Truly Paranoid Shopping

My TPS Report
by
Aaron Grothe
NEbraskaCERT
February 20th 2008

Intro Info

- Brief Bio
- Please ask questions anytime
- Please let me know if I'm mumbling

Intro Quotes

“Just because you're paranoid doesn't mean they aren't after you”- Catch-22 Motion Picture

“The difference between common-sense and paranoia is they common-sense is thinking everyone is out to get you. That's normal – they are. Paranoia is thinking that they're conspiring” - J. Kegler

What This Talk Is

- Some info that might help you increase your security while shopping online
- An example of my personal education/experiences doing online shopping over the last 8+ years
- A funny example of how paranoid/naive I used to be :-)

What This Talk Isn't

- How to hide purchases
- How to be TOTALLY SECURE
- A total solution to online shopping

My Questions for You

- How many of you shop online?
- How many of you take precautions when shopping online?
- How many of you use one time use credit cards?

Truly Paranoid Shopping

My Definition: “Truly Paranoid Shopping is taking steps during shopping that go beyond useful benefit and go off the rails”

“I am recovering from TPS” - Aaron Grothe

A Example of TPS

- Hakin9 Magazine – Great Security Magazine
- You can get it at Barnes & Noble

- You can also get a subscription
- It is published in Poland
- To get a subscription requires you to send your Credit Card number to a foreign country
- Hakin9 is totally legit and a great magazine

Another Example of TPS

- You are buying a CD of hacking toolkits online from a website
- Do you really trust the guy on the other end?
- How do you know he won't be a victim???

The Major Goals to TPS

1) Secure Environment
2) Secure Browser
3) Secure Transactions
4) Protecting your Financial Information afterwards

Five Major Phases to my TPS

1. Way paranoid phase
2. LiveCD Phase
3. USB Phase
4. USB Phase 2/Virtual Machine Phase
5. Virtual Machine Phase (my current one)

Way Paranoid Phase

- Machine with 2 Removable Hard Drive Bays
- Two identical 20gb Hard drives
- Windows 98 Operating System
- Netscape Navigator 4.7
- Norton Anti-Virus on the Box
- This machine's sole purpose was TPS
- Bank account with a check card with minimal money in it

How Well Did Phase 1 Go?

Main Problems were as follows

- Time overhead – constantly making copies of hard drive
- Every purchase required putting money into the bank
- If someone got my number they could continue to try withdrawals until I put more money in the account

LiveCD Phase

- LiveCD (DemoLinux) is used to boot
- Browser is Netscape 4.7 (again)
- No hard drives in the system
- Only purpose for system was this
- Same Bank Card System as Phase 1

How Well did Phase 2 Go?

- At this time 2001-2002 more sites worked with Netscape under Linux
- Time commitment to rebuild machine all the time was reduced
- Was portable if needed
- Updates to LiveCDs can be a bit tardy :-(

USB Phase

- First USB bootable distros started coming out
- Security updates to the Underlying O/S are possible
- Can customize browser as well
- Again this is portable
- Can maintain information on Drive as well
- Still using same bank system

How well did USB phase Go?

- At this time USB drives were still very slow
- While you could patch the O/S you would break it a lot
- If I lost the thumb drive it might have information on it I didn't want to get out
- Didn't really take care of bigger problem/inconvenience of using bank card

USB Phase 2/Virtual Machine

- Flipped to using a Truecrypt encrypted USB thumb drive
- Used QEMU as a virtual machine
- Flipped to using DSL (Darn Small Linux) as operating system
- Got rid of dedicated machines
- Flipped to using One time Use Credit Cards

How did USB 2/VM Go?

- Qemu can be slow, getting better all the time
- DSL doesn't get security updates as often as regular Operating System
- Turned out to be hard to customize Firefox
- True innovation came in the use of One Time Credit Cards

Virtual Machine Phase

- VMware Player used for Virtual Machine
- Image is stored on my server so it is easy to pull a new one
- Latest Firefox with a couple of extensions
- Debian 4.0etch on Encrypted Local Partition
- Continuing to use One Time Use Credit Cards

How is VM phase going?

- Requires installation of VMware player on host machine
- Can patch Guest Operating system
- Seems to be a good balance between ease of use and paranoia
- Requires a pretty secure base operating system as well

Secure Environment

- Currently running Debian 4.0/etch in the virtual machine
- Debian has the ability to do encrypted volumes easily during install
- Security updates happen pretty quickly – E.g. vmsplice was patched on same day as release

Secure Browser

- Currently running Iceweasel (Debian's rebranding of Mozilla Firefox)
- Have installed a couple of extensions as well
- Noscript – Gives you the ability to whitelist javascript and turn it on/off dynamically – popups as well
- ShowIP – gives you lookup options, whois DNS info
- Used to run Spoofstick – hasn't been updated in a while

Secure Transaction/Afterwards

- Using SSL and a patched browser will go a long ways to getting you a secured transaction
- How do you secure your information afterwards? The answer is simply to use One Time Use Credit Cards

One Time Use Credit Card???

- Unique Credit Card Number optionally per transaction
- Limits can be placed on virtual account
- Used instead of real Credit Card Number
- Centralized Billing/Fraud detection etc...

Who Offers This

- Discover offers this through Safeshop and Deskshop
- MBNA/Bank of America and Citibank both have programs that offer this
- Your Credit Card issuing group may also have something like this. It is usually called either a one time use credit card or a SOAN credit card

How can I be a bit More Paranoid?

- Try out VMware Player
- VMware player offers a Secure Appliance (hasn't been updated in a while though)
- Secure your home desktop machine
- See if your Credit Card Company offers One Time Use Credit Cards

Taking it to 11

- Have a separate VMware instance for each task. E.g. Amazon shopping versus Ebay shopping
- In a VMware instance use wine to run either the Microsoft Windows version of Mozilla Firefox OR run Internet Explorer with Active/X and everything else turned off

Taking it to 11 and a half

- Get a mailbox at Mailboxes etc. and have your stuff sent there
- Form a company by filing a Doing Business As and get the credit card/mailing address going through that

Taking it to 12

- Anti-phishing toolbars (Netcraft and Firefox 2/3)
- Changing Browser Identification
- Open Proxies and Tor
- Use a more obscure O/S in your VM (Solaris/OpenBSD)
- Try a different browser Safari has privacy mode and Opera has some nice features as well
- Have a copy of Darrik's Boot and Nuke at the ready

Summary

My .sig for the last couple of years has been “The Journey is the Reward” - Old Zen Buddhist Saying

I hope you've gotten some ideas from this talk

References

Virtual Machines

- VMware Player - http://www.vmware.com/products/player
- QEMU - http://fabrice.bellard.free.fr/qemu
- Parallels - http://www.parallels.com

References

“Secure Browser”

- Noscript - http://www.noscript.net
- ShowIP - http://addons.mozilla.org
- SpoofStick - http://www.spoofstick.com

References

“Secure Machines”

- VMware Secure Appliance http://www.vmware.com/products/player
- QEMU - http://www.freeoszoo.org
- VMware images - http://www.thoughtpolice.co.uk/vmware/

References

One Time Use Credit Cards

- Discover Deskshop - http://www.discovercard.com/customer-service/secu
- Bank of America http://www.bankofamerica.com

Fini

Thank you for Listening...