

## **BALANCED KEY ESCROW**

Lance J. Hoffman

[hoffman@seas.gwu.edu](mailto:hoffman@seas.gwu.edu)

Institute for Computer and Telecommunications Systems Policy

School of Engineering and Applied Science

The George Washington University Washington, D. C. 20052

August 4, 1995

GWU-ICTSP-04

### **Abstract**

This paper presents a framework for key escrow encryption that satisfies most law enforcement and civil liberties concerns. It provides users considerable autonomy in deciding how and with whom information will be escrowed. It relies on no specific technological solution but will accommodate all of them, whether implemented in hardware, software, firmware, or paper! Depending on the specific system, it may provide real-time emergency access to information when requested by authorized entities. Users, not governments, bear the costs of the scheme.

## **BALANCED KEY ESCROW**

Lance J. Hoffman

### **Introduction**

In this paper we present a framework that removes the debate about who should be able to read encrypted messages from the technological domain and pushes it back where it belongs -- into the political and legal arena. We thus hope to move the discussion past the current stalemate among government, private sector, and civil liberties interests. Any technological solution and any cryptographic algorithm can be used within the framework. Specifically,

DES [NBS 1977], RSA [Rivest 1978], PGP [Garfinkel 1994, Zimmermann 1995], Skipjack [Brickell 1993], and Commercial Key Escrow [Walker 1995] can all be supported by this framework.

## Clipper: Flawed First Steps

A system which is both readable by law enforcement authorities under certain circumstances and otherwise capable of very strong encryption has been a recent goal of the United States government. The Clipper chip's objectives were to protect American telephone communications against industrial espionage and other compromises while at the same time maintaining the existing capability of law enforcement and national security agencies to eavesdrop, with a court order, on suspect communications.

Details of this initiative appear in numerous places [Denning 1994, Brickell 1993, Levy 1994]. Clipper will never gain widespread public acceptance since there are too many people who don't trust a scheme with only government escrow agents, especially when there are currently over 15 escrowed encryption products or proposals [Denning 1995], many of which show promise of being more general, less expensive, and/or more politically acceptable to non-U. S. governments. In addition, there are almost 900 encryption products available in 33 countries around the world. Detailed lists of these are as close as the nearest bookstore [Hoffman 1995] and are available on-line via the World Wide Web at <http://www.tis.com/crypto/crypto-survey.html>.

## Key Escrow - What Is Possible Now

Key escrow systems can provide escrowed encryption that is more sensitive to the balance between the citizen and government than the flawed Clipper initiative. If society decides that one does not always have a right to private communications, then when escrow is mandatory the key can be broken up and the various parts stored with escrow agents who are available around the clock. Some of these agents would be trusted by the user and some by the government; ideally, most or all would be trusted by both. Operational requirements could be specified by Congress [HR5199 1994], the private sector, an international standards organization, or some combination of these.

A solution is available, described below, that protects against rogues, rogue governments, and rogue cartels of escrow agents. It allows the cost of encryption and the escrow agencies to be borne by users rather than the government. Persons might still communicate over private networks (e.g., within an organization) without using key escrow, but might be required to use escrowed encryption for some applications (e.g., some communications with financial institutions or the government).

While some [Ellison 1995a] might disagree, this paper assumes that there is no absolute right to encrypted communication (just like there is no absolute right to some types of speech, e.g.

shouting "Fire!" in a crowded theater) and that under certain limited circumstances authorized entities (for example, government authorities) may have the right to surveil communications and/or data. The framework described below allows escrow of both communications and data storage and presents an improved framework for deterring rogue eavesdroppers, rogue governments, rogue escrow agents, and even rogue users. While we are aware of the dangers of "excessive balance" as described by Marc Rotenberg [Rotenberg 1995], we believe that under some circumstances (e.g., prevention of [an unacceptable amount of] [computer-assisted] terrorism), mandatory key escrow may be appropriate.

## Possible Paradigms

One possible paradigm for escrow schemes which are appropriate here might be the conditions proposed by the U. S. Council on International Business [USCouncil 1994a], which stated that if a key escrow system is used, it must meet the following conditions:

- a government may not be sole holder of the entire key except at the discretion of the user
- the key escrow agent is responsible for making keys available to lawfully authorized entities when provided with proper, written legal authorizations; [there is a need for international cooperation when appropriate]
- the process for obtaining and using keys for wiretapping must be auditable
- keys obtained by law enforcement must be used for a specified, limited time frame
- the owner may also obtain the keys from the escrow agent.

Another possible paradigm [Perritt 1995] contains the following criteria:

- no limitation on encryption technique - both authentication and secrecy uses allowed
- no performance degradation due to key escrow scheme
- private key escrow must not be costly
- users can choose their own escrow agents
- escrow agents must be legally liable to follow the rules
- to access escrowed keys, government must demonstrate to a neutral party other than the escrow agent itself probable cause and no other feasible means of access to the information
- government access must not compromise further use of the system
- secure and ultimately public logs of government accesses must be provided
- export barriers must be eliminated and there should be no limitations on where keys can be escrowed
- governments outside the United States should abide by search and seizure rules (see "Note on 'exporting' the Fourth Amendment" in [Perritt 1995])

- system should prohibit government "fronts" and voluntary disclosure by escrow agents
- system must include fora for resolving disputes over its operation

Key escrow under the framework described below provides an appropriate balancing of all the interests involved, and is compatible with each of these paradigms, and allows governments and private parties to hold keys with a mix determined by each country for data [it considers] under its jurisdiction. We thus name it "Balanced Key Escrow."

## Balanced Key Escrow

We propose that future escrow schemes all be balanced. With any balanced key escrow (BKE) scheme, there can be many possible escrow agents. Not all (or even any) need be government agencies. There are several other possible escrow agents such as financial institutions, law offices, and corporate records storage facilities with a history of safeguarding confidential data. We acknowledge that (some) governments (and other entities) may (attempt to) restrict who can be an escrow agent, either to government entities only or to organizations licensed by the government. This paper does not propose such limitations.

The scheme below pertains explicitly to both messages being transmitted and messages being stored. We recognize the argument [Walker 1995] that only messages being stored are valuable enough to users that they will have an interest in using one or more key escrow agents, and that messages being transmitted, if lost, are not "retrieved" but rather retransmitted. However, for a completely general solution, we treat both cases.

The [sender] user/owner of the encrypted [message] data selects  $n$  ( $n > 1$ ) escrow agents out of the (large) set of available ones and deposits some of its key(s) with each one, using an appropriate technological scheme for key splitting. A certain mix of escrow key holders might be required, for example one each from the federal government, a civil liberties organization, an organization outside the user's local geographical area, a financial institution, and an encryption services provider. If the data is a message being sent across a communications medium, the sender also, of course, provides the key (s) to its intended recipient(s). If an authorized entity (such as a government) wishes to decrypt the [message] data, it must request a key portion from each of the  $n$  escrow agents, presenting them with a court order or other suitable authorization. After duly authenticating the authorized entity and logging this transaction, the escrow agent will reveal its portion of the key to the authorized entity. As soon as  $k$  out of  $n$  keys are recovered, it is possible for the authorized entity to obtain the entire key and thus decipher the [message] data. With some underlying systems (e.g., [Balenson 1994]), this could happen in real time or "near real time." We note that  $k$  and  $n$  might be uniform or might vary by application.

This solution protects against rogues (interlopers) because in almost all cases when (say) the government (as authorized entity) requests keys from the  $n$  escrow agents, it will get  $n$  keys

(if the escrow agents are honest) and can read the [message] data. Even if it only gets  $k$  keys ( $k < n$ ).