"An Analysis upon Various Security and Privacy in Wireless Sensor Networks: A Case Study of Pervasive Computing"

Nandita Argal Shrivastava

Research Scholar, Mahatma Gandhi University, Meghalaya

Abstract – Wireless communication continues to make in-roads into many facets of our society and gradually becomes more and more ubiquitous. While, in the past, wireless communication (as well as mobility) was largely limited to first and last transmission hops, today's wireless networks are starting to offer purely wireless, often mobile, and even opportunistically connected operation. The purpose of this paper is to examine security and privacy issues in some new and emerging types of wireless networks and identify directions for future research.

Developments in pervasive computing introduced a new world of computing where networked processors embedded and distributed in everyday objects communicating with each other over wireless links. Computers in such environments work in the background while establishing connections among them dynamically and hence will be less visible and intrusive. Such a vision raises questions about how to manage issues like privacy, trust and identity in those environments. In this paper, we review the technical challenges that face pervasive computing environments in relation to each of these issues. We then present a number of security related considerations and use them as a basis for comparison between pervasive and traditional computing. We will argue that these considerations pose particular concerns and challenges to the design and implementation of pervasive environments which are different to those usually found in traditional computing environments. To address these concerns and challenges, further research is needed. We will present a number of directions and topics for possible future research with respect to each of the three issues.

Million of wireless device users are ever on the move, becoming more dependent on their PDAs, smart phones, and other handheld devices. With the advancement of pervasive computing, new and unique capabilities are available to aid mobile societies. The wireless nature of these devices has fostered a new era of mobility. Thousands of pervasive devices are able to arbitrarily join and leave a network, creating a nomadic environment known as a pervasive ad hoc network. However, mobile devices have vulnerabilities, and some are proving to be challenging.

Security in pervasive computing is the most critical challenge. Security is needed to ensure exact and accurate confidentiality, integrity, authentication, and access control, to name a few. Security for mobile devices, though still in its infancy, has drawn the attention of various researchers.

As pervasive devices become incorporated in our day-to-day lives, security will increasingly becoming a common concern for all users - - though for most it will be an afterthought, like many other computing functions. The usability and expansion of pervasive computing applications depends greatly on the security and reliability provided by the applications. At this critical juncture, security research is growing.

----------♦----------

INTRODUCTION

The importance of security has been supported with thousands of recent surveys, and it is far beyond an afterthought nowadays. Network security has topped the priority list of 47% respondents in the Networking Report Card survey by SearchNetworking.com. Closely related to security are issues of corporate reputation, competitive

position, and monetary gain. A study by eMarketer indicates an average loss of $10 billion per year due to infractions in computer security. Microsoft has defined security as “The protection of information assets through the use of technology, processes, and training”. Wikipedia defines security as a “... platform, designed so that agents (users or programs) can only perform actions that have been allowed. This involves specifying and implementing a security policy”. CIA (Confidentiality, Integrity, and Availability) is the term commonly used to describe the required characteristics of security.

Confidentiality ensures information is not exposed to any unauthorized user. Integrity indicates information has not been altered or falsified by an unauthorized user. Availability denotes information is readily available when required.

Security in pervasive computing has been termed pervasive security. Though pervasive security includes all the characteristics and requirements of computer security, it introduces some novel vulnerabilities and security rifts due to a few unique characteristics of pervasive computing.

Pervasive computing has been defined as “Numerous, casually accessible, often invisible computing devices, frequently mobile or embedded in the environment, connected to an increasingly ubiquitous network infrastructure composed of a wired core and wireless edges”. Pervasive computing is the brain child of Weiser. This vision embeds computation into the environment and ensures transparent interaction of these computational devices with the users. It can be considered the opposite of virtual reality.

Pervasive computing is proving its usability and scope in almost every aspect nowadays. The availability of, and tremendous improvement in, pervasive devices including PDAs, smart phones, tiny sensors, etc., have made this next generation of computing technology suitable for many situations in places like the home, hospital, or battlefield. Recent surveys like indicate 50% of physicians used PDAs in 2002, and they were used by approximately 50% of people in the U.S., indicating the tremendous growth in the use handheld computers and pervasive devices. To overcome several constraints related to capability, pervasive devices actually form a collaborative space where devices are highly inter-connected and mutually cooperative; this becomes the key to success and leads to sharing of resources and information. The downside is that this provides opportunities for theft and hacking. The characteristics of pervasive scenarios sometimes seem to provide an open invitation for active and passive eavesdroppers. In order to increase the usability and spectrum range of scenarios that can benefit from this technique, pervasive computing has yet to prove it is up to solving the security challenges.

Wireless communication plays an increasingly important role in many spheres of our society. It has become an essential (and, in some cases, ubiquitous) means of communication.

The number of wireless phones exceeded that of wired ones and soon there will be more smart-phones than PCs. Wireless LANs are commonplace; they are being routinely used at home, work, and many other public venues, such as cafes and malls. Most current wireless networks are employed in the context of personal communication where end-users are human beings. In such networks, wireless communication typically occurs only at the first and last hops. For example, cell phones communicate indirectly, via base stations that are, in turn, connected to wire networks. Similarly, wireless LANs are usually connected to wire access points that are, in turn, connected to larger wired LANs and/or Internet Service Providers (ISPs). We refer to these networks collectively as: infrastructure-based wireless networks. Since communications originating (or terminating) in cell-phones or WiFi-capable devices usually transit a fixed network infrastructure, few (if any) new security and privacy issues arise from such networks.

Recent advances in technology have motivated new application domains for wireless networks. For example, wireless sensor networks (WSNs) are used for environmental monitoring in both civilian and military settings. Vehicular ad hoc networks (VANETs) promise safer roads and improved driving experience, while disruption-tolerant networks (DTNs) bring low-cost best-effort connectivity to challenged environments with little or no infrastructure. At the same time, there has been a surge of interest in body-area networks (BANs) with envisaged applications in military, law enforcement, sports and medical domains. These emerging wireless networks extend the network function beyond purely personal communication and potentially offer a world of truly ubiquitous computing.

One of their distinctive features is the lack of (or non-reliance on) any wired or fixed infrastructure. Nodes communicate either directly or via peers, instead of using infrastructure elements, such as base stations or access points. Since nodes themselves are responsible for forwarding messages, they play an increasingly active role in networking mechanisms. Also, network formation does not need to follow some pre-defined fashion: nodes might move independently, and the network topology can be formed on an ad hoc basis.

The wide development and integration of sensing, communication and computing have led to the development of pervasive computing, which offers the distribution of computational services within environments where people live, work or socialize. There are advantages in implementing such environments such as, moving interaction with computers out of a person's central focus and into the user's peripheral attention where they can be used subconsciously. Another advantage of pervasive computing environments is to make life more comfortable by providing device mobility and a digital infrastructure that has the ability to provide useful services to people in the environment, when and where they need them. It is common that a user in these environments will maintain various connections with many smart devices regardless of the hardware specifications or the software restrictions. Such devices collectively participate in the provision of the required service without the conscious or explicit knowledge of the user as stated by Weiser . However, at the same time pervasive computing presents many risks and security related issues that were not previously encountered in more traditional computing environments. In particular, issues such as privacy, trust and identity become more challenging to the designers of such environments. Designing secure pervasive environments requires the system to reliably and confidently identify the user who wishes to access the environment's resources. It is also important to appreciate the risks involved in establishing and verifying the identity of users in such environments. Privacy is also important as users need to be confident that their personal information is not used in a way that they do not approve of. Privacy in such environments is particularly important as the system needs to be protective of the users' data and perceived by the user to be that way. Trust within such systems presents another challenge due to the fact that trust relationships are much more complex than those normally found in more traditional environments. In pervasive environments it is very difficult to define the boundary of trust domains, which is important when defining trust relationships. Trust is also important when users often cross such boundaries and therefore normal authentication procedures may not be practical. This paper reviews the technical advances and challenges with respect to each of these issues within pervasive computing.

WIRELESS SENSOR NETWORKS

The original motivation for wireless sensor network (WSN) research stemmed from the vision of Smart Dust in the late 1990-s . This entailed an integrated computing, communication and sensing platform consisting of small devices, enabling applications such as dense environmental monitoring and smart home/office. Since then, progress in WSN research has yielded major advances toward the original Smart Dust vision.

A typical WSN encountered in the research literature consists of a large number of small, cheap and resource constrained sensors and a few base stations or sinks. In most WSN settings, sensors collect data from the environment and forward the collected data hop-by-hop to the sink. A sink is a more powerful entity. It may serve as a gateway to another network, a data processing or storage center, or an access point for human interface. WSN deployment can be ad hoc, e.g., sensors might be air-dropped over a designated area without exact pre-positioning. Because of their allegedly easy deployment, WSNs appeal to a wide range of applications in military, environmental, disaster relief, and homeland security domains.

Security has always been considered to be an important factor in the eventual success of WSNs, especially, in security sensitive applications such as military or homeland security. A flurry of research results appeared in early 2000-s, addressing a number of WSN security issues, including key management, secure routing, DoS attacks, and clone detection. Due to sensor resource constraints, many prior results involved impressive cryptographic contortions aimed at miniaturizations of security functionalities (e.g., key management) that are not specific to WSNs. However, some research addressed issues unique to WSNs, e.g., clone detection and certain DoS attacks. Also, there has been some notable research in application-specific WSN security, such as secure aggregation and secure statistical sampling.

Despite oft-claimed successes, the current range of deployed WSN applications is still far from the ubiquitous and autonomic sensing and computing platform envisaged by Smart Dust. First, although WSN deployment can be ad hoc, the underlying network model is usually not infrastructure-less and information flow is funneled at the sink. The sink is a powerful entity that plays an important security and privacy role for the entire network. Indeed, most WSN security efforts have assumed continuous presence of the sink. Once a sink receives data collected by individual sensors, it takes care of storage of, and access control to, that data. (In the remainder of this paper, we use the term "sink" to collectively denote all management and collection entities, including mobile collectors and static sinks). Also, most WSNs suffer from limited network life span due to finite-capacity sensor batteries. Once the battery runs out of power, the sensor dies. This makes WSNs ill-suited for settings where replacing sensors or recharging sensor batteries is difficult or impossible.

SECURITY MODEL

Several works exist where agent-based applications have proved to be promising. Some projects have come up with different security issues in Mobile Agent System. In order to prevent malicious use , it is suggested that agents should communicate only with trusted and authenticated nodes. Hence several trust models appear which we discuss later. A scenario is described where the credibility of a node will vary depending on the agents' interaction with that node.

Describes a method to defend against several types of attacks and to restrict an agent from occupying a specific resource for a long time.

In a recent interesting study, the researchers proposed a security model named 'QED' (Quarantine, Examination and Decontamination). QED was designed to provide several aspects of security which are well known for fixed infrastructures within the realm of a pervasive computing environment – virus scan, firewall, intrusion detection, and update and patch management. As part of an examination phase, the QED model incorporates a fixed infrastructure based security nodes which can provide updated virus scanners and patches. These nodes are seeking permission to enter in the network, and QED can push the nodes to receive the updated information as a precondition for entrance. The Quarantine phase performs the isolation of clients to ensure that they meet the local integrity constraints. On the other hand, the device can also decide not to access some of the available services of the network due to conflict with its own access policy.

Clients are checked for potential vulnerabilities and malicious code in the Examination period. The probable investigations include virus scans and memory scans. During an active examination, clients need to go through all the defined investigations, whereas in passive investigation the system acknowledges a digital certificate that ensures that the corresponding client have passed similar checks in the previous environment. The Decontamination phase deals with removing vulnerabilities from the examined clients. Several tools can be used for this phase.

At present, we have observed many agent-based pervasive computing applications. Discusses several dimensions of security for a specific environment named Multi Agent System (MAS). It also represents a security model named Buddy where a security feature has been distributed among all the nodes and each node tries to safeguard its neighbor. In contrast with many others, here the authors proposed a non-hierarchical implementation and mentioned that hierarchical models are more likely to be attacked by a malefic force. According to the authors, if a specific agent or group of agents maintain the security features in hierarchical architecture, it is much easier to locate and penetrate them. In the Buddy model, each agent records the presence of its closest neighbor or buddy through a token passing mechanism. When facing danger, each agent will seek help from its buddy. Each agent acts once as 'Token Sender' and once as 'Token Receiver'.

When an agent receives a token in a predefined time limit, it gets the idea that its buddy is in good shape. Otherwise it senses a problem and broadcasts a global message to identify the problem. Each agent in the topology gets a chance to periodically broadcast. Token Sender and Token Receiver classes of Java have been used to implement the scenario.

PRIVACY IN PERVASIVE COMPUTING

In pervasive computing environments, where the concentrations of 'invisible' computing devices are continuously gathering personal data and deriving user context, the user should rightly be concerned with their privacy. Devices may reveal and exchange personal information (such as identity, preferences, role, etc) between smart artifacts in pervasive systems. In a context where devices cannot be assumed to belong to a single trusted domain, privacy becomes a major issue. It is crucial to develop and create privacy-sensitive services in pervasive computing systems to maximize the real benefit of such technologies and reduce feasible and actual risks. Because such systems collect a huge amount of personal information (such as e-mail address, location, shopping history... etc) and because people are typically concerned about their personal information, it is conceivable that they will be reluctant to participate in pervasive environments.

Thus, it is paramount to provide a mechanism that ensures privacy is maintained at all times. Privacy can be defined, according to Steffen et al. , as "an entity's ability to control the availability and exposure of information about itself". In , the authors identify five characteristics that make such systems very different from today's data collection systems, which are:

1. New coverage of smart environments and objects will be presented everywhere in our life;
2. Data collection will be invisible and unnoticeable;
3. The collected data will be more intimate than ever before; for example how people feel while doing something;

4. The underlying motivation behind the data collection;

5. The increasing interconnectivity which is necessary for smart devices to cooperate in order to provide a service to users; this results in a new level of data sharing making unwanted information flows much more possible.

Together, these characteristics indicate that data collection in the age of pervasive computing is not only a quantitative change from today, but also a qualitative change. Users in pervasive computing environments do not know what is done with their personal information and a service may store or process the provided data in some way that is not intended by the user. This fear makes people feel more concerned about their privacy.

As Weiser noted, “If the computational system is invisible as well as extensive, it becomes hard to know what is controlling what, what is connected to what, where information is flowing, how it is being used and what are the consequences of any given action”. Then he referred to privacy as a solution research issue; it has always been raised as a crucial issue for the long-term success of pervasive computing. The concept of privacy has become one of the main concerns as the technology of smart artifacts develops. Moreover, in the developed world there has also been a growing awareness of privacy issues in general, particularly due to the increased use of the World Wide Web. Weiser stated that a well-designed pervasive system should eliminate the need for giving out some items of personal information. For example, schemes based on "digital pseudonyms” could eliminate the need to give out items of personal information that are routinely entrusted to the network’s today, such as a credit card number and an address. Langheinrich stated “Everything we say, do, or even feel, could be digitized, stored, and retrieved anytime later.

We may not (yet) be able to tap into our thoughts, but all other recording capabilities might make more than up for that lack of data.” The author formulated six principles for directing system design based on a set of fair information practices common in most privacy legislation. The principles are: Notice, Choice and Consent, Proximity and Locality, Anonymity and Pseudonymity, Security and Access and Recourse. In another publication, Langheinrich considered designing a perfect mechanism for protecting privacy would be difficult to achieve.

Therefore he proposed a system where the users are allowed to be alerted about their privacy. The system relies on social and legal principles from real life, instead of designing a system to ask other people to respect the user’s privacy. This system, named privacy awareness system (pawS), permits data collectors to process personal data and management policies, and to describe tools for manipulation of personal information (storing, deleting and modifying information). In the main, this system is based on four of the above six principles: (notice, choice and consent, proximity and locality, and access and recourse), while the other two principles (Anonymity and Pseudonymity, and Security) are useful tools and a supportive part of the infrastructure. The developed pawS architecture (Privacy Preferences Project P3P) includes two main parts: privacy proxies and a privacy-aware database.

Privacy protection remains a serious barrier to the widespread deployment of Pervasive Computing environments. Researchers are considering identifying applications and seeking ways for creating interactions that are effective in helping end-users manage their privacy in pervasive computing. Jason and James developed a toolkit (called Confab) for helping the development of privacy-sensitive pervasive computing applications. It provides basic support for building pervasive computing applications, a framework and several customizable privacy mechanisms. In this framework all the personal information of a user will be captured, stored and processed on the user’s computer as much as possible, and then the user can control what information to share with others. They focused on authorizing people with choice and informed permission, so that they can share the right information with the right people and services in the right situations. A number of researchers have worked on another aspect related to privacy, which concerns monitoring users’ behaviour. Within pervasive computing, monitoring capabilities can be intrusive because there are sensors and machines which take over the role of the watchers and begin to store more and more aspects of our daily routine. Because it is difficult to know when people become conscious that they have been monitored and their privacy has been violated, Langheinrich described an approach called privacy boundaries. This approach tries to capture the various reasons a certain flow of personal information is perceived threatening, and then assesses how pervasive computing affects it. The authors also tried to identify and motivate key concepts in personal privacy that should influence the “design and implementation of privacy-aware pervasive computing systems, which are the systems that take the social fabric of everyday life into account and try to prevent unintended personal border crossings”. For example, Rhodes presented the wearable memory amplifier, allowing its wearer to continuously record events of their daily life (multimedia diary), which helps them to remember a lot of small details to provide a useful service. There is, however, a cost in increasing the risk at the privacy boundaries.

SECURITY GOALS

As the sensor networks can also operate in an adhoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of adhoc sensor networks. The security goals are classified as primary and secondary. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self-Organization, Time Synchronization and Secure Localization.

The primary goals are:

A. Data Confidentiality

Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. A sensor node should not reveal its data to the neighbors.

B. Data Authentication

Authentication ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets . Data authentication verifies the identity of the senders and receivers. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys. Due to the wireless nature of the media and the unattended nature of sensor networks, it is extremely challenging to ensure authentication.

C. Data Integrity

Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed. Even if the network has confidentiality measures, there is still a possibility that the data integrity has been compromised by alterations. The integrity of the network will be in trouble when:

- A malicious node present in the network injects false data.
- Unstable conditions due to wireless channel cause damage or loss of data.

D. Data Availability

Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network.

The Secondary goals are:

E. Data Freshness

Even if confidentiality and data integrity are assured, there is a need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To solve this problem a nonce, or another timerelated counter, can be added into the packet to ensure data freshness.

F. Self-Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the risky environment may be devastating.

G. Time Synchronization

Most sensor network applications rely on some form of time synchronization. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pairwise sensors. A more collaborative sensor network may require group synchronization for tracking applications.

H. Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate no secured location information by reporting false signal strengths, replaying signals.

CONCLUSION

In this paper, we examined security and privacy issues in some new and emerging wireless networks. In surveying relevant literature, we tried to identify new security and privacy challenges as well as inadequacies of current approaches.

Certain challenges arise from the unattended, intermittently connected and possibly mobile, network operation. Consequently, we need to anticipate threats arising from malicious exploitation of such network features and design appropriate security counter-measures. Also, since some emerging wireless networks are ad hoc in nature, infrastructure-independent security and privacy techniques are particularly suitable. Finally, emerging wireless devices such as RSensors motivate the development of new cryptographic primitives and protocols.

In this paper, we have presented the current status of pervasive security area. The feedback model presented in the access control section is going to motivate many researchers as this is the first model in this issue, to the best of our knowledge. Risk is another issue that is inseparably related with trust, though it is not a heavily discussed issue in pervasive computing.

As a pervasive computing environment can come in different formats such as static (e.g. sensor network) or mobile (MANET), and pure (where administrator has no prior information about the ad hoc network) or managed (where administrator has some prior knowledge about the network), the security requirements also take different shapes. Combining all these concerns, security in pervasive computing has become a most complex issue. These concerns have to be resolved in every aspect to ensure this latest computing technology will flourish.

REFERENCES

Adrian Perrig, John Stankovic, David Wagner, (2004). "Security in Wireless Sensor Networks" Communications of the ACM, pp. 53-57.

Bussard, L., & Roudier, Y. , (2002). "Authentication in pervasive computing", in the Workshop on Security in Ubiquitous Computing at UBICOMP'02, (Goteborg, Sweden).

E. De Cristofaro, X. Ding, and G. Tsudik (2009). Privacy-preserving querying in sensor networks. In IEEE ICCCN 2009.

F. Bagci, H. Schick, J. Petzold, W. Trumler, and T. Ungerer, (2005). "Communication and security extensions for a ubiquitous mobile agent system (UbiMAS)," in Proceedings of the 2nd Conference on Computing Frontiers, pp. 246–251.

H. Deng, A. Mukherjee, D. P. Agrawal, (2004). "Threshold and identity-based key management and authentication for wireless ad hoc networks," in International Conference on Information Technology: Coding and Computing (ITCC'04), pp. 107–111.

J. E. Bardram, R. E. Kjær, and M. Ø. Pedersen, (2003). "Context-aware user authentication – Supporting proximity-based login in pervasive computing," in Proceedings of Ubicomp 2003: Ubiquitous Comput- ing, LNCS 2864, pp. 107-123, Seattle, Washington, USA, Springer Verlag.

Kate, G. Zaverucha, and U. Hengartner (2007). "Anonymity and security in delay tolerant networks. In 3rd International Conference on Security and Privacy in Communication Networks (Secure Comm 2007).

Langheinrich, M., (2001). "Privacy by design - principles of privacy aware ubiquitous systems", in the Proceedings of the 3rd international conference on Ubiquitous Computing, (Atlanta, Georgia, USA).

M. Blaze, J. Feigenbaum and J. Lacy, (1996) "Decentralized trust management," in Proceedings of the 17th IEEE Symposium on Security and Privacy, pp. 164–173.

M. Raya and J. Hubaux (2005). "The security of vehicular ad hoc networks. In ACM workshop on Security of Ad Hoc and Sensor Networks.

M. Raya, P. Papadimitratos, and J. Hubaux (2006). Securing vehicular communications. IEEE Wireless Communications.

N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, and C. Luo. (2007). "Applicability of identity-based cryptography for disruption-tolerant networking. In MobiOpp.

Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, (2006). "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page (s): 6.

R. Di Pietro, L. Mancini, C. Soriente, A. Spognardi, and G. Tsudik (2008). Catch Me If You Can: Data survival in unattended sensor networks. In 6th IEEE International Conference on Pervasive Computing and Communications (PerCom'08), pages 185–194.

R. H. Campbell, J. Al-Muhtadi, P. Naldurg, G. Sampemane, and M. D. Mickunas, (NOV. 2002) "Towards security and privacy for pervasive computing," in Proceed- ings of Theories and Systems, Mext-NSF-JSPS International Sympsoium, ISSS 2002, pp. 1-15, Tokyo, Japan.

Weiser, M., (1991). “The computer for the 21st century”. Scientific American 265(No. 3), pp. 94 –104.

Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, (2009). “Sensor Network Security: A Survey, IEEE Communications Surveys & Tutorials, vol. 11, no. 2, page (s): pp. 52-62.

Zugenmaier, A., & Walter, T., (2007). “Security in pervasive computing calling for new security principles”, in the Pervasive Services, IEEE International Conference.