Secure Pervasive Computing without a Trusted Third Party

Asad Amir Pirzada and Chris McDonald
School of Computer Science & Software Engineering, The University of Western Australia
{pirzada,chris}@csse.uwa.edu.au

Abstract

The miniaturization of computing devices and the need for ubiquitous communication has augmented the demand for pervasive computing. Security demands that all devices in a pervasive system must be able to authenticate each other and communicate in a secure manner. This is usually achieved through a Trusted Third Party like a Public Key Infrastructure (PKI) or a Key Distribution Centre (KDC). The establishment of such an entity in such a dynamic environment is neither feasible nor pragmatic. In this paper we present a novel mechanism for authentication and key exchange that can operate seamlessly in pervasive computing environments without the presence of a Trusted Third Party. The proposed scheme has minimal computational requirements, which makes it most suitable for devices with limited resources.

1. Security Scheme for Pervasive Systems

ID-based systems [1] were introduced in order to avoid the explicit authentication of public keys through digital certificates. These systems aim at using the identity of a user to represent the public key. The advantage of such systems is that the public key certificates are no longer required to be maintained at a central or distributed trusted third party [2] providing elevated security and efficiency. Such schemes can be configured to perform authentication as well as key exchange without a trusted third party.

We propose using the scheme by Sheih et al. [3] for pervasive computing environments because of its simplicity, lower computational overhead and minimal reliance on a central trust authority. The scheme, when configured for a pervasive system, works in three phases: Initialisation Phase, Authentication Phase and the Key Exchange Phase.

The initialisation phase is completed at the key distribution centre. Each device, before joining the network, presents its one or more identities to the centre. The centre after processing the information gives the device a private key and its own public key. All devices that have been issued keys by the centre will no longer require its services until the time their private key is either lost or compromised.

During the authentication phase, any device desiring communication with another device, computes two special integers using its private key and the key distribution centre's public key. These integers are sent to the destined device along with timestamps for protection against replay attacks. These integers enable the recipient to verify the authenticity of the originator. Similarly, for mutual authentication, the same protocol is executed in the other direction as well.

In the key exchange phase, each device uses one of the received integers to derive a common session key. This key is further used for securing the communication channel between the two devices. A distinguishable feature of this key exchange protocol is that it can also be used to establish group session keys among devices.

Devices desiring secure communication, execute the proposed authentication and key exchange protocol to acquire session keys. These keys are subsequently used in end-to-end encryption for packets. Malicious devices, which try to launch passive or active attacks against the network, are thwarted through an efficient key verification mechanism and a multi-layered enciphering scheme.

2. References

[1] M. Joye and S. Yen, "ID-based secret-key cryptography", ACM SIGOPS Operating Systems Review, 32(4), pp. 33-39, 1998.

[2] A. A. Pirzada and C. McDonald, "Kerberos Assisted Authentication in Mobile Ad-hoc Networks", in Proc. of 27th Australasian Computer Science Conference (ACSC'04), 26(1), pp. 41-46, 2004.

[3] S. Shieh, W. Yang and H. Sun, "An Authentication Protocol Without Trusted Third Party", IEEE Communications Letters, 1(3), pp. 87-89, 1997.