Access Point Security Service for wireless ad-hoc communication

Mark Nijdam
BT plc.
Martlesham Heath, Suffolk, UK
mark.nijdam@bt.com

Hans Scholten
University of Twente
Enschede, the Netherlands
j.scholten@ewi.utwente.nl

Abstract

This paper describes the design and implementation of a security solution for ad-hoc peer-to-peer communication. The security solution is based on a scenario where two wireless devices require secure communication, but share no security relationship a priori. The necessary requirements for the security solution described here comprise topics such as energy efficiency, security standards and ad-hoc networks. The devised solution is called Access Point Security Service (APSS). APSS is able to provide security by delivering a symmetric key to two wireless devices that require ad-hoc peer-to-peer communication. The main principle of APSS is that it makes use of an existing security relationship between a network provider and its customers. The existing security relationship enables the network provider to deliver security to two or more communicating parties in the form of a shared key. An implementation of APSS is provided making use of the existing Wi-Fi security standards.

1. INTRODUCTION

Mobile ad-hoc networks allow two or more mobile nodes to communicate directly with each other as long as they are in transmission range. Communication in an ad-hoc network does not require the existence of a fixed, infrastructure network which provides users a great deal of flexibility; everyone is allowed to join and leave the network at will. This flexibility however is, at the same time, the cause of security issues as it makes it easier for malicious users to share in the communication.

This paper considers a scenario that exposes one of the security problems regarding mobile ad-hoc networks. The scenario comprises of two people meeting each other for the first time at a conference. They decide to keep in touch during the remainder of the conference using a wireless connection between their mobile devices. The communication between their mobile devices can be considered ad-hoc peer-to-peer communication as it connects both mobile devices on an ad-hoc basis and does not require components from a fixed network.

Data confidentiality and authentication are normally provided using cryptographic techniques. These techniques are founded on an existing security infrastructure. Security is an issue in this scenario however as both persons have not established a security relationship yet, making cryptographic techniques impossible or difficult. A security relationship in this paper signifies the establishment of a shared secret. The scenario uncovers a problem that is applicable to situations where two devices require secure ad-hoc peer-to-peer communication for their initial contact.

The paper is structured as follows: chapter two describes and compares existing techniques to set up a security relationship between two devices; chapter three presents a newly devised security solution called Access Point Security Service (APSS); chapter four describes an implementation of APSS using the Wi-Fi security standards.

2. SECURITY SOLUTIONS

Cryptography is either based on symmetric keys or asymmetric keys. The cryptographic keys are used for decrypting and encrypting data and signify a security relationship established between sender and receiver.

2.1. Symmetric key cryptography

Symmetric key cryptography relies on two or more parties sharing a key. Data encryption and decryption are done using the same shared key. In a typical configuration a sending party encrypts the data with the key before sending and the receiving party decrypts this upon receipt, again using the symmetric key.

The matter in which the encryption/decryption is done depends on a symmetric key algorithm. These algorithms are of varying complexity and security. It is important to understand that the level of security of the algorithm greatly depends on the length of the key. Typical symmetric key algorithms are DES, AES and RC4.

The advantage of symmetric key cryptography lies in its relative simplicity. The security of the data relies just on keeping the key secret. This simplicity in cryptography results in the algorithms being efficient with resources. Wireless devices tend to be resource lean devices with limited battery life and processing power, which makes symmetric key cryptography the first choice for this kind of communication.

The disadvantage of symmetric key cryptography is the need for some way to securely install the symmetric key in the communicating parties. It is difficult to establish a common key when no prior security relationship exists between two communicating parties.

Several protocols, called key establishment protocols, exist that are used to set up a shared key between two nodes [1]. Typical key establishment protocols are Needham-Schroeder, Kerberos and Otway-Rees [2]. Total security architecture SPINS makes use of SNEP as a key establishment protocol [3]. All of these protocols require the use of a Key Distribution Centre (KDC), a trusted third party responsible for distributing the keys. The principle of a KDC is depicted in Figure 1.

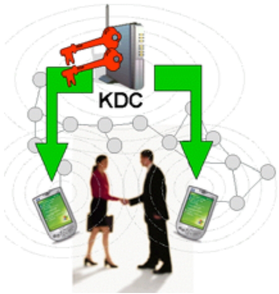

Figure 1. A Key Distribution Centre

The disadvantage of using a KDC is that it also requires a phase where the KDC is set up. All nodes using the key establishment protocols have to register with the KDC beforehand; the nodes have to share a secret with the KDC to make key establishment protocols work securely.

2.2. Asymmetric key cryptography

Asymmetric key cryptography is better known as public key cryptography. Unlike symmetric key cryptography, there is no requirement for a shared key that has to be set up before encryption and decryption is possible. Each communicating party holds a key pair, consisting of a public and a private key. The private key is a secret key and must never be shown to anyone else than the owner. The public key however is not secret and is usually advertised to anyone interested. Data encrypted by one of the keys in the key pair can only be decrypted by the other key. In a typical scenario a sending party uses a public key to encrypt data. The only party able to decrypt this data is the party that possesses the matching private key. Typical public key algorithms are RSA, DSA and ECC, of which RSA is the most popular.

The obvious advantage of public key cryptography is that it does not require a possibly complex key setup phase like in symmetric cryptography; public keys can be sent or advertised in the clear, which makes key setup a breeze.

One of the disadvantages is related to energy consumption. The complexity of the mathematics involved in public key cryptography makes it a non trivial business to encrypt and (especially) decrypt data. It remains to be seen if all devices can perform these operations. Several papers have presented figures about energy consumption regarding security solutions, most notably [4] and [5]. The figures show that symmetric key cryptography can be up to 1000 times more energy-efficient than public key cryptography.

Another disadvantage comes from a security perspective. A public key contains no personal information and any person can claim to be the person with whom you want to communicate by advertising its public key. For this reason public key cryptography requires a Public Key Infrastructure (PKI). A PKI usually involves a trusted third party server called a Certificate Authority. This Certificate Authority couples an identity with a public key. This 'electronic document' is called a certificate. A solution based on public key cryptography has to take into account that connectivity with the Certificate Authority is necessary.

3. ACCESS POINT SECURITY SERVICE

The previous chapter has shown that security can be provided by either using symmetric or asymmetric key cryptography. Symmetric cryptography seems more applicable to the scenario outlined in the introduction, given that the two persons communicating are using handheld wireless devices; energy-efficiency is important to this type of devices. In that case the only remaining issue is of key establishment.

It makes sense to try and apply the principles of key establishment to the scenario mentioned in the introduction. In that case one of the two devices at the conference would contact a KDC and request a symmetric key for both communicating parties using Kerberos or Otway-Rees. Both attendees of the conference would have to share a secret beforehand with the KDC. The KDC would then create a symmetric key for both nodes and send these back encrypted using the shared secrets (obtained at registration). Both attendees would then be able to decrypt the symmetric key. Secure communication between the two attendees would be possible using the established shared key: multihop communication secured by a network layer protocol like IPsec and singlehop communication secured by a link layer protocol like 802.11.

Even though this is theoretically possible, it is not very likely that KDC servers will be set up in every conference hall just for the use of ad-hoc communication. The two nodes would also need to register with this KDC beforehand to establish a security relationship.

Access Point Security Service (APSS) is a solution that makes use of an existing security relationship to create a KDC-like functionality for the two nodes. A registration phase for a KDC is no longer required when it is possible to use existing credentials. APSS is explained in more detail in the next section.

3.1. Existing security relationships

Normally, Wi-Fi Internet access via a hotspot requires a registration phase where credentials are communicated from the wireless service provider to the customer. The customer needs these credentials to make use of the hotspot services. The assumption of the devised solution is now that both attendees of the conference are 'subscribed' to the hotspot provider. This can be assumed with a high degree of confidence as the increase of hotspots in public places has become a visible trend. The assumption gains even more weight considering that many of the popular telecommunication providers are also big players in the hotspot market. Most people already possess a subscription with a telecommunication provider and have been provided with credentials in the form of SIM cards.

The assumption basically means that the conference attendees share a secret with another party in the conference: the wireless service provider. This shared secret comes in the form of the subscription credentials. Thus, the wireless service provider becomes the trusted third party in the scenario, a KDC.

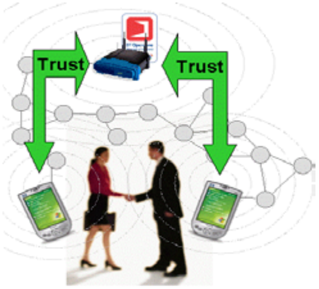

Figure 2. APSS

The resulting trust model proves to be favourable to the considered scenario. The KDC server that is required in the key establishment protocols does not have to be a newly set up server anymore. The wireless access point already has a security relationship with all of the nodes (as customers), so KDC functionality could simply be incorporated. This means the hotspots could provide a security related service, besides just providing Internet access. This security service is the solution to the problem presented in the introduction: APSS (Figure 2). A common opinion is that network providers have no role to play in ad-hoc communication, but APSS proves that this is incorrect. The network providers are in an excellent position to provide all kinds of authenticated services from the infrastructure network to the ad-hoc environment because of the existing security relationship with users. Even the case where both attendees of the conference have different network providers does not present a problem; roaming agreements (for instance in Wi-Fi: [6]) could be used to make authentication in a foreign network possible.

APSS solves the problems that existed with the key establishment protocols. Initialization and registration phases are no longer necessary using the already existing security relationship between the network provider and the user.

3.2. Advantages and disadvantages

The security solution provided by APSS has many advantages:

- Both devices do not have to share a security relationship a priori. APSS is able to establish a symmetric key to provide security between the two nodes. This is especially useful when two nodes have not met before.
- APSS does not require a solution where a KDC has to be set up, but instead makes use of the existing security relationship between wireless nodes and their wireless network provider.
- The shared key delivered by APSS can be used for any peer-to-peer communication afterwards, thereby making the need for availability of an infrastructure network obsolete; the communicating parties can walk away from the access points and still keep on communicating securely with each other.
- The shared key delivered by APSS can be the starting point for many other security protocols. Most of existing security solutions in ad-hoc networks require a pre-shared key to work; APSS provides this.
- APSS makes use of symmetric key cryptography, which is extremely useful in environments where resource-lean devices are used. The (one-time) communication overhead outweighs the energy required for public key cryptography.

There are some side notes to be made regarding APSS however:

- It remains to be seen that APSS principles can be applied to current network access technologies. The next chapter proves it can be done using EAP enabled access control, but EAP is currently only actively used in Wi-Fi access.
- APSS requires an infrastructure network to be in range of the wireless devices. This will not always be the case though.

Overall, the advantages outweigh the disadvantages and therefore the conclusion can be reached that APSS is a suitable solution to the security problems associated with mobile peer-to-peer communication.

The next section introduces an implementation of APSS using the Wi-Fi standards.

4. AN 802.11 IMPLEMENTATION OF APSS

Wi-Fi is a technology based on the IEEE 802.11 standard [7]. Initially, the protocol made use of the ill named Wired Equivalent Privacy (WEP) for both authentication and data confidentiality. The flaws of WEP are well documented [8] and IEEE therefore brought out a security update to the original standard: IEEE 802.11i [9].

Authentication in IEEE 802.11i has been improved with the use of the Extensible Authentication Protocol (EAP) [10]. This protocol is able to incorporate many authentication protocols by making use of flexible challenge-response pairs. Authentication itself is performed by a RADIUS [11] (or similar) authentication server.

Data confidentiality has also been given an upgrade in IEEE 802.11i; keying mechanisms like TKIP, CCMP have been introduced while encryption itself is done using AES.

The authentication framework defined by IEEE 802.1X and EAP is the most relevant when implementing APSS. The next section gives more detail regarding this framework and is followed by the implementation details for incorporating APSS in IEEE 802.11 security.

4.1. EAP and 802.1X

The 802.1X standard provides a framework for authentication in Ethernet based networks [12]. The main principle of 802.1X is that there is a protected resource and that a user can only access this resource by successfully authenticating with an authentication server. In the terminology of 802.1X the protected resource is called a controlled port. There are three entities (see Figure 3):

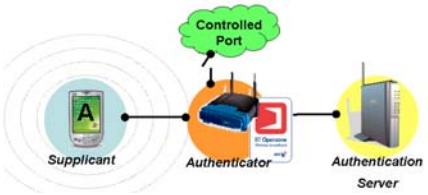

Figure 3. IEEE 802.1X

- Supplicant; this is the role played by a device requesting access to the controlled port. In the figure this is a PDA called A. Authentication takes place between the Supplicant and Authentication Server.
- Authenticator; this is the role played by an access point in 802.11. The controlled port protects a certain resource (for instance: the Internet in hotspots). The Authenticator forwards authentication messages from the Supplicant to the Authentication Server. The controlled port becomes available to the Supplicant after a successful authentication.
- Authentication Server; this role is responsible for performing authentication decisions. Authentication decisions are generally made with the help of user databases, but this is not necessary. The Authentication Server can only be reached through the Authenticator. A secure connection between the two is expected.

802.1X Is strongly linked to the EAP protocol; it specifies the use of this protocol for all authentication messages. EAP is developed to encapsulate authentication data transparently. In theory any two-party authentication protocol can be implemented using EAP messages. Authentication data is carried by means of challenge/response messages.

Several different authentication protocols have been implemented in EAP. These EAP implementations have become standards themselves and have been assigned a type field in the actual EAP standard. Examples of these implementations are EAP-TLS (TLS handshake), EAP-MD5 (password challenge), PEAP (tunneled authentication by Cisco) and EAP-SIM (SIM card authentication).

4.2. A virtual authentication server

Applying APSS to a Wi-Fi environment requires it to make use of the 802.1X framework and EAP messages described above. This is not as straightforward as one might think.

The IEEE 802.1X framework consists of 3 entities. These are the Supplicant, the Authenticator and the Authentication Server. It becomes clear that 802.1X does not fit perfectly when applying these principles to APSS, as there are four parties involved in APSS: the two nodes, the hotspot access point and its authentication server.

For convenience reasons, this paper refers to the two attendees of the conference as Alice and Bob. According to the IEEE 802.1X standard, the controlled port of the Authenticator is only accessible after a successful EAP. In the considered scenario the controlled port indicates secure communication between Alice and Bob; a successful authentication in APSS should open up the controlled port and thus make it possible for secure data exchange. Because of this, Bob and Alice respectively have to attain the role of Supplicant and Authenticator. The hotspot access point however already plays the role of Authenticator in normal operation of the network. It is desirable for the hotspot access point to retain this role so the access point does not need a software update. The Authentication Server in APSS is of course the server managing the customer database (with the credentials of registered users).

A creative solution is required to overcome the incompatibility of APSS with 802.1X and EAP. The key to finding the solution is that the specifications of 802.1X and EAP do not specify any particular Authentication Server implementation. This is done deliberately for reasons of flexibility. This flexibility makes it possible to design a customized Authentication Server. By using a novel idea, a virtual Authentication Server, it is possible to overcome the Authenticator problem. In this case, both node B and the hotspot access point have the Authenticator role. It does not create any problems though, because the APSS process is split up in two 802.1X structures, where the Authentication Server in the first 802.1X structure emulates a Supplicant communicating with the second 802.1X structure (Figure 4).

The problem with the Wi-Fi standards is thus solved. The Authenticator of Bob communicates with an Authentication Server that is also located on Bob's device. This Authentication Server is a piece of software that starts up a Supplicant session (still on Bob's device!). This Supplicant then communicates with the second Authenticator in the hotspot access point. The virtual Authentication Server in Bob's device resumes the first 802.1X session as soon as the second 802.1X instance is successfully concluded. Alice never even notices that this EAP type is fundamentally different than the commonly used ones.

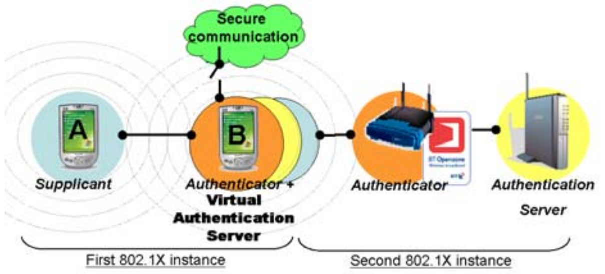

Figure 4. A virtual authentication server

A virtual Authentication Server solution described above can be used for any authentication protocol consisting of three entities. This applies therefore mainly to key establishment protocols like Kerberos and Otway-Rees as these protocols involve two nodes and a KDC.

A solution with a virtual Authentication Server and two EAP methods actually requires the node with the virtual Authentication Server (Bob's device in the scenario) to have link layer associations with two different devices at the same time (ad-hoc mode with Alice's device and infrastructure mode with the hotspot access point). This is not a common thing to do, but could be done in a energy consuming way by using two wireless network cards. However, an application also exists to perform so-called association switching using only one network card. The application keeps track of the state of each of the associations and switches between them, because only one association is allowed to be active at any time [13].

5. CONCLUSIONS AND RELATED WORK

Access Point Security Service is a service that is able to provide a shared secret between two nodes that do not share a security relationship a priori. The difference between existing approaches is that APSS makes use of the existing security relationships between users and network providers. This existing security is used to create a new security relationship between the two nodes. APSS has been implemented for the Wi-Fi link layer.

A demo has been prepared to show the concept of APSS in a Wi-Fi environment. The demo consists of two distinct parts. The first test shows the necessity of security in wireless communication; eavesdropping on unsecured communication is simple and not easily detectable. The second test proves that APSS is able to provide security to the vulnerable wireless communication; eavesdropping is impossible after APSS has been applied to protect the wireless communication.

The solution described here solves the same problem as the solution described in [14]. The difference between the two approaches though is that the latter solution modifies the EAP framework by adding new types of EAP messages. The virtual Authentication Server presented in this section does not require any modifications to the Wi-Fi and authentication standards, which is an advantage.

ACKNOWLEDGMENTS

We would like to thank Mark Pawlewski, Ian Herwono and the other colleagues in the Security Research Centre at BT for helping perform the research presented in this paper.

REFERENCES

[1] A. Menezes, P. Van Oorschot, S. Vanstone, *The Handbook Of Applied Cryptography*, CRC Press, 1996, pp. 497-505.

[2] C. Neuman et al., *RFC4120: The Kerberos Network Authentication Service (V5)*, July 2005, http://www.ietf.org/rfc/rfc4120.txt

[3] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, D.E. Culler, "SPINS: Security Protocols for Sensor Networks" *Wireless Networks 8*, 2002, pp. 521-534.

[4] D.W Carman, P.S. Kruus, B.J. Matt, "Constraints and Approaches for Distributed Sensor Network Security", *NAI Labs Technical Report #00-010*, September 2000

[5] A.S. Wander, N. Gura, H. Eberle, V. Gupta, S.C. Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", *Third IEEE International Conference on Pervasive Computing and Communication (PerCom 2005)*, Kauai, March 2005

[6] GSM Association, "WLAN Roaming Guidelines", *Official Document IR.61*, August 2004.

[7] IEEE Standards for Information Technology, *IEEE 802.11*, 1999, http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[8] N. Borisov, I. Goldberg, D. Wagner, "Intercepting mobile communications: The insecurity of 802.11" *Proceedings of the 7th annual international conference on Mobile computing and networking*, 2001, pp. 180-189.

[9] IEEE Standards for Information Technology, *IEEE 802.11i*, 2004, http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[10] B. Aboba et al., *RFC3748: Extensible Authentication Protocol*, June 2004, http://www.ietf.org/rfc/rfc3748.txt

[11] C. Rigney et al., *RFC2865: Remote Authentication Dial In User Service,* June 2000, http://www.ietf.org/rfc/rfc2865.txt

[12] IEEE Standards for Information Technology, *IEEE 802.1X*, 2001, http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

[13] R. Chandra, V. Bahl, P. Bahl, "MultiNet: Connecting to Multiple IEEE 802.11 Networks Using a Single Wireless Card, *The 23rd Conference of the IEEE Communication Society (INFOCOM 2004)*, Hong Kong, March 2004.

[14] J-H. Lee, H.J. Park, "A User Authentication Protocol Using EAP for Mobile Ad Hoc Networks". *IASTED International Conference on Communication, Network, and Information Security (CNIS 2003)*, New York, October 2003.