Is Entity Authentication Necessary?

Chris J. Mitchell and Paulo S. Pagliusi

Information Security Group, Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
{c.mitchell,p.s.pagliusi}@rhul.ac.uk

Abstract. Conventionally, mutual entity authentication is seen as the necessary precursor to the establishment of a secure connection. However, there exist examples of cases where authentication is not needed. The purpose of this paper is to consider this proposition, illustrated by case studies, and to use the findings of this investigation as input for the design of authentication protocols suitable for use in future Internet access environments supporting ubiquitous mobility.

1 Introduction

In the context of secure communications, mutual entity authentication is very commonly seen as the necessary precursor to the establishment of a secure connection. However, there do exist examples of cases where mutual authentication is not necessary, and, indeed, may impose unnecessary overheads on session establishment. The purpose of this paper is to consider this proposition, using case studies as the basis for this discussion. In these case studies we consider the protocols used in the GSM (Global System for Mobile Communications) and 3GPP (3rd Generation Partnership Project) mobile telecommunications systems.

The main application context of these discussions covers the case where there are three entities involved in the authentication exchange: a mobile user, a local AAA (Authentication, Authorisation and Accounting) server, and a remote (home) AAA server. That is, the mobile user wishes to set up some kind of secure link with a ‘local’ network (with its own AAA server), and the mobile user has a long term cryptographic relationship, typically backed up by some kind of contractual and payment arrangement, with a remote (home) network and AAA server. This ‘roaming user’ model is not only becoming an increasingly common model for Internet access, but it is also fundamental to understanding the air interface security system for present day mobile telecommunications networks (e.g. GSM and 3GPP).

The purpose of this paper is not so much to talk about GSM and 3GPP, but to consider what more general lessons can be drawn regarding future protocol design. In particular, how best should authentication and/or access security be

1 http://www.gsmworld.com
2 http://www.3gpp.org

© Springer-Verlag Berlin Heidelberg 2004
Is Entity Authentication Necessary? 21

designed in the scenario where a mobile user wishes to access the Internet via a multiplicity of different network types? The recently inaugurated IETF PANA (Protocol for carrying Authentication for Network Access) work will provide a general framework for the exchange of authentication messages in this mobile scenario, but will not address the question of exactly how access security should operate. Other relevant work includes the ongoing IST-Shaman project.

2 Entity Authentication and Key Establishment

Before proceeding we need to establish some terminology. We use definitions from the Handbook of Applied Cryptography (HAC), and, where relevant, we indicate the relevant section number from the HAC in brackets after the definition.

*Entity authentication* is the process whereby one party is assured of the identity of a second party involved in a protocol, and that the second has actually participated (10.1.1). Either one or both parties may corroborate their identities to each other, providing, respectively, *unilateral* or *mutual* authentication (10.1.2).

We are particularly concerned here with the case where a protocol simultaneously provides entity authentication (unilateral or mutual) and session key establishment, where this session key (or keys) is used to protect data subsequently transferred. *Key establishment* is a process or protocol whereby a shared secret becomes available to two or more parties, for subsequent cryptographic use (12.2.1). *Key authentication* (sometimes also called *implicit key authentication*) is the property whereby one party is assured that no other party aside from a specifically identified second party (and possibly additional identified trusted parties) may gain access to a particular secret key (12.2.1). *Key confirmation* is the property whereby one party is assured that a second party actually has possession of a particular secret key (12.2.1). *Explicit key authentication* is the property obtained when both (implicit) key authentication and key confirmation hold (12.2.1).

A further property, desirable in some practical applications but not discussed in HAC, is *key freshness*. By this we mean the property that the party to a key establishment process knows that the key is a ‘new’ key. In particular, the party should have evidence that the messages received during the protocol by which the key has been established are ‘fresh’ messages, i.e. they are not replays of ‘old’ messages from a previous instance of the protocol.

To see why this property is necessary in addition to implicit or explicit key authentication, consider the following very simple one-pass key establishment protocol. In this protocol we suppose that $A$ and $B$ share a long term secret key $K$. Entity $A$ chooses a session key $K_s$ and sends it to $B$ in the following message:

$$e_K(K_s || I_B)$$

---


4 [http://www.ist-shaman.org](http://www.ist-shaman.org)