Amazing!

- Sharks score 12 minutes into overtime to beat Calgary, take 2-0 lead in series
- Ulf Dahlen scores the game-winner to complete come-from-behind 5-4 win
- Game 3 set for Thursday at Arena/ **Complete coverage in Sports, Page 1D**

San Jose Mercury News

MORNING FINAL FC
35 CENTS

Serving Northern California Since 1851

WEDNESDAY
MAY 10, 1995

CHANGES ON THE TELEPHONE FRONTIER

Programmers foil wiretaps

Free software will transform PCs into untappable telephones

BY SIMSON L. GARFINKEL
Special to the Mercury News

As the U.S. Senate debates granting the Federal Bureau of Investigation new powers to wiretap personal communications, three West Coast computer programmers have planned their own preemptive strike: a free program, distributed on the Internet, that renders legal and illegal wiretaps useless.

The programmers, Bill Dorsey of Los Altos, Pat Mullarky of Bellevue, Wash., and Paul Rubin of Milpitas, plan to release today a program that turns ordinary IBM-compatible personal computers into an untappable secure telephone. It uses an encryption algorithm called "triple-DES" that is

See WIRETAP, Page 7A

■ *Dramatic increase in wiretaps in '94.* PAGE 3F

Bargains on cell phones end

State Senate panel refuses to allow bundling of phones and service

BY DAVID BANK
Mercury News Staff Writer

The monthlong frenzy of seemingly irresistible deals on cellular phones is over.

Since the state Public Utilities Commission voted April 5 to allow retailers to package cellular service with the cell phone itself, the ads have screamed out the offers: The hottest deal ever! No joke! The phone is free!

On Tuesday, most retailers canceled those offer after a state Senate committee declined to go alon with the PUC's plan.

As a result, California is again the only state i the nation where consumers can't get the kind o giveaway deals on cellular phones that are com mon in other parts of the country.

Those who jumped at the offers while the

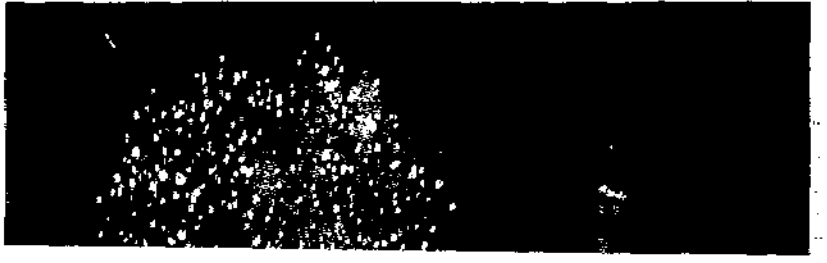
See CELLULAR, Back Pag

Terry Nichols facing charges

McVeigh's Army buddy to be accused in bombing

Burst of pride on Red Square

Russia marks V-E Day with pomp, pageantry in the heart of Moscow



GOP offers budget manifesto

Amazi

San Jose M

MORNING FINAL FC
35 CENTS

Serving Northern

CHANGES ON THE TI

Programmers foil wiretaps

Free software will transform PCs into untappable telephones

BY SIMSON L. GARFINKEL
Special to the Mercury News

As the U.S. Senate debates granting the Federal Bureau of Investigation new powers to wiretap personal communications, three West Coast computer programmers have planned their own preemptive strike: a free program, distributed on the Internet, that renders legal and illegal wiretaps useless.

The programmers, Bill Dorsey of Los Altos, Pat Mullarky of Bellevue, Wash., and Paul Rubin of Milpitas, plan to release today a program that turns ordinary IBM-compatible personal computers into an untappable secure telephone. It uses an encryption algorithm called "triple-DES" that is

See WIRETAP, Page 7A

■ **Dramatic increase in wiretaps in '94.** PAGE 3F

Terry Nichols

Burst of pride on Red Square

Russia r with pon in the he

Programmers foil wiretaps

Free software will transform PCs into untappable telephones

■ WIRETAP

from Page 1A

widely believed to be unbreakable.

"Electronic surveillance by the government is on the rise," says Dorsey, the group's lead programmer. "There also exists an equally large threat from the private sector as well: industrial espionage. Foreign governments are interested in wiretapping and getting information out of our high-tech firms."

Called Nautilus, the program is being released as an attack on the Clinton administration's national encryption standard, the Clipper chip. Civil rights groups have criticized the Clipper initiative, since the federal government holds a copy of every chip's master key and can use that key to decrypt — or decode — any Clipper-encrypted conversation. But since the keys used by Nautilus to encrypt conversations are created by users, the government does not have a copy.

A nod to Jules Verne

Nautilus has another advantage over Clipper: Whereas AT&T's Clipper-equipped Telephone Security Devices Model 3600 costs $1,100, Nautilus is free program.

"You don't need any special expensive hardware for it. You just use ordinary PCs," says Rubin.

The name "Nautilus" was taken from Captain Nemo's submarine in the Jules Verne novel, "20,000 Leagues Under the Sea." But whereas Nautilus the sub was used to sink Clipper ships, the programmers hope that their creation will sink Clipper chips.

To use Nautilus, both participants must have a copy of the program and an IBM PC-compatible computer equipped with a Sound Blaster card and a high-speed modem. The two participants must also agree upon a series of words called a "pass phrase," which is used to encrypt the conversation. Both participants run the program and type in the pass phrase; one person instructs their computer to place the telephone call, the other instructs their computer to answer.

Once the call is in progress, either user must press a key on their computer in order to speak, similar to using a hand-held radio. But unlike walkie-talkies, the users can interrupt each other.

Could help criminals

Such innovations could lead to conversations that would be practically foolproof from eavesdropping, either by pranksters or the government. It could become invaluable in future years to financial institutions and other corporations involved in sensitive negotiations.

"It will certainly be beneficial to many citizens and many other users of it," says Jim Kallstrom, assistant director of the Federal Bureau of Investigation's New York field office.

"I would hope the extremely enterprising and smart people that we have in this country would work toward solutions that would not only protect the communication of citizens . . . but would also allow the law enforcement objectives to be maintained."

Rubin stressed that while Nautilus was a challenge to write, it "isn't rocket science." Much of the program, in fact, was assembled from parts that already were available on the Internet, the worldwide network of computer networks. It will even be easier to construct programs similar to Nautilus once Microsoft releases its computer telephony system for Windows 95. "It will be impossible to keep a program like Nautilus out of the hands of people who want it," Rubin said.

Gene Spafford, a professor of computer science at Purdue University who is an expert on computer security, said: "It will be interesting to see what reaction this provokes from the government." Nevertheless, Spafford said, in order for encryption to be widely adopted, it will have to be "built into the phones."

Dorsey said that anybody in the United States who has Internet access can download it from the computer at ripem.msu.edu (in the directory pub/crypt) or the computer ftp.cs.org (in the directory /mpj). Both of these computers have been set up so that the program cannot be downloaded by people located outside the United States.

Simson Garfinkel is a free-lance writer based outside Boston.

SDAY THROUGH SUNDAY