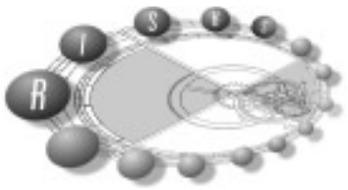

Risks in Email Security

It is easy to create bogus email with someone else's email name and address: SMTP servers don't check sender authenticity. Secure/Multipurpose Internet Mail Extensions (S/MIME) can help, as can digital signatures and globally-known trustworthy certification authorities (CAs) that issue certificates. The recipient's email software verifies the sender's certificate to determine his or her public key, which is then used to verify email signed by the sender. In order to trust the legitimacy of the email signatures, the recipient must trust the CA's certificate-issuance procedures. There are three classes of certificates. The certificate classes and issuance procedures are more or less the same for all CA companies that directly issue certificates to individuals. Verisign, Globalsign, and Thawte are examples of such CA companies.

Class-1 certificates have online processes for enrollment application and certificate retrieval. There is no real identity check, and it is possible to use a bogus name—but the PIN sent by email to complete the application at least connects the applicant to an email address.

Class-2 certificates are more secure than class-1. CAs issue class-2s after some online and offline controls. They automatically check applicant's identity and address against the database of a third party, such as a credit-card company or DMV. As Schneier and Ellison note in their column "Risks of PKI: Secure Email" (*Communications*, Jan. 2000, p. 160), it is possible to create fake certificates using this online method simply by private information theft. In order to reduce the likelihood of impersonation, CAs use a postal service for identity verification and/or confirmation.

Class-3 certificates require in-person presence for strong identity control prior to issuance by CAs, so they are even more secure.

As usually used in S/MIME, class-1 certificates can mislead users. The recipient's email program verifies the signature over a signed message using the sender's class-1 certificate. Because the information in the message and in certificate match, the client program would accept the signature as valid, but taking the sender's word. With a dishonest sender, the spurious verification is garbage-in, gospel-out. The only seeming assurance the signature gives is that the message might have been sent by a person who has access to the email address specified in the message, but this fact isn't clearly specified by the email programs. An average user thinks a class-1 certificate provides identity verification, which is not true. This is neither a bug nor a one-time security flaw. It is exactly how the system works.

CA companies are, of course, aware of this, and put appropriate disclaimers within their Certificate Practice Statements (CPS) and class-1 certificates. However, such disclaimers must be read and interpreted by the verifiers. Who would spend time reading these details when the email program says that the message has been signed?

Some CA companies, like Globalsign, don't include the certificate holder's name in class-1 certificates. This is good approach, but not sufficient. A message signed by such a class-1 certificate would also be verified by the email programs. People who don't read the disclaimers also won't read a lack-of-identification notice. Worse, this lets a sender use the same certificate to impersonate multiple persons.

If you receive an email message without a signature, you might be wary—but are likely to take a signed message at face value. Class-1 certificates, in this respect, provide vulnerability in the name of security.

The verifier should check the level of assurance given in a certificate. Perhaps email programs should be designed to help verifiers by giving clear and direct warnings specifying the exact level of identity validation associated with the certificate. If a class-1 certificate is used, the program should display a box saying that sender's identity hasn't been validated.

Certificate holders as well as verifiers must be aware of the fact that class-1 certificates don't certify real identities. Class-3 certificates must be used for this.

Class-3 certificates have a good level of identity check for personal authentication, but CA companies should still promote class-1 and class-2 certificates for the users who need the convenience of online processing. Refusing to provide them would lose the CAs too many customers. We believe that class-1 certificates will gradually disappear as certificate use reaches maturity and as people become more conscious of the limitations of class-1 certificates. C

MARTIN MAYO

ALBERT LEVI (levi@ece.orst.edu) is a postdoctoral research associate and **ÇETIN KAYA KOÇ** (koc@ece.orst.edu) is a professor of Electrical and Computer Engineering at Oregon State University.