Skype Security Evaluation

Executive Summary

This evaluation report provides a detailed review of the security framework that is incorporated into Skype products. Skype provides its users with protections against a wide range of possible attacks, such as impersonation, eavesdropping and modification of data while in transit. This report describes the protective mechanisms that are in use throughout the Skype infrastructure as well as the general security policy that defines the basis for all designs within Skype's operational framework.

Employment of Cryptography in Skype

Skype uses only standards-based cryptographic functions and the report confirms that each of these functions conforms to its standard and interoperates with reference implementations. Through the use of its own certificate authority and certificate issuance system, Skype is able to provide high assurance that no user may impersonate another Skype user. To perform this verification, Skype uses widely disseminated public keys, the use of which allows Skype software to quickly authenticate the identity of another user without making reference to a central server. The report describes how passwords are stored and how identity certificates are generated for Skype users.

Skype makes user of a number of cryptographic primitives in order to achieve its security goals. There is no proprietary encryption in Skype. The cryptographic primitives used in Skype are: the AES block cipher, the RSA public-key cryptosystem, the ISO 9796-2 signature padding scheme, the SHA-1 hash function, and the RC4 stream cipher.

Beyond identification issues, Skype also ensures user privacy by encrypting peer-to-peer sessions through the use of the Advanced Encryption System (AES) block cipher, employed in 256-bit Integer Counter Mode. In order to set up the AES-encrypted session between a pair of peers, the communicating peers must agree upon a common session key. Skype divides the task of generating the session key between the two communicating clients, each generating 128 bits of the 256-bit key. This means that there is no single point of subversion that, if exploited, could force a weak encryption key to be used.

At its core, cryptography depends heavily upon the generation of high quality random numbers. Skype uses procedures for gathering and mixing entropy sources in a way sufficient to satisfy the cryptographic functions used in Skype. In addition, the methods employed by Skype conform to the practices recommended in RFC 1750 and are similar in style to the Microsoft CryptoAPI function, CryptGenRandom, which is described in *Writing Secure Code*, 2nd Edition, by Microsoft Press.

Defense Against Attack Scenarios

Skype takes care to protect against protocol-based attacks. The evaluation report considers a number of such attacks, including the following: Man-in-the-Middle attacks, replay attacks, password-guessing attacks, weaknesses in the use of checksums, side-channel attacks, and rollover attacks such as the one used in the well-known ASN.1 attack vulnerability.

The evaluation found Skype to be protected against all of these attack scenarios. However, the evaluation turned up two implementation weaknesses: The first was the unsuitability of using CRC-type checksums to validate data and the second was an unbounded network payload decoding routine. Neither of these bugs could cause compromise of a user's communication, but both could result in the denial of service to users. Since receiving the evaluation report, Skype has corrected both of these issues.

Absence of Malware

Skype does not include any adware, spyware, malware or "back door" functions. Among its conclusions, the evaluation report notes the absence of any such mechanism, or of any overarching debugging functions.