PACKET

License to Surf

Digital IDs purport to separate the good guys from the criminals. But they're no panacea.

Do you have your free digital ID yet? They're all the rage. And these days, it's getting harder and harder to find an Internet-aware publication that isn't extolling the virtues of these new identity cards for cyberspace.

Digital IDs are those trendy, trademarked electronic identification certificates being issued by VeriSign, an Internet start-up that's received rave reviews throughout Silicon Valley. Digital IDs are being trumpeted as God's gift to the Internet. In one fell swoop, digital IDs are supposed to eliminate credit fraud, theft of identity, computer viruses, and more.

Digital IDs are based on the RSA public-key encryption algorithm. That's the same algorithm at the heart of things like Phil Zimmermann's Pretty Good Privacy (PGP) program and Netscape's secure socket layer (SSL). To use the RSA algorithm, you create a public key and a secret key. Anything encrypted with the public key can be decrypted with the secret key, and vice versa. So I can send you a secret message by first encrypting it with your public key - and only you can read it.

In one fell swoop, digital IDs are supposed to eliminate credit fraud, theft of identity, computer viruses, and more.

Although the RSA technology works like gangbusters in practice, there's always been a nagging problem. How does somebody know that the remote site's key really belongs to them, and not to somebody else?

Geek This

That's where the digital ID comes in. In addition to sending somebody your public key, the remote site also sends you a signed digital certificate. The certificate contains your key, your "distinguished name," and a digital signature that's signed with one of VeriSign's master keys. VeriSign's keys are distributed far and wide - they're actually built

R U a safe surfer?

Speak up
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.

into every copy of Netscape Navigator and Internet Explorer that's ever shipped. All your friend at the other end of the Internet has to do is verify VeriSign's signature on your public key, which is a simple mathematical operation, and then they know what your name really is. Simply put, the digital ID proves that you are who you claim to be.

VeriSign is now selling its digital IDs to consumers as well. Actually, VeriSign has four kinds of digital IDs. The company's Class One ID doesn't really identify people at all. It simply contains a copy of your distinguished name - whatever name you provide - and an optional email address. It's these Class One IDs that VeriSign is giving away.

Pay US$12 a year and you can get a VeriSign Class Two ID. With these IDs, VeriSign contacts a credit-reporting agency, verifies your address, then sends you a postcard in the mail to verify that you are who you claim to be. It's not the greatest security, but hey, its what the credit-card companies use. Pay $24 and you can get a Class Three ID, which requires you to present a notarized document attesting to your name. There is also a Class Four ID, but the details haven't yet been announced.

Digital IDs have scads of uses. If you get somebody's public key, which you can get from the VeriSign digital ID site, you can send them encrypted mail. Well, you can't do it right now, but you'll be able to once Netscape starts shipping the beta of Netscape Navigator 4.0, which will include built-in support for Secure MIME. A future version of PGP may support S/MIME as well.

You can use your digital ID and your matching secret key to sign a program that you distribute on the Web. Since you are the only person in the world that has your secret key, this is a way to prove the authorship of your software. Already, Microsoft's Internet Explorer will warn users when they download programs that haven't been signed. And with good reason: An unsigned program might contain a virus, or might be a piece of malicious software that could reformat your hard disk. Of course, a signed program can do that as well, but the idea is that at least the victim will know who to blame - or who to sue.

But most people will use their digital IDs to identify themselves at Web sites. Digital IDs will eliminate usernames and passwords. Instead, you'll just sign your name with your secret key and flash your digital ID to gain admittance. Once again, Navigator 3.0 and IE 3.0 do this automatically.

People who charge money for access to Web-based content are going to go nuts over this technology. That's because while a few dozen guys might get together and share a single username and password for a cybersex site, there is no way that any of these clowns will let the others share his digital ID's secret key, which will also unlock his bank account and credit cards.

What's holding back digital IDs right now is server technology. Even though a quarter of a million people have created digital IDs, with 5,000 more going out VeriSign's door every day, there are only a half dozen or so sites on the Internet that are accepting the identification bits, according to VeriSign president Stratton Sclavos. One reason: In order for a Web site to accept them, that site has got to be running a state-of-the-art SSL 3.0 Web server, like the Netscape Enterprise Server 2.0 or the Apache SSL version 1.3 from Community ConneXion. It's only these modern servers that have the necessary smarts to ask a Web browser for its digital ID, read it back, and verify it.

But there's a deeper, more insidious problem with digital IDs. I'll tell you about it next week.

Simson

Talk back to Simson Garfinkel in his column's Threads.

Illustration by Dave Plunkert

webmonkey SURF CENTRAL

Surfing as simsong. Change your preferences.

Previously in Garfinkel ...

Current Garfinkel
Archive Index for Garfinkel

HOME SEARCH HELP