HKU203
07/12/02

亞洲商業案例中心
Centre for Asian Business Cases
School of Business, The University of Hong Kong

Digital Certificates and Signatures: Microsoft Corporation

On 22 March, 2001, the Microsoft Corporation warned computer users that an individual posing electronically as a company representative had fooled VeriSign Inc., the leading digital certificate authority, into issuing two fraudulent electronic certificates in Microsoft's name. The certificates were issued on 29 January and 30 January, 2001. Despite the discovery of the fraud and the follow-up investigation by the FBI, the identity of the person who had registered the certificates remained unknown. The flawed certificates in the Microsoft case were used to prove the origin and authenticity of software programmes and data on the Internet, a key requirement for users who downloaded patches or software updates. Similar certificates issued by companies such as VeriSign were also used in creating secure Internet transactions with commercial Websites, sending secure and authentic e-mail, and in related applications.

The accident posed a great risk to computer users and could have affected all users of Microsoft's operating systems, ranging from Windows 95 to Windows 2000. An attacker armed with such certificates could produce digitally signed code and appear to be an official representative of Microsoft Corporation. In this scenario, the party could potentially host a malicious programme on a Website and then try to deceive users into installing and running the software. This meant that unsuspecting users who thought they were downloading an update of Internet Explorer or some other Microsoft software – from a site not affiliated with Microsoft – could end up with a destructive programme that could trash their hard drive or give hackers access to their entire network. The attacker could also choose to package the malicious code as an ActiveX control (an Office document with macros or other executable content) and send it to users by e-mail.

The Microsoft case was the world's first reported case of digital certificate fraud.[1] It raised serious questions about CA's practices in issuing digital certificates. Class 3 certificates, the kind that were given out to software publishers and developers, were supposed to be issued only after the most stringent measures had been applied to ensure that the identity of the applicant was valid.[2] Obviously, something had broken down in VeriSign's technical control and screening procedures.

[1] Palfreyman, J., "How to ensure e-security for e-biz", *The Business Times Singapore*, 6 August, 2001.

[2] Certificate Authorities usually offer a range of digital certificates, graded according to the level of inquiry used to confirm the identity of the subject of the certificate.

Mary Ho prepared this case under the supervision of Dr. Ali Farhoomand for class discussion. This case is not intended to show effective or ineffective handling of decision or business processes.

This case is part of a project funded by a teaching development grant from the University Grants Committee (UGC) of Hong Kong.

Ref. 02/139C 12 July, 2002

Officials of VeriSign took responsibility for issuing the certificates via an automatic Internet-based system. Mahi deSilva, Vice President and General Manger of the company, blamed the accident on human error and claimed the company's automated and manual process for examining certificate applications and identifying individuals who submitted them had held up. VeriSign cancelled the certificates on 9 March and 12 March, 2002, but could not be certain as to whether the false certificates had been used. Whilst details of the revoked certificates were included in VeriSign's Certification Revocation List, the list could not be downloaded automatically by web browsers. This forced Microsoft to develop an operating system update with information about revoked certificates.

The incident highlighted the tricky nature of ensuring trust on the Internet and the sophistication of digital certificates. Consumers did not know, when they were trusting Microsoft, that they were in fact relying on VeriSign's certification policies and procedures. Yet digital certificates issued by VeriSign could not provide absolute proof of identity. This means that similar e-business transactions that are conducted and secured by electronic certificates are also vulnerable to such a security flaw [see **Example 1**].

Example 1

Company A entered into an on-line business arrangement whereby it performed a service for a company that held a digital certificate of Company B. The digital certificate that Company A relied on was an erroneous certificate but the certificate authority failed to detect it. When Company A later attempted to enforce its electronic contract and collect from the real Company B, it found that it had become a victim of fraud. Should the certificate authority be liable in contract for its acts and omissions? Given that the certificate authority did not have a contract with Company A, what remedies were available to Company A?

The situation could be further complicated if the participants lived in different jurisdictions, as it would often be unclear which jurisdiction's laws would apply. Under the Utah Act, a digital certificate subscriber defrauded by a criminal could be liable for the loss caused by a forgery [see **Example 2**].[3]

Example 2

LCA, a licensed certification authority, duly issued a certificate to Kenny. LCA published the certificate in a recognised repository. Kenny's private key, which corresponded to the public key in the certificate, was kept on his computer's hard disk. Bob, a computer hacker, released a computer virus on the Internet that allowed Bob to gain access into Kenny's computer. Subsequently, when Kenny used his private key, the virus programme sent a copy of Kenny's private key to Bob. Bob immediately used the private key to cash an electronic check drawn upon Kenny's account payable to an anonymous account in a state having rigorous bank secrecy laws. Bob disappeared and could not be found. As soon as Kenny discovered the fraud, he revoked his certificate.

Under the Utah Digital Signature Act, Kenny would be liable for the loss caused by the forgery if he failed to exercise reasonable care in protecting his private key. Thus Kenny would have to obtain the services of an attorney and go to court. He would have to overcome the presumption that the electronic check signed with his digital signature was valid and binding upon him, and he would have to prove that in fact he did not affix the digital signature in question. Furthermore, he would have to show that he did not breach his duty of care in allowing Bob, the criminal, to obtain his private key. Under this Act, a digital certificate subscriber might have to bear an immense amount of risk.

[3] Biddle, C. B., Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure, 18 October, 1996.

How could Microsoft and general subscribers protect themselves against the potential threat posed by these fraudulently acquired certificates or signatures? What possible remedies were available to those who relied on them in electronic transactions? What action could CAs take and how could legislators regulate the conduct of CAs, subscribers and relying parties?