ELECTRONIC BANKING LAW AND COMMERCE REPORT

Encryption Licensing Arrangements as an Alternative to Key Escrow/ Recovery Products

By Elizabeth Kaufman and Roszel C. Thomsen II

Introduction

The Clinton Administration's export control policy is designed to promote development of cryptographic products that provide law enforcement agencies with access to encrypted data. Products that implement key escrow/recovery to provide such access are broadly exportable under License Exception KMI. Although some customers have indicated interest in products that implement key escrow/recovery for stored data, customers generally oppose mandatory key escrow/recovery for data in transit. This article proposes that certain networking encryption products that provide for authorized access without key recovery should also be eligible for broad export under appropriate Encryption Licensing Arrangements.

The Administration's export control policy must also reflect the equities of the intelligence community. Therefore, the proposed Encryption Licensing Arrangements should be approved subject to riders and conditions designed to prevent the export of strong encryption products to military end-users, for military end-uses, or to any government ministry, agency or department of certain countries.

The operational characteristics of networking encryption products to be eligible for export under appropriate Encryption Licensing Arrangements are not complex. Simply stated, the operator action model delivers a "private door-bell," not a "house-key" to parties lawfully seeking access to data. Qualifying products must incorporate an operator-controlled management interface that enables dynamic, real-time access to specified network traffic prior to encryption, or after decryption, at a designated access point.

Background

In Executive Order 13026 of November 15, 1996, President Clinton said that cryptographic products implementing the Key Management Infrastructure ("KMI") would be eligible for export without licenses after a one-time technical review.[1] On December 30, 1996, the Commerce Department's Bureau of Export Administration ("BXA") published an interim rule amending the Export Administration Regulations ("EAR," 15 CFR Part 730 et seq.) that implements Executive Order 13026.[2]

The better-known provision of this interim rule states

Elizabeth Kaufman is with Cisco Systems, Inc.; Roszel C. Thomsen II is a partner with the firm of Thomsen & Burke LLP.

that "key escrow or key recovery products" are exportable under License Exception KMI. The term "key escrow or key recovery products" is defined in great detail in Section 740.8(d)(1)(i) and Supplement No. 4 to Part 742 of the EAR.

A lesser-known provision of this interim rule states that "other recoverable encryption products" shall receive "favorable consideration" for export. The term "other recoverable encryption items" is defined briefly in Section 740.8(d)(1)(ii) of the EAR, and the type of "favorable consideration" that should be accorded to such products is not defined at all. The ambiguity of this provision provides an opportunity to explore new approaches to exporting cryptographic products.

Overview

Industry has studied the technical, market and policy issues surrounding the KMI. These studies suggest that there may be market demand for products implementing key escrow/recovery techniques for retrieval of encrypted stored data. Such products would also appear to meet law enforcement's requirements for retrieval of encrypted stored data. However, no market demand exists for products implementing key escrow/recovery techniques for retrieval of encrypted transient data. Eminent cryptographers have argued that key escrow/recovery techniques create unnecessary risks for encrypted transient data.[3] The National Security Agency ("NSA") has confirmed these findings.[4]

The networking industry proposes that certain networking encryption products described in this White Paper may receive wide market acceptance and meet the requirements of law enforcement with respect to transient data without implementing key recovery. The intelligence community's equities, though not reflected in the EAR, must be respected as well.

Analysis of Market Requirements

In order to meet market requirements, networking encryption products must:

(1) provide strong security;
(2) adhere to open standards; and
(3) support an operator-controlled management mechanism to specify encrypted flows.

Strong security is essential for products that encrypt transient data. Customers, particularly service providers, have stated repeatedly and emphatically that they will not purchase products that encrypt transient data, if those products also facilitate unauthorized, covert surveillance by third parties. The government should encourage the deployment of products that implement strong security, because such products will deter certain kinds of crimes, like theft of trade secrets by third parties.

Deployment of products that encrypt transient data requires open standards. Without open standards, different vendors' products will not inter-operate, and broad deployment will not be possible. The government should encourage the deployment of standards-compliant products, because it has a shared interest in a common cross-vendor solution and the rapid deployment of strong new viable technologies.

Some customers also have indicated that operator-control of encryption flows is a useful feature for network diagnostics and reporting, and for allowing the efficient transmission of non-sensitive data. Customers in regulated industries, such as banking and securities, also may need to monitor their employees' communications from time-to-time. Most customers also desire the ability to respond to a court order without exposing all of their data across the Internet or the public switched telephone network.

Analysis of Government Requirements

The EAR describes key escrow/recovery products primarily in terms of their utility to law enforcement. The government's interests, however, are not monolithic. The law enforcement and intelligence communities have different requirements.

Law enforcement's main priority has been to establish procedures for access to encrypted data in transit that are comparable to existing procedures for voice communications and therefore capable of introduction into evidence in a court of competent jurisdiction. The technical characteristics of the networking encryption products described in this article will be of greatest interest to law enforcement, because these technical characteristics are the key to meeting law enforcement's requirements for access to plaintext.

The intelligence community, on the other hand, has not shown much confidence that key escrow/recovery will meet its requirements since the secret Skipjack algorithm and governmental escrow agents featured in the original Clipper Chip were abandoned in favor of vendor-selected algorithms and commercial escrow agents. Its primary concern currently appears to be the broad deployment of encryption technology that does not interfere with current best operational practices. In this regard, the technical characteristics of qualifying products may be of secondary importance to theintelligence community, and proposed riders and conditions on the ELA may be of greater importance.

An Alternative to Key Escrow/Recovery for Networking Products

Although key escrow/recovery is not acceptable for data in transit, some customers require a mechanism that can reveal real-time plaintext for network diagnostics and reporting, the transmission of non-sensitive data, occasional employee monitoring, and to support law enforcement. The proposed alternative to key escrow/recovery does not require weakened cryptography, yet provides

access similar to that currently available for voice communications.

Packet switched data networks handle traffic differently than circuit-switched voice networks. Circuit switchedvoice networks are characterized by the opening of a dedicated circuit where communications are transferred in "real-time". Packet switched networks are a statistically-multiplexed environment where communications are routed packet-by-packet, so that data is fragmented but delivered in near real time. In spite of these differences, packet switched data networks can, with some limitations, enable real-time access to plaintext. The proposed alternative to key recovery provides customers with full-strength encryption, while simultaneously enabling the dynamic creation of an access point that allows real-time interception of plaintext based upon the target's source or destination, whether the product is located within an enterprise or at a service provider's premises.

Two Access Scenarios: Access in the Enterprise, and Access at a ServiceProvider's Premises

The access point concept is not a perfect solution for all products. For example, it does not easily apply to user-to-user desktop applications. However, it does appear to offer a reasonable alternative to key recovery on many classes of network applications and platforms. Specifically, it is a viable approach to access to plaintext for devices where the individual responsible for data creation/reception is not the same individual responsible for platform operation. Such devices constitute a significant percentage of the available networked platforms, including firewalls, routers, switches and other networking devices.

Meeting Law Enforcement Requirements

In order to be exportable under the proposed Encryption Licensing Arrangements, networking encryption products must contain a management interface that dynamically controls encryption by source and destination address, and by network protocol, to enable real-time access to selected network traffic prior to encryption or after decryption. The operational characteristics of these products may be summarized below:

A qualifying network encryption product must incorporate an encryption management interface that:

- is remotely accessible;
- controls the encryption configuration of the platform;
- configures encryption policy by source and destination network address;
- enables a remote operator to modify the encryption configuration dynamically;
- enables the interception of network traffic between a specific source and destination either prior to encryption or after decryption at a defined access point;

A qualifying network encryption product may:

- be hardware, software, or a combination of hard ware and software;
- encrypt any network protocol and/or at any network layer;
- support any encryption algorithm, key length, key generation mechanism, key management scheme;
- be standalone, or integrated with other functions;
- be a single user, multi-user or infrastructure platform;
- enable interception on the wire, on media (such as a hard disk), via a specialized communications port, or at another defined access point.

Meeting the Intelligence Community's Requirements

Current best operational practices are not widely understood by the public, and they may be compromised by the broad deployment of networking encryption products, whether of U.S. or of foreign manufacture. However, the possible loss of access to plaintext communications due to use of commercial cryptography must be analyzed within the broader framework of advances in new technologies. As one eminent cryptographer testified before the Senate Judiciary Subcommittee on Technology and the Law, "Advances in emitter identification, network penetration techniques, and the implementation of cryptanalytic or crypto-diagnostic operations within intercept equipment are likely to provide more new sources of intelligence than are lost as a result of commercial use of cryptography."[5]

In further recognition of and deference to the intelligence community's equities, industry is not requesting authorization to export products with key lengths exceeding 56 bits to military end-users or for military end-uses, or to any government ministry, agency or department of the countries listed in "Tier 3" (as defined for purposes of computer export controls). Exports of products exceeding 56 bits to these end-users would require a separate license issued by BXA after full inter-agency review under applicable Executive Orders. The differences between the proposed ELA and export under License Exception KMI are summarized in the chart on page 13.

Conclusion

This White Paper has defined a class of networking encryption products that should be authorized for export under appropriate Encryption Licensing Arrangements. The operational characteristics of qualifying products ensure that law enforcement will continue to enjoy authorized real-time access to plaintext. ■

	License Exception KMI	Proposed ELA
Eligible Products	Key recovery products	Products providing access to plaintext at intermediate stations of the data network
Territory	All except Cuba, Iran, Iraq Libya, North Korea, Sudan, and Syria	Same as KMI
Eligible End-Users	All end-users are eligible	(1) All end-users are eligible for 56 bit products, however: (2) Products exceeding 5 bits would not be eligible for government agencies and military end-users in Tier 3 countries
Duration	Indefinite	Three years, renewable in three-year increments
Reporting	Biannual	same as KMI

Footnotes

1 61 Fed. Reg. 58767 (November 15, 1996).

2 61 Fed. Reg. 68572 (December 30, 1998).

3 H. Abelson *et al.*, *The Risk of Key Recovery, Key Escrow and Trusted Third Party Encryption,* (June, 1998).

4 National Security Agency, *Threat and Vulnerability Model for Key Recovery (KR),* X3 (February 18, 1998).

5 *Key Escrow: Its Impact and Alternatives,* Testimony of Dr. Whitfield Diffie, Distinguished Engineer, Sun Microsystems, Inc. before the Subcommittee on Technology and Law of the Senate Judiciary Committee (May 3, 1994).