Open Stance Security

Security for Public Networks

Conventional Wisdom

- My Network should be private.
- A Firewalls keeps hackers out.
- Anti-Virus software.
- Frequent Software Updates.
- Have duct tape and plastic on hand.



Encrypted Links Considered Harmful

- encourages insecure protocols
 - the email problem
- easy to upgrade software
- hard to upgrade hardware
 - Lots of broken WEP boxes



Best Practices and Design Techniques



Foreword by GARY MCGRAW



The Problem With Firewalls

- Home-Office Network Example
 - two or more firewalls
 - applications disabled
- The Office Network Example
 - Soft Underbelly
 - Infected Laptop Scenario



Anti-Virus Promotes Unsafe Software

- "I've got antivirus, so I'm fine"
- Got Updates?
- Lovely Zero-Day, isn't it?
- Viruses are a social problem
- Not an OS X Problem



Software Update Saves Lives

- One out of four isn't bad!
- There is still a risk of bugs...
 - ...and new problems.
- But they're NEW problems
 - flaws take time to exploit.

Software Update
Checking for new software
Install Name Cancel Version Size
^
Note: Use of this software is subject to the original Software License Agreement(s) that accompanied the software being updated. A list of Apple SLAs may be found here: http://www.apple.com/legal/sla/.
Quit Install
Quit Install
Note: Use of this software is subject to the original Software License Agreement(s) that accompanied the software being updated. A list of Apple SLAs may be found here: http://www.apple.com/legal(slaf.

Threats

Hardware Theft
Eavesdropping
Identity Theft
Computer Ownership



7

Security threats come in several flavors, we'll have a look at those most often faced by laptop users outside of an office network. While there are other types of attack these are the ones which are most likely to be faced by laptop users on public networks.

Hardware Theft

It's not the machine
it's the information.
encrypt sensitive data



Physical theft of a laptop or any other device with large amounts of storage can lead to massive loss of data and identifying information. The best mitigation strategy is encrypted storage, which prevents the thief from recovering any sensitive information.

Eavesdropping





9

Catching packets as they flow by on the wire or in the air is the least intrusive way to get ahold of sensative information. From the early days of aligator clips on telegraph wires to the modern protocol analizers which redally provide plain text output from unencrypted network connections the ability to listen in has kept pace with the ability to communicate.

Until recently the concern about evesdropping was a local one, police would need to physically clip wires in order to listen and network based intruders would need access to the physical network (i.e. the wiring) which tends to have the same security level as physical files and is therefor easy to understand. Wireless changes this picture as it allows for a remote intercept by a passive listener which leaves no trace in the target system. The recent NSA wiretap scandal also sheds light on the problem of trusted networks, the listener in the best position to eavesdrop is the common carrier.

Identity Theft

Information in large company databases
be very careful what you reveal
and who you reveal it to



Details of personal identity can be used by unauthorized parties to secure services and credit under the name of an innocent victim. When credit cards and other reputation based systems are involved these details are almost alwasy aquired from a government or corprate database using various means discussed here.

On a more local scale session hijacking can result in the short-term access to privledged services and information by way of intercepting a HTTP cookie or session URL from an insecure web site. Exposure of this types is usually limited but it can lead to other sensative information being disclosed.

Ownership

"We are botnet, resistance is futile"
Not a problem for OS X



Perhaps the most insidious attack is the attempt to gain '0wnership' of many hundreds of remote computers through the use of trojan horse software. These comprimised machines can be turned to any number of nefarious purposes as part of a bot-net. This is a serious problem for owners of insecure computers on home DSL lines which are always connected to the internet and can be comprimised and herded into bot-nets forming powerful distributed systems suitable for launching denial or srevice attacks and hosting phishing and pharming sites.

What is an Open Stance?

- Open Network Access
- Public Addressing
- Secure Applications
- For Home & Laptop Users



iStumbler Recommends that you adopt an **Open Stance** security policy. Open Stance means **securing your computer and it's applications so that it can be safely connected to any network at any time**. We advocate the use of **open networks**, **public addressing** and **secure application layer protocols** which are designed to provide reliable privacy and secure authentication while allowing the full use of existing internet services.

The Open Stance security policy specifically rejects the use of encrypted networks, virtual private networks, firewalls and other technology which is designed to create a safe network context in which insecure applications and protocols can be used with reduced risk. These half-solutions are in fact making security on the internet worse every year, as they allow sloppy security in software development practices to continue and create an Internet of walled-off networks containing extremely vulnerable machines.

Open Stance is not appropriate to all situations, it's intended to protect personal users on public networks not as a replacement for enterprise or business security.

Secure Computing

- Turn off network services
- Reduce Administrative Access
- Encrypt Sensitive Data
- Eliminate Infection Vectors

Looking at the information that needs securing and the present threats we can formulate a few simple rules for securing your computer.

Who's Watching the Listeners?

Show All Q Computer Name: cheetah Other computers on your local subnet can access your computer at cheetah.local Edit Services Firewall Internet Select a service to change its settings. On Service Personal File Sharing Personal File Sharing On Image: Stop Click Stop to prevent users of other computers from accessing Public folders on this computer. Pipe Remote Login FTP Access Apple Remote Desktop Remote Apple Events Printer Sharing Xgrid Other Macintosh users can access your computer at afp://10.0.1.201/ or browse for "cheetah" by choosing Network from the Go menu in the Finder.	Show All (1) Computer Name: cheetah Other computers on your local subnet can access your computer at cheetah.local (1) Cher computers on your local subnet can access your computer at cheetah.local (1) Cher computer computer at cheetah.local (1) Cher computer cheetah (1) Cher computer computer at afp://10.0.1.201/ or browse for cheetah (1) Cher computer computer changes. (1) Cher computer computer changes. (1) Cher computer computer changes. (1) Cher computer computer computer computer computer changes. (1) Cher computer co	Show All Computer Name: cheetah Other computers of your computer at Services Select a service to change its settin On Service Personal File Sharing Windows Sharing Personal Web Sharing Personal Web Sharing Remote Login FTP Access Apple Remote Desktop Remote Apple Events Printer Sharing Xgrid Other Macintosh users can access your co 'cheetah' by choosing Network from the	on your local subnet can access cheetah.local Edit Firewall Internet ngs. Personal File Sharing On Stop Click Stop to prevent users of other computers from accessing Public folders on this computer.
Computer Name: cheetah Other computers on your local subnet can access your computer at cheetah.local Edit Services Firewall Internet Select a service to change its settings. Personal File Sharing On Stop Mindows Sharing Personal File Sharing Click Stop to prevent users of other computers from accessing Public folders on this computer. Mindows Sharing Click Stop to prevent users of other computers from accessing Public folders on this computer. Mindows Sharing Click Stop to prevent users of other computers from accessing Public folders on this computer. Other Macintosh users can access your computer at afp://10.0.1.201/ or browse for "cheetah" by choosing Network from the Go menu in the Finder.	Computer Name: cheetah Our computer at cheetah.local chit Computer Apple Remote Desktop	Computer Name: cheetah Other computers of your computer at Services Select a service to change its settin On Service Personal File Sharing Personal Web Sharing Personal Web Sharing Personal Web Sharing Personal Web Sharing Remote Login FTP Access Apple Remote Desktop Remote Apple Events Printer Sharing Xgrid Other Macintosh users can access your co 'cheetah' by choosing Network from the	on your local subnet can access cheetah.local Edit Firewall Internet ngs. Personal File Sharing On Stop Click Stop to prevent users of other computers from accessing Public folders on this computer.
Select a service to change its settings. On Service Personal File Sharing Windows Sharing Personal Web Sharing Personal Web Sharing Remote Login FTP Access Apple Remote Desktop Remote Apple Events Printer Sharing Xgrid	Select a service to change its settings. On Service Personal File Sharing Personal File Sharing On Windows Sharing Stop Personal Web Sharing Click Stop to prevent users of other computers from accessing Public folders on this computer. FTP Access Apple Remote Desktop Remote Apple Events Printer Sharing Xgrid Other Macintosh users can access your computer at afp://10.0.1.201/ or browse for "cheetah" by choosing Network from the Go menu in the Finder. Image: Click the lock to prevent further changes. Image: Click the lock to prevent further changes.	Select a service to change its settin	ngs. Personal File Sharing On Stop Click Stop to prevent users of other computers from accessing Public folders on this computer.
(?	Click the lock to prevent further changes.		computer at afp://10.0.1.201/ or browse for e Go menu in the Finder.

14

Listeners are processes which listen for incoming network connections. For a personal computer used to read mail, surf the web and create and edit office documents there should be exactly zero listeners.

Network services open ports which are one the vectors along which worms can travel to infect a computer. Only run network services if you need them and make every effort to secure them. On a Mac OS system you can make very good use of another remote computer using just SSH

Restrict Administrative Access

You're glad you got a Mac
This is painful in windows



Limit the use of administrative privilege, which gives you the ability to really make a mess of your computer.

Encrypt Sensitive Data

File Vault may be Overkill

Encrypted Sparse Images



encrypts and decrypts your files while you're using them. WARNING: Your files will be encrypted using your login password. If you forget your login password and you don't know the master password, your data will be lost.

A master password is not set for this computer. Set Master Password... This is a "safety net" password. It lets you unlock any FileVault account on this computer.

FileVault protection is off for this account. Turning on FileVault may take a while.

Turning on Frievault may take a while

Turn On FileVault...

16

OS Vendors provide various methods for securing sensitive information, it's a very good idea to encrypt anything you wouldn't want someone who stole or purchased the device later to recover.

Eliminate Infection Vectors

- Don't open attachments
 - Even on OS X
- Careful With Downloads
- Don't use Explorer
 - or Outlook



Virus and Trojan horse infections rely on a vector to move themselves to your computer. The term is borrowed from epidemieology where it refers to the way in which a virus infects it's host, malaria for e.g. uses mosquitos as one vector of infection.

The two most common vectors for computer infection are Internet Explorer and Outlook, replacing these two pieces of software with Firefox and Thunderbird can almost completely eliminate the problem of virus, spyware and adware trojan infections.

Secure Applications

- Secure Email Protocols
- PGP Mail Not Easy
- Secure Web Sites
- iChat + .mac / Skype / Meetro



18

Public networks are not trustworthy. Read the headlines and you'll quickly see that AT&T is giving access to your traffic for NSA analisys, hotspots are like watering holes on the savanna, everybody comes to drink and predators lurk on the fringes. Since you can't always control or trus the networks you're using the key is to use security applications. This is refefred to as **end to end security** and it can provide you with privacy even when you are using your computer on an open wifi network at the coffee shop down the street.

Secure Email

- Use SSL for IMAP & POP
- Secure SMTP not perfect
- Real email security is hard
 - Deals with Spam



19

SPOP and IMAPS provide transport security for checking your email, use them to keep your email private from local eavesdroppers and to prevent the loss of your username and password. Sending email is a very different issue, you can secure the connection to your SMTP server but the mail will be stored in plain-text on the mail server, which means that your ISP (and potentially the NSA) can read all your mail, coming and going.

Unfortunately email is not a private medium, it's essentially the same as sending a postcard through the mail. Most of the time only the recipient reads it but anyone who handles it along the way can easily turn it over and see it's contents.

There are solutions to securing your email but they rely on public-key cryptography which has not yet achieved the ease of use necessary for widespread adoption. Several problems need to be solved around the issuance and distribution of public keys.

Secure Web Sites



<u>https://secure.com/</u>

000 Bank of America Online Banking Sign In to Or	line Banking
Bank of America Online B.	Inquisitor
Bankof America Higher Standards	Online Banking
Sign In	
Enter Online ID: (6 - 32 characters) Save this Online ID (How does this work?) Constant Where do lenter my Pessode Foroat or need help with your ID2	Not using Online Banking? Enroll now for Online Banking >> about Online Banking >> Service Agreement >> Go to Online Banking for a state other than Catifornia
Secure Area Hone + Localizes + Contact Us + Help + Sign in + Site Hap Personal France + Small business + Corporate & Institutional About the Bank + In the Community + Finance Tools & Renning + Privacy & Security Bank of America, TA, Member 902, Escual Iouxing Londer © 2006 Bank of America Corporation. All rights reserved.	Official Sporney 200, 200
 Approximate Approxim	

20

Web pages come in two flavors, plain-text and secure, you can tell the difference from the protocol portion of the url, which comes before the colon: <u>http://plaintext.com</u> or <u>https://secure.com</u>. When a web site uses the https protocol all the traffic is secure between you and the server hosting the page. When a site uses plain http the text of the web page and any responses that you send to it are sent in plain-text.

For browsing and read the web http is generally acceptable, but when you are providing or looking at sensitive information then https is necessary to prevent eavesdroppers from intercepting your traffic.

Secure Chat

<text>

21

Most chat clients and protocols are insecure and all messages are routed through a central server which is in a position to log or intercept all messages. There are some commercial chat solutions which apply public-key cryptography to secure messages but they have the same problems as email.

Secure P2P



000	Acquisition - De	ownloads		\bigcirc
Q Search			🗈 🚴 🤇	
★ What's New?	All Active (2) Inactive Co	Q Filter		
Q one man wrecking	File Name	Transfer	Progress	▼ Tin…
Q quake 2	V For Vendetta 1 of 2 8 active, 32 busy (of 47)	35.6kB/s 123.9MB/698.5MB		3 4 ho remai
Q quake II Q v for vendetta 24	V For Vendetta 2 of 2 8 active, 124 busy (of 138)	18.4kB/s 43.5MB/699.9MB		3 10 hc remai
📀 Connected				
• 54.0kB/s 2				
13.3kB/s				
¢-				1
0				
0 13 3MR 8				

22

Peer to Peer networks are inherently public, don't share anything you wouldn't want to be associated with. This is especially imprint now that the RIAA is trolling P2P networks looking for 'stolen' networks. Once an RIAA scanner identifies that you have some britney spears in your shared folder it logs your IP address and issues a subpoena to your ISP so that they can forward your information to the settlement center.

Public Addressing

- Just say No to NAT!
 - Better P2P Connections
 - Better Video chat
- Address are getting expensive
 - May wait for Internet 2 (IPv6)
- .public network tagging for wireles
 - identify open networks



23

A typical DSL connection is issues one static or dynamic routable address. For most wireless users this address is used by their wireless access point which allocates and performs Network Address Translation for a private network (numbered 10.x.x.x, 192.168.x.x or 172.x.x.x). While this is convenient since you don't have to manually configure each computer added to the network it is very difficult to connect directly to a computer inside the private network from the the public internet.

Open Network Access

Disable WEP, WPA, 802.1x
Use secure protocols
Tear Down that firewall
Encourages Port Control
Last step in the process



Once your computers and applications are secured it possible to take the final step and open up your own network to public use. As long as there is no reason to suspect abuse (you live upstairs from a coffee shop for e.g.) you can now safely open up your network for visitors, neighbors and people in the





Thank You!

- <u>alf@istumbler.net</u>
- <u>http://istumbler.net</u>
- <u>http://istumbler.net/papers/open-stance.html</u>