"BREAKING POINT: FORGING CHAOS AND DESTRUCTION"

> *"Human rights are not a privilege conferred by government. They are every human being's entitlement by virtue of his humanity. The right to life does not depend, and must not be contingent, on the pleasure of anyone else, not even a parent or sovereign. ... You must weep that your own government, at present, seems blind to this truth."* Agnes Gonxha Beiaxhiu, aka Mother Teresa

High tech wars nowadays seems to be a problem which many people overlook. While many would want to justify the means of fighting for privacy on the Internet for the sake of retaining privacy, others may use this same excuse to justify it for the means of using this shadow of privacy for committing criminal mischief for anything from financial gain, to jealousy, to experimentation. Sky's the limit when thinking of possibilities.

Anyone from the typical citizen whose information is being consumed by some information database, businessmen gathering information via unethical means in order to make a bigger buck, to privacy buffs hell bent on hiding their identity at all costs can end up being victims to someone's wrath on the Internet. Even Microsoft's own Bill Gates fell victim to someone's recent malice when a website was broken into and mentions of Bill Gates intruding into NASA websites was posted. Clearly one can assume that someone with such prestige, and power such as Bill Gates would never do such a thing, but there are those who could probably conclude that Mr. Gates could have done such a thing in an effort to gain some proprietary software to enhance Microsoft's standings.

Governments aren't excluded from falling victims themselves to being accused of partaking in illegal activities of this nature either:

> **Battling Industrial Espionage**
>
> *The European Union has said member nations are hard-hit by industrial spying. While the committee refused to blame Echelon for such spying, it did call for the U.S. to join the E.U. in discussions over economic intelligence gathering.*
>
> *Although the U.S. has long denied the existence of such a spy network, the parliament said Wednesday that it confirms the snooping exists and is run by the U.S., Canada, Australia, the UK and New Zealand.*
>
> *The official statement comes after the committee's May 24th draft report was leaked, confirming Echelon's existence and its breach of European privacy laws.*
>
> *The resolution recommends that European nations provide "effective protection against all forms of illegal interception of their communications," and that citizens use European*

encryption software.

New Hacker Threat

"There will be more corporate crime on the Internet," Frank Prince, a senior analyst at Forrester Research, told NewsFactor Network.

Security software must protect against a new breed of hacker more interested in ferreting out corporate secrets than planting viruses or shutting down individual Web sites, says a new study.

Battling Industrial Espionage

The European Union has said member nations are hard-hit by industrial spying. While the committee refused to blame Echelon for such spying, it did call for the U.S. to join the E.U. in discussions over economic intelligence gathering.

Although the U.S. has long denied the existence of such a spy network, the parliament said Wednesday that it confirms the snooping exists and is run by the U.S., Canada, Australia, the UK and New Zealand.

The official statement comes after the committee's May 24th draft report was leaked, confirming Echelon's existence and its breach of European privacy laws.

The resolution recommends that European nations provide "effective protection against all forms of illegal interception of their communications," and that citizens use European encryption software.

New Hacker Threat

"There will be more corporate crime on the Internet," Frank Prince, a senior analyst at Forrester Research, told NewsFactor Network.

Security software must protect against a new breed of hacker more interested in ferreting out corporate secrets than planting viruses or shutting down individual Web sites, says a new study.

"ONE ARISES FROM A LOW TO A HIGH STATION MORE OFTEN BY USING FRAUD INSTEAD OF FORCE." Niccolo Machiavelli Chapter XIII The Discourses

It should be of no surprise to anyone with enough experience the extent someone will go through to cover their identity, from the simplest of spammers, to someone relocating from an estranged spouse, in an effort to protect oneself from the harm of information that is so readily available to anyone who can type in a name in an effort to gain information on anyone they choose. Especially in today's hi-speed world, anything can be gathered with the quickest of ease.

However, what happens when information, which someone may think is private, and may go through all extents to keep that information safe, is abused for unknown reasons? Moreover what happens when there is something to gain by committing the perfect crime against someone using Internet based technologies? How easy would it be for anyone to frame someone in today's world of information systems, most of which pass somewhere along the line, through insecure channels? Answer? Who hates you well enough to gather your information, and use it for malicious purposes. How far is someone willing to go? How much can someone gain, and how much can someone lose?

It should be said that with today's technologies, one should feel a bit at ease with privacy and security, but with a bit of information and an evil mind, anyone can cause extensive damage to just about anyone they would like to, with the greatest of ease, and this is something that should not be overlooked on any level including those in law enforcement and privacy groups. The jealous friend or spouse, a disgruntled employee, disgruntled employer, government agencies, competitors, these can all be candidates who could possibly destroy lives, careers, friendships at the click of a keyboard. What do you do? How do you protect yourself?

These answers may not be as simple as one would hope. Using tools readily available on security related sites, anyone can digitally frame someone for just about anything they'd like. People can rant on about privacy all they want, they can install the latest in privacy tools, ranging from encryption based tools, to IPSec technologies, but will they hold up in a court of law? Will a court of law or jurors truly understand the extent of someone perhaps spoofing an address? Injecting data into streams? Recreating a complete digital copy of an identity? You could think of bringing in a computer security expert to explain these technologies to a jury, but if you're the accused let me tell you firsthand the jury will be confused, uninterested, and if you're unlucky as I was some may even sleep through large portions of your trial.

So what about the victim of a crime such as this? It would be extremely lengthy and expensive trying to prove their innocence to a jury who will most likely not understand technology on this level. Is there hope for someone who cannot afford to prove their innocence, sure there is, fight all the way but what it all boils down to is a jury's perception of you. What is said during the trial. During my trial for instance, my ISP and phone company stated I did not use the phone at the time the supposed attacks I committed took place, nor was I online, however an FBI agent stated I had "broken into CIA, FBI, NSA, and Military computers" and I "wasn't being charged with that right now." What would your perception have been towards me? Anyway this is irrelevant as a jury managed to fall for the confusion of some FBI computer expert who stated he didn't know or understand what an IP address was. (Boggling isn't it? A so-called computer expert) So what is that telling you should you fall victim to someone trying to stick it to you?

Today we see governments all over the world quick to jump the gun on investigations often passing up on critical information often making drastic decisions. Consider the matter with the President of the United States supposedly being duped by forged documents. We see juries who would not know the meaning of TCP/IP with the power to free or convict anyone on trial with the greatest of ease. So again ponder the thought. How easy would it be to frame someone? Moreover from that thought how do you protect yourself from you being the victim of someone whose intentions are to harm you? Its not a simple answer, it is one that must be thought about with the greatest care and efforts.

"HOW OFTEN THE OPINIONS OF MEN ARE WRONG IN JUDGING IMPORTANT MATTERS."
Niccolo Machiavelli Chapter XXII The Discourses.

Using tools on sites such as SecurityFocus, one could easily create the perfect scenario to cause damage beyond the typical extent of placing a bloody glove on someone's doorstep without anyone ever knowing how it was done. Spoofing, which isn't a new technique, can be so dangerous that anyone with the least technical skills can achieve with ease. Everything from How-To's to programs to automate these tasks, which again can be utilized by anyone with basic to an extreme amount of knowledge of computing.

In a typical environment, measures can be installed to prevent these types of actions from happening, but again the sad reality is, with today's extensive amount of readily available information and techniques, prevention may be far away from fully securing yourself against this type of warfare. Along with that, comes the common knowledge that between every single point connecting you to the rest of the world, all would have to have secure links within the connection and so on and so on.

How many times has anyone gotten spam from an address that seemed rather odd? I know there were times I sent out joke e-mails to friends with odd address on them and it was rather easy. As for the IP addresses, those too can be spoofed with tools like Nemesis, some proxy addresses, or by anyone with enough skills to execute a spoof for whatever underlying factor.

So while everyone screams for privacy against tools like DCS1000, I often see that with so many insecure systems and new technologies being circumvented on grand scales, there isn't enough mention of instances such as the possibility of someone ruining a life via these means, and how to protect oneself from a situation as this. All I see are cases of agency bigwigs trying to close a case faster than gathering thorough evidence on a crime. Maybe they do so to buffer their resumes for future private sector positions, and the notion that they are fighting a "cyber-war" declared on mainly teenagers.

Congress spent about 2 billion budgeting money for so called security in 2001, and the private sectors went ballistic with their own budgets creating or purchasing the latest gadgetry and tools to protect themselves, but we still see little mention of actual crimes other than what can gather oohs and ahhs in the media. All I see is highly watered down information which have hints of people who aren't really interested in crime and criminals but rather how much money can they make, or how many products can they sell in the process, or some case of which they can high five themselves because they arrested someone they define as a "heavy hitter" of sorts.

Instances such as these are a bit reminiscent of many slander cases on which someone may have their career or life shattered with the same effect. Consider a teacher or maybe even a politician, who has been accuses of touching a kid, or someone in the financial field who is rumored to have been doing some insider trading. Even if proven in court that nothing happen or nothing existed, the level of trust among his peers would suffer. Its not easy to protect oneself from situations such as these, and in a vast network of improperly configured gigabit connections, where 14 year olds dictate how long a site stays online with their boring DoS attacks, law makers and law enforcement should take greater strides to "not" target the wrong person. Unless of course they are being promoted to a new division of their office because we all know, it is a dog eat dog world out there.

"FALSE ACCUSATIONS ARE AS HARMFUL TO REPUBLICS AS THE BRINGING OF PUBLIC CHARGES IS USEFUL"
Niccolo Machiavelli Chapter VIII The Discourses

Maybe someday soon lawyers can jump on the bandwagon as well and make the same figures as private sector and government agencies sorting out right from wrong on a technical and morally ethical scale from this type of "Selective Justice" running afoul. Until then though, many should really think about how much they trust technologies, and they should be aware of the inherent dangers of them.

Pretty Good Privacy Doesn't always cut it

Gathering someone's PGP signature is an easy task and has become so typical in the course of a day that one should question whether or not information can be forged by anyone on the fly without the need of expensive equipment and also without the need for attempting to crack someone's PGP key to be able to sign a document as the person your going to forge. (Don't worry much about the dates since this is an update to a file I started in 2000).

From: J. Oquendo sil@antioffline.com
Subject: PGP Test
Date: October, 24 2000 2:39:37 PM EDT
To: sil@antioffline.com
CC:

-----BEGIN PGP SIGNED MESSAGE-----
This is a test of integrity.

sil@antioffline.com

-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 6.5.3 for non-commercial se

iQEVAwUBOa1U5CLUtNYLY2+xAQGghAf/XLn6YFWkZI86KnWCLhIhWiM1LTgPz/V8
BjrBvS8Z4uaI0v2mC1353UJw3xx1mBK6RDF2ovqsY1/TIn1K1U7YaqLW8ZfNL1kI
v0Rz0DT7vXnAmBqKvWVud9NBCRXXwoCQ7+44FWKjRp9Ug/p0H/gEvVjQcfRD8WnL
KZ9z/PzGZeHHTlEONKgPINDKdqMuEVk1DybI9HXXb5jPj0Fr3eu93y+/HZym9rRk
jCZZBu/01tzKrpsxqVQEN5Z1exC4gFwfLmHcp5w+qSzqX/h2KkXuALnhrqbZ/7U9
T1lZK5qZ+uYk2vKkvo/+cRqlKQt20Um0zwyAARmI7laEW6qwCkjtkA==
=PO+3
-----END PGP SIGNATURE-----

This is a valid signature that identifies me as the sender (in theory) and can easily be copied by anyone who comes across any email that I send. (Obviously) But how many people actually use PGP when verifying someone's signature other than those in the security related field, or those who are extremely conscious about security. Now supposing someone wanted to use my signature in effort to maybe cause a rift between a friend, and myself would it be possible? Even with PGP?! Sure it can, and I'll explain why.

Using nothing but typical tools anyone can save this same message if I sent it to them and abuse it. Using nothing more than a Linux based workstation lets see the havoc.

```
1 # hostname antioffline.com
2 # adduser sil
3 # sed s/"This is a test of integrity"/You will die soon"/ savedmail >> badmail
4 # chmod 777 badmail ; mv badmail /anywhere ; su sil
5 $ mail -s Die someone@veryimportant.com < /anywhere/badmail
6 $ pgp -w /anywhere/badmail
7 $ exit
8 $ userdel sil
```

What we see on Line 1 is a hostname changed to reflect to my site followed by someone me as a user in Line 2. Line 3 is the replacement of the words, which were originally e-mailed to reflect something negative.

Line 4 changes the permissions on the file and moves it to a predefined directory, followed by the user assuming the identity of sil. Line 5 the attacker sends out the changed e-mail to someone@veryimportant.com who was possibly an employer, a politician, or other.

Line 6 PGP wipes it from the disk which means it will not be retrievable followed by the user exiting from the created account in Line 7 and the deletion of the account in Line 8.

While this isn't high tech, anyone unfamiliar with checking addressing can be victim to attacks such as these and there is little that can be done to prevent these issues from arising on a wide scale simply because administrators on a wide scale do not take the preventive measures to filter out what information can be sent from where on what network. (spoofing that is) Of course for those using PGP, we would know right away the message was never sent by me, however try explaining that to a jury that might not even know how to turn on a computer. Or a juror who's favorite TV shows are Law and Order, Judge Judy, etc., if you're the accused. I sincerely sympathize with you.

Addressing (IP addresses) can be circumvented also. One of the best tools I've seen in the past was Hailstor, which can sniff and modify packets allowing someone to capture data and resend that data with spoofed addresses, checksums, you name it. So what's one to do to prevent a situation such as this from creating disaster for someone? Well for one a sender can PGP sign all of their messages but it may not be sufficient in most cases since not everyone uses PGP, which would make things difficult. If a user needs to sign a message to show its credibility they would typically sign a message with a signature which can easily be checked with PGP, but again if someone is not validating signatures when they receive a mail, an attacker can ruin someone's life this way too. *But I would* *never fall for that.* Would be the typical words anyone can use but the truth is everyone falls victim to mistakes and errors in life and there is little consolation to someone who's life has been ruined by digital crimes.

Now what do you do when during the following scenario:

John P Quota works as a Chief Technology Officer as IShaftYou Corporation. After dedicating much time to the company John is offered a job elsewhere. His employer upset with John decides John will have to pay. After speaking with the IT administrator, John's boss allowed a keystroke logger to be installed on John's machine. Now John signing a Non Disclosure Agreement never paid much attention to the part which stated the company has the right to `basically do what they want.`

While John was answering mail in typical everyday fashion, his PGP password was recorded. What now? It's your word against someone else's, and keep the following in mind, if you are the accused, again I sympathize with you. Getting a jury to understand the fundamentals of it all will nearly be impossible. If the trial lasts more than two weeks, expect to see upset jurors eager to hurry and get this over with. The more you try to explain the technologies and techniques, the more confusion you will add to the trial and if you're unlucky like me, your jurors will also sleep during portions of the trial.

Packet Engineering

The packet layer is not more difficult than one would expect. It is a well known fact among those in the security field, that networks all around the world would have to be entirely secure in order to prevent a malicious user from sending bad data, and creating havoc using the identity of someone else. This does not apply to networks running IPSec where Point A and Point B are predefined although they too can be trivial.

Only when (without tunneling and IPSec based technologies) the entire connection between every single host, router, switch, and machine connected to every host connected to every other and so forth, can we be sure of the integrity of data traversing a network as being secure.

Spoofing packets throughout a network isn't a difficult task as some may think it is, and there are many programs which will automate it for you. DHCP spoofing where we think of a typical person logging into their ISP, authenticating via a username and password combination and being assigned an IP address is something many have overlooked, and it should be explained in more detail, however I am not going to write about it so hopefully this old snippet will give an idea.

> ***To: Vuln-Dev***
> ***Subject: Re: IP Spoofing with DHCP ?***
> ***Date: Mon Sep 18 2000 15:09:57***
> ***Author: Nathan Einwechter < ceo@investigatecanada.com >***
>
> *Actually, this has been an attack which has been demonstrated, written on, and used in the cable networks which are currently present.*
>
> *What you can do is basically DoS, or wait, untill the other persons box is down. At this*

> *point, it is possible to statically assign your IP to the same as yours.*
>
> *Using this method, you can effectively frame someone for doing net attacks etc. There may be other interesting things you can do with this hijacking of the IP though, which I haven't thought of. It is also possible to hijack an SSL or HTTPS session if this is done with the right timing, and a packet sniffer is utilised. I have actually demonstrated this a few times in the past.*
>
> *Hope this helps.*
> *Original Posting*

Packet Injection Tools such as Nemesis may allow for tactics such as forging information into an existing data stream or creating a new stream of data filled with bad information as anyone you'd like to assume the identity of, quickly, effectively, and possibly criminally. Blind TCP injection of data along with some careful mathematics of sequence information can quite possibly cripple even the toughest firewalls as was proven many times judging by the mirror of hacks on some of the top sites on the Internet. NASDAQ, New York Times, E-Bay, I highly doubt any of these sites had any phf, Cold Fusion, IIS issues, yet still someone was able to bypass most measures to get in.

Could someone have sniffed out data and perhaps injected information into a datastream of the webpage editor while he was editing a site, causing his firewall to think he may have been uploading a defaced page based on only his packet information? (Sequence Number, ID, IP)

It is very possible and not far-fetched and one wouldn't need to see the resulting ACK packets to perform such an attack.

Borrowed from **"A Stateful Inspection of Firewall-1"** and merely used for references on the extent of spoofing on the firewall level.

> *IP Spoofing Protection IP spoofing protection on FireWall-1 is configured per network object at the interface level. Several options are possible, but the typical configuration looks something like this:*
>
> *DMZ and intranet interfaces set to ``This Net'' or perhaps ``This Net +'', restricting valid source IP addresses on the interface to those directly on its network, or routable to its network.*
>
> *External interface set to ``Others'', disallowing packets purporting to originate from any of the DMZ or intranet networks.*
>
> *While this configuration seems simple enough, it leaves out spoofing protection for one important IP address -- the external interface of the firewall.*
>
> *Denial of spoofed packets coming from firewall interfaces is apparently enabled by default in all versions of FireWall-1 other than version 4.1 Service Pack 1. Coupled with*

> *the default rule to allow ISAKMP packets, this hole allows an attacker to send any UDP datagram to the external firewall interface.*
>
> *Another possibility for evading IP spoofing protection is to use the all-hosts multicast address (224.0.0.1) as a mechanism for delivering packets to the underlying operating system of the firewall. For our demonstration, we used FWZ encapsulation to spoof a packet from the multicast address to our attack host, allowing us to respond with a packet sent to the multicast address, passed on to the firewall itself.*
>
> *This attack can also be performed with broadcast addresses.*

So now it should be re-stated that even with preventive amounts of crafty work, a user could pretend to be someone he or she isn't on most levels of networking. Now in order to not jump off base, I'll try to keep in focus the Packet Layer. The attack begins using my account as the victim and another account as the attacker, which we'll call rwxr--r--. (which is my irc handle)

rwxr--r-- is upset with sil@antioffline.com simply because he is jealous and wishes to discredit him and everything surrounding him. rwxr--r-- happens to be a pissed off co-worker who decides he wants to make it seem as if sil is going to issue DoS based attacks to the NSA.

rwxr--r-- jumps online and sees sil in irc and does a simple /whois lookup in order to gain his information.

```
| sil (sil@dhcp517.someinternetprovider.com) (Internic Commercial)
³ ircname : sil
| channels : @#unixgods @#antioffline @#politrix @#/dev/fsck
³ server : irc.Prison.NET (The server that Elian Gonzalez IRCed from...)
: idle : 0 hours 0 mins 4 secs (signon: Wed Jul 25 18:13:49 2003)
```

Using this info rwxr--r-- gains sil's user info and traceroutes the address of dhcp57.someinternetprovider.com (Obviously a sample address) and goes out and downloads APSend, Jolt2, Punk, and Smurftools in order to launch multiple attacks using sil's address he resolved with a simple look up. Here are the explanations for these tools.

apsend.tar.gz

TCP/IP/UDP/ICMP packet sender with syn flood, land attack(=DoS attack against Win95/98/NT), DoS attack against tcpdump 3.4 and **spoofing**. It also includes socket functions (netcat like) and a lot of other options like Time to Live(TTL), Type of service(ToS), sequence number, ack number, urgent pointer, SYN/PUSH/ACK/RST/URG/FIN flag, window size, number of packets to send and so on. It can be used to test firewall configurations or other network applications on your :)

hosts/networks.

Jolt2 is a denial-of-service program. It can be used to bombard a remote computer with a constant stream of data packets. This is supposed to lock-up the remote computer by causing 100% CPU usage while the Trojan program is running. In reality, it is unlikely to greatly affect the target machine, however it will use a lot of CPU time on your machine and cannot easily be terminated (you can terminate it via the Task Manager program - hold down Ctrl-Alt and press Delete). The large number of packets that the program sends each second may cause a significant slowing down of the local network.

Punk is a Syn Flooder code with spoofed source address

Smurftools is a simple ICMP Source Address spoofing utility. A smurfing utility that also comes with log parser

These programs generate spoofed Denial of Service attacks with a few keystrokes, and the sender can be forge any address he chooses in an effort to make it seem as anyone specified has sent them. Its a very dangerous game to play and people will play it. Hailstorm is definitely a tool for any security administrator to have, as far as I remember, as it has many features for testing security on a network. It also has the perfect necessities for someone to forge data via methods of spoofing in an elegant fashion. Anyone with bare knowledge of TCP/IP and motive may use a program such as this for causing other havoc.

Using the sniffer function of the tool, lets say John and Joe are employees who are at odds because Joe received a bigger salary for a lousier job, Joe who may know a bit about TCP/IP and security decides he just wants to get even, besides Joe just purchased a brand new house and brand new car and without a raise he won't be able to afford the luxuries or so. Joe decides to sniff the network using Hailstorm and focuses on packets designated for Joe's workstation. He notices Joe has his banking information online and decided to assume Joe's identity and tinker with his accounts, while this may seem a bit outrageous and dangerous, Joe simply has to watch the sessions and get a couple of packet captures using Hailstorm. After a day or maybe even a week Joe has filtered out the packet information and is only filtering when money is being transferred or a bill being paid. Hailstorm allows you to recreate full packets including payloads, sequences, addresses, you name it, and Hailstorm is not the only program to do so. Joe modifies a packet to inform the bank to pay something John did not agree to, or perhaps transfers funds into some account. Get the picture?

Sure John will fight to the finish in court, but in the digital sense, the bank's connection gathered the information from John via his IP address which is the bottom line that any prosecutor will point to, but is not correct and should never be thought of as a definitive way to identify someone especially on an Internet of billions.

May sound lame, people may think its ludicrous but it can and I am sure it has happened in the past and will eventually be something which law makers, lawyers, courts, experts will have to recognize and weigh factors when dealing with "e-related crimes". I know for a fact **** happens. I've seen it done. So while this article may not have been PhD thesis material, I would hope many would find interest in it, and I sincerely hope no one else get shafted, remember Murphy's law.

Jesus Oquendo
39A7 24C6 A9A0 6C67 96CA 0302 F1D3 2420 851E E3D0
sil / segment
http://www.politrix.org
http://www.antioffline.com