Comments on the Carnivore System Technical Review

Steven M Bellovin
AT&T Laboratories
smb@research.att.com

Matt Blaze
AT&T Laboratories
mab@research.att.com

David Farber
University of Pennsylvania
farber@cis.upenn.edu

Peter Neumann
SRI International
neumann@csl.sri.com

Eugene Spafford
Purdue University CERIAS
spaf@cerias.purdue.edu

3 December 2000

I Introduction

In September, 2000, we were asked by the Chief Scientist of the US Department of Justice to identify technical issues with the FBI's Carnivore Internet wiretap system that should be addressed by an independent review. On October 2, we met with Justice officials in Washington, DC, where we identified various areas of concern and issues that we believed must be addressed by any meaningful review process.

The contractor chosen by the Government to conduct this review, IIT Research Institute, recently

released a draft report of its findings ("Independent Technical Review of the Carnivore System", dated 17 November 2000). We have studied that report and we continue to have serious concerns relating to the Carnivore system.

Although the IITRI study appears to represent a good-faith effort at independent review, the limited nature of the analysis described in the draft report simply cannot support a conclusion that Carnivore is correct, safe, or always consistent with legal limitations. Those who are concerned that the system produces correct evidence, represents no threat to the networks on which it is installed, or complies with the scope of court orders should not take much comfort from the analysis described in the report or its conclusions.

We are especially concerned with several serious limitations of the analysis as presented:

- There is a lack of analysis of operational and "systems" issues, including interactions between the Carnivore code and its host environment and operating system. Many potential security flaws and collection errors are likely to be found in this area.
- There is no evidence of a systematic search for bugs, not even such common (and serious) errors as string buffer overflows or URL or header parsing problems, although these are listed as potential issues.
- The exclusion from analysis or testing of RADIUS is a very serious omission; RADIUS is especially difficult to interpret in a vendor-independent fashion, and has been cited as a source of Carnivore problems in media reports.
- There is inadequate discussion of audit and logging (both of logs maintained by Carnivore itself and of logs maintained by the host operating system and supporting tools). This is especially serious in light of the use of "PC Anywhere" and "Administrator" logins for remote access, which permits any files to be uploaded or changed, including the logs and audit trails.

II Conclusions and Recommendations

Unfortunately, serious technical questions remain about the ability of Carnivore to satisfy its requirements for security, safety, and soundness. While the IITRI report does represent a good starting point for answering these questions, we were disappointed that more attention was not paid to operational and "systems" issues. It is simply not possible to draw meaningful conclusions about isolated pieces of software without also considering the computing, networking, and user environment under which they are running. These and other areas must be examined further if the legal community, ISPs, and the public are to have confidence that Carnivore works as it is supposed to.

We also urge that the report's recommendations with regard to logging and audit be considered carefully and made a high priority. The Carnivore system does not produce meaningful or secure audit trails. This is obviously a very serious deficiency.

We applaud the DoJ and IITRI for their openness in the Carnivore review process, especially in light of the time constraints under which the review was conducted and the extraordinary sensitivity of critical law-enforcement surveillance technology. Nonetheless, we must emphasize that no single review can ever capture every potential problem with critical software of this complexity, especially when it must be run under a wide range of operational environments. Furthermore, as the software is enhanced and the environment under which it runs evolves, existing reviews may well be

rendered obsolete. As such, the Department of Justice must consider an on-going process to maintain confidence in the system. One such approach is to publish the Carnivore source code for public review. Although an extraordinary step, we urge the DoJ to consider it seriously.

III Itemized Comments

Following is a list of comments keyed to the roman page numbers or symbolic section numbers in the draft report.

p. xiii

There is a statement that Carnivore is not powerful enough to capture everything, that unless the filter is configured correctly, it will not accurately collect data. This implies that it might not keep up with heavy load as part of a lawful intercept. As such, this issue should be explored to ensure Carnivore behaves correctly under heavy load.

ES.4

The user must be logged in as Administrator. This is bad, because flaws in the code can easily lead to system penetrations and violations of least privilege.

Putting more and more into the driver is a poor way to produce a robust system. It requires too much privileged code.

There are two typos: DLL stands for "dynamic link library." The correct brand name of the removable disk drive is "Jaz" and not "Jazz" disk.

ES.5

The draft says that "Carnivore represents technology that can be more effective in protecting privacy and enabling lawful surveillance than can alternatives." What alternatives? The scope of this statement is undefined.

ES.6

A "CRC" should not be used. Instead, a cryptographically strong "MAC" (message authentication code) or (at the least) a cryptographic checksum such as SHA-1 should be used. (Note: "CRC" -- "cyclic redundancy check" -- refers to a particular mathematical algorithm; it is simply one form of checksum.)

1.1.1

There is mention in point 17 about possible string buffer overflows in Carnivore or related tools. But there is no further discussion in the report. This is a *very* serious omission in the report; buffer overflows are among the most common causes of security weaknesses in network software.

Clearly, the IITRI team could not do a thorough search for buffer overflows in the allocated time. But some analysis of the possible consequences of an overflow -- in Carnivore, CoolMiner, Packeteer, or wherever -- should be feasible.

More generally, are there sanity checks on collected data?

In general, there should have been a much more thorough search for bugs. The problems with the analysis programs should have been found in earlier testing by the FBI.

3.2.3

Why is the second minimization done by the case agent? If impermissible data is collected by Carnivore, the case agent can learn its contents before deleting it. This seems to violate the separation policy otherwise used.

3.4.3

PCAnywhere is *far* too powerful for this purpose. Any files can be changed or modified, with no auditing. A less general mechanism that provides suitable logging and that does not permit remote modification of log files would be far better.

3.4.4

Apart from the issue of a compiled-in password, standard practice calls for such passwords to be one-way hashes, rather than plaintext.

3.4.4.1.2

What protections are there against forged RADIUS or DHCP packets? What about forged addresses in general? Is the ISP required to do ingress filtering?

3.5.1

The note that "Carnivore is not intended to ... collect all packets" is wrong; that's a function that (as noted elsewhere) is present simply because of its behavior with no filters.

3.5.3

Table 3-1 is unclear on what happens if the strings appear in the middle of a packet, or if the string is split across two packets. See, for example, RFC 2920, for one way in which this can happen for e-mail.

The handling of fragments is frequently problematic and should be addressed further.

3.6.10

DHCP can key on host name, not only MAC address.

4.1

The Windows NT configuration is quite crucial. This *must* be evaluated. Is there an IP stack? Can incoming packets crash or compromise the host environment even before the packets get to Carnivore? What is done for NT installation and configuration management? All conclusions depend on "correct configuration"; how likely is that in practice?

RADIUS is *not* similar to DHCP, and in fact poses a large number of operational issues. In particular, there are numerous non-interoperable, vendor-specific extensions. The crash in the Earthlink case is rumored to stem from limitations in Carnivore's RADIUS-handling code (thus forcing the ISP to fall back to less-stable code that implemented a desired profile of RADIUS); failure to evaluate the Carnivore implementation is not acceptable.

4.2.1

The ISP has no way to verify that the settings have been correctly entered. Indeed, this seems to be a FBI requirement in some cases -- they report that in some cases the name of the person being intercepted is deliberately kept hidden from the ISP. (This suggests that Carnivore provides functionality to the FBI in excess of what can be obtained by cloning the target's e-mail account.) This contradicts the statement that Carnivore is used only when an ISP cannot provide the relevant data.

4.2.2

The report suggests that judicial oversight is the ultimate check on abuse. Given examples of the failure of such processes -- notably the recent wiretap fiasco in Los Angeles -- it is difficult to be completely reassured.

This will become more of an issue if and when Carnivore versions are made available to more police agencies around the country.

4.2.3

Most protocol messages are not guaranteed to start on TCP packet boundaries.

4.2.4

In general, we agree with the report that much more attention needs to be paid to audit trails.

Carnivore seems to allow use of keyword searching on all IP traffic on the subnet (no filtering to specific IP addresses). We would be interested to hear opinions on whether this capability is authorized by wiretap law.

4.2.6

We agree that the lack of a formal development environment, including formal and auditable change management to the source code, is crucial.

4.2.8

It is not legal to look at mail headers with a pen register warrant, because it can disclose correspondence between two or more parties who are not subjects of the court order.

What are the consequences of missed or out-of-order packets? As Carnivore is not in-line in the protocol, it is quite difficult and not always possible to detect missed or out-of-order packets.

The report states that under-collection is never a risk. This isn't true; missed RADIUS packets, missing exculpatory e-mail messages, etc., can have a large impact. How can an agent determine if traffic was missed or lost?

There seem to be a number of cases of potential over-collection in pen mode. It captures entire IP headers for some protocols. It captures the entire packet if it contains an SMTP MAIL FROM: command, even though the rest of the packet might contain content (e.g., the body of an e-mail).

In pen-mode, it captures and displays lengths of various communications. One concern is that this allows traffic analysis -- for instance, in the case of a user visiting a web site, knowing the length of the objects returned can often be used to identify which web page he was visiting (at least for static HTML content), and this is clearly not authorized in pen mode. (Images, in particular, are quite distinctive that way.)

It also collects and displays lengths of, e.g., Subject: lines in pen mode.

4.3.2

There was very little analysis of different ISP configurations. What versions of DHCP or RADIUS is Carnivore compatible with? What DHCP options does it understand? How likely are the operational changes which may be required? Again, the Earthlink case is a warning.

5.2

We very much agree with the suggestion that separate versions be used for pen-register versus full-content intercepts. Usability in general is a concern, especially given that the default is to collect everything; configuration is a matter of telling Carnivore to exclude certain things.

5.5

It would also seem to be a good idea to capture the entire configuration of the machine after it is used; perhaps they could use a removable hard disk (as their only permanent storage, so that all software, everything would live on it), and after finishing an interception, put the the removable disk under seal.

5.9

"Once Packeteer and CoolMiner have had *all* the software bugs fixed, ..." The possibility of removing all bugs is a bad thing to assume. On the other hand, this software is being used now. It would be preferable to give defense attorneys whatever version is being used, even a buggy one, as that is the the tool used in the cases against their clients.