Global Information Assurance Certification Paper

Powered by Carnivore: Updated Legal Issues and the USA Patriot Act

By
Brian Sondreal
(Certification: GSEC)
(Assignment: Version 1.3)

Introduction

The world changed at 8:45am EST September 11, 2001 when two hijacked airliners flew into the New York City World Trade Center, a third crashed into the Pentagon and a fourth hit the ground in Pennsylvania. An emotional shockwave shook the country as Americans rallied to aid the victims. As the numbness wore off, we were struck with the realization that our national security was not up to par. Since then all aspects of security within the United States and around the world have come under intense scrutiny, from airports to city water supplies, we have been forced to look at our infrastructure from another point of view -- that of a terrorist. Because so much of today's infrastructure depends on the Internet, it too has come under the microscope. Not only is the Internet itself vulnerable to attack and espionage, it is also a tool available for use by an attacker as a means of communication. It is this aspect of the Internet, which has brought about changes in legislation that will provide for effective prosecution of any individuals involved in terrorism or other crimes, however, if not properly designed, these same laws can have a frightening impact on legitimate Internet users and administrators.

Background

Since the Internets' inception in the 1970's security has been a concern. The already established anarchistic cyber-society was resistant to any restrictions. The basic act of cracking into a system, at the time, was a means of proving one's technical abilities. In the 1960's, the artificial intelligence lab at Massachusetts Institute of Technology (MIT) was a playground for the first crackers. The 1970's brought about a form of telephone system cracking called "phreaking". John Draper, known as "Cap'n Crunch", discovered that by blowing a whistle, provided by the well-known breakfast cereal, Capn' Crunch, into a phone, he could emulate system tones (2600 Mhz) to gain control of the telephone system and make free long-distance calls in the process. In 1981 Ian Murphy, a.k.a. "Captain Zap" and three of his accomplices cracked into government systems and into electronics manufacturers invoice systems. Also that decade, groups like the Legion of Doom (LOD) and the Masters of Deception (MOD), enlisting the best of the best, engaged in years of online cracking wars. These incidents led to government bills and laws intended to protect Internet users from harm.

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA), which outlawed the unauthorized interception of digital communications. It was followed shortly that same year by the Federal Computer Fraud and Abuse Act (CFAA), which made it a felony to access federal computer systems without authorization and with the intent to commit fraudulent theft or "malicious damage." Penalties ranged from a prison term of five (5) years for a first offense to ten (10) years for a second. A misdemeanor was defined as, trafficking in computer passwords from governmental computers "knowingly and with intent" when it "affects interstate or foreign commerce."

Robert Morris and Kevin Mitnick are examples of two high-profile cases involving the Federal Computer Fraud and Abuse Act. Robert Morris was a first-year graduate student at Cornell University computer science department when he created a program called a 'worm'. The "Morris Worm" exploited the bugs in sendmail and the finger daemon and also took advantage of trust relationships. When Morris released the worm, unfortunately he had miscalculated how fast the worm would replicate itself, and the worm had in affect clogged up the Internet by crashing key computer systems. Robert, the first person to be prosecuted under this act, was convicted of violating the CFAA and received a sentencing of "three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision."[1] Kevin Mitnick, the most notorious hacker, was arrested in 1995 for wire and computer fraud and intercepting communications. Kevin was also convicted under this law and sentenced to 46 months in a federal prison.[2]

New Legislation

Immediately following the September 11 attacks Attorney General John Ashcroft presented several new pieces of legislation intended to aid the FBI, NSA and DOJ in the combat against terrorism. Because these bills were released very quickly, information on them was not readily available and was at times misunderstood or misleading. By the end of 2001, Attorney General Ashcroft had presented the following three legislative acts to Congress:

- The *Mobilization Against Terrorism Act* (MATA)[3]
  - The first drafting of the Anti-Terrorism bill.

- The *Anti-Terrorism Act* (ATA)[4]
  - The second drafting of the Anti-Terrorism bill.

- *The USA Patriot Act* (USAPA)[5]
  - The final drafting of the Anti-Terrorism bill.
  (originally known as *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*)

MATA

The MATA was created to "provide the President and the Department of Justice with the tools and resources necessary to disrupt, weaken, thwart and eliminate the infrastructure of terrorist organizations, to prevent or thwart terrorist attacks, and to punish perpetrators of terrorist acts."[6] Presented by Attorney General Ashcroft this bill would have allowed for in depth surveillance of any suspect of terrorism as well as the ability to crack down on the thousands of illegal immigrants. The bill was also intended to help the victims of September 11th attacks by providing aid to the police officers and firemen disabled as a result of September 11th attacks, and would grant money to the States to assist victims in their local jurisdictions.

Due to its vague wording, this bill immediately came under scrutiny by civil liberties organizations that objected to its underlying surveillance tactics and its potential for abuse of foreign visitors with expired visas. Even before the bill was finished, there was talk on the Senate floor asking for swift but fair resolutions. U.S. Senator George Allen (R-Va.) stated, "...what makes us a great nation is that this is a country that understands that people have fundamental God-given rights and liberties and our government is constituted to protect those rights. We cannot - in our efforts to bring justice - diminish those liberties." Although MATA was intended to aid law enforcement officials in locating and prosecuting terrorists, its underlying flaws and extreme measures led to a second drafting of the MATA bill.

ATA

Immediately following MATA's rejection, Attorney General Ashcroft presented the Anti-Terrorism Act (ATA) designed to "strengthen the nation's defense against terrorism." The revised version also came under great pressure from special interest groups, due to the fact that, although entitled the Anti-Terrorism Act, it was not worded in such a way as to be used primarily in the fight against terrorism. The provisions contained within the bill could have been applied to all criminal investigations. As the Electronic Privacy Information Center (EPIC) reported: "Several of ATA's provisions would vastly expand the authority of law enforcement and intelligence agencies to monitor private communications and access personal information."[7]

The above statement referred to section 101, which expanded the definitions of two wiretap mechanisms used by law enforcement: the "trap and trace" and the "pen register". The ATA would redefine a *trap and trace* as " a device or process, which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling

information relevant to identifying the source or a wire or electronic communication."[8] In other words, it allows a phone call or Internet connection to be traced to its' source. A *pen register* would be redefined as a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," meaning the contents of phone conversations can be recorded. These amendments would have expanded the use of these devices to include information traveling over the Internet, such as e-mail senders, recipients and contents; web sites visits; IRC conversations; and search engine requests.

One problem, brought up in the Internet community was that this bill was worded in such a way as to label legitimate system administration tools as hacking tools. System administrators using these tools to secure their own networks would then have been guilty of committing terrorist acts and could have been subjected to prosecution as terrorists.

USA Patriot Act

On October 26, 2001 Congress voted for, and President Bush signed the USA Patriot Act. The USAPA is designed "To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigative tools, and for other purposes."[9] As its' title implies, this bill is not intended solely to address terrorism but can also be applied as an investigative tool in non-violent domestic computer crimes, not only for federal law enforcement officials, but for local system administrators as well.

The USAPA aids computer system administrators by clarifying some of the laws already set fourth within the Computer Fraud and Abuse Act of 1986 (CFAA). It amends definitions of a penetrated computer system and sets guidelines as to whether or not a system break-in would require the need for Federal investigative involvement and/or allow for compensation for the victims. Prior to the USAPA, the CFAA defined a Federal offense as an "intentional" break in to cause damage, resulting in damages greater than or equal to $5000.00. Unfortunately the CFAA did not clarify the meanings of the words "damages" or "intentional". The USAPA amends the CFAA by restructuring the sentence using "intentional" as the *intention* to break into a system, which results in causing damage, and also by adding a definition for "damages", which means "…any impairment to the integrity or availability of data, a program, a system, or information".[10] The USAPA also clarifies the loss to any person or corporation as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service", which in effect strikes out the $5000 damage minimum.

Another amendment to the laws, which impacts regular users is that prior to the passage of the USA Patriot Act (USAPA), an Internet Service Provider (ISP) could not release information regarding a customers' personal information, including IP address and financial information, without a court order. Under this act the information can now be released from the ISP voluntarily. In addition, cable companies who were once indemnified from releasing information about their subscribers, including cable modem users, now have the same legal standing as analog and digital ISP's.

The use of information obtained via warrants and wiretapping is not a new issue. Provisions within Title III, also known as The Omnibus Crime Control and Safe Streets Act of 1968, allow for "emergency" wiretapping, however, a request for a court order must be made within 48 hours of said wiretapping. The USAPA extends, to 90 days, the time requirement for requesting the court order and judges are no longer permitted to deny the requests.

Both the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) feel that this band-aid for our current laws is actually a spackle of "Big Brother" that is encroaching upon Americans civil liberties. "With this law we have given sweeping new powers to both domestic law enforcement and international intelligence agencies and have eliminated the checks and balances that previously gave courts the opportunity to ensure that these powers were not abused."[11]

Section 216 of the USA Patriot act provides for the most outstanding change to current legislation. Section 216 "…modifies [the pen/trap statute, 18 USC § 3121] to expressly include routing, addressing information, thus expressly including e-mail and electronic communications."[12] Inclusion of the words "routing", "addressing" and the phrase "dialing and signaling information" widens the authoritative scope of law enforcement officials to monitor Internet traffic.

With these new modifications to existing laws, the USAPA allows the use of some of the FBI's most sophisticated and controversial tools.

Tools

In the war on terrorism some new tools, and some not so new tools, have come into play. Due to their sensitive nature, information on these tools is either hard to come by, or incomplete. However, I have tried to supply what limited information there is available on some of these technologies.Programs, such as the "Cyber-Knight" and the "DragonWare Suite" are theorized on the Internet as possible tools to acquire the wiretap information. Technologies such as "Carnivore" and "Magic Lantern" are two of the programs that possibly exist under the "Cyber-Knight" project, and may be implemented under the Patriot Act. However, if information obtained by these tools is used as evidence in legal proceedings, the technology and programming behind them must be

explained and publicized unless the disclosure of such tools would compromise national security.

Carnivore

Carnivore[13], the best known and most controversial tool used by the federal government, is one of many Internet traffic-capturing tools designed by the FBI. Carnivore has also been mentioned in a package called "DragonWare Suite". The official release on this suite states:

- Carnivore – A windows based program that captures packet information.
- Packateer – No official information.
- Coolminer – No official information.

It is theorized that the Packateer and Coolminer programs are filters designed to pick out specific passages of e-mail and/or packet information.

Carnivore, based on the information released by the FBI, is a sniffer, which is placed on the back end of an ISP to watch the movements of a specific user. There are similar systems administration tools available for public use on the Internet. Snort[14] is an example of a sniffer used by computer systems administrators to monitor traffic of their networks. Carnivore is like Snort in that it captures the targeted packet data traveling over the suspects Internet service provider (ISP) network. The data is then filtered to check for specific patterns or information. Any information not intended for the eyes of the law enforcement officials as specified in the court order, is discarded while a copy of the filtered information is saved onto hard drive for possible future use in a case against the suspect.

Magic Lantern

One other possible aspect of the "Cyber Knight" Internet dragnet is the "Magic Lantern" program. [15]Bob Sullivan of MSNBC first wrote about the Magic Lantern project when the Electronic Privacy Information Center (EPIC) requested information on the subject under the Freedom of Information Act. Sullivan describes the Magic Lantern project as a key-logging program, which captures the crypto key from a suspect's computer. Crypto keys are the cornerstone of such programs as Pretty Good Privacy (PGP), and are used to encrypt electronic mail. Only the intended reader holding the corresponding key can unlock/unencrypt the email.

Magic Lantern is more a Trojan horse than anything else. Some have called it a virus, but, as you know, viruses are destructive in one-way or another, hence the name. It is not related to worms because worms propagate from one computer to another usually through e-mail. Magic Lantern would infiltrate a

suspect's computer as an e-mail attachment or possibly trick the user into downloading the program from a website. It's theorized that the program will sit in the background, on any Windows system, and wait until the request for the encryption key is made. The request activates the program, which captures the encryption key. Once the FBI or investigating group has the encryption key of the suspect, they would then be able to read the encrypted e-mail.

Discussion

As you can see, running Magic Lantern on a suspects' computer and Carnivore on the ISP server would give the FBI the ability to grab the e-mails of a suspect and read it even when it has been encrypted. As reported before, the FBI did state that the Carnivore program has filters built in to show only the "to", "from" and "subject" fields of the e-mails only. Several civil liberties groups mention on their websites that the code for the filters on this type of system have not been produced for the public, therefore, it's unproven that it works as the FBI states. Since the USA Patriot Act has only recently been passed, the act has not been put through the process of the court system and therefore there is insufficient evidence to know whether these tools would survive court proceedings and a judges' approval.

As I write this paper, there are new developments on this subject. Magic Lantern or possible variations of the program have already been put to use. In February of 2002, Nicodemo S. Scarfo Jr. pleaded guilty to charges of illegal gambling in a New Jersey federal court. Federal agents installed a keystroke-logging program on his personal computer, and were able to extract his PGP encryption code, thus allowing them to read his e-mails. It was accepted in the courts as evidence, which lead to Mr. Scarfo pleading guilty.

Conclusion

Is this type of surveillance needed? Has it been available to Law enforcement agents for a long time and is this just an amendment to pre-existing law to allow for further intelligence gathering of the average U.S., and international Internet users? Furthermore, what more could have been done, concerning the Internet, to prevent the attacks on September 11th, and how do the provisions set fourth within the USAPA relate to those attacks?

In a related note to this paper, I would like to explain that there are several related topics I cannot write about. This is mainly due to the fact that there is not enough information available at this time, which leaves me suspicious of these new laws. Just as the USA Patriot Act, which was passed so quickly and left so many people confused and suspicious, these new laws seem to have passed without any hearings or public comment.

As recently as last month, February 2002, congress passed new laws in the fight against cyber terrorism:

- *The Cyberterrorism Preparedness Act of 2002*
    - Creates a committee of academic experts and private sector professionals to research cyber terrorism and find "best practice" standards.
- *The Cybersecurity Research and Education Act of 2002*
    - Trains more of the academic and private sector people to study cyber security.

Personally, every time I sit down and read more on this subject, I change my mind on how I feel. To tell you the truth, I end up where I left off, feeling hopeful that this act would aid the Internet community with more powerful tools, but at the same time I feel paranoid that I could be the average user who accidentally comes under investigation. There are provisions within this act that are a must have. Amendments to old law that are of the "of course we need to do that" nature. But there are also broad generalizations of ideas that have not been focused. Tools to snoop on the average Internet user ring of the cold war era, and Big Brother. Unfortunately, there's not enough information on how these new amendments are going to affect the average user and until they are put through the ringer of the Unite States court system a few times it's hard to tell how these enhanced laws will affect us as a society. It's up to the system administrators, the managers, and the average user to keep an eye on and aid in the protection of the Internet. Protection of our own systems is the key to showing the government that we can handle our own backyards without assistance. The tools are there for us to use, and education is the power to correctly use these tools. That's why I chose this topic. I'm currently in the middle of taking computer security classes and these laws might have hindered my ability to learn and use the tools available to my colleagues, and me. It sounds like a vicious circle. Let's hope that we never have to face that day.

I hope anybody reading this paper becomes just a little more paranoid and a little more skeptical of themselves and the users of they're systems. I'm not saying any of these scenarios will happen. But it's a possibility. And as a systems administrator and a student of Internet security, I need to understand why we apply such strict rules to our users and ourselves. Since an estimated 90% of system attacks come from within our own intranets, and without our systems protected to the best of our abilities, we may fall victim to a federal agency watching every move we make.

---

[1] http://www.jmls.edu/cyber/cases/morris.txt, U.S.A. vs. Robert Tappan Morris.
[2] http://www.usdoj.gov/criminal/cybercrime/mitnick.htm, U.S. Department of Justice, "Kevin Mitnick Sentenced to Nearly four years in prison.
[3] http://www.eff.org/Privacy/Surveillance/20010919_mata_bill_draft.html, draft of MATA.
[4] http://www.eff.org/Privacy/Surveillance/20010919_ata_bill_draft.html, draft of ATA.
[5] http://www.ins.usdoj.gov/graphics/lawsregs/patriot.pdf, Public Law No: 107-56.
[6] http://www.usdoj.gov/opa/pr/2001/September/492ag.htm, Attorney General Ashcroft outlines mobilization against terrorism act.
[7] http://www.epic.org/privacy/terrorism/ata_analysis.html, EPIC's analysis of the ATA.
[8] http://www.epic.org/privacy/terrorism/ata_analysis.html, EPIC's analysis of the ATA.
[9] http://www.ins.usdoj.gov/graphics/lawsregs/patriot.pdf, Public Law No: 107-56, U.S.A. Patriot Act.
[10] http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011025_hr3162_usa_patriot_bill.html,

The USA Patriot Act as released by the Congress of the United States of America.
[11] http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html, EFF analysis of the provisions of the USA PATRIOT Act.
[12] http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html, EFF analysis of the provisions of the USA PATRIOT Act.
[13] http://www.FBI.gov/hq/lab/carnivore/carnivore.htm, CARNIVORE diagnostics tool.
[14] http://www.snort.org, The Open Source Network Intrusion Detection System.
[15] http://www.msnbc.com/news/671981.asp?0si=- , FBI confirms 'Magic Lantern' exists, Dec. 12, 2001, www.msnbc.com.

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 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
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 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
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