

Digital Signatures: Use Them, Protect Them

Imagine the future, when we all habitually sign digital documents. How might this work? Alice (a hypothetical computer user) will write a digital document in some application—a word processor, an email program, or whatever—an click on an icon to indicate that she is ready to digitally sign the document. Alice types in her password (or passphrase) and follows the procedures required to prove to the computer that she is Alice, and not an imposter. The signature software will calculate the digital signature for the document, and hands over the digital signature to the original application, where it is attached to the document.

This is now the law. U.S. law grants digital signatures the same legal weight as handwritten signatures. Electronic contracts are as binding in court as paper contracts.

And unless we understand how this technology works and what steps we must follow to protect our digital signatures, Alice may not be the only person signing her name. And you may not be the only person digitally signing yours.

When first invented in the 1970s, digital signatures held amazing promise: better than a handwritten signature, unforgeable and uncopiable. Today, they are a fundamental part of business in cyberspace, and numerous state laws have codified their authority. On June 30, President Clinton signed the Electronic Signatures in Global and National Commerce Act (E-Sign Act).

But unless digital signatures are implemented correctly (and safely), we risk losing our privacy and possibly being forced to refute our own signatures in court.

The math behind encryption and digital signatures is complex, but the mechanics are simple. A user—Alice—has a secret code, called a private key. Using that private key, Alice can create a special "checksum," a digital fingerprint, that anyone can verify (using her public key, which she freely distributes. We call that checksum a digital signature. The digital signature can be electronically attached to an email message, a word processor document, a spreadsheet, practically any type of electronic file.

In law, our signatures indicate we agree with or accept the contents of a document, or at least acknowledgment that the document has been read.

When a judge sees a paper document that Alice or someone else testifies that she signed, he knows that she held the document in her hands, and he has reason to believe that Alice read and agreed to the words on the document. The signature provides evidence of Alice's intentions.

However, if an evil third party, let's call her Eve, gains access to Alice's private key, she may be able to affix Alice's digital signature to documents without Alice's even being aware of the crime.

To effectively use digital signatures, such as those created by Network Associate's Pretty Good Privacy, the industry standard for file encryption and digital signatures, users must protect their private keys. Store them on CDs, not on the computer's hard disk. Insert the private key CD only when signing or encrypting a file. Remove it and store it safely when not in use.

Storing it on your hard disk is only a challenge to dishonest coworkers and competitors to crack into your computer (through the Internet or via your keyboard) and steal or copy your private key.

Mathematics, the basis of all cryptologic ciphers, cannot bridge the gap between computers and humans. The real world is one of systems, not math. This system involves an untrusted computer running untrusted software. Even if the whole system is verified, it becomes untrusted once Alice does something as simple as leave her private key CD sitting unattended on her desk.

Imagine Alice in court, answering questions about that surprising document. She says, "I never saw it. Yes, the mathematics shows that my private key signed the document, but I didn't." The judge calls an expert witness like me to the stand who explains that it is possible that Alice never saw the document; rogue programs can sign documents without Alice's knowledge, and mathematics says nothing about intent. It all comes down to whether you believe Alice.

Digital signatures prove only that a private key was present in a computer when Alice's signature was created. It doesn't prove that she intended to sign a particular document.

The text of this newsletter is excerpted from recent articles by Bruce Schneier, author of Secrets & Lies: Digital Security in a Networked World.