Security in Skype

Prepared by Prithula Dhungel

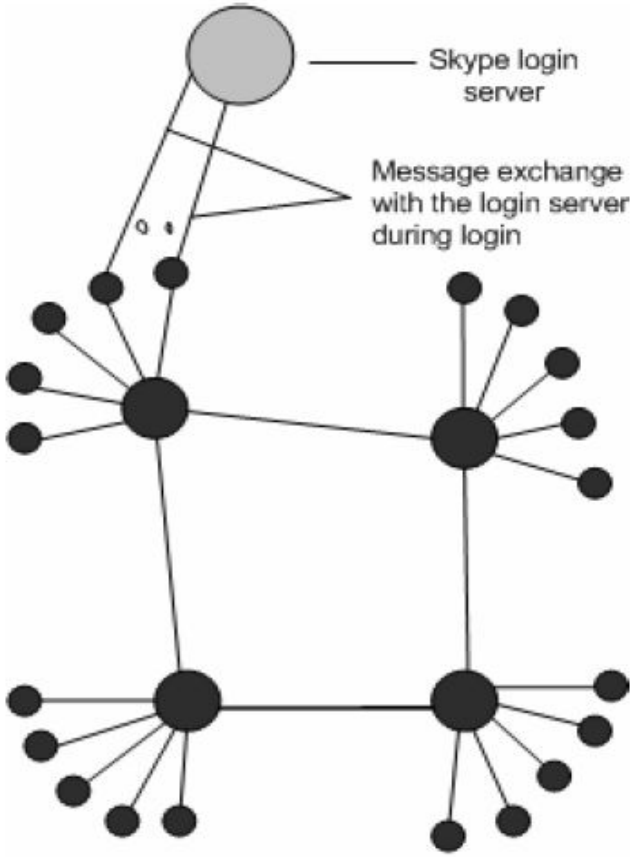
The Skype Service

- P2P based VoIP software
- Founded by the founders of Kazaa
- Can be downloaded free at:
  - http://www.skype.com
- Services
  - Both paid and free services available
  - Free
    - Instant Messaging
    - Voice and Video communication (PC to PC)

A typical Skype user interface

Skype Architecture

Hierarchical P2P architecture but involves a central Skype authority for registration and certification services



Skype Architecture: Normal peers, super nodes, and centralized Skype server

Reverse Engineering of Skype

- Proprietary and closed source software
- Employs countermeasures against reverse engineering
- However, has undergone some reverse engineering attempts over a couple of years
  - Basis of understanding (part of) Skype security protocol

Skype Security Services

- Almost everything is encrypted, including protocol message headers (except some)
- Provides:
  - Confidentiality
  - User authentication

Security Phases

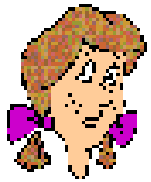
1) User registration
   - Register username at Skype server
1) User login
   - Get the one time public key for the user certified by Skype Server
1) User to User authentication
2) User to User communication

User Registration [1]

1. User selects a unique username (over the skype domain) and a password
2. Sends username and SHA -1 hash of password to the Skype Login Server, encrypted with the public key of the Skype Server
3. Skype server extracts username, hash of password using its private key

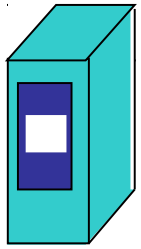
Public Key of Skype Server known to client during Skype installation

User Registration [2]



Alice

1. K_s^+ (Username, H(pwd))



Skype Server

2. K_s-(K_s^+ (Username, H(pwd)))

→ Username, H(pwd)

- Username : unique over Skype's domain
- K_s^+ : public key for Skype Server (hard coded in Skype application)
- H(): SHA -1
- H(pwd) stored securely in the client

Security Phases

1) User registration
   - Register username at Skype server
1) User login
   - Get the one time public key for the user certified by Skype Server
1) User to User authentication
2) User to User communication

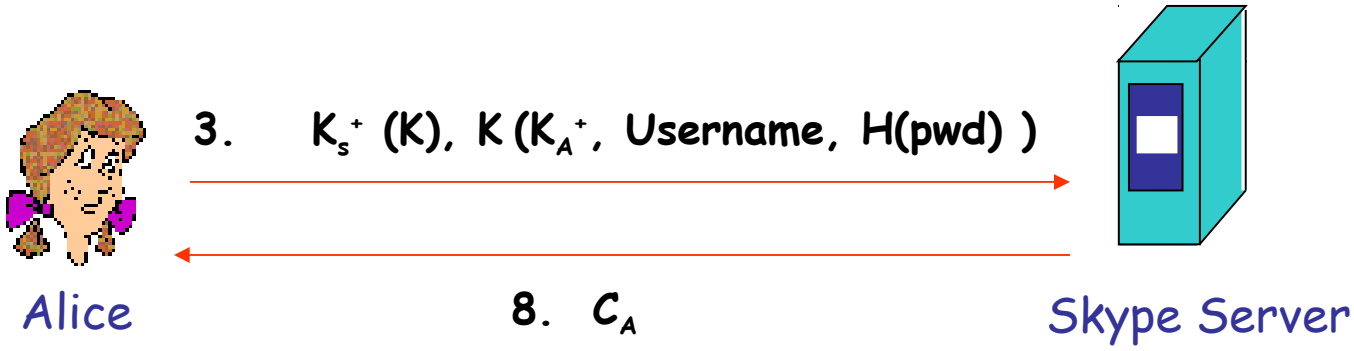
User Login [1]

1. User (client application) generates 1024-bits public and private key pair (K_A^+, K_A^-)→ One time key pair for the user for this login session
2. User generates 256-bits AES symmetric key (K)
3. Encrypts K_A^+, username and SHA-1 hash of password using K.
4. Encrypts K using public key of Skype Server

User Login [2]

5. Encrypted K_A^+, username and password hash and encrypted session key K are sent to the Skype Server
6. Login Server extracts K using its private key and decrypts username, password hash and K_A^+ using K.
7. If username and password hash match, user is authenticated. Skype Server signs username and K_A^+ pair to give certificate (C_A).
8. C_A sent to user

User Login [3]



1. Generate one-time key pair (K_A^+, K_A^-) and K
2. Store K_A^- securely

4. $K_s^-(K_s^+(K)) \rightarrow K$
5. $K(K(K_A^+, \text{Username}, H(\text{pwd}))) \rightarrow K_A^+$, Username, H(pwd)
6. Verify Username and H(pwd)
7. $K_s^-(\text{Username}, K_A^+) \rightarrow C_A$

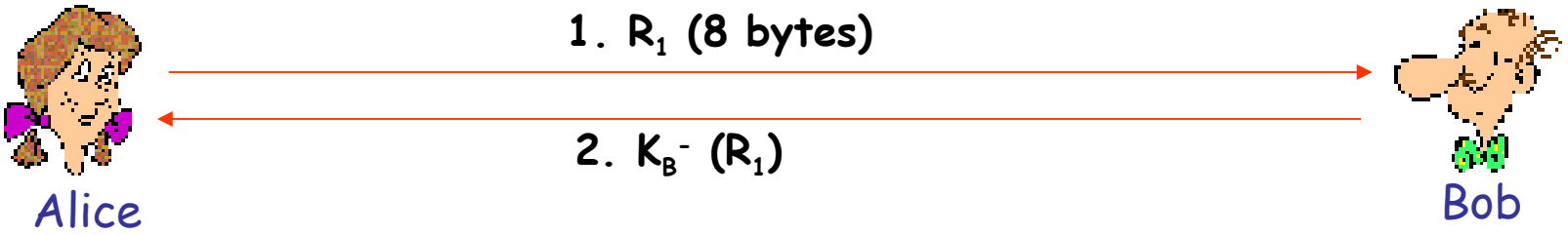
Security Phases

1) User registration
   - Register username at Skype server
1) User login
   - Get the one time public key for the user certified by Skype Server
1) User to User authentication
2) User to User communication

User-to-User Authentication [1]

1. Users Alice (A) and Bob (B) want to authenticate and communicate to each other
2. Users get each other's certificates
   - Alice sends Bob her certificate (that she obtained from Skype Server) and vice-versa
1. Each use 8 bytes challenge-response method to authenticate each other

User-to-User Authentication [2]



3. $K_B^+(K_B^-(R_1)) == R_1$

Security Phases

1) User registration
   - Register username at Skype server
1) User login
   - Get the one time public key for the user certified by Skype Server
1) User to User authentication
2) User to User communication

Encrypted P2P Communication [1]

1. After mutual authentication, Alice and Bob establish a 256-bits common session key K_s (AES) for encryption

2. Each side contributes 128-bits for the 256-bits long K_s

3. Each side sends its contribution to the other side, encrypted with the latter's public key

4. Two 128-bits contributions combined in some way to generate the 256-bits secret session key K_s

5. All traffic (voice, video and text) is encrypted

Encrypted P2P Communication [2]

Alice

$K_B^+(K_1)$

$K_A^+(K_2)$

Bob

- $K_A^-(K_A^+(K_2)) \rightarrow K_2$
- $K_1 + K_2 \rightarrow K_s$

- $K_B^-(K_B^+(K_1)) \rightarrow K_1$
- $K_1 + K_2 \rightarrow K_s$

Summary

- Some part of Skype security protocol has been deciphered
- Skype uses standard cryptographic techniques:
  - RSA
  - AES
  - SHA-1

References

1) An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol by S. A. Baset and H. Schulzrine
   - http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf
2) Silver Needle in Skype by P. Biondi and F. Desclaux
   - http://www.secdev.org/conf/skype_BHEU06.handout.pdf
3) Skype Security Evaluation by T. Berson
   - http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf