VEGAS SPECIAL FILE #1
BY
VEGAS

May 26, 2006

[Updated July 7, 2006]

INTRODUCTION

I have seen a great deal in my twenty plus years of trading [both on the floor and off], and it never ceases to amaze me how otherwise smart people can and will do things that cause themselves [and their families] great financial harm.

When I first started trading in 1980, many veteran floor traders had already made enormous fortunes in gold, silver, cattle, and currencies. What I remember most, though, are the traders who made huge fortunes in the precious metals. You could always spot them on the floor because of their swagger and belief they could never do wrong. When markets quieted down in the months and years thereafter, almost every rich trader I knew from 1980 was dead broke by 1985. It was a painful thing to watch as trader after trader refused to adjust to new market paradigms. The reasons were many and varied, and it is not my intent to dwell on them.

Here is a shocking observation [from all my years of trading] about most traders: direct trading isn't what brings most of them down. It's not the X's and O's of trading per se that cause the harm. It is all the secondary, tertiary, and on down-the -line, issues that pile up during life that do the trick. What are some of these? Well, secondary issues that are right at the top of the list are 1) discipline, 2) risk management, and 3) emotional self-control. Tertiary issues would be things like 1) trading while getting a divorce, or 2) trading after a big emotional event like a loved one passing away or becoming disabled, etc. I hope you get the idea. Most often, it is outside forces that bring about changes in the paradigm we live. Think for second how your life would change if New York got hit by an atomic weapon. Can you imagine 50 years into the future, from this event, a chain-link fence wrapped around half of New England due to the fallout? Forces would be unleashed that would change your life even if you lived in Paris, France.

Since the start of 2000, the changes that have taken place in how financial markets are traded are staggering. The rise of electronic trading and the demise of pit trading, in six years, has brought about a completely new way to trade markets. Issues that were once important no longer have any significance. Other issues, which nobody could have dreamt twenty years ago, suddenly become a very big deal.

It is to these “new issues” that this file is dedicated and written. Specifically, it is to uphold and vigorously protect your privacy, security, and anonymity while you are online and trading. It is to make you completely invisible to the prying eyes of Government and every other wannabe [hackers] lurking out there who wants to make your business their business. Are you completely safe? I'm betting you are not, and that is why I am writing this special file. After reading this, you will have the information you need to enable the most up-to-date protection you can get; military grade encryption from start to finish, without the need of being IT [tech] savvy. Cost you ask? It depends on how paranoid you are, but roughly anywhere from US $ 125 to US $ 250 PER YEAR. Yes, that's right; it is ridiculously low and affordable for everyone.

Now, the best part: IT IS COMPLETELY ANONYMOUS TO IMPLEMENT. ALL PAYMENTS CAN BE MADE WITH E-GOLD, THUS INSURING YOUR ANONYMITY AND PRIVACY.

A couple of months ago [from this file writing] I wrote 'Vegas Wealth Builder Part III'. As most of you know, this file deals with the many issues of taking your affairs “offshore”. It is fifty [50] plus pages of the what, where, how and why of doing it the right way. If you wish to cut through all the crap and learn the details of a proper offshore structure, then this file is worth every penny.

'Vegas Special File #1' is completely compatible with VWB III. Everything you learn in this file can be implemented while being offshore. For those who purchased VWB III, rest assured I am not giving away any of the offshore details found in the file. What I am doing is taking your offshore structure to the next level, thus insuring all of your planning and work will be safe and secure from prying eyes.

Not everyone needs an offshore plan [yet]; but everyone, regardless their circumstance, needs [and should demand] privacy, security, and anonymity while online [and not just online either; all of us should demand these liberties in our lives]. Sadly, this is not the norm in today's environment. In the 50's and 60's it was the war against communism. In the 70's, 80's, and early 90's it was the war on drugs. Since 1993, it has been the war on terrorism. Government always finds an excuse for shaving away our liberties.

You are simply delusional if you think that while you are online [connected to the web], and you haven't implemented the information in this file, that you have some sort of privacy and/or security. Anonymity is totally out of the question; any 7th-grade hacker can finger your IP address in seconds. Between the Government, Microsoft, Google, your ISP, and the zillions of hackers out there, somebody is always trying to find out who you are and what you are doing. Do you want any of these to know where you are trading? Are you comfortable knowing practically anybody can find out your web surfing habits? Is your email secure? How about messaging and chat; are they secure? If you are offshore, do you really want the Government knowing you spend 20 hours every business day at a certain brokerage-house IP address, or log in every day to that offshore bank IP address? How comfortable are you with the fact your ISP knows more about you than your spouse? They track every single click of your mouse and follow you everywhere. I find all these events deplorable, and it is the main reason for this file.

In the chapters that follow, I am going to lay out in detail all the necessary steps you need to take in order to bullet-proof your online activities. Consider each Chapter a step that needs to be implemented before moving to the next Chapter. I encourage you to read and reread this file as many times as necessary before you set things in motion. I have endeavored to make things as clear and simple as humanly possible by assuming most of you are tech idiots. Please, don't take offense if I just insulted you: try and understand the plight of the tech newbie by remembering when you first started trading and were a newbie as well.

Each **APPENDIX** at the end of this file is an important read. **APPENDIX D** is technically oriented and for those who are not very IT savvy, it will be a tough go. That's OK, just skim it to get the idea the author is trying to convey to his readers. I think most of you will be shocked and disturbed by what you read in some of the **APPENDIX.**

I wish I could take credit, for the term I saw used, in describing this “no existence”. It isn't offshore, it is “UNDERSHORE”. What a perfect name. Oh, you're there at the beach alright; it's just that nobody knows you are there because you are buried conveniently in the sand. With all the other specks of sand [billions] you sit perfectly situated. Mixed among all the other specks, it is impossible to a) know you are there, b) know you even exist, and c) know what you are doing on the beach.
And that, fellow traders, is how we want to be situated. So let's get started with the first step.

CHAPTER 1
FIRST THINGS FIRST: DITCH MICROSOFT

At the user level, most of the world runs on the Windows Operating System, and it is very difficult to trade and do other tasks in Mac or Linux. So, I'm not talking about ditching Windows XP, but I am suggesting that you immediately stop using IE [Internet Explorer any version] and Microsoft Office. The security flaws and bugs in these two applications alone are reason enough to replace them with BETTER, MORE SECURE, application software.

Specifically, replace your IE web browser with MOZILLA FIREFOX VERSION 1.5.0.3 [or higher] FOR WINDOWS. If you use Microsoft Outlook as an email client, you will find a BETTER, MORE SECURE email client with MOZILLA THUNDERBIRD [Note: If you don't use an email client, don't worry; FireFox doesn't need Thunderbird to run or operate. They are separate applications. And as for email, later you will discover the BEST and SAFEST email account to use, with military encryption for your protection and security. Of course, it will be simple to use and free!! But, that comes a little later.] Both can be downloaded [for free of course] at the following URL:
http://www.mozilla.com

For those of you who are unfamiliar with FF [FireFox], it is an open-source browser offering the best in security and functionality. Anything you can do with IE, you can do with FF [As you will see, there are a lot more things you can do with FF.].

If you are hyper-ventilating because of the idea of not having your beloved Microsoft IE, I have a simple question for you. Do you still use a rotary dial phone? [I didn't think so.]

After you download the file, install FF to your hard-drive. To install, simply follow the on-screen instructions. Make it your default web browser.

****
OK, you have now finished step 1: download and install FF as your web browser. You are now using FF as your web browser. The IE icon just sits there and looks pretty on your desktop. From now on, you are using FF just like you used to use IE. NO MORE IE.

****

At this early stage, it is time to introduce you to the FF EXTENSIONS. These are small add-on programs that attach to FF and improve its functionality greatly. There are literally thousands of these programs written by the software community, and they are free to download and use in FF. They cover every subject area, and you can browse the titles [with descriptions] when you are at the FF website if you click "Extensions".

One "Extension" that you will definitely need is PREFBAR VERSION 3.3. This places a task bar above your webpage and allows you to control practically everything that happens when you open a webpage. For importance to us, it allows control of JavaScripts, Java, and Pop-Ups [each has a button; check to activate, uncheck to deactivate.] It also includes buttons to Clear Mem Cache, Clear Disk Cache, Clear Cache, Clear History, and Clear Cookies. Also, you will later need the item "Proxy Serverlist" in this taskbar [More on this later].

To get this extension, go to the following link:
http://prefbar.mozdev.org/

[Note: If, when you try and download this extension, it seems as if nothing is happening, please look up at the top of the webpage window. There may be a message line that says your download is being blocked by FF until you give permission for downloads from this website. Click on the options button that appears immediately next to the message at the end, and allow for the download. You only have to do this once.]

If you now close FF and reopen, the PrefBar will now appear near the top of the webpage.

****
******
OK, you now have completed step 2. PrefBar v. 3.3 is installed in FF and can be edited by us later.

[Note: Although it is not absolutely necessary to get rid of Microsoft Office, a better alternative is the open-source office suite from Open Office. It is fully supportive of all Microsoft extensions and is totally functional with other Microsoft applications. However, it doesn't have the security flaws and bugs that bedevil Microsoft Office. It is TOTALLY FREE and open-source and supported by a large user community. You can download the entire package at the following link:
http://www.openoffice.org

For your education and enlightenment I would ask that, after finishing this Chapter, you go to **APPENDIX A** through **APPENDIX F** and read the material there. Believe me, this is just the very tip of the iceberg, when it comes to security flaws involving Microsoft, Google, your ISP, and the never-ending need for Government to know what you are doing. Without ever getting your permission you may be unwittingly giving up a lot more information than you realize. Please return at your leisure.

CHAPTER 2
E-GOLD

By now, I hope most of you have created an E-Gold Account. If not, now is definitely the time to do so. If you don't have this e-currency weapon in your arsenal, then it is time to get in the year 2006 and leave the 20th century behind. It only takes a couple minutes to create, and is extremely safe and easy to use. There are NO documentation requirements, so you and you alone determine what you want to tell the E-Gold people when setting up the account. You can be completely anonymous if you choose, because really the only thing that matters is the pass-phrase. He who knows the pass-phrase owns the gold!! If you are unfamiliar with E-Gold [theory and uses], spend some time at their website and become familiar with its operations and uses.

[Note: I will revisit E-Gold later, in another Chapter. For now, it is enough that you either have an existing E-Gold Account OR are creating one now.]

To create an E-Gold Account, please follow this link:
http://www.e-gold.com/

OK, you now have finished step 3; you have just created or have an existing E-Gold Account.

CHAPTER 3
FUNDING YOUR E-GOLD ACCOUNT

Obviously, since you just created an E-Gold Account, it has a $0 balance and must be funded. At this stage, any reputable third-party exchanger is OK. If you choose to fund your account with more than USD$ 2,5000.00 I would recommend EuroGoldSales. Please follow this link:
http://eurogoldsales.com

If you are going to fund your E-Gold Account with LESS than USD$ 2,500.00 I would recommend GoldAge. Please follow this link:
http://www.goldage.net

OK, you now have finished step 4; you have funded your E-Gold Account. You are now able to spend money [in any currency via gold] for goods and services with privacy and security.

CHAPTER 4
TIME TO GO "UNDERSHORE"

Most of you, I assume, have a direct connection to the Internet via cable modem or DSL. Regardless your firewall, virus protection and wireless router, you are naked in front of the world.

The only way to gain complete privacy, security, and [just as importantly] anonymity while online is to be connected to a VPN [VIRTUAL PRIVATE NETWORK]. In simple English, a VPN is a "TUNNEL" that wraps everything you do into an encrypted "SHELL" that protects ALL of your information from being seen by others. Protected by military-grade encryption, it is virtually impossible for someone who steals your information online to make any sense of the data.

Equally important, is who hosts this network and what type of logs they keep on your activity. Ideally, they keep no records whatsoever. Their motto is “DKYC” [Don't Know Your Customer]. They don't want to know anything about you. They don't take credit cards, because that means they know you. THEY TAKE E-GOLD BECAUSE IT IS SAFE, SECURE AND ANONYMOUS.

The Host also knows that most of the world knows zip, zero, nada, zilch about VPN's and the Linux and Unix commands that make them run. I can't speak for anybody but myself, but if I'm going to be connected to a VPN I don't want to have to become a total computer geek just to get it up and running. And if I have problems, where do I turn? Is there decent customer support or am I on my own with this?

More things to ask of the Host. Where are these guys servers located? In friendly information havens, or in countries that will demand data? Can I switch server jurisdictions at the click of a mouse, so that my VPN TUNNEL can be everywhere but nowhere? Oh yea, how about email; can I get the same protection with that as I can with surfing the web using my browser? By the way, I'm not exactly the richest person in the world. I need this at a very low and ridiculous cost. How about just a few Whoppers per month for cost?

Well, fellow traders, such a Host does exist and I have been using them with complete satisfaction. I am completely anonymous to these people. I paid in E-Gold and they don't even know I exist. Let me answer the above questions.

1) My VPN TUNNELS [yes, I have more than one] were created with a Windows GUI that was so easy to set up a 10 year-old kid could do it in a few minutes. To activate the TUNNELS I simply click on the icon on my desktop and they are up and running. They stay running until I either a) shut them down manually [why would I do this?] or b) shut my computer off. Closing the FF browser does not affect the tunnels. They are always up and running if the computer is on. How easy is this? They are totally silent and working in the background.
2) Everything can be set up and running within minutes using their GUI “The Tube 1.0”. With the application comes a manual that tells you how to set the tube up. If you have problems, their technical support is readily available to help you with any problems.
3) Before you sign up, you decide a) how many tunnels you want, and b) which servers to choose. Currently, they offer 1 to 6 tunnels with the following locations: Holland, Germany, Malaysia, Hong Kong, USA, and the Czech Republic. The key here is to choose servers in countries as far from your physical presence as possible. So if you live and are a citizen of Hong Kong, the USA server would be OK. However, if you are a US Citizen, the US server is the last place you would ever consider. My experience is that Holland is very fast and would be my first choice if you were to only use one tunnel. The choice, of course, is totally up to you.
4) After you decide how many, you must consider cost. The cost of one tunnel is 100 EUROS/YEAR.; the cost of any 2 tunnels is 150 EUROS/YEAR.; the cost of any

3 tunnels is 180 EUROS/YEAR.; the cost of any 4 tunnels is 200 EUROS/YEAR.; the cost of any 5 tunnels is 220 EUROS/YEAR.; and the cost of all 6 tunnels is 240 EUROS/YEAR.

5) With the exception of the US server, all servers [tunnels] are located in data-friendly countries with no questions asked or any data logged about your activities. No logs, no nothing. Remember that “Proxy Serverlist” that I mentioned earlier, that is in the PrefBar 3.3 that you downloaded? Well, that's how you switch servers [tunnels] at the click of the mouse. For example, let's say you have 2 tunnels; one in Holland and the other in Malaysia. Your surfing, and you decide to switch from Holland to Malaysia. All you do is go up to “Proxy Serverlist” and check Malaysia, and either refresh the webpage, go to a different webpage, or close the browser and reopen. Bang! You are now operating through a different server in a different country. Everything you do is now redirected to a new location, where again, no questions are asked.
6) With each server [tunnel] you get an SSL encrypted WEB-BASED email address at the host sight at no additional cost. This is the same encryption technology that is widely used for web credit card purchases. Everything in your email account is SSL encrypted. Now, if you communicate with other people who have an SSL encrypted account as well, then EVERYTHING from point A to point B is totally safe and secure. If you know very little about PGP encryption [the most popular] then this is a dream scenario for you as you don't have to do anything but sign up for the service.
7) As for cost, even the cheapest of you should be able to afford the cost of one tunnel. At 100 Euros/Year, that comes to about USD$ 10/month. A few trips to Burger King will set you back more than this.
8) Now, you can do a ton of surfing and looking all over the net, but they offer the best product [The Tube 1.0], with the best service, and most importantly the right attitude regarding my privacy, security and anonymity. I don't think they can be touched by anybody else.

Now, before I introduce you to these fine privacy people, I would like to ask that you spend some time absorbing everything they offer on their website. It is a complete treasure trove of very good information.

After reading this Chapter, please go to the following link:
http://www.privacy.li

On the left-hand side of the page under Services [near the top] you will see a section titled “Privacy-Tunnel”. This is a must read, and will supplement the information I have given you plus some other very important information. In this section you will learn how to order your tunnel (s). Using E-Gold, it couldn't be any easier.

After you pay for your tunnel (s) and instruct them which one (s) you want, they will email you with your user ID and password for each tunnel. They will also give you the URL where you can download the self-extracting zip file “The Tube-GUI _winfortunnels”.

[Note: By far the easiest way to set up the tunnels is with the windows GUI they offer. They also offer the application “Putty” which will also do the same. Please read the entire manual for important port information.]

OK, you have now completed step 5; you have just purchased the best privacy, security and anonymity VPN protection available on the net. You are ready to set this puppy up and get going [the next Chapter].

CHAPTER 5
EASY INSTALLATION USING “THE TUBE 1.0”

You have downloaded the self-extracting zip file “The Tube-GUI_winfortunnels” and it is sitting on your desktop. When you unzip the file, you will get two [2] files. One is the manual and the other is the application. At your leisure, you may read the manual for other important information regarding “The Tube 1.0” and/or “Putty”.

As a service to everyone, newbie and experienced alike, I am going to guide you through this installation step-by-step. My instructions will save you some time since I have done this on my own system and am familiar with the procedure.

The following information is needed in order to determine how to set up your tunnel (s):

UID [username provided by adminus at privacy.li],
PWD [password provided by adminus at privacy.li],
HOST [TUNNEL]: bull1.hereno.info - This is the Malaysia server,
HOST [TUNNEL]: grizzly.ns666.com - This is the Hong Kong server,
HOST [TUNNEL]: sam.hitrust.net - This is the Czech Republic server,
HOST [TUNNEL]: neon.trighost.org - This is the Holland server,
HOST [TUNNEL]: dark.lastunicorn.info - This is the Germany server.
I am assuming nobody wants the US server.

The destination ports for each server are as follows:

Grizzly is 4912
Sam is 4567
Bull is 4192
Neon is 4910
Dark is 4111

All servers use SSH port 22, except trighost which uses SSH Port 4022.

Also, localhost = 127.0.0.1

Now, if all this is Greek to you don't worry. This is ALL the information you need to fill in the appropriate fields in “The Tube 1.0”. For example, let's say you signed up for 2 tunnels; Holland and Hong Kong. You received your User ID [UID] and Password [PWD] in an email. Now, the only information you care about is that your HOST for Hong Kong is grizzly.ns666.com with a destination port of 4912, using SSH Port 22. For Holland, your HOST is neon.trighost.org with a destination port of 4910, using SSH Port 4022. That's it!! If you signed up for others, then you would just use the grid above and fill in the blanks as I have outlined.

It's now time to open the application [The Tube 1.0]. Each tunnel that you sign up for must be created individually, so with each tunnel you would repeat the step-by-step process below.

Here is the step-by-step process.

Step 1.
Open the application. A box appears titled “Create Or Choose SSH Connection”. Choose create NEW connection.

Assuming you purchased the Hong Kong server [tunnel], you enter the following information from the grid above into the fields in “The Tube 1.0”:

SSH Host: **grizzly.ns666.com**
SSH Port: **22**
Encryption Cipher: **Blowfish**
User Login: **Put in “username” chosen by you and confirmed by email**
User Password: **Put in “password” given to you by email**

[Important Note: If you choose a different server (tunnel) than Hong Kong, you must put in the appropriate information in the SSH Host, SSH Port fields.]

HIT THE NEXT BUTTON WHEN YOU ARE FINISHED

Step 2.
This is the “Create or Choose Tunnel” Box.

Check create New Tunnel.

Again, assuming you have chosen Hong Kong as a server, fill in the following fields as follows:

Local Port: **4912**

Remote Host: **localhost**
Remote Port: **4912**

[Important Note #1: localhost is in small letters with no space.]

[Important Note #2: Your computer has about 65,000 ports. The smaller number ports are used for specific things. For example, port 110 is used by practically all computer systems for receiving POP3 email. The higher you go up, the less likely your computer is using a port. However, some ISP's block higher ports to prevent hacking. For my money, it's very easy to just use the same port as the server, but if you so desire, you can use any number that is free in your system. I'm betting 4912 is free.]

[Important Note #3: All servers (tunnels) will use the Remote Host = localhost]

HIT THE NEXT BUTTON WHEN YOU ARE FINISHED.

Step 3.
This is the "Configure Applications" Box.

Check Browser Box.
Check Internet Explorer
Check FireFox

[Note: Even though you probably won't use IE again, you might as well check the box in case you have to use IE in an emergency or some tech issue arises in your computer and you have to use IE.]

HIT THE FINISH BUTTON WHEN YOU ARE FINISHED.

Step 4.
You get "The Tube Security Alert"

Please Ignore.

Check YES

CONGRATULATIONS, YOU HAVE JUST ACTIVATED YOUR FIRST TUNNEL.

In the SSH section of "The Tube 1.0" you will notice a GREEN lighted box. This indicates the tunnel is active; YELLOW indicates it is ready for use; grey indicates it is turned off. In the TUNNEL section of "The Tube 1.0", you have the same colored box. The colors mean the same as in the SSH section.

If you only ordered one [1] tunnel, then you are finished setting up the tunnel. You may minimize "The Tube 1.0" to the Start-Bar.

If you ordered more than one [1] tunnel, then you must repeat the process [Steps 1 – 4 in this Chapter] **FOR EACH ONE.**

To do this after you created the first one, you simply bring up [or maximize] “The Tube 1.0” and select “Run Tunnel Wizard”. Then check “Create New SSH Connection”. You are now back at Step 1, and can begin the process again for each tunnel you ordered.

We aren't quite finished, though, because we must now configure FireFox to accept these new proxy servers. Here is the step-by-step process to get this done.

Step 1.
Open the FF browser to any page.

Step 2.
Find the PrefBar that you installed near the top of the webpage. Somewhere on the right side is a “Customize” button. Click to open.

Step 3.
If the choice “Proxy Serverlist” is still in the “Available Items” column, then highlight this choice and click the “Add” button in the middle. This will put “Proxy Serverlist” in the PrefBar on your webpage.

Highlight “Proxy Serverlist” in the “Enabled Items” column. Click the “Edit Item” button in the middle.

Step 4.
An “Edit Item” Box appears. Leave the “Set Function” and “Get Function” sections alone. In the “Common” section, under “Item Data” you will see the following information:

ID: Proxylist
Label: Proxy Serverlist

Underneath this is the “Label” and “Value” fields. In the “Label” field you put in whatever nickname you want to call your server. For example, in my personal case, I picked GRIZZLY-HK for the Hong Kong server. In the box put in the nickname.

In the “Value” fields, put in the following information **EXACTLY** as I have it here for the respective servers you are using:

Hong Kong server:	**127.0.0.1:4912**
Holland server:	**127.0.0.1:4910**

Czech Republic server:	**127.0.0.1:4567**
Malaysia server:	**127.0.0.1:4192**
Germany server:	**127.0.0.1:4111**

For example, let's assume you ordered the Hong Kong and Holland tunnels. Then you would put something like this in the “Label” field and the exact information in the “Value” field:

Grizzly-HK	**127.0.0.1:4912**
Neon-Holland	**127.0.0.1:4910**
None	

[Note: When you are finished putting in the nicknames and appropriate value fields for all of your tunnels, you should put “None” in the final label field and leave the value field empty.]

When you are finished click the OK button.

Now click OK to leave “Preferences Tool bar”

Now, close FF and reopen to your homepage. In PrefBar, next to “Customize” on the far right you will either see a “Proxy Serverlist” button or a box with a drop-down menu..

If you have a button, and click it you should see a drop-menu listing your proxy [tunnel] servers with None at the bottom. If you have a windowed box, click on to see server list. Choose one of your choices. Now, either refresh the webpage, go to a different webpage, or close and reopen the FF browser.

Go to the following link:
http://showmyip.com

Here, you will see that you are now connected through your tunnel [to whichever server] to the web. You can change servers at your whim.

CONGRATULATIONS! YOU HAVE FINISHED EVERYTHING . FROM NOW ON, YOU ARE “UNDERSHORE”.

CHAPTER 6
YOUR WEB-BASED EMAIL

To access your Web-Based SSL email from the Holland server, please go to the following link:
https://securemail.trighost.org:563

You will use the same User ID and password that you used to set up the tunnel. When you have logged in, you can then change the password to the account. **Please remember that when you change your password, it affects the tunnel. You have to open “The Tube 1.0” and highlight the neon tunnel and then choose “edit”. You then put in the new password. When you are finished, check and make sure in the SSH section of “The Tube 1.0” that neon is green. If not, highlight and click the on/off button. When it's green, you are OK to go.**

I am assuming, of course, that you will choose neon as a server choice. I personally think it is the fastest server. Not that the others are slow, because they are not. With neon, you shouldn't notice any difference from what you currently have. However, the choice is completely up to you.

I think you will enjoy the use of this email account. It is great for sensitive and important
information. With SSL encryption, you have nothing to worry about if the party you are conversing with has it also.

CHAPTER 7
BACK TO E-GOLD

Now that you have your tunnels set up and you are in “Undershore” mode, it is time to revisit the financially sensitive website of E-Gold.

Many people don't realize that E-Gold keeps very close track of your IP address when you log in. If you use an ISP that uses dynamic IP addresses, every time you log in you will be logging in with a different IP address. By default, E-Gold sets your security settings such that when you log in with a different IP address than the last time you logged in, E-Gold won't log you in to your account without a special pin number that must be entered into a special box within the next 15 minutes. They send your email address of record the pin number. After you get into your account, you can obviously change this security setting, but by doing so you lower the security of the account. It should be noted that even if you change this setting, or have no problem entering pin numbers every time you log in, E-Gold still keeps track of each and every IP address.

What's the big deal? Well, some people like to have multiple accounts and layer their transactions. They think by doing this they can have greater security, privacy, and most importantly anonymity. The problem is that if you have 5 anonymous accounts and they all use your home address IP, E-Gold knows that these 5 accounts belong to YOU!! They link these accounts in their database, so in effect you have achieved nothing.

If, on the other hand, you always make sure to use one of your tunnel proxies, the only thing they [or anybody else for that matter] are EVER going to see is IP 127.0.0.1.

OK, but they still see this on each and every E-Gold Account you have, so what's the difference? The difference is that tens of thousands of people use the proxy, while only you use your home or office IP address. Your home or office IP goes straight to you.

How do we correct this?

Step 1.
Open a NEW E-Gold Account through one of your proxy tunnels. Now that you are undershore, your new Account will NOT be associated with you.

Step 2.
Transfer your balance from your old E-Gold Account to your new E-Gold Account; then never use the old Account again.

Step 3.
ALWAYS ACCESS YOUR NEW E-GOLD ACCOUNT ONLY THROUGH THE SAME PROXY SERVER [TUNNEL]. For example, if you are connected to Neon [Holland], make sure you are on neon every time you log in to E-Gold.

Step 4.
ALWAYS DELETE COOKIES BEFORE ACCESSING YOUR E-GOLD ACCOUNT, AND THEN DELETE COOKIES AGAIN AFTER YOU LEAVE.

Step 5.
Turn off Java, in your PrefBar, when you use your proxy tunnels. Java is not needed on most websites including E-Gold. Enabled Java may compromise the security of your tunnel. See **Appendix E.**

Step 6.
If you have the neon-Holland proxy server [tunnel], use the web-based SSL email account from trighost with your E-Gold Account.

You now have total security, privacy, and anonymity with your E-Gold Account (s).

USE THE SAME PROCEDURES WITH ALL SENSITIVE WEBSITES; YOUR BROKERAGE HOUSE AND BANK FOR SURE.

CHAPTER 8
UPDATED CHAPTER JULY 8, 2006
SECURING YOUR COMPUTER

Now that your network and online activities are secure, private, and anonymous it is time to do the same to YOUR ENTIRE COMPUTER. What I'm talking about is ENCRYPTING YOUR ENTIRE HARD DRIVE. Please go to the following link: http://www.securstar.com

Here you will find DriveCrypt PlusPack [DCPP], the award winning on the fly encryption product that secures your entire hard drive from anyone who has no business knowing what your business is about. I could spend pages raving about this product, but I see no need to be redundant. You can go to their website and surf their site and learn why you should have this product on your computer. Their customer support is excellent [any questions use the online chat feature], and the product is easy to download and install. Of course, you can pay with e-gold. Cost is about USD $160 or 125 Euros.

One of the great features in DCPP is the ability to put a virtual hard drive WITHIN another hard drive so that nobody has the slightest clue you have sensitive files or programs on your computer. [This is known as “Plausible Deniability”.] If necessary, you could give up your entire computer to third parties and they would never know you have a brokerage house application and/or offshore bank files on your computer. NEVER!! It is impossible to distinguish random data stored on your computer [in the free space] from sensitive files that are encrypted. Please see the application help file [not the doc manual that you download] for more information on this operation.

In case you think this is way beyond your technical level, you couldn't be more wrong. Yes, the software is extremely sophisticated, but putting it to work is a breeze. You buy it, you download it, you install it, you register it to your machine, and your are ready to go.

Here is a heads up on what you need to do if you want to get this going ASAP. Once you have the software fully installed and registered, start the application. You need to do things in a certain order, and this is the order:

1. Create a key store [or keyring] with the wizard,
2. Create a key to put in the key store,
3. Encrypt your hard drive [probably C:\]. [Note: This takes about 2 hours for a 100 G HD.]

Of course, along the way, you need to think of a double pass phrase that nobody should ever know. When you boot your computer up, a screen appears for you to enter your double pass phrase. After you enter it, the computer boots up as normal and you are on your way as normal.

Since you need these pass phrases BEFORE the computer boots, nobody can ever gain access to your data by doing anything pre-boot. Before you enter your pass phrases, your computer is nothing but a paperweight!!

Just a reminder: **IF YOU LOSE OR FORGET YOUR PASS PHRASES – YOU ARE SCREWED!!** Nobody can help you decrypt your hard drive if you forget or lose your pass phrases. This software uses military grade encryption and there are NO back door protocols to rescue your hard drive. Without the pass phrases, NOBODY [Not the CIA, NSA, FBI, Local Law Enforcement, or anybody else] can get at your computer and learn what data is stored on the hard drive.

To protect your privacy, security, and anonymity you need this product on your computer. This software is on ALL of our computers.

CHAPTER 9
SUMMARY

You now have the information at your fingertips to become “undershore”. I sincerely hope you take advantage of this information. I want all of you to know that I have no relationship with privacy.li except as a satisfied [totally unknown and anonymous] customer. Same goes for Securstar.

I know that some of you may consider this whole privacy, security, and anonymity issue a waste of time. Maybe you think only people who have something to hide or are criminals would consider such a move. My response to this is as follows: criminals buy clothes, use cell phones, eat food, drink water, and breath air. Are we to ban these also because they are used by the criminal element?

Ultimately, all of us have the right to demand privacy, security, and anonymity in our affairs. Sadly, unless you take the lead you can expect none.

Take the lead for yourself and for your family.

-vegas

APPENDIX A

By Internet Correspondent Chris Nuttall

Cryptographers are sounding the alarm on a major security issue involving Microsoft Windows that could eclipse its Hotmail public relations disaster.

The findings of a computer security expert that America's National Security Agency (NSA) may have been given a back door into every copy of Windows 95, 98, NT4 and 2000 worldwide are being debated across the Internet.

Microsoft has issued a strong denial of allegations of misuse of a second encryption "key" in Windows. "These are just used to ensure that we're compliant with US export regulations," said Scott Culp, Microsoft's security manager for its Windows NT Server software.

"We have not shared the private keys. We do not share our keys."

But cryptographers in the UK described the implications of the findings as "immense". Windows is installed on more than 90% of the world's computers.

Second key for Windows

Andrew Fernandes, Chief Scientist at the Ontario-based Cryptonym Corporation, is credited with discovering the identity of a second key used by Windows for encryption purposes.

Caspar Bowden, director of London-based Internet think-tank FIPR, said: "The allegation is that every copy of Windows contains an extra 'magic number' which would permit it to work with encryption modules designed by the US National Security Agency, as well as those approved by Microsoft."

The approval mechanism was introduced to ensure that the weak encryption in non-US versions of Windows could not be replaced with stronger software without it being checked against a "key" embedded in Windows, proving that it had been digitally signed off by Microsoft.

Two years ago, cryptographers found an alternative, and apparently superfluous, second embedded key. The new details came to light through debugging information erroneously left in the latest service pack for Windows NT.

Significantly, the key has the data tag "_NSAKEY" giving rise to speculation that the NSA persuaded Microsoft to give it special access to Windows in a secret deal.

Microsoft says it called its function an "NSA key" because the body reviews technical details for the export of data-scrambling software.

MS talked with NSA

It is known that Microsoft negotiated with the NSA on including encryption in its product. The export of strong encryption is banned by the Clinton administration, which fears terrorists and other criminals could turn it against the US.

There are two theories on why this unnecessary second key is included in Windows:

Conspiracy theorists say the key can be used to infiltrate targeted computers. It gives the NSA a direct way of doing this without having to use Microsoft's own key. A more charitable theory is that Microsoft allowed the NSA a special key to secure the thousands of government computers running Windows.

"The innocent explanation is that the US wished to create bespoke encryption modules for official use on government systems without reference to Microsoft," said Mr Bowden.

"Ironically, introducing the second key has created a major security loophole in a mechanism which was designed to enforce US export controls on strong cryptography."

Microsoft suffered serious embarrassment on Monday when hackers exposed a simple way of breaking into the mailboxes of more than 40 million users of its Hotmail e-mail service.

*******END APPENDIX A*******

APPENDIX B

Congress and Your ISP

Published: April 28, 2006, 5:06 PM PDT

It didn't take long for the idea of forcing Internet providers to retain records of their users' activities to gain traction in the U.S. Congress.

Last week, Attorney General Alberto Gonzales, a Republican, gave a speech saying that data retention by Internet service providers is an "issue that must be addressed." Child pornography investigations have been "hampered" because data may be routinely deleted, Gonzales warned.

Now, in a demonstration of bipartisan unity, a Democratic member of the Congressional Internet Caucus is preparing to introduce an amendment--perhaps during a U.S. House of Representatives floor vote next week--that would make such data deletion illegal.

Colorado Rep. Diana DeGette's proposal (click for PDF) says that any Internet service that "enables users to access content" must permanently retain records that would permit police to identify each user. The records could not be discarded until at least one year after the user's account was closed.

It's not clear whether that requirement would be limited only to e-mail providers and Internet providers such as DSL (digital subscriber line) or cable modem services. An expansive reading of DeGette's measure would require every Web site to retain those records. (Details would be left to the Federal Communications Commission.)

Rep. Diana DeGette ;
"We're still addressing some of the issues, and we will have those issues or answers before we introduce this as either an amendment or a standalone bill," Brandon MacGillis, a spokesman for DeGette, said in an interview on Friday.

CNET News.com was the first to report last June that the Justice Department was quietly shopping around the idea of legally required data retention. In a move that may have led to broader interest inside the United States, the European Parliament last December approved such a requirement for Internet, telephone and voice over Internet Protocol (VoIP) providers.

U.S. politicians began talking publicly about mandatory data retention during a series of House of Representatives hearings on child pornography and in speeches, News.com reported earlier this month. Legislation similar to DeGette's has been circulating in the Colorado legislature, and another hearing on child exploitation is planned for next Wednesday.

The Bush administration's current position is an abrupt reversal of its previous long-held belief that data retention is unnecessary and imposes an unacceptable burden on Internet providers. In 2001, the Bush administration expressed (click for PDF) "serious reservations about broad mandatory data retention regimes."

DeGette said in a statement that her amendment was necessary because: "America is the No. 1 global consumer of child pornography, the No. 2 producer. This is a plague we had nearly wiped out in the seventies, and sadly the Internet, an entity that we practically worship for all the great things it has brought to us, is being used to commit a crime against humanity."

For their part, Internet providers say they have a long history of helping law enforcement in child porn cases and point out that two federal laws already require them to cooperate. It's also unclear that investigations are really being hindered, according to Kate Dean, director of the U.S. Internet Service Provider Association.

MacGillis, a spokesman for DeGette, said his boss is likely to introduce her data retention proposal as a standalone measure or as an amendment to a broad telecommunications bill that's moving rapidly through the House.

The bill best known for a debate this week over its Net neutrality sections--was approved by a House committee on Thursday and is expected to receive a floor vote next week. (DeGette had considered adding it as an amendment during the committee vote but decided against it at the last minute.)

"Our main concern on the bill is privacy, protecting the privacy of everyone out there on the Internet, but also retention of those records so law enforcement officials will have access to them, so we just need to really tinker with the language," MacGillis said.

Child porn as surveillance excuse?

Critics of DeGette's proposal have said that, while the justification for Internet surveillance might be protecting children, the data would be accessible to any local or state law enforcement official investigating anything from drug possession to tax evasion. In addition, the one-year retention is a minimum; the FCC would receive the authority to require Internet companies to keep records "for not less than one year after a subscriber ceases to subscribe to such services."

Jim Harper, director of information policy studies at the free-market Cato Institute, said: "This is an unrestricted grant of authority to the FCC to require surveillance."

The FCC would be able to tell Internet service providers to monitor our e-mails, monitor our Web surfing, monitor what we post on blogs or chat rooms, and everything else under the sun," said Harper, a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. "We're seeing a kind of hysteria reminiscent of the McMartin case. The result will be privacy that goes away and doesn't come back when the foolishness is exposed."

The McMartin case was probably the most extreme example of the hysteria over "Satanic ritual abuse"--a widespread scare in the 1980s that children were molested, murdered and tortured, even though no evidence was found. In the McMartin preschool case, a family was falsely accused of Satanic activities and the charges were eventually dropped.

At the moment, Internet service providers typically discard any log file that's no longer required for business reasons such as network monitoring, fraud prevention or billing disputes. Companies do, however, alter that general rule when contacted by police performing an investigation--a practice called data preservation.

A 1996 federal law called the Electronic Communication Transactional Records Act regulates data preservation. It requires Internet providers to retain any "record" in their possession for 90 days "upon the request of a governmental entity."

In addition, Internet providers are required by another federal law to report child pornography sightings to the National Center for Missing and Exploited Children, which is in turn is charged with forwarding that report to the appropriate police agency.

*******END APPENDIX B*******

APPENDIX C

Thank you Google!

JOHN INNES

GOOGLE, the Internet giant, is planning a massive online facility that could store copies of users' hard drives - a move set to spark alarm among civil liberties campaigners.

Plans for the "GDrive", previously the subject of rumor among computer experts, were revealed accidentally after notes in a slide show were wrongly published on Google's site.

The device would create a mirror image of data stored on consumers' computer hard drives, letting users search data stored on other computers via Google accounts.

While offering more convenient access to data, the service will stoke debate about the dangers of storing so much personal data on Google systems. Google recently squared up against the United States Justice Department, which has subpoenaed a limited set of data on Google search habits, drawing an outcry from privacy advocates.

In the presentation notes, the chief executive, Eric Schmidt, made a cryptic comment that one goal of Google was to "store 100 per cent" of consumer information".

A Google spokeswoman declined to comment on any specific service, but confirmed that the presentation containing the notes had been mistakenly released on the Internet. "We deleted the slide notes because they were not intended for publication," she said.

"We are constantly working on ways to enhance our products and services for users, but have nothing to announce at this time."

The new service could save computer users from loss of data by keeping a "golden copy" on Google's centralized computers. However, the plan could be thwarted by privacy concerns.

Recently, the Electronic Frontier Foundation, a digital rights advocate, issued a similarly stern warning to consumers to not use such facilities because it would reduce their level of privacy protection.

Google has been at the center of privacy row in the United States. Last August, Google rejected US government efforts to access its search logs to prop up a contested 1998 law designed to protect minors from objectionable material on the Internet.

Microsoft, Yahoo, and America Online have all since admitted that they have provided the government with some of that data from their logs.

The revelations triggered a privacy rights row in Washington that has placed the administration of the president, George Bush, on the defensive and has sparked at least two investigations in Congress.

*******END OF APPENDIX C*******

APPENDIX D

From a SysAdmin at the privacy forum www.privacy.li
A must read.

Introduction

Context, context, context. I was sick hearing that phrase from Egyptologists in regards to my research on the Great Pyramid. They never could grasp that context is irrelevant to the scientific process or methodology, science examines facts, not interpretation. In saying that, they taught me a lot, it is funny how the entire aspect of a thing or situation can change, just by applying a different context to it.

In this article, I intend to do just that, with Microsoft's Windows Operating System.

If you have ever wondered, if;

1. Microsoft, was secretly spying on end-user machines?
2. Big Brother deployment scenarios were real?
3. M$ Windows was a type of bugging device?

Then this, is for you my friend, the 'Top-47 Windows bugging functions', and then some. There is also an appendix on forensic methodology and Magnetic Force Microscopy (MFM).

All sing...'There may be trouble ahead...' □

If You Could See, What I Can See, Reinstalling Windows...

In general, to people in the western hemisphere; bugging devices, parabolic microphones, signal tracing, satellite tracking and secret government agencies, performing highly illegal activities, on a covert basis, are the source of inspiration for novels, movies and theater, rather than any real event.

These devices and activities have been part-and-parcel of my life (and almost anyone else in Northern Ireland), from the moment of birth and conspiracy theories are simply facts of daily life that, could put, any of my friends, or myself, into an early grave. Therefore, it is only natural for me to see things in a military context and this provides a very interesting picture of odd behavior, at Redmond and various other big names, throughout the US.

Microsoft is of the 'opinion' that its software is an operating system with a wide range of 'features'. As I am about to demonstrate, that is simply a matter of 'how you see things' and the context in which they are highlighted in. This is a very subjective experience and different people tend to see different things, simply because their own personal context is automatically applied, a 'bias', if you will.

The point to hold, in the front of your mind, throughout reading this article, is the fact that the 'features' and their descriptions, presented here, are accurate representations of Window functions, in their own right, however, any suggestion as to motivation would be speculation.

More clearly, Microsoft has presented it own 'opinion' on the various features within Windows, other 'opinions' do exist and this article presents one of them, in a hypothetical scenario. For this analysis to hold, the hypothetical scenario must be demonstrated to be consistent throughout the design of the OS, not just its usage.

The style and tone throughout, is based upon the working hypothesis, that Microsoft has altered the Windows OS, to reflect US military requirements and that its primary role is that of a modern variation of a 'bugging device'. It is simply taken as a given fact throughout.

This clarification allows for a more direct style of writing and legal protection for publishers. In addition to this, the views expressed in this report are the authors and have nothing whatsoever to do with anyone else.

There are no accusations being made, this is presented only as a 'working hypothesis', at all times, to allow for the fullest exploration of this particular train of thought. If the hypothesis holds, then we will expand it a little, to place it in proper context and draw the conclusion from the entire investigation.

Report On Analysis of Microsoft Windows XP

1. Start -> Search □

Each and every time a search is conducted using the search option under the start button on Windows XP, the system automatically checks if your online and transmits information directly to Microsoft.

This is done, without informing the end-user in any fashion, nor providing a clear method to disable. It has been hidden by design. In technical terms, a form of Trojan.

A good application level, stateful firewall, will catch this communication attempt.

Done by design.

2. Help System, F1

When accessing Microsoft Help systems, through the F1 key. A communication attempt to Microsoft's ActiveX site is made.

Done by design.

3. Microsoft Backup

Designed to bypass all security, even ownership rights of a drive. Try it.

Done by design.

4. Process Viewer (Task Manager)

No mapping to executable file, nor will it show all running processes. Designed to hide important information required for determining system infections and sources of network data transmission.

Done by design.

5. Dr Watson

This used to load up with information on dlls that had been hooked. Hooked DLLs are used to intercept keystroke, etc. Microsoft removed end-users capability to see this. It now generates a simple message box.

Done by design.

6. The Windows Registry

Now, on the face of it, this may seem like a good idea, however, as any developer will tell you, they only use it because the commands are quick, simple and, when it comes down to it, security is mainly the end-users responsibility.

It would be much faster, simpler and provide greater system security to use an ini file. Linux uses this approach with config files. An entire database must be examined each time request is made. This is why Windows slows down after you begin installing applications. The registry grows and more cycles must be dedicated to completing each query.

When you multiply this, by the wide range of systems accessing the registry, it is clear to see, that as a design architecture, it is completely moronic.

That is, until it is examined from another perspective, try the following perspectives as examples:

a. HKEY_CURRENT_USER - psychological profile of logged on user, real-time usage focus.

b. HKEY_LOCAL_MACHINE - Detailed reporting of hardware and a wide range of traceable unique identifiers

c. HKEY_USERS - psychological profiling of all users, post-forensic usage focus.

d. HKEY_CURRENT_CONFIG - Advanced psychological profiling based on a ranking system of 'psychologically-based options' embedded throughout the system. This could include things like favorite color, pictures, sounds, etc.

Throughout the registry are an extensive amount of MRUs. These areas store your recently accessed documents each application and other information. Now instead of having a single area were these are stored, for both rapid access and cleaning purposes, Windows was designed to fragment these throughout the registry database.

Firstly, this makes cleaning the registry a specialized job, as a mistake can corrupt Windows. Secondly, and most importantly, this is what we call 'fragmentation'.

Now 'fragmentation' is a well known source of problems when accessing information. Many will point out, that the registry is a hierarchy and that that this eliminates fragmentation. I must point out that I am referring to the 'entire structure of recorded information' and not the technical definition of fragments of data.

By fragmenting the various forms of 'recorded information' throughout the registry, it can take upwards of a week to list every key that should be cleaned. The entire process must be repeated each time a new application is installed, to determine what exactly was placed into the registry. Windows also uses an extensive amount of MRUs that have been altered to an 'unreadable' format. This would leave 95% of users completely unaware of Microsoft was recording.

There is no need or requirement for a registry, other than to provide central access to 'private information'. As a programming architecture model, the design borders on the moronic and is directly opposing every known, best practice, in programming.

The true motivations behind the registry design are quite clear and highly specific.

Done by design.

7. Temporary Files

Temporary files are retained under 'Document and Settings' for a prolonged period of time and in most case require manual clearance.

Done by design.

8. Recycle Bin

Even when told to not use deleted item to the recycle bin, it is used anyway, only with out the prompt. This generates a ghost copy on your hard disk of any deleted files.

Two copies are better than one for recovery purposes, especially were Magnetic Force Microscopy is concerned. The two copies can be referenced with each other for rapid recovery procedures, its an attempt to eliminate bit errors in overwritten files.

The more ghosts images, the better the chances are for fast and complete recovery of during post-forensic examination.

Done by design.

9. Recent Files

Only a small portion/subset of the recent files accessed is displayed in 'Documents' section under the start button. The folder that contains the shortcuts has a far longer list hidden from general view.

For example, 11 files are listed under the Start buttons 'My Documents', however, 'My Recent Files' contains 17 entries. The other 6 came from my last list of files which I deleted using the 'Clear' button.

Done by design.

10. NotePad

Windows XP versions cannot word wrap properly and have been redesigned to make their usage as frustrating as possible. For example, when saving text only file, the screen resets the position of the text to the line where the cursor is at.

This takes specific coding and not something that happens by accident. The idea is to push people towards Microsoft Office, where all security can be breached and copies written, at will, across your drive.

Done by design.

11. Swap Space/Virtual Memory/Page File

    Regardless of how much memory is in your system the page file can not be disabled. Its main function is too swap memory to disk and allow memory to be freed for running applications. With a large amount of RAM, this function becomes redundant, except under exceptional circumstances.

    What is the useful purpose of a 2MB page file? Other than writing data, across the drive, in 2MB chunks, none.

Its designed to flush encryption keys and sensitive information to disk. This also generates ghost images which can be retrieved.

Done by design.

12. Firewall

Incoming firewall only. This allows spyware to transmit information without any problems or detection. 90% of spyware information is transmitted to and shared throughout the US.

Done by design.

13. Memory Usage

Designed to use large amounts of memory to drive the hardware industry sales of components. For Windows XP to function correctly, it requires at least 1GB RAM and at two physical drives on separate IDE channels or SCSI interface I/O.

Even then, it hogs everything and leaves random fragments in memory. These fragments or 'memory leaks' are then flushed to disk, in an effort to capture some information from running applications, encrypted viewers, etc.

The ever expanding registry is designed to keep up, with ever expanding hardware and slow the system. End users think programs have gotten more powerful and they must upgrade. Its simply that more and more cycles are dedicated to various expanding databases, each and every boot.

Done by design.

14. Automatic Updates

Can allow remote installation of any form of software at Microsoft's whim.

Done by design.

15. Raw Sockets

Microsoft prevents new protocols being developed on Windows to prevent usage of nonstandard protocols. This allows for easy access to information. It also prevents the disabling of Microsoft's TCP/IP stack, which for all we know, could have 30,000 extra 'ports' coded into it.

Windows 2000 was actually programmed to reject any driver, that would allow custom protocols to be developed, without Microsoft certification. Microsoft claimed this was a 'mistake'.

Now lets all try to picture the conversation at Microsoft on this one, shall we?

{In an office at Redmond...}

Executive 1: '...my hand slipped and wrote 10 pages of code..., no wait...,
Executive 2: the dog coded it, ah nuts..., erm...,
Executive 1: Can we blame Bin Laden?'

Raw socket access also bypasses every known firewall, from Sygate to Zone Alarm. The reason being that these applications, rely on the Windows message/event handling and Microsoft designed Raw Sockets not to report to this layer.

Komodia produce a TCP/IP Packet Crafter, install that and Sygate's Personal Firewall on WinXP service pack one. Craft a few packets to see this in action. Nice Trojan tool M$.

Reverse psychology was employed, although not a very good example of it, in Microsoft's deployment decision to support raw sockets. It was to get people to focus on a 'hoax' alert, rather than the high level of security such a system would provide.

The truth is, raw sockets is not required, however, it just makes life simpler. For real time software, the overhead presented by TCP, is too great and the effects can be seen on excessive lag during online gaming, or media playback. A streamlined custom stack, allows for faster processing of the IP packet and over a 1000% improvement to connectivity management than TCP encapsulation.

Many developers do not realize that TCP is not required and that custom packets can be encapsulated within IP alone. IP routes the packet, from A to B, and TCP provides a data path encapsulated with the IP packet. This allows Internet routing to change, without effecting application support. Custom stack creation is a 'walk in the park', all it involves is parsing a binary stream and executing functions based on flags or value, it also, automatically, supports the OSI/DoD model.

By breaking support for raw sockets on Windows 2000, Microsoft manipulated the entire global market, as no developer could be assured their applications would function after 12-24 months. It also provided a way for Microsoft to eliminate tools such as 'Ethereal' that could inspect the communications of a Windows system.

An active attempt at blocking end-users knowing what information a Windows system was transmitting, as Microsoft is aware, that over 80% of end users only have a single PC.

Done by design.

16. Remote Access Bugs

This is a good example of 'context and highlighting' (perspective). I want you to consider this statement:

Is a remote access bug, not the same thing as a back door access code?

Write a detailed essay on your conclusion, no less than 30,000 words. You should consider statements such as 'buffer overflow executes code', 'invalid datagram shuts down PC', etc. □

Open BSD has no such remote exploits and no money.

Done by design.

17. Music Tasks

A nice big link to 'Shop for Music Online'. This is a direction to US based enterprises and also a violation of the Microsoft EULA, as it mentions nothing whatsoever in regards to Microsoft Windows being an advertising supported platform.

No matter how small the feature, that is still what it represents. If Microsoft is in breach of its EULA, does that invalidate it?

Done by design.

18. Windows Media Player

No way to disable automatic check for updates. This allows any form code Microsoft chooses to be used as an upgrade. Defaults to uniquely identifying an end user and stored media.

Certain websites warn their visitors that using Windows Media Player version 7 on their websites will reveal your 'personal information' to Microsoft. An example can be located here:

http://ekel.com/audio

Have you ever wondered how p2p information on end users is gathered? Think about it the next time you connect to a commercial Internet radio, video or media service.

Done by design.

19. Alternate Data Streams

This 'feature' of Microsoft Windows relates to how information is stored on your hard drive. Under NTFS, not only is there the file, but there is a second, hidden aspect to each file. This hidden aspect is stored separately on your hard drive and not as part of the file.

I suppose the term, 'Alternate Data Streams' make better business sense, than 'hidden information gathering process combined with standard file functions'. □

All additional information to a file, such as date/time stamps, file name, size, etc. is stored in this layer. Not only this, but so is the thumbnail cache of all images viewed by the system. This 'feature' is hidden by design and requires either a 1 month long 'disk nuke' (for average 80GB HD) or physical destruction of the disk platters to remove.

Physical destruction is recommended, as it requires specific manufacturers codes to access bad blocks, internal scratch areas and internal swap/cache areas of the drive. Even with the codes, certain problems can arise from unreadable sectors which may contain copies of sensitive information.

Nothing beats an nice afternoon with a screwdriver and grinder. □

The caching can be disabled, however, Microsoft has made this as 'obscure' as possible. Microsoft Windows also does not explain the function of 'Do not cache Thumbnails'.

It is aware 90% of end-users have the technical aptitude of 'a banana with a with a drink problem' and would never grasp the implications, let alone, understand.

Done by design.

20. Stability

Microsoft Windows is designed to collapse upon extensive number crunching, of large arrays, of floating point calculations. This would prevent; nuclear modeling, physics modeling, and genetic modeling. These three aspects can produce Nuclear, alternative and biological weapons.

I don't know about you, but this 'feature', I can live with, or couldn't live without, for very long. □

Done by design.

21. Internet Explorer 'Features'

MSN Search

When Internet Explorer fails to locate a web address it initiates a search through Microsoft. Therefore, every failed access attempt is sent to Microsoft, with all your system information in the X header structure. to Microsoft, cleverly disguised as 'assistance'.

Done by design.

22. Temporary Internet Files

Without extensive reconfiguration of Windows end users will not see the real files. Instead they see a database generated representation drawn from a file called index.dat.

Even the controls to access the drive are hidden with an obscure setting called 'Simple File Sharing (Recommended)'. Windows XP does not always delete the actual files from your hard disk. Even the emulated DOS reports the database, unless windows is substantially reconfigured.

Windows goes to great lengths to prevent this reconfiguration. Also, many do not know there is no need for this cache, other than to go back to pages. Its main role is to maintain a record of users activities and generate ghost images throughout the drive.

Done by design.

23. Index.dat

A database file of the contents of an area of the drive, including deleted files. In the 'Temporary Internet Files' it records date, time, Internet location and file name information of downloaded graphics/images and sites accessed, with user IDs in a nice big list.

There are various 'index.dat' files throughout Windows, a dat file is generally a database. A users activities can be recorded for several weeks and user names (etc) recovered. The index.dat file retains information about recently deleted files and Microsoft has failed to provide any reasonable explanation.

You cannot provide, what does not exist, there is no genuine reason to retain deleted files information other than deliberately recording an end users activities for forensic analysis.

This is used for rapid identification, file recovery and time-plotting of a users activities. A small application produces a timetable of a user's usage, referenced against the recorded information for each second of activity.

On large networks, this can be used to verify each member of staff location and movement across an entire infrastructure, this type of output in normally rendered in a full 3D layout of the target building.

Done by design.

24. Cookies

The official explanation for cookies is to offload information from the server, to the client. This can be authentication, preferences, etc. As you can see, its just a cheap solution, designed to cut costs.

When costs are cut, so are corners and in this case a corner that presents a major threat to information security. Cookies retain a lot of information such as logon IDs. In fact, the first cookie I look for, is generally, passport.com. This cookie will have the last recorded Hotmail address stored within it. Combined with index.dat information, I can tell the following;

1. Windows logon ID of the person involved
2. The Hotmail email address
3. The Date and time the account was accessed
4. External graphics viewed and the sources of those graphics
5. The machine from which it was accessed.
6. The duration of viewing.
7. And generally, the individuals sexual, political, social, personal and religious preferences based upon the information accessed.

That's with only two file sections.

Cookies can also be accessed remotely and are used to track the movements of end users as they move from site to site. Passport, Microsoft's common logon system, relates itself against the Windows account by default.

There is no need for this, it is these 'subtle functional intrusions' that Microsoft prefers. I honestly do not know what is going on in these people's heads, to think for one second, that the world would spot this a million miles off. It really does show the level of intelligence these people have; my dog demonstrates more social engineering skills when looking for food.

Done by design (very poorly executed).

25. Auto-Complete

Designed to record search terms, web addresses, and anything else it can get its grubby little digital hands on, for rapid post-forensic retrieval.

Done by design.

26. MSN Messenger

Microsoft has been retaining each persons deleted contacts from messenger. M$ has been monitored in this area and is known to retain everyone's deleted contacts for 3 years, at least.

This could be seen using a console-based version of MSN Messenger under Linux. Microsoft has since changed the protocols, so I am unaware if you can still see some of the information, M$ retains, on over 150 million people.

Messenger is also activated on accessing Hotmail. Microsoft claims to be using the 'features' provided by Messenger and will not allow it to be disabled. Now, as millions access M$ Hotmail without messenger, I must seriously question this behavior.

The 'features' provided by MSN Messenger are the transmission and reception of typed text and files. So, Microsoft has stated that it is, 'transmitting typed text and files', to and from, end users machines, when Hotmail is being accessed.

Just cleverly worded.

Done by design.

27. Web-Cams and Microphones

These devices can be remotely activated providing visual and audio feedback from the target subject. There is also no way of telling if your devices have been remotely activated. These features are demonstrated in 'proof of concept' applications such as NetBus, etc.

With raw sockets (or driver) this information can bypass your firewall without any problems.

Microsoft Windows XP Services

1. Application Layer Gateway Service

Microsoft's Description:
Provides support for 3rd party protocol plug-ins for Internet Connection Sharing

and the Internet Connection Firewall,,Manual,Local Service

Alternative Description:
This thing just loves making remote connections and accepting them. Set this up in your firewall to ask each time using ADSL or higher.

Have fun. □

Done by design.

2. Automatic Updates

Microsoft's Description:
Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site.,,Disabled,Local System

12. Alternative Description:
Enabled by default. Enables Microsoft to distribute and incorporate any 'feature', at will. Not the greatest thing in the Universe to be allowing.

Done by design.

3. Computer Browser

Microsoft's Description:
Maintains an updated list of computers on the network and supplies this list to computers designated as browsers. If this service is stopped, this list will not be updated or maintained. If this service is disabled, any services that explicitly depend on it will fail to start.,Started,Automatic,Local System

13. Alternative Description:
This stupid design will breach security. The only computer a client needs to know, is the server and it should coordinate everything.

Why does Microsoft Windows identify and map every computer on the network?

The design principal is based upon 'remote orientation' requirements, using insecure clients as targets. Servers would be difficult to compromise and arouse to much suspicion.

The flow of information on any network is about 'the need to know'. Clients do not need to know any other computer, other than the server. The server acts as a 'proxy' to the entire network, data transfers may, optionally, be proxied too.

Done by design.

4. Fast User Switching Compatibility

Microsoft's Description:
Provides management for applications that require assistance in a multiple user environment.,,Disabled,Local System

Alternative Description:
Switches to every account, but the Administrator account. In fact, unless you know exactly what your doing, an end user cannot access the administrator account.

Post-Forensics can, that includes your Windows Encrypting Filesystem. Cheers M$.

Done by design.

5. IMAPI CD-Burning COM Service

Microsoft's Description:
Manages CD recording using Image Mastering Applications Programming Interface (IMAPI). If this service is stopped, this computer will be unable to record CDs. If this service is disabled, any services that explicitly depend on it will fail to start.,,Manual,Local System

Alternative Description:
Part of CD Burning and this thing is a nightmare. Any CD you make, it first makes a copy to the system drive, then only to use a scratch drive after that. Why?

That action is a waste of time. This is designed to generate 'ghost images' that can be recovered by Magnetic Force Microscopy. It is unlikely that the target subject will destroy their boot drive. Also, pointing the scratch to another drive, just makes more ghost copies.

Not only that, but I have caught Windows XP, pointing me to the CD burning directory when viewing CDs. That would suggest a cached image of some form.

Done by design.

6. Indexing Service

Microsoft's Description:
Indexes contents and properties of files on local and remote computers; provides

rapid access to files through flexible querying language. ,,Manual,Local System

Alternative Description:
A search using the DOS emulator will run like a bullet. Windows search, however, will take its time unless the indexing service is activated. This provides quick post-forensic and real-time access to files remote files.

This behavior is by design. □

7. Internet Connection Firewall(ICF)/Internet Connection Sharing(ICS)

Microsoft's Description:
Provides network address translation, addressing, name resolution and/or intrusion prevention services for a home or small office network.,,Manual,Local System

Alternative Description:
First off information is sent to both Microsoft and to a range identified as belonging to ARIN whenever a PC connects to the Internet. Random connection attempts are made by Explorer, NT Kernel, Internet Explorer, Windows Help, svchost.exe, csrss.exe and numerous others. I have even caught calc.exe (The calculator) attempting to initiate a remote connection, now and again. Without reverse engineering, I was unable to tell if it really was the applications, or a subsystem calling the applications. Very odd.

Microsoft Windows defaults to sharing your files using SAMBA across the Internet. This even bypasses most domestic firewalls or security setups, unless specific options are set in the firewall. This allows for remote access to files, documents, etc. without breaching any known legal regulations.

Try entering random IP addresses into your 'My Network Places' window when online, preceded by the '\\' network identifier.

i.e. '\\91.111.2.80', or '\\222.54.88.100'

Within about 30 attempts (of a good netblock), you should get a remote machine to share files with you, in the same manner as a LAN setup. Expect your machine to freeze when performing any remote operations for up to 4 minutes at a time (i.e. such as right-clicking a file).

The reason for behavior is that native SAMBA is designed for 10Mbit networks (at least) and is therefore a very bulky protocol. Also, the remote host may be using their Internet connection, have a low bandwidth connection or performing processor intensive tasks.

A quick examination of Sygate's instruction on how to use their firewall with ICS, reveal that your kernel cannot be blocked, nor can several other systems. These systems are not required on a LAN, so Microsoft has designed these systems to breach security.

There is no difference between TCP/IP over a LAN and the Internet, other than settings. As a programmer I know Network Address Translation is simply a case of storage and substitution of IP addresses, with a few whistles and bells. There is no excuse for these systems to be exposed to the network.

Done by design.

8. Messenger

Microsoft's Description:
Transmits net send and Alerter service messages between clients and servers. This service is not related to Windows Messenger. If this service is stopped, Alerter messages will not be transmitted. If this service is disabled, any services that explicitly depend on it will fail to start.,,Disabled,Local System

Alternative Description:
Messages should only be broadcast, by and to, the main server. Having this on every machine provides a method of transmitting real-time keystroke intercept across the Internet. This service is also enabled by default, even with the known Internet abuse of the function. This only indicates design manipulation.

Done by design.

9. Network Connections

Microsoft's Description:
Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.,Started,Manual,Local System

Alternative Description:
Only weakens security by providing a central reporting mechanisms. These aspects have been combined by design, with no logical requirement for the function. Again, a single-point of failure is introduced into the system.

Done by design.

10. Protected Storage

Microsoft's Description:
Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.,Started,Automatic,Local

System

Alternative Description:
Also provides quick access to this information. Swift breaking of security. Sweet.
□

Done by design.

11. Remote Procedure Call (RPC)

Microsoft's Description:
Provides the endpoint mapper and other miscellaneous RPC services.,Started,Automatic,Local System

Alternative Description:
May the saints preserve us from RPC. RPC provides remote computers with the ability to operate your PC and listens for these connections on the network/Internet.

What sort of idiotic decision making was behind an RPC service that cannot be disabled? Why not just come into my living room M$? You're practically there anyway!

(I'm just losing my head now! This is disgraceful.)

Done by design.

12. Remote Registry

Microsoft's Description:
Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.,,Disabled,Local Service

Alternative Description:
This nifty service is enabled by default. It provides remote access to the windows registry, allowing run-time modifications to be made to your PC. Hmmm....what an excellent idea! Just what I always needed, a way to 'tweak' my running spy applications remotely.

I knew M$ was thinking about me, I'm touched, or at least they're close enough to reach out and touch me. □

Done by design.

13. Server

Microsoft's Description:
Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.,Started,Automatic,Local System

Alternative Description:
This is not required, it provides a central management for open files and printing operations. It also provides a method of remotely monitoring a users activities.

This 'service' (ha!) provides a single-point of failure for an entire network. It is linked to the authentication, so if the server collapses, so does the entire network, as this is managed by the server. Again, security and functionality have been manipulated to focus on information retrieval and access.

Done by design.

14. SSDP Discovery Service

Microsoft's Description:
Enables discovery of UPnP devices on your home network.,,Disabled,Local Service

Alternative Description:
What in Gods name for? This is part of the 'remote orientation' facilities encoded into Windows, allowing remote hackers the ability to explore the network swiftly, reducing chances of alarm and excessive activity through exploration.

Done by design.

15. System Event Notification

Microsoft's Description:
Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.,Started,Automatic,Local System

Alternative Description:
No way of knowing, without full reverse engineering, how many undocumented events exist throughout Windows. Windows could have an entire additional level of event reporting.

Event and thread management in Windows is very suspicious due to its sluggish and sometimes unpredictable behavior. Compensation for this is normally done by 'peeking' into the message cue, however, sometimes it simply refuses to work. This would tend to suggest the interaction of an unknown component (or several component) with the event system producing conflicts.

Done by design.

16. System Restore Service

Microsoft's Description:
Performs system restore functions. To stop service, turn off System Restore from the System Restore tab in My Computer->Properties,,Automatic,Local System

Alternative Description:
Keeps ghost copies of various forms of cached information in a nice quick accessible format. We can't let our hard earned information go down the pan now.
□

Done by design.

17. Terminal Services

Microsoft's Description:
Allows multiple users to be connected interactively to a machine as well as the display of desktops and applications to remote computers. The underpinning of Remote Desktop (including RD for Administrators), Fast User Switching, Remote Assistance, and Terminal Server.,, Disabled,Local System

Alternative Description:
I just bet its interactive and highly 'functional' too. This is enabled by default, providing a remote desktop for any hacker. Wow, what a service M$.

I'll agree with you on this one, that is a 'service and a half'!

Done by design.

18. Windows Time

Microsoft's Description:
Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start. ,,Disabled,Local System

Alternative Description:
Sends information to Microsoft and keeps your date and time stamps nice and fresh for post-forensic analysis. At least they're tidy when they invade your privacy. □

Done by design.

19. Wireless Zero Configuration

Microsoft's Description:
Provides automatic configuration for the 802.11 adapters,,Disabled,Local System

Alternative Description:
Zero configuration means zero security and that's exactly what you get. The entire network is exposed to anyone within reception range. Therefore, if you are using this in your home environment, that can mean remote monitoring from up to 3Km using proper equipment, or someone else using your Internet connection from a range of around 50-80m radius.

Even with security, the IEEE specification for WEP was clearly manipulated and weakened by interested parties. There is no other acceptable excuse for that level of incompetence.

Done by design.

20. Microsoft Works

Breach of trade descriptions act? Microsoft 'probably' Works. □

Really, it is an 'implied' suggestion based on the play of words. It can be described as 'psychologically misleading', human psychology is extremely complex, even if most humans are not.

This implied statement is registered at a deeper level of the brain and assigned its true meaning. Otherwise, you would have never considered the relationship in the first place.

One way of describing this is, 'marketing', the accurate description is 'subliminal programming', it does not matter how slight the incident.

This is very, similar in style, to the 'French Fries' and 'Freedom Fries' incident in the US, used to blind the US citizens from war opposition, through manipulation of patriotic beliefs.

Shameful.

Done by design.

Windows Security, Not What You Think

Since all security products that operate on the Microsoft Platform are both designed from, and encapsulated by the OS, then it is ultimately Microsoft Windows that is providing your security and not your firewall, etc.

So, any product that claims to provide security FOR windows, is simply reflecting the limited understanding the company has of what it is doing.

I bet that will inspire confidence in computer security. □

The accurate description is that M$ Windows, secures itself, through execution of a 3rd party application, which M$ Windows must inform, to provide security. As we seen in 'Raw Sockets', this does not always happen. Linux does not have this problem, as the systems is a mosaic rather than a full encapsulation, or sandbox environment.

Therefore, even with all the security, in the known Universe, installed on a Microsoft Windows Platform, it is still the responsibility of Windows to inform the security products of each event happening. If Microsoft Windows fails to report, or hides certain messages/events, then your security software becomes 100% completely redundant.

This is a source of great concern with Microsoft's plans to encrypt the system area of new versions of Microsoft Windows. Somehow, I don't think this system, nor any variation of it, will ever see the light of day.

If this was to happen (the encrypted system), instead of an EULA, I think Microsoft Windows should be required to read end-users their rights. Microsoft is not the Law, nor is it above it, in any way.

You have the right to be bugged, click OK to continue! □

Bugs Of The Third Kind

How long as Microsoft been programming Windows for?

Ten, maybe fifteen years, and we are seriously asked to believe that a company with the financial resources of Microsoft cannot a create a bug-free Operating System?

Companies with lesser resources than Microsoft provide such systems for Air-

Traffic control and medical purposes (Heart Monitors, etc). A perfect example here is OpenBSD. OpenBSD is a free Operating System and with very little funding (nowhere near what Microsoft has, in a million years) the only remote exploits you will find, anywhere in the world, will be at least 12 months old.

Most of Microsoft's problems are at least that old before anyone decides to analyze them, let alone, fix them.

This is a very clear example, honestly, there is no acceptable excuse here. If Microsoft claims 'compatibility', then I simply refer them to the current deployment of service packs that destroy 'compatibility'.

Also, the important thing to business is their data and data cannot have 'compatibility' issues. Its simply a binary stream that can be used on any known operating system.

Wild Speculation On Codenaming Strategy

Microsoft has had a consistent naming policy for its operating systems, in the form of city names. Code names for various releases have included; Chicago, Memphis, etc.

Now all this changed with the arrival of Windows XP. Its codename was 'whistler' and the next version of Windows is codenamed 'LongHorn'. I was interested in the reasoning behind the switch. I was thinking that these codenames could be based on one, or more, of the following points:

1. A play on the term 'whistleblower'?
2. A play on a reference to 'pinocheo'? (tells stories, reference to Long (Nose) and Horn (Whistle Blower))
3. Horn, as in a form of 'early warning system' and Long because of its distributed nature?

Can Windows Be Secured?

Yes, with FDisk. (Recommended) □ Otherwise, due to its encapsulated nature, the answer is a pointblank, no.

Additional Observations

All we need now is Intel's 'processing and storage' layer to the Internet and we have a, full-scale, 100% genuine, deployment of a Big Brother scenario. Thanks Intel, but, we'll pass on that one, nice to see you are thinking of everybody for a change. □

If anyone is wondering what on Earth is going on, well Congress went a little nuts passing resolutions, without its normal due caution. Looking down the barrel of a gun 24/7, does not provide the ideal circumstances for making these decisions, nor the environment for full, open debate, for security reasons. As such, mistakes can only be expected, congress is still only human, despite the rumors.

I am just worried that this is the entire intention, due to Microsoft's modifications, its software predates 9/11, so it could not use 9/11 as an excuse. I wouldn't like to consider the implications of that statement 'being inaccurate'.

I know many readers would be enjoy this analysis taken further, however, it is well beyond the scope of this report. It is also an area I feel is best left to the authorities.

Alterations to M$ Windows also coincides with antitrust cases and the reversal of the ruling to split Microsoft into two companies. This leads to three important questions:

1. Was Microsoft hijacked by the US government, CIA or NSA?
2. Is this why M$ Windows was altered?
3. What would the suggested reason be for military adaptations to M$ Windows prior to 9/11?
4. Why 3 Operating Systems (ME, 2000 and XP) between 1999-2001?

I only mention this to be fair, rather than shoot first, ask questions later. I'm a Zen Buddhist and politics, ain't my bag baby. □

Google's ranking methods have come under question recently and in the context of this report, I think the follow will speak volumes for itself:

Search for the term 'Book'. Conducted September 11th, 2004.

Top 10 results from Google.com

1. US
Barnes & Noble.com, 6000 Freeport Ave - Suite 101, Memphis, TN 38141.
2. US
onlinebooks.library.upenn.edu, University of Pennsylvania
3. US
www.cia.gov, CIA - Factbook.
4. US
BookFinder.com - Berkley California
5. US
www.kbb.com - Orange County
6. US

www.worldbookonline.com - Country Wide, with world-wide divisions
7. US
www.superpages.com - 651 Canyon Drive. Coppell, TX 75019.
8. US
www.amazon.com
9. US
www.abebooks.com - Victoria B.C.with offices in Canada and Germany.
10. US
www.bookwire.com - 630 Central Ave. New Providence. New Jersey.

May I remind everyone that Google is behind nearly every major search engine in the World. Is this what they describe as 'free enterprise' in action?

I wouldn't like to see systematic manipulation of the global economy, if that's the case.

A Small Bit of Advice

Linux...Open Source...Free...No worries.

*******END APPENDIX D*******

APPENDIX E

Java Anyone?

Java is a programming language and allowing java means that your computer may, without your knowledge, download an applet (read: Program) which will run on your computer. If as part of its design, it can read your local IP address and send this to the website that sent the applet(or anywhere the applet is designed to send such info).

Cookies are to be cleared if you use the same browser for privacy AND non private connections. The reason is because if for example you visit site ABC and they deposit a cookie and then you visit the same site using a VPN tunnel, then if the cookie reader is clever enough, they can tie your local IP to your tunneled IP.

*******END APPENDIX E*******

*******END OF FILE*******