An Introduction to Escrowed Encryption Systems

Steven M. Bellovin

smb@research.att.com

908-582-5886

AT&T Bell Laboratories

Murray Hill, NJ 07974

A *Very* Brief Tutorial on Cryptography

- A cryptosystem is a function that maps input *plaintext* and a *key* to output *ciphertext*.
- The inverse function takes a key (which is sometimes different) and the ciphertext, and produces plaintext.
- In general, a separate *session key* is used for each conversation. (There are lots of ways to agree upon a session key.)
- The security of a cryptosystem must lie in the secrecy of the keys. Specifically, the system must be secure even if the enemy knows the function.
- Most common encryption algorithms are *block ciphers*, which operate on fixed-length input blocks. Various *modes of operation* can be employed to encrypt longer objects, such as files, network connections, phone calls, etc.

What is “Key Escrow”?

- “Key escrow” is a system wherein cryptographic keys are given to a third party.
- The concept is valuable in the commercial world, to ensure access to encrypted files in case an employee dies, leaves, or simply forgets a password.
- The government has proposed a encryption standard (popularly known as *Clipper*) wherein it will have copies of all keys.

Why Key Escrow?

These are NSA's stated goals.

- The current standard encryption algorithm (DES) is at the end of its useful life.
- Sensitive but unclassified government data needs protection.
- This should be made available to U.S. Citizens.
- U.S. business data abroad especially needs protection.
- ☞ The new technology should not preclude law enforcement access.

All but the last point are reasonably uncontroversial.

Key Escrow as a Deterrent

- A published algorithm such as DES can be used against NSA.
- Even a government-only deployment of a secure (but unclassified) cryptosystem would be subject to theft and abuse.
- "Illicit" use of such cryptographic technology is virtually certain if deployed commercially.
- NSA does not want strong cryptosystems to be deployed by its adversaries. They appear to view the deterrent effect of key escrow as more important than the ability to eavesdrop on criminals.

Who Will Use Key Escrow Devices?

- The government, for secure phones.
- The civilian market (the government hopes).
- The export market, especially foreign subsidiaries of U.S. firms.
- "Stupid" criminals.

How Key Escrow Works: Preliminaries

- When a session key is loaded, a key escrow device emits a *LEAF* (Law Enforcement Assistance Field). This must be transmitted to the far end.
- The decrypting device loads the received LEAF; if it appears invalid, the device will not decrypt the actual message.
- A wiretapper can receive the LEAF as well.
- The cryptographic keys necessary to utilize the LEAF are split up among several government agencies, so that more than one party must co-operate if the encrypted traffic is to be read.

How Key Escrow Works: Technical Details

- Key escrow chips use the *Skipjack* encryption algorithm.
- Each chip has a *unit key* (U) assigned at time of manufacture.
- The unit key is created by XORing two key halves U_1 and U_2.
- All chips share a *family key* (F).
- The LEAF consists of the session key encrypted by the unit key, and a 16-bit checksum, a 32-bit chip serial number, all encrypted by the family key:

$$\{\{K\}_{U_1 \oplus U_2}, \mathsf{cksum}, \mathsf{serial}\}_F$$

- The checksum is said to be some constant encrypted by the session key; how the IV fits in isn't clear.

How Key Escrow Works: Administrative

- There are two escrow agents (currently Treasury and NIST); each holds half of U.
- The two also supply seeds to a (classified) pseudo-random number generator that is used to produce U_1 and U_2. (Software is used because it is more auditable.)
- Escrowed conversations are recognized by the LEAF; requests for the escrowed keys are made on the basis of the serial number, not the caller's phone number.

How Key Escrow Works: Legal

- Key requests must be from authorized sources; they must certify that they have legal authority to read the conversation (i.e., domestic wiretap law, FISA, etc.).
- The requesters do *not* present warrants or other information beyond the chip serial number.
- Comprehensive audit trails will be kept of requests.
- Technical mechanisms (not yet finalized) will be used to ensure that wiretap requests expire.
- These procedures do *not* create an actionable legal right.

The Skipjack Encryption Algorithm

- Block cipher; 80-bit keys; 64-bit blocks.
- Algorithm will not be published, ostensibly to prevent implementation of such a strong cipher without escrow capabilities, and also to avoid teaching others new cryptographic principles.

☞ But some people suspect that the cipher is weak, or that there is a back door.

- Skipjack was reviewed by an outside panel; they found no weaknesses, but they (and NSA) admit that the review was necessarily cursory. On the other hand, they did examine NSA's own certification analyses.

Availability

- Key escrow encryption *must* be implemented by approved, secure hardware. No software versions.
- Two basic chips, one with just Skipjack (and the LEAF), and one that also implements key negotation, digital signatures, random number generation, etc.
- Key escrow chips are claimed to be very resistant to reverse engineering, to safeguard Skipjack and the family key.
- The chips must be installed in approved devices, with approved user interfaces, to guard against LEAF-free use.
- One such device is a tamper-resistant PCMCIA card; this card is expected to be generally available.

Open Issues and Concerns

- Will non-escrowed encryption be outlawed? (NSA says that won't happen.)
- Is Skipjack really secure? Can people have confidence in it?
- Is the government trying to manipulate the encryption market?
- Is the subkey generation process secure? How are the random seeds guarded?
- Is the escrow mechanism trustable? Are the *people* who run the repositories trustable? Are there loopholes in the access procedures?
- Is the key negotiation procedure trustable?
- Will the government use the chip serial numbers for traffic analysis?
- Is the concept covered by other folks' patents?

☞ The right to privacy.

A Note on NSA's Names

Clipper NSA's code name for the Mykotronx MYK-78 chip. Not to be confused with other (trademarked) uses of the word "Clipper", nor with the concept of key escrow in general.

Capstone The MYK-80, the (current) high-end key escrow chip.

Tessera NSA's code name for a PCMCIA card containing the MYK-80. There is no relation between this and any products from Tessera, Inc.

Mosaic The API spec for the PCMCIA card. Click here to escrow your keys.

Catapult A PC library implementing that API. Not related to any of the Catapult companies.

Skipjack The encryption algorithm used by current key escrow devices. Not to be confused with various fish. . . .