Internet Wiretapping

Government and Law Enforcement Use

Overview

- Origins of Internet Wiretapping
- How Does It Work
- Targets of Internet Wiretapping
- Programs and Laws Involving Internet Wiretapping
- Controversy surrounding Internet Wiretapping
- Protection from Internet Wiretapping
- Potential Future of Internet Wiretapping

Origins (Omnivore)

- In 1997, the FBI deployed the second generation program of online-detection software, **Omnivore**.
- According to information released by the FBI, **Omnivore** was designed to look through e-mail traffic traveling over a specific Internet service provider (ISP) and capture the e-mail from a targeted source, saving it to a tape-backup drive or printing it in real-time.

Origins (Carnivore)

- In late 1999, **Omnivore** was retired in favor of a more comprehensive system, the **DragonWare Suite**, which allowed the FBI to reconstruct e-mail messages, downloaded files or even Web pages.
- **DragonWare** contained three parts: Carnivore, Packeteer and Coolminer.

Origins (Carnivore)

- **Carnivore** was the third generation of online-detection software used by the FBI.
- Information about the first version has never been released, but it is believed that it was actually an available commercial program called **Etherpeek**.

Carnivore

- **Carnivore -** A Windows NT/2000-based system that captures the information.

No official information was released about Packeteer and Coolminer.

- **Packeteer** – It is presumed that is an application for reassembling packets into cohesive messages or Web pages
- **Coolminer –** It is presumed that it is an application for extrapolating and analyzing the data found in the messages

Carnivore

- Officials never released much information about the **DragonWare Suite**, **Packeteer** and **Coolminer** and very little detailed information about **Carnivore**.
- What is known about Carnivore is that it was basically a **packet sniffer**

Packet Sniffer

- A packet sniffer is a program that can see all of the information passing over the network it is connected to.
- As data streams back and forth on the network, the program looks at, or "sniffs," each packet.

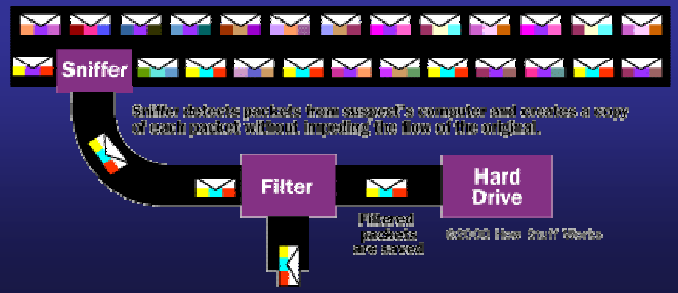
Packet Sniffer

A packet sniffer can usually be set up in one of two ways:

- **Unfiltered** - Captures all of the packets
- **Filtered -** Captures only those packets containing specific data elements

Packet Sniffer

- Packets that contain targeted data are **copied** as they pass through.
- The program stores the copies in memory or on a hard drive, depending on the program's configuration.



Packet Sniffer

A packet sniffer located at one of the servers of your ISP would potentially be able to monitor all of your online activities, such as:

- Which Web sites you visit
- What you look at on the site
- Whom you send e-mail to
- What's in the e-mail you send
- What you download from a site
- What streaming events you use, such as audio, video and Internet telephony
- Who visits your site (if you have a Web site)

How Carnivore Works

- FBI agents take an off-the-shelf PC with the Carnivore software on it directly to the offices of an Internet service provider (ISP), i.e. AOL.
- They leave it there for about 45 days, making daily visits to retrieve captured data, for example, the e-mails sent to or from a suspect.
- Like the more common phone tap, such an Internet tap must be authorized by court order.

Requirements for Carnivore

- A type of physical lockout system that requires a special passcode to access the computer (This keeps anyone but the FBI from physically accessing the Carnivore system.)
- A **network isolation device** that makes the Carnivore system invisible to anything else on the network (This prevents anyone from hacking into the system from another computer.)

Targets of Carnivore

The FBI planned to use Carnivore for specific reasons. The FBI would request a court order to use Carnivore when a person was suspected of:

- Terrorism
- Child pornography/exploitation
- Espionage
- Information warfare
- Fraud

- Between 1998 and 2000: The Carnivore was used about 25 times.

End of Carnivore

- In 2002: FBI performed only 5 internet wiretaps.
- In 2003: FBI performed only 8 internet wiretaps.
- According to FBI reports, Carnivore was not used in these wiretaps
- In 2005: The FBI effectively abandoned Carnivore and switched to an unspecified commercial software.

Criticism of Carnivore

- Critics say Carnivore gives the FBI access to private information that exceeds a court order. In theory, it could process all the e-mail that passes through the ISP not just messages sent to or from the suspect.

Criticism of Carnivore

- Critics complained they have unlimited access to all Internet users' personal correspondence, whether it is covered by warrant or not.

Criticism of Carnivore

- Critics compare the software's activity to snooping on all the phones in a neighborhood to zero in on one phone. Others claim Carnivore goes beyond e-mail surveillance to also monitor overall Internet usage.

Flaw in Carnivore

- "The Denver field FBI office's terrorist electronic surveillance probe of bin Laden's network not only snatched targeted e-mails "but also picked up e-mails on non-covered targets," said a March 2000 memo to agency headquarters in Washington. "

- foxnews.com

Internet Wiretapping Programs and Laws

- USA PATRIOT ACT
- NSA Terrorist Surveillance Program
- FISA ACT

The Patriot Act

- Parts of the Patriot Act, including a section on "roving wiretaps," Such wiretaps allow the FBI to get permission from a secret federal court to listen in on any phone line or monitor any Internet account that a terrorism suspect may be using, whether or not others who are not suspects also regularly use it.

NSA Terrorist Surveillance Program

The NSA program intercepted phone calls and e-mails on U.S. soil, bypassing the normal legal requirement that such eavesdropping be authorized by a federal court. The program began after the September 11 terrorist attacks and continued until January 17, 2007, when the white house resumed seeking surveillance warrants from the foreign intelligence surveillance court.

Arguments (NSA TSP)

Gen. Michael Hayden

- “this program has given us information that we would not otherwise have been able to get."
- “If the surveillance had been used before Sept. 11, we would have detected some of the 9/11 al-Qaeda operatives in the United States."

Sen. John Kerry

- “by instituting the surveillance without explicit congressional approval, Bush seemed to be saying he was ‘above the law.’”

- Were the program's actions legal?
- Were the program's actions ethical?
- Were innocent Americans' privacy sacrificed to ensure their safety?

- Sen. Arlen Specter, R-Pa., who chairs the Senate Judiciary Committee, has questioned the legality of the program. A 1978 law requires the NSA to obtain federal court-approved warrants before eavesdropping on U.S. targets.

Bush's Defense of NSA TSP

"Congress gave me the authority to use necessary force to protect the American people, but it didn't prescribe the tactics,"

-President Bush

Bush's Defense of NSA TSP

- Bush characterized the surveillance program as a concept brought to him by senior aides in response to his question posed internally following the 9/11 attacks: "Is there anything more we can do, within the law, within the Constitution, to protect the American people?"

Arguments (warrantless wiretaps)

For making it easier to track suspects

- Acquiring warrants is time consuming. It unnecessarily slows down U.S. intelligence officials as they track suspects.

For limited warrantless wiretaps

- Placing limits on wiretapping without a warrant are aimed at protecting Americans from unnecessary surveillance.

- The controversy over President Bush's warrantless domestic eavesdropping program also prompted calls for change in the FISA law.

FISA Updated

- The FISA law requires court orders when the target of any eavesdropping is an American citizen or individual living in the U.S. **Warrants are not necessary** if the target is overseas.

Questions about FISA

- **Question:** What are the key provisions in the FISA bill?

Answer

Pam Benson, CNN's National Security Producer

Benson: The bill explicitly establishes FISA as the exclusive means for authorizing electronic surveillance; requires a court order for the surveillance of any targeted American, whether the person is in the United States or abroad; and requires a secret court set up to oversee FISA issues to sign off on provisions for removing the name of any American inadvertently captured in a communication with a foreign target.

Questions about FISA

- **Question:** Under the proposed FISA bill, can Americans be spied on without a court warrant? Are their civil liberties protected?

Answer

- **Benson:** Under the new revised law, a warrant is required to spy on any American, including, for the first time, Americans who are abroad.

Answer

- If the intelligence community should unintentionally intercept a phone call or an e-mail involving an American, the agency involved must get a warrant if the person is of interest or take steps to erase that person's name from any report.

Answer

- The bill states that domestic electronic surveillance is authorized exclusively by the provisions of FISA. This is an effort to prevent the president from secretly authorizing warrantless eavesdropping, which some lawmakers and civil rights groups claim violates the public's Fourth Amendment protection against unreasonable searches.

Answer

- However, the bill does not address President George Bush's claim that he has Article 2 constitutional authority as the commander-in-chief to order such activity during times of war.

Protection From Packet Sniffing

Encrypting Data

MIT Recommends:

- While sniffer programs usually capture only the first 128 characters of a packet, they can be set to capture all data as it passes over the network. This includes data sent via FTP or email. Your best protection against such eavesdropping is to use a public key encryption system such as Pretty Good Privacy (PGP).

Potential Future of Internet Wiretapping

In 2001:

- **The FBI is seeking to broaden considerably its ability to tap into Internet traffic in its quest to root out terrorists, going beyond even the new measures afforded in anti-terror legislation signed by President Bush.**

Potential Future of Internet Wiretapping

- Stewart Baker, a former general consul to the National Security Agency, said the FBI has plans to change the architecture of the Internet and route traffic through central servers that it would be able to monitor e-mail more easily.

Potential Future of Internet Wiretapping

- FBI Spokesman Paul Bresson said he was unaware of any development in the e-mail surveillance arena that would require major architectural changes in the Internet, but **acknowledged that such a plan is possible**. Any new efforts would be in compliance with wiretapping statutes, Bresson said.