

Comparison of protocols for secure mobile phone communications. Analysis of existing implementations.

Abstract

This document gives a brief introduction into algorithms and protocols for entity authentication (verifying the identity of communication partners) and analyzes the approaches for realizing authentication in current mobile communication standards. The main results of this comparative analysis concerning an authentication infrastructure for wireless Internet access are, that

- 1) The protocols as proposed in current IETF working groups still need further evaluation of their security characteristics, and, in particular,
- 2) Do exhibit serious deficiencies regarding the location privacy of mobile nodes. Furthermore, it is concluded that in order to assess the performance implications of (re-)authentication during frequent handovers further study is needed which will be addressed in a future report.

Introduction

Upcoming next generation wireless networks aim to support data and multimedia services to mobile nodes (MNs), in principle regardless of the origin of the MN. "In principle" means that a visited network, e.g. a radio access network (RAN), may require some kind of general or specific service agreement between its administrative domain and the MNs original administrative domain. This objective poses considerable requirements on the authentication service which assures that entities have in fact the identity they claim to have.

This report gives a brief introduction to authentication protocols and analyzes the approaches to authentication of current mobile communication standards including ongoing work of the Internet Engineering Taskforce (IETF)

Project specification:

We will be discussing the following key elements in secure mobile phone communications.

Authentication: The act of verifying a claimed identity, in the form of a pre-existing label from a mutually known name space, as the originator of a message (message authentication) or as the end-point of a channel (entity authentication).

1) Data Integrity.

2) Entity authentication.

Arbitrated Authentication: in which two (or more) entities, that want to verify the authenticity of one or more entities make use of a so-called trusted third party (TTP).

The Needham-Schroeder Protocol

The Needham-Schroeder protocol [32] allows two entities Alice () and Bob () to authenticate each other by the help of a trusted third party (.). The protocol uses a symmetric encryption algorithm as basic cryptographic primitive.

The Kerberos Authentication System.

The Kerberos authentication system has been designed in the late 1980's in the course of the project *Athena* at the Massachusetts Institute of Technology (MIT), Boston, USA. Kerberos provides an authentication and access control service for workstation clusters.

Cryptographic Algorithms

1) Encryption Algorithms.

- a) **Symmetric Encryption Algorithm.** Prominent algorithms in this category are the Data Encryption Standard (DES) and the International Data Encryption Algorithm (IDEA).
- b) **Asymmetric Encryption Algorithms.** Prominent examples for asymmetric encryption algorithms are the Rivest-Shamir-Adleman (RSA) algorithm and the ElGamal algorithm.

2) Integrity Check Values.

- a) **Modification Detection Codes (MDC).** Common algorithms in this class are the Message Digest 5 (MD5) and the Secure Hash Algorithm.
- b) **Message Authentication Codes (MAC).** A very common algorithm for computing a MAC is to use a symmetric block cipher like DES or IDEA in a

special mode called Cipher Block Chaining Mode and to use the output block of the encryption process as the MAC.

Current Approaches to Authentication in Mobile Communications

Authentication in GSM

- a)** Subscriber identity confidentiality.
- b)** Subscriber identity authentication.
- c)** Signaling information element confidentiality.
- d)** User data confidentiality.