Sign Your Name on Internet

“E-signature” Sign Your Name on Internet.

Haw Hsin Yang

Rutgers University-Camden

Introduction

In the past decade, human beings have been experiencing an unprecedented and radical technological change, especially in business solutions brought by the rapid popularity and the widespread applications of Internet. On one hand, Internet does create a lot of benefits that we've never had before; on the other hand, what comes together is a number of unexpected challenges.

One of the most rigorous challenges is Internet fraud. The amount of money consumers are losing to Internet fraud is obviously increasing. According to the IFCC (Internet Fraud Complaint Center) 2002 Internet Fraud Report, from January 1, 2002 to December 31, 2002, the IFCC Web site received 75,063 complaints. This amount includes many different kinds of complaints, such as auction fraud, credit/debit card fraud, computer intrusions, SPAM mails, and child pornography. Meanwhile, IFCC has filed 48,252 complaints as fraudulent cases, and this number also means a three-fold increase from the previous year. The total dollar loss from all referred cases of fraud was dramatically increased, from$17 million in 2001 to $54 million in 2002, with a median dollar loss of $299 per complaint. (IFCC 2002 Internet Fraud Report [EPA], 2002)

Overview

In addition, it is believed that a lot of fraudulent cases are still not reported to law enforcement agencies, which makes exact numbers impossible to calculate. According to numerous reports and studies, there is a strong positive correlation between the sales amount of online market and the security of transferring transaction data. In order to keep on-line sales thriving, security of transaction is the most important issue in Internet era.

According to the Federal Trade Commission's figures, ID theft is the most popular form of consumer fraud, in part because it is the most profitable. As long as someone's personal data is stolen, unauthorized buying as well as fraudulent selling behaviors will be easily made and intentionally used for illegal economic gains. In an e-commerce model, payments for goods are always the most critical part of a business model and also the most insecure part of it for both buyers and sellers since identity data can be intercepted and reproduced without consciousness. There are up to 700,000 people in the United States may be victimized by identity thieves each year, according to the Justice Department (during press release- 2002 Federal Trade Commission Study). For a single consumer, the loss may be limited, but for a business, the loss may seriously affect its normal operations. ID thieves stole nearly $100 million from financial institutions last year, or an average of $6,767 per victim. (National Consumers League [NCL], 2002)

Background of E-signature

To regulate the order of on-line transactions and to decrease the situation of identity theft, U.S. regulators adopted laws bit by bit that put e-signature into action. The turning point happened in 2000 as President Clinton signed the "Electronic Signature in Global and National Commerce Act" (or the "E-Signature Act"). This act gives the E-signature a legal position in the real world, and, hopefully, E-signature would reduce the situation of identity theft and fraud.

The technology of E-signature is based on Public Key Infrastructure (or PKI). A PKI tool enables users of a basically insecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair. (Fields, 2001). The key pair must be obtained and shared through a trusted authority. Users are responsible for taking care of their own private key, and all public keys are under issuers' custody. Those issuers of digital certificates are called "Certification Authority" (CA), which is the most fundamental section of PKI system. Above CAs, a Registration Authority (RA) acts as the verifier for the CA before a digital certificate is issued to a requestor. In this way, both RA and CA should be independent third parties between buyers and sellers.

The concept of how E-signature works is, first, requiring a user, an individual or an organization, to register and verify his identity with CAs that issues "digital certificates." And then, the certificate that includes a unique private key can be used to "sign" documents. This "signing" process employs encryption to rule out tampering and following adjustment. Finally, the receiver electronically checks back with the CAs by verifying whether the key pair is matching or not. Therefore, the sender's identity can be recognized, and then, the origin of this document is therefore confirmed.

Benefits of E-signature

By applying e-signature, not only e-business but also traditional businesses will benefit in several ways. Some of the benefits are presented as follows.

1. Enhanced security. E-signature allows companies to share confidential information with intended entities and keeps unintended others away. In addition, electronically signed documents dramatically reduce chances of being forged. In this way, traditional handwriting forgers cannot fabricate signatures on a check or a document anymore.
2. Decreased communications cost. E-signature creates an easier internal communication system for employees. All internal activities which require managers' authentication or colleagues' responses are able to be simplified just by e-mails.
3. Elimination of time for business processes. Since verification and authentication jobs in financial businesses can be very time-consuming, E-signature handles this process rapidly and creates a great deduction of needed time.
4. Reduced headcount. As business processes can be eliminated, those employees who are previously responsible for manual jobs become redundant.
5. Paperless documentation. Even though the using of ERP applications has already reduce the usage of papers, business processes still require a lot of paper work, such as legal documents, checks, and so forth. E-signature is able to validate an electronic document as a physical one.

Concerns of E-signature

One thing, however, is certain in such a rapid changing world: there are always pros and cons existing in a new technology. Some points need to be made here.

1. Once a company employs E-signature, new risks are also introduced. It brings a persistent and fundamental change to business processes, especially in accounting and internal audit functions. There are some essential concerns to lower the new risk.
   1) Regular review for digital processes and examination of their results to prevent from white collar crimes.
   2) Update storage facilities of digital files to keep transactions records current in case hardcopies are required.
   3) Agreements between CA and business partner should be reviewed periodically and kept to comply present laws.

2. Since CAs are the most fundamental section of PKI infrastructure, there are some issues dealing with it.
    1) As a trusted authority, a CA has to meet some requirements, such as a minimum amount of capital and technical standards, to prove that it is able to offer such an important service since companies will trust it to fulfill their obligations to other companies.
    2) Once a mistake of an authentication happens, how to make up for the loss resulted from the error? Who needs to pay the insurance fees?
    3) Once a CA goes bankrupt, there should be a standard procedure to take care of existing clients, such as how to look for another CA as soon as possible, whether the new CA can extend previous contract, and so forth.
3. Although all public key are under CAs' supervision, another concern is that users are also required to take care of their own private keys. The computer which is responsible for keeping and using the private key needs to be very secure to keep from intended penetration by hostile code or physical tampering.
4. A key's lifetime, "Certificate Revocation" should be limited. Regular updating of both public and private keys is able to increase the security when applying E-signature.
5. As long as a consumer or corporate buyer makes a mistake, he should have a right to withdraw consent in a certain period of time and the procedure for withdrawal should be informed to every purchaser.

Summary

Many countries, including U.S., German, Italy, Japan, Taiwan, and so forth, are developing PKI infrastructure to drive E-signature to make its mark. Large corporations and governments in those countries have been investing in a lot of resources to set E-signature in motion as all of them can make a huge cost saving through digital documentation. So far, there are nearly 123 CAs offering digital certificate in world. This number seems enough, but actually insufficient. Since Internet is a phenomenon of globalization, PKI infrastructure needs to be in the same world-wide way.

However, U.S. companies are not adopting the technology as quickly as those in Asia and Europe. Although Utah State legislate their own E-signature law in 1995 and federal government also passed the aforementioned "E-signature Act" in 2000, E-signature has not been very popular yet.

It seems reasonable to conclude that; first, PKI infrastructure needs sufficient planning and preparation. Inside U.S., waiting for all states to legislate E-signature still has a long way to go. Further, in order to achieve a global PKI infrastructure, it is crucial to wait for U.S., the biggest economic entity in world, to prepare itself. Second, as a result of the concerns mentioned above, there may be any unexpected operational and technical problems which hinder E-signature. Finally, and most importantly, it is extremely hard to change a thousands-of-years habit of human beings. A single click is so different from someone's own handwriting that many people still spend time to handle an important thing in person rather than sit in front of a computer to deal with it.

Reference:

Bushong, J.G., Helms, G.L. & Nelms, L. (2002) Security in Internet e-commerce. *Ohio CPA Journal, Vol.61*, 12-15.

Etheridge, Y. (2001). PKI-how and why it works. *Health Management Technology, Vol.22,* 20-21.

Fields, J. (2001, January 25). E-signatures Wait to Make Their Mark. *BusinessWeek online.* Retrieved October 30, 2003, from http://businessweek.com/smallbiz/content/jan2001/sb20010125_385.htm

Grupe, F., Kerr, S.G., Kuechler, W. & Patel, N. (2003) Understanding Digital Signatures. *The CPA Journal, Vol.73*, 70-75.

Mann, K. (2000). *Unlocking public key infrastructure.* Retrieved November 3, 2003, from http://www.vnune.com/features/1104266

National Consumers League. (2002). Internet Fraud Statistics for all of 2001. Retrieved November 3, 2003, from http://www.fraud.org/internet/2001stats.htm.

National White Collar Crime Center & Federal Bureau of Investigation. (2002). *IFCC 2002 Internet Fraud Report.* Richmond, VA: Author.

Piazza, P. (2001). Can you trust online IDs? *Security Management, Vol.45*, 39.

PKI. (2002). SearchSecurity.com. Retrieved November 3, 2003,
from http://searchsecurity.techtarget.com/sdefinition/0,,sid14_gci214299,00.html