Global Information Assurance Certification Paper

USA PATRIOT Act of 2001: Uncuffing Law Enforcement in the Battle Against Cyber Crime

I spoke recently with an official from my local police department, asking him just what were the difficulties being faced by law enforcement in battling cyber crime. Frankly, I was stunned by what I was told.

Law enforcement has been so incredibly hamstrung by out-dated laws and statutes that until the recently-enacted USA PATRIOT Act was passed, involving the police in the investigation of an ongoing computer trespass was about the LAST thing you'd ever want to do.

Case in point: Let's pretend, for the sake of discussion, that I manage the security of a local company's network. This network is attached to the Internet, and has appropriate perimeter defenses and intrusion detection equipment. One day, the Intrusion Detection System (IDS) alerts me to an unauthorized access to a system, and my countermeasure systems begin recording the traffic to and from the trespasser. If I were to call law enforcement for assistance in stopping and/or catching this perpetrator, I would be prevented BY LAW from further monitoring of this individual, even though the traffic is flowing on my own network.

I would have had to immediately cease my monitoring and tracing activities until I (or the law enforcement official) acquired a warrant and/or a wiretap order from my local court.

You see, once I made the call to Law Enforcement, and they advised me in any way, I became an Agent of Law Enforcement, and my abilities to monitor my network were severely curtailed. I suddenly needed a court order to monitor the traffic on my own network.

If a burglar breaks into my office in the middle of the night and makes off with my files, do I not have every right to enlist the services of my local law enforcement officials in apprehending the criminal? Why is it any different if they come in through the Internet? The damage done is just as real, is it not?

In his book "*Are We Overprotecting Code? Thoughts on First Generation Internet Law*", Orin S. Kerr observes correctly that an anomaly in the law has been created, where "a computer hacker's undeserved statutory privacy right trumps the legitimate privacy rights of the hacker's victims."[1]

There have been other issues hampering law enforcement's ability to fight cyber crime. Let's look at the state of things pre-PATRIOT:

[1] Kerr, Orin S., "Are We Overprotecting Our Code? Thoughts on First-Generation Internet Law", Wash. & Lee L. Rev. 1287, 1300 (2000)

Jurisdiction Issues

- Local courts could only authorize wire taps within the jurisdiction of the court. That is to say, if a court in Seattle Washington ordered the monitoring of data from a laptop that suddenly dialed up from New York, law enforcement would have no jurisdiction to execute the wire tap. Law enforcement would be required by law to acquire wiretap orders and search warrants from every individual carrier involved in the transmission. And given the lengthy effort and time requirements of obtaining such permission, this was seldom a viable method of collecting intelligence on a suspected hacker.
- Search warrants issued for email did not extend beyond the jurisdiction of the court issuing it. For example, if a court in Seattle ordered a search warrant on Wile E Hacker, and during the course of the investigation a new email box is discovered on an ISP in San Jose, law enforcement had no right to search that email box without obtaining an additional search warrant for that jurisdiction.
- National boundaries. There was nothing state or federal law enforcement could do to prosecute a hacker in America attacking a machine in a foreign country. In addition, foreign hackers discovered that they could route their nefarious traffic through US service providers with impunity. The lack of an American victim or an American criminal often discouraged US law enforcement agencies from involving themselves in such investigations, even at the behest of the foreign governments.

Warrants, Wire Taps and Subpoenas

- With the advent of MIME email attachments, it has been possible to include voice communications in email. This created another quandary for law enforcement, as search warrants providing them the authority to search the contents of an email box did not contain sufficient authority to include in that search email that MIGHT contain a voice transmission (voice communications are protected by the much more restrictive, and more difficult to obtain, wiretap order).
- Law enforcement, even armed with a subpoena, could only compel a very limited class of information regarding a suspect's account at an ISP. This list included his/her name, address, length of service, and means of payment. However, since many criminals had not bothered giving their REAL name to service providers, police were left with very little information with which to act upon. Without a method of payment, and more detailed information about session times and durations, police had a difficult time tying an actor to a crime.
- Then there is the case of the "Cable Act". The Cable Act set out an extremely restrictive set of rules governing law enforcement access to records held by local cable companies. For example, the Cable Act expressly prohibited the use or search warrants or subpoenas to obtain any information whatsoever about the customers of the involved cable company. Instead, the cable company had to notify the customer (yes, the suspected Bad Guy™) that this investigation was

happening. And then, the customer had the right to appear in court with a lawyer and compel law enforcement to justify the need for such information. The court would only order the disclosure of the information if it found "clear and convincing evidence" that the subscriber was "reasonably suspected" of engaging in criminal activity. Obviously, this process would immediately blow any investigation targeted at this individual, so law enforcement almost never attempted to acquire these records. And hackers, knowing they were protected to the extreme by the Cable Act, lined up around the block to order cable Internet service from their local providers (I won't discuss how cable modems give hackers more bandwidth to conduct attacks than most companies have for their entire network).

Other Hurdles

- If an ISP independently learned of a nefarious plot by one of its customers to commit a criminal act, it could not reveal to law enforcement officials the existence of said plot without exposing itself to civil lawsuits. Even when the disclosure of said information could save lives.
- Along the same lines, ISPs could not disclose customer records to law enforcement officials for the purposes of self-protection. In the case where an ISP's email system was compromised, the ISP could not legally disclose all the pertinent information to law enforcement authorities without violating the privacy rights of its customer under various federal laws and precedent.
- Federal courts had issued maximum penalties that were not sufficiently stiff to deter computer criminals (5 years maximum incarceration for first-time offenders, and 10 years for repeat offenders). In addition, state convictions could not be considered "prior offenses" when calculating the maximum allowed sentence of a federally-convicted hacker.
- By the wording of federal law, an offender had to "intentionally damage without authorization". "Damage" was defined as "impairment to the integrity or availability of data, a program, a system, or information that (1) caused loss of at least $5000; (2) modified or impaired medical treatment; (3) caused physical injury; or (4) threatened public health or safety". Sounds simple enough, eh? The problem was, law enforcement had to prove the perpetrator's INTENT to cause this damage. What if the hacker only intended to cause $1000 of damage to a single computer, but due to circumstances beyond their knowledge, it caused $50,000? No intent, no dice.
- Dealing with the same subset of law, the hacker had to have committed the $5000 of damage to a SINGLE computer. If the hacker had done $1000 of damage to 5 (or 10, or 1000) different computers, that didn't count as a criminal act under the wording of the law.
- There were no special provisions for attacking computers used for national defense, national security, or the furtherance of justice. Basically, this meant that Wile E Hacker could hack into the NSA's computer system, steal vitally important national security secrets, and expect no stricter response than if he hacked into Kentucky Fried Chicken™ and stole the Colonel's secret recipe.

- Funding. Would you rather have your tax dollars spent finding murderers, rapists and wife abusers, or fighting Internet crime? Tough call, isn't it?

Given all these restrictions, it's not surprising in the least that the World Wide Web is often referred to as the Wild Wild Web. Law enforcement agencies are so incredibly restricted in investigating and prosecuting Internet crime that it simply was not worth the effort and time involved. Instead, companies have to resort to employing "hired guns" (sometimes ex-hackers) to protect and defend the assets that are the lifeblood of their existence.

USA Patriot Act of 2001

Enter September 11th, 2001, a day that has in so many ways changed our lives. The United States is shown, at a level previously unimagined, how vulnerable it really is when faced with a determined foe. Terrorists, using every tool available to them, from steganography[2] to encryption[3], execute a previously-inconceivable plot to kill thousands of innocent Americans by coordinating multiple simultaneous hijackings and piloting the commandeered aircraft and their doomed passengers into various symbols of American prosperity.

Now, suddenly and terribly, the United States realizes how incredibly unprepared it is to fight the battles it is now facing.

After evaluating security across every spectrum, the federal government passes into law the USA Patriot Act of 2001 on October 26th, 2001 (you can read the entire 342 pages of this legislation, if that's your idea of a good time, at the Library of Congress web site, http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:.).

The Act, as we will refer to it here, set out to address many of the problems law enforcement has had in fighting terrorist activity in America, and they took the opportunity to address some of the restrictions hampering law enforcement's ability to fight computer crimes.

The Act directly addresses many of the complaints listed above:

Jurisdiction Issues

- The Act gives the courts permission to compel assistance from any communications provider in the United States whose assistance is appropriate to further an investigation. This allows federal investigators to

[2] McCullagh, Declan, "Bin Laden: Steganography Master?", Wired News, Feb 7 2001, http://www.wired.com/news/politics/0,1283,41658,00.html
[3] Kelley, Jack, "Terrorist Instructions Hidden Online", USAToday.com, June 19 2001, http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen-side.htm

execute the same search warrant on any downstream communication provider, regardless of which state it was operating in. The Act also states that, if the provider requests, law enforcement must provide a written or electronic certification that the order applies to the provider.

- The Act allows courts to authorize the use of pen/traps in other districts, so long as the issuing court has jurisdiction over the crime being investigated.
- The Act grants investigators who have previously obtained an applicable search warrant to compel records outside of the district in which the court was located. This amendment to law sunsets (expires) December 31, 2005.
- The Act expands the definition of "protected computer" to include those outside the borders of the United States, so long as they affect interstate or foreign commerce or communications of the United States
- The Act also specifically grants the ability to prosecute foreign hackers in US courts.

Warrants, Wiretaps, and Subpoenas

- Law enforcement can now obtain voice mail, and other stored voice communications, once a search warrant has been obtained. There is no longer a requirement for a wiretap order to be obtained to investigate stored voice communications (such as those stored as an email attachment or in a voicemail box). This amendment to law sunsets (expires) December 31, 2005.
- The Act expands significantly the data that can be subpoenaed from a service provider. Now they can specifically request information regarding session connect times and durations, the assigned IP Address of the session, as well as the means and source of payment. This allows law enforcement to more accurately tie an actor to a crime.
- Amendments to the Cable Act now allow law enforcement to subpoena customer records relevant to an ongoing investigation without having to notify the suspect. This, in effect, gives cable Internet traffic the same level or protection that is provided to Internet traffic conducted over standard modem lines. It is important to note that if the service provider also provides cable television service to the customer involved in the investigation, those records CANNOT be released under this amendment. Only those records pertinent to the investigation into Internet activities can be released.
- The Act further clarifies that pen/trap orders can be used to trace communications on the Internet and other computer networks.
- The Act grants federal pen/trap orders nationwide jurisdiction
- The Act requires federal agencies to notify the court when they use a pen/trap order to install their own monitoring device or software on computers owned by a public service provider.
- The Act further clarifies that pen/trap orders may be used to collect all non-content information used in transmitting and receiving electronic communications. That means they can monitor things like the To and From lines of an email header, but they cannot look INTO an email and view the

contents without additional authority (a search warrant)

- In the case where a pen/trap order is issued for a public service provider, it is specified that the provider must conduct the installation, monitoring, data gathering, and removal of the device. In the rare cases where this is not possible, the courts can allow law enforcement officials to conduct the installation, operation, and removal of the device, but they are bound by additional restrictions. They MUST provide the following information to the court under seal within 30 days: (1) The identity of the officers who installed or accessed the device; (2) the date/time the device was installed, accessed and removed; (3) the configuration of the device at the time is was installed, and any modifications made to it; and (4) the information collected by the device.

Other Issues

- The Act permits (but does not REQUIRE) a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious injury to any person. This amendment to law sunsets (expires) December 31, 2005.
- The Act allows service providers to reveal to law enforcement information to protect their rights and property. This amendment to law sunsets (expires) December 31, 2005.
- The Act allows victims of computer attacks to authorize law enforcement or "persons acting under the color of law" to monitor trespassers on their computer systems. The owner/operator of the computer system MUST authorize the interception of the trespasser's communications. In addition, law enforcement must have reasonable grounds to suspect the contents of the intercepted communications will be relevant to the investigation. And lastly, law enforcement can ONLY intercept the communications sent or received by the trespasser. This amendment to law sunsets (expires) December 31, 2005.
- The Act further clarifies the term "computer trespasser" as any person who accesses a protected computer without authorization.
- Maximum penalties for violations for damaging a protected computer have been raised to 10 years for first offense and 20 years for repeat offenders
- State convictions for computer crimes can now be considered when determining if a federally-convicted hacker is a first-time offender, or a repeat offender.
- The Act further clarifies the notion of "damage" and states that all aggregate damage occurring within the course of a single year can be used to meet the $5000 minimum required to prosecute an offender. That is to say, if an offender has caused $1000 on 10 different systems, the aggregate damage is $10000, which exceeds the required minimum.
- The Act also further clarifies that intent need not be proved when prosecuting a suspected hacker. It is only necessary to prove that the offended did cause damage, impairment of medical records, harmed a person, or

threatened public safety.

In addition to all the amendments to law, the Act also requires Attorneys General to establish regional forensic laboratories to be used to investigate and prosecute computer crime. These laboratories are also to be used to provide training and forensic capabilities to local law enforcement agencies and personnel.

Other Legislation

There is a flurry of new legislation coming from lawmakers far and wide, with the focus clearly on improving our stance towards cyber crime.

Some of the more interesting (some of these pieces of legislation are still in process, and have not yet become law):

HR 3482, "Cyber Security Enhancement Act of 2001"

- Provides liability protection to service providers while they are operating in "good faith" with investigative authorities.
- Encourages courts to consider the sophistication of the attack (among other things) when determining sentences for convicted hackers (this provision was in the USA PATRIOT Act at one point, but did not survive to the version President Bush signed into law).

HR 3400, "Networking and Information Technology Research Advancement Act"

- Increases government IT research by 46% over the next 5 years

HR 3394, "Cyber Security Research and Development Act"

- Authorizes $800M over the next 5 years to fund additional research and education in the private sector. The money is to be distributed mostly by the National Science Foundation and the National Institute of Science and Technology, and will go largely to universities to further educational efforts in the cyber security arena (universities have been screaming for years about the lack of funding for security research and education).

Council of Europe, "Convention on Cybercrime"

- Though years away from actual implementation, this international proposal is designed to set standards for the cooperation of international law enforcement agencies in pursuing hackers, terrorists, child pornographers, and other universally-agreed-upon cyber-miscreants.

Privacy Advocates Have a Collective Cow

Any encroachment on the rights of citizens in the United States, and the Internet

everywhere, is sure to cause a ruckus amongst privacy advocates. And the USA Patriot Act of 2001 is certainly no exception.

The Electronic Frontier Foundation (EFF) posted their objections to the Act on their web site (http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html).

Among their many objections, they contend that the Act was rushed through the lawmaking process, in the furor over the acts on Sept 11th. They also (alertly) observed that the Act was presented as an anti-terrorism weapon, but included expansions of federal capabilities not directly related to fighting terrorism. The blurring of the lines between "hacker" and "terrorist" by the federal government is a little disconcerting, I have to admit.

The ACLU has vowed to monitor the activities of law enforcement closely. "We will now work with ACLU affiliates around the country to monitor its implementation.", said ACLU Executive Director Anthony Romero.[4]

Another privacy advocate organization, Electronic Privacy Information Center (EPIC), has also vowed to monitor the situation closely: "We will begin a Freedom of Information Act campaign to learn more about what the government will be doing with these new authorities," said Chris Hoofnagle, EPIC privacy advocate.[5]

Summary

While I'm not usually excited about giving more investigative powers to our federal government, everyone in the security industry has known for ages that law enforcement officials at every level have been vastly outclassed when it comes to crimes on the Internet.

There has been no deterrent. There has been no 'downside' to hacking. Sad as it is, the vast majority of computer crimes are not even *investigated*, much less prosecuted. Hopefully the USA Patriot Act will give law enforcement some teeth.

Obviously, the private sector has some work to do as well. We have to hold up our end of the bargain. We have to continue to be vigilant in our protection and vigilant in our monitoring. We have to allow our local law enforcement agencies to spend money on the facilities and training required to be effective in combating computer crimes.

We have to cooperate with each other and communicate. Holding back exploit information helps only the bad guys.

---

[4] Olsen, Stephanie, "Patriot Act draws privacy concerns", CNet News.com, Oct 26 2001, http://news.cnet.com/news/0-1005-200-7671240.html?tag=rltdnws

[5] "An Invasion of Privacy?" ABCNews.com, Nov 5 2001, http://abcnews.go.com/sections/scitech/TechTV/techtv_civilliberties011104.html

Software vendors must do a better job. Not just Microsoft, but every developer out there. Yes, Linux too. Somewhere we have to draw the line about what is *useful* and what is *safe*.

ISPs HAVE to get with the program. There are so many things ISPs could be doing to curb attacks. Put egress filtering on your routers, for starters. If you can't operate responsibly on the Internet, I would argue you should not be providing services.

Until the private sector gets behind (seriously behind) creating secure products and providing secure services, law enforcement will always be fighting a losing battle. No amount of legislation is going to fix that.

I wish to especially thank Sergeant Mike Case of the Bellevue Police Department for his contributions to this document.

Bibliography

Kerr, Orin S., "Are We Overprotecting Our Code? Thoughts on First-Generation Internet Law", 2000

"Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001", US Department of Justice (Computer Crime and Intellectual Property Section), Nov 5 2001, http://www.cybercrime.gov/PatriotAct.htm

USA Patriot Act, Library of Congress, HR3162, http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:.

McCullagh, Declan, "Bin Laden: Steganography Master?", Wired News, Feb 7 2001, http://www.wired.com/news/politics/0,1283,41658,00.html

Kelley, Jack, "Terrorist Instructions Hidden Online", USAToday.com, June 19 2001, http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen-side.htm

Olsen, Stephanie, "Patriot Act draws privacy concerns", CNet News.com, Oct 26 2001, http://news.cnet.com/news/0-1005-200-7671240.html?tag=rltdnws

"An Invasion of Privacy?" ABCNews.com, Nov 5 2001, http://abcnews.go.com/sections/scitech/TechTV/techtv_civilliberties011104.html

Strang, Robert. "Recognizing and Meeting Title III Concerns in Computer Investigations", US Department of Justice (Computer Crime and Intellectual Property Section), March 2001, http://www.usdoj.gov/criminal/cybercrime/usamarch2001_2.htm

Kerr, Orin S., “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations”, US Department of Justice (Computer Crime and Intellectual Property Section), Jan 2001, http://www.cybercrime.gov/searchmanual.htm

“The Convention on Cybercrime, a unique instrument for international co-operation”, Nov 23 2001, Council of Europe, http://www.coe.int/T/E/Communication_and_Research/Press/Themes_Files/Cybercrime/e_CP893.asp#TopOfPage

“Cyber Security Enhancement Act of 2001”, HR3482, Library of Congress, http://thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c1073IjAT3

“Networking and Information Technology Research Advancement Act”, HR 3400, Library of Congress, http://thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c107Uz8yrT

“Cyber Security Research and Development Act”, HR 3394, Library of Congress, http://thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c107KZszua

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event