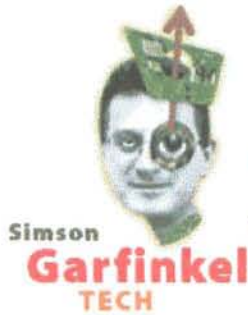


PACKET

9 oct 96



False Sense of Security

Why digital IDs won't make the Net a safer place.

Last week, I wrote of the wonders of digital signatures and [VeriSign](#), a company that has received great publicity for its electronic "driver's license" for cyberspace. This week, I'll show you why it pays to read between the lines, and why the currently available digital IDs might create as many problems as they solve.

The first problem with the digital IDs that VeriSign is giving away, as well as those that the company hopes to sell, is that they don't have enough information on them to be truly useful. Sites that distribute pornography might want to use digital IDs to see if their customers are over 21, but they can't because, unlike a driver's license, VeriSign's Digital ID doesn't specify age. Sites that would like to have "women-only space" on the Net can't, because VeriSign's Digital IDs don't specify gender. They don't even have your photograph or [fingerprint](#), which makes it almost impossible to do business with somebody over the Internet and then have them show up at your office and prove that they are the same person.



Of course, if VeriSign's digital ID did have fields for your age, gender, or photograph, netizens would say that the IDs are a violation of privacy. And they would be right. That's the whole point of an identification card: to remove privacy and anonymity, producing identity and accountability as a result. That's why Social Security cards have the words "not to be used for identification" printed on them. Without personally identifying characteristics, there's no way to perform identification.

Indeed, VeriSign's digital IDs don't identify people at all - they identify secret keys. But there is no proof that a digital John Hancock belongs to the person that VeriSign thinks it does.

Leaving aside VeriSign's Class One certificates, which don't identify anything but email addresses, VeriSign says that it goes to great lengths to be sure that people applying for certificates are in fact the people they claim to be. But a day later, how do you guarantee that I am the only person who has my secret key? For that matter, how do you guarantee that the key was randomly generated in the first place? The security of digital signatures depends on the security of cryptographic keys. Just how secure can these keys be?

But there is no proof that a digital John Hancock belongs to the person that VeriSign thinks it does.

VeriSign doesn't have answers to these questions. The closest the company comes, in its [Certification Practices Statement](#), is this: "[E]ach certificate applicant shall securely generate his, her, or its own private key, using a

Add your
safe-surfing
strategies
in [Threads](#).

The latest
post to Tech is
"Nortel's Entrust"
by Simson L. Garfinkel
(simsong)

PacketChat:
[Chat here](#).

[Subscribe to
PacketFlash,](#)
for Packet news.

trustworthy system, and take necessary precautions to prevent its compromise, loss, disclosure, modification, or unauthorized use."

Unfortunately, this technique - system engineering by fiat - simply doesn't solve the underlying computer security problems inherent in nearly all computer systems today. Today's computers aren't trustworthy, because they can't prevent the intentional modification of programs by other programs. A simple computer virus or other rogue program could search your computer's hard drive for your copy of Netscape Navigator and modify the random number generator so that it always returned one of a million possible values. Sure, your public key would *look* uncrackable, but anybody who knew about the virus would be able to forge your digital signature in no time.

Your computer is no better at storing your secret key once it's been generated. Even though both Navigator and Internet Explorer can store your keys encrypted, they have to be *decrypted* in order to be used. All an attacker has to do is write an ActiveX component that hangs around, waits for the key to be decrypted, and then sends it out over the network. And don't think that those ActiveX log files will help you figure out who is to blame: They're just as vulnerable.

Don't blame VeriSign for this mess: Blame Apple, Microsoft, and the other vendors of these PC operating systems. "We do not, and cannot, control or monitor the end-users' computer systems," says VeriSign's president Stratton Sclavos. "In the absence of implementing high-end PC cards for all subscribers, or controlling or participating in key generation, the storage of end-user keys is fully within the control of end users."

In other words, Stratton probably realizes that every time somebody downloads a digital ID from VeriSign, they're violating the company's license agreement - to keep it on a "trustworthy machine" - by doing so.



Geek
This

One thing that VeriSign has started doing right, though, is assuming liability for its digital IDs. Starting on 22 August 1996, with the publishing of its new Certification Practice Statement, the company has placed a liability cap of US\$100 for each Class One certificate, \$5,000 for each Class Two certificate, and \$100,000 for each Class Three certificate. This doesn't mean that VeriSign is giving users a \$100,000 insurance policy against the theft of their secret keys. What it really means is that if VeriSign doesn't follow its stated policies, there is a greater chance of winning a cash settlement against the company in court. Compare that with the disclaimers that haunt today's shrink-wrapped software.

[Michael Froomkin](#), a professor at the University of Miami Law School, has written an [extensive article](#) on the subject of liability for certificate authorities such as VeriSign. One of the biggest problems, Froomkin says, is that a fraudulent key can be used over and over to defraud thousands or millions of individuals worldwide. Unfortunately, VeriSign says that its liability caps are *per certificate*, rather than per transaction. A system like that can only work, Froomkin believes, if there is some way to limit the number of transactions that you can perform with a certificate within a given time period. Currently, there are no plans to do so.

To make things worse, in some states - such as New York - a victim of a fraudulent certificate can't even sue VeriSign, because the victim and VeriSign never entered into a legal contract with one another. New laws will be required to give third-party victims standing in court. So far, Utah and Washington are the only two states to adopt such legislation.

On the other hand, digital IDs are great for enforcing policy, especially when that policy runs counter to the interests of users. Back in the 1980s, Atari used digital signatures to prevent unauthorized games from running on their home videogame systems. Today Microsoft is using similar technology as part of its Cryptography API: You can't load an encryption engine into Windows 95 or Windows NT unless that engine has been specially signed by Microsoft's corporate key. The reason for this restriction, says the company, is the Clinton administration: Microsoft couldn't have gotten export permission for its operating systems if users could easily plug in crypto engines that hadn't been approved.

Simson

Talk back to Simson Garfinkel in his column's [Threads](#).

Illustration by Dave Plunkert



Surfing as [simsong](#).
Change your [preferences](#).

Previously in [Garfinkel](#) ...



[Copyright](#) © 1996 HotWired, Inc. All rights reserved.