Network Working Group IAB
Request for Comments: 1984 IESG
Category: Informational August 1996

IAB and IESG Statement on Cryptographic Technology and the Internet

Status of This Memo

Copyright

July 24, 1996

The Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG), the bodies which oversee architecture and standards for the Internet, are concerned by the need for increased protection of international commercial transactions on the Internet, and by the need to offer all Internet users an adequate degree of privacy.

Security mechanisms being developed in the Internet Engineering Task Force to meet these needs require and depend on the international use of adequate cryptographic technology. Ready access to such technology is therefore a key factor in the future growth of the Internet as a motor for international commerce and communication.

The IAB and IESG are therefore disturbed to note that various governments have actual or proposed policies on access to cryptographic technology that either:

(a) impose restrictions by implementing export controls; and/or

(b) restrict commercial and private users to weak and inadequate mechanisms such as short cryptographic keys; and/or

(c) mandate that private decryption keys should be in the hands of the government or of some other third party; and/or

(d) prohibit the use of cryptology entirely, or permit it only to specially authorized organizations.

We believe that such policies are against the interests of consumers and the business community, are largely irrelevant to issues of military security, and provide only a marginal or illusory benefit to law enforcement agencies, as discussed below.

The IAB and IESG would like to encourage policies that allow ready access to uniform strong cryptographic technology for all Internet users in all countries.

The IAB and IESG claim:

The Internet is becoming the predominant vehicle for electronic commerce and information exchange. It is essential that the support structure for these activities can be trusted.

Encryption is not a secret technology monopolized by any one country, such that export controls can hope to contain its deployment. Any hobbyist can program a PC to do powerful encryption. Many algorithms are well documented, some with source code available in textbooks.

Export controls on encryption place companies in that country at a competitive disadvantage. Their competitors from countries without export restrictions can sell systems whose only design constraint is being secure, and easy to use.

Usage controls on encryption will also place companies in that country at a competitive disadvantage because these companies cannot securely and easily engage in electronic commerce.

Escrow mechanisms inevitably weaken the security of the overall cryptographic system, by creating new points of vulnerability that can and will be attacked.

Export controls and usage controls are slowing the deployment of security at the same time as the Internet is exponentially increasing in size and attackers are increasing in sophistication. This puts users in a dangerous position as they are forced to rely on insecure electronic communication.

TECHNICAL ANALYSIS

KEY SIZE

It is not acceptable to restrict the use or export of cryptosystems based on their key size. Systems that are breakable by one country will be breakable by others, possibly unfriendly ones. Large corporations and even criminal enterprises have the resources to break many cryptosystems. Furthermore, conversations often need to

be protected for years to come; as computers increase in speed, key sizes that were once out of reach of cryptanalysis will become insecure.

PUBLIC KEY INFRASTRUCTURE

Use of public key cryptography often requires the existence of a "certification authority". That is, some third party must sign a string containing the user's identity and public key. In turn, the third party's key is often signed by a higher-level certification authority.

Such a structure is legitimate and necessary. Indeed, many governments will and should run their own CAs, if only to protect citizens' transactions with their governments. But certification authorities should not be confused with escrow centers. Escrow centers are repositories for private keys, while certification authorities deal with public keys. Indeed, sound cryptographic practice dictates that users never reveal their private keys to anyone, even the certification authority.

KEYS SHOULD NOT BE REVEALABLE

The security of a modern cryptosystem rests entirely on the secrecy of the keys. Accordingly, it is a major principle of system design that to the extent possible, secret keys should never leave their user's secure environment. Key escrow implies that keys must be disclosed in some fashion, a flat-out contradiction of this principle. Any such disclosure weakens the total security of the system.

DATA RECOVERY

Sometimes escrow systems are touted as being good for the customer because they allow data recovery in the case of lost keys. However, it should be up to the customer to decide whether they would prefer the more secure system in which lost keys mean lost data, or one in which keys are escrowed to be recovered when necessary. Similarly, keys used only for conversations (as opposed to file storage) need never be escrowed. And a system in which the secret key is stored by a government and not by the data owner is certainly not practical for data recovery.

SIGNATURE KEYS

Keys used for signatures and authentication must never be escrowed. Any third party with access to such keys could impersonate the legitimate owner, creating new opportunities for fraud and deceit.

Indeed, a user who wished to repudiate a transaction could claim that his or her escrowed key was used, putting the onus on that party. If a government escrowed the keys, a defendant could claim that the evidence had been forged by the government, thereby making prosecution much more difficult. For electronic commerce, non-repudiation is one of the most important uses for cryptography; and non-repudiation depends on the assumption that only the user has access to the private key.

PROTECTION OF THE EXISTING INFRASTRUCTURE

In some cases, it is technically feasible to use cryptographic operations that do not involve secrecy. While this may suffice in some cases, much of the existing technical and commercial infrastructure cannot be protected in this way. For example, conventional passwords, credit card numbers, and the like must be protected by strong encryption, even though some day more sophisticated techniques may replace them. Encryption can be added on quite easily; wholesale changes to diverse systems cannot.

CONFLICTING INTERNATIONAL POLICIES

Conflicting restrictions on encryption often force an international company to use a weak encryption system, in order to satisfy legal requirements in two or more different countries. Ironically, in such cases either nation might consider the other an adversary against whom commercial enterprises should use strong cryptography. Clearly, key escrow is not a suitable compromise, since neither country would want to disclose keys to the other.

MULTIPLE ENCRYPTION

Even if escrowed encryption schemes are used, there is nothing to prevent someone from using another encryption scheme first. Certainly, any serious malefactors would do this; the outer encryption layer, which would use an escrowed scheme, would be used to divert suspicion.

ESCROW OF PRIVATE KEYS WON'T NECESSARILY ALLOW DATA DECRYPTION

A major threat to users of cryptographic systems is the theft of long-term keys (perhaps by a hacker), either before or after a sensitive conversation. To counter this threat, schemes with "perfect forward secrecy" are often employed. If PFS is used, the attacker must be in control of the machine during the actual conversation. But PFS is generally incompatible with schemes involving escrow of private keys. (This is an oversimplification, but a full analysis would be too lengthy for this document.)

CONCLUSIONS

As more and more companies connect to the Internet, and as more and more commerce takes place there, security is becoming more and more critical. Cryptography is the most powerful single tool that users can use to secure the Internet. Knowingly making that tool weaker threatens their ability to do so, and has no proven benefit.

Security Considerations

Security issues are discussed throughout this memo.

Authors' Addresses

Brian E. Carpenter
Chair of the IAB
CERN
European Laboratory for Particle Physics
1211 Geneva 23
Switzerland

Phone: +41 22 767-4967
EMail: brian@dxcoms.cern.ch

Fred Baker
Chair of the IETF
cisco Systems, Inc.
519 Lado Drive
Santa Barbara, CA 93111

Phone: +1-805-681-0115
EMail: fred@cisco.com

The Internet Society is described at http://www.isoc.org/

The Internet Architecture Board is described at http://www.iab.org/iab

The Internet Engineering Task Force and the Internet Engineering Steering Group are described at http://www.ietf.org