

Introduction

This paper briefly describes the cryptographic mechanisms used to secure data exchanged between a Privaris plusID personal biometric device and an external host over a wireless Bluetooth connection.

Overview

Bluetooth has found much success in the consumer market for which it was designed, however, the consumer-oriented nature of the wireless technology has led to the perception that the security features it supports are not sufficient for environments where security is a primary concern. Indeed, a number of successful attacks have been made against the security model adopted in early versions of the Bluetooth specification. More recent versions have largely addressed these issues; however, the security model continues to place a significant burden on the end user to choose their configuration correctly in order to maintain a sufficient level of security. As an example, Bluetooth's encryption keys are typically generated from a PIN supplied by the user. By requiring the user to determine the PIN, the effective security is strongly dependant on the user's choice of PIN length. In environments where a high level of security must be maintained, such variations in strength are unacceptable. For this and other reasons, *the plusID personal biometric device avoids Bluetooth's standard security features in favor of more robust protocols.*

A number of strong cryptographic techniques are used to ensure the confidentiality of information exchanged using Bluetooth between a plusID device and external hosts. Each plusID contains a unique public/private key pair and associated certificate signed by Privaris' manufacturing private key. This key pair and certificate are placed securely on the plusID during the manufacturing process.

When a Bluetooth connection between the plusID and external host is initiated, the host extracts the plusID's certificate and confirms its authenticity by verifying the digital signature using the Privaris public key. The host then generates a random temporary public/private key pair that is used to calculate a common shared secret between the plusID and the host. This shared secret is used to derive a session key used to encrypt all further communication between the plusID and the host during the session, which ends when a party terminates the connection.

Once the authentication and key exchange takes place, the host may securely request the user's credential, which is released by the plusID only after the identity of the device holder is biometrically verified.

Technical implementation

At manufacturing, each plusID generates a 2048-bit Diffie-Hellman key pair with a 256-bit private exponent. The manufacturing software then extracts the public portion and generates

a certificate for it that is signed by Privaris' 2048-bit private RSA manufacturing key before uploading it to the plusID device.

After each Bluetooth connection to a host is established, the host downloads the plusID's certificate, verifies its authenticity and extracts its public key. The host then generates an ephemeral Diffie-Hellman key pair and uses Diffie-Hellman Key Agreement as outlined in NIST Special Publication 800-56A: "Recommended for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" to calculate the shared secret between the plusID key and the host's ephemeral key. A 128-bit AES session key is then derived from the shared secret using the Key Derivation Function (KDF), as described in NIST Special Publication 800-56A.

All further communications between the plusID and the host are encrypted using AES in CCM mode (Counter with Cipher Block Chaining-Message Authentication Code) as described in NIST Special Publication 800-38C. This mode provides both confidentiality of data through the use of the AES encryption algorithm in counter mode, as well as data integrity through the use of a Cipher Block Chaining (CBC) message authentication code.