WIRED

GO

SEARCH

enter email

GO

S/MIME Cracked by a Screensaver

by Simson Garfinkel

4:59am 26.Sep.97.PDT Cracking encrypted email just got much easier - as long as the message was encrypted with Netscape Navigator or Microsoft's Outlook Express.

Bruce Schneier, a cryptography consultant based in Minnesota, has created a Windows 95 screensaver that cracks encrypted email messages on computers that are otherwise unused. "On average, it takes 35 days on a 166 MHz Pentium," said Schneier, who is also the author of the book *Applied Cryptography*.

The real power of Schneier's program is that it's designed to work on multiple machines in parallel over a local-area network. Got an office with a dozen machines? You can crack a message in a little less than three days. Got a thousand? Your wait will be just 50 minutes. The program, which began as a screensaver that searched for large prime numbers, will be made available on Schneier's Web site today.

The program will only crack messages encrypted with RSA Data Security's S/MIME mail encryption standard, and at that, only messages that are encrypted with a 40-bit key. But that's exactly the encryption that's being offered today by the most commonly used versions of Netscape Messenger and Microsoft Outlook Express.

"What really pisses me off is that [these products] are being marketed as secure," said Schneier. "The products don't say that they use 40-bit encryption - be careful. They say this is security."

The S/MIME standard implemented by Netscape and Microsoft does provide for higher-level security by using different encryption algorithms. But Schneier maintains that messages encrypted with these stronger algorithms cannot be exchanged between the two vendors' products. "The S/MIME security standard is really hard to work with," said Schneier. "None of [the products] interoperate at any level other than 40-bit RC2."

Schneier says he's releasing his program to demonstrate the fundamental vulnerabilities in the S/MIME standard. But S/MIME's maker disagrees, saying there is no problem using longer keys.

"Bruce is mistaken," said Scott Schnell, vice president of marketing for RSA Data Security, the co-author of the S/MIME specification. "We have mail messages on file in our interoperability test lab which demonstrate interpretability between Outlook Express and Netscape's Messenger using triple-DES," which has a 168-bit key.

Related Wired Links:

RSA Creates Email Standards Battle

S/MIME Cracked by a Screensaver

TECHNOLOGY
Today's Headlines

Tilling the Tech for Better Tractors

Orbital Launches into Competition

Intel Weeds Pixels and Makes the Web Scream

S/MIME Cracked by a Screensaver

ISP Goes Wireless

Street Cred: DVD on Trial

Geek Talk: Java-Enabling, Border-Removing