PS4: Secure Messaging

Eric Chin John McGuiness

Architecture

1. Any number of clients
2. A server that will act as the key distribution center for clients

Note: Server will be used only for authentication, key distribution, and client listing. Clients will communicate direclty with other clients

Assumptions

- Client knows the public key of the server
- Client and server will share knowledge of password
- Users will only remember one password
- Symmetric keys are at least 128-bit keys
- Asymmetric keys are at least 1024-bit keys

Assumptions (cont.)

- Symmetric encryption operations use the AES encryption protocol
- Asymmetric encryption operation use the RSA encryption protocol
- Message authentication codes are generated using HMAC

Protocol: Overview

1. Client-server authentication and key exchange
2. Server-client key distribution
3. Client-client session establishment

Protocol: Terminology

K_{AS} = symmetric key between A and S

P_A = password shared between A and S

Pu_A = public key of A (randomly generated on client initialization)

Pr_A = private key of A (randomly generated on client login)

h_1, h_2 = cryptographic hashing functions

R_S is a random number

Protocol: C/S Auth./Key Exchange

$A \rightarrow S$: “A”, $Pu_s\{K_{AS}\}$, $K_{AS}\{Pu_A, h_i(P_A)\}$

$A \leftarrow S$: $Pu_A\{R_S\}$, $K_{AS}\{h_2(P_A)\}$

$A \rightarrow S$: $h_1(R_S)$

Protocol: S/C Client Key Distribution

$S \rightarrow A: K_{AS}\{Pu_B, \text{“B”}\}, K_{AS}[Pu_B, \text{“B”}]$

$S \rightarrow B: K_{BS}\{Pu_A, \text{“A”}\}, K_{BS}[Pu_A, \text{“A”}]$

Protocol: C/C Session Establishment

$$A \rightarrow B: \; Pu_B\{K_{AB}\}, \; K_{AB}\{R_A\}$$
$$A \leftarrow B: \; Pu_A\{R_B\}, \; K_{AB}\{h_1(R_A)\}$$
$$A \rightarrow B: \; h_2(R_A, \; R_B)$$

Protocol: C-S Requests

$A \rightarrow S: K_{AS}\{Request\}, K_{AS}[Request]$
$A \leftarrow S: K_{AS}\{Response\}, K_{AS}[Response]$

For this assignment, the client can make requests for the list of clients

Protocol: C-C Messages

$A \rightarrow B: K_{AB}\{message_A\}, K_{AB}[message_A]$

$A \leftarrow B: K_{AB}\{message_B\}, K_{AB}[message_B]$

Messages are communicated directly between clients