Rohit Kr. Sahu CH-8
31999685792
SBI Rurri Saidpur

Legal and Ethical Issues Related to Cryptography and Information

Information infrastructure for cryptography

Cryptography has become a technology of broad applications, so the decisions about cryptography have increasingly broad effects on society. Applications of cryptography have evolved along with cryptography techniques. Originally cryptography was used to protect the confidentiality of communications; encryption is now also used to protect the confidentiality of electronic information and to protect the integrity and authenticity of both transmitted and stored information.

There is a need to internationally create an infrastructure to support encryption. This is important especially with the use of public-key encryption and digital signatures. However, there are many conflicting interests that make this effort a very demanding task. The main global challenges are:

- International cryptography policies and regulations
- Commercial cryptography
- Key escrow encryption
- Business requirements, use of cryptography with electronic payments
- Privacy and trust.

Digital certificates and trusted third parties

Symmetric encryption is not well suited to open networks with spontaneous communication. With the advent of public-key techniques, cryptography came in use for digital signatures that are of widespread interest as a means for electronically authenticating and signing commercial transactions, as well as ensuring that unauthorized changes or errors are detected. For a system using public key cryptography, a certificate for demonstrating identity would, at a minimum, contain the public portion of the subjects public key and be signed by the issuer [4]. Certification Authorities (CA) guarantee the authenticity of their clients. X.509 is becoming to be the internationally recognised standard form of digital certificates.

Key management is fundamental to the security afforded by any cryptography-based safeguard. Different key administration policies, such as hierarchical (PEM) and user-centered (PGP), have many implications on the required infrastructure for the overall system. VeriSign (a spin-off of RSA Data Security) and COST are commercial companies that provides CA-services.

The "key escrow system" refers to a policy under which users of encryption systems give copies of their encryption keys either to their government, or to a third party that the government trusts.

If the person, who has used digital signature at a certain time, wants to prove it to someone else, a digital notary is needed. The notary can time-stamp the signatures with a unique "digital fingerprint". This service can be used, for example, to time-stamp research data and papers, witness fraud, and to form non-forgeable digital agreements. Surety Technologies is an example of a commercial digital notary service.

Global vs. national interests

It is a well-known fact that, despite the global nature of the information networks, there do not exist global laws or agreements on how to handle conflicts between different legal systems. A Good example is the recent attempt of the Iranian government to charge Michael Jackson and Madonna for violating the Iranian laws of indecency. Our European notions of basic rights, morality, law, and ethics are generally individually oriented, and not accepted worldwide. Liable laws are traditionally national, yet they are applied in Cyberspace. Is there a notion of global liability? How do I sue a person in another nation? What happens to global commerce if there is not a common understanding? Can there be an international agreement on the transport of cryptography material across national boundaries?

Cryptography has traditionally been a national-security issue, and several countries, especially the U.S., have placed export controls on cryptography technology. Export controls intend to restrict international availability of this technology and cryptography products. U.S. export controls on cryptography have substantially slowed the proliferation of strong encryption to foreign adversaries over the years. Some countries like France or Russia, have also import controls on cryptography. This is because the local government wants to have full control over cryptography technology.

Phil Zimmermann's PGP is a good example of a very controversial case of export restrictions. Zimmermann is currently charged for exporting the PGP overseas, because this strong algorithm has been accessible on the Internet.

Government vs. public interests

A lot of the current controversy over cryptography can be characterised in terms of tension between government and individuals. Powerful encryption tools are widely available to people all around the world, and there seems to be nothing that can stop these technologies from spreading, also to criminal use [3]. From the government's point of view, the availability of strong encryption methods to the general public is a threat to public security and safety - terrorists and criminals can communicate freely, since the officials do not have any possibility to decrypt these digital signals. Therefore, there are initiatives in the U.S. and in Europe that intend to preserve the law-enforcement and signal-intelligence capabilities of governmental agencies.

The Escrowed Encryption Standard (EES) was approved in 1994 as a Federal Information Processing Standard in the U.S. This standard is intended for voluntary use by all federal departments and agencies, and to replace DES as the federal encryption system. The

standard is better known as the "Clipper chip", because of the early implementation of the encryption algorithm was called Clipper. This U.S. government initiative has raised a lot of debate about the misuse of the technology, by possible violation of telephone and computer privacy. There seems to be a large mistrust on government motives to introduce this technology. These protocols have been designed secretly, without consultation and open critics by the academia or industry.

From a public point of view, the encryption should not be based on classified algorithms, it should be voluntary to use, and there should not be any restrictions in using it internationally. The computer industry in the U.S. has complained furiously about the competitive disadvantage the export control has on their international operations. Recently, U.S. administration lifted the export regulations on strong cryptography (such as DES), when it is coupled with a key escrow mechanism. There is a commercial need for escrowed key systems, so the system could be based on other trusted third parties than governmental organisations. Some of the open questions related to these "key escrow agents" include:

- What kind of organisations should be approved as key escrow agents? Should there be international co-operation?
- What sort of legal agreement between the government and the key escrow agent is needed?
- Should intentionally misreleasing or destroying a key be criminalised?
- Should approval of key escrow agents be tied to public key infrastructure?
- What procedures are needed for the storage and safeguarding of keys?

The Council of Europe has proposed a similar standard to EES to monitor signals in all member states, and the European Commission has recently announced that the EU will introduce European cryptography standards that are based on key escrow. The Commission plans to propose that member states can choose private trusted third parties, rather than governmental departments, to regulate networks.

Electronic commerce

As businesses replace conventional paper-based business with standardized computer-based communications, the need arises to secure the transactions and establish means to authenticate and provide non-repudiation services for electronic transactions. In a very short period, the Internet has changed into an international electronic marketplace, where all types of goods are being bought and sold.

The digital transactions should provide a way to securely:

- order the goods
- pay for the goods
- deliver the goods, and in such a manner that the customer can get money back, if not satisfied

The universal acceptance of networks for transacting business requires security measures to ensure the privacy needed for commercial transactions in a global environment. The legal issues regarding electronic commerce are:

- contractual writing requirements
- legally binding signatures
- use of electronic communications as evidence of a contract

Contractual requirements

One of the primary goals of electronic transactions is the elimination of paper, which ultimately means the elimination of conventional signatures. Digital signatures provide a way to enhance the traditional security of commerce by introducing signatures that are non-forgeable. The law of evidence in the electronic context could require the following [6]:

- proof that an electronic communication actually came from the party that it purports to come from
- proof of the content of the transaction, namely, the communications that actually occurred between the parties during the contract formation process
- reducing the possibility of alteration of the contents of electronic record of the transactions

There is some controversy in the laws regarding contract writing and signatures. Even in traditional means of paper/fax/telex -based commerce there is always a possibility of fraud. It seems that encrypted digital signatures are not required for an electronic message to have the status of a legal contract. According some law cases in the U.S., even plaintext email messages can be used in court as proof of a contract, even though they are easily forgeable. This is because email is currently already used for binding contracts. Ethically email is of course as binding as any given word.

In the world of electronic commerce also the integrity of the documents is questionable. Digital notary services can be used to ensure the non-repudiation of the documents.

Commercial transactions, time-stamping and trusted entities

The area of cyber-economy and electronic transactions is developing very rapidly. Digital signatures have been proposed to solve some of the problems related with security and privacy. For example, DigiCash uses a mechanism of so called blind digital signatures.

The inherent limitation of the use of digital signatures, is their inability to provide time-related non-repudiation. While a digital signature attached to a message will have a time-stamped audit trail through the network, digital signatures cannot, in the absence of a trusted entity, provide an non-forgeable, trusted time stamp.

The key attributes of a trusted entity are that it is a disinterested third party trusted by the parties to the transaction, and subject to the dispute resolution mechanisms relevant to a

transaction or record. A trusted entity can perform a variety of functions to facilitate electronic contracts:

- producing a document audit
- storing a record copy of electronic documents
- providing time stamps
- generating authentication certificates to ensure the identity of communicating parties.

Digital money

Digital money can have fundamental implications on the way the international economy works. The introduction of international digital money has happened very quickly, and the economical and social implications are unpredictable. This is because electronic money can move without leaving a trace, and it is impossible to control trans-border flow of electronic money.

Some of the biggest legal and ethical questions are:

- Who collects taxes and duties? When should they be collected?
- Will grey economy flourish because of the electronic money?
- Can electronic cash be transmitted directly from one person to another without a third party?
- Who is allowed to make electronic money?
- Will there be many types of electronic money?
- How to change electronic money from one currency to another? Who is authorized to do this?

As a summary, the tools that national governments and national central banks have to control the monetary flows will be severely diminished. The legislation is lagging far behind this new technology.

Digital copyright

Laws that are presently used to protect the creators and vendors of digital information often predate the development of computer technology, and it is not clear which laws apply to digital information. Ways in which digital information differs from information in more traditional forms include [6]:

- digital works are easily copied, with no loss of quality
- works can be easily transmitted to other users or be accessed by multiple users
- works that are treated differently under current copyright law are essentially equivalent: text, video, audio are all series of bits
- works are inaccessible to the user without hardware and software tools for retrieval, decoding, and navigation
- material can be searchable, linked, and interactive

Cryptography can provide new means of protecting intellectual property in the digital world. However, this raises other important ethical and sociological issues: should there be free copies of information available for lend in libraries? If so, what prevents all users from taking a free copy of the work.

Justification for copyright

The copyright law is a social construct tailored to encourage intellectual work. Technological innovations have traditionally changed the notion of copyright. There was no copyright law before the invention of the printing press.

The producer of information is granted a reward for his efforts by the copyright law. Copyright protects the owner of intellectual property against unauthorized copying, manipulation, and re-distribution of copyrighted material.

If there were other effective methods for assuring the availability of adequate supplies of information to the public, copyright might not be needed. It may be that contracts and licensing will prove to be a better and more flexible alternative. Some people argue that information should be free to everyone.

Richard Stallman's GNU project is perhaps the best-known example of an effort to make good-quality free software. The fundamental idea behind the GNU Manifesto is that limiting access to software hinders a programmer's capability to share his work with other programmers. Copying all or parts of a program is as natural to a programmer as breathing, and as productive. It should be as free, argues Stallman. His ideas are easily extendable to any kind of information.

John Perry Barlow goes further and defines our notions of intellectual property fundamentally flawed. He also claims that the current practises regarding Internet and software piracy are based more on a "social contract" than on existing laws. Software users pay for programs they really need (to get the latest version, good service, etc.). Where the law has failed, ethics have re-emerged.

Encryption and copyright

Cryptography seems to be the basis for implementing copyright and access authorization in cyberspace. However, the software market rejected copy protection in most cases. The same will probably happen to many of the upcoming efforts to use cryptography-based protection schemes.

An obvious problem with encryption as a global solution is, that once something has been decrypted by an authorized user, it may be available to massive reproduction. In some products this is not a problem, since the information degrades rapidly in value with time.

Data hiding

Data hiding (i.e. steganography) is the process of embedding data into digital signals. These techniques can be used in copyright protecting and tamper-proofing of data. For example an image could be interwoven with code which continues to protect the data. The file could include code that would "sense" the surrounding environment and interact with it. The owner could be contacted whenever the file is being accessed, or files might require periodic "feeding" with digital cash from the user, which they would relay back to their authors.

Data hiding is distinct from encryption. The goal of data hiding is not to restrict or regulate access to the host signal, but to ensure that embedded data remains inviolate.

Data hiding can be used to provide solid proof of the copyright and assurance of content integrity. An owner's digital signature is hidden in the copyrighted material. The key to successful data hiding is to find "holes" in the digital signal that are not suitable for exploitation by compression algorithms. Technically data hiding is a very demanding task.

Digital libraries

The introduction of digital libraries raise difficult and complex copyright issues that do not arise with traditional libraries. If the digital library is connected to the international networks, as soon as the first copy of the work is available free in the library, it is potentially simultaneously accessible to everybody connected to cyberspace. Why would anybody then pay for the information?

On the other hand, there is a fundamental problem with a system that requires, through technology, payment for every access to a particular piece of information. This is against the principles of public library systems that are based on free and fair use, as in Finland. It would be difficult to refer to scientific facts, if checking (and possibly also making) the reference costs money. Thus pay-per-use may deter learning and research work. In scientific work, it is very often the interest of the publisher to insist for copyrights and payments for all uses of the material.

It is a very demanding task to find a balance between author/publisher interests in receiving compensation and user/library interests in having access to information on fair and reasonable terms. The strict pay-per-use scenario is unlikely to succeed in cyberspace. Consumers will probably fear excessive pricing from pay-per-use schemes [7]. License-based arrangements can solve the problem, at least partly.

The alternative, having totally free services, will most probably lead to overuse, imbalances, and access restrictions based on allocation rules. This will also lead to reduction of quality [10].