acmqueue

Communications Surveillance: Privacy and Security at Risk

As the sophistication of wiretapping technology grows, so too do the risks it poses to our privacy and security.

Whitfield Diffie and Susan Landau

We all know the scene: It is the basement of an apartment building and the lights are dim. The man is wearing a trench coat and a fedora pulled down low to hide his face. Between the hat and the coat we see headphones, and he appears to be listening intently to the output of a set of alligator clips attached to a phone line. He is a detective eavesdropping on a suspect's phone calls. This is wiretapping—as it was in the film noir era of 1930s Hollywood. It doesn't have much to do with modern electronic eavesdropping, which is about bits, packets, switches, and routers.

WIRETAPPING TECHNOLOGY

Scarcely a generation ago, phone calls traveled through wires between fixed locations, encoded as fluctuating electric signals. Now phones are mobile, and, through most of their journeys, phone calls are encoded in bits. Voices are digitized shortly after they leave the speaker's lips, carried over an IP network as packets, and returned to analog for presentation to the listener's ears.

Although big changes in telephony have given rise to equally big changes in wiretapping, the essentials remain the same. The interception and exploitation of communications has three basic components: accessing the signal, collecting the signal, and exfiltrating the signal. Access may come through alligator clips, a radio, or a computer program. *Exfiltration* is moving the results to where they can be used. Collection may be merged with exfiltration or may involve recording or listening.

A phone call can be intercepted at various points along its path. The tap can be in the phone itself, through introduction of a bug or malware that covertly exfiltrates the call, often by radio. The tap can be at the junction box, in a phone closet down the hall, on a telephone pole, or on the *frame* where incoming subscriber lines connect to the telephone company *central office*.

The development in the 1980s of digital switches and the features they made possible created problems for traditional *local-loop* wiretapping. Call forwarding in particular, which diverts the call to a different number before it ever reaches the frame, was problematic. To avoid the possibility of being bypassed, the tap must be placed at or above the level of the diversion. Fortunately for wiretappers, digital switches also introduced conferencing, which allowed several people to converse at once. Taps could be implemented by conferencing in a silent additional party. Taps on analog circuits can, in principle, be detected by the power they drain. Digital wiretaps are invisible to the target but require changes in the programming of the switch rather than extra connections to the frame.

In the 1990s the FBI, claiming that advanced switching technology threatened the effectiveness of wiretapping, persuaded Congress to require that telephone companies build wiretapping capability into their networks. This resulted in CALEA (Communications Assistance for Law Enforcement Act) of 1994.

It is a long way from putting clips on wires to having government standards for electronic

eavesdropping. These changes, made in the name of security, have created risks. How did this come about? Does wiretapping actually make us more secure?

We start with an overview of the convoluted history of wiretapping, focusing on the United States, and then turn to issues of privacy and security.

THE LEGAL SIDE

The telegraph was invented in the 1830s, the telephone in the 1870s. Police wiretapping appeared in the 1890s but saw limited use until Prohibition when the production, sale, and transport of alcoholic beverages were made illegal in 1919. Law or no law, alcohol remained popular, and illegal enterprises grew to serve the demand.

Wiretapping was the perfect tool for investigating crimes such as these that lack victims who complain and give evidence to the police; it performed a search that was invisible and could provide law enforcement with detailed information about the criminal activity. Wiretapping produced search-like results without requiring intrusion into the suspect's property. Was it to be regulated as a violation of the right to be free from unreasonable searches and seizures guaranteed by the Fourth Amendment? Decades were to pass before this question was answered.

In the 1928 *Olmstead* case, the Supreme Court ruled that wiretapping was not a search and therefore did not violate the Fourth Amendment. Following the Federal Communications Act of 1934, which made "interception and divulgence" of wired communications illegal, the Supreme Court changed direction. In a 1937 ruling based on the new law, the court refused to allow wiretap evidence against a bootlegging suspect.

The Communications Act might have put an early end to wiretapping's law-enforcement career, but the Justice Department interpreted the court decision narrowly, permitting interception as long as the results were not divulged outside the federal government. The FBI took advantage of this interpretation to continue wiretapping without court orders—sometimes with Department of Justice oversight, sometimes not—for another 30 years.

The Communications Act said nothing about *bugs*, which listen to sounds in the air rather than signals on wires. This led to an odd split: bugs yes, wiretaps no. Over the decades, the Supreme Court saw less and less distinction. In 1967, in the *Katz* decision, it finally recognized that "the Fourth Amendment protects people, not places." Henceforth, warrants would be as much a requirement of electronic searches as physical ones.

The following year, Congress addressed wiretapping and bugging in Title III of the Omnibus Crime Control and Safe Streets Act, which set out the circumstances under which wiretap orders could be obtained for criminal investigations. Congress saw wiretaps as a particularly insidious search and made the warrant requirements more stringent than those for normal searches (though these have been relaxed somewhat over the years).

In 1978 Congress passed FISA (Foreign Intelligence Surveillance Act), which established a basis for wiretapping quite different from that of Title III. Title III wiretap orders are intended to collect evidence of a crime and require probable cause to believe that the suspect is involved in serious illegal activity. FISA wiretaps are intended to collect intelligence and require that the suspect be an agent of a foreign power or terrorist group.

Title III wiretaps are summarized in an annual *Wiretap Report* produced each year by the Administrative Office of the United States Courts. It lists the prosecutor, judge, crime, number

of intercepted conversations, and number of incriminating conversations. By contrast, except in rare cases in which the evidence they yield is presented in court, only the annual number of FISA wiretaps is made public. There are currently about 2,000 Title III and another 2,000 FISA wiretap warrants each year.

Eavesdropping practices vary from country to country, and since many nations release no information about electronic surveillance, a comprehensive view is hard to attain. Britain did not pass a wiretap law until 1985 when a European Court ruling faulted the country's lack of a clear warrant procedure. A similar European Court ruling in 1990 led to a French wiretapping law in 1991. Both Britain and France report having significantly more wiretaps than the U.S.

Not all wiretaps are a result of official or acknowledged government action. When SMS messaging went awry in Athens in 2005, an investigation found that for 10 months someone had been wiretapping senior members of the Greek government. The eavesdropping appears to have been stopped after it was discovered. Although no information has surfaced about who did the wiretapping, a good bit is known about how it was done. The 1994 CALEA law requiring telephone systems to be wiretap ready applies only to switches installed in the U.S., but since manufacturers try to have as few versions of their products as possible, it has had worldwide impact. When the Greek Vodaphone network purchased a switch from Ericsson, it didn't order wiretapping capabilities; wiretapping software was present in the switch but was supposed to be shut off. In particular, auditing software that would have been operating if the wiretapping feature had been ordered was not present. When unknown parties turned some of the wiretapping features on, their actions went unrecorded.

WIRETAPPING WITHOUT A LEGAL FOUNDATION

The Greek case wasn't the only warrantless wiretapping uncovered during that period. In 2005 the *New York Times* revealed that the U.S. government had been wiretapping communications to and from the U.S. without a warrant. After the passage of FISA, NSA (National Security Agency), America's foreign-intelligence eavesdroppers, had been forbidden to listen in on radio communications inside the U.S. without a warrant unless at least one end of the communication was outside the country and the internal end was not a targeted "U.S. person." Interception of purely domestic communications within the country always required a warrant. As more messages came to travel by fiber-optic cable and fewer by radio, NSA was forced to turn to other, not necessarily legal, approaches.

The vast American investment in communications infrastructure makes it economical for parties in other parts of the world to route their calls through the U.S., and this *transit traffic* seems a reasonable foreign intelligence target. When transiting communications were in the form of a radio signal that could be intercepted from U.S. soil, it was not difficult for NSA to determine what was transit traffic. When traffic moved to optical fibers and IP-based communications, separating out the transit traffic, which could be eavesdropped upon without a warrant, became more difficult. That was one concern. There was another.

In the post-9/11 anti-terrorist climate, some government elements wanted a substantive change, permitting warrantless interception of communications in which one end was "reasonably believed to be located outside the United States," regardless of the status of the U.S. end. Interception was placed not at the cable heads where calls entered the country, but at switches carrying both internal and transit traffic. This meant that purely domestic calls were likely to be intercepted as well.

A technician at an AT&T switching office in San Francisco leaked documents showing that a fiber-optic signal at the office was being split: a copy of the signal went into a "secret room," where it was analyzed and part of its contents sent elsewhere for further analysis. The leaked documents—whose authenticity was confirmed by AT&T during a subsequent court case—reveal that the San Francisco office was only one of a number of offices set up this way.

From the wiretapper's viewpoint, the end of the rainbow would be the ability to store all traffic, then decide later which messages were worthy of further study. Although this is usually not feasible, storing the transactional information about telephone calls—calling and called numbers, time, duration—is. These CDRs (call detail records) are routinely retained by the carriers who use them for planning and billing purposes. Law enforcement had previously been able to obtain call details—in police jargon *pen register* and *trap-and-trace*—collected in response to court orders targeted at individual phones. By comparison, the CDR database provides information on all the subscribers over long periods of time, a rich source of information about customer activities, revealing both the structure of organizations and the behavior of individuals. Several telephone companies appear to have surrendered them in response to government pressure without demanding court orders.

WIRETAPPING IN AN IP-BASED WORLD

Internet communications cannot be effectively exploited using the facilities of traditional telephony, so as early as 2000 the FBI developed a tool for wiretapping at ISPs. The tool—initially named Carnivore but eventually given the less menacing title DCS-3000—examined packets passing through the ISP and copied those that met intercept criteria stored in internal tables. The tables were set through a remote connection to the FBI's own offices. Surprisingly for law enforcement, which places great store on the chain of custody of evidence, Carnivore had little provision for auditing and overall poor internal security. Rather than having a separate name and password for each user, it relied on a single shared login. More significant from a privacy standpoint, Carnivore bypassed the traditional process of wiretapping in which the court issues an order but the carrier's personnel execute the order. This gives the carrier both the obligation and opportunity to challenge the order in court if it believes the order to be illegal. When the order is implemented by a message sent directly from the FBI to the Carnivore box, this additional layer of oversight is lost.

In parallel with its technical activities, the FBI worked to extend wiretapping law to the Internet. CALEA had been passed with an exemption for "information services" (i.e., the Internet), and with the rise of VoIP (voice over IP), the FBI feared it would lose an important investigative tool. VoIP comes in many flavors, from the peer-to-peer model employed by Skype to others in which the path between the subscriber and the telephone central office is traditional telephony but IP communications are used throughout most of the call's path.

The FBI began slicing the salami with the "easy" cases in which VoIP communications behave most like traditional phone calls, and it was successful in getting the courts to agree to this extension. Most IP communications, however, do not behave as telephone calls; peer-to-peer VoIP systems, for example, use a centralized mechanism to provide the communicating parties with each other's IP addresses but rely on the Internet for actual communication. In this scheme there is no central point at which a wiretap could be authorized. If regulation were to require that IP-based communications adopt a centralized architecture like the telephone network, the innovation that is the engine of high-tech industry could be stifled.

In 2007, Congress legalized warrantless wiretapping; in 2008, it went a long step further, not only legalizing new wiretapping practices but also giving retroactive immunity to telephone companies that had colluded with the government in performing warrantless electronic eavesdropping. The FISA court previously had reviewed individual warrants; now certain classes of wiretaps would not be reviewed individually but conducted under procedures reviewed periodically by the court.

WHITHER PRIVACY

At the time the U.S. wiretap laws were passed, realtime access to transactional information of who was talking to whom and when was not easy to acquire. Modern switching technology introduced in the 1980s changed that, and police hungrily pursued the investigative possibilities. Because transactional data—phone number, time of call—are analogous to the information on the outside of a letter, access requires only a subpoena, which is much easier to obtain than a wiretap warrant. Whom you talk to and when may be less intimate than the transcripts of your conversations but can reveal a great deal about you. When your spouse calls you from the office in the late afternoon, do you frequently respond by calling a certain number? Perhaps when you learn your spouse is working late, you let someone else know you are free.

In a cellphone world people are constantly at their telephones. Not only do they make more calls, but they also reveal more information: times and numbers are joined by location in the transactional record. In an Internet world, each connection to a Web site is a transaction. Even though a query string is not transactional data, the sites visited after the search engine frequently make the character of the query clear.

Curiously, the greatest threat to privacy may not be snooping on people but snooping on things. We are moving from a world with a billion people connected to the Internet to one in which 10 or 100 times that many devices will be connected as well. These range from the much-discussed smart refrigerator that knows when it is time to order more milk to RFID (radio-frequency identification) tags in products that enable the tracking of where the goods are located before, and perhaps after, retail sale. Particularly in aggregation, the information reported by these devices will blanket the world with a network whose gaze is difficult to evade. The future of privacy will depend on a combination of legal and technical measures by which device-to-device communications are protected.

WHITHER SECURITY

It is not just privacy that is at risk under the new regime, it is security as well. National security is much broader than simply enabling intelligence and law-enforcement investigations. Although undertaken in the name of national security, building wiretapping into our telecommunications system may be a greater threat to that security than the spies and terrorists against whom it is aimed.

First and foremost, information security means protecting public and private computing and communications systems against attacks from both inside and outside. It was the need for that type of protection that caused the European Union in 1999 and the U.S. government in 2000 to relax their export controls on strong cryptography, a change that bolstered the security of Internet communications.

A network may be designed to provide security to its individual users against everything except authorized intrusions by the network itself, a plausible goal for a DoD (Department of Defense) network. Such a model requires centralization of authority that is possible for DoD, and might have

been possible for the Internet in 1985—when it was a U.S. project—but is not feasible now.

The Internet has become essential to modern life. Business and personal communications—and even critical infrastructure—rely upon the network to function. Yet the combination of attacks on the network and on network hosts means that we are increasingly reliant upon an unreliable network.

A number of efforts are under way to improve this, from the use of SSL (Secure Sockets Layer) to protect Internet commerce, to the deployment of IPsec (Internet Protocol security) to protect any IP communication, to the implementation of DNSSEC (Domain Name System Security Extensions) to protect the domain-name system. Research is occurring in both Europe and the U.S. on secure Internet protocols and such plans as expounded in the recently released White House *Cyberspace Policy Review.*

The unauthorized use of wiretapping facilities in the Greek Vodaphone system shows one level at which surveillance facilities can be misappropriated. NSA's activities under the Bush administration show another. FBI expansion of its wiretapping authority beyond what was originally envisioned in CALEA shows a third.

Building wiretapping capabilities into communications infrastructures creates serious new risks. The complexity that wiretapping introduces led the IETF (Internet Engineering Task Force) to conclude that it should not "consider requirements for wiretapping as part of the process for creating and maintaining IETF standards" (RFC 2804).

The surveillance we are attempting to build may increase security in some ways, but it also creates serious risks in a network infrastructure that supports all of society. Given the importance of the Internet to society—and given the importance the network has in communications between people and their friends, governments and their citizens, businesses and their customers, and in all of society—communications security is critical, and that should take precedence in the debate over communications security versus communications surveillance. Q

LOVE IT, HATE IT? LET US KNOW

feedback@queue.acm.org

WHITFIELD DIFFIE is a visiting professor in the Information Security Group at Royal Holloway, University of London. For nearly two decades Diffie worked at Sun Microsystems Laboratories, where as Chief Security Officer he was the chief exponent of Sun's security vision and responsible for developing Sun's strategy to achieve that vision. He is best known for his discovery of the concept of public key cryptography and has spent many years of his career working on the public policy aspects of cryptography. He and Susan Landau are joint authors of the book *Privacy on the Line* (MIT Press), which examines the politics of wiretapping and encryption.

SUSAN LANDAU is a Distinguished Engineer at Sun Microsystems Laboratories, where she works on security, cryptography, and policy, including surveillance and digital-rights management issues. She serves on the Commission on Cyber Security for the 44th Presidency, the editorial board of IEEE Security and Privacy, and as a section board member of the *Communications of the ACM*; she previously served for six years as a member of the National Institute of Standards and Technology's Information Security and Privacy Advisory Board. Landau is the recipient of the 2008 Women of Vision Social Impact Award, a AAAS Fellow, and an ACM Distinguished Engineer.