Project 4: Network security

Department of Computer Science
University of Stellenbosch
7600 Stellenbosch
South Africa

1 The Simple Secure Registration Protocol

The Simple Registration Protocol (SRP) was presentedin Project 1 as a simple registration protocol which does not include any security features. This assignment will add minimal authentication capabilities to the SRP protocol using message digests (mandatory) or some other authentication method. In its simplest form, the Simple Secure Registration Protocol (SSRP) will protect the database locatedat the server side of the client/server model from being updated by non-trusted users. A password-based model usingthe following ideas will be used

- The security system will not send cleartext passwordsfrom the client to the server.
- The password-based scheme will include the following steps: 1. The client prompts the user for a password 2. The client relays the information to the server 3. The server checks the name and password 4. The server either allows the user into the systemor denies access.

Sending a message digest of a copy of the password is vulnerable to a ”replay attack” where a malicious user can listen to the digested password and replay it later to gain illicitaccess to the server.

It is proposed in [1] that session-specific information be added to the message digest such as a random number and a timestamp.

1.1 Specification of Messages

The secure version of the SRP protocol will include the basic SRP messages and authentication messages following the model described in [1] chapter 6.

1.2 Client and Server programs

The basic SRP client/server model will be extended to include authentication by defining a new type of service referred to as ”UPDATE”. This service updates a database on the server side under mandatory authentication by requiring that every access to the server be authenticated.

1.3 Implementation Constraints

- Programs will be developed in Java and may be derived from samples provided by [1].
- The code must be (1) clearly written (2) easily understandable (3) neatly formatted and (4) self documenting.

References

References

[1] J. Knudsen, ”Java Cryptography”, *O’Reilly & Associates, First Edition, ISBN 1-56592-402-9*, 1998.