Available online at www.sciencedirect.com
ScienceDirect
Computer Standards & Interfaces 29 (2007) 289–301
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

EAP methods for wireless networks

Ram Dantu *, Gabriel Clothier, Anuj Atri

Department of Computer Science and Engineering, University of North Texas, PO Box 311366, Denton, TX, 76203, USA

Received 14 December 2005; accepted 18 April 2006
Available online 27 September 2006

Abstract

This paper presents an overview and analysis of Extensible Authentication Protocol (EAP) and its place in securing wireless LANs. A number of specific widely used EAP methods are examined and evaluated for their advantages and susceptibility to types of attack. Next we propose suitable EAP methods for wireless technologies beyond LANs, including RFID and WiMAX. After analyzing requirements for different wireless networks, we conclude that a new lightweight and secure EAP method is warranted for fixed mobile convergence interoperability.

Keywords: Wireless LAN; 802.11; Security; EAP; Extensible authentication protocol; RFID; WiMAX; 802.16

Contents

1. Introduction . . . 290
1.1. WLAN architecture . . . 291
1.2. Authentication and authorization . . . 291
1.3. Data protection . . . 291
1.4. Recent advancements . . . 292
1.4.1. WPA and 802.11i . . . 292
2. EAP requirements . . . 292
2.1. Mandatory requirements [10,11,28] . . . 292
2.1.1. Generation of symmetric keying material . . . 292
2.1.2. Mutual authentication support . . . 292
2.1.3. Self-protecting . . . 292
2.1.4. Synchronization of state . . . 293
2.1.5. Resistance to dictionary attacks . . . 293
2.1.6. Protection against man-in-the-middle attacks . . . 293
2.1.7. Protected cipher suite negotiation . . . 293
2.2. Recommended requirements [10,11,28] . . . 293
2.2.1. Fragmentation . . . 293
2.2.2. End-user identity hiding . . . 293
2.3. Optional requirements [10,11,28] . . . 293
2.3.1. Channel binding . . . 293
2.3.2. Fast reconnect . . . 293
2.4. Enterprise-specific requirements . . . 293
2.4.1. Enterprise architecture framework . . . 294
2.4.2. Reuse of existing hardware . . . 294
2.4.3. Network layout . . . 294

* Corresponding author.
E-mail addresses: rdantu@unt.edu (R. Dantu), gclothier@unt.edu (G. Clothier), anujatri@hotmail.com (A. Atri).

0920-5489/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2006.04.001

3. EAP methods . . . 294
3.1. Legacy based methods . . . 294
3.1.1. EAP–MD5 [12] . . . 294
3.2. Certificate based methods . . . 294
3.2.1. EAP–TLS . . . 294
3.2.2. EAP–TTLS . . . 294
3.2.3. EAP PEAP . . . 295
3.3. Password based methods . . . 295
3.3.1. LEAP . . . 295
3.3.2. SPEKE . . . 295
3.4. EAP SIM . . . 295
3.5. EAP–AKA . . . 296
3.6. Issues with certificate based methods . . . 296
3.6.1. Administration cost . . . 296
3.6.2. High protocol exchange . . . 296
3.6.3. Unable to authenticate user . . . 296
4. Possible attacks [23,28] . . . 296
5. Mobility issues . . . 297
5.1. Fast reconnection during handoff . . . 297
5.2. Home and visitor networks . . . 297
5.3. Handoff between heterogeneous networks . . . 297
6. RFID . . . 297
6.1. Requirements for RFID authentication . . . 297
6.1.1. Mutual authentication . . . 297
6.1.2. Re-authentication required . . . 298
6.1.3. Access control . . . 298
6.1.4. Logging . . . 298
6.1.5. Immunization to attacks . . . 298
6.1.6. Limited memory required . . . 298
6.2. Authentication mechanisms . . . 298
6.2.1. Fixed read access protocol . . . 298
6.2.2. Randomized read access control . . . 298
6.3. Selection of an EAP method for RFID . . . 298
7. WiMAX . . . 299
7.1. WiMAX architecture . . . 299
7.2. Authentication and authorization . . . 299
7.3. Selection of an EAP method for WiMAX . . . 299
8. Conclusion . . . 300
Acknowledgements . . . 300
References . . . 300

1. Introduction

Along with the widespread acceptance and implementation of wireless local area networks have also come concerns about the security of these networks. Transmitting data via an air interface rather than a more secure physical conduit brings along with it certain inherent vulnerabilities to security, such as eavesdropping. While enterprises have embraced the benefits of accessing their networks wirelessly, such as increased mobility and productivity for their workers, they have also kept a focus on keeping their sensitive data within their boundaries. It is mainly the need for enterprise security that has driven the development of wireless LAN security methods and protocols, and these advancements have also had a positive effect in personal and small office settings.

One of the most challenging and important aspects of securing wireless LANs in enterprises is that of authentication and authorization. This topic addresses establishing the valid identity of the user or device attempting to access a network as well as deciding whether that entity is going to be allowed to join the network and access its services and resources. The extensible authentication protocol (EAP) provides a framework for addressing these concerns. Within the EAP framework, there are a number of specific methods that can be used for authentication. The choice of an authentication method is essential to securing any network and should be made considering the unique requirements of each individual network. *To date, we have not found a noncommercial paper addressing a comparison of the various EAP methods available and their appropriateness for use in a variety of wireless networks. In addition to comparison, we added enterprise-specific requirements for EAP methods and discussed suitable EAP methods for RFID and WiMAX.*

Section 1 gives a background and overview of wireless LANs and their security issues to be addressed. In Section 2, we present some requirements which an EAP method selected for

use with a wireless LAN should support and discuss the relevance and importance of these requirements. Section 3 surveys some popular EAP methods which exist and their suitability to the requirements. In Section 4, we address some of the security issues which an EAP method should guard against. Section 5 discusses some scenarios that might be encountered when a user or device is mobile and needs to travel between networks employing an EAP method. Sections 6 and 7 address the use of EAP methods with RFID and WiMAX technologies, respectively. Section 8 summarizes the conclusions drawn from the evidence presented and makes the argument for interoperability of an EAP method.

1.1. WLAN architecture

Wireless LANs can operate in one of two modes: *ad hoc* or *infrastructure*. In *ad hoc* mode [2], each device present in the wireless network communicates directly with other devices on the network without the use of any central hub between the devices. This method of operation has the main benefit of not requiring any additional equipment beyond the wireless interface cards present in the wireless devices themselves. However, it does not fit the traditional hub and spoke topology in which wired LANs have typically been deployed.

In *infrastructure* mode [1], wireless devices communicate with each other and usually with a wired network via a centralized access point. This topology fits well with existing wired networks and allows the existing infrastructure to be augmented by access points, providing wireless access only at the last hop between the access point and the user devices. Since wireless LANs operating in infrastructure mode are more popular, especially among enterprises, these will be the focus of this paper.

The pertinent standards defining the operation of wireless LANs are IEEE standards 802.11a, b, and g. The 802.11a standard specifies operation of a wireless network at 54 megabits per second in the 5.8 GHz band. 802.11b specifies operation of a wireless network at 11 megabits per second in the 2.4 GHz band and is the most popularly implemented type of WLAN. 802.11g specifies operation of a wireless network at 54 megabits per second in the 2.4 GHz band and is quickly catching up with 802.11b in number of installations due to its backward compatibility with 802.11b access devices. All of these bandwidths are shared between all users on an access point and wireless channel or frequency.

While these standards do not include in their definition a complete specification for enterprise-level security [3], there are certain options available in the suite of 802.11 standards which do provide some options for implementing a secured wireless LAN. The options on which to base an authentication method are:

- Pre-shared key, typically implemented for individuals, home offices, and small offices.
- Password based security, typically implemented by enterprises that have extant strong password policies and mechanisms for authentication.
- Certificate based security for enterprises that require and choose to deploy certificates [5].

Rather than having a simple authentication protocol defined in a standard, the designers have chosen to provide a framework for a variety of authentication methods to be used. This concept of an extensible authentication protocol (EAP) provided the network administrator the flexibility to choose a method appropriate for their organization as well as the opportunity to change the authentication method to one that is possibly more secure. Based on the above options, EAPs can be categorized according to the various methods employed in their design. Although many methods exist, only those more frequently used will be discussed in this paper. Prior to discussion of these methods, some fundamental WLAN security procedures will be addressed.

1.2. Authentication and authorization

One of the fundamental issues to be addressed when considering network security is that of authentication and authorization. Authentication addresses establishing the genuine identity of the device or user wishing to join a wireless network. Authorization addresses determining whether the authenticated user or device is permitted to join the network [5].

The first generation of wireless LAN security was wired equivalent privacy, or WEP. The mechanism employed by WEP to handle authentication and authorization is that of the shared secret. If a user or device is programmed with the same secret as the access point of the network it is attempting to join, then it is permitted on the network. One of the major flaws with this mechanism is that if the key is gained through any means, then unauthorized parties can access the network. There are no rules existing in the WEP standard for enforcing key changes over time and the key usually remains static for long periods time.

WEP is particularly vulnerable to attacks when the shared secret key is not changed regularly because that key can be discovered by capturing packets transmitted across a network. As the combination of the shared secret key and a 24-bit initialization vector is used for data encryption, and this vector value is repeated, then it is possible to discover the common information including the secret key [4].

1.3. Data protection

In addition to authentication and authorization, the issue of data encryption must also be addressed when considering security of a wireless network. Once a user or device has been authenticated and authorized to join the network, their data must be secured continually for as long as they are transmitting data on the network. The mechanism WEP [4] uses for data encryption is a stream cipher based on the RC4 algorithm with keying provided by the shared secret key and an initialization vector.

As stated earlier, the vulnerability with RC4 in this configuration lies with reuse of the initialization vector due

to its finite size. While this is more of a concern on larger networks having a lot of traffic being transmitted and received, even smaller networks are susceptible but the time necessary to stage an attack may be increased. One-way to circumvent attacks of this nature is to enforce key changes, but these changes must be communicated to all the devices on the network in some fashion and cannot be implemented in a centralized manner.

1.4. Recent advancements

1.4.1. WPA and 802.11i

Once the vulnerabilities with WEP were identified, work was launched to create a standard for security in wireless networks. This resulted in the current standard for wireless network security, IEEE standard 802.11i. Prior to acceptance of the 802.11i standard, a consortium of parties involved with wireless networking called the Wi–Fi Alliance sought to make a subset of certain security aspects of the 802.11i draft available in an early stage and developed WPA, or Wi–Fi Protected Access.

Both WPA and the full 802.11i standard support two modes of operation: one for small office or personal networks called *personal* mode and one for large corporations or enterprises called *enterprise* mode. In personal mode, there is a shared key between the access point and devices or users wishing to authenticate with the access point. But instead of using this key directly as the basis for encryption as with WEP, the key is used to permit admission to the network and a new key, unique to each user or device is generated for data encryption purposes.

WPA and 802.11i operating in enterprise mode handle authentication through a standard developed for controlling admission to a network which is published as IEEE standard 802.1X. This standard is not unique to wireless networks and rather can apply to any point-to-point network.

802.1X [6–8] proposes a solution by which a supplicant is authenticated to an authenticator via the use of an authentication server. In terms of a wireless LAN in infrastructure mode, the supplicant is usually a wireless device or user, the authenticator is the access point with which the device or user wishes to communicate, and the authentication server is a device such as an authentication, authorization, and accounting (AAA) server or a remote authentication dial-in user service (RADIUS). However, in stronger authentication methods, as will be discussed later, the network will authenticate the device but the device will also authenticate the network in a mutual authentication scheme. 802.1X does not specify the method by which the authentication transaction will take place; rather, it uses the concept of an extensible authentication protocol (EAP) as specified in IETF RFC 3748. This allows the flexibility of a different authentication method to be chosen based on which is most appropriate for the circumstances of the network that needs to be secured. In this context, we define an authentication protocol as the mechanism by which a user or device is authenticated and allowed to join a network or rejected in its attempt to do so. An authentication protocol is considered to be *extensible* in this case as only a framework is defined for its operation; there are a variety of specific methods that can be used for the authentication procedure.

While WPA does use the same data protection and encryption scheme as WEP, it is made significantly more secure against attacks with the inclusion of an EAP protocol. In addition, WPA does enforce that keys are changed through use of a temporal key integrity protocol, or TKIP [9]. The full 802.11i standard enhances this by keeping the same options for EAP authentication available and strengthening data encryption through allowing a choice of data encryption modes of RC4 or the use of the advanced encryption system (AES) in a CCM block cipher mode, which is far more resistant to attacks than the RC4 algorithm employed by WEP and WPA.

While the previous methods of securing wireless LANs did have some inherent vulnerabilities, the state of the art with 802.11i and WPA allow selection of a method well suited to the individual requirements of a particular network. In the next section, we will discuss the requirements for authentication across a variety of networks.

2. EAP requirements

RFC 4017 describes some mandatory, recommended, and optional, requirements for EAP methods to be used to secure wireless LANs. The mandatory requirements can be considered as the base level functionality which is required in order to provide security to the wireless network. Recommended requirements would add desirable functionality in most scenarios. Optional requirements add functionality that may or may not be necessary depending on the circumstances of the individual network. We have also included some enterprise-specific requirements that have been seen as beneficial in experience with deploying an EAP in a corporate setting.

2.1. Mandatory requirements [10,11,28]

2.1.1. Generation of symmetric keying material

The EAP method should have an ability to generate unique keys for use in post-authentication key derivation for use in encrypting data transfers.

2.1.2. Mutual authentication support

The EAP method should provide for a mechanism by which the device an be authenticated to the access point as well as the access point and network authenticated to the device. Two one-way authentication methods will not satisfy this requirement; there must be a common mutual authentication scheme employed.

2.1.3. Self-protecting

The EAP method must be able to protect itself from eavesdropping, meaning that any party examining the packets used in the EAP procedure should not be able to gain any information that would be useful in impersonating the user.

2.1.4. Synchronization of state

There should be a mechanism built into the EAP method by which certain state attributes can be exchanged between the parties involved. This might include the protocol used, cryptographic keys used, and data encryption method used. The state should be synchronized when the EAP exchange is complete.

2.1.5. Resistance to dictionary attacks

If the EAP method uses a secret password as an authentication key, then a mechanism must be in place to ensure that the method will not be susceptible to an attacker trying to go through a list of passwords in order to gain access.

2.1.6. Protection against man-in-the-middle attacks

The EAP method should not be susceptible to a man-in-the-middle attack by which an attacker convinces the user to connect to an access point other than that authentically present on the network to which the user desires to connect. In order to prevent this attack, a certain set of features should be supported.

- *Cryptographic binding* assures both the user and server that a single entity has acted during the authentication procedure.
- *Integrity protection* assures the parties involved in the authentication procedure that the messages exchanged have not been tampered with between source and destination.
- *Replay protection* protects against replay of the authentication dialog between user and authenticator to allow an unauthorized party to gain access later by replaying such an exchange.
- *Session independence* in order to assure that an attack on a single session would not compromise prior or subsequent sessions.

2.1.7. Protected cipher suite negotiation

If the EAP method negotiates the cipher type used to protect the authentication transaction, then this negotiation itself should be protected.

2.2. Recommended requirements [10,11,28]

2.2.1. Fragmentation

EAP transactions may be carried out over lower-layers which have limits on the size of transmissions that can occur. The EAP method should be able to segment its transactions into smaller units and reassemble them in order to accommodate a smaller maximum transmission unit (MTU).

2.2.2. End-user identity hiding

The messages used within the EAP exchange should be encrypted so as to hide the identity of the actors participating in the exchange.

2.3. Optional requirements [10,11,28]

2.3.1. Channel binding

The EAP method should support a mechanism by which endpoint identifiers of the authenticator and device being authenticated can be conveyed to out of band devices such as lower-layer protocols.

2.3.2. Fast reconnect

In the event that a security association needs to be reestablished, as might be the case with a mobile device in a handoff state, the re-establishment of the security association should be with a reduced number of message exchanges or round-trips necessary.

2.4. Enterprise-specific requirements

As wireless LANs have become more popular in both homes and enterprises, significant research has been done to find ways of improving the security of such networks. EAP methods and the 802.11i standard have made progress toward this goal. However, when considering wireless LANs in an enterprise setting, security is not the only concern.

Table 1
Overview of EAP methods and technologies

EAP type	Dynamic rekeying	User ID and password	Comments
EAP–MD5	No	Yes	• Easy to implement • Supported on many servers, but insecure • Requires clear text transmission • Uses databases
EAP–TLS	Yes	No	• Requires client as well as sever side certificates • Increases maintenance costs
EAP–LEAP	Yes	Yes	• Proprietary solution from CISCO • AP must have LEAP support
EAP–SIM	Yes	No	• Uses SIM card and authentication methods from GSM wireless standards
EAP–TTLS	Yes	No	• Creates secure SSL tunnel • Supports legacy authentication methods • User identity is protected
EAP–PEAP	Yes	No	• Similar to EAP–TTLS • Creation of a secure SSL tunnel • User identity is protected
EAP–SPEKE	Yes	No	• Proprietary solution from Interlink Networks • Based on Diffie–Hellman algorithm

2.4.1. Enterprise architecture framework

The architecture framework followed by EAP standards involves three basic entities to complete the authentication procedure: the user, authenticator, usually an access point in wireless LANs, and an authenticating server, such as an AAA or RADIUS server. While many methods have been devised which are not proprietary have seen some success, proprietary standards like Cisco LEAP and Interlink SPEKE have encountered obstacles to their widespread acceptance. Some of these include the requirement for client software to be installed and limited choice of access points. Still other EAP methods do not enjoy universal support among operating systems or require database support for authentication servers. Thus network administrators must balance the need for security against other deployment concerns such as cost and user convenience.

2.4.2. Reuse of existing hardware

While advances have been made to the security methods available, there are still numerous existing wireless networks with no security or very vulnerable security methods in place. For these scenarios, it is beneficial to the enterprise to have an EAP method which can make use of existing hardware.

2.4.3. Network layout

Even more prevalent than the existing wireless networks requiring upgraded security measures are the number of wired networks which have not had wireless access implemented. For these scenarios, an EAP method is desirable which requires a minimum of required change to existing wired networks.

With these requirements in mind, we can assess which are applicable to the network in consideration. In Section 3, we survey the available EAP methods and see which methods satisfy a particular subset of the requirements discussed. Table 1 gives a brief snapshot of the requirements supported by various EAP methods.

3. EAP methods

Modern wireless networks secured with Wi–Fi Protected Access (WPA) or the 802.11i standard also referred to as WPA2 in enterprise mode use authentication techniques based on the IEEE 802.1X standard. 802.1X dictates the use of an extensible authentication protocol (EAP) in a point-to-point network. EAP definition in 802.1X does not specify an exact method, algorithm, or procedure for the authentication but rather specifies a framework into which a particular method can be plugged.

Some EAP methods have been developed specifically for wireless networks in addition to EAP methods existing for wired networks. This includes a class of methods based on public key encryption and the use of certificates as well as a class of methods that use not certificates but passwords for their authentication methods.

3.1. Legacy based methods

3.1.1. EAP–MD5 [12]

The mechanism of action of EAP–MD5 is to collect a username and password from the user to be authenticated, encrypt that via the MD5 message hashing algorithm, and pass that data on to a RADIUS server. However, it is a rather simple EAP method and has significant flaws. It offers no mechanism by which to change keys over time so the same issue of constant keys which WEP faces is an issue with MD5. In addition, MD5 encryption cannot fulfill the requirement for symmetric authentication between client and access point and access point and client as specified in the RFC pertaining to EAP over wireless networks. This makes it susceptible to man-in-the-middle attacks as well. Due to these vulnerabilities and no significant advantages over WEP, there are no good arguments for it to be implemented instead of WEP. It should not be considered to be a secure EAP method.

3.2. Certificate based methods

3.2.1. EAP–TLS

EAP–TLS [13] (Transport Level Security) is an EAP method based on RFC 2716 using a public key certificate authentication procedure within the EAP framework. It provides a means for mutual authentication between the client and the authenticator as well as between the authenticator and the client. This has a prerequisite that each entity being authenticated, including the client and access point, possess a public key certificate signed by a mutually trusted certificate authority. This solution has strong authentication properties and is very secure. However, it does require a public key infrastructure to be in place in order to work. This necessitates purchase of certificates from an outside central authority or the added deployment of the infrastructure for the enterprise itself to become a certificate authority. For this reason it is more costly to implement than password based methods. There is also the issue of distributing the certificates to all the entities on the network. The notable features provided by EAP–TLS are mutual authentication, key exchange and establishment, support for fragmentation and reassembly, and fast reconnect.

3.2.2. EAP–TTLS

TTLS [14], or tunneled TLS (Fig. 1), is an extension on transport layer security. In this EAP method, a secure tunnel is established between the server and the client using a public key algorithm and certificates issued by a mutually trusted

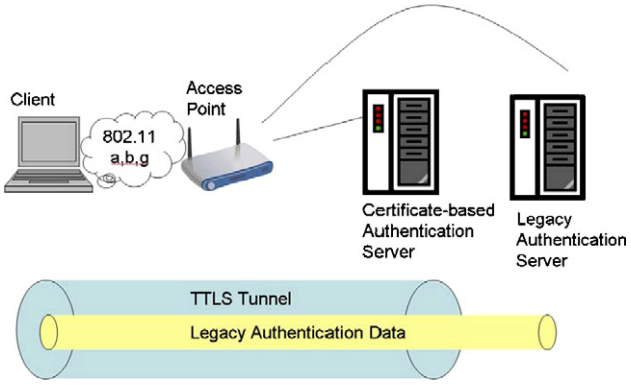

Fig. 1. TTLS authentication [16].

certificate authority. Once this tunnel is established, another authentication method is employed and that transaction is communicated via the secure tunnel.

Because the authentication exchange now takes place via a secured tunnel, a less secure authentication method can be used. This is often a less secure EAP method, such as MD5, or another legacy method of authentication such as PAP or CHAP. If the client is authenticated and authorized to join the network, another tunnel can be established to handle data encryption. This EAP method provides benefits of mutual authentication, secured cipher suite negotiation, the ability to use both passwords and certificates, and to keep the user's identity private since any password authentication would occur inside of a certificate-secured tunnel.

3.2.3. EAP PEAP

Protected EAP (PEAP) [5,15] is an EAP method which behaves in a manner similar to that of TTLS. It creates a TLS session in order to carry an authentication transaction in an encrypted fashion (Fig. 2). Within the encrypted tunnel, another potentially less secure authentication method can be used. However, unlike TTLS, PEAP authenticates the authenticator to the client, but not in the other direction. This reduces the complexity and cost by only requiring certificates to be present on the authenticators, not on the clients. Some benefits of PEAP include message authentication and encryption, secure key exchange, fragmentation and reassembly ability, and fast reconnect. PEAP is one of the most secure EAP methods, but has not gained universal acceptance because Microsoft and Cisco each support differing implementations of the method.

3.3. Password based methods

Using a password based authentication method has some advantages over a certificate based method, most notably cost and ease of use. Cost is potentially less due to no certificate purchases or self-certificate authority setup being necessary for the enterprise. Ease of use is enhanced by allowing users to have an easy to remember password rather than a cryptic key. However, unlike certificate based methods, password based methods can be susceptible to dictionary attacks.

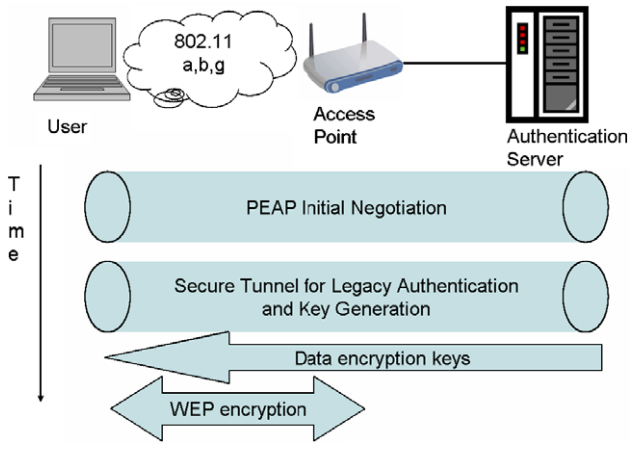

Fig. 2. PEAP authentication [16].

3.3.1. LEAP

LEAP [5,16,17,21], or Lightweight Extensible Authentication Protocol, was developed by Cisco and is their proprietary method for EAP based on mutual authentication between server and client and using a username/password scheme.

LEAP promotes session independence by regenerating keys for each session, thereby leaving prior and subsequent sessions secure even if a single session is attacked. It also helps protect against denial of service attacks or theft of service by authenticating all connections before allowing traffic to be transmitted to a device.

However, since it is a password based method and the challenge and response dialog is not via an encrypted tunnel, LEAP is susceptible to dictionary attacks. Still, if implemented with a strong password policy, LEAP can provide a significant security advantage over WEP without the added complexity or expense of using public key certificates.

3.3.2. SPEKE

SPEKE, or Simple Password Exponential Key Exchange, is a proprietary EAP method from Interlink Networks. The SPEKE [11,17] method uses mutual knowledge of a password in both the authenticator and the client to generate a series of messages to be exchanged of apparently random contents. Once both parties are in agreement that the password is correct, a master session key will be shared between the devices for subsequent use. The additional strength in this method is derived from a public key computation which creates a large random number modulo a large prime, effectively giving a one-way function due to the relative difficulty of performing the discrete logarithmic functions required to reverse it.

The advantages of the SPEKE method is that it gains the security of public key encryption methods for key transfer and authentication procedures without the expense and complexity of deploying certificates. In addition, the mechanism is not as sensitive to dictionary attacks as other password based methods.

3.4. EAP SIM

RFC drafts are under way to submit a new method for EAP using Subscriber Identity Modules, [18,19,22] which provide the current standard authentication method used by many cellular equipment providers. This EAP method uses as a credential a smartcard-like device which can provide storage for a variety of data. Clients would use these SIMs in order to provide credentials contained on them for use in authentication procedures.

The method of using EAP with SIM cards in a wireless network would be similar to that of the current authentication technique used in GSM wireless networks. Identity privacy is provided via the mechanism of pseudonyms and provides for key derivation from a master key. The procedure is based on a challenge and response method using a series of RAND

challenges to generate a set of keys for data encryption. While this method has the benefit of allowing a physical device to be used as a credential rather than a key or password, it is not session-independent as the same SIM card would be reused for all sessions by a user or device.

3.5. EAP–AKA

A slight variation on EAP–SIM under consideration is EAP–AKA, or authentication and key agreement [20,17,5]. This standard is developed by the 3GPP and replaces the SIM cards used in EAP–SIM and on GSM networks with user service identity modules or USIMs used in UMTS networks. Though the procedures and methods are similar between EAP–SIM and EAP–AKA, EAP–AKA presents a stronger level of security than EAP–SIM due to the use of permanent keys for mutual authentication.

3.6. Issues with certificate based methods

Despite the many advantages of certificate based EAP types, there are some disadvantages as well [5,17].

3.6.1. Administration cost

The concept of certificates assumes that there will be a mutually trusted third party that will attest to the validity of the certificates in use. Due to this requirement, there is significant cost involved in either purchasing certificates from a well-known issuer for all devices or setting up the software and requisite training and procedures in order for an enterprise to become their own certificate issuer and central authority.

3.6.2. High protocol exchange

Certificate based EAP methods comparatively require longer message exchanges in order to authenticate on a network. This has the disadvantages of lengthening the time required to complete the exchange and increasing the computing power required to do so. The time involved would be disadvantageous in a roaming scenario while the increase in computing power necessary would be detrimental to small independent devices such as PDAs or RFID tags.

3.6.3. Unable to authenticate user

Finally, certificate based methods authenticate whatever the certificate is programmed within; almost universally, this is the device rather than the user. This leaves the network susceptible in the event that devices are compromised.

Tables 1 and 2 below give an overview of the methods and technologies introduced for EAP as well as how they fit the requirements detailed in Section 2. While implementation of an EAP method is a significant step in securing a network, wired or wireless, even within the EAP procedure there are security issues and vulnerabilities which must be addressed. These shall be discussed in Section 4.

4. Possible attacks [23,28]

Use of an EAP method to securely authenticate users or devices to a network does not necessarily provide guaranteed security. There can be attacks against the EAP procedure. A secure EAP method will have protections against such attacks. Some of the attacks possible on the EAP method include:

- Discovering user identities by reading unencrypted authentication exchanges.
- Modifying or spoofing EAP packets. Denial of Service attacks using spoofed authentication responses, replay attacks, or packets with overlapping identifiers.
- Dictionary attack, or using a list of common passwords in order to attempt to gain access by simulating the authentication exchange offline.
- Recovery of keys if an EAP method uses key generation techniques which are not secure.
- Man-in-the-middle attack in which an attacker pretends to be a point of access into a trusted network to the client wishing to connect but in reality is not that network at all.
- Interfering with negotiation of encryption parameters including the encryption type used in order to negotiate a less secure type which is easier to launch a subsequent attack against.
- Simulating an authenticator and providing false information to either the client or the EAP authenticating server.

Table 2
EAP requirements for wireless LANs [11]

Requirements	EAP–MD5	EAP–TLS	EAP–TTLS	EAP–LEAP	EAP–PEAP	EAP–SPEKE
Mandatory						
Generation of keying material	No	Not required	Yes	Yes	Yes	Yes
Mutual authentication	No	Yes	Yes	Yes	Yes	Yes
Self protecting	Yes	Yes	Yes	Yes	Yes	Yes
Resistance to dictionary attack	Only with long passwords	Yes	Yes	No	Yes	Yes
Protection to MITM attack	No	Yes	Yes	Yes	Yes	Yes
Protected cipher suite negotiation	No	Not required	Yes	Yes	Yes	Yes
Recommended						
User identity hiding	No	No	Yes	No	Yes	No
Faster reconnect	No	Yes	Yes	No	Yes	No

Table 3
Comparison of encryption technologies and possible attacks

EAP method	Encryption technologies	Possible attacks
EAP–MD5	One-way message digest	• Dictionary attack • Man-in-the-middle attack
EAP–TLS	Digital certificates	Strong authentication, resistant to attacks.
EAP–TTLS	• Digital certificates or • Diffie–Hellman algorithm to generate keying material • Symmetric key for data encryption	Strong authentication, resistant to attacks
EAP–SIM	Symmetric key generated using GSM authentication key	• Possible spoofing • Does not provide session independence
EAP–PEAP	• Digital certificates or • Diffie–Hellman algorithm to generate keying material • Symmetric key for data encryption	Strong authentication, resistant to attacks
EAP–LEAP	• Diffie–Hellman algorithm to generate keying material • Symmetric key for data encryption	Dictionary attack

In Table 3, a comparison of the various EAP methods and the attacks to which they may be susceptible is presented. As wireless LAN coverage becomes more ubiquitous, the likelihood that a user will roam between access points and even networks also increases. For these reasons, we consider in the next section some mobility issues related to the EAP methods discussed.

5. Mobility issues

As more and more users join wireless networks, some consideration must be given to the flexibility of an EAP method chosen to operate in a mobile scenario. This might include a user who travels from one wireless LAN to another wireless LAN implementing the same or a different EAP protocol. Moreover, consideration should be given to the use of EAP in scenarios traversing different networks, such as a user moving between a wireless LAN to a cellular network or from a wireless LAN to a WiMAX network. This could also be extended to address macro-mobility as in the cellular model, which may see a user roaming between a home and visitor network. Here we address three issues in a mobile environment.

5.1. Fast reconnection during handoff

When a mobile user moves within the same network, it requires re-authentication to the access point to remove the possibility of rogue access point or malicious user. A new session has to be established with new access point in range. The optional characteristics of fast reconnect are required to reduce the burden of authentication. As discussed in the requirements, all the certificate based methods have the capability of fast reconnect but the password based methods have to follow the complete procedure again.

5.2. Home and visitor networks

For a mobile user moving from one network to another having dissimilar characteristics, the authentication procedure becomes more complex. The visited network may use the same or a different authentication method. No such technique or provision is available in current EAP methods to communicate in above this scenario. A protocol such as the emerging Protocol for Carrying Authentication for Network Access (PANA) [29,30] must be used along with an EAP method. In this manner, networks using different link or physical layer technologies or even entirely different network topologies would be able to securely transmit authentication data.

5.3. Handoff between heterogeneous networks

One of the current topics of research in WLAN is roaming of a wireless user between heterogeneous networks. [31] Significant work has been done on making and deciding categories on handoff procedures. Still, a universal method to authenticate roaming user into foreign domain having different characteristics does not exist. For example, when a cellular user moves from cellular network to a WLAN, the authentication mechanism used by the WLAN should be able to inter-work with authentication mechanism used by the cellular user.

The EAP methods discussed are not limited to use with wireless LANs; they can be used in a variety of wired and wireless networks. Two types of wireless technology growing in popularity are RFID and WiMAX. These networks, like wireless LANs, also have a requirement for security when used in enterprise settings. In Sections 6 and 7, we address the unique security issues related to these networks and investigate the possibility of using EAP methods to secure them.

6. RFID

Radio frequency identification is a new generation technology used to identify objects to which transponders are attached. In this method, each object has a transponder with some unique data encoded to it; a reader is used to retrieve this data using near field communication. Some common applications of RFID are tracking items throughout a manufacturing process, identifying shipping containers, and inventory management in supply chain services. Use of RFID technology can bring about benefits in any situation where objects need to be identified or tracked. Here we will analyze the various authentication schemes available for RFID authentication.

6.1. Requirements for RFID authentication

6.1.1. Mutual authentication

RFID tag and reader must mutually authenticate before an RFID reader could access information stored on tags.

6.1.2. Re-authentication required

As a reader has to regularly monitor the tag, the authentication mechanism should have a possibility of re-authenticating tag as well as reader.

6.1.3. Access control

The RFID EAP mechanism should be capable to support multiple authentication methods such as allowing users to log in using a user ID and password, digital certificates, shared secrets, secure tokens, etc.

6.1.4. Logging

There should be support for logging and auditing events such as authentication and authorization events, including both successful and unsuccessful access to resources, password changes, and administration or management events [2].

6.1.5. Immunization to attacks

RFID mechanism should be able to defeat eavesdropping, traffic analysis, spoofing, man-in-the-middle attacks, and denial of service.

6.1.6. Limited memory required

RFID tags are commonly being deployed as a replacement for optical bar codes. For that reason, it is important that the RFID tags be low in cost. The most important factor which increases the cost of tag is the size of memory. In order to reduce the cost, it is important for authentication mechanism to have a small memory requirement.

6.2. Authentication mechanisms

6.2.1. Fixed read access protocol

This is a fixed read access control as the authentication key is fixed. The reader has a unique authentication key to authenticate with each tag. The tag holds the hashed value of this key. As the reader requests for tag ID, the tag sends the hashed value. In response, the reader sends the key corresponding to the hashed value sent by the tag. The tag then hashes the key and compares it with the hashed value. Once the comparison is successful, tag sends its own ID to the reader.

The fixed read access protocol has the advantage of requiring only a small amount of memory on the tag as it needs only to store the hash function and the hashed value. This method also provides privacy control at low cost. However, the method is susceptible to eavesdropping of both the key and tag ID and is also susceptible to a man-in-the-middle attack.

6.2.2. Randomized read access control

There are two possible schemes proposed for a randomized approach:

6.2.2.1. Randomized hashing. The first approach was proposed by MIT Auto ID center as a randomized hash scheme. [32] Compared to fixed access control method, the hashed value stored in a tag changes every time the tag is queried. Each tag shares an authentication key ID_k with the reader. Every time a tag is queried it generates a random number R and sends output $(R, h(ID_k \| R))$. On receiving this output, the reader accesses all the authentication keys present in backend database and applies the hash function to all the values. If the calculated value matches the value sent by the tag, the reader identifies the authentication key for the tag and sends it.

Randomized hashing has the benefit that since the random number changes every time, the possibility of tracking and eavesdropping of the information is removed. However, it introduces the limitation that if the number of tags is high, the computational load to calculate the hashed value for each key becomes very high. This method is optimally used by applications where there are a smaller number of tags involved.

6.2.2.2. Multiple function hashing. In the second approach [33], the tag uses two hash functions H and G — one to produce the output which is sent to the reader and the other to generate a random number for the next access to the tag. An initial random number is shared between the tag and reader. The output is then sent to the reader. In the backend database, a pair of values are stored (Random number, ID).This random number is updated with each access to tag using the same hash function G.

This method employing multiple hashes provides forward security due to its use of a one-way hash function and reduces the risk of eavesdropping, man-in-the-middle attacks, and spoofing. However, it is computationally intense and requires numerous comparisons which also lead to an increased tag cost and load on the tag's ROM.

6.3. Selection of an EAP method for RFID

RFID is coming into widespread use as a means to communicate data between objects and readers in business contexts. EAP has proven its usefulness as a means of securing authentication of networks, both wired and wireless. EAP, if combined with RFID, can provide a safe and secure path for transfer of data. Here, we try to analyze the EAP methods which can satisfy EAP requirements and can be adopted as a possible conjunctive approach for RFID mechanism.

As one of the requirements states, it should mutually authenticate tag and reader which removes EAP MD5 as a possibility. Also, the chosen RFID authentication mechanism should be capable of authenticating user using user ID and password, digital certificates, shared secrets, secure tokens, etc. and should be free from eavesdropping, man-in-the-middle attack, and spoofing. This makes EAP–PEAP a good choice for being embedded in RFID authentication mechanism, as it is one of the EAP methods where once the TLS tunnel has been established, the user can use credentials of its choice to authenticate. Other than PEAP, no other major EAP method has such a facility.

Though EAP–PEAP satisfies most of the requirements, the important factor to be considered is whether RFID tags will be able to bear the burden of maintaining the certificates, at least from the authentication party side. Another constraint is that EAP–PEAP should not increase the memory size and in turn

cost of the tag, which is important for the widespread deployment of RFID Technology.

7. WiMAX

WiMAX, or Worldwide Interoperability for Microwave Access, is an emerging technology based on the IEEE 802.16 standard for a Metropolitan Area Network (MAN) which strives to provide broadband wireless access capabilities across a wider area than the typical WLAN. [24] As with any wireless data transmission method, there are some issues relating to securing these transmissions which must be addressed in order for users and service providers to have confidence in the platform. As with WLAN, attention should be given to preventing unauthorized access to the wireless broadband network as well as assuring the confidentiality of data transmitted across the network.

7.1. WiMAX architecture

WiMAX can operate in either point-to-point or point-to-multipoint modes. Point-to-point operation would be typical for use as a high-speed backhaul between base stations, using primarily licensed frequencies near the microwave spectrum with line-of-sight propagation. Point-to-multipoint operation would be typical for transmissions between a base station (BS) and subscriber station (SS) using lower licensed or unlicensed frequencies and non-line-of-sight propagation. There is also an option to extend the point-to-multipoint operation to include mesh networks, thereby enhancing the robustness of the network and making it less susceptible to single points of failure. Bandwidth varies due to such factors as distance and attenuation between the base station and subscriber station. The IEEE standard 802.16 and its extensions took experience of security with WLANs and used it in order to integrate robust security measures to become part of the standard.

The 802.16 standard allows for different PHY layer implementations, making it flexible in terms of available frequency, topology, and transmission techniques. On top of the multiple options for the PHY layer is a multi-layered MAC layer. One of the layers within the MAC layer is the security sublayer. It is this layer which is responsible for providing the services which serve to implement security in the standard, such as authentication, secure key exchange, and encryption [25,26].

The 802.16 standard introduces the idea of a Security Association, defined as "the set of security information a BS and one or more of its client SSs share in order to support secure communications across the IEEE Std 802.16 network." [26] The data contained within a security association is all the keying information necessary at either endpoint, data determining what encryption or keying method will be used, and the lifetime of such data. The standard sets out three types of security associations (SAs):

- *Primary* SAs, established during SS initialization and initial communication with the BS, which may be used for any transport connection, as well as multicast transport connections and secondary management connections between the BS and the SS.
- *Static* SAs, which are specific to a BS and used to communicate with multiple SSs as part of a multicast connection.
- *Dynamic* SAs, which are similar to static SAs but are provisioned and destroyed as necessary.

7.2. Authentication and authorization

When a subscriber station wishes to initiate communication with a base station for the first time, it must go through an authentication procedure. In this procedure, the BS must authenticate the identity of the SS, assign to the SS an authorization key, and inform the SS of any SAs it may have access to. This authorization procedure is periodically repeated to refresh keys whose lifetimes are near expiry as defined by the lifetimes present in the SA definition.

Each 802.16-compliant device shall use an X.509 certificate to establish its authenticity and validity against an external source for use as a public key. As part of its authentication procedures, the SS shall provide this certificate to the BS, as well as a listing of the encryption and keying capabilities it supports. If this data is acceptable to the BS, it shall send back to the SS an authorization key and the information about the primary SA as well as other static or dynamic SAs.

The authorization key provided during authorization of the SS is one of many types of keys used in 802.16 security. The standard dictates use of the following keys:

- *Authorization Key* (*AK*). Encrypted using the RSA public key scheme with the SS's public key in its X.509 certificate, this key is granted during initial SS authorization and is refreshed at the end of its lifetime as specified in the SA parameters.
- *Key Encryption Key* (*KEK*). Derived from the authorization key by the BS, this key is used to encrypt the traffic encryption key when it is transmitted to the SS.
- *Traffic Encryption Key* (*TEK*). Encrypted with the key encryption key, this key is used as the key for the encryption mechanism that will be used to secure the actual payload traffic between the SS and BS and vice-versa.

Once the SS is authorized, it performs traffic encryption key exchange procedures in order to retrieve keys to be used in encrypting the payload traffic. As with the authorization key procedure, this procedure is repeated periodically when the lifetime of the TEK is approaching expiry.

7.3. Selection of an EAP method for WiMAX

Efforts are being made to learn from the experiences with 802.11 regarding security and integrating a strong level of security into the 802.16 standard. This is evidenced by the inclusion of a more secure data encryption mode in the 802.16-2004 standard, not present in the original 802.16 standard. Still,

the standard does not support EAP which would even further enhance WiMAX security; however, use of any externally defined EAP method, including those mentioned above for wireless LANs, will become part of the to-be-released 802.16e amendment.

The standard proposes to extend the privacy layer to include an EAP layer which contains the externally defined EAP method. The specific method chosen can be any method following the 802.1X guidelines which could be used for other wireless or wired networks. In the proposed standard, a control interface is implemented in the privacy layer to convey data between the EAP method and the existing security methods [27].

The proposed updates to the 802.16e standard give some discussion of which EAP method might be appropriate to secure WiMAX connections, especially in a mobile context. It outlines some requirements for the EAP method chosen: it must be compatible with 802.16 systems not using EAP, it must support all other functionality currently defined as part of the standard, including security associations, it should provide for cipher suite selection and negotiation, and should be compatible with standard EAP methods such as those used with 802.11 networks. [27] Additionally, support for faster reconnect would be beneficial as 802.16 might later be used in a mobile environment.

With these requirements in mind, EAP–MD5 can be eliminated as a possibility due to its previously discussed security vulnerabilities and lack of support for mutual authentication. Because it provides support for mutual authentication, protected cipher suite negotiation, and faster reconnect, EAP–PEAP would be a good choice as a method to secure WiMAX.

8. Conclusion

Since the advent of wireless LANs in 1997, the technological progress in this field has been tremendous. With the technological progress, however, came security vulnerabilities. All the methods discussed in the report have had their share of flaws and limitations. Most of the methods are either currently deployed or still in the process of deployment.

As discussed in the report, we have two major sets of methods currently deployed, namely certificate based and password based. Large corporations and enterprises choose certificate based methods as they can afford more security at the cost of their deployment and administrative burden, while password based methods which are more user-friendly are more suitable for individual users. Other than their ability to be suitable for deployment in different conditions, most of these methods are also hampered by interoperability issues.

Nearly a decade ago when widespread research started on technologies related to telecommunication and wireless LANs, both fields had a different mode of operation and a completely different set of protocols. With the widespread use of these technologies and the progress they have made, current research work is now concentrated on how different technologies can be combined and made mutually beneficial to end users.

The need for security in emerging wireless technologies such as RFID and WiMAX is evident. Based on the benefits that EAP methods can bring to securing a wireless LAN, along with the flexibility of being pluggable to any procedure that supports an EAP, the methods discussed are also candidates for securing networks based on new technologies. New physical and link layer techniques as well as different network technologies will have their unique set of requirements for what functionality an EAP method should support.

As the use of wireless devices in a mobile context increases, authentication of users in inter-domain environments will be a key issue to be addressed by EAP methods. The qualities of security, lightweight demands on processor and memory, and interoperability across networks and network types and topologies will all be essential in EAP methods moving forward. Further research is needed in developing an EAP method which resolves some interoperability issues with the current methods and is well suited to deployment in a wide variety of scenarios. Additionally, work should continue to be done to improve the strength of the algorithms used for authentication and key management.

Acknowledgements

This material is based upon work supported by the National Science Foundation under grants CNS-0516807 and CNS-0551694. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] B. Mitchell, What is infrastructure mode in wireless Networking, www.compnetworking.com.
[2] J. Geier, Understanding Ad Hoc Mode, www.wirelessnetworking.com., Aug 2002.
[3] H. Boland, H. Mousavi, Security issues of IEEE 802.11b wireless LAN, Canadian Conference, 2004.
[4] J. Geier, 802.11 WEP: Concepts and Vulnerability, www.wirelessnetworking.com., June 2002.
[5] Securing Wireless LANs with PEAP and Passwords, Introduction: Choosing a Strategy for Wireless LAN Security, www.microsoft.com., April 2004.
[6] J. Snyder, Network World Global Test Alliance, What is 802 1x? www.networkworld.com., May 2002.
[7] J. Geier, 802.1X Offers Authentication and Key Management, www.wi-fiplanet.com., May 2002.
[8] P. Congdon, B. Ababa, A. Smith, Zorn. Roese, IEEE 8021X Remote Authentication Dial in User Service (RADIUS) Usage Guidelines, RFC 3580, September 2004.
[9] Trapeze Networks, Enterprise WLAN Security: Making Sense of the options, White Papers.
[10] D. Stanley, J. Walker, B. Aboba, EAP Method requirements for Wireless LANs, RFC 4017, March 2005.
[11] Interlink Networks, Advantages of EAP–SPEKE over EAP–PEAP for Password Based Authentication, March 2003.
[12] L. Blunk, J. Vollbrecht, PPP Extensible Authentication Protocol (EAP), RFC 2284, March 1998.

[13] B. Aboba, D. Simon, PPP EAP TLS Authentication Protocol, RFC 2716, October 1999.
[14] P. Funk, S. Blake-Wilson, EAP Tunneled TLS Authentication protocol version 1, February 2005.
[15] H. Andersson, S. Josefsson, G. Zorn, D. Simon, A. Parlekar, I-D ACTION: draft-josefsson-pppext-eap-tls-eap-tls-eap-04.txt: Protected EAP, IETF Draft, , September 2002.
[16] S. Convery, D. Miller, S. Sundaralingam: Cisco Systems, Cisco SAFE: WLAN security in Depth, White Paper.
[17] Interlink Networks, EAP Methods for Wireless Authentication, April 2003.
[18] Meeting House, EAP SIM, White Paper.
[19] H. Haverinen, J. Salowey, Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP–SIM), IETF Draft, December 2004.
[20] J. Arrko, H. Haverinen, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key agreement (EAP–AKA), IETF Draft, June 2005.
[21] J. Snyder, EAP (Extensible Authentication Protocol): What is 802.1x? www.Networkworld.com., May 2002.
[22] S. Patel, Analysis of EAP–SIM Session Key agreement, www.Drizzle.com.
[23] N. Borisov, I. Goldberg, D. Wagner, Intercepting Mobile Communications: The insecurity of 802.11.
[24] IEEE 802.16 Working Group, IEEE 802.16 Backgrounder, http://grouper.ieee.org/groups/802/16/pub/backgrounder.html..
[25] D. Johnston, J. Walker, Overview of IEEE 802.16 Security, Security and Privacy Magazine, IEEE 2 (3) (2004) 40–48.
[26] IEEE Computer Society, IEEE Microwave Theory and Techniques Society, IEEE Standard for Local and Metropolitan Area Networks: Part 16. Air Interface for Fixed Broadband Wireless Access Systems, IEEE Std 802 16™-2004. 1 October 2004.
[27] J. Mandin, Enhancement of 802.16e to Support EAP-based Authentication/Key Distribution, 802.16e Security Ad Hoc Committee, http://www.ieee802 org/16/tge/contrib/C80216e-03_71r4.pdf.
[28] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Extensible Authentication Protocol (EAP), 3748
[29] M. Parthasarathy, Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security 4016.
[30] A. Yegin, Y. Ohba, R. Penno, G. Tsirtsis, C. Wang, Protocol for Carrying Authentication and Network Access (PANA) Requirements, RFC 4058.
[31] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, Network Mobility (NEMO) Basic Support Protocol, RFC 3963.
[32] S. Weis, S. Sarma, R. Rivest, D. Engels, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, MIT Auto ID Center, http://theory.lcs.mit.edu/~sweis/spc-rfid.pdf.
[33] M. Ohkubo, K. Suzuki, S. Kinoshita, RFID Privacy Issues and Technical Challenges, Communications of the ACM 48 (9) (September 2005).