MANAGING THE ADVANCEMENT OF DOCUMENTS GOING DIGITAL

By
Zahri Yunos and Ahmad Nasir Mohd Zin
National ICT Security and Emergency Response Centre (NISER)

(This article was published in The Star InTech on 29 April 2004)

Protecting digital information has been looked at from different angles since the inception of the computer. Today, once the enterprises complie information in the digital format, they are at the mercy of the end user. When information is on the desktop, the end user has the ability to copy, paste, forward and print any part of that information. Hence information getting into the wrong hands presents a major problem for the enterprises.

Among the issues involved in managing digital information are:

- **Integrity of documents**

  Integrity is about safeguarding the accuracy and completeness of digital documents and its processing method. However, advances in digital technologies and the widespread availability of relatively easy-to-use, low-cost PCs, scanners and printers have made it easy to counterfeit documents. These same advances have made it more difficult to discern authentic from counterfeit documents.

- **Confidentiality of documents**

  Confidentiality is about ensuring that the digital document is accessible to authorised users. There must be adequate protection while ensuring confidentiality of digital information. Information of all types – word processing documents, PDF (Portable Document Format) document, spreadsheets, presentations, digital images, even sound and digital movies must be securely handled.

  Once the information is deposited into the system, only intended recipients are allowed to view the information. The Identity of the person who places the information into the system as well as audit trails should be recorded for every visit to the document. Nowadays, various technologies are used to prevent the information from leaking to unintended parties.

- **Availability of documents**

  Availability is about ensuring that the digital document is made available to authorised users when required. Without proper management, documents could be lost due to unintentional errors. For businesses, not

being able to access a document may cause a company to not function effectively, thus causing a lower return on investment and missed business opportunities.

Possible solutions to these problems include:

- **Digital signature**

  The combination of encrypted hash total and sender's private key represent the sender's digital signature, which is attached to the original document. The recipient then runs the document through the hash function algorithm and the sender's public key to see whether that same total is still generated to verify that the document is intact. These complex calculations are invisible to users, who simply click an icon to sign a document.

  A digital signature can only be forged if the criminal has obtained the target's private encryption key. Furthermore, digital signatures, as explained, can be used to verify that the message has not been altered en route. Therefore, digital signatures have gained wide support in electronic commerce transactions.

  Uncertainty as to the legal status of digital signatures can be an obstacle to electronic commerce, since it makes the legal consequences of commercial activities over electronic networks unpredictable. Therefore, digital signature legislation, regulations, and guidelines have been formulated by several countries and international organisations. In Malaysia, digital signature technology has to be in compliance with the Digital Signature Act of 1997.

- **time stamping server**

  Time-stamping server is a service that enables Internet transactions, electronic documents or signatures be signed with trusted time. Recorded time is provided by a centralized stamping server. This is to provide undeniable proof that digital data were not modified or backdated. Time-stamping provides strong protection to a digital document by ensuring non-repudiation characteristic of the document.

- **Hardened operating system**

  Terminals with hardened operating system (hardened PC) prevent unauthorized copying of files from the terminals through USB drive, floppy disk, CD, network etc.

- **Three factor authentication**

  A three factor authentication using smart card activation password, smart card with digital certificate and fingerprint biometric provide a state-of-the-art authentication mechanism that is superior to conventional username-

password login to computer terminal. This method of protection ascertains what you have, what you know, who you are. In other words, it ascertains the token one has, such as smartcard, the password one keys in, and one's fingerprint or iris scan. All these will ascertain one's identity – who you claim you are.

- **Digital Watermarking**

  Digital watermarking can be embedded as an additional security feature to enhance the security of documents. While digital signature technology securing the transmission of document, digital watermarking technology controls the distribution of document by providing ownership rights protection, authentication (both visible and non-visible), various information access control (e.g. print, save, view) and information tracking. Digital watermarking technology can be applied to video, picture and audio.

CONCLUSION

It is imperative that organisations provide some security features and interactive authorisation systems to meet the rising security demands of documents transferred over the Internet. This will enhance data security measures, protecting how data is communicated and identifying and securing the system at the user's terminal.

The most important consideration is that all organisations must embrace a solution that fits easily into the existing workplace rhythm. An organisation should have secure transmission and control of digital information by using one or more of the above solutions.

ACKNOWLEDGEMENT

The authors would like to thank Mr Ng Kang Siong of MIMOS Berhad who has given valuable inputs to this article.