Skype Cryptosystem Overview

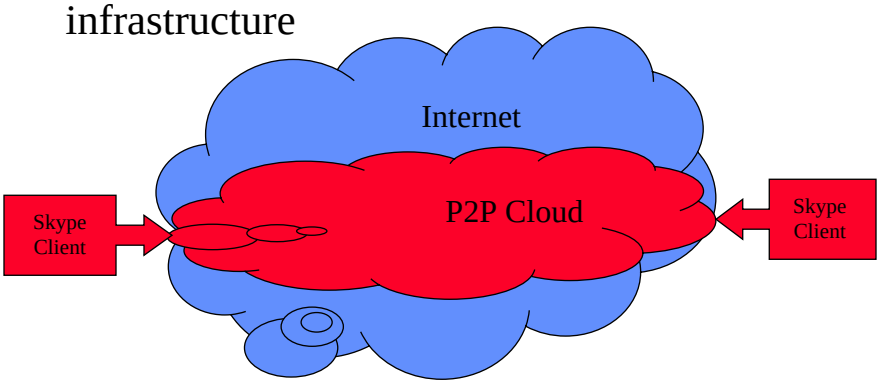
Tom Berson
Anagram Laboratories
December 2005

What is Skype?

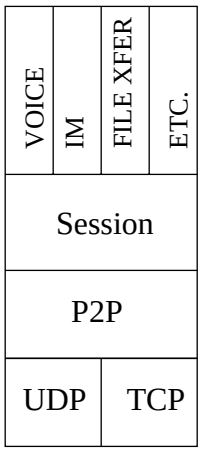
- Peer-to-peer (P2P) network
  - Voice, IM, File Transfer, Video, …
- PSTN Gateways (Voice)
  - SkypeOut, SkypeIn
- Network Services
  - Voicemail, Value-added
- Ecosystem
  - Partners for software, hardware, services, etc.

Why a cryptosystem?

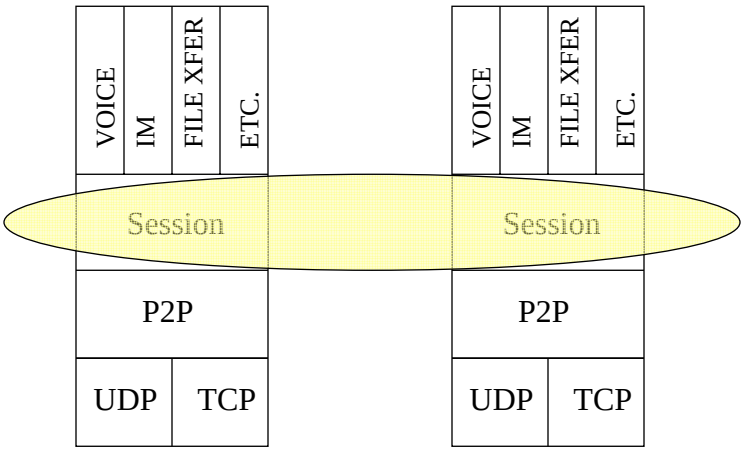
- To protect user data across P2P cloud
- Skype doesn't own any transport infrastructure



Skype Protocol Stack



Session Layer Encryption



Cryptosystem Phases

- 1. Enroll
- 2. Establish Session
- 3. Encrypt Traffic

Skype Certificate Authority

- Skype operates a Certificate Authority for users
- The central cryptographic secret is CA's private signing key, S_s
- Corresponding public verification key, V_s, is in every client image
  - RSA, 1536 or 2048 bits

1. Enroll

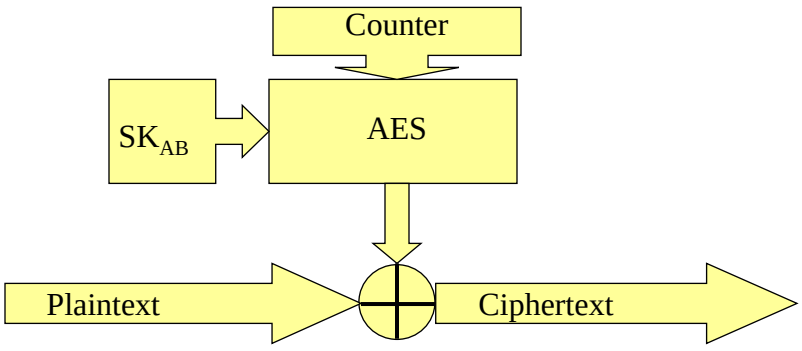
- User selects username (A) and password (P_A)
- Client generates a public-key pair (S_A, V_A)
  - RSA 1536 bit
- Client securely stores $H(P_A)$, S_A
- Client to Server: A, $H(P_A)$, V_A
  - AES 256 bit
- Server validates A, signs IC_A: $\{A, V_A\}^{S_s}$
  - ISO 9796-2
- Server to Client: IC_A

2. Establish Session

- A connects with B across P2P cloud
- A and B use a protocol to agree SK_{AB}
  - Bilateral random nonce challenge-response
  - Bilateral exchange of IC
  - Bilateral exchange of random (as RSA c'grams)
  - A and B derive same 256 bit SK_{AB}

3. Encrypt Traffic

- A and B possess SK_{AB}
- Use AES in Integer Counter Mode



The Bottom Line

- Skype uses a mixture of public-key and secret-key cryptography
- It uses standard algorithms and non-standard certificate formats
- Skype provides authenticity and confidentiality from Peer to Peer
- For more information, follow links from http://anagram.com