CALEA, Carnivore, and Countermeasures

Introduction 19

Information warfare is a term used by the military to describe conflict wherein the battlefield is a nation's information infrastructure. Most governments are preparing contingency plans for this sort of attack. The very plans they are preparing are, in effect, acts of aggression against the people outside their country and often against their own citizens. The defense is communications intelligence and it is, in effect, a weapon against individual liberties, privacy, and intellectual property.

The title of this talk, CALEA, Carnivore, and Countermeasures, refers to recent developments in United States domestic policy, that mirror worldwide trends in aggressive and pervasive growth in official and unofficial intelligence gathering. CALEA is the Communications Assistance for Law Enforcement Act, which grants unprecedented access to private communications. Carnivore is a tool developed by the US Federal Bureau of Investigation to exploit that access.

It can be safely assumed that every country in the world has implemented some digital information gathering program. Some of the better known ones include the FBI's Carnivore, Britain's GTAC, and Echelon, headed by the UK and the USA with junior members Australia, New Zealand, and Canada.

In general, more is known about the state of government sponsored surveillance than corporate surveillance which, without regulatory oversight, is certainly far more extensive, though usually in the guise of "marketing research" or competitive analysis.

Individual surveillance of other individuals or organizations is assuredly the most extensive and the least observed or documented of all spying activities. If one considers every activity from open source harvesting such as credit reports and usenet postings to intercepting or stealing personal mail, one feels very naked indeed. 9

However, protecting an individual or organization is neither difficult nor expensive. What is required is a change in basic attitude, a shift from a presumption of anonymity and confidentiality to the assumption that the Internet is a public place, with a permanent memory of only the things we wish were forgotten, that we are surrounded not only by friends but also foes who will use any slip against us.

The purpose of this talk is to present an overview of the state of surveillance in the world today, to introduce some of the many threats to data, some overt, most covert, to introduce and to highlight the value of security in a very insecure world.

The Eyes of Governments 8

Governments recognize it is nearly impossible to win a technology race against a world of hackers, hackers who fit no universal profile, fall into no specific categories. What good are guns when the technology needed by rebels in Kurdistan to shut down the Russian military communications links is developed by a ten year old in Bangladesh and known world-wide hours later?

The only way to stop such threats is to catch them as soon as possible. The military is at a disadvantage, but the only hope they have is to catch the exploit at least as soon as the Kurdistani rebels do, so they are not blindsided by a communications blackout or worse.

Therefore governments can turn only to universal surveillance. They must watch everything, or as near to everything as they can. Even if one were to assume that governments were not targeting their own citizens, every citizen will ultimately be subject to extra-national surveillance by just about every other country in the world. In general these methods are covert, often in violation of existing domestic and international law; it is naive to believe that intellectual property will be respected.

Legislative Developments [6, 16]

Governments, especially elected bodies, tend to be sensitive to the impression that they are violating their own rules. Typically there is a presumption that the legitimacy of the government is related to the degree by which it complies with the law it is charged to enforce. Most countries in the pre-digital era had rules which limited the government's right to access citizen's private information. Transgressions of these laws were generally easy to recognize as they required an agent of the government to physically retrieve some piece of personal property on which was kept personal information. It was therefore not the information, per-se, that was being protected as much as the citizens right to physical property.

The advent of the telephone provided an entirely new sort of intelligence channel. Law enforcement found this too tempting to resist, as have communities of radio phreaks, cell phone scanners, and all manner of equally prurient pursuits. Wiretaps became a common method of gathering intelligence, and while this information was rarely critical in prosecuting criminal cases, it was just too much fun not to gather. While intelligence gathering is an ancient art, the modern version reached maturity during WWII. Many critical events of the war can be traced to either success or failure of secrecy.

The development of packet switched communications, and the displacement of circuit switched channels has created difficulty for law enforcement in their efforts to continue and increase access to private communication. These channels, though difficult to tap, carry ever more, and ever more valuable information.

Law enforcement has more or less universally requested and more or less universally been granted access to packet switched networks. But because of the difficulty of pulling useful data off any single wire, law enforcement asked for access to the switch itself. New laws in the US and elsewhere require equipment manufacturers to make a ground breaking change in the design of their equipment: not only would law enforcement be granted access, but the equipment would be *designed* for that access.

Specific Laws

Many countries have passed or are considering legislation to make surveillance easier and more comprehensive. A common characteristic of these laws is that they address specifically the packet switched nature of the Internet, wherein information is sent in coded packets over multiple parallel paths. In this way the laws merely extend the same capabilities law enforcement had in monitoring circuit switched networks into a packet switched environment.

Another characteristic is that these new laws require everyone involved in the conveyance of information to ensure that their equipment is designed to provide law enforcement access to this data. A design requirement that bears some cost, the cost borne by the consumers of the technology. That is: part of our phone bill goes to paying for equipment to make it easy for law enforcement to listen to our conversations.

United States: CALEA 12, 13, 24, 27, 29

US laws generally have a formal title and a "short" title. the short title is often a very thinly veiled political statement. The Communications Assistance for Law Enforcement Act is formally titled Interception of Digital and Other Communications. The preamble defines the purpose as "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes."

The law, as interpreted by the FBI, requires all companies providing telecommunications services in the United States to install remote control ports on their routers which allow law enforcement, acting autonomously and remotely (though theoretically only on a warrant) to easily extract any conversation in it's entirety, up to 1% of the hub's total traffic simultaneously. This capability must have been implemented by 1998, unless a waver until 10/24/2000 was granted.

Given a large installed base of equipment, there was a controversial element of cost involved. The FBI played down the cost, asking congress to allocate $500 million. The FBI admits now that the cost may be 4-8 times that high. Industry estimates the cost at $10 Billion.

Congress was convinced to allocate the original FBI estimate out of tax revenues, meaning the cost of implementation is borne by taxpayers. The difference in implementation cost is borne by customers of communication services.

Britain: RIP 10, 14, 15, 20

RIP, the Regulation of Investigatory Powers is, according to the Guardian, "the most pernicious invasion of privacy ever imposed by a modern democratic state. Under its terms, every UK internet service provider will have to install a black box which monitors all the data passing through its computers and feed this to MI5 headquarters."

The Guardian is not understating it. RIP goes far beyond CALEA in scope. First CALEA specifically exempts ISPs, many of which are small operations. RIP's application to "any system... which exists (either wholly or partly in the United Kingdom or elsewhere)" pretty much covers everyone under British law.

In keeping with the practice and intent of existing surveillance, RIP specifically allows "the interception of external communications." Everything you send to or *through* Britain is subject to surveillance under the law. Unfortunately the IP protocol doesn't have a header for "avoid Britain" and your packets could be routed through Britain at any time whether you intend it or not.

In a very clever move, RIP states that all acquisition must be permanently secret. If a telecom provider is served with a warrant, they may not, under penalty of law, tell anyone about the warrant, ever. There can be no public check on the use of this surveillance program because the public can never know its scope.

Traffic data is not subject to a warrant. This data can be extremely sensitive, but is dismissed as statistical. Data such as every web site you visit, everyone you correspond with, every newsgroup you check out, every download. All of this is available to anyone in law enforcement should they choose to look.

Under RIP, encryption keys must be made available to *any agency* that asks, or for a person under suspicion for *any crime*. Failing to hand over keys, or failing to be able to remember codes for keys makes the forgetful person liable for up to two years in prison.

Canada: Longitudinal Labor Force File

On May 29th, Canada closed it's "Longitudinal Labor Force File." It was a huge and secret database that was collated by Human Resources Development Canada, containing approximately 2000 critical bits of information on every Canadian.

The information was collected from various sources available to different government organizations including the Tax Board, federal job data, insurance filings, welfare files, and the social insurance master file.

India: Information Technology Bill

India passed it's information Technology Bill on May 16. In the draft version, there was a provision which would have mandated that cybercafes keep detailed records of their users and their user's activities. That was dropped, but a provision that allows warrantless searches by the deputy superintendent of police passed.

Australia: TILAB 2000 [25]

Australia's Telecommunications (Interception) Legislation Amendment Bill 2000 was passed on June 7th. It creates a new "named person" warrant whereby law enforcement need only request permission to track a person, not a more rigorous requirement that they identify why, and where they will track the person.

The bill also creates a special "foreign communications warrant" which permits the interception of communications crossing Australia's border "for the purposes of collecting foreign intelligence."

Germany: In Contrast [17]

Germany, in contrast, may be the only country other than Sealand to unequivocally advocate encryption. Germany, beyond simply protecting civil rights, sees encryption and effective privacy as central to it's national strength and more a way to prevent crime than a path to commit it. It is perhaps indicative of the German government's inclination to view its population as citizens rather than merely consumers and criminals.

The German Federal Ministry of Economics and Technology released a document titled Key Elements of Germany's Encryption Policy in June 1999.

> *Based on the national debate to date and on international developments, the Federal Government herewith adopts the following key elements for its encryption policy:*
>
> *1. The Federal Government has no intention of restricting the free availability of encryption products in Germany. It regards the use of secure encryption as a decisive prerequisite for data protection for the public, for the development of electronic business transactions and for the protection of company secrets. The Federal Government will thus actively sup-*

port the spread of secure encryption in Germany. This particularly includes the promotion of security-consciousness among the public, in the economy and in the administration.

2. It is the aim of the Federal Government to strengthen the confidence of users in the security of encryption. It will therefore take steps to establish a framework of confidence for secure encryption, specifically by improving the verifiability of the security functions of encryption products and recommending the use of tested products.

3. For reasons relating to the security of the state, the economy and society, the Federal Government considers it indispensable that German manufacturers be capable of developing and manufacturing secure and powerful encryption products. It will take steps to improve the international competitiveness of this sector.

4. The spread of powerful encryption procedures must not undermine the statutory telecommunications surveillance authority of the criminal prosecution and security authorities. The responsible Federal Ministries will therefore continue to monitor developments closely and report on this subject after two years. Independently of this, the Federal Government will support the improvement of the technical competencies of the criminal prosecution and security authorities within the framework of its capabilities.

5. The Federal Government attaches great importance to international cooperation in the field of encryption policy. It advocates open standards and interoperable systems developed in the market and will support the strengthening of multilateral and bilateral cooperation.

Organizational Threats 11, 18, 22

Just about every country in the world maintains some level of electronic surveillance, typically under the management of that country's traditional foreign intelligence agency. Each of these organizations sees every other country's citizens, ally or foe, as a source of potentially critical information. Every one of us is likely to be monitored by any or all of these organizations. Some of the more prominent include the following.

UK/USA, NZ, Canada, Australia: Echelon 23

Echelon is perhaps the best known and broadest secret monitoring agency. Echelon is a cooperative venture, borne out of the joint efforts and successes of the United States and the United Kingdom in breaking codes and gathering information during World War II. The post war collaborative program was created by secret agreement in 1947. The lead agency for the US is the NSA, with support from the military and parts of the CIA. Later, Australia, Canada and New Zealand joined.

Echelon's goal is to monitor *all* global communications extra-national to the member nations. The scope of the program is huge, and includes monitoring of every possible communications medium. The only media that pose some exceptional difficulty are fiber optic communication and, apparently, irridium phones, due to the handoffs between LEO satellites.

Part of echelon's resources include rather large satellites, as long ago as 1985, huge unfurling parabolic antennae were put into orbit. Satellites of the class MAGNUM and ORION are capable of directly monitoring cellular communications.

Unsubstantiated rumors suggest that every international communication is monitored and that keywords are detected automatically and conversations thereby chosen for analysis. If true, it suggests an attack against the system: flooding communication with probable keywords.

Britain: MI5 - GTAC [28]

Britain's secret service is known as MI-5. Between RIP, discussed above and GTAC, the new central monitoring station which is part of the physical implementation of RIP, MI5 may be the most aggressive national spying organization in the world.

Russia: SORM-2/FAPSI [7, 26]

Russia's SORM, or System of Operative and Investigative Procedures, has followed the lead of the US and Britain and now requires that ISPs provide direct taps to their switch equipment. This ensures that all information passing through can be monitored. Russians have responded with more resistance than Britain or the US, as memories of the KGB are fresh there. Russia's efforts are also undermined by the regular appearance of captured information in blackmail sagas, keeping the risk fresh in the citizens minds.

Echelon group, Hong Kong, :ILETS

The International Law Enforcement Telecommunications Seminar is an organization founded by the FBI in 1993. Members include Australia, Canada, Hong Kong, New Zealand, Norway, and the United States. Little is known about ILETS except that it's goal is to provide a forum for law enforcement agencies of the member countries to establish guidelines to ensure access to intelligence and has apparently served a significant role in the creation of laws mandating switch level taps.

Another purpose of the organization was to promote the US policy regarding key escrow worldwide, a policy that has not been entirely abandoned despite the spectacular failure of clipper.

US: NSA, FBI, CIA, DIA, etc.

The United States maintains a veritable alphabet soup of organizations spying on just about everything.

The basic breakdown is that the NSA (or National Security Agency) is responsible for national security and the collection and dissemination of foreign intelligence.

The CIA (or Central Intelligence Agency) is responsible for foreign intervention and ground level foreign intelligence.

The DIA (or Defense Intelligence Agency) is the military's intelligence and spying organization.

The FBI (or Federal Bureau of Investigation) is responsible for federal domestic crimes.

Typically it is known that the FBI spies on citizens. In general it is scandalous when the CIA does, though it happens regularly, especially *when monitored citizens leave the country.*

Neither the NSA nor the DIA generally tip their hands, but both are known to operate domestically. The NSA most flagrantly in the design of domestic cryptographic tools such as clipper, and the DIA far more covertly in investigating developments in Encryption technology.

Technology Threats

Carnivore - The FBI's "power" sniffer.

Carnivore is the FBI's highly controversial hardware implementation of a packet sniffer. Carnivore has been installed at several ISPs in response to CALEA requests by the FBI. It is a high performance packet sniffer capable of sorting through all the header information that passes through a large sized ISP. Complaints against it center around it's capability of extracting and storing body information as well, and that the device, in effect, spies on every customer of the ISP being monitored.

GTAC - MI5's central sniffing facility.

MI5 recently unveiled a plan for a facility within it's London headquarters called the Government Technical Assistance Center or GTAC. It is a national strength version of Carnivore, capable of sorting the entire country's correspondence. The facility will cost MI5 almost $50 million, but the cost to ISPs to implement the hardwire tap will be much higher. The center is also said to be able to decode encrypted messages, but the provision in RIP requiring the submission of keys on request suggests that MI5 does not expect to be able to break strong encryption.

Anyone doing sensitive business which might pass through Britain would be well advised to use strong encryption. So far, neither Britain nor the United States have claimed the right to extra-territorial enforcement of anti-privacy laws.

Van Ecks Monitoring - Capturing lost data.

Van Ecks monitoring is an interesting method whereby a sensitive antenna is used remotely to pick up standard emissions from electronic equipment, and by proper processing extract useful information. The most dramatic example is picking up flyback signals from a TV monitor, restoring sync, and replicating the image remotely. Since it is passive detection, it is very hard to defend against.

It is not a new technology, and the US military has a standard called Tempest for equipment that is resistant to it, basically controlling unintentional emissions.

In open source, it is only known that tempest monitoring can be accomplished relatively locally by a high gain antenna. It is interesting to consider the possibility that satellites could be used for long range Van Ecks monitoring. Though I can't imagine it being selective, it would more or less bypass the whole debate on cryptography and line tapping systems.

Packet Sniffing - Who's on your LAN?

Packet sniffing is the core technology of Carnivore. Over most LANs the traffic for the entire LAN or at least the local loop, travels in clear text and is quite easily extracted. Sniffing at a entrance router captures all the local traffic.

Cookies, bots, and browsing habits.

Cookies and bots are used to track browsing habits. This data is usually collected somewhat covertly and usually to target advertising of some sort. The potential for damage is very high. A users's cookie collection typically reveals far more than the user would intend. Bots often track browsing habits, compiling a view of the user that might not be relevant or reasonable or fair, and is most basically non-consensual. Marketing teams have found browsing habits to be invaluable sources of information; it seems likely that governments will to (or do).

Countermeasures

Given the vast range of resources being applied world wide it should be apparent that it is not possible to do business without using monitored channels. The prudent businessman assumes every fax, email, phone call, etc. is monitored sometime between the moment it leaves the local environment and before it arrives at it's destination.

In general, the protocol used to protect oneself is more important than the core technology. Correctly implementing DES with it's breakable 56bit key is far more secure than incorrectly implementing 3DES, with it's practically unbreakable 129 bit effective key length. At issue is that most implementations are dramatically flawed.

Usually the flaws are in the form of foolish key management: many security programs encode the key weakly in the cyphertext at some predictable point which makes key recovery possible if the user forgets his password... or to anyone who knows the secret. Other failures include using server side encryption, for example password hashing usually happens on the server, the password itself being transmitted in the clear over the LAN or WAN.

Typically users encrypt only critical communications, flagging those communications as important to anyone looking. If you do not choose to encrypt everything, what you do choose to encrypt is very interesting. Encrypting everything with a very weak key is more effective than encrypting a few things with a very strong key. If those few things indicate potentially valuable data, it is easy to track their destination and use various means to extract the content.

There are a small number of companies, including my own badabiz.com and hushmail, that have implemented moderately rigorous end to end encryption in a client-server environment via client side encryption and server "common carriage". While many applications manage this in traditional "heavy" applications, most "secure" client-server applications trust in the reliability of firewalls.

Ultimately the buyer bears the burden of understanding the value and real strength of any security measures they implement. The most difficult challenge any organization faces is responsible, universal implementation. Even the best software, the best protocols, are most often defeated by carelessness.

Examples of Use [21]

An Extremely well written document, *DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION,* Contains a short list of confirmed examples wherein information acquired by government agencies regarding foreign nationals was disseminated for domestic economic gain, and to the detriment of the surveilled party.

Thomson CSF and Brazil

In 1994, NSA intercepted phone calls between Thomson-CSF and Brazil concerning SIVAM, a $1.3 billion surveillance system for the Amazon rain forest. The company was alleged to have bribed members of the Brazilian government selection panel. The contract was awarded to the US Raytheon Corporation - who announced afterwards that "the Department of Commerce worked very hard in support of U.S. industry on this project." Raytheon also provide maintenance and engineering services to NSA's ECHELON satellite interception station at Sugar Grove.

Airbus Industrie and Saudi Arabia

According to a well-informed 1995 press report: "from a commercial communications satellite, NSA lifted all the faxes and phone calls between the European consortium Airbus, the Saudi national airline and the Saudi government. The agency found that Airbus agents were offering bribes to a Saudi official. It passed the information to U.S. officials pressing the bid of Boeing Co and McDonnell Douglas Corp., which triumphed last year in the $6 billion competition."

International trade negotiations

Many other accounts have been published by reputable journalists and some firsthand witnesses citing frequent occasions on which the US government has utlitised communications intelligence for national commercial purposes. These include targeting data about the emission standards of Japanese vehicles; 1995 trade negotiations the import of Japanese luxury cars; French participation in the GATT trade negotiations in 1993; the Asian-Pacific Economic Conference (APEC), 1997.

Targeting host nations

The issue of whether the United States utilizes communications intelligence facilities such as Menwith Hill or Bad Aibling to attack host nations' communications also arises. The available evidence suggests that such conduct may normally be avoided. According to former National Security Council official Howard Teicher, the US government would not direct NSA to spy on a host governments such as Britain: "[But] I would never say never in this business because, at the end of the day, national interests are national interests … sometimes our interests diverge. So never say never - especially in this business."

Conclusion

Surveillance is used constantly to advance national interests, at the expense of other nations. In most countries, official surveillance is not directed at citizens of that nation. In general the activities of the spy organizations is directed against suspected direct and economic threats from outside it's boarders. This information is rarely disseminated outside highly secure channels in any direct way, as to do so would be to compromise the detection means.

However, just because your private personal or business correspondence does not turn up where you can find it does not mean that it isn't being read, and that the information contained therein is not regularly being used to advance interests other than your own.

The very public actions of governments to increase the availability of intelligence information have, more than any hacker's actions, created the market for strong security products. There are many such

products on the market, and people who can properly implement them. We all have a need to make correct use of these products to protect the interests of our companies. But we also have an obligation: if the success of the controversial and expensive programs described in this paper were significantly undermined by universal encryption, it is likely that they would lose the support they have.

The threats created by government spying are the most pernicious. And the most dangerous of these are changes in legislation which force weaknesses to be built into communications systems. These weaknesses, once installed, become a long term part of the communications infrastructure. Once they are installed it will be very difficult to remove them.

Governments have not, in general, showed their trustworthiness. While it is reasonable to assume that your government is sincere, that the laws it passes it does really intend to strengthen national security and domestic tranquility; it shows a profound ignorance of history to be willing to take the risk that you government will always use its power that way. The twentieth century was littered with the corpses of people killed by governments that used personal information to marginalize or scapegoat entire populations.

Our governments are ultimately accountable to us, and we each have a responsibility to ensure that our own government acts in an ethical and trustworthy manner. The risk should we fail is tremendous.

Sources

(All sources are linked)

1. Electronic Privacy Information Center
2. Privacy International Organization
3. Foundation for Information Policy Resarch
4. The Internet Society of England
5. American Civil Liberties Union
6. 1997 encyption developments.html
7. ABC report on Russia's SORM-2.html
8. ACLU report on SEC snooping.html
9. bodysearch.gif
10. British Home Office RIP report.pdf
11. EPIC infrastructure and civil liberties.pdf
12. EPIC's CALEA brief.pdf
13. Federal Register, FBI report on CALEA.pdf
14. Guardian report on RIP.html
15. ISOC RIP analysis.html
16. ISP copyright liability-Mike Harrington.html
17. Key Elements of Germany's Encryption Policy.pdf
18. OTA report Electronic surveillance in a digital age.pdf
19. RAND report on strategic information warfare.html
20. STAND's Guide to the RIP bill.html
21. STOA report on econmoics of interception.pdf
22. STOA report on interception and abuse.pdf
23. STOA report on surveillance and ECHALON.pdf
24. techweb report on CALEA.html
25. text of austrialian telecommunications bill.html
26. Text of SORM laws.html
27. Text of the Calea Law.html
28. Times report on MI5 snooping.html
29. Wireless magazine report on CALEA.html