Open Stance Security

Security for Public Networks

2016 Edition

Conventional Wisdom

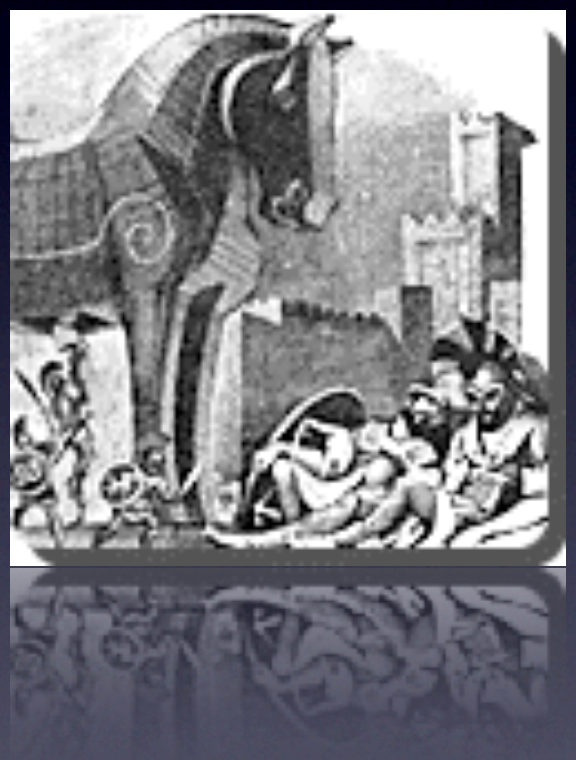
- My Network should be private.
- A Firewalls keeps hackers out.
- Anti-Virus software.
- Frequent Software Updates.
- Have duct tape and plastic on hand.

Encrypted Links Considered Harmful

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

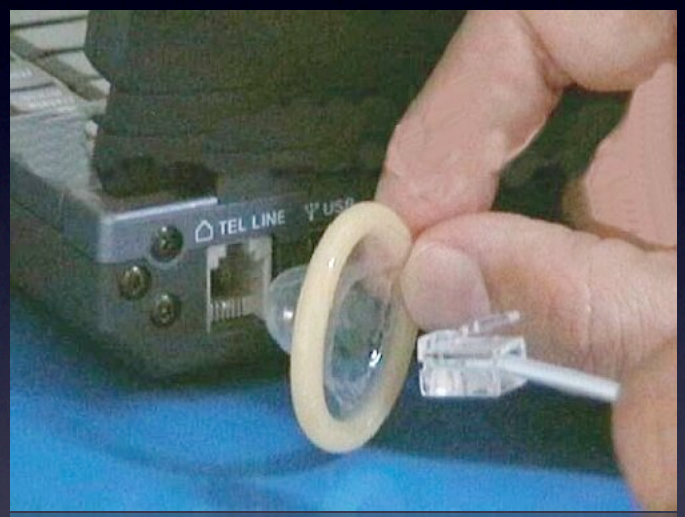
The Problem With Firewalls

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



Anti-Virus Promotes Unsafe Software

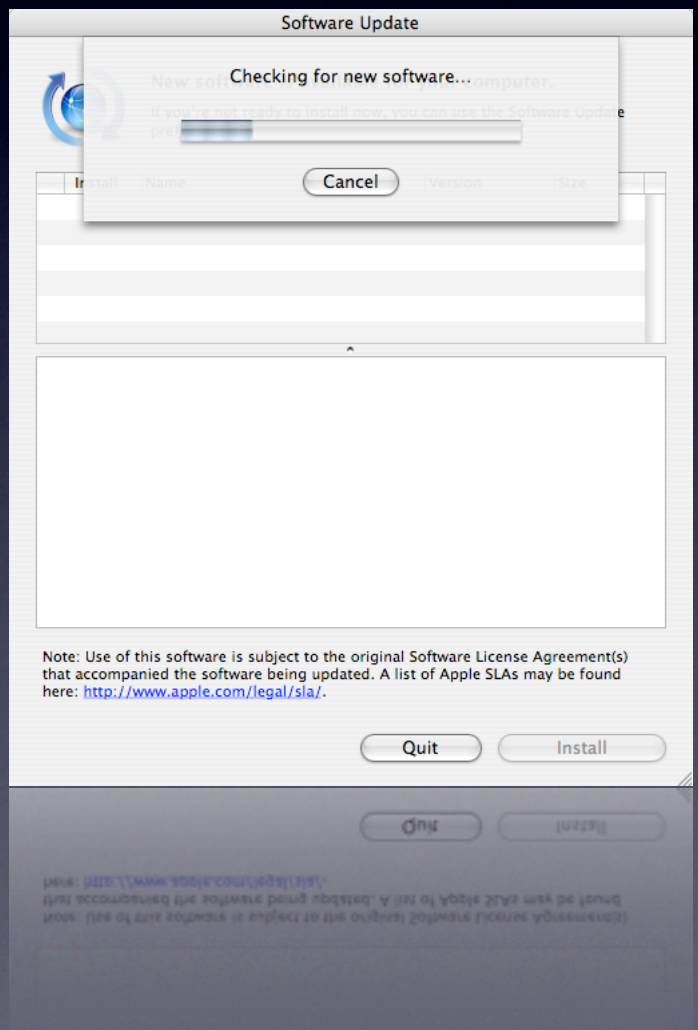
- "I've got antivirus, so I'm fine"
- Got Updates?
- Lovely Zero-Day, isn't it?
- Viruses are a social problem
- Not an OS X Problem



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.

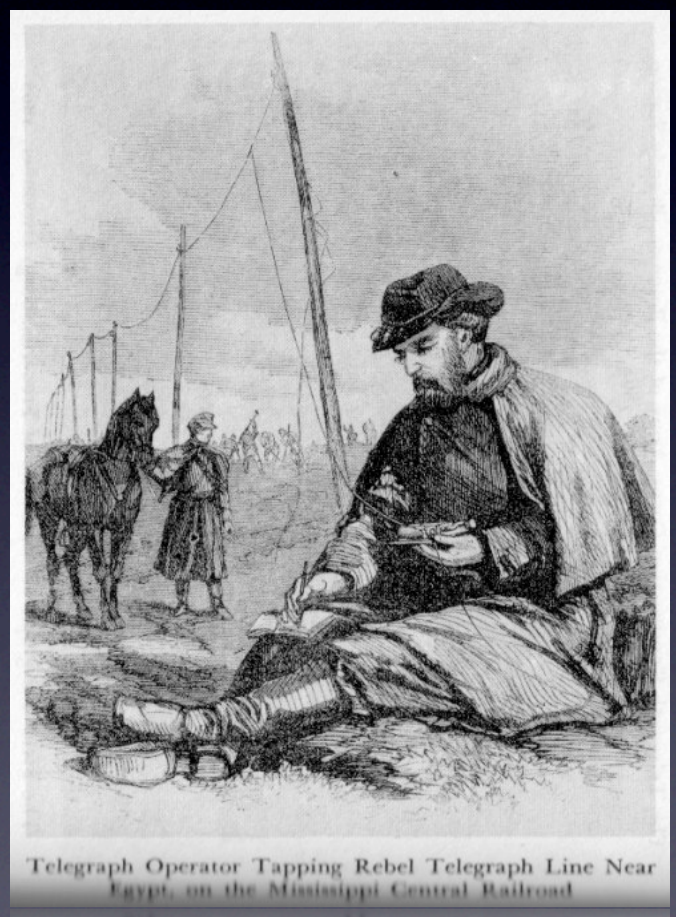
Hardware Theft

- 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.

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.

Thank You!

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