

# Is Starbucks Safe?

Network Security  
Wireless in particular

# Caveat

- I'm not an expert
- I'll share what I know
- A basis for discussion

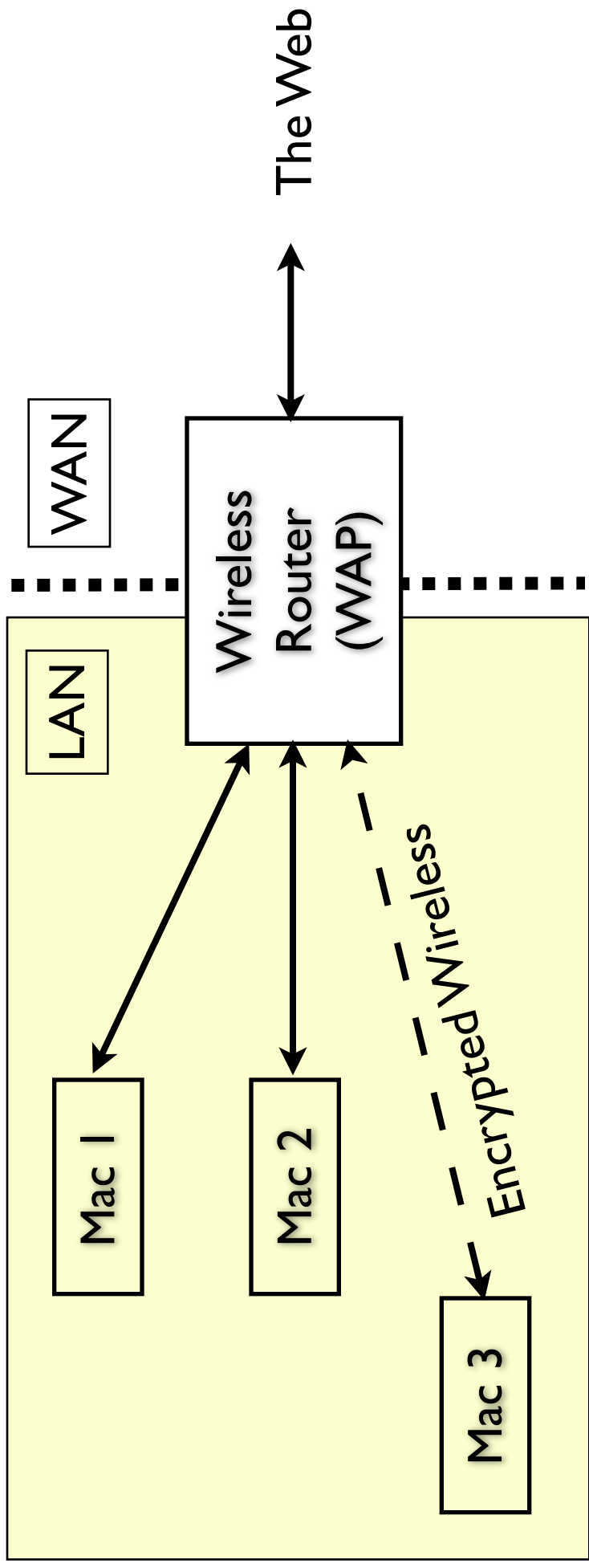
# Geek Speak

- WAN = Wide Area Network = the web
- LAN = Local Area Network = your house
- WAP = Wireless Access Point = router
- SSL = Secure Socket Layer = secure communication using encryption
- VPN = Virtual Private Network



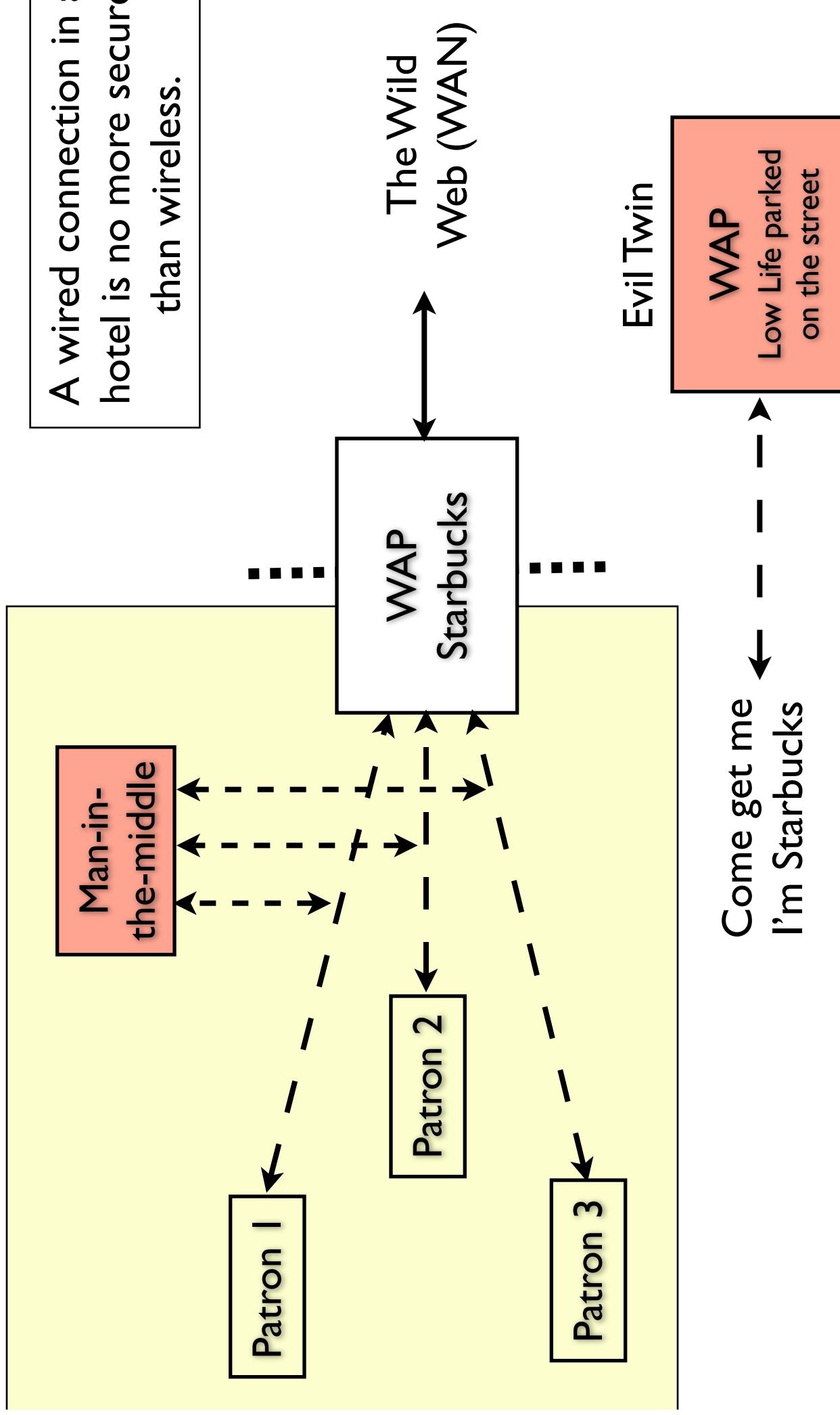
# Home Network (LAN)

A router connects two networks together  
Usually a local network to the Internet



Firewall  
Hides your LAN  
from the WAN

# Starbucks = public LAN

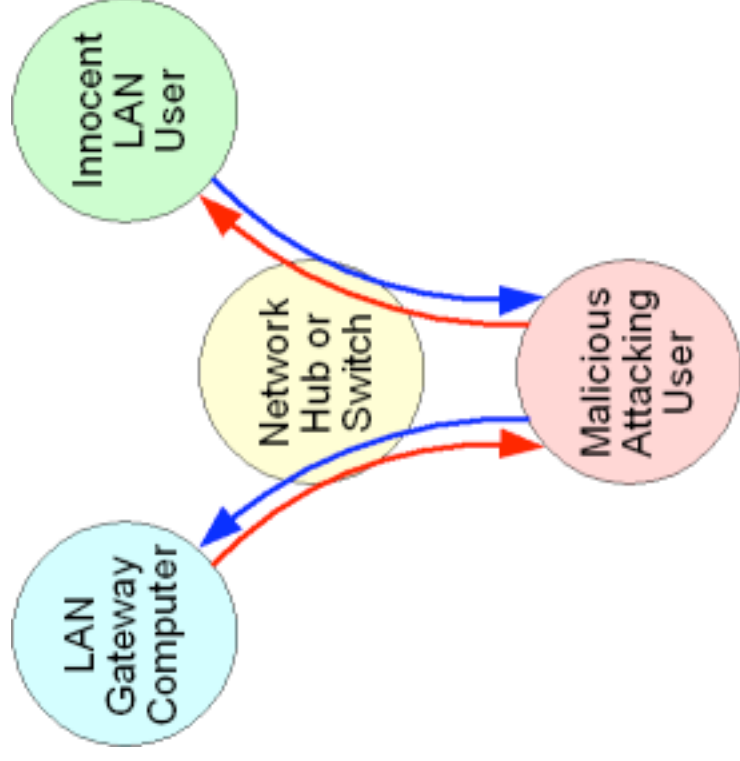
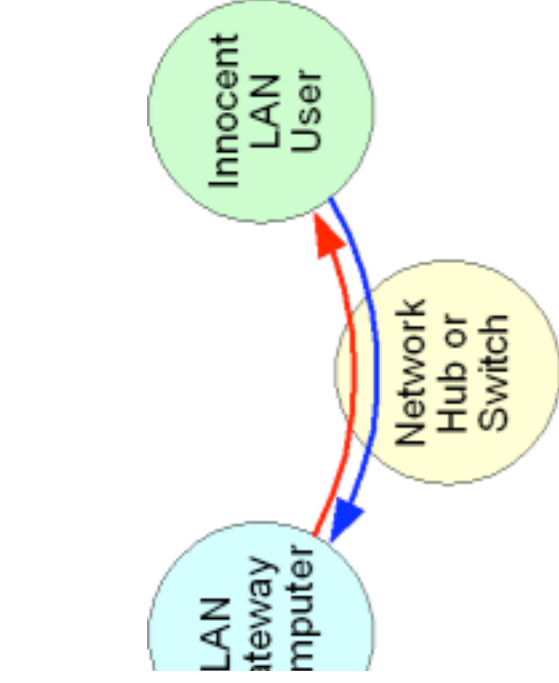


# Bad Guys

- **Man-in-the-middle = Enemy hacker listens & can modify, delete, & replay messages**
- **Evil Twin = a rogue Wi-Fi access point that poses as legitimate.**
- **Key logger = malware that sends out what you type**

# Man-in-the-Middle

From Steve Gibson: <http://www.grc.com/nat/arp.htm>



Normally computers on the LAN use the ARP protocol to acquire and store in their ARP tables the IP addresses and MAC addresses of each other's NICs. This process allows them to use for routing network data to each other.

This "ARP Cache Poisoning" can be used to redirect traffic throughout the LAN, allowing any malicious computer to insert itself into the communication stream between any other computers for the purpose of monitoring and even alter the data flowing across the LAN.

# Sniffer Ads

“Ettercap” is a suite for man in the middle attacks on LANs. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols (even ciphered ones) and includes many feature for network and host analysis.” Check out the Ettercap screen shots showing, among other things, it capturing eMail passwords passing over a LAN.

“The latest version of “Cain and Able” is faster and contains a lot of new features like APR (Arp Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. The sniffer in this version can also analyze encrypted protocols such as SSH-1 and HTTPS, and contains filters to capture credentials from a wide range of authentication mechanisms.”

Only if your computer's network traffic is securely encrypted through the use of some sort of virtual private network or other encrypted tunneling technology would our use of public LANs be immune from exploitation of ARP cache poisoning.




# Secure Socket Layer (SSL)

This is how you talk to your Bank

- Encrypts communication with the Bank
- Authenticates the server (e.g. the Bank) using Digital Certificates





### Secure Connection Failed

ocwalk.kintera.org uses an **invalid security certificate.**

The certificate is only valid for www.kintera.org  
(Error code: ssl\_error\_bad\_cert\_domain)

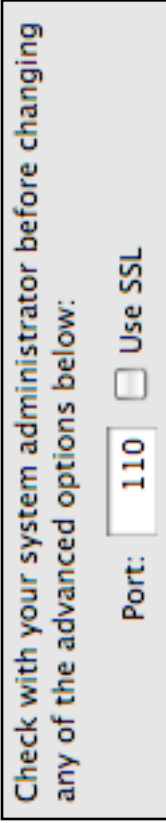
- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be

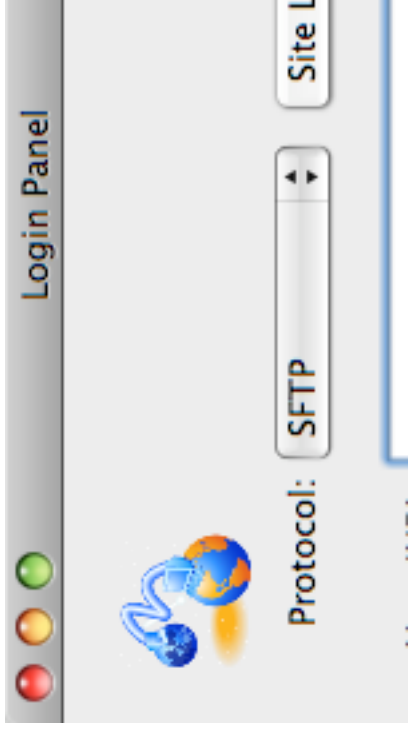
# Secure Socket Layer (SSL)



- A protocol to secure communication using encryption
- A type of “Public Key Encryption”
- Used by banks & big companies
- See **https** in the address
- Traffic is encrypted - bad guys locked out

# Beyond the web

- Email
- Gmail   Always use https  
 Don't always use https
- Apple Mail   Use SSL  
Port:
- PGP program encrypts mail
- Skype Uses encryption to protect Skype users
- SFTP - Secure File Transfer Protocol

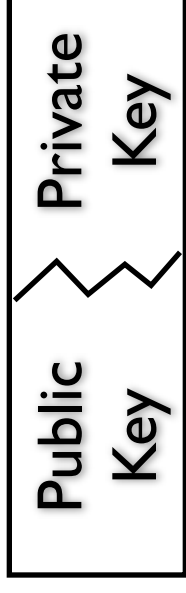


# How Public Key Encryption works

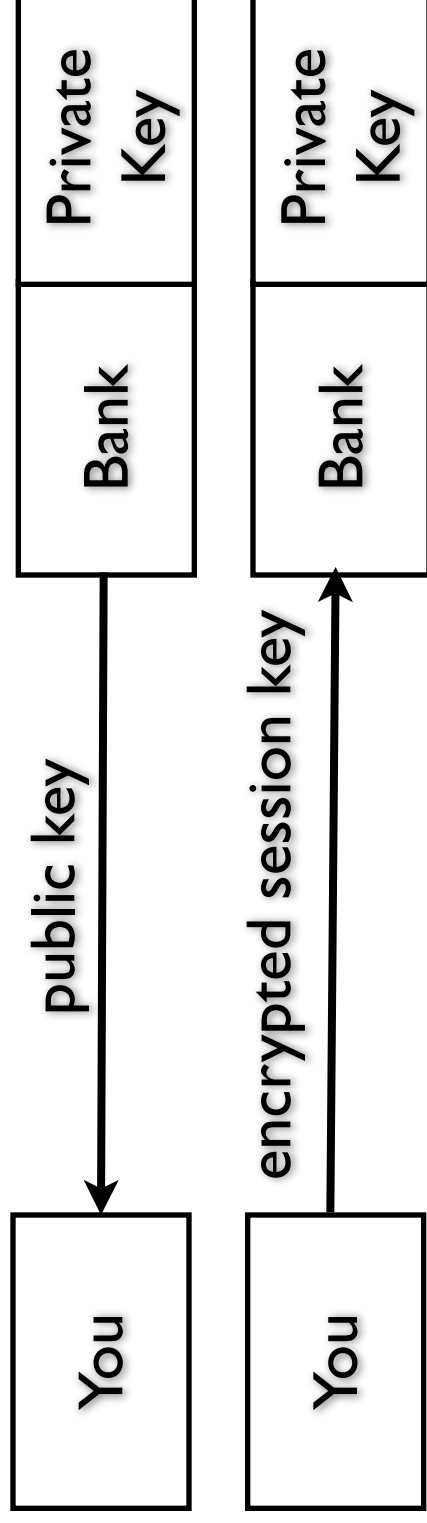
- Uses a random “session” key to encrypt communications
- Only you & the bank possess it
- Distribution?

# Public Key Cryptography

- Bank has another pair of keys
- Mathematically entwined
- Public key is broadcast
- Private key is secret



# Public Key Cryptography



- Bank sends the public key
- Your browser generates a “session key”
- Encrypt it with the public key
- Send it back to the bank

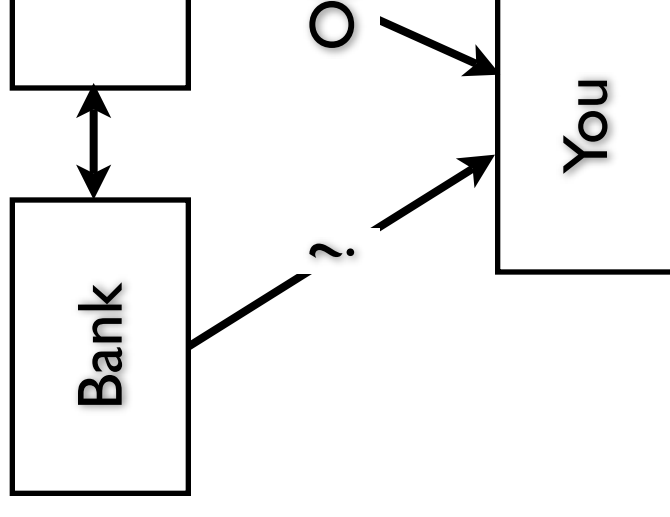
# Public Key Cryptography

- Bank decrypts it using its private key
- Now you and bank have the session key
- An evesdropper can't get it

# Digital Certificate

issued by the Bank & verified by a trusted CA (certificate authority)

- Verifies a web site is who they say
- Bank sends a certificate
- Verified by a CA in a “web of trust”

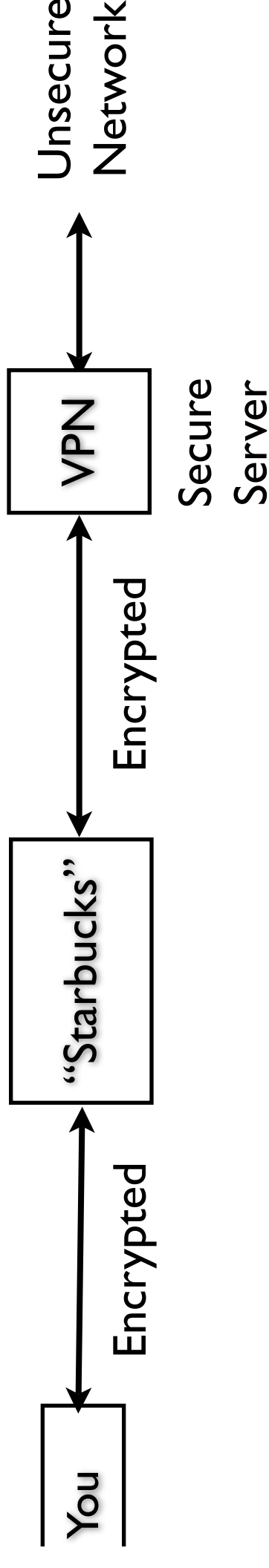


Verisign is the CA



# Virtual Private Networks (VPN)

For communicating with unsecured networks  
A secure intermediary



# Little Snitch

Alert: when applications want to phone out

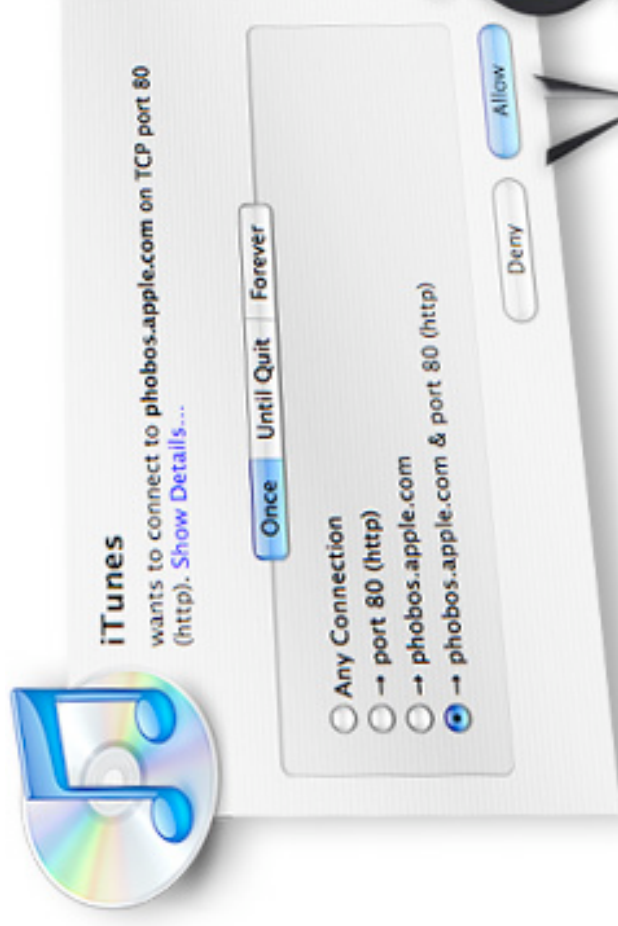
rewall blocks intruders

pps can phone out

ttle Snitch tells you

's usually benign:

g. software update



## Little Snitch 2

Protect your privacy.

# Simple Security Tips

from LowEndMac, Aug 13, 2008

- Turn on firewalls
- Use good passwords - don't reuse
- Careful what you download
- Be sure it's <https>: on sensitive sites
- Verify a public networks before using