Global Information Assurance Certification Paper

Computer Surveillance, How do we protect our privacy?

Robert Marcoux

June 5, 2001

This paper is being written for the SANS Security Essentials GSEC Practical Assignment, Version 1.2e, Current as of December 2000 (Amended May 22, 2001)

Introduction

Big Brother isn't just a show on television

As a security professional, I am a firm believer in the philosophy that the majority of threats to network security come from within.

But perhaps more dangerous than the disgruntled employee, rebooting users PC's and wreaking havoc with the mail server, is the security professional operating under questionable ethics. They are the silent enemy within and whether we would like to admit it or not, they are out there. It is that enemy within that poses the greatest threat to privacy.

For most of the larger IT companies, this is a non-issue. Security engineers at larger IT firms require background checks similar to what it takes to obtain a Top Secret clearance.

It's the small to medium sized businesses that become easy prey for this silent predator. An unethical security professional is like a parasite with all the latest high tech gadgets at his disposal to listen in and keep tabs on anyone he so chooses.

With the focus rapidly shifting toward network security, businesses are now employing security tools like content scanners, firewalls, packet sniffers, and intrusion detection sensors that meticulously capture and log network traffic.

The data these devices capture can be used to recount the events during and leading up to a DoS attack.

They are also being utilized as management tools to track employee productivity. If your manager has reason to suspect that you aren't being productive, he can have the technology department deliver a report on your surfing habits. But is this ethical? More importantly, is this legal? Does your company have a policy concerning this? Do you know?

According to an April 2000 survey conducted by the American Management Association, nearly three-quarters of U.S. firms (73.5%) record and review employee communications and activities on the job, including their phone calls, e-mail, Internet connections, and computer files.[1]

As Enterprises adopt VoIP (Voice over IP services) on the corporate network, voice traffic will be as easy to monitor as HTTP, FTP and Telnet. Voicemail will be stored on the same medium as e-mail and susceptible to the same tools used to scan e-mail messages; the potential to infringe on employees' privacy will be greater than ever.[2]

When you agree to work for a company, you should not be asked to check your privacy at the door.

Do you think the monitoring ends at work?

I am sure everyone is familiar with the highly publicized network capture device developed for the FBI called "Carnivore". For those of you who aren't, The Carnivore is a packet sniffer designed to capture and log network traffic.

It has been widely rumored that the FBI has installed the device known as Carnivore at several Internet Service Providers (ISPs) across the United States.

When privacy issues were raised, the FBI insisted this device would be used to analyze only the packets the Bureau is lawfully authorized to collect. The question is "How will we know?

The FBI has yet to fully comply with a Freedom of Information Act request filed by The Electronic Privacy Information Center (EPIC) detailing specifically how the device works.[3]

Clearly I don't believe all the hype "Carnivore" is receiving. As a matter of fact, I believe Carnivore is little more than a supped up Windows NT "Network Monitor". However, This does not change the fact that the Federal Government has installed a device used for the sole purpose of monitoring and collecting electronic communications and they are all but refusing to tell us how this device works. Who has access to the raw data this device gathers? What controls are in place to guarantee that the person or persons monitoring this "system" don't compromise the fourth amendment? Who is making sure the person collecting this data is doing so in an "ethical" manner?

The sweeping push for information systems security, although warranted, has brought with it many ethical dilemmas. None are more important than, "Who is monitoring this stuff?"

Does that creepy guy, who comes around to swap out the toner cartridge, know you've been surfing links about breast cancer? If he doesn't, could he find out?

The bottom line here is that these new "security devices" collect data. Data collection is the first step toward invasion of privacy. No matter how trivial, all data is worth something to the right person.

Protecting yourself from unwanted surveillance

Be Pro-Active. Security does not begin or end when you go to work or come home. Don't trust someone else to protect your privacy. Your privacy begins and ends with you.

The best place to start is by safeguarding all usernames and passwords assigned to you.

Always remember to secure your terminal when you are not using it. What good is having a password, if your terminal is not secured? Use a password screensaver with a one minute timer if necessary.

Know your company's e-mail and Internet usage policy. Find out what things (i.e. Internet content, E-mail) if any, are being monitored in your workplace. It is your right, or it should be, to know how that monitoring data is stored and who is responsible for safeguarding it. Most importantly, know who has access to that data.

What else can be done to preserve our anonymity and safeguard our privacy? Privacy conscious users are turning to encryption technologies like PGP (Pretty Good Privacy) to ensure data integrity. PGP can be used to encrypt your e-mail messages, while Secure Sockets connections (SSL) are used to encrypt your web traffic. Data encryption is the best way to ensure integrity, confidentiality, and authenticity.

Another significant threat to privacy is the Trojan. A Trojan is a set of computer instructions purposely hidden inside a program. Most Trojans, like Back Orifice, instruct systems to listen on a specific port for a connection. These ports are well-known to hackers, who frequently scan for systems awaiting connections on them. Once connected to a compromised system, an enterprising hacker can operate it just as if he/she were sitting at the terminal.

A good way to avoid Trojans is by not opening any programs or files, running any commands, batches or scripts unless you are 100% certain who it's from and what it's for. Most anti-virus solutions will sniff out well-known Trojans (i.e. Back Orifice).

As a general rule, you should never open an unsolicited e-mail attachment, even if you do know the person who sent it to you. Use your common sense. Think for a minute, does it make sense that your boss sent you a message with a subject that reads "ILOVEYOU". I hope not.

Scanning attachments for virus' helps, but what if the virus update hasn't yet been triggered. Better still, what if this is a new virus for which there are no updates.

Installing a good virus scanner is crucial. But remember, there are new Trojans and virus' being released into the wild everyday. Therefore, making sure you are up to date with the latest virus definitions also helps protect personal privacy.

Anonymous surfing is another form of security. Websites like www.thecloak.com, www.siegesurfer.com, www.safeweb.com and finally www.orangatango.com have provided to enjoy surfing the web in complete anonymity. These sites take a "man in the middle" approach to web browsing. You connect and make requests for URL's through their server. Their server goes out and retrieves the data and delivers or *"Proxy's"* it back to you through a secure SSL session.

One caveat to using a registered anonymous web proxy is, they are relatively useless if your company denies access to them. In fact, if your network is being "monitored", there is a good chance that your Security Administrators are aware of these sites and are blocking access to them.

Peer-to-peer (P2P) networking is gaining a lot of support among privacy advocates. Peer-to-peer networking is not a new concept in the networking arena. Peer-to-peer networks come in two basic versions-Napster-style models that use servers as hubs to direct traffic to other desktops, and server-free implementations that directly connect desktops over an IP network. [4]

Unlike server based P2P networking, the server-free implementations pose a severe headache to security professionals because blocking them is virtually impossible. Locking down the desktop (isn't that where security starts) is pretty much the only way to prevent P2P traffic on the network.

One company that has taken the P2P concept a step further is SafeWeb.

SafeWeb has developed a product they call "Triangle Boy". Triangle Boy was designed for the purpose of constructing an anonymous trusted network of peer web proxies.

Triangle Boy is SafeWeb's response to Internet censorship. It is a free, peer-to-peer application that **volunteers** download onto their PCs so that users who have been blocked from SafeWeb (or any other site) can circumvent firewalls and filtering software and regain access to the site.[5]

Here's how it works:

A user who is blocked from directly accessing SafeWeb or any other site can access it through any other computer running "Triangle Boy". That user's Web requests are then forwarded (i.e. the packets are reflected) to the SafeWeb server.[6]

As the demand for anonymity and privacy increases, expect services similar to Triangle Boy to become more prevalent. As an investor, I see a strong market for subscription-based services like these in the near future.

Virtual Private Networking is another way of assuring your traffic stays "snoop-free". Virtual Private Networks (VPN's) create encrypted static tunnels through public circuits from one point to another.

VPN's are ideal for remote access or sharing data between to sites over the internet.

In summary, I mentioned several techniques that will afford some privacy and anonymity. They are:

- Username/Password security.
- Terminal security (Lock your workstation or Log out).
- Use PGP to encrypt your e-mail messages.
- Never open any unsolicited attachments or run any foreign files or programs.
- Use Anonymous Web Proxies when applicable.
- Consider VPN technologies when it is cost effective.

One method I didn't cover, which is very important to data integrity is archiving. I cannot stress the importance of backing up your data. After all, if your data is important enough to secure, you ought to be backing it up as well. Most back-up software allows for secure (password protected) archiving.

If you cannot afford back-up software or secure archiving is not in your budget. Use NT back-up and store the media in a secure place.

I don't want to bore you with all the Big Brother hysteria and paranoia. The fact of the matter is the network surveillance tools mentioned above are very necessary. They are essential pieces of any network security architecture installed to prevent corporate sabotage. But, it's important to note that these tools are very powerful and can be very dangerous when in the wrong hands.

As a security professional, the last thing I want is security policies being circumvented. Remember, before attempting anything in this article, you should check your company's security policy.

Bibliography:

1. American Management Association. "2000 AMA Survey: Workplace Monitoring & Surveillance" April 2000 Research Report. URL: http://www.amanet.org/research/archives.htm 28 Jun 2001
2. Doherty, Sean. "Monitoring and Privacy: Is your head still in the sand?" 25 Jun 2001. URL: http://www.networkcomputing.com/1213/1213f12.html 03 Jul 2001.
3. Electronic Privacy Information Center (EPIC) "Carnivore Release Document" URL:http://www.epic.org/privacy/litigation/carnivore_release.html Jul 2001
4. Seifried, Kurt. Security Portal "Peer to Peer – Security Risks" 25 Jul 2001 URL: http://securityportal.com/closet/closet20010725.html 25 Jul 2001
5. SafeWeb "Triangle Boy" https://fugu.safeweb.com/webpage/tboy1.php3 Jul 2001