Global Information Assurance Certification Paper

Carnivore – An issue of trust, a legal framework, a necessary tool

Dennis Burns, AICP

The Federal Bureau of Investigation (FBI) in 1999 implemented a newly developed system designed to make it easier for them to monitor electronic communications. The system was developed and deployed with no fanfare, and it was not until July of 2000 that the use of the Carnivore system was noted in the media. While few details have been made public regarding this system, privacy advocates and others have been quick to criticize the use of such a system for monitoring email, and for the secrecy surrounding the use of the system. The Department of Justice has defended the deployment of this tool as an necessary approach to dealing with crimes and criminals who use electronic communication to facilitate their activities, and notes that it has been used in only about 25 cases (unknown number of taps) since its initial development and deployment. [7] The legal basis for the collection of electronic data is similar in some ways to telephone taps, and thus the term electronic taps is an appropriate term to use.

Privacy rights and civil liberties collide with the legitimate needs of the criminal justice system on a regular basis. The inherent friction between these necessary components of a free society is a given, and the issues are not always clearly black-or-white issues. The functions played and the roles assumed by groups such as these work to keep our society free and crime under control. A number of players have weighed in on the Carnivore issue, including the American Civil Liberties Union (ACLU), members of the U.S. Congress, and the Center for Democracy and Technology. [3, 4, 7] One major Internet Service Provider (ISP) has reported some issues and problems. [2, 6]

Overview of the Carnivore system

According to the FBI, the Carnivore system is essentially a network sniffer, which employs a series of sophisticated filter sets to segregate out the network traffic that is desired. [1] The system has been characterized by others (not by the FBI) as a Black Box, because so little is known about the actual internal workings. A public information piece on the FBI public web page notes that the actual device is a commercially available tapping device. [1]

Once the legal authority has been granted to the FBI to deploy a Carnivore unit, it is placed at an ISP's data center, with the cooperation of the ISP. An appropriate data access point is identified, with the intent of capturing all of the ISP's network traffic that contains the suspect's data, but as little extraneous traffic as possible. In some cases, the ISP is able to provide the FBI with an access point that only includes traffic from the suspect. [1]

Once the data stream of interest has been identified, that data is separated from the ISP's main data stream. At this point, the first filter set is applied which segregates the suspect's data from the rest of the segregated network traffic. The suspect's traffic is copied and passed to the Carnivore system as it falls through the filter. All of the segregated traffic (including the original suspect data) is then merged back into the ISP main data stream.

At this point, the Carnivore system has a copy of the target, or suspect's data and it applies additional filters to meet the requirements of the court order authorizing the electronic tap. As each successive filter is applied, some data is allowed to fall though the filter and some is stopped. The data that is allowed to fall through the filter is permanently archived on the Carnivore unit and the data that is stopped by the filter is permanently deleted. All of the data that is retained (and according to the FBI, all of the data that is ever seen by human eyes) is ONLY that data that has been explicitly and specifically authorized to have been collected as evidence. [1, 5]

As a technical note, the data stream itself is (apparently) unchanged, including both the intercepted messages that are copied to the Carnivore system and the "uninteresting" messages (data that is not the subject of the FBI's interest). One implication of this is that any encryption that has been applied to any part of the message will still be encrypted. [4] Further, concluding that the data stream is itself unchanged is based on some assumptions, which just are not known at this point. For example, as the Carnivore system 'touches' files, it may leave some tell-tale mark on them, either in the form of a bit or file modification, or as a small (but perhaps detectable?) delay in the packets that are segregated then reinjected in the main ISP data stream. This may potentially be exploited and used to determine if one's data were being intercepted or not.

Legal requirements

The basis of the authority to conduct electronic wiretaps are ". . . the stringent requirements of the federal wiretapping statutes." [5] According to testimony given to the U. S. House of Representatives Committee on the Judiciary, Constitution Subcommittee by the FBI [8, 9], the requirements for receiving authorization to conduct an electronic tap are much more strenuous than are the requirements for obtaining a search warrant, even though both are covered under Title III of the Omnibus Crime control and Safe Streets Act of 1968 (commonly referred to as Title III) and the Electronic Communications Privacy Act of 1986 (ECPA). Court orders are required in all cases (in the case of emergencies the court order must be obtained within 48 hours of the initiation of the tap).

Constitutional guarantees on unreasonable search and seizure are based on the Fourth Amendment with additional provisions. Applications must be approved by a high level Department of Justice official, they must be reviewed by federal district court judges, and interception of communications is limited to only include certain specified felony offenses. Further requirements include specificity in the kinds of communications that may be intercepted, limiting the data collected to the class of evidence rather then intelligence. And, finally, the applications must indicate that other investigative techniques have been tried and failed to gather evidence. [8]

These safeguards are not enough, according to some civil liberty groups, privacy advocates, ISPs, and congressional members. The use of the Carnivore system first came to public attention when a major ISP (Earthlink) complained about it [7]. Apparently,

Earthlink installed the software at the request of the FBI at a data center in Pasadena, California in 1999 after losing a court decision on the matter in federal court. After some operating system problems were detected, an older system was installed for the device, which led to some server crashes, disrupting Internet access for some customers. [2, 6] Earthlink has reached an agreement with the FBI as a result of this which allows Earthlink to monitor and gather the information themselves, and to provide it to the FBI [2].

Earthlink, however, and others, remain wary of the FBI's use of this tool. Kurt Rahn of Earthlink is especially concerned when a court order would result in a compromise of operations. He says, ". . . . since delivering email and delivering the internet to our members is what we do, [and] having that threatened is not going to work for us." [2]

The American Civil Liberties Union weighs in on this issue and notes that the Carnivore system may breach an ISP's rights of all its customers by reading both sender and recipient addresses, as well as subject lines of emails, to decide whether to make a copy of the entire message. [6] Barry Steinhardt, associate director of the ACLU suggests that citizens should not trust that such a powerful and sweeping tap would be used only against criminal suspects. [4] Several members of the House of Representatives Judiciary Committee's Subcommittee on the Constitution were critical of the system on similar grounds. The subcommittee meeting of July 24, 2000 (at which the FBI testified [8]) was reported as being 'contentious', with some committee members suggesting that the FBI was not being as forthcoming as they should have been regarding Carnivore. Other committee members expressed ". . . . grave concerns about the potential for privacy violations and skepticism that Carnivore's operations are as confined as the FBI says they are." [7]

The Center for Democratic Action and the ACLU have requested that one solution would be for the FBI to release the source code, and the ACLU subsequently filed a Freedom of Information Act request for the source code in July, 1999. [3] The FBI does not support this approach, but has suggested an independent review of the Carnivore system. On August 24, 1999 a formal request for proposals was issued by the FBI, and a 63-page description of the desired technical review was posted on the FBI public website, but was apparently removed once bids were due (September 6, 1999).

The Electronic Privacy Information Center (EPIC), an advocate for civil liberties and privacy, believes that the FBI should make more information on the internals of the Carnivore system available to the public, and feels that the audit/independent review will not be sufficient. David Sobel, legal counsel for EPIC states ". . . . this review will not be able to resolve all of the questions, either technical or legal." He also questions whether or not substantial and significant portions of the final report will ultimately be released to the public. [10]

Conclusion

The battle between the 'good guys' and the 'bad guys' is a battle of high stakes, and successful early adopters of new technologies definitely have the upper hand. If criminals are able to use tools and technologies against society for personal gain, then it only makes sense for law enforcement to have access to these same tools. But, from a free society's perspective, one of the fundamental differences between the 'white hats' and the 'black hats' is the idea of *enablement* – society itself has given the 'good guys' the authority to identify and track down the 'bad guys' – we grant the authority to a select group of its representatives to be the 'good guys' and give them the tools (white hats, search warrants, the Carnivore system, loud guns, and big budgets) that *enable* them to perform these functions. History has shown time and time again that societies that have not taken this delegation of power seriously have often become the victims rather than the benefactors.

Thus there are few surprises in this story. The actors are predictable, and their comments are not necessarily profound. The system of checks and balances requires that these actors play these roles, and as citizens of a free society, we should all be grateful that they are indeed doing just that. The technology is not new – the idea of network packet sniffing is a tried and true method of detecting, filtering, and analyzing packets and network traffic. And it is no surprise that the FBI would prefer that the details of the Carnivore system be kept out of public's scrutiny. But there should also be no surprise from the Department of Justice that there is intense public interest in this. Citizens generally place a high value on their privacy, and they are sensitive to any loss, real or perceived, of that privacy.

What lessons, beyond those already offered, can be gleaned from this? First, technology is a series of small, incremental steps. We use existing tools and techniques to bring us to a new place every day. Second, if you wear a black hat, know that there are posses out there wearing white hats, and they are using the same tools you are. Know that society has enabled them and given them authority to use these tools to try and keep up with you. And if you wear a white hat, know that you answer to a higher authority, and that is society. Keep in mind that while there are strict guidelines in place to honor that trust which has been placed in you, the final result is not necessarily those guidelines and laws, but rather the spirit of the trust. And for the rest of us, a little trust goes a long way, but it should be tempered with a healthy dose of skepticism.

This year it is Carnivore in the news. What will next year bring?

References

1. FBI. "Carnivore Diagnostics Tool, Large Chart, Description." URL:http://www.fbi.gov/programs/carnivore/carnlrgmap.htm (9/12/00).

2. The Associated Press (AP). "Earthlink will do FBI's surveillances itself." Special to CNET News.com 7/14/00, 3:55 pm PT. URL:http://news.cnet.com/news/0-1005-200-2257522.html (9/12/00).

3. McCullagh, Declan. "FBI gives a little on Carnivore." WiredNews. 7/25/00, 9:35 am PDT. URL:http://www.wired.com/news/politics/0,1283,37765,00.html (9/12/00)

4. The Associated Press (AP). "Privacy groups protest FBI email scanner." Special to CNET News.com 7/12/00, 5:55 am PT. URL:http://news.cnet.com/news/0-1005-200-2245549.html (9/12/00).

5. FBI. "Carnivore Diagnostics Tool, Information Sheet." URL:http://www.fbi.gov/programs/carnivore/carnivore2.htm (9/12/00).

6. Sellers, Dennis. "Carnivore snooping software loses some bite." MacCentral Web Site. 7/17/00 7:00 am ET. URL:http://www.maccentral.com/news/0007/17.carnivore.shtml (9/12/00)

7. Johnston, Margaret (IDG News Service). "House panel grills FBI over Carnivore." Computerworld. 7/25/00. URL:http://www.computerworld.com/cwi/story/0,1199,NAV47_STO47490,00.html (9/13/00).

8. Kerr, Donald M. (Asst. Dir. FBI). Congressional Statement on Internet and Data Interception Capabilities Developed by the FBI. 7/24/00. URL:http://www.fbi.gov/pressrm/congress/congress00/kerr072400.htm. (9/12/00).

9. Kerr, Donald M. (Asst. Dir. FBI). Congressional Statement on Carnivore Diagnostic Tool. 9/6/00. URL:http://www.fbi.gov/pressrm/congress/congress00/kerr090600.htm. (9/12/00).

10. Sniffen, Michael J. (The Associated Press, AP). Justice Department seeks outside review of e-mail surveillance tool. 8/24/00, 10:03 pm EDT. URL:http://ap.pqarchiver.com/cgi-bin/display.cgi?id=39c1860150cd1Mpqaweb1P11018&doc=document.html&url=http%3a%2f%2fpqacontent1%3a10001%2fservlet%2fcom.infonautics.panama.content.document_repository.RetrieveDocumentForDisplayServlet%3fpublisherName%3dAP%26publicationName%3dAssociated%2bPress%26providerName%3dAP%26publishingDocID%3dD76IQTA80 (9/12/00). (Note – this article was originally accessed through a link on http://www.nandotimes.com on 9/12/00, but the URL on the downloaded printed page was incomplete when this references page was compiled. An extensive web search for the article on 9/14/00 resulted in the article only being located as an archive on the AP (Associated Press) web site (http://wire.ap.org), accessible at the rather cumbersome URL above, or accessible through the search engine located at http://wire.ap.org. Any AP archive articles from this site that are older than 2 weeks (including this article) are fee-based.

Test questions for submitted paper
Paper topic – Carnivore – An issue of trust, a legal framework, a necessary tool
Dennis Burns, AICP
Submitted 9/14/00

MultChoice

1. Carnivore is a:
    a. email virus
    b. open-source, secure Unix-based web server based on Apache
    c. email scanning program used by the Department of Justice
    d. hoax

{1 (c)}

2. The Carnivore system is based on which of the following families of popular network analysis tools:
    a. ICMP – echo/request
    b. nmap
    c. netbus
    d. packet sniffer

{2 (d)}

3. The network traffic segregated out of the ISP's main data traffic stream by Carnivore is:
    a. copied to the Carnivore server
    b. sent to alternate data paths depending on the results of filtering
    c. dumped to a SYSLOG file
    d. analyzed for keywords through a focused dictionary

{3 (b)}

4. The use of the Carnivore system is restricted to:
    a. federal officers acting under a court order
    b. authorized computer security professionals
    c. any sysadmin logged in as root
    d. a domain user

{4 (a)}

5. The main use of the Carnivore email scanning system is to:
    a. identify vulnerabilities in sendmail smtp servers
    b. scan emails for large file attachments in order to comply with policy
    c. scan outgoing email messages for known virus signatures
    d. collect evidence when a crime is suspected

{5 (d)}

TrueFalse

1. The Department of Justice's Carnivore email scanning system was well received by the Congress and the media when it was first introduced.

{1 (False)}

2. The Carnivore system has been in use since the initial introduction of the Unix operating system.

{2 (False)}

3. When the Carnivore email scanning system is installed at an ISP's site, all customers are notified by the ISP that the system is operational.

{3 (False)}

4. The installation of Carnivore has resulted in server crashes and internet outages for some ISP's and their customers.

{4 (True)}

5. The Carnivore system is popularly referred to as a Black Box, because the internals are a closely guarded secret.

{5 (True)}