Open Stance Security

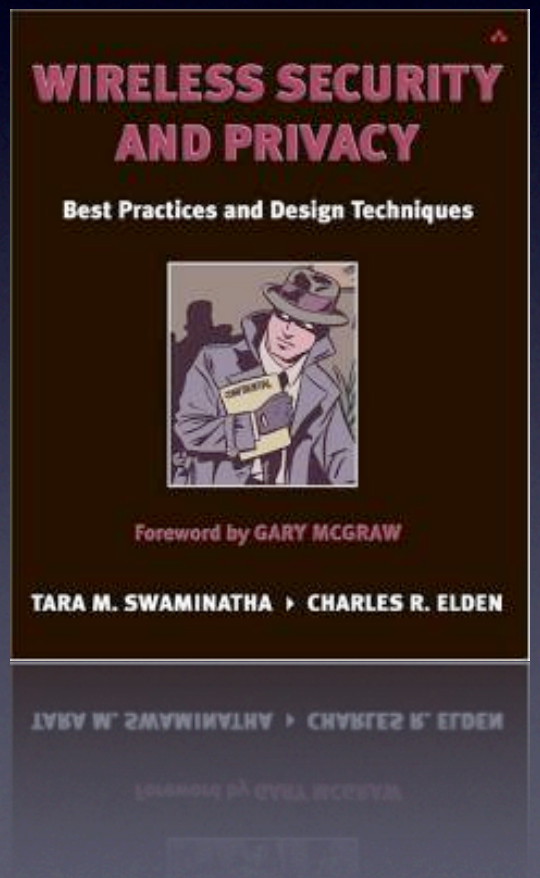
Security for Public Networks

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.

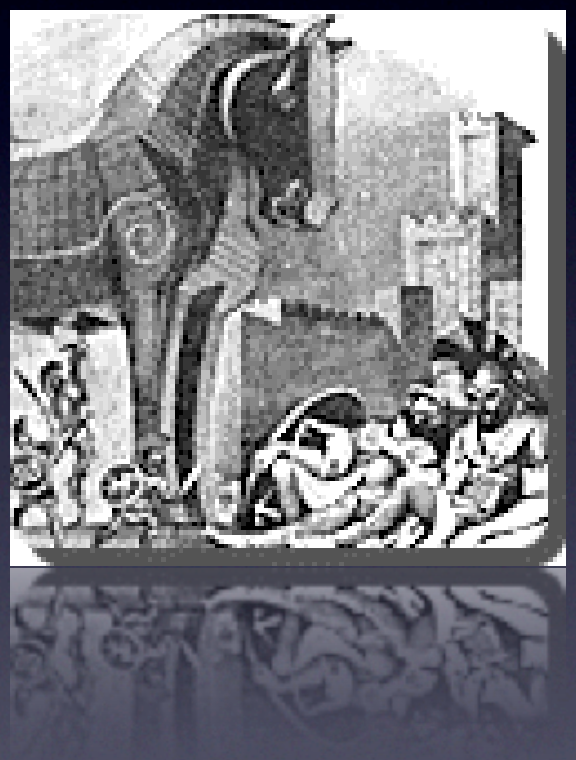
Encrypted Links Considered Harmful

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



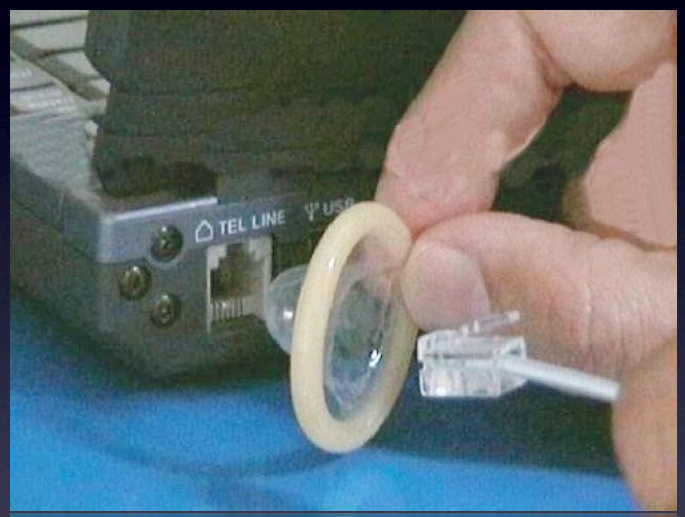
The Problem With Firewalls

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



Anti-Virus Promotes Unsafe Software

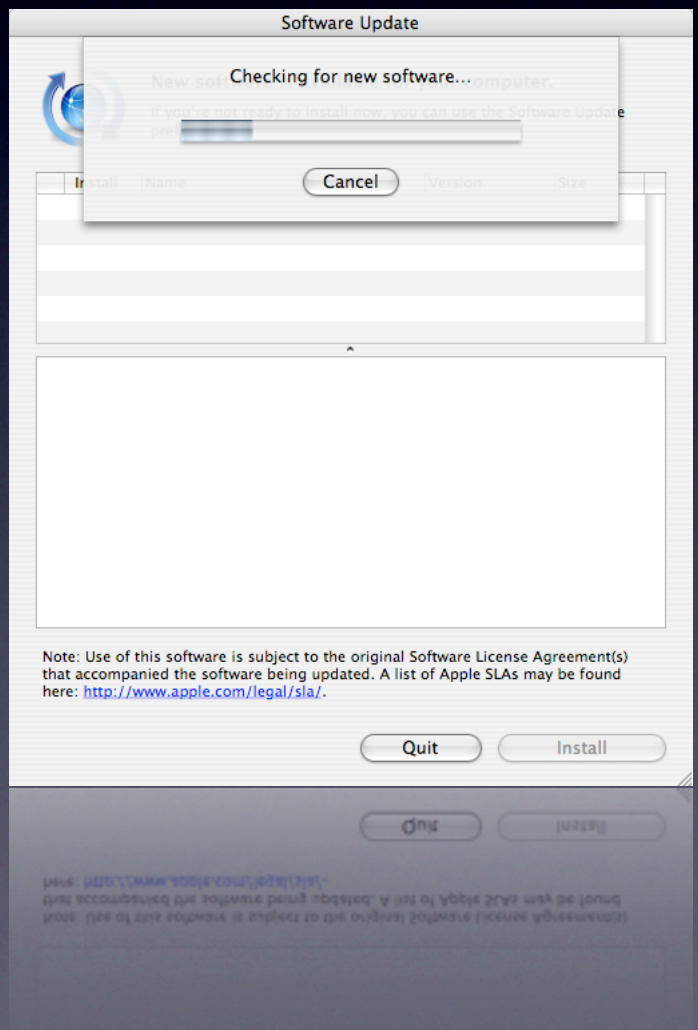
- "I've got antivirus, so I'm fine"
- Got Updates?
- Lovely Zero-Day, isn't it?
- Viruses are a social problem
- Not an OS X Problem



Anti-Virus Promotes Teen Sex

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.



Threats

- Hardware Theft
- Eavesdropping
- Identity Theft
- Computer 0wnership

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.

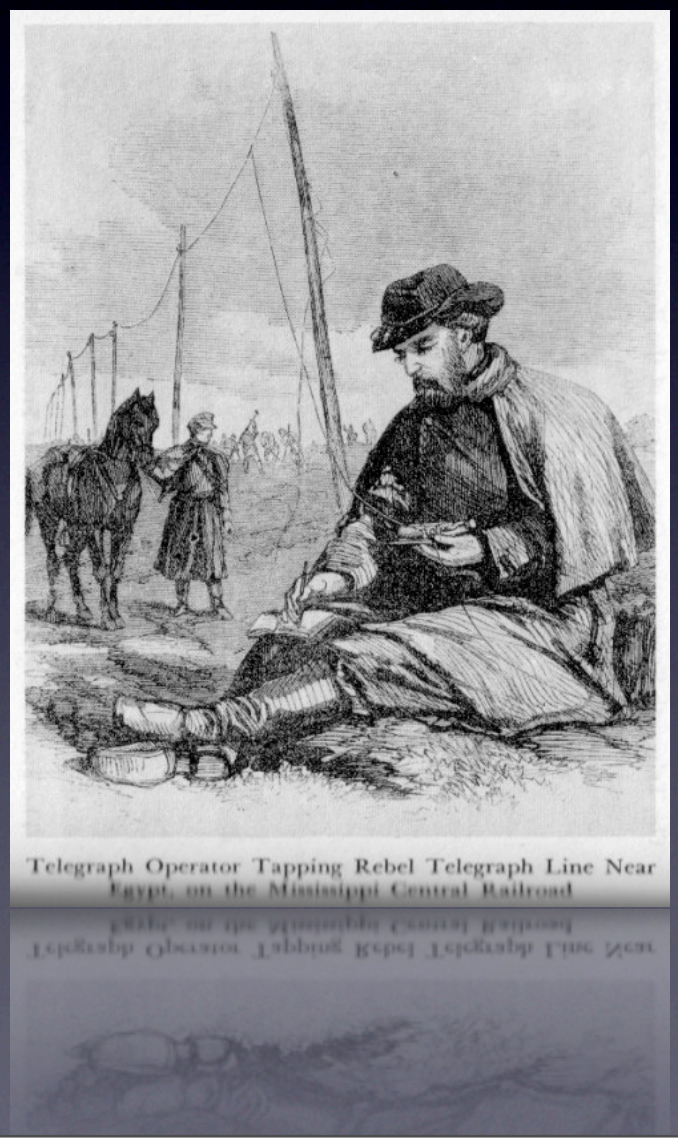
Hardware Theft

- 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

- NSA Wiretap System
  - in the core of the net
- Nearby Listeners
  - at the hotspot



Telegraph Operator Tapping Rebel Telegraph Line Near Egypt, on the Mississippi Central Railroad

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 usutally limited but it can lead to other sensative information being disclosed.

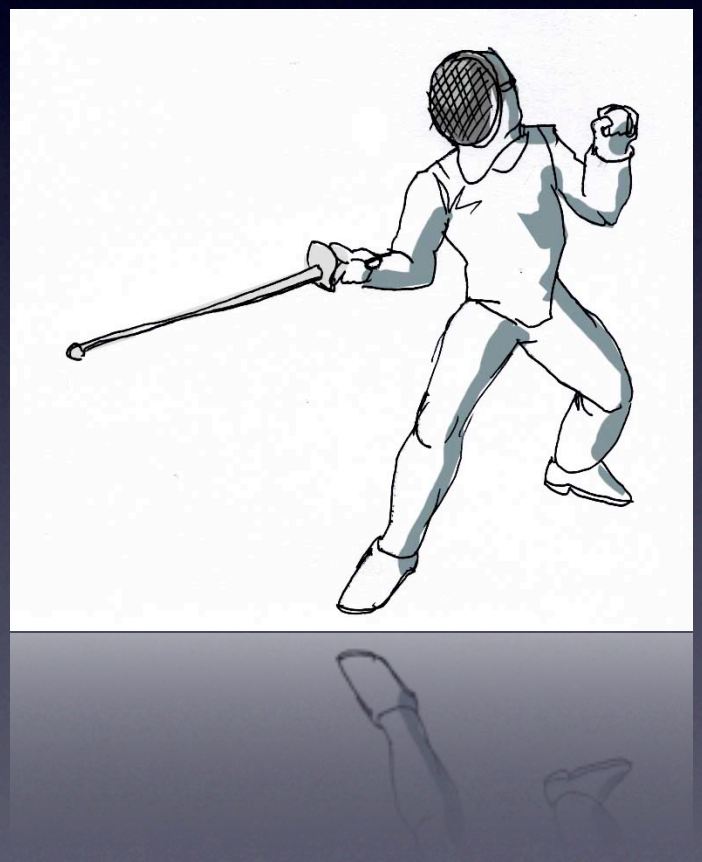
0wnership

- "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.

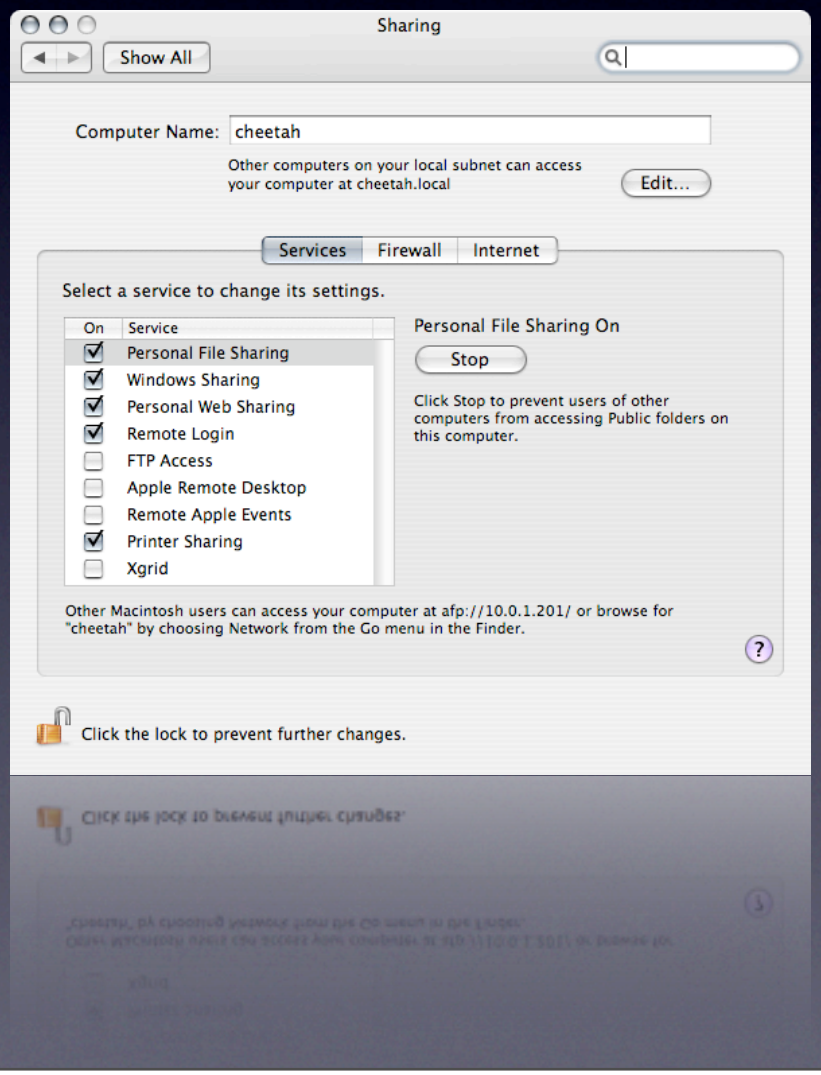
Open Stance is not appropriate to all situations, it's intended to protect personal users on public networks not as a replacement for enterprise or business security.

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?

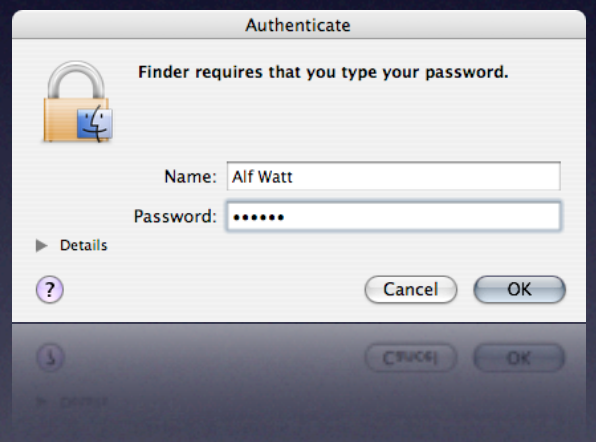


Listeners are processes which listen for incoming network connections. For a personal computer used to read mail, surf the web and create and edit office documents there should be exactly zero listeners.

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

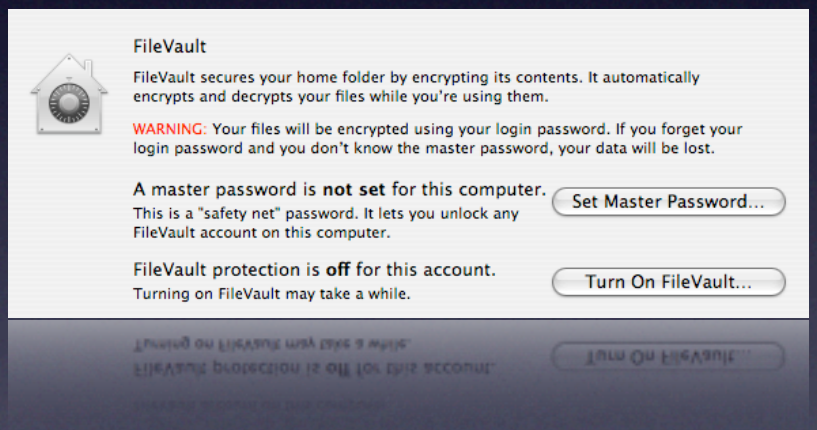
- You're glad you got a Mac
- This is painful in windows



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



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

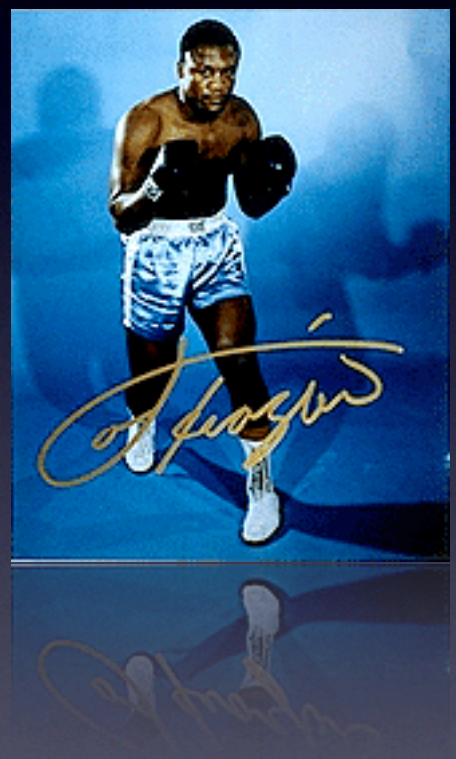
- Don’t open attachments
  - Even on OS X
- Careful With Downloads
- Don’t use Explorer
- or Outlook

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

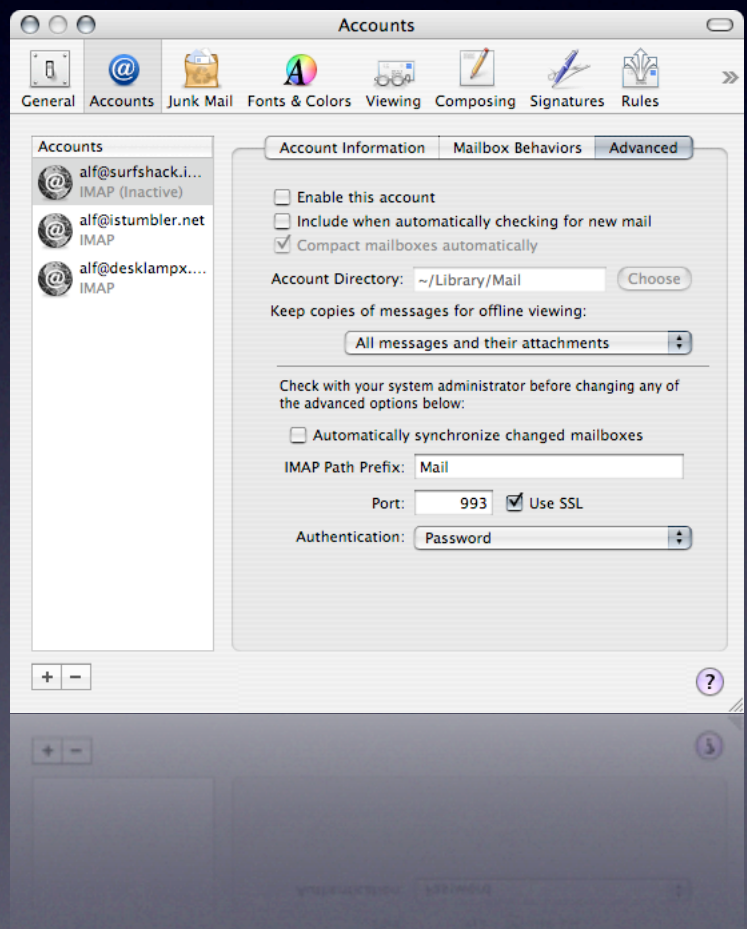
- Secure Email Protocols
- PGP Mail – Not Easy
- Secure Web Sites
- iChat + .mac / Skype / Meetro



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



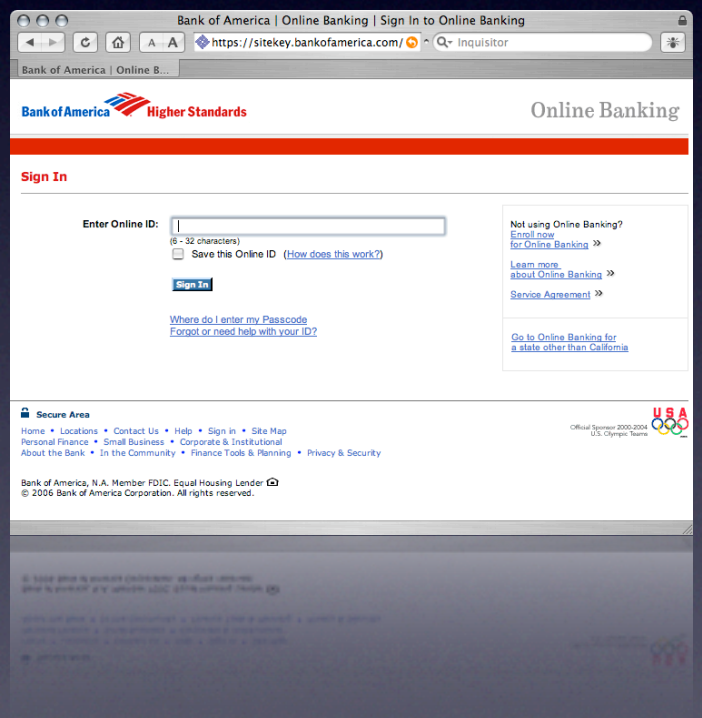
SPOP and IMAPS provide transport security for checking your email, use them to keep your email private from local eavesdroppers and to prevent the loss of your username and password. Sending email is a very different issue, you can secure the connection to your SMTP server but the mail will be stored 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

- http://insecure.org/
- https://secure.com/

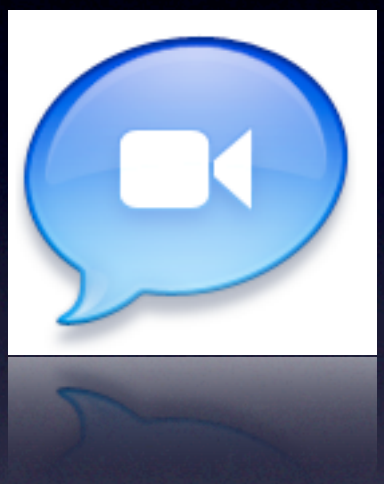


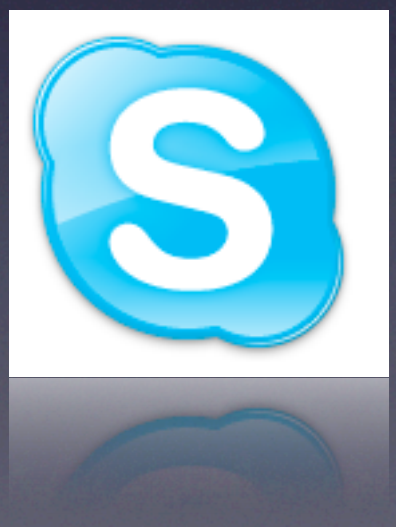
Web pages come in two flavors, plain-text and secure, you can tell the difference from the protocol portion of the url, which comes before the colon: `http://plaintext.com` or `https://secure.com`. When a web site uses the https protocol all the traffic is secure between you and the server hosting the 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.

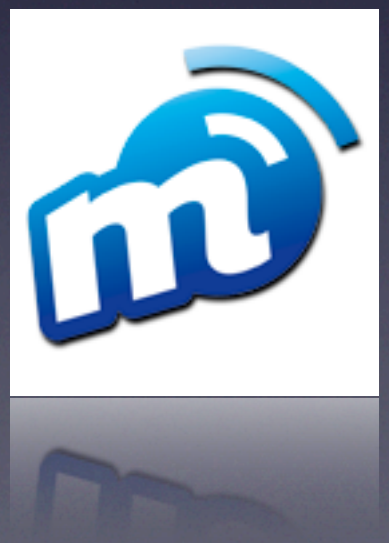
For browsing and read the web http is generally acceptable, but when you are providing or looking at sensitive information then https is necessary to prevent eavesdroppers from intercepting your traffic.

Secure Chat

- iChat + .mac
- Skype and Meetro
  - Out of the box!



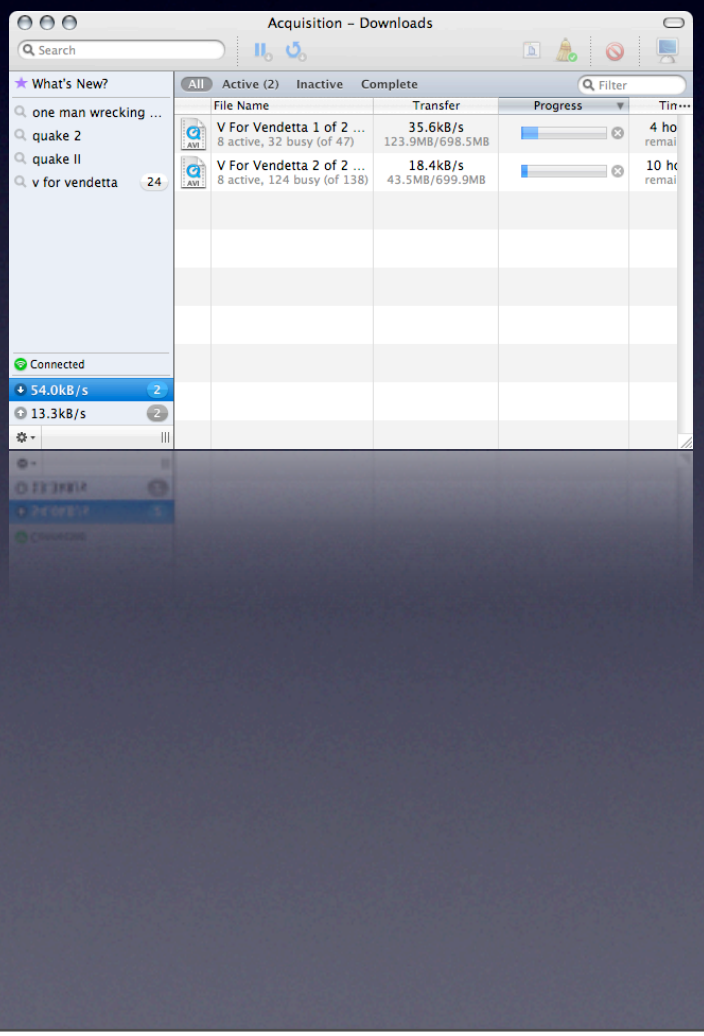




Most chat clients and protocols are insecure and all messages are routed through a central server which is in a position to log or intercept all messages. There are some commercial chat solutions which apply public-key cryptography to secure messages but they have the same problems as email.

Secure P2P

- Careful what you share
- It's a public space



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

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

Q&A

- Questions?

Thank You!

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