Key Establishment Using Secure Distance Bounding Protocols

Dave Singelée

ESAT-COSIC

Katholieke Universiteit Leuven

Belgium

Email: Dave.Singelee@esat.kuleuven.be

Bart Preneel

ESAT-COSIC

Katholieke Universiteit Leuven

Belgium

Email: Bart.Preneel@esat.kuleuven.be

Abstract

Key establishment is one of the major challenges in Wireless Personal Area Networks, as traditional security mechanisms often do not cope with the dynamic characteristics of wireless ad-hoc networks. In this paper, we present an efficient key establishment protocol, based on the basic Diffie-Hellman protocol. It enables mutual device authentication through presence and establishes a session key between personal mobile devices which do not yet share any authenticated cryptographic material. Distance bounding protocols, which have been introduced by Brands and Chaum at Eurocrypt'93 to preclude distance fraud and mafia fraud attacks, are employed to determine an upper-bound on the distance to another entity. Our solution only requires limited user-interaction: the user of a mobile device is expected to perform a visual verification within a small physical space.

1. Introduction

1.1. Security Problems in Wireless Personal Area Networks

During the last couple of years, there is a strong tendency towards mobility for IT and computer networks. Wireless networks are rapidly gaining in importance; after all, wiring collides with the increasing demand for mobility. This paper focusses on *Wireless Personal Area Networks (WPANs)*. A WPAN is a small, heterogeneous, wireless ad-hoc network used for communication among several personal mobile devices, which often belong to the same user. The range of a WPAN is typically limited to a few meters.

It is clear that providing security for Wireless Personal Area Networks is essential as wireless links are easy to eavesdrop undetected. The fact that these

networks usually run on battery operated devices with limited processing power means that the security solutions should be as efficient as possible and avoid intensive use of expensive cryptographic operations such as public key encryption or digital signatures [1]. Moreover, these networks normally operate autonomously without access to online key servers or certification authorities. This means that conventional means of key establishment are not always applicable to these networks. To make things even more difficult, WPANs are often quite dynamic. This means that mobile devices do not have a clear idea of the continuously changing network topology.

These specific properties present interesting challenges when designing security and privacy solutions in these environments. In the rest of this paper, we will focus on how to establish a session key between two personal mobile devices that do not yet know each other, and hence do not share any authenticated cryptographic material (e.g., pre-established or pre-certified keys).

1.2. Organization of the Paper

This paper is organized as follows. In the introduction, we briefly discussed some of the major challenges when designing a security architecture for Wireless Personal Area Networks. In the rest of this paper, we focus on how to establish a session key between two personal mobile devices. This problem can be solved by assuming the existence of a secure authentic side-channel. A short overview of different techniques to construct such a channel, and a discussion on how it can be used to establish secret keys, is given in Sect. 2. The key establishment protocol proposed in this paper, employs the fact that both devices are in each other proximity. To cryptographically enforce this property, distance bounding protocols should be

used. This is explained more in detail in Sect. 3. Our key establishment protocol is presented in Sect. 4. Section 5 concludes the paper.

2. Related Work

In this paper, we want to investigate how two personal mobile devices, which are in the proximity of each other, can establish a secret session key. This problem can be generalized to the following research challenge: How to establish a shared secret (key) between two nodes in a wireless ad-hoc network that do not yet know each other and hence do not share any secret data? This problem is known in literature as *the pairing problem* [2]–[6]. Most solutions assume that the two mobile nodes share an extra, low bandwidth authentic channel. This *secure side-channel* is often called *the out-of-band channel*. The resulting system model is shown in Fig. 1. An attacker is not able to insert/delete/modify messages on this secure authentic side-channel. Note however that all data that appears on this channel, can be eavesdropped by everybody.

How to establish a session key using such a secure out-of-band channel? Basically, the two mobile devices (denoted by *Alice* and *Bob* in the rest of this paper) carry out the *Diffie-Hellman protocol*¹ [7]. Due to memory and resource constraints, it is recommended to carry out this protocol in the group of points defined by an elliptic curve $\mathcal{E}$ over a finite field [8], [9]. The protocol starts by *Alice* and *Bob* exchanging their (temporary) public keys. To avoid man-in-the-middle attacks, these keys have to be authenticated. To accomplish this, the mobile devices exchange some bits via the out-of-band channel. Next, *Alice* and *Bob* can compute a shared Diffie-Hellman key, which depends on their own private key, and the public key of the other party. The secure side-channel, which is used to authenticate the public keys of *Alice* and *Bob*, typically has a very low bandwidth, so as few bits as possible have to be exchanged through this channel.

Constructing a secure authentic out-of-band channel is quite a challenge. Different techniques have been suggested in literature, some of them more difficult to realize in practice than others. A first category of solutions employs the user itself as the secure out-of-band channel. These methods require some *user interaction* to authenticate the public keys sent over the insecure wireless ad-hoc network. Gehrmann et al. present several MANA protocols [3], [10]. These techniques enable mobile devices to authenticate their public keys

1. Other key agreement protocols based on asymmetric cryptographic algorithms could be used as well.

Figure 1. Mobile devices share a secure out-of-band channel

by manually transferring data between the devices. Hoepman proposes several ephemeral key exchange protocols, both for traditional wireless ad-hoc networks [4], as for anonymous wireless ad-hoc networks [5]. Singelée and Preneel improve this idea, and present an improved pairing protocol [11], in which the user has to enter a check-value to authenticate the data sent over the wireless network. In [12], the user has to compare the visual representation of a truncated hash value, computed on the public keys exchanged over the wireless ad-hoc network, and displayed on the screen of both mobile devices.

Not all solutions require the user to manually enter or compare data. Stajano and Anderson propose the resurrecting duckling security policy [6], [13]. The basic idea of this method is to make *physical contact* between the two mobile devices (e.g., via a connector), and then exchange some bits via this secure channel. In [14], a system that utilizes 2-dimensional barcodes and camera-telephones to implement a *visual channel* for authentication and demonstrative identification of devices is presented. Strong mutual authentication in this system requires running two separate unilateral authentication steps. Saxena et al. improve this technique, and show how strong mutual authentication can be achieved with a unidirectional visual channel [15]. Kindberg and Zhang suggest to use *ultrasound* to validate and secure spontaneous associations between wireless devices [16]. Goodrich et al. introduce the Loud-and-Clear system, which uses the *audio channel* for human-assisted authentication of mobile devices that do not yet know each other [17].

In [18], Čapkun and Čagalj introduce the concept of *integrity regions*, a security primitive that enables integrity protection of messages exchanged between mobile devices that do not hold any mutual authentication material. Their solution makes use of lightweight ranging techniques and visual verification within a small physical space, and offers unilateral authentication. In Sect. 4 of this paper, we present an improved version of this protocol, which is also based on the visual verification of entity proximity, but achieves mutual entity authentication.

3. Distance Bounding Protocols

Our key establishment protocol makes use of proximity information to mutually authenticate mobile devices in the wireless ad-hoc network. To cryptographically enforce the concept of “proximity”, distance bounding protocols can be used. These protocols combine physical and cryptographic properties and enable a verifying party to determine an upper-bound on the distance between itself and a prover, who claims to be within a certain range. Distance bounding techniques can measure the received signal strength (RSS) [19], measure the angle of arrival (AoA), or measure the time-of-flight (ToF) to estimate an upper-bound on the distance. The first two techniques (RSS and AoA) are typically discarded because of security reasons: e.g., an attacker can construct a directional antenna to largely increase the sending or receiving range [20]. This only leaves measuring the time-of-flight as a possible technique for secure distance bounding protocols.

Secure distance bounding protocols measure the time-of-flight to determine an upper-bound on the distance between prover and verifier. This is typically done during a challenge–response protocol, the main building block of the distance bounding protocol. During n fast bit exchanges, the time between sending a challenge and receiving the corresponding response is measured. Multiplying the time-of-flight with the propagation speed of the communication medium gives the distance between prover and verifier. One should however take into account some important details. It should be impossible for the prover to send the response before receiving the challenge [21]. This implies that the response should depend on the (random) challenge. One should also notice that the round trip time is not equal to the propagation time. It takes some time to compute and transmit the response. This processing delay should be as small as possible compared to the propagation time, because we are only interested in the latter.

Two communication technologies are commonly used: (ultra-)sound and electromagnetic signals. (*Ultra-sound*) is interesting to measure distances because it is relatively slow. The processing delay can be neglected compared to the propagation time and the accuracy of the measurements is not very critical. It can hence be used to measure small distances (in the order of centimeters). There are however some security problems. (Ultra-)sound is not resistant to physically present attackers. Such an attacker can modify the medium or use wormholes to claim that he is closer than he really is. By delaying the response, he can also claim to be further away. When the distance bounding

protocol makes use of *electromagnetic signals*, an active attacker can not use wormholes. The signals travel with the speed of light and nothing propagates faster. This means that an attacker can only claim to be further away than he really is (by delaying the response). There are however some practical issues. The verifier has to be able to measure the round trip time with very high precision. A small deviation of the measured time-of-flight influences the estimated distance a lot.

By employing the principle of distance bounding in a clever way, one can preclude one or more fundamental attacks: *distance fraud attacks*, *mafia fraud attacks* and *terrorist fraud attacks* (more details can be found in [22], [23]). Secure distance bounding protocols should at least be resistant to distance and mafia fraud attacks, but some of them prevent all three kind of attacks. This is however not sufficient. Hancke et al. show that one has to optimize the choice of communication medium and transmission format according to several design principles [24], if one wants to prevent certain “physical” attacks. One of those principles is to employ a communication format in which the recipient can instantly react on each single transmitted bit. This excludes the application of several (secure) distance bounding protocols.

4. Our Key Establishment Protocol

4.1. Problem Statement

We consider the following problem. Two personal mobile devices (denoted by *Alice* and *Bob*), which do not yet share any authenticated cryptographic material, want to establish a session key to communicate securely over an insecure wireless ad-hoc network. We assume that no secure visual, infrared or acoustic side-channels are available, and that it is impossible (or not practical) to connect both devices via a wire. In addition, we want to limit the required user interaction as much as possible.

To solve this problem, we can apply the Diffie-Hellman key agreement protocol and authenticate the exchanged public keys using a secure side-channel, as discussed in Sect. 2. We assume that *Alice* and *Bob* know the public protocol parameters. To create an out-of-band channel between both devices, we use the concept of a *user’s (device’s) private space*, which was introduced by Čapkun and Čagalj [18]. The user’s (device’s) private space can be (informally) defined as follows: *it is the largest spherical space, centered around the user’s (device’s) location, within which the user can visually verify the presence of other*

Figure 2. The concept of a user's (device's) private space

trusted devices AND the absence of untrusted nodes and adversaries. This is graphically depicted in Fig. 2. In this figure, A and B are in each other's private space, but all other nodes are not. The size of the user's private space is variable (e.g., it will be much smaller in a crowded room than in open air). By combining the notion of a user's private space and the concept of secure distance bounding protocols, one can achieve mutual device authentication, as shown in Sect. 4.2.

In this paper, we expect that the users operating the mobile devices are able to visually verify the presence of each other's devices within a very small range. Depending on the situation and the environmental constraints (presence of walls, other people, ...), this radius can vary between a few centimeters up to a couple of meters. By introducing the concept of a user's private space, we assume that the attacker is not in the proximity of *Alice* and *Bob* (i.e. outside the user's private space), as illustrated in Fig. 2. However, this does not imply that all communication between *Alice* and *Bob* is confidential. We assume that the attacker is able to modify its antenna, and hence can transmit and receive signals from a very large distance (much larger than the communication range of other devices in the wireless ad-hoc network). In addition, an attacker could have control over several devices in the network, but all of these malicious nodes are also located outside the private space of *Alice* and *Bob*. Finally, the attacker is computationally bounded, and is not able to break the Diffie-Hellman protocol in polynomial computation time.

4.2. User Friendly Key Establishment Based on Proximity Information

Our key establishment protocol, which is shown in Fig. 3, is carried out as follows:

First, *Alice* and *Bob* start the key establishment protocol by generating a random nonce (N_A and N_B respectively) and a (temporary) public key (g^{x_A} and g^{x_B} respectively), which is going to be used in the

Diffie-Hellman protocol. To simplify our discussion, we will employ the Diffie-Hellman key agreement protocol over a finite cyclic group $\mathbb{G}$ with generator g . $\mathbb{G}$ is a subgroup of $\mathbb{Z}_p^*$, the multiplicative group of non-zero integers modulo a large prime p . Note that any group in which the Diffie-Hellman problem is hard can be used, and for efficiency reasons, we especially recommend the group of points defined by an elliptic curve $\mathcal{E}$ over a finite field.

Next, *Alice* and *Bob* construct a string m_A (or m_B) which consists of the constant 0 (or 1), the (temporary) public key g^{x_A} (or g^{x_B}) and the random nonce N_A (or N_B). A commitment to this bitstring is sent over the wireless ad-hoc network to the other party. Any secure commitment scheme which is *unconditionally hiding* and *conditionally binding* (or *conditionally hiding* and *unconditionally binding*) can be used.

Now both parties start to conduct a secure distance bounding protocol. Since we assume that no active attackers are present in the private space of *Alice* and *Bob*, ultra-sound can be used as a communication medium. This relaxes the constraints on the processing delay, which becomes negligible to the propagation time. The accuracy of the measurements is also not very critical. As a consequence, *Alice* and *Bob* can be located very close to each other (even in the order of centimeters). Another advantage of assuming that no attackers or malicious nodes are present in the users' device's private space, is the fact that terrorist attacks can not occur. It is sufficient to select a secure distance bounding protocol which precludes mafia fraud attacks. In our key establishment protocol, we chose to employ the MAD protocol of Čapkun et al. [25], which offers mutual device authentication. If errors due to noise are likely to occur, one should preferably use a noise resilient secure distance bounding protocol [26]. The MAD distance bounding protocol consists of a series of fast bit exchanges. During this phase, the following two steps are repeated n times:

- *Alice* sends the bit s_i to *Bob* where $s_0 = N_{A,0}$ and $s_i = N_{A,i} \oplus r_{i-1}$.
- *Bob* sends the bit r_i to *Alice* where $r_i = N_{B,i} \oplus s_i$.

During the n fast bit exchanges, the time between sending s_i and receiving r_i (or sending r_i and receiving s_{i+1}) is measured. These measurements determine an upper-bound on the distance between *Alice* and *Bob*. This value should be smaller than the radius of the private space of *Alice* (or *Bob*), otherwise the protocol fails.

Next, both devices compute the random nonces (N_B and N_A respectively) and open the commitments sent in the beginning of the protocol. *Alice* and *Bob* check each other's commitment and if this verification is

Figure 3. Our efficient key establishment protocol

successful, both devices accept the messages m_B and m_A (and hence the corresponding temporary public keys) as being authentic. Finally, *Alice* and *Bob* can compute the shared Diffie-Hellman key ($g^{x_A \cdot x_B}$).

An attacker can try to impersonate *Alice* (or *Bob*). In order to be successful, the attacker has to guess all n responses right, and send them in advance to the other party. This way, the attacker can pretend to be closer than he really is (and appear to be in the user's device's private space). The probability of sending n correct responses is $(\frac{1}{2})^n$. This *false-acceptance ratio* determines the security parameter n (e.g., 40 rounds of fast bit exchanges results in a false-acceptance ratio of $9.1 \cdot 10^{-13}$). Security-critical applications require a higher number of rounds n than other, less critical, applications.

5. Conclusion

A Wireless Personal Area Network (WPAN) is a small, wireless, dynamic, heterogeneous ad-hoc network consisting of several personal mobile devices. Key establishment is one of the major challenges in WPANs, as traditional security mechanisms often do not cope with the dynamic characteristics of wireless ad-hoc networks. The Diffie-Hellman key agreement protocol seems very suitable to establish a session key between personal mobile devices which do not yet share any authenticated cryptographic material (e.g., pre-established or pre-certified keys).

In this paper, we presented an efficient key establishment protocol, based on the Diffie-Hellman protocol. Our proposed scheme enables mutual device authentication through presence. This way, one can prevent man-in-the-middle attacks. We require the user of a mobile device to visually verify within a small physical space the presence of the other trusted device, with whom a secure communication channel has to be established, and the absence of other (untrusted) nodes or adversaries. Distance bounding protocols are employed to determine an upper-bound on the distance to another entity.

Acknowledgment

Dave Singelée is funded by a research grant of the Katholieke Universiteit Leuven. This work was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government and by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy).

References

- [1] A. Hodjat and I. Verbauwhede, "The Energy Cost of Secrets in Ad-Hoc Networks," in *Proceedings of the IEEE Workshop on Wireless Communications and Networking (CAS '02)*, 2002.

- [2] D. Balfanz, D. Smetters, P. Stewart, and H. Wong, "Talking to Strangers: Authentication in Adhoc Wireless Networks," in *Proceedings of the Network and Distributed System Security Symposium (NDSS '02)*. The Internet Society, 2002.
- [3] C. Gehrmann, C. Mitchell, and K. Nyberg, "Manual Authentication for Wireless Devices," *RSA Cryptobytes*, vol. 7, no. 1, pp. 29–37, 2004.
- [4] J. H. Hoepman, "The Ephemeral Pairing Problem," in *Financial Cryptography*, ser. Lecture Notes in Computer Science, LNCS 3110. Springer-Verlag, 2004, pp. 212–226.
- [5] —, "Ephemeral Pairing on Anonymous Networks," in *Proceedings of the 2nd International Conference on Security in Pervasive Computing (SPC '05)*, ser. Lecture Notes in Computer Science, LNCS 3450. Springer-Verlag, 2005, pp. 101–116.
- [6] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks," in *Proceedings of the 7th International Workshop on Security Protocols*, ser. Lecture Notes in Computer Science, LNCS 1796. Springer-Verlag, 1999, pp. 172–182.
- [7] W. Diffie and M. Hellman, "New Directions in Cryptography," in *IEEE Transactions on Information Theory*, 1976, pp. 644–654.
- [8] A. J. Menezes, *Elliptic Curve Public Key Cryptosystems*. Springer, July 1993.
- [9] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, October 1996.
- [10] C. Gehrmann and K. Nyberg, "Security in Personal Area Networks," in *Security for Mobility*. IEEE, 2004, pp. 191–230.
- [11] D. Singelée and B. Preneel, "Improved Pairing Protocol for Bluetooth," in *Proceedings of the 5th International Conference on Ad-Hoc, Mobile, and Wireless Networks (ADHOC-NOW '06)*, ser. Lecture Notes in Computer Science, LNCS 4104. Springer-Verlag, 2006, pp. 252–265.
- [12] M. Čagalj, S. Čapkun, and J.-P. Hubaux, "Key Agreement in Peer-to-Peer Wireless Networks," in *Proceedings of the IEEE (Special Issue on Security and Cryptography)*, vol. 94, no. 2, 2006, pp. 467–478.
- [13] F. Stajano, "The Resurrecting Duckling – what next?" in *Proceedings of the 8th International Workshop on Security Protocols*, ser. Lecture Notes in Computer Science, LNCS 2133. Springer-Verlag, 2001, pp. 204–214.
- [14] J. McCune, A. Perrig, and M. Reiter, "Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '05)*, 2005, pp. 110–124.
- [15] N. Saxena, J.-E. Ekberg, K. Kostiaainen, and N. Asokan, "Secure Device Pairing based on a Visual Channel (Short Paper)," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '06)*, 2006, pp. 306–313.
- [16] T. Kindberg and K. Zhang, "Validating and Securing Spontaneous Associations between Wireless Devices," in *Proceedings of the 6th Information Security Conference (ISC '03)*, ser. Lecture Notes in Computer Science, LNCS 2851. Springer-Verlag, 2003, pp. 44–53.
- [17] M. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun, "Loud And Clear: Human-Verifiable Authentication Based on Audio," in *Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS '06)*, 2006, p. 10.
- [18] S. Čapkun and M. Čagalj, "Integrity Regions: Authentication Through Presence in Wireless Networks," in *Proceedings of the 5th ACM workshop on Wireless security (WISE '06)*. ACM Press, 2006, pp. 1–10.
- [19] P. Bahl and V. Padmanabhan, "RADAR: An In-Building RF-based User Location and Tracking System," in *Proceedings of IEEE INFOCOM '00*, vol. 2, 2000, pp. 775–784.
- [20] H. Cheung, "The Bluesniper Rifle," 2004, <http://www.tomsnetworking.com/Sections-article106.php>.
- [21] S. Brands and D. Chaum, "Distance-Bounding Protocols," in *Advances in Cryptology - EUROCRYPT '93*, ser. Lecture Notes in Computer Science, LNCS 765. Springer-Verlag, 1994, pp. 344–359.
- [22] Y. Desmedt, "Major Security Problems with the "Unforgeable" (Feige)–Fiat–Shamir Proofs of Identity and How to Overcome Them," in *Proceedings of SecuriCom '88*, 1988, pp. 15–17.
- [23] D. Singelée and B. Preneel, "Location Verification using Secure Distance Bounding Protocols," in *Proceedings of the 2nd IEEE International Conference on Mobile, Ad Hoc and Sensor Systems (MASS '05)*, 2005, pp. 834–840.
- [24] J. Clulow, G. Hancke, M. Kuhn, and T. Moore, "So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks," in *Proceedings of the 3rd European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS '06)*, ser. Lecture Notes in Computer Science, LNCS 4357. Springer-Verlag, 2006, pp. 83–97.
- [25] S. Čapkun, L. Buttyán, and J. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)*, 2003, pp. 21–32.
- [26] D. Singelée and B. Preneel, "Distance Bounding in Noisy Environments," in *To Appear in the Proceedings of the 4th European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS '07)*, ser. Lecture Notes in Computer Science, LNCS 4572. Springer-Verlag, 2007.