F. Sanchez-Cid, A. Munoz, D. Serrano, and C. Fernandez-Gago, "Software Engineering Techniqes Applied to AmI: Security Patterns", *First International Conference on Ambient Intelligence Developments (AmID06)*, pp. 108-123, 2006.
http://doi.org/http://dx.doi.org/10.1007/978-2-287-47610-5_8
NICS Lab. Publications: https://www.nics.uma.es/publications

Security and Dependability in Ambient Intelligence

Daniel Serrano, M. Carmen Fernández-Gago, Antonio Muñoz

Department of Computer Science
University of Málaga. Spain.
{ serrano,mcgago, amunoz }@lcc.uma.es

Abstract. One of the key aspects of the new emerging environments of Ambient Intelligence is Security. Dependability for these environments is also an important feature to be considered. In this paper, we will consider the problems and challenges arising concerned to security and dependability in Ambient Intelligence. We will provide an overview of the current solutions proposed for them and the challenges arising for these new scenarios. We also provide a revision of the projects devoted to Ambient Intelligence and give some future research lines.

1 Introduction

The way we interact with computers and other devices such as PDAs, mobile phones, etc. is increasing. The systems as we know them nowadays will become in a future more dynamic than what they are, evolving to pieces of hardware and software or communication links that will be sensitive, context-aware and will react to users' needs. This new emerging scenarios are called Ambient Intelligence (AmI). AmI contain a number of heterogeneous computing and communication infrastructures and devices providing new functionalities enhance productivity and facilitate everyday tasks.

In contrast to this promising scenario provided by AmI environments some problems arise. The combination of heterogeneity, number of devices or dynamism will make the security and dependability problems grow. Also, it will be almost impossible to achieve the provision of security and dependability solutions with the current existing solutions. The complexity of the unbounded nature of devices will make impossible for security engineers to foresee all the possible situations in order to provide all the possible solutions. The smart devices involved in the AmI ecosystem will have different security and dependability solutions, and sometimes will act under different policies (contracting at times). Thus, securing each device or piece of information separately might not work. Finally, the elements of an AmI environment could have different owners, the resulting solutions should be monitored in order to detect threat attacks and decide on recovery actions.

Thus, it becomes clear that some work needs to be done in this emerging area.

In this paper we do not introduce any security and dependability solution, since this remains ongoing and future work. However, we will online some of the problems and

propose possible ways of tackling them based on the existing solutions for general distributed systems. The paper is organised as follows. In Section 2 we mention some of the security problems that arise from the new AmI scenarios. In Section 3 we propose some existing solutions that we believe could be adapted to AmI. We conclude the paper in Section 4 and give some directions for future work.

2 Security Concerns for AmI

2.1 Common Problems

AmI environments impose some constraints in the connectivity framework, power computing and energy budget. This makes of AmI a significantly different case within distributed systems. The combination of heterogeneity, dynamism, sheer number of devices, along with the growing demands placed on software security and dependability (see Section 2.3 for dependability in AmI environments), make application development vastly more complex. Also, the provision of security and dependability for applications becomes increasingly difficult to achieve with the existing security engineering mechanisms and tools. Security related common problems of systems can be classified into three main categories, according to whether they threat confidentiality, integrity or availability of systems. In the following we will describe each of them.

Confidentially is the property that information holds when it remains unknown to unauthorized principals. In the case of AmI environments almost all the communications are carried out through wireless connections. It is well known that wireless connections are more vulnerable to attacks than wired connections since the information could be transmitted to anyone in the network range. Hence, we would expect that some of the security solutions existing for wireless networks could be adapted to AmI environments. Among the most used techniques for achieving confidentiality in distributed systems it is worth to mention those based on encryption and decryption. These techniques achieve a certain level of security by obscurity. Examples of these techniques are stream cipher and block cipher techniques by Vernam and Maubogne [1]. More recent techniques, in the same line of research, include those introduced in [2] by Schneier.

Public Key Infrastructures are also techniques used in order to achieve confidentiality. In some cases, it is more convenient to combine both, public and private key cryptographic systems. This leads to the well known hybrid systems Reference???

Integrity is the property that is violated when information is altered without authorization. This definition applies to the information held in a host as well as for the information in transit between hosts. As we mention before, wireless networks are more vulnerable to attacks than wired ones. The main reason being that anyone on the range of the wireless network can receive the signal. Thus, a man-in-the-middle attack is easy to be performed and, as a consequence, an attack on the data integrity.

Some of the techniques widely used in distributed systems are Errors Detection Code [3], Hash's tables [4], MAC (Message Authentication Code) or Digital

Signature. These techniques could be also applied to the new emerging environments of AmI, though we should take into account the nature of AmI.

Availability is the property of a system that grants and legitimizes requests by the authorized parties. A possible attack occurs when a malicious principal is able to achieve the denial of a service to an authorized principal by means of overloading the system. In any AmI environment where the users are connected to the host, it is possible to carry out an attack by denying the service. This could put under risk the availability of the system.

2.2. Trust: Authentication and Authorization

Trust plays an important role in security. The notion of trust in Computer Science has been borrowed from the concept in human society, where interactions are made constantly. Thus, in environments such as AmI where interactions among their members should be constant trust becomes an essential part of the security solution. The term of trust in Computer Science is closely linked to the combination of authentication authorization and access control

Authentication. In a type of environments as AmI, where the identity of the users is not always known, some form of authentication should be performed in order to grant access. Authentication does not only include identification of the user but also establishing whether the user belongs to the system.

User identification is typically accomplished via password-based systems where users know a piece of information that no one else in the system knows. When the user is requested, he provides all or part of the information to the verifier. This kind of systems includes also credit cards and mobile phone PINs.

Authorization. Most current access control schemes base their approaches on locally-issued credentials that are closely related to user identities. These types of credentials present many drawbacks. Among them we highlight: (a) they are not interoperable; (b) the same credentials are issued many times for each user, what introduces management and inconsistency problems; (c) credentials are issued by the resource administrator, but in most cases, this administrator does not have enough information to establish trustworthy credentials; and (d) they are dependent on user identity. However, in practice, it is frequent that the identity of the user is not relevant for the access decision. Sometimes it is even desirable that the identity is not considered or revealed. Furthermore, in systems based on identity, the lack of a global Public Key Infrastructure (PKI) forces the use of local authentication scheme.

In these cases, subscription is required and users have to authenticate themselves to every accessed source. To solve the aforementioned problems, single-sign-on mechanisms are becoming popular. These mechanisms are based on federation of sources that represent a limited improvement because credentials remain local (not to a site, but a set of them). Moreover, all federated sources must agree on a homogeneous access control scheme.

2.3. Dependability

Dependability can be defined as that property of a computer system such that reliance can justifiably be placed on the service it delivers. The service delivered by a system is its behaviour as it is perceptible by its user(s); a user is another system (human or physical) which interacts with the former (dependability).

The development of a dependable computing system calls for the combined utilization of a set of methods and techniques which can be classified into different categories:

- fault prevention: how to prevent fault occurrence or introduction,
- fault tolerance: how to ensure a service is still running to fulfil the function of the system in the presence of faults,
- fault removal: how to reduce the presence (number, seriousness) of faults,
- fault forecasting: how to estimate the present number, the future incidence, and the consequences of faults.

From the security point of view, dependability is a very interesting property for distributed systems. However, it becomes more relevant for the case of AmI environments. This is due to some of the characteristics of these environments, for example, intermittent connections of both, users and devices within the system; or the heterogeneity of the devices simultaneously connected. Thus, dependability should be an essential requirement for AmI systems.

2.4. Other Problems

Non repudiation -The concept of "non-repudiation" implies that a service should provide proof of the integrity and origin of data, in a trusted relationship which can be verified by any third party at any time. Also, an authentication process with high assurance can be asserted to be genuine. This proof can not subsequently be refuted. This property has been widely explored in the literature [5].

Non-repudiation is a property achieved through cryptographic methods which prevent an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection or authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership). It is this denial of the right of being able to repudiate [2] a digital signature that causes great concern and it is resulting in a misinterpretation of its use within digital signature regimes.

In the electronic commerce environment, the technical meaning of the term "non-repudiation" either shifts the responsibility of proof from the recipient to the alleged signatory or entirely denies the signatory the right to repudiate a digital signature. That is, if a digital signature is verified so as to identify the owner of the private key that was used to create the digital signature in question, then it is that person who is responsible for proving that it is not their digital signature. Therefore, the evidences are altered. This crypto-technical position does not correspond to what occurs in the paper-based environment.

Research in the area of AmI is growing considerably, most of the times backed by big companies, mainly due to the fact that electronic commerce is one of the main applications of AmI environments. Hence, non- repudiation becomes an essential requirement for AmI systems. The same occurs with the fair-exchange property that we will see next.

Fair exchange- Fair-exchange protocols are necessary in order to ensure that no party involved in an e-commerce transaction gains an unfair advantage over the other party by misbehaving, misrepresenting or by prematurely aborting the transaction. A fair exchange protocol can then be defined as a protocol that ensures that no player in an electronic commerce transaction can gain an advantage over the other player by misbehaving, misrepresenting or by prematurely aborting the protocol. It is important to mention that the problem of fair exchange is not just limited to information goods. We always assume that fairness is ensured in any business transaction. In an electronic commerce, transactions where the product is not a piece of information, but rather something more tangible, we automatically have the same set of safeguards that ensure fair exchange in conventional transactions. However, if the product is a piece of information that is transmitted electronically over an inherently insecure medium such as the Internet, with the destination address possibly not bound to any physical address, fair exchange is more difficult to achieve. Thus, the problem of fair exchange for information goods has called the widest attention lately, and the term is now mostly used to denote such protocols. Further, the problem is not always primarily a cryptographic problem. For example, we can achieve fair exchange by utilizing an escrow agent in the transaction. The escrow agent receives the item to be exchanged from each player and performs the exchange. Assuming that there is a reliable communication mechanism (in the sense that it does not produce errors or it cannot be tapped into) between the escrow agent and each player, such a protocol can be implemented without recourse to any cryptographic protocols. Over the Internet, reliable communication can be achieved only by utilizing cryptographic techniques. It is no surprise, therefore, that fair exchange electronic commerce protocols have received the maximum attention from researchers in cryptography.

3 Challenges and Possible Solutions

3.1. Challenges

In this section we will concentrate on some relevant challenges for AmI environments from the security point of view. This will help us to show the importance of each of the properties that we outlined above.

Challenge 1. In the new AmI scenarios, not only systems as a whole, but also individual applications should be able to adapt dynamically to new execution environments. As a consequence, pre-defined trust relationships between components, applications and their system environments can no longer be taken for granted.

The most specific characteristics of AmI are present in this challenge. Thus, in order to achieve a solution for it, we should solve problems related to the dynamism of the environment (new elements appearing and disappearing constantly) as well as those related to the connectivity methods (for instance, wireless).

The concept of authentication has a special meaning when considering the scenario described in challenge 1 due to the dynamic nature of AmI. Thus, some devices will be authenticated without human action whereas in some other cases the authenticated

user could log on and off from the system. It is in this case where the authentication should be transparent. Even in an extreme case where a user changes the device to access the system it will be desirable that authentication is clear and transparent.

Additionally and very related to authentication, we consider confidentiality. In this case we need to consider two cases: (1) again, due to the dynamic nature of AmI environments, the amount of possible attacks increases; (2) new security requirements should be considered in order to satisfy confidentially in an environment which is not Peer to Peer.

Concerning availability in AmI environments, besides the proper problems arising in any system, again dynamism constitutes an issue. Also, availability does not only affect the functionality of a system but how to solve the lack of functionality.

The problem arising for data integrity is worsened by the fact that the components of the AmI system appear and disappear constantly. This is mainly due to the mean of communication among devices. It may occur that the communication is interrupted or intermittent. It could even happen that the information destination changes during the communication process, for instance, if the user has moved during it. Moreover, this appearing-disappearing situation could lead to malicious third parties to access the system and try to threat the data integrity of the system.

Authorization becomes a complex issue in dynamic environments. The mechanisms used for static environments in order to manage privileges and authorizations should change in these cases. The appearance of new elements could lead to the need for new privileges for them. Also, the disappearance of services should be predicted in order to not to depend on them for managing users' authorizations.

Non-repudiation problems should be enforced for AmI systems since users could change device or uses more than one.

Fair-exchange could be affected as the source and the destination of a transaction change during the communication process..

Challenge 2. AmI environments will contain a large number of heterogeneous computing and communication infrastructures and devices that will provide new functionalities, enhance user productivity, and ease everyday tasks. These devices will hold a variety of data with different security and privacy requirements. This information will be used in different ways in different applications and computing contexts and, therefore, different policies (possibly contradicting) will be applied.

The more relevant properties affecting this challenge are integrity and confidentiality. Both properties impose more constraints due to that different devices might use different formats during the information process. The possible solutions should apply criteria that could unify the different data and presentation formats existing in AmI.

Authentication in AmI introduces two new characteristics. On one hand, the fact of adapting authentication mechanisms to devices that are provided with very different communication interfaces. On the other hand, we should take into account the case when a device has to authenticate itself to another one. Hence, heterogeneity increases the scope of the problem.

Concerning to availability, even if in some cases there exists a logical availability of a service, it is important to ensure availability at a usability level from the devices.

The problem with authorization arises because of the intermingling nature of the different platforms within the environment itself. We need to provide mechanisms that allow the use of privileges from all of them.

Fair-exchange and non-repudiation are less relevant for the requirements of this second challenge.

Challenge 3. Finally, because of their complexity, and because elements will be under the control of different owners, security mechanisms will need to be supervised (monitored) in order to identify potential threats and attacks and decide on recovery actions, if possible.

This challenge aims to achieve monitoring tasks. It will also aim to adapt the applied security mechanisms since a certain mechanism could be used by different users. In general, most of the problems mentioned in Section 2 will be affected if monitoring is introduced.

The problem for confidentiality increases in two ways. On one hand the devices could be used for more than one user and, on the other hand, because in the scenario proposed by challenge 3 there will be more many devices. Concerning to integrity we will need monitoring mechanisms for this challenge. The application of methods in order to apply crash-recovery measures makes the problem of integrity grows. The main reason for this is that AmI ecosystems are very vulnerable to the wrong use that malicious users could carry out.

Authentication and authorization should adapt to monitoring. The fact that different users could be under several users' control adds new constraints which could be incorporated to the authentication mechanisms. The same occurs for authorization.

The situation for availability is quite similar to the previous requirements: the problem becomes more complex due to the amount of users of the system and how they use the devices.

Concerning to fair-exchange and non-repudiation, the problem arises when some users, for instance, use a device which will be used later on for another user or when some users carry out the same action using different devices.

Challenge 4. The provision of S&D in AmI ecosystems requires the dynamic application of the expertise of security engineers in order to dynamically react to unpredictable and ever-changing contexts.

The dynamic application of the security engineer expertise leads the security problems to a new level. This new challenge brings additional requirements in order to both, store expertise and apply it in a dynamical way. New problems, derived from dynamic, and run-time, management are added to the problems proposed in section 2. These new problems are generated not only because security needs to be applied dynamically, but also because the way these mechanisms perform should vary.

Challenge 5. Can we take advantage of the recent developments in technologies of security engineering, run-time monitoring, semantic description and self-configuration that are able to capture some of the expertise of security engineers and make it available, supported by automated tools, to the AmI ecosystems?

The achievement of this challenge cannot be possible without taking into account the previous ones, together with the need to adapt the security mechanisms for AmI environments. This challenge introduces the use of auto-configuration features, the semantic description, the run-time monitoring mechanisms and the use of the more novel security advances. All of these techniques should be implemented in order to

solve common security problems; however we should take into account that these problems become more complex when they are analysed from the AmI point of view.

3.2 Possible Solutions

This section provides a review of all the existing solutions taken from the Internet to mobile telephony. They might help us to build solutions in AmI systems.

Back in 1978 the Needham-Schroeder protocol [6] was published. This is one of the first authentication protocols for distributed systems. Later in 1981 Denning and Sacco found a flaw in this protocol. They modified it and provided a new version. It was Needham himself, together with Burrows and Abadi, who proposed the BAN logic [8,9], a logic for authentication. However, one of the most relevant protocols in the area of authentication is Kerberos [10]. This protocol is based on the previous approaches. Its main problem is that it depends on a secure distribution system time. This problem led to the development of public key infrastructures (PKI). They first appeared by the recommendation of the CCITT X.509 [11], although it was first implemented within the PGP software by Zimmermann. It is important to mention other two relevant works in this area. SPKI (Simple Public Key Infrastructure) by Ellison [12,13] and SDSI (Simple Distributed Security Infrastructure) by Rivest and Lampson [14].

Another interesting protocol is IPSEC [15], also known as IP level security. This protocol fits into the IPv6 category. SSL and TLS are also protocols worth to be mentioned. SSL (Secure Socket Layer) was developed by Netscape as a security protocol for electronic commerce. This protocol evolved to the TLS (Transport Layer Security) version 1.0 [16], which is currently under IETF use.

In the following we will outline the technologies which could be more relevant for AmI environments. First of all, we will consider the GSM network. The devices are originally registered with an entity (home network). However authentication by other entities in which the home network does not fully trusted may be needed later on. Details of the GSM technology can be found in [17,18]. Bluetooth is an embedded radio system for short-range communication between small devices. It is the commercial system whose intended usage pattern most closely matches the ubiquitous computing. The security services provided by Bluetooh are authentication and encryption. The authentication algorithm, called E1, is a MAC based on SAFER+. This algorithm eliminates extra unneeded negotiations, which makes of it an easy algorithm. At the highest level, Bluetooth link security may be described as follows. If two devices wish to communicate securely, they establish a shared secret called a link key. This may be temporal or permanent. In the case that this is temporal, it lasts only for one session. However if this is permanent, it may be reused in later sessions, so that when the two devices meet again they do not have to regenerate one. Finally, we mention the IEEE 802.11 wireless networking standard [19] together with its variations 802.11a and 802.11b, also known as Wi-Fi and used primarily as a convenient Ethernet replacement for laptops within homes and offices, has become rather popular in recent years. Concerning security, the Wired Equivalent Privacy (WEP) algorithm is part of the 802.11 standard: its name describes its intended goal. Nevertheless, it is important to mention that WEP is not the best solution; in fact Borisov, Goldberg and Wagner [20] published on their web site a draft document

highlighting several flaws in WEP. Fluhrer, Martin and Shamir [21] found some weaknesses in the key scheduling algorithm of the widely deployed RC4 stream cipher. In particular, they found it completely insecure in a certain mode of operation which WEP happened to adopt. However, Stubblefield, Ioannidis and Rubin [22] implemented and optimized the attack proposed by Fluhrer et al demonstrating its practicality and effectiveness.

4 Related Projects

In this section we will mention some of the research projects that deal with Ambient Intelligence. We start by mentioning OpenTC[1]. The Open Trusted Computing (OpenTC) is an R&D project focusing on the development of trusted and secure computing systems based on open source software. The project targets traditional computer platforms as well as embedded systems such as mobile phones. The project is characterised for the high heterogeneity of the devices considered as well as the use of the new Technologies in order to achieve the expected solution. The INDICARE[2] project deals with Consumer Acceptability of DRM Solutions in Europe. The overall goal of INDICARE was to raise awareness, help to reconcile heterogeneous interests of multiple players, and to support the emergence of a common European position with regard to consumer and user issues of Digital Rights Management (DRM) solutions. This project tackles some of the security requirements we mentioned in previous sections. In particular, authorization, delegation and privacy derived from a very heterogeneous environment with a large number of users. The Mobius[3] project aims to develop the technology for establishing trust and security for the next generation of global computers, using the Proof Carrying Code (PCC) paradigm. Mobius is quite related to. Re-Trust Project and InspireD[4] Project in the sense that all of them use the new Technologies in order to deal with heterogeneous systems(challenges 2 and 4 of previous section). MediaNet, ENTHRONE, TIRAMISU, FASTMATCH, DANAE and DIVAS[5] projects propose an integrated management In particular these projects consider the management of privileges in dynamic environments (as challenge 1 aims to consider for AmI). The objective of S3MS[6] is to create a framework and a technological solution for trusted deployment and execution of communicating mobile applications in heterogeneous environments. This project tackles all the challenges we mentioned earlier. 4S[7] (Smart Chips for Smart Surroundings): The overall mission of the proposed 4S project (Smart Chips for Smart Surroundings) is to define and develop an efficient (ultra low-power), flexible,

[1] The OpenTC Project. IST-027635. http://www.opentc.net/
[2] The INDICARE Project.. http://www.indicare.org/
[3] The Mobius Project. http://mobius.inria.fr/twiki/bin/view/Mobius/WebHome
[4] Re-Trust Project. http://re-trust.dit.unitn.it/ and The InspireD Project. http://www.inspiredproject.com/
[5] The MediaNet Project. http://www.ist-ipmedianet.org/. The ENTHRONE Project http://www.ist-enthrone.org/. The TIRAMISU Project. http://www.tiramisu-project.org/. The FASTMATCH Project. http://www.fastmatch.org/. The DANAE Project. http://danae.rd.francetelecom.com/. The DIVAS Project http://www.ist-divas.eu/portal/.
[6] The S3MS Project. http://www.s3ms.org
[7] The 4S Project. http://www.smart-chips.net/public/html/index.php

reconfigurable core building blocks, including the supporting tools, for future Ambient Systems. The main objectives for the 4S project are: First, the design of a flexible reconfigurable platform based on heterogeneous building blocks such as analogue blocks, hardwired functions, fine and coarse grain reconfigurable tiles, DSPs and microprocessors that can adapt to several algorithms for Ambient Systems without the need for specialized ASICs. Conclusions and Future Work
The emergence of a new kind of distributed systems, Ambient Intelligence (AmI), brings together the appearance of new security problems proper of the nature of these systems. The main security problems are the same as for any distributed system, although, as we mentioned before, the nature of the AmI environment strengths some of them. In this paper we have outlined those problems as well as the possible solutions for them. The existing security solutions for distributes systems are not sufficient for AmI due to the specific characteristics of them. However, we believe that they could be adapted to the new AmI environments. Thus, in the future we intend to first identify in detail the security problems specific for AmI and then to study how the existing solutions can be adapted SERENITY (Reference).

5 Conclusions and Future Work

The emergence of a new kind of distributed systems, Ambient Intelligence (AmI), brings together the appearance of new security problems proper of the nature of these systems. The main security problems are the same as for any distributed system, although, as we mentioned before, the nature of the AmI environment strengths some of them. In this paper we have outlined those problems as well as the possible solutions for them. The existing security solutions for distributed systems are not sufficient for AmI due to the specific characteristics of them. However, we believe that they could be adapted to the new AmI environments. Thus, in the future we intend to first identify in detail the security problems specific for AmI and then to study how the existing solutions can be adapted SERENITY (Reference).

6 References

[1] Auguste Kerckhoffs. La cryptographie militaire (Military Cryptography). Journal des Sciences Militaires, IX :5-38, Jan 1883.
[2] Bruce Schneier. Applied Cryptography, 2nd ed. Protocols, Algorithms, and Source Code in C. Wiley, 1996.
[3] Richard W. Hamming. Coding and Information Theory. Prentice-Hall, 1980.
[4] Gideon Yuval. How to Swindle Rabin. Cryptologia, 3(3): 187-189, Jul 1979.
[5] W. Caelli, D. Longley, and M. Shain, Information Security Handbook. Stockton Press New York, NY, USA, 1991.
[6] Roger M. Needham and Michael D. Schroeder. Using Encryption for Authentication in Large Networks of Computers. Communications of the ACM, 21(12):993-999, Dec 1978.

[7] Dorothy E. Denning and Giovanni Maria Sacco. Timestamps in Key Distribution Protocols. Communications of the ACM, 24(8):533-536.
[8] Michael Burrows, Martin Abadi and Roger Needham. A Logic of Authentication. Tech. Rep. 39. Digital Equipment Corporation Systems Research Center, Feb 1989.
[9] Michael Burrows, Martin Abadi and Roger Needham. A Logic of Authentication. ACM Transactions on Computer Systems, 8(1):18-36, 1989.
[10] J. Kohl and C. Neuman. The Kerberos Network Authentication Service (V5". RFC 1510, IETF, 1993.
[11] CCITT. Data Communications Networks Directory. Tech Rep. 8, CCITT, Melbourne, Nov 1988. Recommendations X.500-X.521, 9th Plenary Assembly.
[12] Carl M. Ellison. The nature of a useable PKI. Computer Networks, 31(8):823-830, 1999.
[13] C. M. Ellison, B. Frantz, B. Lampson, R. Rivest, B. M. Thomas and T. Ylomen. SPKI Certificate Theory, rfc 2693. In Network Working Group. The Internet Society.
[14] R. L. Rivest and B. W. Lampson. SDSI – A Simple Distributed Security Infrastructure, Crypto 96, 1996.
[15] S. Kent and R. Atkinson, Security Architecture for IP, Internet Draft, July 1998.
[16] T. Dierks and C. Allen. The TLS Protocol, Version 1.0. RFC 2246, IETF, 1999.
[17] Michel Mouly, Marie-Bernadette Pautet. The GSM System for Mobile Communications (Hardcover). Telecom Publishing (June 1992).
[18] Jain Cai Goodman, D.J. Rutgers. General packet radio service in GSM. Communications Magazine, IEEE. Oct 1997.
[19] IEEE. Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. ANSI/IEEE Std 802.11, IEEE, 1999.
[20] N. Borisov, I. Goldberg and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11, In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (Association for Computing Machinery, New York, NY), p. 180, 2001.
[21] S. Fluhrer, I. Mantin and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. 8th Annual International Workshop on Selected Areas in Cryptography. Lectures Notes in Computer Science, vol. 2259, pp. 1-24, 2001.
[22] A. Stubblefield, J. Ioannidis and A. D.Rubin. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. Tech. Rep. TD-4ZCPZZ, AT&T Labs, Aug 2001.