Computer Security for the Home and Small Office

By Thomas C. Greene

Published by Apress (Berkeley, CA)

Reviewed by
Eric Beversluis
Kalamazoo Linux Group April 19, 2005

1984: “Big Brother is Watching”

Orwell's novel depicts a world in which the “benevolent dictators” control everyone else by virtue of the technology that permits Big Brother to be watching everywhere.

This is accomplished by two-way sound/video panels.

I've actually seen a M$ rep show pictures of prototypes of such panels.

Franz Kafka, The TRIAL

- Josef K. wakes up in his bed one morning to find his landlady gone and two men in his rooms who inform him that he has been arrested.
- He goes through long, nightmare-ish bureaucratic processes without ever learning what he has been charged with or coming to trial
- Today
  - multiple, inter-linked databases that contain and share information about us (Homeland Security)
  - already complexities of trying to fix “identity theft”
  - future: how to protect ourselves against mistakes and lies that get into these DBs and get shared from one to another?

Computer Security for the Home and Small Business: Themes

- Windows vulnerabilities
- Good-enough security: weigh threats and risks
- Multiple layers
- Don't expect or rely on absolute security
- Where the threats come from
- How-to's

Computer Security for Home and Small Office: Preface

Computer Security for Home and Small Office: Preface

- No special skills needed
- Extent of home users' lack of security
- Business also susceptible
- Demystify security—take it from the realm of gurus
- Focus on XP and Linux
- Thesis: Linux is easier for a non-specialist to make secure

Computer Security for the Home and Small Office: Introduction

Computer Security for the Home and Small Office: Introduction

- The Magic of Firewalls
  - addresses a small but important aspect of security
  - NAT contribution to security
  - stateful packet filtering
  - active services open ports that “will respond to packets sent from anywhere on the internet”
  - egress filtering: what's your computer sending out?
  - limits of firewalls

Computer Security for HOSO: Introduction

- “Hackproofing”
  - prevention: making it unlikely that your machine will be subject to attack
  - resistance: making your machine harder to hack if it is attacked
  - tolerance: protecting your data and communications should the box be compromised or communications intercepted
  - Security is a process; skepticism about claims of others and about one's own behavior and equipment; risks cannot be eliminated but can be managed.

Computer Security for HOSO: Introduction

- An Open-Source Solution
  - M$ weakness
    - archaic code
    - lack of transparency
    - problemmatic applications from other vendors
    - interdependent components
  - Why Mozilla?
    - modular
    - not a black box
    - more control (HTTP, Java, JavaScript)

Computer Security for HOSO: Introduction

- “Now that Microsoft has finally begun to address the security problems with HTML rendering and scripting support in their e-mail clients, the chief problems remaining are the numerous duplicate data traces that Internet Explorer and Outlook Express scatter about the system, the difficulty of removing them, and the integration of these applications into the low-level realm of Windows kernel, where risky client behavior can lead to radical system difficulties. . . . As Internet Explorer and Outlook Express can't be made secure enough no matter how hard one might try to overcome their shortcomings, we will simply bypass these problems by installing Mozilla in their place.” (xxxi)

Computer Security for HOSO: Introduction

- Secure Configuration
  - browsing history: set for one day
  - downloads: choose progress dialog option rather than download manager
  - disable automatic replies
  - block third-party cookies; block all cookies in Mozilla Mail; limit lifetime of cookies to current browser session
  - limit images to originating server; block all images in Mail
  - Forms, Password, Master Password options
  - Java can be left on if all the other computer security is in place.

More....

Computer Security for SOHO: Introduction

- Secure Configuration (cont)
  - JavaScript: probably should be disabled on Windows, though probably safe on Linux (and disable on Mail)
  - set page cache to 0 MB
  - set Mail to display incoming in plain text

Computer Security for SOHO: Ch 1, Introducing the Dark Side

Computer Security for SOHO: Ch 1, Introducing the Dark Side

- Overview of the sources of trouble
  - nuisances
  - plausible threats: “virus writers, script kiddies, spammers, carders (credit-card fraudsters), identity thieves, marketing profilers, social engineers (con artists), phreaks or phreakers (telephone system experts), overzealous law enforcement officials practicing the art of entrapment, and finally, a few exceptional, all-around hackers with superb programming skills and an intimate knowledge of network infrastructure.” (1)
- Debunking the “hacker mythology”
- Detailed hypothetical example and some real-world examples

Computer Security for SOHO: Ch 1, Introducing the Dark Side: Threats

- Trojans
- Rootkits and RATs
- Dictionary Crackers
- HTTP Exploiters
- Vulnerability Scanners
- Port Scanners
- Malware
- Viruses
- Worms
- Packet Sniffers
- Scripted Exploits
- Adware and Spyware

Computer Security for SOHO: Ch 1, Introducing the Dark Side: Child's Play

Why security can be compromised in organizations:

“In the employee's mind—and this is perfectly natural, even universal—the long-term relationship of trust with a friend takes precedence over the presumed expertise of a stranger, so he plays the CD on his workstation with hardly a second thought—and inadvertently installs a malicious virus on his company's professionally defended network behind a $60,000 firewall. He does this because no one has explained to him in truthful, adult language exactly what can happen when good security practices are ignored.” (14)

Computer Security for SOHO: Ch 1, Introducing the Dark Side: Child's Play

- Hypothetical example: 15-year old Robbie hacks his girlfriend's lawyers office computer via the lawyers home computer
- Lawyer's errors
  - publishing his home e-mail address
  - didn't use an anonymous proxy server to his true IP address
  - exposed shared directories to the Internet and left vulnerable services running on his home computer
- The Real World: script kiddies infect M$'s internal network with a root kit (QAZ)

Computer Security for SOHO: Ch 1, Introducing the Dark Side: Child's Play

- Free Porn and Easy Credit
  - Password cracking
    - unprotected plain text pass files
    - how to crack a hashed pass file
    - “Dictionary attacks work because people choose simple passwords.” (23)
  - Carders: stealing and using on-line credit card data bases
    - skilled hackers can even break into professionally defended credit card DBs (Petco and Guess exploits)
    - virtually impossible to protect our credit details from script kiddies and professional hackers.
    - one option: acct with dynamic CC number

Computer Security for SOHO: Ch 2, Vectors

Computer Security for SOHO: Ch 2, Vectors

- “A *vector* is any mechanism or agent that spreads, or enables the spread of, malware and scripted exploits.” (32)
- “The Internet may not be crawling with dangerous hackers as the news media like to pretend, but it is inundated with billions of bytes of incredibly lousy and often malicious code, while most PCs are loaded with gigabytes of wretched software that either offers no protection or is itself malicious. Hackers are *not* your primary security concern; bad software is.” (33)

Computer Security for SOHO: Ch 2, Vectors

- Common vectors
  - e-mail
  - browsers
  - scripts
  - instant messaging
  - P2P software
- Other vulnerabilities
  - OS vulnerabilities
  - application vulnerabilities
  - vulnerable services

Computer Security for SOHO: Ch 2, Vectors

- “Unsafe at Any Speed”
  - single-user vs multiple-user environments
  - risks of single-user environment: everyone is “root” all the time, so any exploit (remote or “hands on”) can gain full control
  - W98 and ME are single-user only
  - XP and 2000 are multiple-user, but the default user typically has full administrative privileges—need to create and use a second user with limited privileges.
  - M$ “security zone” approach
    - helps for W98 and WME, but foolish to extend it to 2000 and XP

Computer Security for SOHO: Ch 2, Vectors

Critique of “Security Zone Approach”:

“Windows is designed to grant and deny system privileges to third-party software and even to outside parties, based on preselected trust criteria. Digital certificates for Web sites and for software are proffered to persuade users that their trust criteria have been met. Meanwhile, the operating system is designed to trust code when Microsoft or the user trusts it or its provider, and this means that even users on a multi-user system can sometimes run or install powerful and potentially destructive code from an unprivileged account. =>

Computer Security for SOHO: Ch 2, Vectors

"This approach is wrong-headed from the start. It is the *user* whose privileges should be regulated, not the *provider* of a service or a piece of software. By making it possible for a piece of code to be trusted automatically *by the system*, Microsoft has made it possible for software to exceed the privileges of the user who installs it and scripts to exceed the privileges of the user who runs them. Thus a malicious program, apparently certified by Microsoft with a digital certificate, can be installed by a user and the system will grant it access to the deeper layers of the kernel. . . ." (44)

--Next-Generation Secure Computing Base (NGSCB), aka Palladium, continues and expands this approach. (Stay tuned.)

Computer Security for SOHO: Ch 2, Vectors

Critique of “Security Zone Approach” (cont)

“Unfortunately, this approach ignores the fundamental problem of allowing the system to trust code that the administrator has not approved, and even to exceed the administrator's authority in these matters. You can see the problem: even a minor flaw in this scheme could allow malicious code to be trusted and permit it to operate at a low level regardless of who installs it. This completely undermines the security benefits inherent in a multi-user environment. It means that your security will only be as good as Microsoft's grand trust scheme makes it, and considering Redmond's history in this area, I wouldn't put much faith in it.” (44)

Computer Security for SOHO: Ch 2, Vectors

- DEFENSE
  - “Disabling unnecessary services to reduce our attack profile.”
  - “'Sandboxing' users, or limiting their access to the system so that the code they run will also have limited access.” (45)

Computer Security for SOHO: Ch 2, Vectors

- DEFENSE (cont)
- Windows services to disable
  - Automatic Updates
  - ClipBook
  - Error Reporting Service
  - Indexing Service
  - Internet Information Service
  - Messenger (aka Windows Messenger; not MSN Messenger)
  - Net Logon
  - NetMeeting Remote Desktop Sharing
  - Network DDE
  - Network DDE DSDM
  - Network Location Awareness
  - Protected Storage

More =>

Computer Security for SOHO: Ch 2, Vectors

- DEFENSE (cont)
- Windows services to disable (cont)
  - QoS RSPV
  - Remote Access Auto Connection Manager
  - Remote Access Connection Manager
  - Remote Desktop Help Session Manager
  - Remote Packet Capture Protocol
  - Remote Registry Service
  - Routing and Remote Access
  - Server
  - SNMP Service
  - SNMP Trap Service
  - SSDP Discovery Service
  - TCP/IP NetBIOS Helper Service

More=>

Computer Security for SOHO: Ch 2, Vectors

- DEFENSE (cont)
- Windows services to disable (cont)
  - Telnet
  - Terminal Services
  - Universal Plug and Play (UPnP) (not PnP)
  - Upload Manager
  - WebClient
- Major no-no: cannot disable Remote Procedure Call (RPC), since a number of crucial services depend on it. Set firewall to block ports 135-139, 445, 593.
- Uninstall NetBIOS over TCP/IP
- DCOM (Distributed Component Object Model): (how MSBlaster was able to attack the Windows RPC service)

Computer Security for SOHO: Ch 2, Vectors

- DEFENSE (cont)
- Linux services to disable (“If you're using a major packaged distribution, it's likely that only a few of these services will have been enabled by default.” (56))
  - Apache
  - Berkely Internet Name Domain (BIND)
  - File Transfer Protocol (FTP)
  - Line Printer Daemon (LPD)
  - Nessus
  - Network Information Service (NIS)
  - Network FIle System (NFS)
  - Postfix
  - Remote Procedure Call (note: can disable this on Linux)

  More=>

Computer Security for SOHO: Ch 2, Vectors

- Disable on Linux (cont)
  - Rlogin
  - Samba
  - Secure Shell (SSH)
  - Sendmail
  - Simple Network Management Protocol (SNMP)
  - Squid
  - Telnet
  - Webmin
  - Ypbind

Computer Security for SOHO: Ch 2, Vectors

- Becoming a User: gives step by step instructions for setting up a low-privileged user in Windows
- Setting group and individual privileges

Computer Security for SOHO: Ch 3, Social Engineering

Computer Security for SOHO: Ch 3, Social Engineering

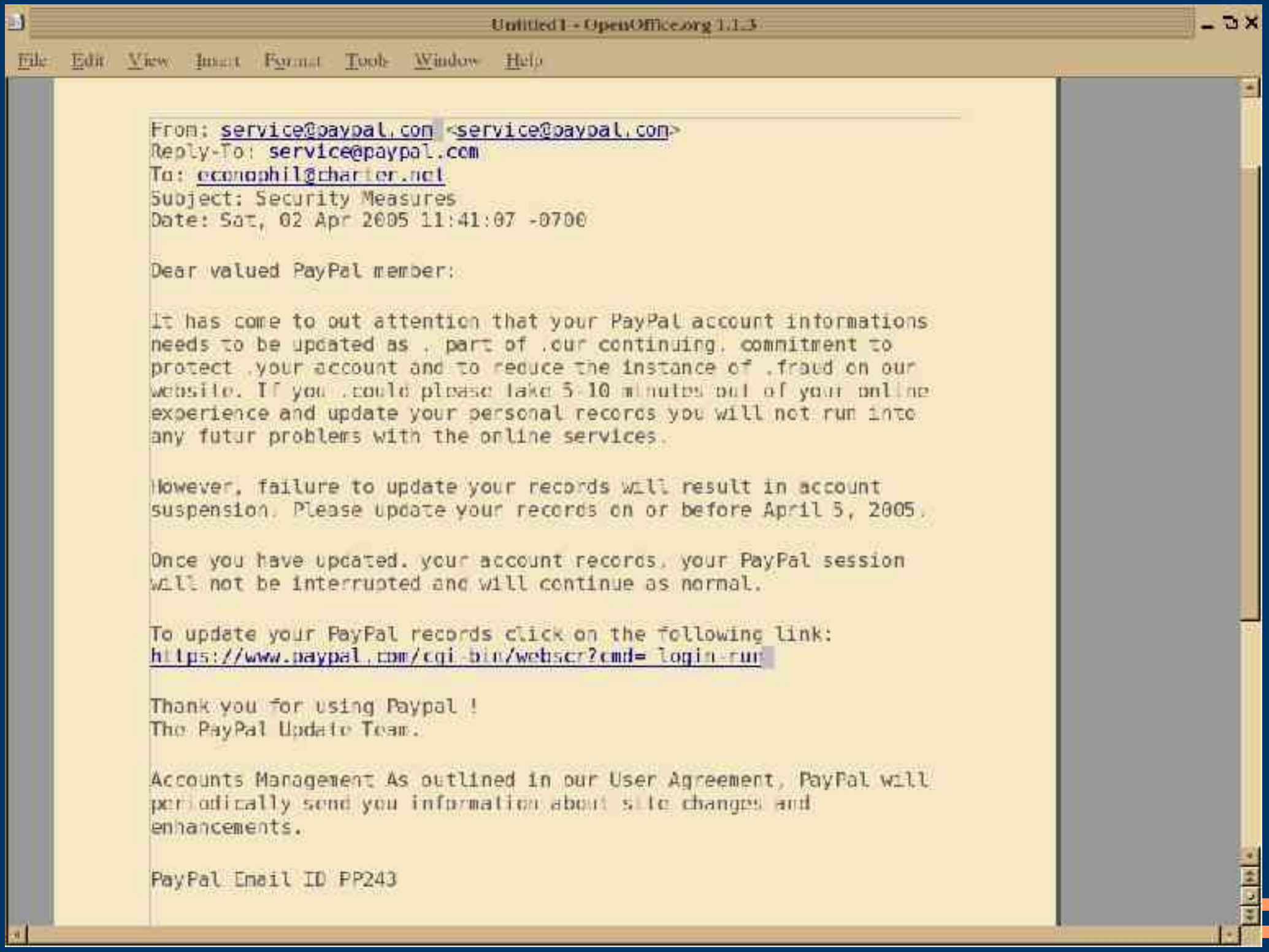
- Social Engineering: the fine art of getting someone to help you compromise computer security by giving you information that you need (passwords, account numbers, e-mail addresses) or by other cons (confidence games).
- Social engineering threats are the hardest to defend against
  - they utilize inter-personal relations
  - they are explicitly designed not to appear as threats.
- “. . . it's equally possible that SE is brutally effective not because it is neglected but because it is the most difficult type of attack to defend against. The entire game is based on the premise that victims should never suspect that they're being manipulated.” (76)

Computer Security for SOHO: Ch 3, Social Engineering

- “The best attacks involve the routine.” (76): thieves rolling a customs service server out of Sydney International Airport
- Clever attackers prepare thoroughly: they can learn more about an organization than most of its members know, just by research and friendly talk with various employees. Hypothetical case p. 78.

Computer Security for SOHO: Ch 3, Social Engineering

- Things that can be done
  - authenticate identities
  - call people back on a company-verified phone number if there is doubt as to who the person is
  - verify claims
  - avoid the on-the-job pressure to be servile to contacts
  - (scam e-mail): be alert to things like bad grammar and word choice


Untitled 1 - OpenOffice.org 1.1.3
File Edit View Insert Format Tools Window Help
From: service@paypal.com <service@paypal.com>
Reply-To: service@paypal.com
To: econophil@charter.net
Subject: Security Measures
Date: Sat, 02 Apr 2005 11:41:07 -0700
Dear valued PayPal member:
It has come to out attention that your PayPal account informations needs to be updated as . part of .our continuing. commitment to protect .your account and to reduce the instance of .fraud on our website. If you .could please take 5-10 minutes out of your online experience and update your personal records you will not run into any futur problems with the online services.
However, failure to update your records will result in account suspension. Please update your records on or before April 5, 2005.
Once you have updated. your account records, your PayPal session will not be interrupted and will continue as normal.
To update your PayPal records click on the following link:
https://www.paypal.com/cgi-bin/webscr?cmd= login-run
Thank you for using Paypal !
The PayPal Update Team.
Accounts Management As outlined in our User Agreement, PayPal will periodically send you information about site changes and enhancements.
PayPal Email ID PP243

RE: Q510 - Thank you for your email to PayPal (KMM941405V68525L0KM)

File Edit View Actions Tools

Reply Reply to All Forward Move Copy Print Delete Junk Not Junk Previous Next

Thank you for contacting PayPal.

We appreciate you bringing this suspicious email to our attention. We can confirm that the email you received was not sent to you by PayPal. The website linked to this email is not a registered URL authorized or used by PayPal. We are currently investigating this incident fully. Please do not enter any personal or financial information into this website.

If you have surrendered any personal or financial information to this fraudulent website, you should immediately log into your PayPal Account and change your password and secret question and answer information. Any compromised financial information should be reported to the appropriate parties.

If you notice any unauthorized activity associated with your PayPal transaction history, please immediately report this to PayPal by following the instructions below:

1. Log in to your account at https://www.paypal.com/ by entering your email address and password into the Member Log In box.

2. Click on Security Center at the bottom of the page.

3. Click on the 'Unauthorized Transaction' link under the Report a Problem column.

Computer Security for SOHO: Ch 3, Social Engineering

- Mad Cows and Englishmen (*pace* W. C. Fields?): Greene goes off on one of his tangents here, spending a couple of pages discussing the problems of Bovine Spongiform Encephalopathy (BSE), which is linked to the human *variant Creutzfeldt-Jakob disease* (vJCD).
- Distinguishing between *threat* and *risk*.
  - although the *threat* from vJCD is very high (if you get it, you die), the *risk* of getting it in the US is extremely low.
  - it is important to make this distinction in considering computer security =>

Computer Security for SOHO: Ch 3, Social Engineering

“Using, maintaining, and relying on a computer system involves threats and risks too, and these need to be appreciated separately and assessed individually, always on the basis of good information. But we must always accept compromises between security and convenience.... The goal of good security is to mitigate both threats and risks without making the whole affair more trouble than it's worth. Security, then, involves the art of making informed, sensible compromises . . .

More =>

Computer Security for SOHO: Ch 3, Social Engineering

“That's tough enough, but social engineering operates outside the realm of risk assessment and informed compromise. The threat can be anything from installing an irritating but nondestructive virus to the involuntary sharing of a decade's worth of R&D with a competitor. The risk is similarly unknown. What is the chance that someone will attack you in this manner? Might they use an insider for assistance? Might they be able to pass themselves off as an employee? A contractor? A business partner? . . .

“Remember, the social engineer is a chameleon, and his job is to convince victims that no danger exists and that caution and suspicion are therefore unnecessary. If he's good at it, he'll likely have his way in the end.” (90)

Computer Security for SOHO: Ch 3, Social Engineering

- Countermeasures
  - “. . . good social engineers attack in so many ways that the threat must be assessed as the worst that can happen.” (91)
  - make the defenses good enough that they will exceed the attacker's risk tolerance
  - home risk is mostly from script kiddies, unless there is particularly valuable material or access to a company computer, perhaps via VPN from the home user--Deutch of CIA
  - in business: all employees must be aware that they may be manipulated at any time—follow all protocols. The company needs good databases so employees can verify contacts seeking information or other privileges. Vendors etc. expected to provide good security at their end.

Computer Security for SOHO: Ch 4, From Newbie to Power User

Computer Security for SOHO: Ch 4, From Newbie to Power User

- Passive defenses: “narrowing our target and removing unnecessary features that attackers and malware can leverage against us.”
- Active defenses: “monitor our systems, investigate suspicious behavior, and take action.” (95)
- Home systems, unlikely to experience high-level, concerted attack; should use active defenses
  - “when software has been installed, updated or patched”
  - “when we wish to communicate privately via the Internet” (99)

Computer Security for SOHO: Ch 4, From Newbie to Power User

- Netstat: Identifies which network and Internet connections your computer has made—comes installed on nearly all computers
  - tells what connections are there
  - what the IP address of the connection is
  - what ports are involved in both computers
    - the specific ports let you know what services are involved
    - appendix to the book has lists of ports and associated services both *malus* and *bonus*
  - if there are connections and ports that you haven't opened, this can indicate malware

Computer Security for SOHO: Ch 4, From Newbie to Power User

- Ethereal is the open source packet sniffer that let's you see what data are actually being sent and received by your computer.
- Book contains “how to's” for Netstat and Ethereal

Computer Security for SOHO: Ch 4, From Newbie to Power User

- System Monitoring:
  - Adware/spyware detection: Ad-aware; Spybot Search & Destroy
  - Antivirus Software—scan all files downloaded from the I'net or received from IM, P2P, or e-mail

Computer Security for SOHO: Ch 4, From Newbie to Power User

- Why Linux is less at risk
  - less attractive: fewer boxes out there
  - harder to attack: not root; easier to disable vulnerable services; e-mail clients don't run scripts
  - Linux users with mail or file servers do need virus protection, to protect their Windows clients

Computer Security for SOHO: Ch 4, From Newbie to Power User

- Malicious processes
  - using Windows Task Manager to ID which processes are running
  - techniques for killing processes
  - malware names made to look like normal Windows processes
  - Use Google to check out process names you don't recognize
  - how to kill processes on Linux

Computer Security for SOHO: Ch 4, From Newbie to Power User: Encryption

"Data interception is an inherent feature of the Internet. Unless you take positive steps to prevent it, every byte of data that you exchange is logged and can be traced to you and whomever you exchanged it with. Cryptography makes data interception unproductive. " (120)

- Government opposition to encryption: misguided since the benefits of encryption outweigh the costs

Computer Security for SOHO: Ch 4, From Newbie to Power User

- “But crypto does enormously more good than harm. It secures intimate personal details against disclosure, protects sensitive business and financial data, and ensures that privileged communications between people and their doctors, lawyers, clergy, and the press will remain privileged. It enables relief workers and human rights advocates to communicate securely and to protect documents from disclosure in countries where what they say can get them imprisoned, tortured, even killed. . .” (121)
- “Personal crypto products are the last means of secure, and private, electronic communication left to us today.” (121)

Computer Security for SOHO: Ch 4, From Newbie to Power User: Encryption

- Types
  - hashing (basically one-way crypto: e.g, hash a password, and then when someone enters a password, hash it and compare the results)
  - asymmetrical paired-key cryptosystem =>

Computer Security for SOHO: Ch 4, From Newbie to Power User: Encryption

- How asymmetrical paired-key crypto system works:
  - Person A encrypts the message with the *public* key of the person whom the message is for.
  - The message is stored or transmitted securely—only the intended recipient can decode it
  - The recipient uses his *private* key to decode the message.
  - Public key is for anyone to use: it encodes
  - Private key decodes. It must be kept secure (if lost, no decoding)
    - very strong password
    - keep backup copies on separate media

Computer Security for SOHO: Ch 4, From Newbie to Power User: Encryption

- Sidebar: an interesting book:
  - Singh, Simon. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (1999) ISBN 0385495323

Computer Security for SOHO: Ch 4, From Newbie to Power User: Encryption

- PGP (Pretty Good Privacy): a semi-closed-source encryption tool for Windows
- GnuPG: free, open-source tool; works on Windows and Linux, but not easily on Windows
- Greene walks the reader through how to use these

Computer Security for SOHO: Ch 4, From Newbie to Power User: Encryption

- Crypto Snafus
  - someone with physical access to you computer could get your private key if its password is not strong enough
  - key logger: “It's ironic to consider the effort that's gone into making personal crypto products unbreakable by even the world's top mathematicians, and then to realize that some 13-year-old cretin with a rootkit can defeat them with ease. That is why I say there's no security without privacy, and no privacy without security. Hardening your system will make it a lot more difficult for someone to attack your machine with a rootkit and violate your privacy.” (143)
  - use PGP Wipe and Shred and Wipe to get rid of old data traces

Computer Security for SOHO: Ch 4, From Newbie to Power User: Encryption

- MD5: a hashing algorithm
  - basically, a one-way encryption.
  - store passwords
  - check integrity of downloads and other files, including those on your own computer (check if they've been tampered with)
- ”Unfortunately, AV scanners don't detect all malware. Some powerful commercial rootkits like eBlaster, SpyAnywhere, NetVizor, and the like are deliberately overlooked/ by the antivirus industry. (Apparently, so long as someone is earning a profit from malware, it ceases to *be* malware.) MD5 checking is a useful trick to know for those situations when you can't trust your antivirus software.” (144-5)

Computer Security for SOHO: Ch 4, From Newbie to Power User: Encryption

- SSH (Secure Shell)
  - “Essentially, it encrypts Internet and network traffic between two computers so that any traffic intercepted can't be deciphered.” (146)
  - uses
    - log in securely to your computer from a remote location
    - log in securely to a proxy server
    - SSH tunneling: encrypt all Internet traffic
  - SSH session
    - need SSH client (on your computer)
    - server that you connect to (e.g., your home computer or a proxy server)

Computer Security for SOHO: Ch 4, From Newbie to Power User

- SSH and anonymity: “. . .you can subscribe to a service like one offered by Anonymizer, which provides an SSH-enabled proxy server to which you can log in from anywhere. Essentially, it's a public SSH server that anyone can hire. Wherever you are, you can establish an SSH session with the Anonymizer proxy. The proxy will fetch all your Web, e-mail, IM traffic, etc., and encrypt it before forwarding it to you. Whatever equipment happens to lie between your computer and the proxy is irrelevant; all the data passing between them is protected.” (147)

Computer Security for SOHO: Ch 4, From Newbie to Power User

- SSH tunneling
  - works with *port forwarding*, so that the SSH port is the only one on my computer open to the I'net
  - does not keep your *e-mail provider* from reading your email: need to encrypt the message for that
- SSH for Windows:
  - various closed-source, commercial programs
  - PuTTY (just a client): free and open-source
- Linux: most distros include and install OpenSSH

Computer Security for SOHO: Ch 4, From Newbie to Power User

- SSL (Secure Socket Layer)
  - encrypts between browser and web-server
  - use with SSH to encrypt between the proxy server and the *terminus ad quem*
- WEP (Wireless Equivalent Privacy): use with WiFi to protect between your computer and the wireless access point
  - Greene does not note that WEP has been replaced by the more secure WPA (Wi-Fi Protected Access) in the newer 802.11g wireless systems

Computer Security for SOHO: Ch 5, Treasure Hunt

Computer Security for SOHO: Ch 5, Treasure Hunt

- Chapter deals with “data hygiene”: how do you keep your computer (and those computers out there) free of data traces that you don't want others to be able to access?
- “Anyone who might some day confront a court order for the contents of the PC needs [data hygiene].” (156)

Computer Security for SOHO: Ch 5, Treasure Hunt: Local Stealth

- Virtual Memory (aka swap file aka paging file)
  - not dynamic sizing
  - wipe periodically
  - try doing without it altogether
- File slack and unallocated space
- FAT32 easier to wipe clean than NTFS; on Linux, ext2 better than journaling file systems
- Shadow data
- The Windows Registry: no way to know what data it contains or to control what data it contains.

Computer Security for SOHO: Ch 5, Treasure Hunt: Local Stealth

- Windows Indexing Service: “The service creates and then consults a number of index catalogs, or databases. These catalogs contain data about your data, and therefore seriously undermine the practice of good hygiene” (167)
  - disable
  - delete the various index files
  - also the index.dat files (Windows give you a hard time; use Mozilla and they won't record data from it.)
- System Restore
- Temporary files
- E-mail traces

Computer Security for SOHO: Ch 5, Treasure Hunt: Local Stealth

- Print Spool
- Clipboard
- Recently accessed files—need to hack the Registry to disable this
- Browser traces: minimize the problem by using Mozilla, which, unlike IE, gives you complete control over the traces
- Command history: passwords can accidentally end up here

Computer Security for SOHO: Ch 5, Treasure Hunt: On-line Stealth

- “For all the utility and personal enjoyment it offers, the Internet remains the largest and most insecure network ever devised.” (178)
- Key asset we need to protect on the I'net is our *privacy*
- Myth that I'net allows criminals to perpetrate things anonymously
- Because of packet switching, each packet needs origin and destination information

Computer Security for SOHO: Ch 5, Treasure Hunt: On-line Stealth

- Online Stealth
  - SSH and content encryption (PGP and GPG) provide privacy (people can't read what you send) but not *anonymity* (people can tell who sent the transmission and where they sent it from)
  - When we might want anonymity but not privacy: e.g., political critiques, other censorship situations; others . . . (next slide)
  - Crowds as source of anonymity (Is Greene right here?)
  - Anonymizing proxy servers use the crowd principle
    - don't trust just any anonymizing service

Computer Security for SOHO: Ch 5, Treasure Hunt: On-line Stealth

- A Healthy Contempt for Surveillance
  - “If someone tells you that only criminals have something to hide, ask to install a wireless video camera in their bedroom and see how they react.” (186)
  - “Privacy and anonymity are your best defenses again the intrusions of marketers, spammers, data miners, social engineers, stalkers, overzealous police officers, sexual perverts, and other Internet parasites.” (186)
  - “It's as true today as it was in the Dark Ages: anonymity is the only shield capable of defeating censorship and enabling free speech. . . . Anyone who can afford to outspend you in court can shut you up.” (187)

Computer Security for SOHO: Ch 5, Treasure Hunt: On-line Stealth

- Notice: You Have No Privacy
  - Privacy policies (ISP, on-line businesses) are basically meaningless
  - Government beginning to use the data in various private DBs
  - To do:
    - skip on-line marketing surveys
    - set cookies to expire with each browser session
    - block third party cookies
    - supply fictitious info where there is no valid claim on correct info
    - use anonymous Web-mail accts for many purposes

Computer Security for SOHO: Ch 5, Treasure Hunt: On-line Stealth

- Wired Sprouts
  - children are objects of massive marketing efforts
  - children not equipped to deal with misleading, dishonest, or dangerous adults
  - “Parents should talk frankly about the dangers of privacy invasion with their older children, while small children should never be allowed to venture onto the Internet alone, but should always be supervised by a parent, teacher, sitter, or older sibling while using any Internet-related software.” (192)

Computer Security for SOHO: Ch 5, Treasure Hunt: On-line Stealth

- To do:
  - “Rather than pressure Congress to transform the Internet into a virtual “Sesame Stret,” parents should take more practical and effective steps toward protecting their children from pornography, hate speech, tasteless humor, profanity, marketing come-one, and sexual predators.” (192)
  - Internet filtering software—can be quite unhelpful
  - family-oriented ISPs—better bet
  - spyware only as last resort (“...so if a child insists on defying household rules and puts himself at risk with Internet use, it may be necessary to resort to an extreme measure like installing spyware.” (193))

Computer Security for SOHO: Ch 5, Treasure Hunt: On-line Stealth

- Keep I'net threats in perspective: the risk here is much lower than from most of the threats children are exposed to (media hype)
- I'net is like a bar: it's primarily an adult space, not a child space

Computer Security for SOHO: Ch 6, The Open-Source Escape Hatch

Computer Security for SOHO: Ch 6, The Open-Source Escape Hatch

- Brief history of Linux and open-source
- Caveats
  - PC games mostly not available
  - no adequate subs for MS Word or Excel—suggests CrossOver Office from CodeWeavers
  - installation
  - availability of drivers
  - laptop power mgmt functions—not all mfg's BIOS's support Linux in these areas
- LUGS (we know all about those) [Let's hear it for KLUG]
- Value for Money: dollars and sense

Computer Security for SOHO: Ch 6, The Open-Source Escape Hatch

- The Sins of William Perfidious
  - Why is Windows so bad?
  - Dogfood:
    - When MS bought Hotmail, their own internal analysis showed that it did not make economic or computing sense to switch from UNIX servers to MS servers.
    - However, MS should “eat its own dogfood” (quoted p 208)
  - Overview of other MS rantings and strategies against Linux
  - “Studies” comparing Windows and Linux whose outcome is “known” in advance

Computer Security for SOHO: Ch 6, The Open-Source Escape Hatch

- Suggestions on switching to Linux
- Summary: “Security is the chief topic of this book and from that perspective alone I would recommend Linux to just about anyone. Windows can be made fairly secure by firewalling, using antivirus software and adware/spyware scanners, patching regularly, disabling unnecessary services, setting up a multi-user environment, and replacing its Internet client software with open-source equivalents, and this is a perfectly reasonable strategy. But considering Windows' tremendous complexity, hidden functions and inescapable security flaws, migrating to Linux really is the best option, especially for people who aren't entirely confident =>

Computer Security for SOHO: Ch 6, The Open-Source Escape Hatch

- (cont) in their computer skills. Indeed, the *less* confident you are, the *better* Linux will suit you. Migrating alone will make your system harder to attack. The very transparency of a UNIX-based system, recognized by Microsoft, makes it easier to configure Linux for superior security. And Linux does a better job of sandboxing users so that any malware they encounter will have less impact on the system. Add a firewall or packet filter, disable unnecessary daemons, patch regularly, don't go on line as root, and your system will be safe from all but the top two or three percent of potential attackers. If you're a home user, you needn't worry about those people; they're not interested in your computer. The vast =>

Computer Security for SOHO: Ch 6, The Open-Source Escape Hatch

- (cont) majority of script kiddies and virus authors just don't have enough game to deal with a Linux box.” (216)

Computer Security for SOHO: Ch 7, Trust Nothing, Fear Nothing

Computer Security for SOHO: Ch 7, Trust Nothing, Fear Nothing

- This last chapter is long and, in places, tedious Probably could have been edited down and still served Greene's purposes well.
- What it does is explore the broader social/political context of computer security, with a lot of time looking at
  - areas in which gov't and private interests use fear-mongering about security to get questionable products and policies in place
  - areas in which gov't and private interests do the opposite, downplaying real threats to security, privacy and liberty

Computer Security for SOHO: Ch 7, Trust Nothing, Fear Nothing

- Trust nothing:
  - don't trust any particular software or hardware
  - don't trust what people tell you or try to sell you if you don't understand it
  - use layers of defense

Computer Security for SOHO: Ch 7, Trust Nothing, Fear Nothing

- “Again, the three essential layers of computer security are
  - *Prevention*: Keeping a low profile on line, using more trustworthy open-source clients and applications, and avoiding risky behavior like opening e-mail attachments.
  - *Resistance*: Making your machine difficult to attack by firewalling, disabling services, and tightening user permissions.
  - *Tolerance*: Using encryption and practicing data hygiene so that the fruits of a compromise are worthless to an attacker.” (276)

Computer Security for SOHO: Ch 7, Trust Nothing, Fear Nothing

- Fear Nothing
- “To use your computer and surf the Web without anxiety, simply refuse to trust your own machine, any network whether local or remote, any single security tool or service, any crypto scheme, any slogan like Trustworthy Computing, any digital certificate, any trust authority, any local client, or any remote host. Practice defense in depth, but never assume it's foolproof. . . .” (277)

Computer Security for SOHO: Ch 7, Trust Nothing, Fear Nothing

“Now you're paranoid in a healthy way, yet free from anxiety. Your computer, his network, their shopping cart—these things aren't the digital equivalent of bank vaults. So don't treat them as if they were, and move on and enjoy your life.

“If you're cautious and skeptical, and apply common sense to security, the odds against a system compromise or major invasion of privacy will be very much in your favor. But always remember that, regardless of the odds, it's foolish to wager something you can't afford to lose. Your credit card number is not a big deal: your total liability if $50 if you report its =>

Computer Security for SOHO: Ch 7, Trust Nothing, Fear Nothing

(cont) misuse promptly and you can get a new one in a week or so. The combination of your credit card number, Social Security number, name, date of birth, and address packaged together is a far greater worry because it makes identity theft so easy, so never give out more information than absolutely necessary to complete a transaction, and never let the merchant store your data." (277)

Computer Security for SOHO: Appendices

- Appendix A: Glossary
- Appendix B: Procedures, Processes and Ports.
  - step-by-step directions with screen shots for a lot of the techniques discussed in the text
  - lists of ports and their typical use (friendly or unfriendly)
- Appendix C: On-Line Resources

Summary and Reflections

- Is Greene excessively paranoid?
  - emphasizes the need for a match between security efforts and the worth of what you're trying to protect
  - e.g., most of my e-mail doesn't need any more privacy than, say, a conversation at a crowded beach
  - but some needs much more
  - broader issue of “creeping Big-Brother-ism”
  - if you're a staunch defender of liberty, then you need to be a staunch defender of privacy.

Summary and Reflections: Security Techniques

- Use Mozilla (Firefox?)
- Firewall w/ stateful packet filtering
- Anti-virus, anti-spyware, anti-adware
- Disable unnecessary services
- Mundane user accounts (shun Admin/root accts)
- Strong passwords
- File permissions
- Netstat and Etheral to check network traffic
- SSH and SSI when necessary
- Anonymizer when necessary
- Crypto when necessary
- Be alert for social engineering: don't compromise security procedures in response to cons
- Eliminate dangerous file traces
  - which are “dangerous”?
  - use across the board to be sure?
- Be stingy with info about yourself—protect your identity

Trust Nothing, Fear Nothing