SECURING PERSONAL AREA NETWORKS

Theodoulos Garefalakis, Chris J. Mitchell

Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom
{theo.garefalakis, c.mitchell}@rhul.ac.uk

Abstract - We consider the applicability of ID-based cryptography to providing security within a Personal Area Network (PAN). An initialisation process appropriate for use within a PAN is proposed, and a detailed comparison between the ID-based approach and a more conventional PKI approach is given.

Keywords - ID-based cryptography, PAN, security

I. INTRODUCTION

One emerging application of wireless technologies is the so-called Personal Area Network (PAN). It consists of a small number of devices, often with limited capabilities, that are physically close and communicate over wireless interfaces (e.g., Bluetooth). These devices usually belong to the same owner. A challenging problem in this setting is that of securing the communications between the devices in the PAN. It is assumed that the devices do not share any keys.

In this work, we propose one possible solution to the problem of securing the intra-PAN communications. More specifically, we propose a method for providing authenticated, integrity protected and private channels between any two devices in the PAN. The solution uses identity-based cryptographic techniques. Our solution is perhaps one of the first realistic application of identity-based techniques, with certain advantages over traditional PKI methods.

The rest of the paper is structured as follows. In Section II we describe the requirements posed by a PAN. In Section III we describe the main functionality of identity based cryptographic schemes. In Section IV we describe a method for establishing an authenticated and private channel that is used for distributing private keys. Finally in Section V we compare the solution based on identity based techniques to a traditional PKI solution.

II. REQUIREMENTS

The underlying requirement is for two devices, which do not share any pre-existing keys, to be able to set up a secure channel. In this section we identify the requirements that arise if an ID-based solution is adopted to this problem.

As described below, an ID-based scheme allows public keys for public key cryptosystems to be reliably distributed without any need for public key certificates. If such a system is employed within a PAN, the immediate availability of public keys for asymmetric encryption and/or signature schemes allows a secure channel to be established between any two PAN devices with the minimum of overhead.

The problem remains of initialising the scheme. As described in more detail below, one of the devices within the PAN is defined as the *Private Key Generator*, and is responsible for issuing public domain parameters and a device private key to every device within the network. This transfer must provide data integrity and origin authentication — in addition, confidentiality is required for the private key transfer. A method by which this can be achieved is described in Section IV.

III. IDENTITY BASED SCHEMES

The use of ID-based cryptography presents an interesting alternative to the use of a conventional PKI solution within a PAN environment. Whilst ID-based cryptography will not avert the need for a secure initialisation process, involving a trusted exchange between a mobile device and a Trusted Third Party, it will remove the need for any subsequent exchanges of public key certificates between mobile devices. Moreover, whilst the trust model for an ID-based system may not always be appropriate, in a PAN environment the requirement for all devices to strongly trust one entity does not seem likely to present a major problem.

The origin of ID-based cryptography goes back to 1984, when Shamir described the potential utility of an encryption scheme in which the public key can be an arbitrary string. The original motivation was to simplify certificate management in e-mail systems. In such a scheme, the public key is derived (using a publicly known function) from the identity of owner, e.g., from the owner's e-mail address. According to the definition in the Handbook of Applied Cryptography [6], an ID-based cryptographic system is an asymmetric system wherein an entity's public identification information plays the role of its public key, and is used as input by a trusted authority (along with the authority's private key) to compute the entity's private key.

A. Identity-Based Encryption

In an ID-based encryption scheme, the encryption and decryption functions have the same functionality as in a traditional scheme. The only difference is in the key management. The scheme is best illustrated by an example. Suppose that device A wants to send a message to device B. It first encrypts

it using, as device B's public key, a string that is derived from device B's identity (e.g., its name or serial number). There is no need for device A to obtain device B's public key certificate, thus simplifying the certificate management.

The role of the CA, however, is not eliminated. The first time that device B receives an encrypted message (or before), it has to contact a trusted third party, the Private Key Generator (PKG), authenticate itself and obtain its private key. The private key it obtains is valid as long as its public key is valid. Methods for key revocation are discussed later. ID-based authentication and signature schemes are analogously defined.

Until recently there was a lack of practical and secure ID-based encryption schemes. However, in the last couple of years, two promising ID-based encryption schemes have been proposed, by Boneh and Franklin [1] and Cocks [2].

B. Identity-Based Signatures

ID-based signature schemes are the ID-based analogues of traditional signature schemes. As expected, if device B wants to generate a signature, it first contacts the PKG, authenticates itself and obtains the private key. This is then used as in a traditional scheme to generate a signature. When device A receives a signed message from device B, it can verify the signature in a traditional way using device B's identity information as its public key, thus avoiding the use of any certificates. Satisfactory ID-based signature schemes have been known since 1986. See for instance [3], [4].

C. Key Revocation

Key revocation in ID-based systems can be done in a very efficient way by limiting the lifetime of public keys. This can be achieved by defining the public key to consist not only of the identity of the owner, but the identity with a date appended to it. Continuing the previous example, if the public key of device B is to be renewed once a year, then its public key for the year 2002 would be "deviceB2002", and it would have to obtain a fresh private key once a year. Also, one can add more granularity to the revocation system by simply adopting a different convention for the public key (e.g., instead of the year append the month). However, unless the lifetime of public keys is made very short (with a consequent overhead relating to the need for new private keys to be distributed very regularly) one cannot completely avoid Certificate Revocation Lists (CRLs). If a public key is revoked due to compromise of the corresponding private key, then the public key, i.e., the public identity, has to be added to a CRL.

IV. Key Distribution

The problem of private key distribution and update is a non-trivial one, as the private keys have to be communicated from the PKG to the appropriate mobile device via a private and authenticated channel. In this section, following the proposals of Gehrmann and Nyberg, [5], we describe how such a channel can be established using weak password based techniques.

The protocol that we describe here is an authenticated Diffie-Hellman protocol. We describe the protocol in terms of a general group G, and an element $g \in G$. For specific implementations this can be taken to be, for instance, the multiplicative group of integers modulo a prime or the group of points on an elliptic curve over a finite field. (The usual care is required in selecting G and g — see, for example, [6]).

1) The PKG generates a random integer x and sends g^x to the device.
2) The device generates a random integer y and sends g^y to the PKG.
3) The PKG generates a random key K suitable for use with a MAC function shared by all devices in the PAN.
4) The PKG computes $\text{MAC}_K(g^x, g^y)$. The MAC and the key are then output by the device acting as a PKG to the user (e.g., via a display).
5) The user types the MAC and the key K into the mobile device, and the mobile device then recomputes the MAC value and compares it with the input value.
6) If the two values match, then both devices can generate g^{xy}; otherwise, they abort.

We note that even if the keying material for the MAC, and the MAC itself, are very short (and indeed they have to be short for reasons of usability), the security of the system is not compromised. The reason is that these values are used only to authenticate the exchange of the "Diffie-Hellman" values. Moreover, the key K is generated *after* the values g^x and g^y have been exchanged, and is entered manually into the mobile device. Thus, an attacker cannot know which values to substitute for g^x and g^y in order for the two computed MACs to match.

After the authenticated Diffie-Hellman exchange, the mobile device and the PKG share a secret key, which can be used to establish the authenticated and private channel.

V. Comparison

In this section we compare the solution using ID-based techniques to a solution using traditional PKI. This comparison is inevitably provisional since investigations of appropriate protocols for pairing two devices (which could be used for a simultaneous exchange of public keys) are at an early stage. Hence this comparison is based on working assumptions about the properties of protocols to support and manage the personal PKI.

For the comparison we use the following measures: *Communications complexity* (i.e., the number and length of messages exchanged between a mobile device and the personal CA/PKG, and/or between a pair of mobile devices), *Computational complexity* (i.e., the amount of computation that the various parties need to perform), *Management complexity* (i.e., the management overhead for the particular operations), and the *Overall security level* (i.e., the strength and trust properties of the security mechanisms).

- *Communications complexity.* The personal PKI approach requires more bandwidth, as public key certificates have to be distributed to the members of the PAN. For interactive communications, this distribution may not require more messages (certificates may be attached to other messages) but they certainly make some messages lengthier. For connectionless communications, such as email, the advantage offered by ID-based schemes is even more significant, as the sender needs to obtain the certificate of the receiver in advance (which implies one request and one reply message). On the other hand, the distribution of private keys by the PKG in the ID-based approach requires an authenticated and private channel (as opposed to simply an authenticated channel in the traditional approach). This clearly complicates matters.
- *Computational complexity.* The main computations in both schemes come from key generation, and computations involving the key, e.g., signature generation, signature verification, and encryption. Key generation is of approximately the same complexity in both schemes. One possible advantage of the ID-based scheme is that all the keys are generated by the PKG, which may be considerably more powerful than the other devices in the PAN. Once the keys have been generated and distributed to the interested parties, the computations are again of approximately the same complexity. More precisely, ID-based signature generation and verification is done in exactly the same way as in traditional schemes, and are thus of the same computational complexity. Encryption on the other hand is slightly slower for ID-based schemes, as it involves operations on elliptic curves. We stress however, that public key encryption is very rarely performed, as one establishes shared secret keys, and uses them to encrypt messages. By far the most frequent public key operations are signature generation and verification, which as mentioned above, are of the same complexity as in traditional schemes.
- *Management complexity.* In both schemes there is a need for maintaining keys (preserving their integrity and/or privacy), and checking for the validity of public keys before using them. A solution such as certificate revocation lists is therefore unavoidable in both cases. In the ID-based approach (in principle) one can avoid public key certificates, thus reducing the complexity of managing the system. Even in ID-based systems, however, a device still has to know the current identity of the device it wants to communicate with. Depending on how this problem is solved, the above observation is of greater or lesser significance.
- *Overall security level.* The cryptographic primitives in both schemes provide the same security level. A disadvantage of the ID-based encryption schemes of Boneh-Franklin and Cocks (the only practical such schemes), is that they have only been known for a short time, and the underlying assumptions have not yet been sufficiently tested. Therefore, it is possible that the schemes are not as strong as they were initially thought to be. Interestingly, ID-based digital signature schemes have been known for almost as long as traditional schemes. Another issue with ID-based schemes is that of the trust placed in the PKG. The device acting as a PKG has access to all private keys, and therefore has to trusted by all devices in the PAN. However, given that the PAN will typically consist of devices owned by a single individual, the trust issue is probably not a significant one.

We summarise the comparison in the following table.

	ID-based	Traditional
Communications Complexity	+	–
Computational Complexity	same	same
Management Complexity	+	–
Overall security	same	same

REFERENCES

[1] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In *Proceedings of Crypto 2001*, *Lecture Notes in Computer Science*, volume 2139, pages 213–229. Springer-Verlag, 2001.

[2] C. Cocks. An identity based encryption scheme based in quadratic residues. In *Lecture Notes in Computer Science*, volume 2260, pages 360–363, 2001.

[3] A. Fiat and A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Lecture Notes in Computer Science*, volume 263, pages 186–194. Springer Verlag, 1986.

[4] U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. *J. of Cryptology*, 1:77–94, 1988.

[5] C. Gehrmann and K. Nyberg. Enhancements to Bluetooth baseband security. In *Proceedings of Nordsec 2001*, *Copenhagen*, pages 39–53, November 2001.

[6] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of applied cryptography*. The CRC Press series on discrete mathematics and its applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 1997.