following the examples of other systematic reviews (Mahdavi-Hezavehi *et al.*, 2013; Radjenović *et al.*, 2013), the papers placed in the *poor quality* category were excluded from our review.

After applying all the EC, performing the quality assessment and obtaining full versions of papers (EC7), the final number of papers was reduced to 282. Our findings are based on those papers[7].

3. Results and synthesis of the findings

3.1 RQ1 – *demographic data and trends*

Our first findings reveal that the topic of security in ubicomp has been researched worldwide, with the most contributions coming from the USA, followed by China, UK, South Korea and Canada (Figure 2(a)). Moreover, over the time span between 2003 and 2015, there has been an increasing interest in ubicomp security. The coefficient of determination ($R^2 = 0.783$) indicates that there is a noticeable trend in the amount of papers published per year.

In the subsequent sections, the most frequent security issues that have motivated the papers analyzed, as well as the corresponding countermeasures will be classified, summarized and discussed.

3.2 RQ2.1 – *motivation for the research*

Mobile and ubiquitous computing devices, dynamically changing context and a large number of heterogeneous devices participating in the environment are exposed to a variety of security-related threats. For example, threats to user's privacy, service and infrastructure availability, data integrity and the user's well-being have been repeatedly identified in the corresponding scientific literature. On the one hand, the use of malicious services or apps, presence of untrustworthy nodes in the underlying network or attacks (such as impersonation or eavesdropping) may lead to leaking of user's private information. On the other hand, trusted services may become available to users with forged or untrustworthy identities (Wang *et al.* 2013). To preserve their anonymity,

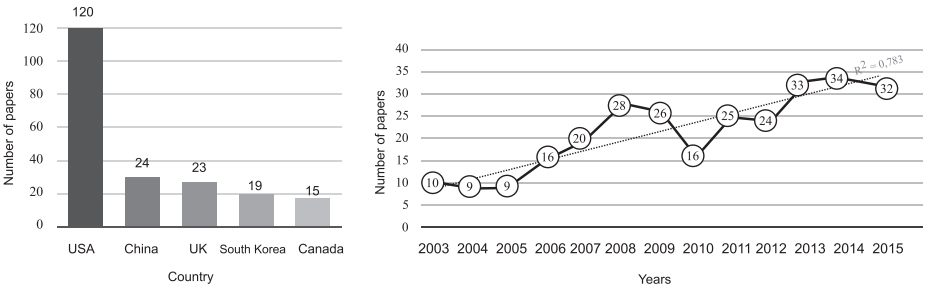


Figure 2.
Distribution of publications over years

Notes: (a) Countries with most published papers; (b) distribution of papers over the last decade

users typically prefer accessing to services without having to disclose confidential information. However, often some portion of a user's private information is needed for authentication to services. Thus, privacy may be in *conflict* with some security goals. In the remainder of this section, we report on the threats, vulnerabilities and attacks that were identified in our SLR.

The results indicate that the security-related research in ubicomp was motivated by five main categories of security-related issues (Figure 3).

3.2.1 Attacks. The findings of our SLR show that various attacks have predominantly been recognized as a security challenge in ubicomp over the past decade, covering 46 per cent of all motivating factors for security-related research in ubicomp. To further examine the nature of these attacks, each attack identified in the reviewed papers (in total 364 attacks) has been categorized into the eight categories shown in Figure 4(a). Our data analysis revealed that the most frequently addressed attacks are different types of *Denial of Service (DoS)* attacks (28 per cent) that aim at making services or resources unavailable to its intended users. In a ubicomp environment, DoS attacks especially include power-draining, network jamming, denial of proof and on–off attacks. The second most commonly addressed group of attacks (21 per cent) belongs to *impersonation attacks* in which an adversary masquerades as a trusted party. The results of our SLR indicate that 38.5 per cent of the impersonation attacks are man-in-the-middle attacks, 27 per cent are different types of spoofing, 17 per cent are Sybil attacks, 5 per cent are phishing attacks and 3 per cent are relay attacks. *Eavesdropping attacks* are the third most commonly addressed attacks and cover 17.5 per cent of attacks, whereby 37.5 per cent of the eavesdropping attacks are passive attacks, such as monitoring or spying on a communication between trusted parties. One of such attacks is the so-called shoulder surfing attack (33 per cent of passive attacks) that refers to observing the content on a screen of a mobile device behind a user's shoulder. Nevertheless, the majority of eavesdropping attacks (67 per cent) are active attacks which assume that an adversary somehow interferes with the communication channel between a sender and a receiver. The category *Other*, which covers 10.5 per cent of the attacks, includes diverse attacks such as RFID cloning attacks, physically stealing a mobile device, session hijacking and modifying patient's sensor readings, to name a

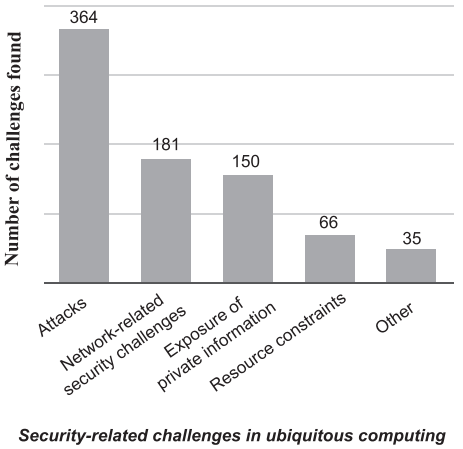
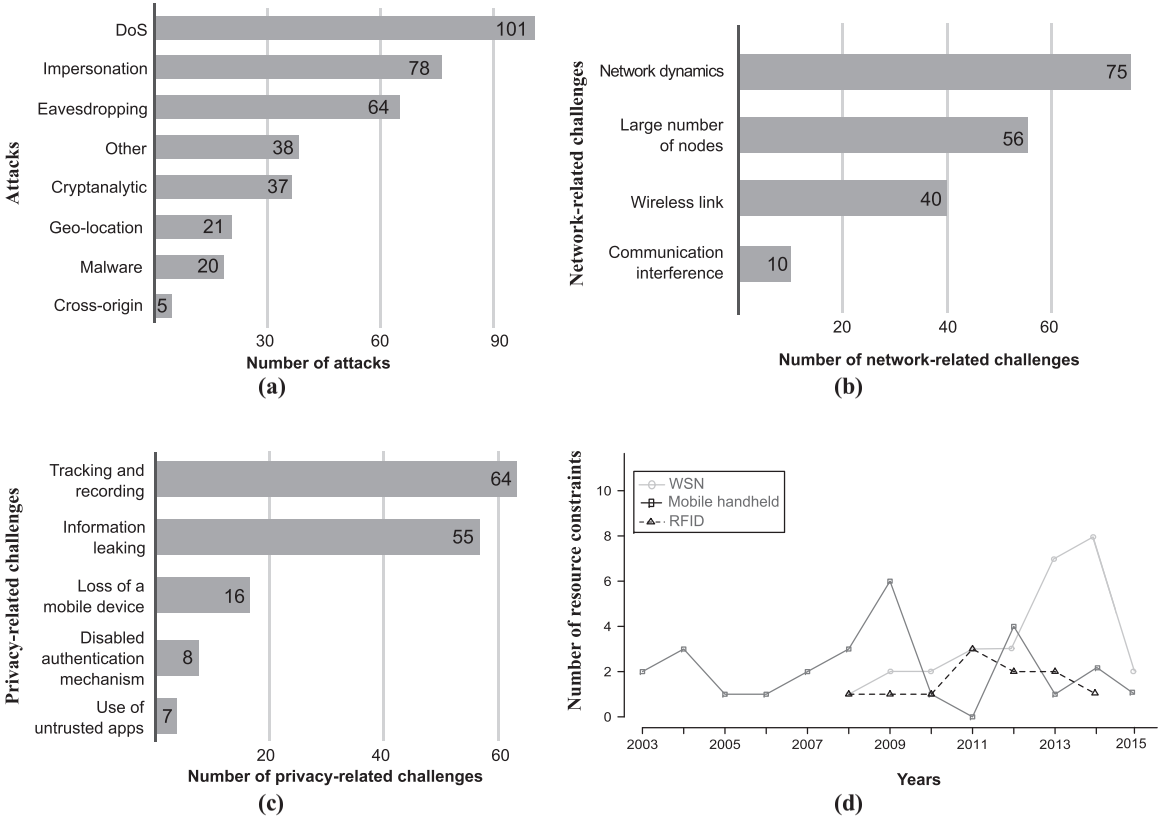


Figure 3.
Security challenges that have motivated papers

Figure 4.
Security challenges related to attacks, network security, privacy and resource constraints



Notes: (a) Attacks; (b) network-related security challenges; (c) exposure of private information; (d) resource constraints

few. The final four categories include *cryptanalytic attacks* (10 per cent of attacks) which include password guessing, acoustic cryptanalysis and electromagnetic attacks; *geo-location attacks* (6 per cent of attacks), which include tracking user's whereabouts and location inference attacks and *malware* (5.5 per cent of attacks). The least number of attacks belong to cross-origin attacks (1.5 per cent), which include confused deputy and cross-site request forgery attacks.

3.2.2 Network-related security challenges. Network-related security challenges cover 23 per cent of all challenges identified in the papers. As shown in Figure 4(b), the most commonly addressed issue in this group refers to *network dynamics* (41 per cent). In general, networks for ubicomp environments, such as mobile *ad hoc* networks (MANET), wireless sensor networks (WSN) and wireless body area networks (WSN), differ from traditional networks. In contrast to more traditional distributed systems, the devices in a ubicomp environment are usually mobile and they can join or leave the network dynamically. For example, a mobile device intentionally leaves the network when its user enters an aircraft and it intentionally rejoins the same or another network after arriving at the aircraft's destination. Moreover, the behaviors or intentions of those highly mobile devices are initially unknown to other mobile devices and to devices providing the ubicomp infrastructure. Thus, such networks often do not have a fixed topology, central authorities or globally trusted third parties (Zhang *et al.*, 2003). Among other things, the resulting *ad hoc* nature of interaction poses challenges for administrating trust relationships between the different, dynamically changing nodes. Furthermore, because of the *large number of nodes* participating in the network, issues occur when a malicious node joins the network, addressed in 31 per cent of the papers. These issues include detection of a compromised node (Boukerche and Ren, 2008) and a potential collapse of the whole network (Ahamed *et al.*, 2009). Another network-related challenge refers to the wireless communication services (22 per cent) that, unlike wired networks, use radio waves for data transmission and are vulnerable to a number of different attacks. To a lesser amount, the reviewed papers have identified communication interference (6 per cent) as an additional challenge to network security.

3.2.3 Exposure of private information. Privacy-related issues have been addressed as the third most common security-related challenge in ubicomp, covering 19 per cent of all challenges identified. As shown in Figure 4(c), *user-tracking and recording* have been addressed in a majority of the papers (43 per cent) on privacy-related issues. In particular, related issues include attaining the current geographical coordinates of a user or recording a user without his/her consent or notification. Apart from location data, leaking other private information (37 per cent) has been the second most commonly addressed privacy issue and refers to *leaking* of medical and fitness data, sensitive ambient information, and other confidential information, such as phone-call history or images stored on a mobile device. Apart from various attacks on the user's device and using malicious services, privacy leaks and misuse of user's data may also result from a *physical loss of a mobile device*, which has been recognized as the third category addressed in 10.5 per cent of the papers on privacy-related issues. This category encompasses leaving a mobile device behind or having it stolen[8]. As a threat to user's data stored on a mobile device, *disabled or weak authentication mechanisms* have been addressed in 5 per cent of the papers, which discuss the design of authentication mechanisms for devices that frequently change their contexts, weaknesses of currently existing passwords and other locking mechanisms, as well as the misuse of users' oily

residues (touchscreen smudges) by adversaries. The final privacy-related challenge refers to a *poor selection of apps* that request permissions to and collect information about a user (4.5 per cent).

3.2.4 Resource constraints. Limited battery capacity and the (comparatively) low computing power of mobile devices, sensor network motes (sensor nodes), as well as RFID-based systems have been identified in 8 per cent of all the security challenges found in our review. As shown in Figure 4(d), limited resources of smartphones, PDAs and wearable devices (such as smart glasses or fitness trackers) have been recognized as an important issue while designing corresponding security mechanisms. Although the findings from our SLR do not clearly show a trend in addressing resource constraints in mobile devices as a potential security-related issue, many papers recognize that resource constraints of the mobile devices have not kept up with energy requirements demanded in the security-related research. These findings are also backed up by other studies (Islam and Want, 2014; Coughlin, 2015). As shown in Figure 4(d), the number of papers on resource constraints found in WSNs increased over the past decade. To a lesser amount, our SLR has identified a few papers addressing resource constraints found in RFID-based systems.

3.2.5 Other. In total, 4 per cent of the papers further address other vulnerabilities and threats, such as harming a patient by modifying sensor readings of medical wearable devices, various bluetooth vulnerabilities, absence of a tamper resistant hardware, as well as the definition of complex and context-dependent security policies.

3.3 RQ2.2 – *countermeasures presented in the papers*

Over the past decade, numerous security countermeasures and defense mechanisms have been proposed in the papers analyzed. In this SLR, they are grouped into five main categories: access control and authentication mechanisms; privacy-preserving mechanisms; cryptographic protocols; trust computation and management; and other (Figure 5).

3.3.1 Access control and authentication mechanisms. In total, 31.5 per cent of the papers reviewed propose *access control and authentication mechanisms*. Our findings show that passwords are the most commonly used *authentication mechanism* proposed in the papers on security-related research in ubicomp (reported in 21 papers), followed by tokens (17), such as wearable devices, smart cards and RFID badges; and biometrics (13), which includes palmprint, fingerprint, iris and face recognition, as well as recognition of user's behavioral traits, such as walking patterns, pen strokes, gestures and mobility patterns (Figure 6 and Table II). The fourth category, Other (8), includes context-based authentication (Al-Muhtadi *et al.*, 2003), proximity-based authentication (Chen *et al.*, 2008; Mayrhofer *et al.*, 2007; Rasmussen *et al.*, 2009), USIM (Park *et al.*, 2010), trust-based tickets (El Husseini *et al.*, 2013; Luo *et al.*, 2004) and the use of sensor data (accelerometer) (Mayrhofer *et al.*, 2013; Park *et al.*, 2010).

The sum of unique papers on authentication mechanisms for each year (Table II) reveals that there is an incline in the number of authentication mechanisms proposed over the past decade. Moreover, as depicted in Figure 6, there is a noticeable tendency in adopting authentication mechanisms to the unprecedented characteristics of ubicomp, namely, context-awareness and context dynamics, reflected in different types of biometrics proposed in the literature. Even though biometrics have been present throughout the entire time period covered by our SLR, the years from 2012 to 2015

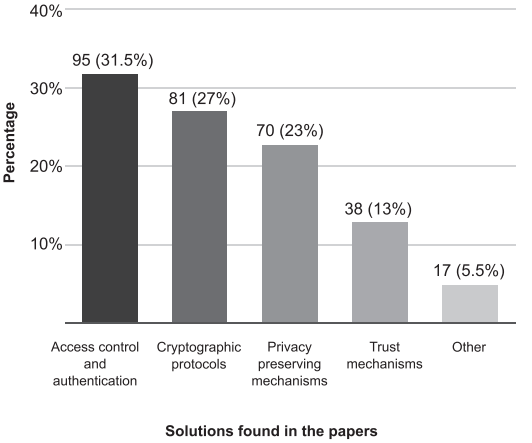


Figure 5. Countermeasure presented in the papers reviewed

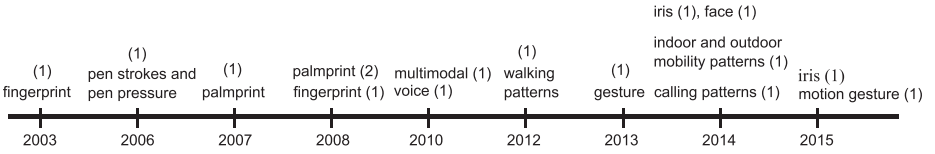


Figure 6. Biometrics in authentication mechanisms

especially resulted in novel biometric features that go beyond fingerprints, voice recognition, pen pressures and palmprints and take into account other behavioral patterns (such as walking patterns, gestures, calling patterns, as well as indoor and outdoor mobility).

Moreover, our findings reveal that eight authentication mechanisms identified in our SLR propose multimodal authentication, whereby the most common combination of authentication mechanisms is a *credentials–token* pair (proposed in four papers) and *credentials–biometrics* pair (proposed in three papers), which refers to the use of fingerprint, palmprint and voice recognition combined with username-password pairs as a complementary security measurement.

Over the past decade, different types of contextual information have been integrated with traditional *access control models*, especially by introducing dynamic attributes, such as time and location, in addition to the static ones (identity and role). The countermeasures proposed in the respective papers are mainly focused on RBAC, access control lists (ACL) and mandatory access control (MAC). In total, eight papers report on context-related extensions of RBAC models (Table III) by introducing contextual constraints such as location (eight papers) and time (five papers). Such spatial and temporal information can be generally obtained by special purpose sensors, such as GPS sensors, or derived from other data sources, such as time retrieved from a system clock or a device's IP address requested from the corresponding network subsystem. While a majority of countermeasures proposed relies on the latter, Damiani *et al.* (2007) and Oh (2008) suggest the use of sensor information, such as GPS coordinates, to locate a user or sensor readings providing the state of a machine, e.g. a milling machine will operate only if materials are correctly placed on the milling machine. Apart from spatial and temporal constraints, other contextual information has also been incorporated within the

Table II.
Summary of authentication mechanisms

Year	Username/password	Token	Biometrics	Other	# unique
2003	Al-Muhtadi *et al.* (2003)	Al-Muhtadi *et al.* (2003)	Al-Muhtadi *et al.* (2003)	Al-Muhtadi *et al.* (2003)	1
2004				Luo *et al.* (2004)	1
2006	Ren *et al.* (2006)	Nicholson *et al.* (2006), Zhu *et al.* (2006a)	Dozono *et al.* (2006)		4
2007	Byun *et al.* (2007)		Leung *et al.* (2007)	Mayrhofer *et al.* (2007)	3
2008	Chen *et al.* (2008), Lei *et al.* (2008)	Jabbar (2008), Kang *et al.* (2008), Sun *et al.* (2008a)	Chen *et al.* (2008), Liang *et al.* (2008)	Chen *et al.* (2008)	6
2009	Aboudagga *et al.* (2009), Kindberg *et al.* (2009), Rasmussen *et al.* (2009)	Rasmussen *et al.* (2009)		Rasmussen *et al.* (2009)	3
2010	Park *et al.* (2010), Yoon *et al.* (2010)		Park *et al.* (2010)	Park *et al.* (2010)	2
2011	Barisch (2011), Wang *et al.* (2011)	Kim *et al.* (2011), Moon and Lee (2011), Saxena *et al.* (2011), Wang *et al.* (2011)			5
2012	Drira *et al.* (2012), Moessner and Khan (2012), Tan (2012)		Casale *et al.* (2012)		4
2013	Chen *et al.* (2013)	Agudo *et al.* (2013), Ferdous and Poet (2013), Li *et al.* (2013a, 2013b), Mayrhofer *et al.* (2013)	Shahzad *et al.* (2013)	El Husseini *et al.* (2013), Mayrhofer *et al.* (2013)	7
2014	Hsieh and Leu (2014), Kwon and Na (2014), Schneegass *et al.* (2014), Wang and Wang (2014)	Wang and Wang (2014)	Buthpitiya *et al.* (2014), De Marsico *et al.* (2014)		6
2015	Mayer and Volkamer (2015)	Mayer and Volkamer (2015)	Ahmed *et al.* (2015), Barra *et al.* (2015), Mayer and Volkamer (2015)		3
Σ	21	17	13	8	

Paper	Contextual constraint Spatial	Temporal	Other
Compagnoni *et al.* (2008)	✓		
Damiani *et al.* (2007)	✓		
Fu and Xu (2005)	✓	✓	
López *et al.* (2007)	✓		✓
Oh (2008)	✓	✓	✓
Preda *et al.* (2011)	✓	✓	✓
Rohrer *et al.* (2013)	✓	✓	✓
Toahchoodee and Ray (2011)	✓	✓	✓
Σ	8	5	5

Table III. Summary of RBAC constraints

standard RBAC model. For example, López *et al.* (2007) propose the use of policies to assign roles to users switching between different domains. Preda *et al.* (2011) suggest that the spatial context of a device does not only include information about the location of a user, but also other context-related information, such as the number of people in a room based on the count of people leaving or entering through the door. Rohrer *et al.* (2013) and Toahchoodee and Ray (2011) propose similar approaches to handling role delegation based on an event or a circumstance. Both approaches suggest the notion of so-called shared rules to account for a temporary allowance of privileges, e.g. a doctor may temporarily allow a nurse to use an application (Rohrer *et al.*, 2013).

In total, four papers propose a different approach to RBAC models, which do not directly associate permissions to specific roles (Corradi *et al.*, 2004; Le *et al.*, 2010; Ning *et al.*, 2015; Wang *et al.*, 2008). In particular, Le *et al.* (2010) report on an activity-based access control mechanisms, which grants access rights based on activities assigned to a user instead of their roles. In the study by Corradi *et al.* (2004), permissions are directly associated with different kinds of context information, such as location boundaries in which resources can be accessed and logical contexts which describe resource availability and status. Another approach based on permissions that is directly associated to location is presented in the study by Wang *et al.* (2008). The approach assumes that users are registered at a central administrator and use their accounts to access a space for which a list of rights is defined. In the study by Ning *et al.* (2015), entities can only access data that are within their permission hierarchy.

The use of ACLs in a ubicomp context has been proposed by Minami and Kotz (2005) and Zachary and Brooks (2003). Minami and Kotz (2005) use rules and facts to define ACLs based on confidentiality policies that are used to assign trust levels to principals. To reduce the administrative work while defining policies, principals may refer to the policies of other principals. In the study by Zachary and Brooks (2003), ACLs are used by a software provider to map mobile code packages to an appropriate security level which determines whether a user is to be granted access to a mobile code package.

One paper proposes a MAC approach (Weippl and Essmayr, 2003) which supports three identification modes (anonymous, masqueraded and identified) between a service provider (grants access to a service based on a user's mode) and a user requesting a service. Based on the combination of identification modes, security-related precautions are pre-determined to preserve user's privacy. For example, if a service provider offers services to anonymous users and an anonymous user requests a service, there will be no

precautions taken. However, if a user with the same mode requests a service from a provider that requires a verified identity token for granting access, disguising techniques, such as onion routing, are suggested to preserve the user's location privacy.

Two papers suggest device-pairing mechanisms based on proximity and radio frequency that utilize wearable devices to grant access rights to a service, information or a physical location (Agudo *et al.*, 2013; Rasmussen *et al.*, 2009). A continuous authentication and access control mechanism for implantable medical devices, such as pacemakers, drug delivery systems and neurostimulators, has been proposed in the study by Rasmussen *et al.*, (2009), which is based on an ultrasonic distance-bounding protocol to enable implanted medical devices to grant access to other devices in its proximity. Another continuous authentication scheme (Agudo *et al.*, 2013) assumes that wearable devices have pre-established security associations with the authentication server. To avoid the direct link between the server and wearable devices and to mitigate a threat of compromising zone keys, authentication is carried out with the help of an intermediate device that detects wearable devices nearby and communicates with the server over an SSL channel. A similar approach to proximity-based access control is proposed by Hengartner and Steenkiste (2005). It allows a user to access the information about another user only if the requesting user is at one of the locations listed in the corresponding location policy. These location policies may further contain a time interval in which access is granted.

3.3.2 Cryptographic protocols. Cryptographic protocols have been proposed in 27 per cent of the papers. Our analysis of cryptographic algorithms uses the categories proposed by Kaps *et al.* (2007), which distinguish between symmetric-key algorithms/protocols, asymmetric-key algorithms/protocols and approaches based on hash functions. In recent years, demonstrating the feasibility of using strong cryptography on small and resource-constrained devices has become an important research topic. Several papers have addressed the resource usage of complex cryptographic techniques on resource-constrained devices (Jang *et al.*, 2011; Burmester *et al.*, 2009). In particular, the trade-off between security, cost and performance must be considered when designing lightweight protocols (Eisenbarth *et al.*, 2007). This class of protocols has been proposed over the past years to target wireless mobile devices with constrained resources and low capabilities, such as processing power and battery, and operate under low-bandwidth and error-prone wireless links (Chien, 2007; Lee *et al.*, 2011). In addition to pure symmetric-key and asymmetric-key algorithms, several studies have proposed a hybrid solution which is based on combining symmetric and asymmetric algorithms to reduce the computation overhead (Jang *et al.*, 2011; Mihovska and Prasad, 2007). Table IV summarizes the different approaches found in the papers reviewed.

The results depicted in Figure 7 indicate that asymmetric cryptography has been the most frequently proposed variant, out of which 25 per cent describe their protocol as lightweight. The second and third most frequently addressed algorithms belong to symmetric-key cryptography and hybrid cryptography. Table V summarizes different encryption algorithms reported in the papers analyzed. The least amount of papers present approaches that are based on hash functions only (9 per cent).

3.3.3 Privacy-preserving mechanisms. In total, 23 per cent of the papers analyzed in our SLR propose privacy-preserving mechanisms can be grouped into four categories (Table VI). The most commonly suggested privacy-preserving mechanism is hiding

Cryptographic algorithm	Papers	No.
Asymmetric-key	Beaufour and Bonnet (2004), Chen *et al.* (2008, 2013), Chuchaisri and Newman (2012), Dolev *et al.* (2015), El Husseini *et al.* (2013), He *et al.* (2007), He and Zeadally (2015), Hengartner and Steenkiste (2006), Huang *et al.* (2009a, 2009b), Hsieh and Leu (2014), Hu *et al.* (2013), Liu *et al.* (2013, 2014), Ning *et al.* (2015), Patwardhan *et al.* (2005), Rahman *et al.* (2014), Shi *et al.* (2011), Studer *et al.* (2011), Su *et al.* (2012), Sun *et al.* (2015), Undercoffer *et al.* (2003), Wang and Fang (2007), Wang *et al.* (2011), Xu *et al.* (2015), Yao *et al.* (2014), Yoon *et al.* (2010)	28
Symmetric-key	Abd-Alhameed *et al.* (2014), Ahamed *et al.* (2009), Burmester *et al.* (2009), Chen *et al.* (2014), Decker *et al.* (2004), Dimitriou (2006), He *et al.* (2004), He *et al.* (2014a, 2014b), Hoque *et al.* (2011), Keoh *et al.* (2009), Kumar and Madria (2013), Li *et al.* (2013a, 2013b), Liu and Xiao (2011), Lufei *et al.* (2008), Miettinen *et al.* (2014), Narain *et al.* (2014), Shi *et al.* (2012), Sun *et al.* (2008a), Tan (2012), Venkatasubramanian and Gupta (2010), Wang and Yan (2006), Xu *et al.* (2015)	23
Hybrid	Arapinis *et al.* (2012), Braeken *et al.* (2012), Drira *et al.* (2012), Dragoni *et al.* (2009), Garcia-Morchon *et al.* (2009), Gupta *et al.* (2005), Jang *et al.* (2011), Jara *et al.* (2013), Jehangir and de Groot (2006), Kim *et al.* (2011), Lam *et al.* (2003), Malasri and Wang (2009), Mihovska and Prasad (2007), Molla *et al.* (2009), Moon and Lee (2011), Park *et al.* (2010, 2008), Ren *et al.* (2006), Riaz *et al.* (2008), Rocha *et al.* (2010), Seigneur and Jensen (2005), Zhong and Richard Yang (2006), Zhu *et al.* (2003)	23
Hashing	He *et al.* (2014a, 2014b), Henrici and Muller (2008), Kang *et al.* (2008), Mathur *et al.* (2008), Safkhani *et al.* (2014), Subramanian *et al.* (2007), Yao *et al.* (2009)	7
Lightweight Protocols		
Lightweight	Abd-Alhameed *et al.* (2014), Ahamed *et al.* (2009), Arapinis *et al.* (2012), Burmester *et al.* (2009), Chen *et al.* (2014), Dimitriou (2006), Dragoni *et al.* (2009), Drira *et al.* (2012), El Husseini *et al.* (2013), Garcia-Morchon *et al.* (2009), Gupta *et al.* (2005), He *et al.* (2004), He *et al.* (2014a, 2014b), Hsieh and Leu (2014), Jara *et al.* (2013), Jehangir and de Groot (2006), Kang *et al.* (2008), Keoh *et al.* (2009), Kumar and Madria (2013), Lam *et al.* (2003), Liu and Xiao (2011), Liu *et al.* (2013, 2014), Lufei *et al.* (2008), Mihovska and Prasad (2007), Narain *et al.* (2014), Ning *et al.* (2015), Ren *et al.* (2006), Riaz *et al.* (2008), Rocha *et al.* (2010), Sun *et al.* (2008a, 2008b), Tan (2012), Undercoffer *et al.* (2003), Venkatasubramanian and Gupta (2010), Yao *et al.* (2009, 2014)	37

Table IV.
Cryptographic protocols proposed in the papers analyzed.

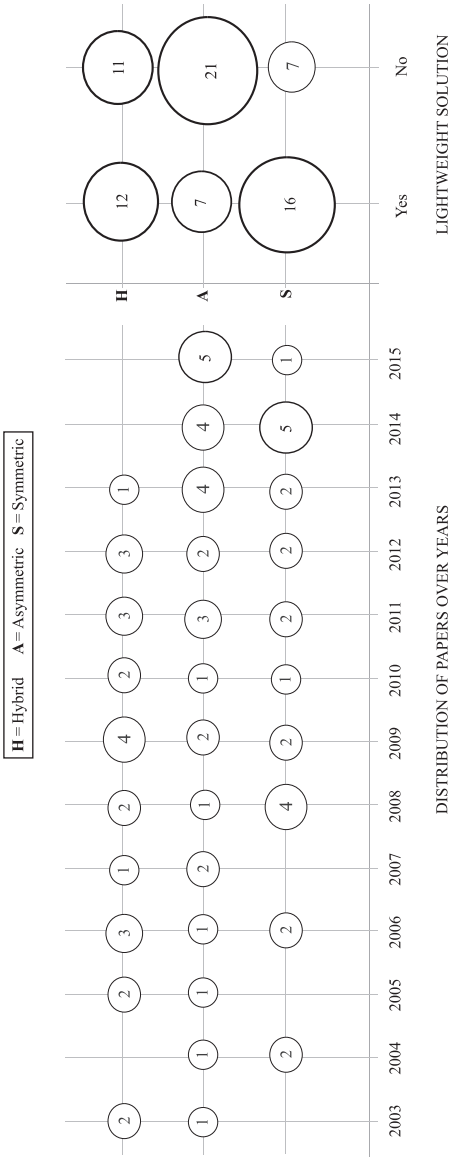


Figure 7.
Distribution of cryptographic algorithms over years and lightweight solutions

Symmetric-key cryptography		
Block cipher	Block cipher	Sun *et al.* (2008a)
	Blowfish	Decker *et al.* (2004)
	Skipjack	Keoh *et al.* (2009)
	RC4	Lufei *et al.* (2008)
Stream cipher	AES	He *et al.* (2014a, 2014b), Narain *et al.* (2014)
Asymmetric-key cryptography		
	RSA	Beaufour and Bonnet (2004), Hengartner and Steenkiste (2006), Patwardhan *et al.* (2005), Shi *et al.* (2011), Su *et al.* (2012), Wang and Fang (2007)
	Elliptic curve	Chuchaisri and Newman (2012), El Husseini *et al.* (2013), He and Zeadally (2015), Hsieh and Leu (2014), Huang *et al.* (2009a, 2009b), Yao *et al.* (2014), Yoon *et al.* (2010)

Table V. Encryption algorithms used in the papers analyzed

user data, proposed in 53 per cent of the privacy-related papers. This category encompasses four subcategories with the first one being:

- *removal of information*, such as *k*-anonymity, which assumes cloaking information among *k-1* users (Belsis and Pantziou, 2014; Gedik, 2008);
- *obfuscation* or degrading the quality of data, which refers to face blurring during lifelogging (Ye *et al.*, 2014) and location blurring (Tschersich *et al.*, 2011);
- *masking* real data, which includes use of pseudonyms, shadow data and other masking techniques;
- *combining fake with real information*, proposed by Srinivasan *et al.* (2008); and
- *other*, such as detecting speech rather than recording it and hiding information based on user's preferences.

The second category (17 per cent) refers to other countermeasures, such as RFID blocker tags, random walk algorithms for location-privacy, privacy metrics and a credit earning game. The third and fourth categories share the same amount of papers. The third category includes privacy-preserving mechanisms that utilize original user data, but propose an approach to storing or revealing user data while preserving privacy. This category includes a distributed approach which assumes that user data are exchanged across multiple databases or multiple network nodes (Boutsis and Kalogeraki, 2013; Gambs *et al.*, 2014; Hashem *et al.*, 2013), progressive exposure of user data (Zhu *et al.*, 2006a, 2006b, 2007, 2009), as well as approaches that rely on notification and user consent to reveal their personal data (Iachello *et al.*, 2006; Kelly *et al.*, 2013). The final category includes countermeasures based on privacy policies.

3.3.4 Trust management and computation. As discussed above, sophisticated cryptographic algorithms may require more hardware resources, such as memory, processing power and communication bandwidth. Thus, it is important to optimize those algorithms for the usage in resource-constrained nodes of ubicomp networks, such as MANETs, WSNs and VANETs. Moreover, cryptographic algorithms alone do not help detecting malicious and selfish nodes, which may lead to faults in packet routing, for example. Therefore, trust computation has been proposed to mitigate issues of identifying nodes in large scale networks for secure packet routing.

Table VI.
Privacy-preserving mechanisms.

Privacy-preserving mechanism	Papers	No.
1. *Hiding*		42 (53%)
1.1 Removal of information	Agudo *et al.* (2013), Arapinis *et al.* (2012), Arnedo-Moreno *et al.* (2013), Belsis and Pantziou (2014), Gambs *et al.* (2014), Gedik (2008), He *et al.* (2004), Hoque *et al.* (2011), Jana *et al.* (2013), Lee and Vasilakos (2011), Li *et al.* (2008), Li *et al.* (2013a, 2013b), Li and Cao (2013), Liu and Xiao (2011), Liu *et al.* (2014), Meyerowitz and Roy Choudhury (2009), Moon and Lee (2011), Pandit *et al.* (2014), Pingley *et al.* (2012), Popa *et al.* (2011), Ren *et al.* (2006), Shokri *et al.* (2012), Solanas and Martínez-Ballesté (2008), Tan (2012), Wang *et al.* (2013), Wang and Wang (2014), Wang *et al.* (2011), Wang and Zhang (2015), Weippl and Essmayr (2003), Wu *et al.* (2015), Xu *et al.* (2010)	*31*
1.2 Obfuscation	Duckham and Kulik (2005), Srinivasan *et al.* (2008), Tschersich *et al.* (2011), Ye *et al.* (2014)	4
1.3 Masking	Freudiger *et al.* (2013), Hengartner and Steenkiste (2006), Hornyack *et al.* (2011), Ma *et al.* (2006)	4
1.4 Combining fake with real information	Srinivasan *et al.* (2008)	1
1.5 Not recording but detecting speech	Davies *et al.* (2015)	1
1.6 Hiding information based on user's preferences in a context	Schaub *et al.* (2015)	1
2. *Other*	Enck *et al.* (2009), Groat *et al.* (2012), Holtzman *et al.* (2009), Juels *et al.* (2003), Kim *et al.* (2015), Li *et al.* (2013a, 2013b), Meyerowitz and Roy Choudhury (2009), Pallapa *et al.* (2012), Riedl *et al.* (2015), Shokri *et al.* (2012), Vahedi *et al.* (2011), Xu *et al.* (2010), Xie and Knijnenburg (2014), Yao *et al.* (2009)	14 (17%)
3. *Dealing with original data*	Backes *et al.* (2015), Boutsis and Kalogeraki (2013), Fanaeepour *et al.* (2015), Gambs *et al.* (2014), Hashem *et al.* (2013), Iachello *et al.* (2006), Kelly *et al.* (2013), Lee and Kwon (2010), Schaub *et al.* (2012, 2015), Zhu *et al.* (2006b, 2007, 2009)	13 (16%)
4. *Policies*	Ahamed *et al.* (2007), Clarke and Steele (2015), Hengartner and Steenkiste (2006), Kwon (2010), Omoronyia *et al.* (2012), Pallapa *et al.* (2007), Schaub *et al.* (2012), Thomas *et al.* (2014), Toch (2014), Tschersich *et al.* (2011), Wang *et al.* (2013)	11 (14%)

Trust management and computation countermeasures are found in 38 (13 per cent) papers analyzed in our SLR. In this context, the following four types of entities have been identified:

(1) well-behaved entity;

(2) selfish entities that maliciously refuse to forward packets to other entities, or disadvantaged entities that are forced to act selfishly because of scarce resources (Aime and Lioy, 2005; Luo *et al.*, 2004);

(3) malicious entities that seek to damage network operations (Luo *et al.*, 2004); and

(4) entities with selective (opportunistic) behavior that may behave well or maliciously, depending on their benefit (Ben Saied *et al.*, 2013; Das and Islam, 2012; Denko *et al.*, 2011).

Even though quantifying a subjective concept such as trust has been proven challenging (Tschersich *et al.*, 2011), papers analyzed in this SLR have proposed various approaches to obtaining trust values. In general, the trust lifecycle goes through the phases of information collection about a node's behavior, reporting on the witnessed observations, trust assessment and computation, decision-making (punish, penalize or degrade the untrusted entity), monitoring the behavior of entities participating in the network and updating trust values over time. Typically, evidence or history about an entity's behavior used to obtain trust values can be done in a direct and/or an indirect manner. Direct trust evaluation assumes immediate interaction between two entities and takes into account experience gathered over time. Indirect trust evaluation, on the other hand, is based on recommendations given by a central trusted party or other entities (witness entities) participating in the network (Almenarez *et al.*, 2008; Zhou *et al.*, 2008). The findings of our SLR reveal that trust values obtained through direct observation are time dependent. A study published in 2004 (Shand *et al.*, 2004) assigns time stamps and validity periods to trust recommendations to keep the trust values up to date. Similarly, another early study (Luo *et al.*, 2004) argues that the value of trust may change over time and is associated within a certain time period. The study proposes local trust of an entity which, if trusted by its surrounding k number of trusted entities, is said to be locally trusted and also accepted as a trusted entity network-wide. Analogously, a locally distrusted entity is considered untrustworthy in the entire network. The k number of entities is a network-wide fixed value based on the network density and desired system robustness. Aime and Lioy (2005) suggest modeling an entity's experience based on time at which a transaction occurred, behavior of the entity in the transaction, entity's identity and behavior that an entity has adopted. The trust value is obtained using the statistical average of the observed behaviors. However, to address the issue of malicious entities changing identities once they have accumulated enough negative trust values, the study proposes weighting recent experience more than the past ones. Therefore, the statistical interpretation of trust values is based on a correlation between the behavior of a peer and the time at which the behavior was experienced. Similar approaches that evaluate trust over time are presented in further studies analyzed in this SLR (Almenarez *et al.*, 2008; Boukerche and Ren, 2009; Safa *et al.*, 2010; Zhou *et al.*, 2008).

Apart from receiving information from direct neighbors (immediate interaction), trust assessment can be done using information sent by multiple (remote) sources. In addition to direct observations, Huynh *et al.* (2006) utilize so called witness reports which include information given by a third-party authority. The approach suggests obtaining the trust

value as a weighted mean of ratings provided by each source. An approach to identifying the impact to the accumulated trust value for each entity is proposed by Bahtiyar and Ufuk Çalayan (2012). Trust values are obtained as a weighted average of the extracted trust information. The study suggests the use of an impact factor which shows how much the extracted trust information contributed to the overall extracted trust information, taking over a value between [0,1], with 1 being the maximum impact. In the study by Ahamed *et al.* (2010), trust values are obtained from indirect and direct sources for each device and each context in a ubicomp environment. Context is regarded as an important criterion in defining trust management policies (Cahill *et al.*, 2003; Wang *et al.* 2013; Ray *et al.*, 2009). For example, Wang *et al.* (2013) propose a trust computation model which aims at combining two conflicting security goals of anonymity and trust to preserve privacy of contextual data, such as location obtained through a sensor-enhanced mobile computing device. Hoque *et al.* (2009) argue that the need for security in a ubicomp differs for each service. The study approaches the issue by categorizing services in different security levels which are shared in an initial trust assessment of the devices requesting services. Another context-based countermeasure dealing with trust negotiation for mobile social networking scenarios, is presented in (Manweiler *et al.*, 2009). The study proposes trust establishment based on direct encounters and without assuming pre-established relationships between people. For example, two users may establish a trust relationship if they manage to prove that they were at the same place at the same time. Otherwise, persons remain anonymous to each other to preserve their privacy.

Progressing from some of the early work on trust published in 2003, which assumes that trust negotiation is conducted between entities that are familiar with each other (Zachary and Brooks, 2003), recent trust-based mechanisms include dynamics in dealing with unknown and newly joined entities. Based on the type of an entity (well-behaved, selfish and malicious) that participates in a trust assessment procedure, trust models may suffer from potential false recommendations (El Husseini *et al.*, 2013). To address the challenge of interacting with potentially dishonest or malicious entities, two papers propose evaluating truthfulness of an entity before receiving its witness report (El Husseini *et al.*, 2013; Lagesse and Kumar, 2008). In the study by Lagesse and Kumar (2008), the proposed countermeasure is based on the idea that each entity may send exploratory requests to reveal the true nature of the entities participating in the network. The approach assumes that an entity responding to the exploratory request cannot differentiate between real and exploratory requests. A similar approach is presented in the study by El Husseini *et al.*(2013) where entities may send trust questions before asking for recommendations, such as questions about geographical location or values in a trust table. These questions are sent to multiple entities and the answers received are compared either with each other or against a set of pre-known answers. A different approach to handling false recommendations is proposed in (Ahamed *et al.*, 2010), which introduce a malicious recommendation handler to improve the accuracy of the trust values. In addition to the techniques that improve trust computation accuracy described above, various credibility and confidence measures have been proposed in recent years. To evaluate credibility of an entity participating in a trust assessment, a study by Das and Islam (2012) proposes feedback credibility by applying a function of similarity over feedback given by entities participating in the network. The higher the similarity between the entities with respect to their trust evaluation, the more credible is the feedback. Another approach based on credibility is

proposed by Ben Saied *et al.* (2013). In particular, it assesses the credibility of an entity (evaluator) who provides trust evaluation based on the reports sent by a number of other evaluators. If one evaluator sends a report which is in conflict with the assessment provided by its peer evaluators, it will be marked as a less credible evaluator. Apart from credibility measures, confidence levels have also been utilized in trust computation models to quantify the level of certainty that one entity has in the trust assessment of another entity. In the study by Denko *et al.* (2011), confidence of an entity providing trust evaluation is obtained through a variant of the β-distribution. Qureshi *et al.* (2012) obtain the confidence level based on the number of positive and negative interactions with targeted entities. Moschetta *et al.* (2010) suggest periodical degradation of the witnessed trust assessment by applying an aging factor, which gradually allows entities to gain confidence in newly joined entities and deal with traitors.

After the computation of a trust value of an entity has been completed, decisions are typically made to allow a well-behaved entity to extend its membership in a network or to punish untrusted entities. Different studies typically suggest isolating malicious nodes (Ahamed *et al.*, 2010; El Husseini *et al.*, 2013), but provide no further information on how to act in the situation when excluded nodes try to re-enter the network. To deal with this issue, Boukerche and Ren (2008) propose clustering nodes into communities which consist of one central node and all of its immediate neighbors. The immediate neighbor nodes with the highest trust values are assigned to the central node as their assistants in trust evaluation. Apart from evaluating trust, the role of the central node is to assign an initial trust value to newly joining nodes, update the list of neighboring nodes and set a threshold value for its community which represents the minimum trust value neighboring nodes need to have in order to continue being members of the community. Upon detecting misbehavior in the network, the trust value of a malicious or non-cooperative node will be decreased and finally the node is excluded from the community once its trust value drops beyond the threshold value. To keep such nodes from re-joining the network, the central nodes keeps black lists of all malicious nodes that have been excluded from its community and is therefore able to identify previously excluded nodes and refuse to re-include them into the community.

Figure 8 summarizes different approaches for trust computation and management and maps those approaches to their corresponding phase in the trust lifecycle. The findings reveal that trust-based countermeasures differ most in the way they obtain (assess) the final trust value (by assigning validity periods, assigning impact factors, or using credibility and confidence measures).

In recent years, a smaller amount of papers have pointed to the importance of transferring behavioral insights concerning trust into the software development process (Hoffmann and Sóllner, 2014) and into the development of recommender system for mobile applications (Yan *et al.*, 2012). In particular, Hoffmann and Sóllner (2014) propose a systematic process for deriving trust-related attributes from specific context. The process consists of four steps and begins with identifying and prioritizing the prospective users' uncertainties by conducting interviews, scenario descriptions or applying ethnographic methods. To alleviate an uncertainty, the study proposes applying antecedents, such as faith, judgment, motivation and consistency while considering the situational context. These antecedents are then used to derive corresponding nonfunctional requirements. The next step is to refine those requirements into specific functional requirements. The final step refers to designing activities in the software development process. The study points to a lack of a

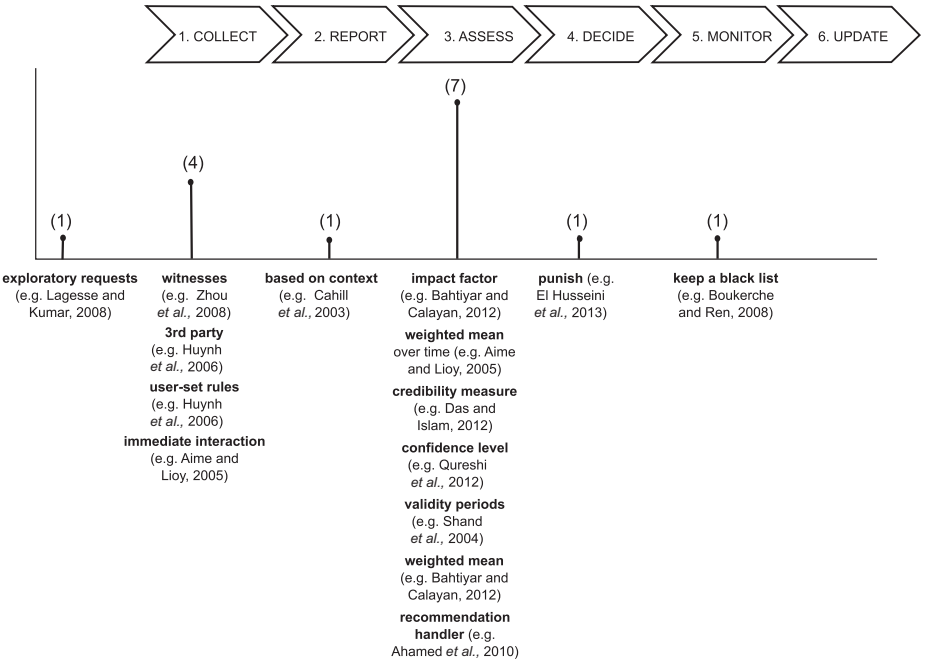


Figure 8.
Summary of trust-based countermeasures according to the trust life cycle

systematic ways for selecting appropriate antecedents in the existing literature for each type of uncertainty. To address this issue, Hoffmann and Sóllner (2014) suggest selecting as less antecedents as possible, as each results in at least one additional functional requirement. In the study by Yan *et al.* (2012), a way to measure trust is established by translating trust (regarded as a subjective concept) into a machine-readable conceptual trust model by conducting user surveys (questionnaires).

3.3.5 Other. The final category, "Other" (5.5 per cent), includes intrusion detection, anomaly detection and other mechanisms that could not be put into any of the categories proposed in this review.

3.4 RQ2.3 – *security goals*

Our SLR began with the following list of security goals, which distinguishes between basic and composite goals (Bacon and Moody, 2002; Sandhu and Samarati, 1996; Strembeck and Rinderle-Ma, 2013):

- *Confidentiality*: It ensures that classified objects can be only read by designated subjects.
- *Integrity*: It ensures that important objects are in their original or intended state.
- *Authentication*: It ensures that a subject in a system can be identified.
- *Availability*: It ensures that legitimate subjects can access/use software services and data at any time.

Moreover, the following security goals are considered the composite goals:

- *Authenticity of data*: It enables a proven identification of authorship for a data object.
- *Non-repudiation*: It ensures that no subject can deny its active or passive participation in a certain procedure.
- *Access control*: It ensures that access requests are granted if and only if the requesting subject is authorized to perform a requested action.
- *Accountability*: It allows to determine which subjects accessed/used which system resources.
- *Privacy*: It defines that each subject can determine the use of its personal data.

The security goal *audit* refers to the collection and analysis of security-related data to discover violations of one or more of the above-mentioned basic and composite security goals.

In addition to the keywords mentioned above, an additional security goal, *trust*, has been identified while manually screening the abstracts, titles and keywords of a subset of papers (see Section 2.1). Trust has been recognized as an important factor to achieve privacy and security of entities in distributed, pervasive and mobile environments (Denko *et al.*, 2011; Ahamed *et al.*, 2010; Bacon *et al.*, 2003; Blaze *et al.*, 1996; Yu *et al.*, 2003). Although there is no commonly accepted definition of trust (Cahill *et al.*, 2003), there has been an agreement among authors on its properties (Ahamed *et al.*, 2010; Blaze *et al.*, 1996; Boukerche and Ren, 2008; Liu and Issarny, 2006; Mondal and Kitsuregawa, 2006):

- trust is a relation among entities (Boukerche and Ren, 2008);
- trust is based on evidence related to the previous interactions of entities (Cahill *et al.*, 2003);
- trust deals with the estimation of an entity's future behavior (Denko *et al.*, 2011);
- trust builds a bridge between privacy and security (Boukerche and Ren, 2008); and
- trustworthiness of an entity depends on the context (Ben Saied *et al.*, 2013).

The results shown in Figure 9 indicate that authentication is the most commonly addressed security goal in the papers analyzed, followed by privacy, access control and trust. While performing the data extraction process, additional security goals emerged that occur less frequently and were thus placed in the "Other" category. These include *tamper-resistance*, *unforgeability of proofs of location* and *rogue blacklisting*.

3.5 RQ3 – *is there a difference in addressing security in distributed systems in general as compared to ubiquitous computing?*

Traditional distributed systems are defined as systems that involve multiple and heterogeneous entities that work together toward a common goal, bounded by a common language and/or protocols (Belapurkar *et al.*, 2009; Coulouris *et al.*, 2011; Tanenbaum and van Steen, 2006). To understand whether there are any differences between security mechanisms for distributed computing in general as compared to ubicomp environments, first the relationship between both computing paradigms has been examined. In total, 64 papers were identified in our pool of 282 papers that provide

information useful for this analysis. According to the papers in our SLR, different authors basically promote three different opinions when it comes to distinguishing between distributed computing in general and ubicomp:

(1) distributed computing is one of the *characteristics* of ubicomp (Liang *et al.*, 2008; Su *et al.*, 2012);

(2) distributed computing and ubicomp are two *distinct* paradigms (Compagnoni *et al.*, 2008); and

(3) ubicomp is seen as a form of *modern distributed computing* (Zachary and Brooks, 2003).

In total, 60 papers (94 per cent) use the term distributed computing to describe the *characteristics/nature* of ubicomp, supporting the relationship between the two by suggesting that ubicomp builds upon distributed systems by utilizing distributed services, distributed computation approaches and a decentralized architecture. The papers analyzed mostly use the term *distributed* to describe distribution of computational workload among different entities in the ubicomp environment. The second most common use of the term is associated with a description of the ubicomp environment, where the authors commonly use the terms *heterogeneous* (Chin *et al.*, 2010; López *et al.*, 2007), *open and dynamic* (see Chin *et al.*, 2010; Li *et al.*, 2008; Park *et al.*, 2010) and *decentralized with flexible network topologies* (Boukerche and Ren, 2008; Gedik, 2008; Manweiler *et al.*, 2009; Meyerowitz and Roy Choudhury, 2009) in conjunction with the term *distributed*.

Apart from using the term *distributed* to describe one of the *characteristics* of ubicomp, a smaller amount of papers explicitly *differentiate* between the two computing paradigms. In particular, three papers discuss differences between distributed computing and ubicomp in detail, identifying context-awareness as a core requirement that makes ubiquitous computing distinct from traditional distributed computing (see Compagnoni *et al.*, 2008; Freudiger *et al.*, 2013; Park *et al.*, 2014). It is worth noting that the same difference has been recognized and reported in non-security related papers (Hess and Campbell, 2003).

Another paper describes ubicomp as a paradigm that evolved from traditional distributed computing and names it a form of "*modern distributed computing*" (Zachary and

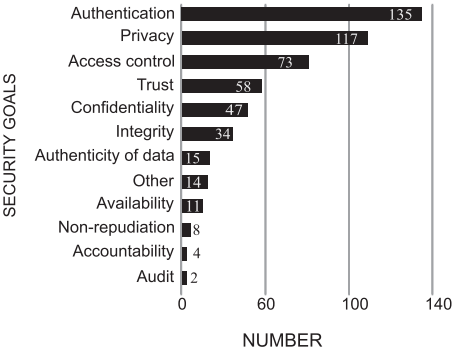


Figure 9.
Security goals and validation mechanisms

Brooks, 2003), while highlighting software (and device) mobility, modern network infrastructures and mobile agents as novel elements to traditional distributed computing.

Thus, there is a relationship between the two computing paradigms and, as presented in Section 3.4, there is similarity in the list of security goals between both. However, the clear distinction between both computing paradigms is that in a ubicomp environment, the corresponding security goals and security countermeasures must consider the dynamically changing *context* as a result of the devices' mobility. Therefore, *context-awareness* is a novel characteristic of ubicomp and the corresponding security countermeasures must also be context-aware (to a certain degree). As discussed in the papers analyzed, the introduction of context has brought challenges to the attempts in transferring traditional security countermeasures used in distributed systems to a ubicomp environment. A significant number of papers have reported on the extension of access control approaches, such as RBAC models and access policies, with context-specific attributes (Agudo *et al.*, 2013; Damiani *et al.*, 2007; dos Santos *et al.*, 2011; Strembeck and Neumann, 2004; Schefer-Wenzl and Strembeck, 2013). Another group of countermeasures (Pingley *et al.*, 2012; Xie and Knijnenburg, 2014) have reported on context-aware privacy-preserving mechanisms that aim at protecting the user's sensitive information, such as a personal ID or the current location. In addition to context, the quickly expanding heterogeneity of devices participating in a ubicomp environment, as well as its dynamics, can also be regarded as novel to ubicomp. To ensure interaction between such devices, a number of papers propose pairing mechanisms for devices without prior security associations (Miettinen *et al.*, 2014), dynamic trust computation (Das and Islam, 2012), adaptive access control policies with respect to diverse environmental requirements (Lufei *et al.*, 2008), as well as proximity-based access control mechanisms (Agudo *et al.*, 2013; Rasmussen *et al.*, 2009).

Therefore, one can conclude that the traditional security goals of distributed computing remain important in ubicomp, as well (also backed up by our findings in Section 3.4). However, ubicomp introduces novel requirements that should be considered while designing security countermeasures (such as context-awareness, low computation overhead, unobtrusiveness and increased system dynamics, as discussed above).

4. Discussion on the validity threats to our review

4.1 Search procedure

Our SLR began with carefully defining the keywords and designing the corresponding search strings. While conducting the search procedure over five scientific databases, there was an average number of 14.6 per cent of double entries over all engines. Obviously and as also discussed by Fernández-Sáez *et al.* (2013), duplicate papers may influence the statistics and overall results of an SLR. To mitigate this threat, Mendeley reference manager was proven helpful while managing double entries before proceeding with the SLR.

A significant drawback in searching for papers in scientific databases lies in its efficiency. In particular, this is because search mechanisms of today's scientific databases are not designed for systematic reviews, resulting in a large number of irrelevant papers. As a result, authors of systematic reviews have to take additional steps to revise their collection of papers before they can begin extracting the data. In addition to drawbacks resulting from today's scientific search engines, another challenge occurs because of the inconsistent terminology used by the authors of papers indexed in scientific databases. Therefore, one cannot exclude the possibility that our

SLR missed some relevant papers. To mitigate this drawback, other SLR studies (Radjenović *et al.*, 2013) have proposed backward snowballing as an additional search strategy. Following the remark by Jalali and Wohlin (2012), and because of the large number of papers initially found in our SLR, our SLR did not use backward snowballing.

4.2 Validity of results

While reporting on the findings, our judgment was based on the reports provided by the authors of papers we analyzed. To ensure transparency and traceability of the findings reported in our SLR, detailed information is provided for the following procedures:

- *Search procedure*: Keywords, search strings, search criteria are provided. Additionally, search strings adapted for each database are given in our research protocol.
- *Paper selection*: Selection criteria and the full list of papers selected for the SLR are given in the protocol. Also, a Mendeley backup is available on request.

5. Summary and future research directions

The goal of the SLR was to provide a comprehensive overview of security-related research in ubicomp. For this purpose, a SLR has been conducted which included dedicated planning, conducting and reporting phases. To ensure rigor in our procedure, the guidelines described in our research protocol have been carefully followed (the protocol is available at: http://epub.wu.ac.at/4826/).

After filtering the initial 12,705 papers, data were extracted from 282 quality papers. Our findings indicate that as the number of papers addressing security issues in ubicomp rises, most of the research has been motivated by different types of attacks. For instance, these attacks include compromising the nodes of a wireless network, draining battery of a mobile device, denying access to ubiquitous services, as well as compromising a patient's health by sending false test results on a sugar level in blood. While trying to synthesize and categorize the attacks and threats in a meaningful way, a number of challenges occurred. First, taxonomies of attacks proposed in the literature (Hansman and Hunt, 2005; Igure and Williams, 2008; Mo and Wei, 2001; Wu *et al.*, 2011) do not take into account attacks specific to ubicomp and are therefore unable to assign a fitting category to the most of the attacks identified in our SLR. This led to the conclusion that more work is needed in proposing a tailored taxonomy which includes novel attacks that are unique to ubicomp environments, as well as those inherited from traditional distributed computing.

Moreover, our findings indicate that network-related challenges, such as dynamics of *ad hoc* networks and a large number of participating heterogeneous and resource-constrained devices have been recognized as the most frequently addressed motivating factors in the security-related papers. This finding complements those reported by Subramanian *et al.* (2007), who state that security-related research in a ubicomp context has mainly focused on securing the corresponding communication networks. Although there are papers in our SLR that address device-level security issues, such as installing malicious apps, leaving smudges on touchscreens or stealing one's device, as well as papers on context-aware access control or novel biometric techniques to authenticate a user, network-related papers are still to a great extent predominant. This observation opens the possibilities in addressing the security challenges of other aspects of ubicomp.

Moreover, considering the "disappearing/calm" nature of the ubicomp technologies (as envisioned by Mark Weiser), surprisingly no papers (e.g. about trust mechanisms) analyzed

in our SLR discussed self-healing properties of ubicomp systems. Furthermore, the papers discussing an *ad hoc* adaptation to the changes in the state of a ubicomp environment have generally addressed spatial and temporal changes, while disregarding other contextual information. Thus, this opens a possibility for further research.

While examining the security goals reported in the papers, authentication, privacy, access control and trust proved to be the most commonly reported goals over the past decade. Having used the predefined list of security goals traditionally used in software systems in general, our findings revealed that each of those goals has also been addressed in a ubicomp context. As part of our review, a closer look at the relationship between ubicomp and distributed computing provided interesting insights that reveal that ubicomp builds upon distributed computing. While comparing the requirements in designing security countermeasures between both computing paradigms, our findings have revealed increased dynamics and mobility, context-awareness, lightweight design and unobtrusiveness while addressing ubicomp security countermeasures. However, it would be interesting to further investigate other requirements that have not been addressed in the papers analyzed in our SLR. For example, the large-scale nature of a ubicomp environment implies that there is yet another requirement in designing algorithms that are able to scale with the frequently changing large number of users/devices that have different privileges and agendas within the system. This issue has also been recognized and discussed as potential future work by the authors of the papers analyzed in our SLR (Agudo *et al.*, 2013).

Having recognized the lack of comprehensive overviews of security attacks, vulnerabilities and threats, as well as defense mechanisms proposed in ubicomp-related research, we believe that the findings of this SLR are useful for researchers novel in the area as well as to the established researchers who want to position their research with regard to other contributions.

Notes

1. For a full version of our 79-page long research protocol, please refer to: http://epub.wu.ac.at/4826/
2. IEEE International Conference on Pervasive Computing and Communications (PerCom), IEEE Pervasive Computing, Personal and Ubiquitous Computing, and ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp).
3. Mendeley reference manager: www.mendeley.com
4. Even though there are earlier papers on security in ubicomp available, we were interested in the security issues and countermeasures discussed over the past decade.
5. SJR ranking: www.scimagojr.com/journalrank.php
6. CORE conference ranking: www.core.edu.au/index.php/conference-rankings
7. The full list of the papers is available in our research protocol, pp. 50-70.
8. Note that some of the ways adversaries obtain private data from a stolen device, such as cracking authentication mechanisms (see also the category *Attacks*) or stealing a device whose authentication mechanism has been deliberately deactivated by its legitimate user, are distributed over other categories proposed in this SLR.

References

Abd-Alhameed, R., Mapoka, T. and Shepherd, S. (2014), "A new multiple service key management scheme for secure wireless mobile multicast", *IEEE Transactions on Mobile Computing*, Vol. 14 No. 8, pp. 1545-1559.

Aboudagga, N., De Meulenaer, G., Eltoweissy, M. and Quisquater, J.J. (2009), "IMAPS: Imbricated authentication protocol suite for mobile users and groups", *Proceedings of the 34th Annual IEEE Conference on Local Computer Networks, Zurich, Switzerland, IEEE Computer Society, Washington, DC*, pp. 30-36.

Afzal, W., Torkar, R. and Feldt, R. (2009), "A systematic review of search-based testing for non-functional system properties", *Information and Software Technology*, Vol. 51 No. 6, pp. 957-976.

Agudo, I., Rios, R. and Lopez, J. (2013), "A privacy-aware continuous authentication scheme for proximity-based access control", *Computers & Security*, Vol. 39 No. B, pp. 117-126.

Ahamed, S., Talukder, N. and Haque, M. (2007), "Privacy challenges in context-sensitive access control for pervasive computing environment", *Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking Services, MobiQuitous'07, Philadelphia*, IEEE Computer Society, pp. 1-6.

Ahamed, S.I., Haque, M.M., Hoque, M.E., Rahman, F. and Talukder, N. (2010), "Design, analysis, and deployment of omnipresent Formal Trust Model (FTM) with trust bootstrapping for pervasive environments", *Journal of Systems and Software*, Vol. 83 No. 2, pp. 253-270.

Ahamed, S.I., Li, H., Talukder, N., Monjur, M. and Hasan, C.S. (2009), "Design and implementation of S-MARKS: a secure middleware for pervasive computing applications", *Journal of Systems and Software*, Vol. 82 No. 10, pp. 1657-1677.

Ahamed, S.I., Sharmin, M. and Ahmed, S. (2008), "A Risk-aware Trust Based Secure Resource Discovery (RTSRD) model for pervasive computing", *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications, Hong Kong*, IEEE Computer Society, Washington, DC, pp. 590-595.

Ahmed, I., Ye, Y., Bhattacharya, S., Asokan, N., Jacucci, G., Nurmi, P. and Tarkoma, S. (2015), "Checksum gestures: continuous gestures as an out-of-band channel for secure pairing", *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Osaka, Japan, UbiComp '15, ACM, New York, NY*, pp. 391-401.

Aime, M. and Lioy, A. (2005), "Incremental trust: building trust from past experience", *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks in Taormina, Giardini Naxos, Italy, 2005*, IEEE Computer Society, Los Alamitos, CA, pp. 603-608.

Alemán, J.L.F., Señor, I.C., Lozoya, P.N O. and Toval, A. (2013), "Security and privacy in electronic health records: a systematic literature review", *Journal of Biomedical Informatics*, Vol. 46 No. 3, pp. 541-562.

Almenarez, F., Marin, A., Diaz, D., Cortes, A., Campo, C. and Garcia-Rubio, C. (2008), "A trust-based middleware for providing security to Ad-Hoc Peer-to-Peer applications", *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications, Hong Kong, IEEE Computer Society, Washington, DC*, pp. 531-536.

Al-Muhtadi, J., Ranganathan, A., Campbell, R. and Mickunas, M.D. (2003), "Cerberus: a context-aware security scheme for smart spaces", *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, Dallas-Fort Worth, TX, IEEE Computer Society, Washington, DC*, pp. 489-496.

Arapinis, M., Mancini, L., Ritter, E., Ryan, M., Golde, N., Redon, K. and Borgaonkar, R. (2012), "New privacy issues in mobile telephony: fix and verification", *Proceedings of the 2012*

ACM Conference on Computer and Communications Security, *Raleigh, NC*, *ACM, New York, NY*, pp. 205-216.

Arnedo-Moreno, J., Pérez-Gilabert, N. and Domingo-Prieto, M. (2013), "Anonymously accessing JXTA community services through split message forwarding", *Mathematical and Computer Modelling*, Vol. 58 No. 56, pp. 1313-1327.

Backes, M., Barbosa, M., Fiore, D. and Reischuk, R. (2015), "ADSNARK: nearly practical and privacy-preserving proofs on authenticated data", *IEEE Symposium on Security and Privacy in Fairmont*, *San Jose, CA*, IEEE Computer Society, Washington, DC, pp. 271-286.

Bacon, J. and Moody, K. (2002), "Toward open, secure, widely distributed services", *Communications of the ACM*, Vol. 45 No. 6, pp. 59-64.

Bacon, J., Moody, K. and Yao, W. (2003), "Access control and trust in the use of widely distributed services", *Software: Practice and Experience*, Vol. 33 No. 4, pp. 375-394.

Bahtiyar, S. and Ufuk Çalayan, M. (2012), "Extracting trust information from security system of a service", *Journal of Network and Computer Applications*, Vol. 35 No. 1, pp. 480-490.

Barisch, M. (2011), "Design and evaluation of an architecture for ubiquitous user authentication based on identity management systems", *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, *Changsha, China*, pp. 863-872.

Barra, S., Casanova, A., Narducci, F. and Ricciardi, S. (2015), "Ubiquitous iris recognition by means of mobile devices", *Pattern Recognition Letters*, Vol. 57 No. C, pp. 66-73.

Beaufour, A. and Bonnet, P. (2004), "Personal servers as digital keys", *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications*, *Orlando, FL*, *IEEE Computer Society, Washington, DC*, pp. 319-328.

Belapurkar, A., Anirban, C., Harigopal, P., Niranjan, V., Srinivas, P. and Srikanth, S. (2009), *Distributed Systems Security: Issues, Processes, and Solutions*, John Wiley & Sons, Chichester, Hoboken, NJ.

Belsis, P. and Pantziou, G. (2014), "A k-anonymity privacy-preserving approach in wireless medical monitoring environments", *Personal and Ubiquitous Computing*, Vol. 18 No. 1, pp. 61-74.

Ben Saied, Y., Olivereau, A., Zeghlache, D. and Laurent, M. (2013), "Trust management system design for the internet of things: a context-aware and multi-service approach", *Computers & Security*, Vol. 39 No. B, pp. 351-365.

Blaze, M., Feigenbaum, J. and Lacy, J. (1996), "Decentralized Trust Management", *Proceedings of the IEEE Symposium on Security and Privacy*, *Oakland, CA*, *IEEE Computer Society, Washington, DC*, pp. 164-173.

Boukerche, A. and Ren, Y. (2008), "A trust-based security system for ubiquitous and pervasive computing environments", *Computer Communications*, Vol. 31 No. 18, pp. 4343-4351.

Boukerche, A. and Ren, Y. (2009), "A secure mobile healthcare system using trust-based multicast scheme", *IEEE Journal on Selected Areas in Communications*, Vol. 27 No. 4, pp. 387-399.

Boutsis, I. and Kalogeraki, V. (2013), "Privacy preservation for participatory sensing data", *IEEE International Conference on Pervasive Computing and Communications*, *San Diego, CA*, *IEEE Computer Society, Washington, DC*, pp. 103-113.

Braeken, A., De La Piedro, A. and Wouters, K. (2012), "Secure event logging in sensor networks", *Lecture Notes in Computer Science: Public Key Infrastructures, Services and Applications*, Vol. 7163 No. 1, pp. 194-208.

Burmester, M., Van Le, T., De Medeiros, B. and Tsudik, G. (2009), "universally composable rfid identification and authentication protocols", *ACM Transactions on Information and System Security* Vol. 12 No. 4, pp. 1-33.

Buthpitiya, S., Dey, A.K. and Griss, M. (2014), "Soft authentication with low-cost signatures", *2014 IEEE International Conference on Pervasive Computing and Communications*, Budapest, Hungary, pp. 172-180.

Byun, J.W., Lee, D.H. and Lim, J.I. (2007), "EC2C-PAKA: An efficient client-to-client password-authenticated key agreement", *Information Sciences*, Vol. 177 No. 19, pp. 3995-4013.

Cahill, V., Gray, E., Seigneur, J.M., Jensen, C.D., Chen, Y., Shand, B., Dimmock, N., Twigg, A., Bacon, J., English, C., Wagealla, W., Terzis, S., Nixon, P., Di Marzo Serugendo, G., Bryce, C., Carbone, M., Krukow, K., Nielson, M., Seigneur, M., Jensen, C.D., Shand, B., Dimmock, N., Twigg, A., Bacon, J., Serugendo, M., Carbone, M. and Krukow, K. (2003), "Using trust for secure collaboration in uncertain environments", *IEEE Pervasive Computing*, Vol. 2 No. 3, pp. 52-61.

Casale, P., Pujol, O. and Radeva, P. (2012), "Personalization and user verification in wearable systems using biometric walking patterns", *Personal and Ubiquitous Computing*, Vol. 16 No. 5, pp. 563-580.

Chen, C., Mitchell, C. and Tang, S. (2013), "Ubiquitous one-time password service using the generic authentication architecture", *Mobile Networks and Applications*, Vol. 18 No. 5, pp. 738-747.

Chen, C.H.O., Chen, C.W., Kuo, C., Lai, Y.H., McCune, J.M., Studer, A., Perrig, A., Yang, B.Y. and Wu, T.C. (2008), "GAnGS: gather, authenticate 'N Group Securely", *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, *San Francisco, CA*, ACM, *New York, NY*, pp. 92-103.

Chen, M., Chen, S. and Xiao, Q. (2014), "Pandaka: a lightweight cipher for RFID systems", *IEEE Conference on Computer Communications*, *Toronto, ON*, *IEEE Computer Society*, Washington, DC, pp. 172-180.

Cheng, B.C., Chen, H., Li, Y.J. and Tseng, R.Y. (2008), "A packet marking with fair probability distribution function for minimizing the convergence time in wireless sensor networks", *Computer Communications*, Vol. 31 No. 18, pp. 4352-4359.

Chien, H.Y. (2007), "SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity", *IEEE Transactions on Dependable and Secure Computing* Vol. 4 No. 4, pp. 337-340.

Chin, J., Zhang, N., Nenadic, A. and Bamasak, O. (2010), "A context-constrained authorisation (CoCoA) framework for pervasive grid computing", *Wireless Networks*, Vol. 16 No. 6, pp. 1541-1556.

Chuchaisri, P. and Newman, R.E. (2012), "Multi-resolution elliptic curve digital signature", *37th Annual IEEE Conference on Local Computer Networks*, *Clearwater, FL*, *IEEE Computer Society, Washington, DC*, pp. 93-101.

Clarke, A. and Steele, R. (2015), "Smartphone-based public health information systems: anonymity, privacy and intervention", *Journal of the Association for Information Science and Technology*, Vol. 66 No. 12, pp. 2596-2608.

Compagnoni, A., Gunter, E.L. and Bidinger, P. (2008), "Role-based access control for boxed ambients", *Theoretical Computer Science*, Vol. 398 Nos 1/3, pp. 203-216.

Corradi, A., Montanari, R. and Tibaldi, D. (2004), "Context-based access control management in ubiquitous environments", *Proceedings of the Third IEEE International Symposium on Network Computing and Applications*, *Cambridge, MA*, *IEEE Computer Society, Washington, DC*, pp. 253-260.

Coughlin, T. (2015), "A Moore's law for mobile energy: improving upon conventional batteries and energy sources for mobile devices", *IEEE Consumer Electronics Magazine*, Vol. 4 No. 1, pp. 74-82.

Coulouris, G., Dollimore, J., Kindberg, T. and Blair, G. (2011), *Distributed Systems: Concepts and Design*, 5th ed., Pearson, Boston, MA.

Damiani, M.L., Bertino, E., Catania, B. and Perlasca, P. (2007), "GEO-RBAC: a spatially aware RBAC", *ACM Transactions on Information and System Security*, Vol. 10 No. 1, pp. 1-34.

Das, A. and Islam, M.M. (2012), "Securedtrust: a dynamic trust computation model for secured communication in multiagent systems", *IEEE Transactions on Dependable and Secure Computing*, Vol. 9 No. 2, pp. 261-274.

Davies, N., Friday, A., Clinch, S., Sas, C., Langheinrich, M., Ward, G. and Schmidt, A. (2015), "Security and privacy implications of pervasive memory augmentation", *IEEE Pervasive Computing*, Vol. 14 No. 1, pp. 44-53.

De Marsico, M., Galdi, C., Nappi, M. and Riccio, D. (2014), "FIRME: face and iris recognition for mobile engagement", *Image and Vision Computing*, Vol. 32 No. 12, pp. 1161-1172.

Decker, C., Nguissi, S., Haller, J. and Kilian-Kehr, R. (2004), "Proximity as a security property in a mobile enterprise application context", *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, *Big Island, HI*, *IEEE Computer Society, Washington, DC*, pp. 1-10.

Denko, M.K., Sun, T. and Woungang, I. (2011), "Trust management in ubiquitous computing: a Bayesian approach", *Computer Communications*, Vol. 34 No. 3, pp. 398-406.

Dimitriou, T. (2006), "A secure and efficient RFID protocol that could make Big Brother (partially) obsolete", *Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, *Pisa, Italy*, *IEEE Computer Society, Washington, DC*, pp. 1-6.

Dolev, S., Krzywiecki, Ł., Panwar, N. and Segal, M. (2015), "Vehicle authentication via monolithically certified public key and attributes", *Wireless Networks*, Vol. 22 No. 3, pp. 1-18.

dos Santos, A.L.M., Scarlata, V., Lima, A.C., Alves, I.C. and Sampaio, D.D.C. (2011), "SACM: stateful access control model", *2011 IEEE 36th Conference on Local Computer Networks*, *Bonn, Germany*, *IEEE Computer Society, Washington, DC*, pp. 159-162.

Dozono, H., Nakakuni, M., Sanada, H. and Noguchi, Y. (2006), "The analysis of pen inputs of handwritten symbols using self organizing maps and its application to user authentication", *International Joint Conference on Neural Networks*, *Vancouver, BC*, *IEEE Computer Society*, Washington, DC, pp. 2577-2582.

Dragoni, N., Massacci, F., Walter, T. and Schaefer, C. (2009), "What the Heck is this application doing? A security-by-contract architecture for pervasive services", *Computers and Security*, Vol. 28 No. 7, pp. 566-577.

Drira, W., Renault, E. and Zeghlache, D. (2012), "A hybrid authentication and key establishment scheme for WBAN", *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, *Liverpool*, *IEEE Computer Society*, Washington, DC, pp. 78-83.

Duckham, M. and Kulik, L. (2005), "A formal model of obfuscation and negotiation for location privacy", *Proceedings of the Third International Conference on Pervasive Computing*, *Munich, Germany*, *Springer-Verlag, Berlin, Heidelberg*, pp. 152-170.

Dybå, T. and Dingsøyr, T. (2008), "Strength of evidence in systematic reviews in software engineering", *Proceedings of the Second ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*, *Kaiserslautern, Germany*, *ACM, New York, NY*, pp. 178-187.

Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A. and Uhsadel, L. (2007), "A survey of lightweight-cryptography implementations", *IEEE Design and Test of Computers*, Vol. 24 No. 6, pp. 522-533.

El Husseini, A., M'hamed, A., El Hassan, B. and Mokhtari, M. (2013), "Trust-based authentication scheme with user rating for low-resource devices in smart environments", *Personal and Ubiquitous Computing*, Vol. 17 No. 5, pp. 1013-1023.

Enck, W., Ongtang, M. and McDaniel, P. (2009), "On lightweight mobile phone application certification", *Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, ACM, New York, NY*, pp. 235-245.

Fanaeepour, M., Kulik, L., Tanin, E. and P. Rubinstein, B.I. (2015), "The CASE histogram: privacy-aware processing of trajectory data using aggregates", *GeoInformatica*, Vol. 19 No. 4, pp. 747-798.

Ferdous, M.S. and Poet, R. (2013), "Portable Personal identity provider in mobile phones", *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, Australia, IEEE Computer Society*, Washington, DC, pp. 736-745.

Fernández-Sáez, A.M., Genero, M. and Chaudron, M.R.V. (2013), "Empirical studies concerning the maintenance of UML diagrams and their use in the maintenance of code: a systematic mapping study", *Information and Software Technology*, Vol. 55 No. 7, pp. 1119-1142.

Freudiger, J., Manshaei, M., Hubaux, J.P. and Parkes, D. (2013), "Non-cooperative location privacy", *IEEE Transactions on Dependable and Secure Computing*, Vol. 10 No. 2, pp. 84-98.

Fu, S. and Xu, C.Z. (2005), "A coordinated spatio-temporal access control model for mobile computing in coalition environments", *Proceedings of the 19th IEEE International Symposium on Parallel and Distributed Processing, Broomfield, CO, IEEE Computer Society, Washington, DC*, pp. 1-8.

Gambs, S., Killijian, M.O., Roy, M. and Traore, M. (2014), "PROPS: a privacy-preserving location proof system", *IEEE 33rd International Symposium on Reliable Distributed Systems, Nara, Japan*, IEEE Computer Society, Washington, DC, USA, pp. 1-10.

García-Borgoñóna, L., Barcelona, M., García-García, J., Albab, M. and Escalonab, M. (2013), "Software process modeling languages: a systematic literature review", *Information and Software Technology*, Vol. 56 No. 2, pp. 103-116.

Garcia-Morchon, O., Falck, T., Heer, T. and Wehrle, K. (2009), "Security for pervasive medical sensor networks", *6th Annual International Conference on Mobile and Ubiquitous Systems: Networking Services, Toronto, Canada, IEEE Computer Society*, Washington, DC, pp. 1-10.

Gedik, B. (2008), "Protecting location privacy with personalized k-anonymity: architecture and algorithms", *IEEE Transactions on Mobile Computing*, Vol. 7 No. 1, pp. 1-18.

Groat, M., Edwards, B., Horey, J., He, W. and Forrest, S. (2012), "Enhancing privacy in participatory sensing applications with multidimensional data", *IEEE International Conference on Pervasive Computing and Communications, Lugano, Switzerland, IEEE Computer Society*, Washington, DC, pp. 144-152.

Gupta, V., Millard, M., Fung, S., Zhu, Y., Gura, N., Eberle, H. and Shantz, S. (2005), "Sizzle: a standards-based end-to-end security architecture for the embedded Internet", *Third IEEE International Conference on Pervasive Computing and Communications, Kauai, HI, IEEE Computer Society*, Washington, DC, pp. 247-256.

Hansman, S. and Hunt, R. (2005), "A taxonomy of network and computer attacks", *Computers and Security*, Vol. 24 No. 1, pp. 31-43.

Hashem, T., Ali, M.E., Kulik, L., Tanin, E. and Quattrone, A. (2013), "Protecting privacy for group nearest neighbor queries with crowdsourced data and computing", *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Zurich, Switzerland*, ACM, New York, NY, pp. 559-562.

He, D., Chan, S. and Tang, S. (2014a), "A novel and lightweight system to secure wireless medical sensor networks", *IEEE Journal of Biomedical and Health Informatics*, Vol. 18 No. 1, pp. 316-326.

He, D., Chan, S., Zhang, Y. and Yang, H. (2014b), "Lightweight and confidential data discovery and dissemination for wireless body area networks", *IEEE Journal of Biomedical and Health Informatics*, Vol. 18 No. 2, pp. 440-448.

He, D. and Zeadally, S. (2015), "Authentication protocol for an ambient assisted living system", *IEEE Communications Magazine*, Vol. 53 No. 1, pp. 71-77.

He, Q., Wu, D. and Khosla, P. (2004), "The quest for personal control over mobile location privacy", *IEEE Communications Magazine*, Vol. 42 No. 5, pp. 130-136.

He, W., Huang, Y., Nahrstedt, K. and Lee, W. (2007), "SMOCK: a self-contained public key management scheme for mission-critical wireless ad hoc networks", *Fifth Annual IEEE International Conference on Pervasive Computing and Communications*, *White Plains, NY*, *IEEE Computer Society*, Washington, DC, pp. 201-210.

Hengartner, U. and Steenkiste, P. (2005), "Access control to people location information", *ACM Transactions on Information and System Security*, Vol. 8 No. 4, pp. 424-456.

Hengartner, U. and Steenkiste, P. (2006), "Avoiding privacy violations caused by context-sensitive services", *Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, *Pisa, Italy*, *IEEE Computer Society*, Washington, DC, pp. 222-233.

Henrici, D. and Muller, P. (2008), "Providing security and privacy in rfid systems using triggered hash chains", *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, *Hong Kong*, *IEEE Computer Society*, Washington, DC, pp. 50-59.

Hess, C. and Campbell, R. (2003), "A context-aware data management system for ubiquitous computing applications", *Proceedings of the 23rd International Conference on Distributed Computing Systems*, *Providence, RI*, *IEEE Computer Society*, Washington, DC, pp. 294-301.

Hoffmann, H. and Sóllner, M. (2014), "Incorporating behavioral trust theory into system development for ubiquitous applications", *Personal and Ubiquitous Computing*, Vol. 18 No. 1, pp. 117-128.

Holtzman, H., Lee, S. and Shen, D. (2009), "Opentag: privacy protection for RFID", *IEEE Pervasive Computing*, Vol. 8 No. 2, pp. 71-77.

Hoque, M., Rahman, F. and Ahamed, S. (2009), "An adaptive initial trust and demand aware secure resource discovery (AID-SRD) model for pervasive environments", *IEEE International Conference on Pervasive Computing and Communication*, *Galveston, TX*, pp. 1-6.

Hoque, M., Rahman, F. and Ahamed, S. (2011), "AnonPri: an efficient anonymous private authentication protocol", *IEEE International Conference on Pervasive Computing and Communications*, *Seattle*, *IEEE Computer Society*, Washington, DC, pp. 102-110.

Hornyack, P., Han, S., Jung, J., Schechter, S. and Wetherall, D. (2011), "These aren't the Droids you're looking for: retrofitting Android to protect data from imperious applications", *Proceedings of the 18th ACM Conference on Computer and Communications Security*, *Chicago, IL*, *ACM, New York, NY*, pp. 639-652.

Hsieh, W.B. and Leu, J.-S. (2014), "Anonymous authentication protocol based on elliptic curve Diffie-Hellman for wireless access networks", *Wireless Communications and Mobile Computing*, Vol. 14 No. 10, pp. 995-1006.

Hu, C., Zhang, N., Li, H., Cheng, X. and Liao, X. (2013), "Body Area network security: a fuzzy attribute-based signcryption scheme", *IEEE Journal on Selected Areas in Communications*, Vol. 31 No. 9, pp. 37-46.

Huang, K.H., Chung, Y.F., Liu, C.H., Lai, F. and Chen, T.S. (2009a), "Efficient migration for mobile computing in distributed networks", *Computer Standards & Interfaces* Vol. 31 No. 1, pp. 40-47.

Huang, Y., Hsieh, M., Chao, H., Hung, S. and Park, J. (2009b), "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks", *IEEE Journal on Selected Areas in Communications*, Vol. 27 No. 4, pp. 400-411.

Huynh, T.D., Jennings, N.R. and Shadbolt, N.R. (2006), "An integrated trust and reputation model for open multi-agent systems", *Autonomous Agents and Multi-Agent Systems*, Vol. 13 No. 2, pp. 119-154.

Iachello, G., Truong, K.N., Abowd, G.D., Hayes, G.R. and Stevens, M. (2006), "prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, *Montreal, Quebec*, *ACM*, *New York, NY*, pp. 1009-1018.

Igure, V. and Williams, R. (2008), "taxonomies of attacks and vulnerabilities in computer systems", *IEEE Communications Surveys & Tutorials*, Vol. 10 No. 1, pp. 6-19.

Islam, N. and Want, R. (2014), "Smartphones: past, present, and future", *IEEE Pervasive Computing*, Vol. 13 No. 4, pp. 89-92.

Jabbar, H. (2008), "Viewer Identification and authentication in IPTV using RFID technique", *IEEE Transactions on Consumer Electronics*, Vol. 54 No. 1, pp. 105-109.

Jalali, S. and Wohlin, C. (2012), "Systematic literature studies: database searches vs backward snowballing", *Proceedings of the ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*, *Lund, Sweden*, *ACM, New York, NY*, pp. 29-38.

Jana, S., Narayanan, A. and Shmatikov, V. (2013), "A scanner darkly: protecting user privacy from perceptual applications", *IEEE Symposium on Security and Privacy*, *San Francisco, CA*, *IEEE Computer Society*, Washington, DC pp. 349-363.

Jang, C.S., Lee, D.G., Han, J.W. and Park, J.H. (2011), "Hybrid security protocol for wireless body area networks", *Wireless Communications and Mobile Computing*, Vol. 11 No. 2, pp. 277-288.

Jara, A.J., Zamora-Izquierdo, M.A. and Skarmeta, A.F. (2013), "Interconnection framework for mhealth and remote monitoring based on the internet of things", *IEEE Journal on Selected Areas in Communications*, Vol. 31 No. 9, pp. 47-65.

Jehangir, A. and de Groot, S.M.H. (2006), "A Security architecture for personal networks", *2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking Services*, *San Jose, CA*, *IEEE Computer Society*, Washington, DC, pp. 1-8.

Juels, A., Rivest, R.L. and Szydlo, M. (2003), "The blocker tag: selective blocking of RFID tags for consumer privacy", *Proceedings of the 10th ACM Conference on Computer and Communications Security*, *Washington, DC*, *CCS'03, ACM, New York, NY*, pp. 103-111.

Kang, S.Y., Lee, D.G. and Lee, I.Y. (2008), "A study on secure RFID mutual authentication scheme in pervasive computing environment", *Computer Communications*, Vol. 31 No. 18, pp. 4248-4254.

Kaps, J.P., Gaubatz, G. and Sunar, B. (2007), "Cryptography on a speck of dust", *Computer*, Vol. 40 No. 2, pp. 38-44.

Kelly, P., Marshall, S.J., Badland, H., Kerr, J., Oliver, M., Doherty, A.R. and Foster, C. (2013), "An ethical framework for automated, wearable cameras in health behavior research", *American Journal of Preventive Medicine*, Vol. 44 No. 3, pp. 314-319.

Keoh, S.L., Lupu, E. and Sloman, M. (2009), "Securing body sensor networks: Sensor association and key management", *IEEE International Conference on Pervasive Computing and Communication*, *Galveston, TX*, *IEEE Computer Society*, Washington, DC, pp. 1-6.

Kim, J., Baek, J. and Shon, T. (2011), "An efficient and scalable re-authentication protocol over wireless sensor network", *IEEE Transactions on Consumer Electronics*, Vol. 57 No. 2, pp. 516-522.

Kim, S.H., Ko, H.G., Ko, I.Y. and Choi, D. (2015), "Effects of contextual properties on users' privacy preferences in mobile computing environments", *The 13th IEEE International Symposium on Parallel and Distributed Processing with Applications*, *Helsinki, Finland*, *IEEE Computer Society*, Washington, DC, Vol. 1, pp. 507-514.

Kindberg, T., Bevan, C., O'Neill, E., Mitchell, J., Grimmett, J. and Woodgate, D. (2009), "Authenticating ubiquitous services: a study of wireless hotspot access", *Proceedings of the 11th International Conference on Ubiquitous Computing*, *Orlando, FL*, *UbiComp'09, ACM, New York, NY*, pp. 115-124.

Kitchenham, B. and Brereton, P. (2013), "A systematic review of systematic review process research in software engineering", *Information and Software Technology*, Vol. 55 No. 12, pp. 2049-2075.

Kitchenham, B. and Charters, S. (2007), "Guidelines for performing systematic literature reviews in software engineering", *EBSE Technical Report*, Vol. 2 No. 3.

Kumar, V. and Madria, S. (2013), "PIP: privacy and integrity preserving data aggregation in wireless sensor networks", *IEEE 32nd International Symposium on Reliable Distributed Systems*, *Braga, Portugal*, *IEEE Computer Society*, Washignton, DC, pp. 10-19.

Kwon, O. (2010), "A pervasive P3P-based negotiation mechanism for privacy-aware pervasive e-commerce", *Decision Support Systems*, Vol. 50 No. 1, pp. 213-221.

Kwon, T. and Na, S. (2014), "TinyLock: affordable defense against smudge attacks on smartphone pattern lock systems", *Computers & Security*, Vol. 42, pp. 137-150.

Lagesse, B. and Kumar, M. (2008), "A novel utility and game-theoretic based security mechanism for mobile P2P systems", *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, *Hong Kong*, *IEEE Computer Society*, *Washignton, DC*, pp. 486-491.

Lam, K.Y., Chung, S.L., Gu, M. and Sun, J.G. (2003), "Lightweight security for mobile commerce transactions", *Computer Communications*, Vol. 26 No. 18, pp. 2052-2060.

Le, X.H., Lee, S., Lee, Y.K., Lee, H., Khalid, M. and Sankar, R. (2010), "Activity-oriented access control to ubiquitous hospital information and services", *Information Sciences*, Vol. 180 No. 16, pp. 2979-2990.

Lee, D., Jang, H.S. and Kim, K.C. (2011), "A lightweight protocol based on the ssl protocol for handheld devices", *International Conference on Information Science and Applications*, *Jeju Island, South Korea*, *IEEE Computer Society*, Washignton, DC, pp. 1-4.

Lee, K.D. and Vasilakos, A.V. (2011), "Access stratum resource management for reliable u-healthcare service in LTE networks", *Wireless Networks*, Vol. 17 No. 7, pp. 1667-1678.

Lee, Y. and Kwon, O. (2010), "An index-based privacy preserving service trigger in context-aware computing environments", *Expert Systems with Applications*, Vol. 37 No. 7, pp. 5192-5200.

Lei, M., Xiao, Y., Vrbsky, S.V. and Li, C.C. (2008), "Virtual password using random linear functions for on-line services, ATM machines, and pervasive computing", *Computer Communications*, Vol. 31 No. 18, pp. 4367-4375.

Leitner, M. and Rinderle-Ma, S. (2014), "A systematic review on security in process-aware information systems: constitution, challenges, and future directions", *Information and Software Technology*, Vol. 56 No. 3, pp. 273-293.

Leung, M.K.H., Fong, A.C.M. and Hui, S.C. (2007), "Palmprint verification for controlling access to shared computing resources", *IEEE Pervasive Computing*, Vol. 6 No. 4, pp. 40-47.

Li, C., Zhang, Y. and Duan, L. (2008), "Establishing a trusted architecture on pervasive terminals for securing context processing", *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, *Hong Kong*, *IEEE Computer Society*, Washignton, DC, pp. 639-644.

Li, C.T., Lee, C.C. and Weng, C.Y. (2013a), "An extended chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments", *Nonlinear Dynamics*, Vol. 74 No. 4, pp. 1133-1143.

Li, M., Yu, S., Guttman, J.D., Lou, W. and Ren, K. (2013b), "Secure Ad Hoc trust initialization and key management in wireless body area networks", *ACM Transactions on Sensor Networks*, Vol. 9 No. 2, pp. 18:1-18:35.

Li, Q. and Cao, G. (2013), "providing privacy-aware incentives for mobile sensing", *IEEE International Conference on Pervasive Computing and Communications*, *San Diego, CA*, *IEEE Computer Society*, Washignton, DC, pp. 76-84.

Liang, X., Xiong, N., Yang, L.T., Zhang, H. and Park, J.H. (2008), "A compensation scheme of fingerprint distortion using combined radial basis function model for ubiquitous services", *Computer Communications*, Vol. 31 No. 18, pp. 4360-4366.

Liu, H., Ning, H., Zhang, Y., He, D., Xiong, Q. and Yang, L.T. (2013), "Grouping-proofs-based authentication protocol for distributed RFID systems", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 24 No. 7, pp. 1321-1330.

Liu, J. and Issarny, V. (2006), "an incentive compatible reputation mechanism for ubiquitous computing environments", *Privacy, Security and Trust, Vol. 380 of ACM International Conference Proceeding Series*, ACM, Oshawa, Ontario, pp. 1-36.

Liu, J. and Xiao, Y. (2011), "Temporal Accountability and anonymity in medical sensor networks", *Mobile Networks and Applications*, Vol. 16 No. 6, pp. 695-712.

Liu, J.K., Yuen, T.H., Au, M.H. and Susilo, W. (2014), "Improvements on an authentication scheme for vehicular sensor networks", *Expert Systems with Applications*, Vol. 41 No. 5, pp. 2559-2564.

López, G., Cánovas, O., Gómez, A.F., Jiménez, J.D. and Marín, R. (2007), "A network access control approach based on the AAA architecture and authorization attributes", *Journal of Network and Computer Applications*, Vol. 30 No. 3, pp. 900-919.

Lufei, H., Shi, W. and Chaudhary, V. (2008), "Adaptive secure access to remote services in mobile environments", *IEEE Transactions on Services Computing*, Vol. 1 No. 1, pp. 49-61.

Luo, H., Kong, J., Member, S., Zerfos, P., Lu, S. and Zhang, L. (2004), "URSA: ubiquitous and robust access control for mobile Ad Hoc networks", *IEEE/ACM Transactions on Networking*, Vol. 12 No. 6, pp. 1049-1063.

Ma, X., Pang, H. and Tan, K.-L. (2006), "Masking page reference patterns in encryption databases on untrusted storage", *Data & Knowledge Engineering*, Vol. 58 No. 3, pp. 466-483.

Mahdavi-Hezavehi, S., Galster, M. and Avgeriou, P. (2013), "Variability in quality attributes of service-based software systems: a systematic literature review", *Information and Software Technology*, Vol. 55 No. 2, pp. 320-343.

Malasri, K. and Wang, L. (2009), "Design and implementation of a secure wireless mote-based medical sensor network", *Sensors*, Vol. 9 No. 8, pp. 6273-6297.

Manweiler, J., Scudellari, R. and Cox, L.P. (2009), "SMILE: Encounter-based Trust for Mobile Social Services", *Proceedings of the 16th ACM Conference on Computer and Communications Security*, *Chicago, IL*, *CCS'09, ACM*, *New York, NY*, pp. 246-255.

Mathur, S., Trappe, W., Mandayam, N., Ye, C. and Reznik, A. (2008), "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel", *Proceedings of the 14th ACM*

International Conference on Mobile Computing and Networking, *San Francisco, CA*, *ACM, New York, NY*, pp. 128-139.

Mayer, P. and Volkamer, M. (2015), "Secure and efficient key derivation in portfolio authentication schemes using Blakley Secret sharing", *Proceedings of the 31st Annual Computer Security Applications Conference*, *Los Angeles, CA*, ACM, New York, NY, pp. 431-440.

Mayrhofer, R., Fuss, J. and Ion, I. (2013), "UACAP: a unified auxiliary channel authentication protocol", *IEEE Transactions on Mobile Computing*, Vol. 12 No. 4, pp. 710-721.

Mayrhofer, R., Gellersen, H. and Hazas, M. (2007), "Security by spatial reference: using relative positioning to authenticate devices for spontaneous interaction", *Proceedings of the 9th International Conference on Ubiquitous Computing*, *UbiComp '07, Springer-Verlag*, *Berlin*, pp. 199-216.

Mellado, D., Blanco, C., Sánchez, L.E. and Fernández-Medina, E. (2010), "A systematic review of security requirements engineering", *Computer Standards & Interfaces*, Vol. 32 No. 4, pp. 153-165.

Meyerowitz, J. and Roy Choudhury, R. (2009), "Hiding stars with fireworks: location privacy through camouflage", *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, *Beijing, China*, *ACM, New York, NY*, pp. 345-356.

Miettinen, M., Asokan, N., Nguyen, T.D., Sadeghi, A.R. and Sobhani, M. (2014), "Context-based zero-interaction pairing and key evolution for advanced personal devices", *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, *Scottsdale, AZ*, *ACM, New York, NY*, pp. 880-891.

Mihovska, A. and Prasad, N.R. (2007), "Adaptive security architecture based on EC-MQV algorithm in Personal Network (PN)", *2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, *Philadelphia, PA*, *IEEE Computer Society*, *Washington, DC*, pp. 1-5.

Minami, K. and Kotz, D. (2005), "Secure context-sensitive authorization", *Pervasive and Mobile Computing*, Vol. 1 No. 1, pp. 123-156.

Mo, C.M. and Wei, V. (2001), "A taxonomy for attacks on mobile agent", *Proceedings of the International Conference on Trends in Communications*, *Fei Stu Tratislava, Slovakia*, *IEEE Computer Society*, Washington, DC, pp. 385-388.

Moessner, M. and Khan, G.N. (2012), "Secure authentication scheme for passive C1G2 RFID tags", *Computer Networks*, Vol. 56 No. 1, pp. 273-286.

Molla, M.M., Madiraju, P., Malladi, S. and Ahamed, S.I. (2009), "An XML based access control architecture for pervasive computing", *IEEE International Conference on Pervasive Computing and Communications*, *Galveston, TX*, *IEEE Computer Society*, Washington, DC, pp. 1-6.

Mondal, A. and Kitsuregawa, M. (2006), "Privacy, security and trust in P2P environments: a perspective", *Proceedings of 17th International Conference on Database and Expert Systems Applications*, *Porto, Portugal*, *IEEE Computer Society*, *Washington, DC*, pp. 682-686.

Moon, J.S. and Lee, I.Y. (2011), "An AAA scheme using ID-based ticket with anonymity in future mobile communication", *Computer Communications*, Vol. 34 No. 3, pp. 295-304.

Moschetta, E., Antunes, R.S. and Barcellos, M.P. (2010), "Flexible and secure service discovery in ubiquitous computing", *Journal of Network and Computer Applications*, Vol. 33 No. 2, pp. 128-140.

Narain, A., Feamster, N. and Snoeren, A.C. (2014), "Deniable Liaisons", *ACM Conference on Computer and Communications Security*, *Scottsdale, AZ*, ACM, New York, NY, pp. 525-536.

Nguyen, P.H., Klein, J., Kramer, M.E. and Traon, Y.L. (2013), "A systematic review of model-driven security", *Proceedings of the 2013 20th Asia-Pacific Software Engineering Conference, Bangkok, Thailand, IEEE Computer Society, Washington, DC*.

Nicholson, A., Corner, M. and Noble, B. (2006), "Mobile device security using transient authentication", *IEEE Transactions on Mobile Computing*, Vol. 5 No. 11, pp. 1489-1502.

Ning, H., Liu, H. and Yang, L.T. (2015), "Aggregated-proof based hierarchical authentication scheme for the internet of things", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 26 No. 3, pp. 657-667.

Oh, S. (2008), "New role-based access control in ubiquitous e-business environment", *Journal of Intelligent Manufacturing*, Vol. 21 No. 5, pp. 607-612.

Omoronyia, I., Pasquale, L., Salehie, M., Cavallaro, L., Doherty, G. and Nuseibeh, B. (2012), "Caprice: a tool for engineering adaptive privacy", *Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering, Essen, Germany, ACM Press, New York, NY*, p. 354.

Pallapa, G., Di Francescoy, M. and Das, S.K. (2012), "Adaptive and context-aware privacy preservation schemes exploiting user interactions in pervasive environments", *2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, San Francisco, CA, IEEE Computer Society*, Washington, DC, pp. 1-6.

Pallapa, G., Kumar, M. and Das, S. (2007), "Privacy infusion in ubiquitous computing", *Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking Services, Philadelphia, PA, IEEE Computer Society*, Washington, DC, pp. 1-8.

Pandit, A., Polina, P., Kumar, A. and Xie, B. (2014), "CAPPA: context aware privacy protecting advertising: an extension to clopro framework", *IEEE International Conference on Services Computing, Anchorage, AK, IEEE Computer Society*, Washington, DC, pp. 805-812.

Park, H.A., Hong, J.W., Park, J.H., Zhan, J. and Lee, D.H. (2010), "Combined authentication-based multilevel access control in mobile application for dailylifeservice", *IEEE Transactions on Mobile Computing* Vol. 9 No. 6, pp. 824-837.

Park, K.W., Lim, S.S. and Park, K.H. (2008), "Computationally efficient PKI-based single sign-on protocol, PKASSO for mobile devices", *IEEE Transactions on Computers*, Vol. 57 No. 6, pp. 821-834.

Park, M.W., Choi, Y.H., Eom, J.H. and Chung, T.M. (2014), "Dangerous Wi-Fi access point: Attacks to benign smartphone applications", *Personal and Ubiquitous Computing*, Vol. 18 No. 6, pp. 1373-1386.

Patwardhan, A., Parker, J., Joshi, A., Iorga, M. and Karygiannis, T. (2005), "Secure routing and intrusion detection in Ad Hoc networks", *Third IEEE International Conference on Pervasive Computing and Communications, Kauai, HI, IEEE Computer Society*, Washington, DC, pp. 191-199.

Pietro, R.D. and Mancini, L.V. (2003), "Security and privacy issues of handheld and wearable wireless devices", *ACM Communications*, Vol. 46 No. 9, pp. 74-79.

Pingley, A., Yu, W., Zhang, N., Fu, X. and Zhao, W. (2012), "A context-aware scheme for privacy-preserving location-based services", *Computer Networks*, Vol. 56 No. 11, pp. 2551-2568.

Popa, R.A., Blumberg, A.J., Balakrishnan, H. and Li, F.H. (2011), "privacy and accountability for location-based aggregate statistics", *Proceedings of the 18th ACM Conference on Computer and Communications Security, Chicago, IL*, ACM, New York, NY, pp. 653-666.

Preda, S., Cuppens, F., Cuppens-Boulahia, N., Garcia-Alfaro, J. and Toutain, L. (2011), "Dynamic deployment of context-aware access control policies for constrained security devices", *Journal of Systems and Software*, Vol. 84 No. 7, pp. 1144-1159.

Qiu, M., Zhang, L., Ming, Z., Chen, Z., Qin, X. and Yang, L.T. (2013), "Security-aware optimization for ubiquitous computing systems with SEAT graph approach", *Journal of Computer and System Sciences*, Vol. 79 No. 5, pp. 518-529.

Qureshi, B., Min, G. and Kouvatsos, D. (2012), "A distributed reputation and trust management scheme for mobile peer-to-peer networks", *Computer Communications*, Vol. 35 No. 5, pp. 608-618.

Radjenović, D., Heričko, M., Torkar, R. and Živković, A. (2013), "Software fault prediction metrics: a systematic literature review", *Information and Software Technology*, Vol. 55 No. 8, pp. 1397-1418.

Rahman, M., Carbunar, B. and Topkara, U. (2014), "SensCrypt: a secure protocol for managing low power fitness trackers", *IEEE 22nd International Conference on Network Protocols*, *North Carolina*, *IEEE Computer Society*, Washington, DC, pp. 191-196.

Rasmussen, K.B., Castelluccia, C., Heydt-Benjamin, T.S. and Capkun, S. (2009), "Proximity-based Access control for implantable medical devices", *Proceedings of the 16th ACM Conference on Computer and Communications Security*, *Chicago, IL*, ACM, New York, NY, pp. 410-419.

Ray, I., Ray, I. and Chakraborty, S. (2009), "An interoperable context sensitive model of trust", *Journal of Intelligent Information Systems*, Vol. 32 No. 1, pp. 75-104.

Ren, K., Lou, W., Kim, K., Deng, R. and Member, S. (2006), "A novel privacy preserving authentication and access control scheme for pervasive computing environments", *IEEE Transactions on Vehicular Technology*, Vol. 55 No. 4, pp. 1373-1384.

Riaz, R., Naureen, A., Akram, A., Akbar, A.H., Kim, K.H. and Farooq Ahmed, H. (2008), "A unified security framework with three key management schemes for wireless sensor networks", *Computer Communications*, Vol. 31 No. 18, pp. 4269-4280.

Riedl, P., Mayrhofer, R., Möller, A., Kranz, M., Lettner, F., Holzmann, C. and Koelle, M. (2015), "Only play in your comfort zone: interaction methods for improving security awareness on mobile devices", *Personal and Ubiquitous Computing*, Vol. 19 No. 5, pp. 941-954.

Rocha, B.P., Costa, D.N., Moreira, R.A., Rezende, C.G., Loureiro, A.A. and Boukerche, A. (2010), "Adaptive security protocol selection for mobile computing", *Journal of Network and Computer Applications* Vol. 33 No. 5, pp. 569-587.

Rohrer, F., Zhang, Y., Chitkushev, L. and Zlateva, T. (2013), "DR-BACA: dynamic role based access control for android", *Proceedings of the 29th Annual Conference on Computer Security Applications, New Orleans, LA*, *ACM, New York, NY*, pp. 299-308.

Safa, H., Artail, H. and Tabet, D. (2010), "A cluster-based trust-aware routing protocol for mobile Ad Hoc networks", *Wireless Networks*, Vol. 16 No. 4, pp. 969-984.

Safkhani, M., Peris-Lopez, P., Hernandez-Castro, J. and Bagheri, N. (2014), "Cryptanalysis of the Cho et al. protocol: a hash-based RFID tag mutual authentication protocol", *Journal of Computational and Applied Mathematics*, Vol. 259 No. B, pp. 571-577.

Sandhu, R. and Samarati, P. (1996), "Authentication, access control, and audit", *ACM Computing Surveys*, Vol. 28 No. 1, pp. 241-243.

Santiago, I., Jiménez, l., Vara, J.M., de Castro, V., Bollati, V.A. and Marcos, E. (2012), "Model-driven engineering as a new landscape for traceability management: a systematic literature review", *Information and Software Technology*, Vol. 54 No. 12, pp. 1340-1356.

Saxena, N., Uddin, M., Voris, J. and Asokan, N. (2011), "Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal rfid tags", *IEEE International Conference on Pervasive Computing and Communications*, *Seattle*, *IEEE Computer Society*, Washington, DC, pp. 181-188.

Schaub, F., Kónings, B., Dietzel, S., Weber, M. and Kargl, F. (2012), "Privacy context model for dynamic privacy adaptation in ubiquitous computing", *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, *Pittsburgh, PA*, ACM, New York, NY, pp. 752-757.

Schaub, F., Konings, B. and Weber, M. (2015), "Context-adaptive privacy: leveraging context awareness to support privacy decision making", *IEEE Pervasive Computing*, Vol. 14 No. 1, pp. 34-43.

Schefer-Wenzl, S. and Strembeck, M. (2013), "Modelling context-aware RBAC models for mobile business processes", *International Journal of Wireless and Mobile Computing*, Vol. 6 No. 5, pp. 448-462.

Schneegass, S., Steimle, F., Bulling, A., Alt, F. and Schmidt, A. (2014), "smudgesafe: geometric image transformations for smudge-resistant user authentication", *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, *UbiComp '14, ACM*, *New York, NY*, pp. 775-786.

Seigneur, J.M. and Jensen, C.D. (2005), "The claim tool kit for ad hoc recognition of peer entities", *Science of Computer Programming*, Vol. 54 No. 1, pp. 49-71.

Shahzad, M., Liu, A.X. and Samuel, A. (2013), "secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it", *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*, *MobiCom '13, ACM*, *New York, NY*, pp. 39-50.

Shand, B., Dimmock, N. and Bacon, J. (2004), "Trust for ubiquitous, transparent collaboration", *Wireless Networks*, Vol. 10 No. 6, pp. 711-721.

Shi, Q., Zhang, N. and Llewellyn-Jones, D. (2012), "Efficient autonomous signature exchange on ubiquitous networks", *Journal of Network and Computer Applications*, Vol. 35 No. 6, pp. 1793-1806.

Shi, Q., Zhang, N., Merabti, M. and Askwith, R. (2011), "Achieving autonomous fair exchange in ubiquitous network settings", *Journal of Network and Computer Applications*, Vol. 34 No. 2, pp. 653-667.

Shokri, R., Theodorakopoulos, G., Troncoso, C., Hubaux, J.-P. and Le Boudec, J.-Y. (2012), "Protecting location privacy: optimal strategy against localization attacks", *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, *Raleigh, NC*, CCS'12, ACM, New York, NY, pp. 617-627.

Solanas, A. and Martínez-Ballesté, A. (2008), "A TTP-free protocol for location privacy in location-based services", *Computer Communications*, Vol. 31 No. 6, pp. 1181-1191.

Srinivasan, V., Stanković, J. and Whitehouse, K. (2008), "Protecting your daily in-home activity information from a wireless snooping attack", *Proceedings of the 10th International Conference on Ubiquitous Computing*, *Seoul, Korea*, *UbiComp'08, ACM*, *New York, NY*, pp. 202-211.

Strembeck, M. and Neumann, G. (2004), "An integrated approach to engineer and enforce context constraints in RBAC environments", *ACM Transactions on Information and System Security*, Vol. 7 No. 3.

Strembeck, M. and Rinderle-Ma, S. (2013), "Security and privacy in business processes: a posteriori analysis techniques", *IT – Information Technology*, Vol. 5 No. 6, pp. 247-253.

Studer, A., Passaro, T. and Bauer, L. (2011), "Don't bump, shake on it: the exploitation of a popular accelerometer-based smart phone exchange and its secure replacement", *Proceedings of the 27th Annual Computer Security Applications Conference*, *Orlando, FL*, ACM, *New York, NY*, pp. 333-342.

Su, C., Wang, G. and Sakurai, K. (2012), "Analysis and improvement of privacy-preserving frequent item protocol for accountable computation framework", *IEEE 11th International*

Conference on Trust, Security and Privacy in Computing and Communications, *Liverpool*, *IEEE Computer Society*, Washington, DC, pp. 1012-1017.

Subramanian, N., Yang, C. and Zhang, W. (2007), "Securing distributed data storage and retrieval in sensor networks", *Pervasive and Mobile Computing*, Vol. 3 No. 6, pp. 659-676.

Sun, B., Xiao, Y., Li, C.C., Chen, H.H. and Yang, T.A. (2008a), "Security co-existence of wireless sensor networks and RFID for pervasive computing", *Computer Communications*, Vol. 31 No. 18, pp. 4294-4303.

Sun, D.Z., Huai, J.P., Sun, J.Z., Zhang, J.W. and Feng, Z.Y. (2008b), "A new design of wearable token system for mobile device security", *IEEE Transactions on Consumer Electronics*, Vol. 54 No. 4, pp. 1784-1789.

Sun, H.M., He, B.Z., Chen, C.M., Wu, T.Y., Lin, C.H. and Wang, H. (2015), "A provable authenticated group key agreement protocol for mobile environment", *Information Sciences*, Vol. 321 (10 November), pp. 224-237, availabe at: www.sciencedirect.com/science/article/pii/S0020025515000754

Tan, Z. (2012), "A lightweight conditional privacy-preserving authentication and access control scheme for pervasive computing environments", *Journal of Network and Computer Applications*, Vol. 35 No. 6, pp. 1839-1846.

Tanenbaum, A.S. and van Steen, M. (2006), *Distributed Systems: Principles and Paradigms*, 2nd ed., Prentice Hall, Upper Saddle River, NJ.

Thomas, K., Bandara, A.K., Price, B.A. and Nuseibeh, B. (2014), "Distilling privacy requirements for mobile applications", *Proceedings of the 36th International Conference on Software Engineering*, *Hyderabad, India*, *ACM*, *New York, NY*, pp. 871-882.

Toahchoodee, M. and Ray, I. (2011), "On the formalization and analysis of a Spatio-temporal role-based access control model", *Journal of Computer Security*, Vol. 19 No. 3, pp. 399-452.

Toch, E. (2014), "Crowdsourcing privacy preferences in context-aware applications", *Personal and Ubiquitous Computing*, Vol. 18 No. 1, pp. 129-141.

Tschersich, M., Kahl, C., Heim, S., Crane, S., Bóttcher, K., Krontiris, I. and Rannenberg, K. (2011), "Towards privacy-enhanced mobile communities architecture, concepts and user trials", *Journal of Systems and Software*, Vol. 84 No. 11, pp. 1947-1960.

Undercoffer, J., Perich, F., Cedilnik, A., Kagal, L. and Joshi, A. (2003), "A secure infrastructure for service discovery and access in pervasive computing", *Mobile Networks and Applications*, Vol. 8 No. 2, pp. 113-125.

Vahedi, E., Shah-Mansouri, V., Wong, V., Blake, I. and Ward, R. (2011), "Probabilistic analysis of blocking attack in RFID systems", *IEEE Transactions on Information Forensics and Security*, Vol. 6 No. 3, pp. 803-817.

Venkatasubramanian, K.K. and Gupta, S.K.S. (2010), "Physiological value-based efficient usable security solutions for body sensor networks", *ACM Transactions on Sensor Networks*, Vol. 6 No. 4, pp. 1-36.

Wang, D. and Wang, P. (2014), "On the anonymity of two-factor authentication schemes for wireless sensor networks: attacks, principle and solutions", *Computer Networks*, Vol. 73 (14 November), pp. 41-57, availabe at: www.sciencedirect.com/science/article/pii/S1389128614002643

Wang, H., Zhang, Y. and Cao, J. (2008), "Access control management for ubiquitous computing", *Future Generation Computer Systems*, Vol. 24 No. 8, pp. 870-878.

Wang, N.C. and Fang, S.Z. (2007), "A hierarchical key management scheme for secure group communications in mobile ad hoc networks", *Journal of Systems and Software*, Vol. 80 No. 10, pp. 1667-1677.

Wang, O.X., Cheng, W., Mohapatra, P., Abdelzaher, T., Wang, X., Cheng, W., Mohapatra, P. and Abdelzaher, T. (2013), "ARTSense: anonymous reputation and trust in participatory sensing", *2013 Proceedings of IEEE International Conference on Computer Communications*, *Turin, Italy*, *IEEE*, *Washington, DC*, pp. 2517-2525.

Wang, R.C., Juang, W.S. and Lei, C.L. (2011), "Robust authentication and key agreement scheme preserving the privacy of secret key", *Computer Communications*, Vol. 34 No. 3, pp. 274-280.

Wang, R., Xing, L., Wang, X. and Chen, S. (2013), "unauthorized origin crossing on mobile platforms: threats and mitigation", *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, *Berlin, Germany*, *CCS'13, ACM*, *New York, NY*, pp. 635-646.

Wang, S.C. and Yan, K.Q. (2006), "Byzantine agreement under dual failure mobile network", *Computer Standards & Interfaces*, Vol. 28 No. 4, pp. 475-492.

Wang, W. and Zhang, Q. (2015), "Toward long-term quality of protection in mobile networks: a context-aware perspective", *IEEE Wireless Communications*, Vol. 22 No. 4, pp. 34-40.

Want, R. (2014), "The Power of smartphones", *IEEE Pervasive Computing*, Vol. 13 No. 3, pp. 76-79.

Webster, J. and Watson, R. (2002), "Analyzing the past to prepare for the future: writing a literature review", *MIS Quarterly*, Vol. 26 No. 2, pp. 13-23.

Weippl, E. and Essmayr, W. (2003), "Personal trusted devices for web services: revisiting multilevel security", *Mobile Networks and Applications*, Vol. 8 No. 2, pp. 151-157.

Weiser, M. (1991), "The computer for the 21st century", *Scientific American*, Vol. 265 No. 3, pp. 66-75.

Wu, X., Yang, P., Tang, S., Zheng, X. and Xiong, Y. (2015), "Privacy preserving RSS map generation for a crowdsensing network", *IEEE Wireless Communications*, Vol. 22 No. 4, pp. 42-48.

Wu, Z., Ou, Y. and Liu, Y. (2011), "A taxonomy of network and computer attacks based on responses", *International Conference on Information Technology, Computer Engineering and Management Sciences (ICM'11)*, *Nanjing, Jiangsu*, Vol. 1, 24-25 September 2011, pp. 26-29.

Xie, J. and Knijnenburg, B.P. (2014), "Location sharing preference: analysis and personalized recommendation", *Proceedings of the International Conference on Intelligent User Interfaces*, *Haifa, Israel*, pp. 189-198.

Xu, G., Wu, Q., Daneshmand, M., Liu, Y. and Wang, M. (2015), "A data privacy protective mechanism for wireless body area networks", *Wireless Communications and Mobile Computing*, pp. 1-13. doi: 10.1002/wcm.2649. availabe at: http://onlinelibrary.wiley.com/doi/10.1002/wcm.2649/abstract

Xu, J., Tang, X., Hu, H. and Du, J. (2010), "Privacy-conscious location-based queries in mobile environments", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 21 No. 3, pp. 313-326.

Yan, Z., Zhang, P. and Deng, R.H. (2012), "TruBeRepec: a trust-behavior-based reputation and recommender system for mobile applications", *Personal and Ubiquitous Computing*, Vol. 16 No. 6, pp. 485-506.

Yao, Q., Qi, Y., Han, J., Zhao, J., Li, X. and Liu, Y. (2009), "Randomizing RFID private authentication", *IEEE International Conference on Pervasive Computing and Communications*, *Galveston, TX*, *IEEE Computer Society*, Washington, DC, pp. 1-10.

Yao, X., Han, X. and Du, X. (2014), "A light-weight certificate-less public key cryptography scheme based on ECC", *2014 23rd International Conference on Computer Communication and Networks*, *Shanghai, China*, *IEEE Computer Society*, Washington, DC, pp. 1-8.

Yau, S.S., Huang, D., Gong, H. and Yao, Y. (2006), "Support for situation awareness in trustworthy ubiquitous computing application software", *Journal of Software Practice and Engineering*, Vol. 36 No. 9, pp. 893-921.

Ye, T., Moynagh, B., Albatal, R. and Gurrin, C. (2014), "Negative faceblurring: a privacy-by-design approach to visual lifelogging with google glass", *Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management*, *Shanghai, China*, *CIKM '14, ACM*, *New York, NY*, pp. 2036-2038.

Yoon, E.J., Yoo, K.Y., Kim, C., Hong, Y.S., Jo, M. and Chen, H.H. (2010), "A secure and efficient SIP authentication scheme for converged VoIP networks", *Computer Communications*, Vol. 33 No. 14, pp. 1674-1681.

Yu, T., Winslett, M. and Seamons, K. (2003), "Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation", *ACM Transactions on Information and System Security*, Vol. 6 No. 1, pp. 1-42.

Zachary, J. and Brooks, R. (2003), "Bidirectional mobile code trust management using tamper resistant hardware", *Mobile Networks and Applications*, Vol. 8 No. 2, pp. 137-143.

Zhang, Y., Lee, W. and Huang, Y.-A. (2003), "Intrusion detection techniques for mobile wireless networks", *Wireless Networks* Vol. 9 No. 5, pp. 545-556.

Zhong, S. and Richard Yang, Y. (2006), "Verifiable distributed oblivious transfer and mobile agent security", *Mobile Networks and Applications*, Vol. 11 No. 2, pp. 201-210.

Zhou, B., Shi, Q. and Merabti, M. (2008), "Balancing intrusion detection resources in ubiquitous computing networks", *Computer Communications*, Vol. 31 No. 15, pp. 3643-3653.

Zhu, F., Mutka, M. and Ni, L. (2003), "Splendor: a secure, private, and location-aware service discovery protocol supporting mobile services", *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications*, *Dallas-Forth Worth, TX*, *IEEE Computer Society*, *Washington, DC*, pp. 235-242.

Zhu, F., Mutka, M.W. and Ni, L.M. (2006a), "A private, secure, and user-centric information exposure model for service discovery protocols", *IEEE Transactions on Mobile Computing*, Vol. 5 No. 4, pp. 418-429.

Zhu, F.W., Mutka, M.W. and Ni, L.M. (2006b), "The master key: a private authentication approach for pervasive computing environments", *International Conference on Pervasive Computing and Communications*, *Sydney, Australia, 2006*, *IEEE Computer Society*, Washington, DC, pp. 212-221.

Zhu, F.W., Zhu, W., Mutka, M.W. and Ni, L.M. (2007), "Private and secure service discovery via progressive and probabilistic exposure", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 18 No. 11, pp. 1565-1577.

Zhu, F., Carpenter, S., Kulkarni, A., Chidambaram, C. and Pathak, S. (2009), "Understanding and minimizing identity exposure in ubiquitous computing environments", *6th Annual International Conference on Mobile and Ubiquitous Systems: Networking Services*, *Toronto, Canada*, *IEEE Computer Society*, Washington, DC, pp. 1-10.

Corresponding author
Ema Kusen can be contacted at: ekusen@wu.ac.at