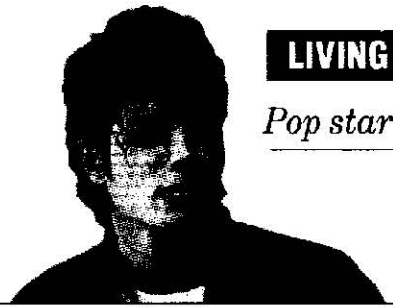
GARDEN

HOW TO BE A WEED WHACKER

*Getting rid of them/***1E**



LIVING

AND NOW, JACKSON ON-LINE

*Pop star takes spin control another step: to cyberspace/***1C**

NEWS

WILLIAM FLOYD INJURED

*Niners fullback could be out three weeks/***1G**

San Jose Mercury News

MORNING FINAL
35 CENTS

Serving Northern California Since 1851

THURSDAY
.. AUGUST 17, 1995

Netscape security encryption is cracked

Breach spurs concern for commerce on Internet

BY SIMSON L. GARFINKEL
Special to the Mercury News

The built-in security features that are one of the major attractions of Netscape Communications Inc.'s World Wide Web "browser" software aren't nearly as secure as people might believe, a French researcher has proven — a chilling thought for companies aiming to do business in cyberspace.

Using a networked collection of 120 computers, including two supercomputers, Damien Doligez, of the French National Institute for Research in Computer Science and Control in Le Chesnay, France, was able to read a supposedly secure Internet message that had been sent using Netscape's popular Navigator program.

The vast majority of Internet sessions that use Netscape's software are not encrypted; indeed, the whole point of networks like the World Wide Web is to allow for the free exchange of information.

But a key marketing point for

See NETSCAPE, Back Page

Netscape security breach blamed on U.S. encryption export rules

■ NETSCAPE

from Page 1A

Netscape has been that in addition, its software will also allow for secure communications, the sort that will be needed before the Internet — with its reputation for eavesdropping and hacking — becomes routinely used for banking or commerce. Financial transactions on the Internet would involve sending highly confidential information, such as credit card and bank account numbers, over regular telephone lines.

It is that sort of potential of the Web — a portion of the Internet network of networks that lets computer users with browser software skip between storehouses of text, photos, audio files and even video — that last week fueled the wildly successful initial public offering of stock by the Mountain View company. It has yet to turn a profit but controls more than 70 percent of the market for Web browsers.

It's doubtful that a hacker would be able to easily repeat the work of the French researcher, since it requires either a great deal of time or an enormous collection of computers. Still, the mere chance that a message can be cracked may be enough to keep some people or corporations from doing sensitive business on the Internet.

The problem that Doligez unearthed, though, is not with any bug or shortcoming in Netscape's software. Instead, experts say the situation is a predictable consequence of U.S. export laws, which in effect prohibit U.S. firms from exporting encryption software that is too powerful.

U.S. computer companies consider that restriction a major disadvantage as they try to operate in global markets, since it forces them to sell one version of some programs in this country and a weaker one overseas.

In his work, Doligez used the international version of Navigator, which has a numerical "key" — roughly analogous to the combination to a lock — that is 40 bits long. Security experts say that a key at least 128 bits long is necessary for truly secure communications; the longer the key, the more time it will take a computer to crack it. The domestic version of Navigator has a 128-bit key.

The 40-bit restriction dates from 1992, and was put in place out of a fear by Washington officials that more effective cryptography would give shelter to terrorists and other miscreants overseas.

"We have said for a long time that given the right amount of computer power, that a 40-bit key encrypted message could be decrypted," said Mike Homer, Netscape's vice president of marketing.

The technique for reading an encrypted message used by Doligez is known as the "brute force" method, because computers are programmed to try every conceivable variation on a key.

In the past, Homer said, Netscape has said that an attacker would need "64 MIPS-years" to crack a message on its 40-bit key, roughly the equivalent of a top-of-the-line personal computer running non-stop for six months. The approach that Doligez took — of getting many different computers collaborating over a network — is one that computer scientists have used more often in recent years on problems that require a huge number of basically repetitive computer operations.

U.S. computer firms have long argued that the 40-bit restriction is meaningless, since many of the same encryption programs that can't be officially exported can be easily obtained over the Internet itself.

In addition, critics of the law say it leads to untenable situations, like the one Netscape finds itself in.

When the 40-bit limit was put in place, "we warned then that (40 bits) was too weak," said Jim Bidzos, president of RSA Data Security, the Redwood City company that invented the software approach used by Netscape and many others. "They were supposed to review it every year and allow it to be strengthened." But no such review process has taken place.

Homer said that a future version of the Navigator will contain special provisions for encrypting financial information, such as credit card numbers, with a 56-bit key. He said the company hopes that the new program will be exportable, since Netscape maintains the 56-bit portion of it is too specialized for general cryptography.

IF YOU'RE INTERESTED

For a full report on the breaking of Netscape's encryption on the World Wide Web, point your browser to http://pauillac.inria.fr/~doligez .