PKI: A Question of Trust and Value

On March 22, 2001, Microsoft issued a security bulletin (MS01–017) alerting the Internet community that two digital certificates were issued in Microsoft’s name by VeriSign (the largest digital certificate company) to an individual—an imposter—not associated with Microsoft. Instantaneously, VeriSign (a self-proclaimed “Internet trust company”) and the entire concept of Public Key Infrastructure (PKI) and digital certificates—an industry and service based on implicit trust—became the focus of an incident seriously undermining its level of trustworthiness. This incident also challenges the overall value of digital certificates.

In theory, certificates are worthwhile to both businesses and consumers by providing a measure of confidence regarding whom they are dealing with. For example, consumers entering a bricks-and-mortar business can look around at the condition of the store, the people working there, and the merchandise offered. As desired, they can research various business references to determine the reliability and legitimacy of the business. Depending on the findings, they decide whether or not to shop there. However, with an Internet-based business, there is no easy way to determine with whom one is considering doing business. The Internet business may be a familiar name (from the “real” business world) and an Internet consumer might take comfort from that and enter into an electronic relationship with that site. Without a means to transparently verify the identity of a given Web site (through digital certificates), how will they really know with whom they are dealing?

Recall the incident involving Microsoft. Potentially, the erroneously issued certificates were worth a considerable amount of money should their holders have attempted to distribute digitally signed software purporting to be legitimate products from Microsoft. In fact, these certificates were worth much more than the “authentic” certificates issued to Microsoft because (as mentioned earlier) end users do not have the ability to independently verify the validity of certificates. Since users can’t verify the validity of certificates—legitimate or otherwise—the genuine Microsoft certificates are essentially worthless.

In “Risks of PKI: Secure Email” (“Inside Risks,” Jan. 2000), cryptanalysts Bruce Schneier and Carl Ellison note that certificates are an attractive business model with significant income potential, but that much of the public information regarding PKI’s vaunted benefits is developed (and subsequently hawked) by the PKI vendors. Thus, they are skeptical of the usefulness and true security of certificates.

As a result of how PKI is currently marketed and implemented, the only value of digital certificates today is for the PKI vendor who is paid real money when certificates are issued. For the concept of certificates to have real value for both purchaser and end user, there must be real-time, every-time, confirmation that the presented certificate is valid, similar to how credit cards are authorized in retail stores. Unless a certificate can be verified during each and every use, its value and trustworthiness is significantly reduced.

In the real world, when submitted for a purchase, credit cards are subjected to at least six steps of verification, including: when the Point of Sale (POS) terminal contacts the credit-card issuer, the issuer verifies the POS terminal belongs to an authorized merchant; when the customer’s card information is transmitted, the issuer verifies the card number is valid, active, and the card balance is not over the approved limit; and, the merchant, after receiving an approval for the transaction by the credit-card company, usually (but not always) verifies the customer’s signature on the receipt matches the signature on the card.

The Schneier-Ellison article and recent real-world events demonstrate that a system of robust, mutual and automatic authentication, checks-and-balances, and active, ongoing cross-checks between all parties involved is necessary before PKI can be considered a secure or “trusted” concept of identification. Without such features, certificates simply become a few bits of data with absolutely no value to anyone but the PKI vendor.

Without effective revisions to the current process of generating and authenticating new and existing certificate holders, the concept of PKI as a tool providing “Internet trust” will continue to be a whiz-bang media buzzword, full of the sound and fury of marketing dollars, but, in reality, securing nothing.