Hackers pose threat to Internet security systems

NEW YORK (AP) — Intruders have learned how to penetrate sophisticated barriers and hijack computer systems linked to the Internet, posing a vast new security threat on the global network, authorities said Monday.

Millions of computers linked to the Internet are vulnerable to theft and eavesdropping by people who use the new technique, first described in an academic paper 10 years ago but known to be used successfully only in recent weeks, experts said.

Intruders can gain "root" or top-level access to host computers, then copy or destroy documents or do other damage by masquerading as an authorized user on the host system, the government-financed Computer Emergency Response Team said.

"Once the attack is completed, it is difficult to detect," the team said in an advisory distributed Monday on the Internet.

An unknown number of attacks already have been reported, Tom Longstaff, manager of research and development at the CERT coordination center in Pittsburgh, said in a telephone interview.

For many computer systems, "Even when you bought a security package for the Internet... there was no security" from the new type of attack, Longstaff said. That's because the attackers have learned how to defeat sophisticated hardware and software "firewall" defenses.

An estimated 20 million people use the Internet, most logging in through "host" computers at universities or commercial access providers.

In coming months the Internet is expected to continue growing rapidly as a medium for commerce, with expanded use of credit card numbers and the introduction of "digital cash" — all of which increases the security threat.

"There have been a lot of cases where credit card information has been asked for and given" on-line, said Sanford Sherizen, president of Data Security Systems, a consulting firm in Natick, Mass. "People might as well stand on a street corner and yell the information out, or get a plane and trail it in the sky."

"We're in a real battle now," Sherizen said. "There are a lot of people, beyond hackers, who are the real computer criminals... who are interested in industrial espionage" and other white-collar crime and who could use the new technique, Sherizen said.

The new attacks, initially reported Monday by *The New York Times*, were first detected in a Christmas Day break-in at the computer of Tsutomu Shimomura, a computer security specialist at the San Diego Supercomputer Center.

The culprit or culprits controlled the computer for more than a day and electronically stole a large number of security programs that Shimomura had written.

"They destroyed some records and attempted to destroy others," Shimomura said in a telephone interview. "I think they were trying to prevent us finding out what technique they were using to break in."

Only after four days of investigation were officials at the center able to confirm what had happened, Shimomura said.

The *Times* said federal officials are investigating subsequent break-ins at several organizations' computers. FBI officials wouldn't comment Monday.

Shimomura called the attack "a new order of sophistication."

"I expect that attacks like this will continue, especially as there is more commerce on the 'net... until we have real security and strong cryptography in place" to encode digital transmissions, Shimomura added.

The new technique is called Internet protocol spoofing. The Internet breaks computer messages into digital data "packets" with addressing information — the protocols — used by network computers known as routers, which deliver the data.

Spoofing fools the router into believing a message is coming from a trusted source, potentially giving the intruder complete access to what was considered a well-guarded system.

"Intruders can use IP spoofing to gain root access for any purpose," the CERT advisory said.

Once inside the system, intruders can use a "hijacking tool" to take over connections from any user on the system, the advisory said, adding that there's no way to prevent use of the "hijacking tool" once an intruder has gained access to a computer system.

The attacks were described in theory in academic papers in 1985 and 1989, CERT said.

The advisory listed types of computers, routers and software applications that are vulnerable to Internet protocol spoofing. Some types of networks already include filters that should prevent the attacks, but for other types, a filter must be installed.

The solutions are difficult, Longstaff said. "Sometimes it's hard to understand why you're doing a solution, even for experts, which is what makes this particular problem so insidious."

Classified government computer systems are not thought to be at risk because they are not directly connected to the Internet, the *Times* said.

The Internet originally was created by academic researchers to share computer data easily around the world.

We the People members indicted for fraud, theft

DENVER (AP) — Eleven members of a group that considers the nation's banking system illegal were indicted on charges of bilking more than $300,000 out of people who thought they were sharing in proceeds from a court victory.

Members of We the People, based in Fort Collins, face charges of securities fraud, conspiracy, criminal impersonation and theft, state Attorney General Gale Norton said Monday.

The money was collected from people who were told that the group was authorized to collect millions of dollars on behalf of anyone who paid taxes, had a bank account or even used currency, Norton said.

Despite warnings by the state about the group's practices, more than 1,000 Colorado residents paid the group a $300 "filing fee" touted as a way to share in the proceeds of a court victory the group claimed, she said.

Group founder Roy Schwasinger, who is named in the indictment, claimed the U.S. Supreme Court had declared the nation's banking system, the Federal Reserve and the Internal Revenue Service illegal because of a We the People class action lawsuit.

The group's lawsuit was dismissed without going to trial on grounds it had no legal basis, Norton said.

Teen pleads guilty to slaying tourist

MONTICELLO, Fla. (AP) — A 16-year-old pleaded guilty Monday to a reduced charge for fatally shooting a British tourist and wounding his companion at a highway rest stop, the latest in a year of road attacks on Florida visitors.

Prosecutors were prepared to claim that Aundra Akins was the triggerman in the attack that killed Gary Colley and wounded Margaret Jagger. He becomes the third of four youths to plead to lesser charges in the case.

Akins, who was 14 at the time of the 1993 attack, pleaded guilty to second-degree murder and attempted murder about an hour before his trial was to begin. As part of the plea bargain, he faces a maximum 40 years in prison and will testify against John "Billy Joe" Crumitie, an 18-year-old facing a second trial after a jury was unable to reach a verdict the first time around.

Jagger was in court with her mother, Muriel, and said afterward she was happy another phase of the case had ended.

"I was consulted in all this," Jagger said in a brief statement. "I'm pleased it's happened. I'm glad it's over with at the moment."

Colley, 34, and Jagger, 36, dozed in a rental car at an Interstate 10 rest stop during a drive from New Orleans to South Florida when the youngsters tried to rob them on Sept. 14, 1993. When Colley tried to back up the car to escape, Akins and Crumitie opened fire, hitting Colley in the neck and wounding Jagger, prosecutors said.

Prosecutors said Akins fired the fatal shot. His lawyers had called the case weak. The state hasn't recovered the guns and has little physical evidence linking the suspects to the crime.

In exchange for Akins' plea, the state dropped lesser charges of attempted armed robbery and shooting into an occupied vehicle.

He faces three to 40 years in prison. Sentencing was scheduled for April 11. Akins could have received life in prison if convicted of first-degree murder.

Colley was the ninth foreigner killed on Florida roads in a single year. The unrelated shootings battered the state's tourism trade and prompted lawmakers to pass tough juvenile justice reforms.

Deron Spear, 18, pleaded guilty to conspiracy to commit armed robbery and accessory after the fact. Spear, who said he drove the getaway car, faces up to 10 years in prison at his March 14 sentencing.

Spear's half-brother, 14-year-old Cedrick Green, pleaded no contest to lesser charges. He was sentenced last month to community control, placed on a curfew and ordered to perform 50 hours of community service.