Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 3, No. 3. April, 2001

Grrr. . . Carnivore: Ethernet Packet Wiretaps

Carnivore is the name given to an FBI system designed to monitor IP packets on ethernet networks. It has become very controversial because it has access to all packets, with selection of relevant packets done by the system.

Many people want to know:
Does Carnivore merely do its job or is it likely to be used to scan through communications that law enforcement does not have legal access to?

Wireless carriers providing data services may need to allow law enforcement agencies to install Carnivore or similar devices at their base stations or at their switch sites or at places where they interconnect to the internet.

Analysis of Carnivore

The Illinois Institute of Technology Research Institute (IITRI — www.iitri.org/home.html) performed a semi-independent analysis of Carnivore under contract to the Department of Justice. Full public review of Carnivore is impossible, because full details of its implementations might significantly reduce its usefulness; these might facilitate the avoidance of surveillance. Their report was published as:
IITRI CR-030-216. A copy of it is available at:

www.usdoj.gov:80/jmd/publications/carniv_final.pdf

Implications for Wireless

Wireless systems are inexorably moving from purely voice systems to mixtures of data and voice. Lawful intercepts of voice are legally available in different ways, most notably by the requirement to adhere to US CALEA legislation, probably using the joint ATIS/TIA J-STD-025 standard. The wireless industry has examined packet data, but it has not as yet produced a detailed solution. As wireless data systems turn more towards IP-based standards, it becomes more likely that law enforcement will take the initiative, and they will provide packaged solutions such as Carnivore.

Wireless monitoring (i.e, over the radio interface) of wireless data is unlikely to occur much; it is simply too inconvenient for most applications. Monitoring will occur within the network where data flows are consolidated, where radio interface encryption has been removed, and where more standard protocols are likely to be employed. This is similar to the situation in J-STD-025, where monitoring of voice is done on the 'back end' of each MSC (Mobile Switching Center) or other types of network elements.

Intercept Concepts

Information about telephone calls is conceptually divided into *call content,* the actual voice conversation, and *call identifying information.* Court orders are either for call content only, or for both call content and call identifying information.

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is $300 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$350 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

We provide discounts to educational institutions and small businesses (less than 10 employees).

Back issues are available individually, or in bulk at reduced prices.

Delivery is by first class mail or by email (Acrobat PDF file).

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due

May 15th, 2001.

Future Topics

IP security • Public Keys & Wireless • Kerberos PKINIT• Public Key Infrastructure (PKI) • IKE • Wireless Data Security • IETF Security Standards • AES (Rijndael)

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone:** 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** http:/www.cnp-wireless.com/wsp.html. **Subscriptions:** $300 for delivery in the USA or Canada, US$350 elsewhere. **Payment:** accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery:** Email or 1st class mail. **Back Issues:** Available individually for $35 in the US and Canada and US$40 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Copies:** Each subscriber is licensed to make up to 10 copies of each issue or back issue. Call for rates to allow more copies.

Upcoming Security Events

The following are several upcoming fraud and security conferences that may be of interest to the wireless security practitioners.

Techno Security 2001
22-25 April 2001
Myrtle Beach, SC
www.techsec.com

Security of Mobile and Wireless Business Applications in Government
April 24, 2001
Washington, DC
(Ronald Reagan Building)
www.marketaccess.org

The ISI forum on Information Security in Government
24-26 April 2001
Washington, DC
www.misti.com/conference_show.asp?id=MI2M

SANS 2001
13-20 May 2001
Baltimore, Maryland
(Hyatt Regency Inner Harbor)
www.sans.org/SANS2001.htm

ctst 2001 - Navigating the Digital Frontier
14-17 May 2001
Las Vegas (The Venetian)
www.ct-ctst.com/CTST2001

Electronic Signatures Summit
31 May - 1 June 2001
London, UK (Café Royal)
www.iqpc.com/cgi-bin/templates/98739215485375976562400002/genevent.html?event=1525&topic

Netsec '01 - Exhibition and Conference
18-20 June 2001
New Orleans (Hyatt)
www.gocsi.com/netsec01

SIM and SmartCard
9 - 12 July 2001
London, UK
www.iir-conferences.com/site/_prodgrp.cfm?DirName=CC0263&ConfCode=CC0263&iv=23

In the US, wiretaps identifying the calling party information are called *Trap and Trace,* and those monitoring dialed digits and other call identifying information *from* a phone line are called *Pen Registers.* Court orders allowing surveillance of call content and call identifying information are known as Title III's.

Surveillance of packet data is based on the same concepts, even though they do not fit quite as well. To emphasize this parallel, we will refer to user data as *content,* and we will refer to information about the packets (e.g, destination) as *identifying information.*

Surveillance usually results in the collection of information that is outside the scope of the court order. This is particularly true in the case of packet data networks. Eliminating the extraneous information is the process of *minimization*

Packet Problems

Monitoring packet data raises legal and technical problems. Traditional voice communications have generally separated voice (call content) from signaling data (call identifying information). Tone based signaling systems generally use the voice facility for signaling as well as for voice transmissions, but generally, signaling occurs during call setup when voice is not being transmitted. Digital signa1ing systems, such as SS7, transmit signaling on dedicated channels which may be physically separate from the voice facilities, and these are certainly treated as logically separate. This has allowed the legal distinction between *call identifying information* and *call content* to be realized in practice without undue technical difficulties.

Packet systems are very different. Packets may contain only identifying information, but they are very unlikely to contain only content. Consequently, it is very difficult to identify packets relevant to a court order, and it is even more difficult to tease apart the identifying information from the content. This problem does not apply to Title III court orders, where law enforcement has a right to the entire packet.

Furthermore, whereas voice systems generally dedicate a single channel to a single user for the duration of a call, packet systems use shared channels, and, worse yet, they do not necessarily send all packets between a pair of users over the same routes. Figure 1 illustrates how transmission of data packets differs from circuit-oriented voice communications.

Another problem to overcome is that most packets do not fully identify the end points of a communication. Protocols like TCP have a set-up phase where a stream is created and identified, with following packets using the much smaller temporary identifier. Although this identification problem also occurs with voice communication, there is always at least one static point in every voice call, which will be traversed by all voice communications during the call. For mobile-terminated calls, this is the incoming switch port on the Anchor MSC.

These problems are increased by the proliferation of protocols in data communications —IP, UDP, TCP, SMTP, etc.

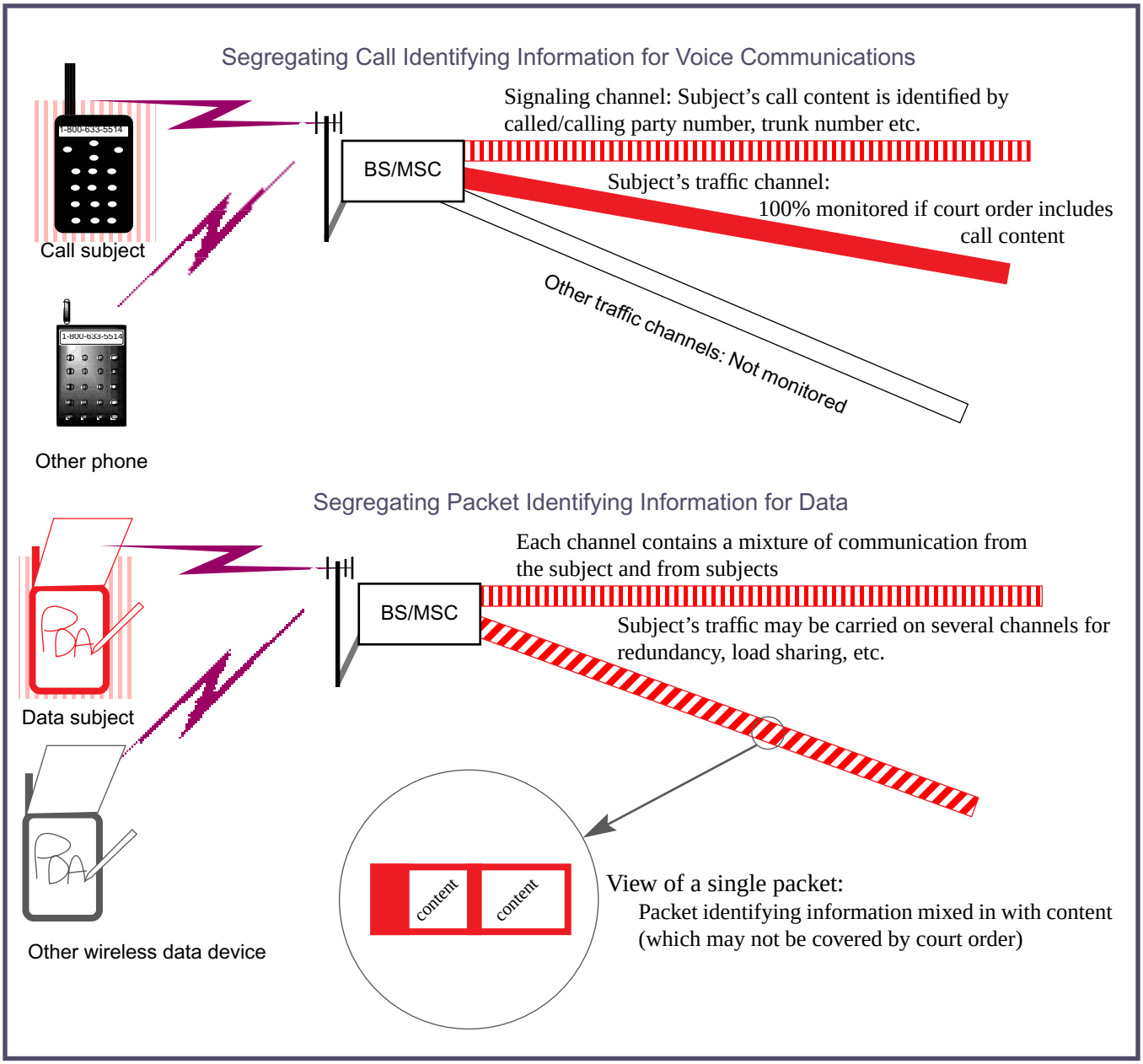
Need for Carnivore

Monitoring packet data requires a great deal of sophistication. Specialized equipment, such as Carnivore, is likely a necessity. It is not essential, however, that the equipment be owned and configured by law enforcement. In the case of CALEA (J-STIJ-025), by contrast, it is more likely the collection equipment will be owned and operated by the telecommunications carrier.

Major Risks

Surveillance requires consideration of a balance of the interests of law enforcement, the judicial system, the subject, innocent people who communicate with the subject, and the public at large. No system will ever be perfect, because of the inherent uncertainty. It is important to remember, for example, that not everyone whose communications are intercepted is guilty of a crime.

Figure 1: Segregating Call or Packet Identifying Information



Some of the major risks with intercept systems are:

- Information which is not covered by the court order may be monitored, which could illegally result in further investigations.
- Law enforcement agents might use the information for their own personal benefit, including criminal activities.
- Communications employees might find out who is being monitored, or worse, they might be able to record the legally authorized monitoring.
- Intercept information transported over a network — often used to centralize the monitoring function — might itself be monitored.
- Information regarding intercepts might be stolen.
- Malfunctions in equipment (such as Carnivore) could result in the wrong communications being monitored.

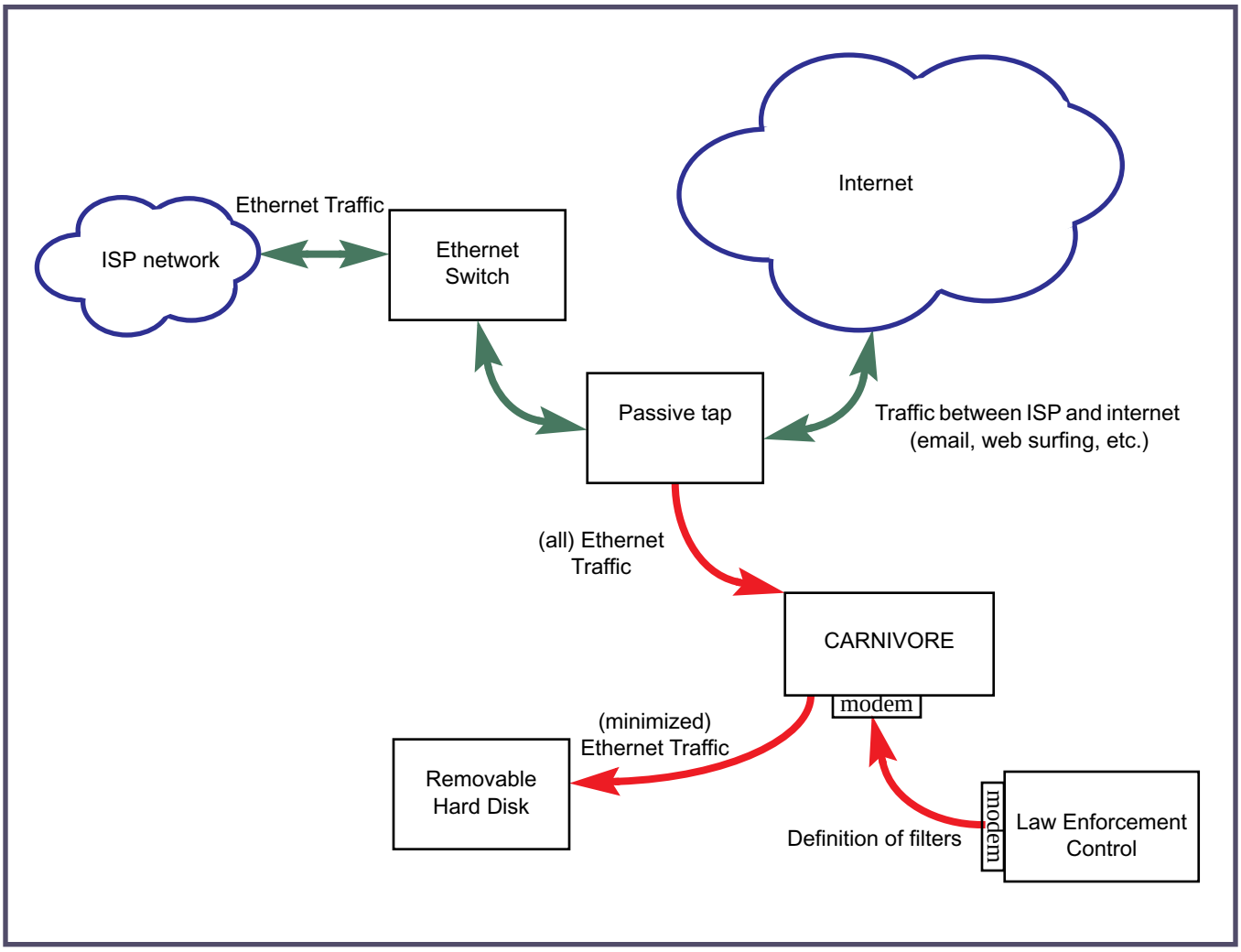
How Carnivore Works

Carnivore monitors traffic on an ethernet network through a 10Mbps/100Mbps passive tap. This allows data to be monitored without disrupting it in any way. Obviously, changes in content would be obvious to most people, but even delays in packets could be detected by sophisticated observers.

Carnivore is controlled by a remote computer using commercial software providing encryption to protect against illegal interception. Monitored data is first minimized; the remainder is stored on a removable disk drive in a locked partition.

Figure 2 illustrates a possible Carnivore configuration.

Figure 2: Carnivore Configuration



Packet Identifying Information

When an intercept is authorized to collect only packet identifying information, Carnivore collects the identity of the sender and recipient, the time, the length of the entire packet and some information regarding the length of individual fields.

Technical Limitations

Carnivore has a number of technical limitations that will mostly result in the collection of too little information, rather than too much:

- Carnivore has significant performance limitations, although these can obviously be reduced by newer versions involving more powerful processors and higher speed links (e.g, 1 Gbps Ethernet).
- Carnivore can only be used to monitor protocols that it supports, which will eliminate some communications from surveillance.
- Carnivore also has no ability to decrypt packets (such as SSL used extensively for e-commerce and m-commerce).
- Loss of packets during overload conditions could result in Carnivore assigning communications to the wrong subject (e.g, when a dynamic IP address is re-assigned).

Strengths of Carnivore

Carnivore can be configured to quite precisely collect information according to the court order. This is a significant improvement over the more manual methods where the minimization may be done with considerable participation by agents, exposing a considerable amount of information to view. This ability does not remove the risk that the humans configuring Carnivore will intentionally or accidentally collect more information than they are entitled to.

ISP network

Carnivore can filter based on a combination of:

- Text strings
- TCP or UDP ports
- IP addresses (static or dynamic)
- e-mail addresses (SMTP or POP3)

IITRI Recommendations

IITRI noted some areas where Carnivore needs to be improved:

- Better auditing is required to ensure monitoring activities can be properly supervised by law enforcement agencies or representatives of the courts. Currently, even the identity of the agent — logged into the Carnivore user interface — is not known.
- Protecting audit logs from modification.
- Preventing carrier personnel from plugging in a terminal and a keyboard to access the system.
- Time synchronization
- Protection against power failures. A considerable amount of buffered data may be lost.
- Filter information is not stored in the log files, so it might be difficult to prove the monitoring query — item(s) being monitored — at any particular time.
- Not all protocols can be monitored, and not all are monitored correctly.
- High throughput (e.g, overly general filters) can easily overwhelm the output capabilities of the removable storage devices.

Surveillance equipment is only a tool within a system. The quality of the system is probably more important than the quality of the tools used. Carnivore makes it possible for surveillance to better achieve goals of the public (e.g, security from unlawful surveillance) and goals of law enforcement (e.g, saving time and money), but those goals will not be achieved if the system breaks down and when the equipment is misused.

Conclusions

Wireless data carriers have a responsibility to cooperate in the surveillance of their customers, when it is legally authorized. They need to ensure employees dealing with surveillance are properly screened, monitored and trained. With Carnivore, there will be an additional need to ensure physical security of the installation, so that unauthorized access is not possible.

Cryptographic News — DSL: Always on ... Always open?

DSL – Digital Subscriber Line is a fast growing technology for telecommuters and small to medium size businesses. It is attractive because of the increased performance – nearly 100 times greater than 56k modems – while using existing copper phone lines. Security has always been a concern with this “Always On” technology - static IP addresses and 24x7 connections are opportunities for hackers. Several network-security experts indicate there are additional things to be concerned with some DSL modems – it may always open. These experts identified multiple vulnerabilities in a DSL modem built by the French telecom-equipment maker, Alcatel. The reports claim that security vulnerabilities include possible unauthorized access and monitoring, denial of service, and permanent disabling of the device.

Researchers at the San Diego Supercomputer Center (SDSC) identified several flaws in Alcatel's “Speed Touch” ADSL modems. One of the problem identified is a “back door” – typically defined as a hardware or software mechanism that:

- provides access to a system and its resources by unusual procedures,
- was deliberately left in place by the system’s designers or maintainers, and
- usually is not publicly known.

The discovered backdoor completely bypasses any passwords users may have set on the device. Intruders (internet based adversaries) can potentially log on to the modem with the user name “expert” and change or delete embedded software.

As always, if a vulnerability appears in one product, other similar products by a manufacturer may also be vulnerable. Alcatel, any word?

Have you checked your DSL modem today?

For more information:

update.informationweek.com/cgi-bin4/flo?y=eDPY0BdB7M0V20Ml70Ai

security.sdsc.edu/self-help/alcatel