Firm looks to fight forgery by fingerprinting' papers

By Simson L. Garfinkel
SPECIAL TO THE GLOBE

First there were human fingerprints. Then there were DNA fingerprints. Now a firm in New Jersey has commercialized a system for electronic fingerprints. Only instead of fingerprinting people, the company wants to "fingerprint" your electronic documents.

"A digital time bomb is ticking away within the halls of corporate America," said Dr. W. Scott Stornetta, chairman of Surety Technologies,, based in Chatham, N.J., who warns that if we don't fingerprint our documents, thieves and forgers will change our digital past without leaving a trace.

The problem, it seems, is that computers are too good at making corrections. If you write your name on a piece of paper, then change your mind and try to write someone else's, you are sure to leave a mark. Even if you write in pencil, you are bound to leave smudges, microscopic rips in the paper, and dents. On the other hand, if you edit a file with a word processor, there is simply no way that you can tell that one person's name has been crossed out and replaced with another's.

That can be a real problem if the file being edited is someone's last will and testament, or instructions in somebody's medical file. AB more and more businesses keep the only copies of their records on computer, those records are likely to be the subject of forgery more and more often.

One low-tech way of dealing with the problem is to simply print out each electronic document, have die pages notarized, and put them into a safe-deposit box. But that approach would surely be unworkable in the corporate or medical fields.

A new technique was developed four years ago at Bellcore, the research arm of the regional Bell operating companies. The system, invented by Stornetta and Dr. Stuart Haber, is based on a kind of electronic fingerprint called a hash function. Their system, called The Digital Notary, is now open for business on the Internet.

Here's how the Digital Notary works: To electronically notarize a document, a piece of software on your computer calculates the digital fingerprint and sends that fingerprint to a special computer at Surety Technologies. At Surety, your document's fingerprint is mathematically combined with the current date and time, and the resulting block of data is itself fingerprinted and sent back to you. Your computer then affixes the time certificate to the bottom of the document

Back at Surety, the fingerprint and time is recorded in a master database, which is updated once a second. If two or more fingerprint requests are received during the same second, those fingerprints are electronically combined into a "super" fingerprint called a Universal Validation Record.

And just to keep everybody honest, the company publishes a special super validation record for every fingerprint issued during the week in The New York Times. Surety may also produce CD-ROMs containing all of the validation records issued during the year.

There is no way that the time certificate can prevent somebody in the future from modifying the contents of the electronic document. But the certificate will tell you if the document has been modified. If just one letter in the electronic document is changed, the resulting document won't have the same digital fingerprint And since the time certificate contains the date and time that the certificate was issued, it is possible to prove that the electronic document existed in its exact form on a particular date.

"I think that this is really valuable, as long as it is priced reasonably," said David P. Pollak, an attorney and the president of Athena Design, a Boston-based company that sells financial software. "It is something that I would recommend to my clients. And if it were inexpensive enough, we would probably adopt it here,"

Surety's first product, the Digital Notary Personal Edition, is a program for Windows-based computers that can notarize electronic documents over the Internet The system is secure, since only the document's fingerprint, rather than the entire document, travels through the network. The program costs $49, a price which includes the user's first 75 certificates.

But Surety isn't planning sell many copies of its software. Instead, Surety hopes to sell companies its Enterprise Server, a system that will allow organizations to do their own time-stamping. Companies can then program their servers to synchronize with the Surety master server once a day, once an hour, or even more frequently.