Microsoft Authenticode analyzed

Rohit Khare (*khare@pest.w3.org*)
Mon, 22 Jul 96 17:52:07 -0400

- **Messages sorted by:** [date][thread][subject][author]
- **Next message:** Rohit Khare: "Andreesen moving sloooowly to objects"
- **Previous message:** Rohit Khare: "Tim's comments on W3C appear in PCWeek"

[private w3c editorial comments expurgated]

July 22, 1996 10:00 AM ET
IE 3.0 applets will earn certification
By _Norvin Leach_ and _Michael Moeller_

In preparation for the mid-August launch of Internet Explorer 3.0, Microsoft Corp. next week will announce tools and services that let vendors digitally sign ActiveX, Java and Netscape Communications Corp. plug-in components.

As a result, users of Internet Explorer 3.0 will be able to identify the creator of an Internet-based applet before downloading it.

But for some IS managers, this approach misses the point of Internet security by a long shot. Many say they are less interested in knowing who built a component than in providing seamless protection for users, as the Java "sandbox" model does.

The Microsoft model, designed to provide users with the same level of security found in shrink-wrapped software, is based primarily on a level of trust and market pressure to keep ISVs honest.

To put the digital signature architecture in place, VeriSign Inc. and, in the future, other certificate authorities will issue digital certificates to ISVs for a $20 fee. Several hundred ActiveX controls will be digitally signed by the time Internet Explorer 3.0 ships, sources said.

But such a certificate does not authenticate the specific applet--it only certifies that the vendor has pledged not to build any malicious code into its software. "If a user downloads a buggy piece of signed code, then he will never go back to that vendor again," said Rob Price, group product manager for

Internet security at Microsoft.

Beyond the credibility aspect, the signature concept raises a broader issue for some IS managers.

"Just the fact that they have to create this kind of workaround causes me concern," said Eric Goldreich, information manager with Sheppard, Mullin, Richter & Hampton, a Los Angeles law firm.

Other IS managers are worried that digital signatures may add complexity to an already complicated method of trying to manage who downloads what from the Internet.

Internet Explorer 3.0 will modify a user's system files to detect digital certificates as components are downloaded. Once found, a dialog box will appear, stating where the component came from and asking if users want to continue downloading the component.

System administrations will be able to restrict users from downloading any components, and users will be able to list "trusted" companies that can load components onto their client machine without confirmation.

Security "should be something the end user isn't aware of," said Erik Goldoff, computer specialist for the Centers for Disease Control, in Atlanta. "End users don't even understand Internet busy signals today."

The issue of component security has not been widely discussed because the technology is only beginning to mature; Internet Explorer 3.0 is the first browser to apply the digital signature approach.

Two Microsoft competitors, Netscape and Sun Microsystems Inc., are adding digital signature schemes as a means of extending the functionality of software and components found on the Internet. However, officials at both companies believe digital signatures alone perpetuate a flawed model found in shrink-wrapped software.

"Digital signatures are just a part of the answer, not the whole solution," said Jeff Treuhaft, director of security at Netscape, of Mountain View, Calif. "Besides, you need to sign the code, not the vendor."

- **Next message:** Rohit Khare: "Andreesen moving sloooowly to objects"
- **Previous message:** Rohit Khare: "Tim's comments on W3C appear in PCWeek"