Bob Brooks, 8-27-08

Is Starbucks Safe?

Network Security
Wireless in particular

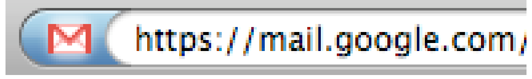
Caveat

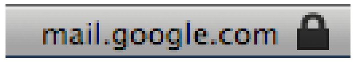
- I’m not an expert
- I’ll share what I know
- A basis for discussion

Bob Brooks, 8-27-08

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


https://mail.google.com/

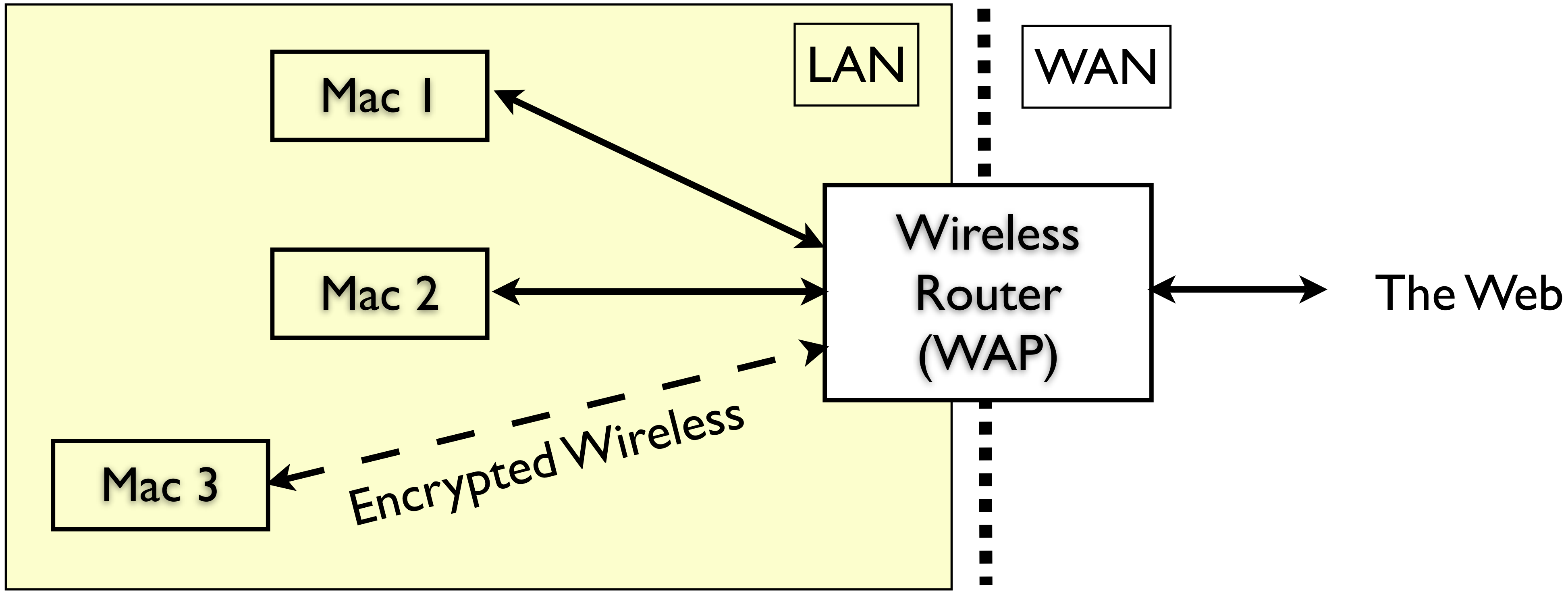

mail.google.com 🔒

- VPN = Virtual Private Network

Bob Brooks, 8-27-08

Home Network (LAN)

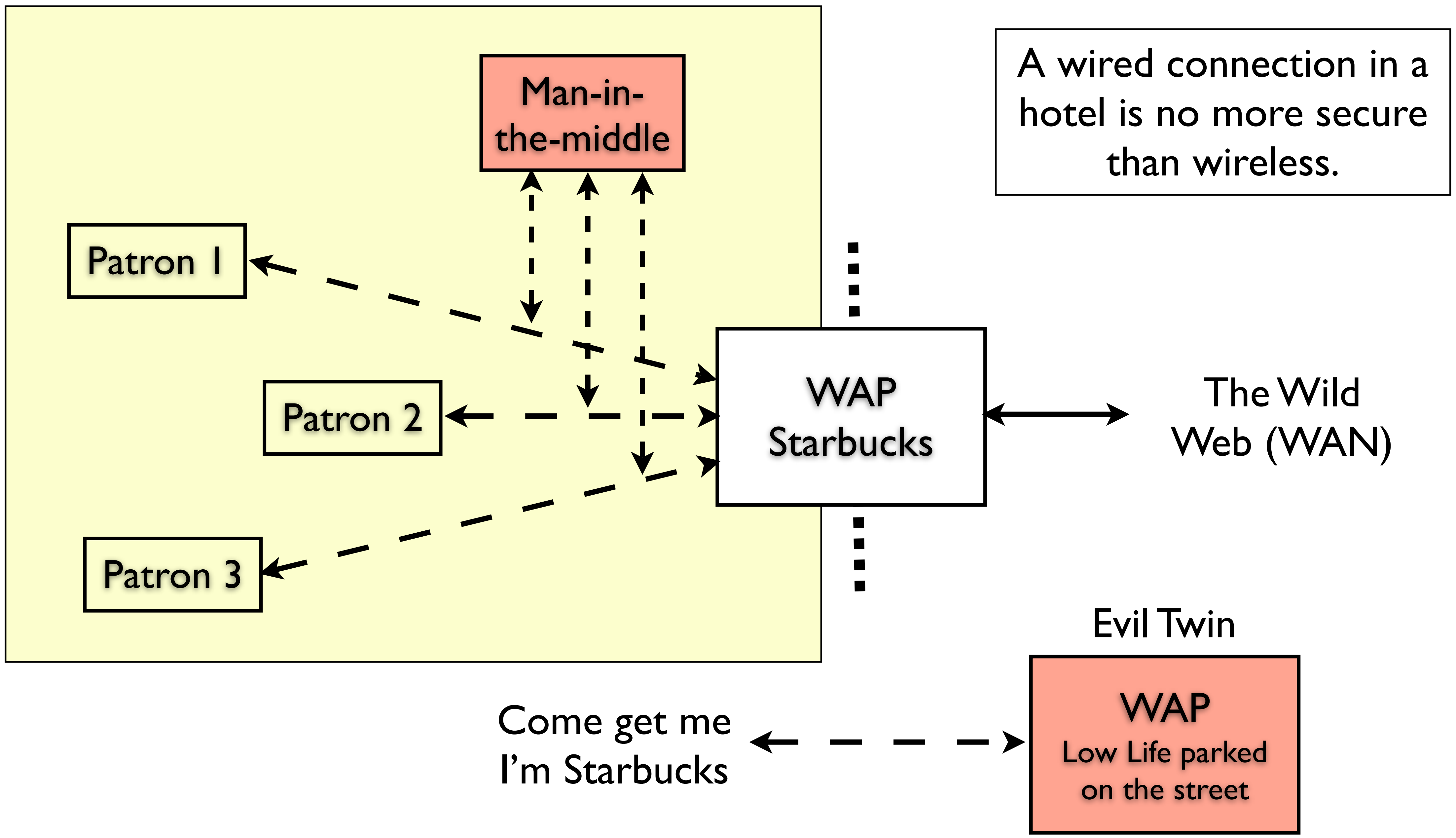
A router connects two networks together
Usually a local network to the Internet



Firewall
Hides your LAN
from the WAN

Bob Brooks, 8-27-08

Starbucks = public LAN



A wired connection in a hotel is no more secure than wireless.

Bob Brooks, 8-27-08

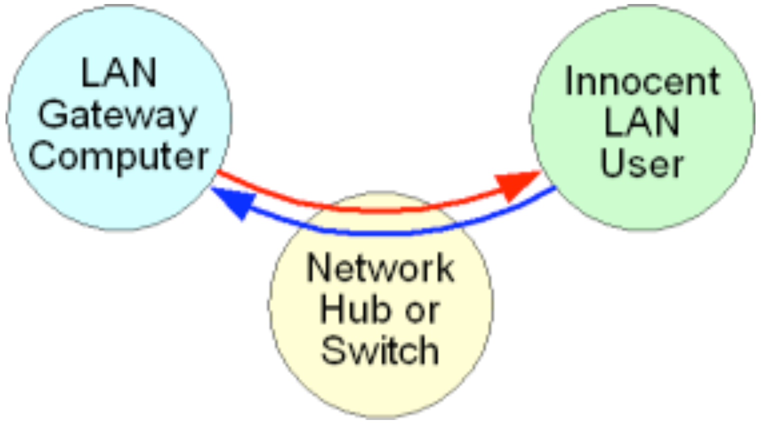
Bad Guys

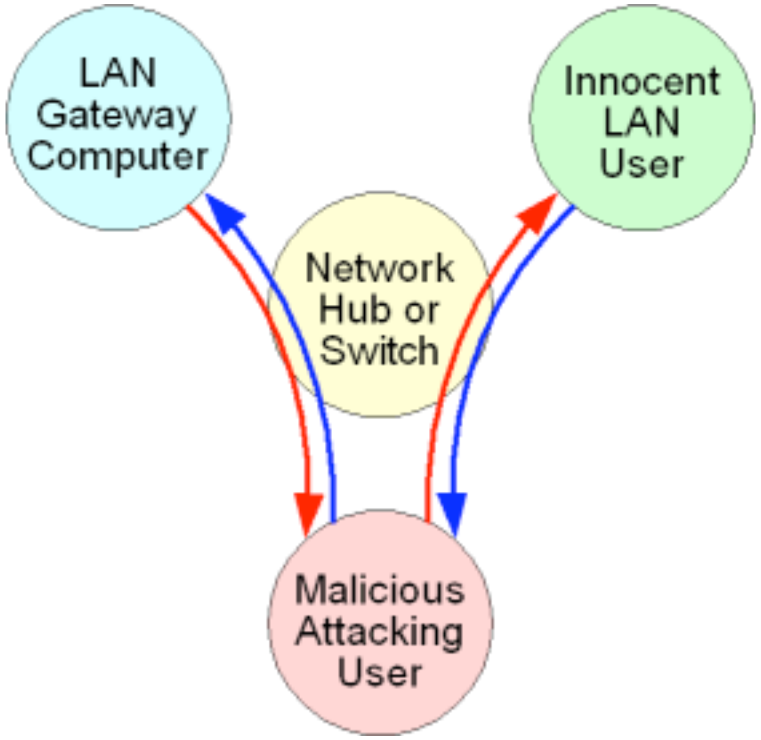
- Man-in-the-middle = Enemy hacker listens & can modify, delete, & replay messages
- Evil Twin = a rogue Wi-Fi access point that poses as legitimate.
- Key logger = malware that sends out what you type

Bob Brooks, 8-27-08

Man-in-the-Middle

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





Normally computers on the LAN use ARP protocol to acquire and memorize each other's NIC MAC address which they use for sending 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 communications stream between any other computers for the purpose of monitoring and even alter the data flowing across the LAN.

Bob Brooks, 8-27-08

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.

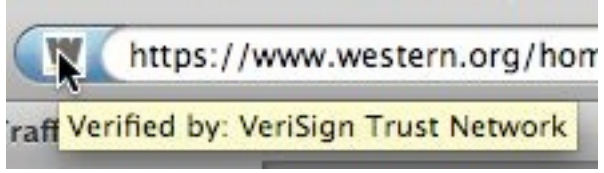
"The latest version of “Cain and Able” is faster and contains a lot of new features like APR (Arp Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. The sniffer in this version can also analyze encrypted protocols such as SSH-1 and HTTPS, and contains filters to capture 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 your use of public LANs be immune from exploitation of ARP cache poisoning.

Secure Socket Layer (SSL)

This is how you talk to your Bank

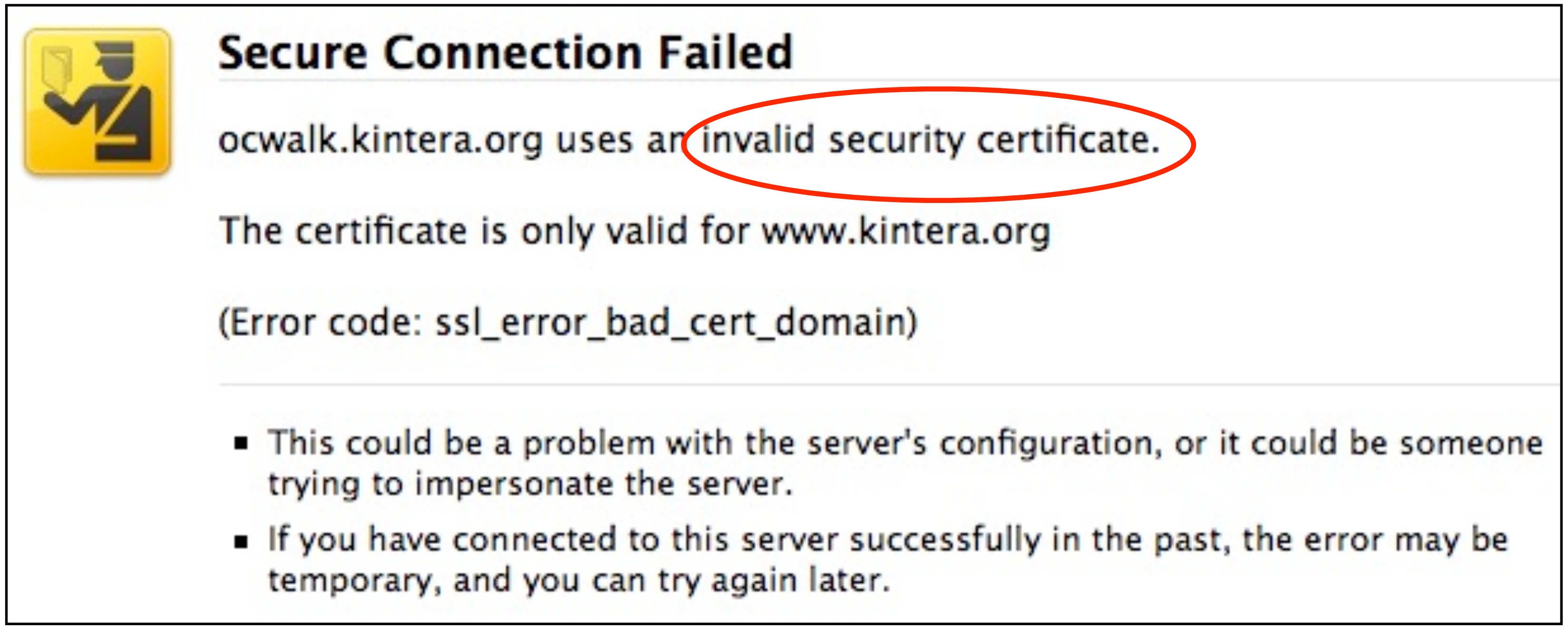
- Encrypts communication with the Bank
- Authenticates the server (e.g. the Bank) using Digital Certificates



https://www.western.org/hon

Verified by: VeriSign Trust Network

Yes



Secure Connection Failed

ocwalk.kintera.org uses an invalid security certificate.

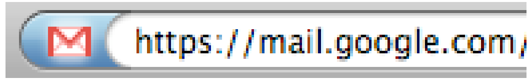
The certificate is only valid for www.kintera.org

(Error code: ssl_error_bad_cert_domain)

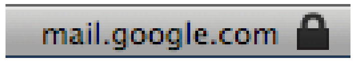
- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

No

Secure Socket Layer (SSL)



https://mail.google.com/

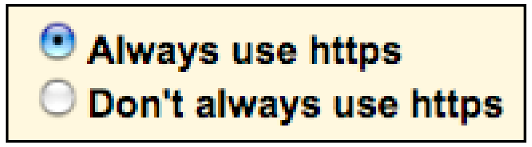


mail.google.com

- 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

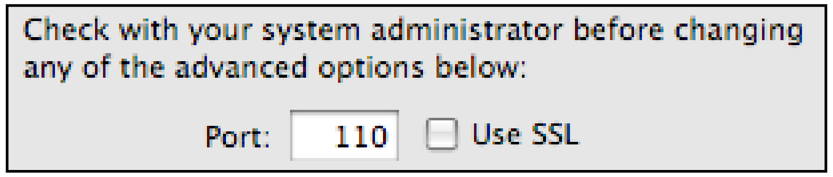
Beyond the web

- Email
  - Gmail



● Always use https
○ Don't always use https

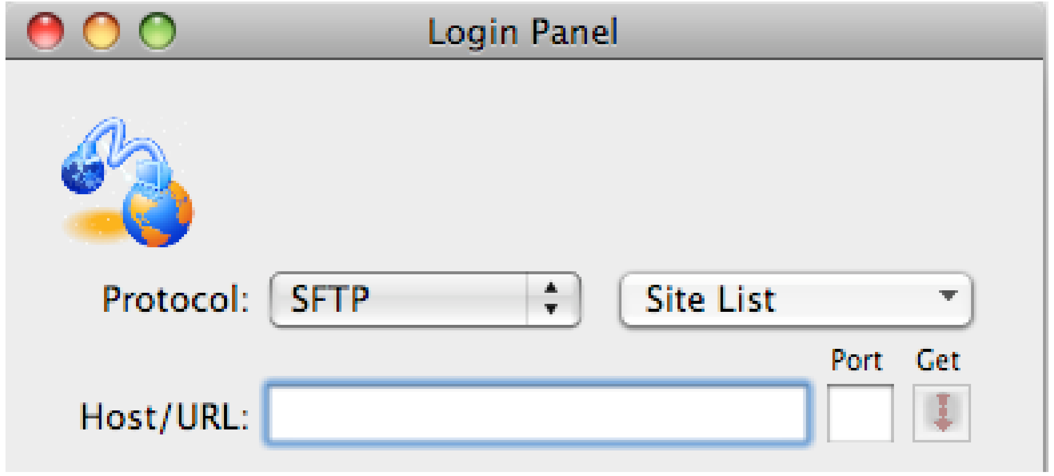
  - Apple Mail



Check with your system administrator before changing any of the advanced options below:

Port: 110 □ Use SSL

  - PGP program encrypts mail
- Skype Uses encryption to protect Skype users
- SFTP - Secure File Transfer Protocol



Login Panel

Protocol: SFTP

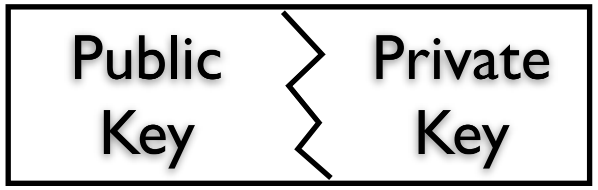
Host/URL:

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

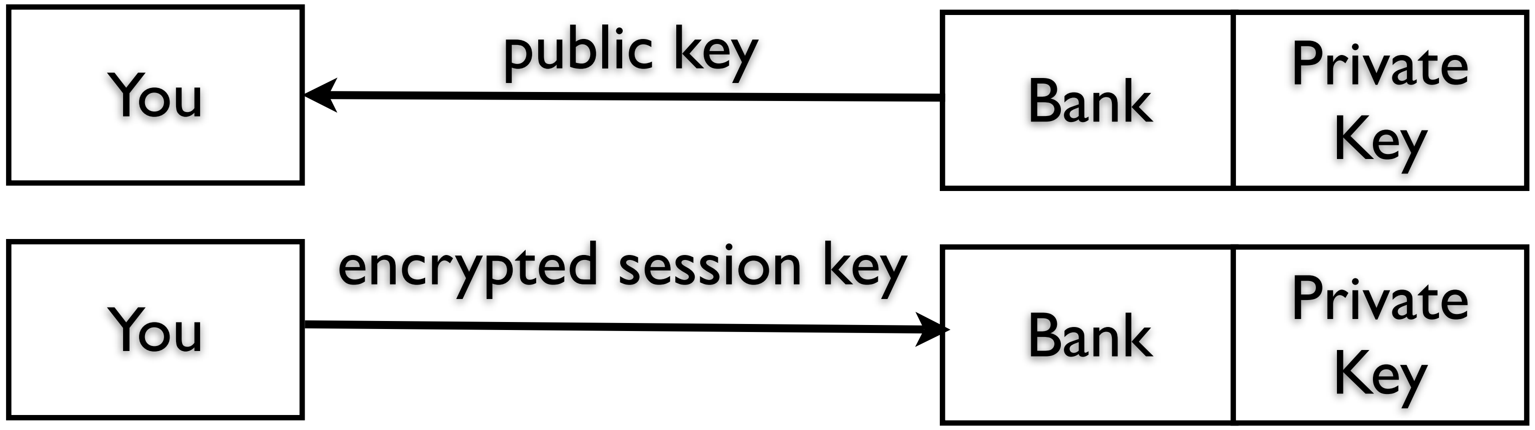


Public Key

Private Key

Bob Brooks, 8-27-08

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

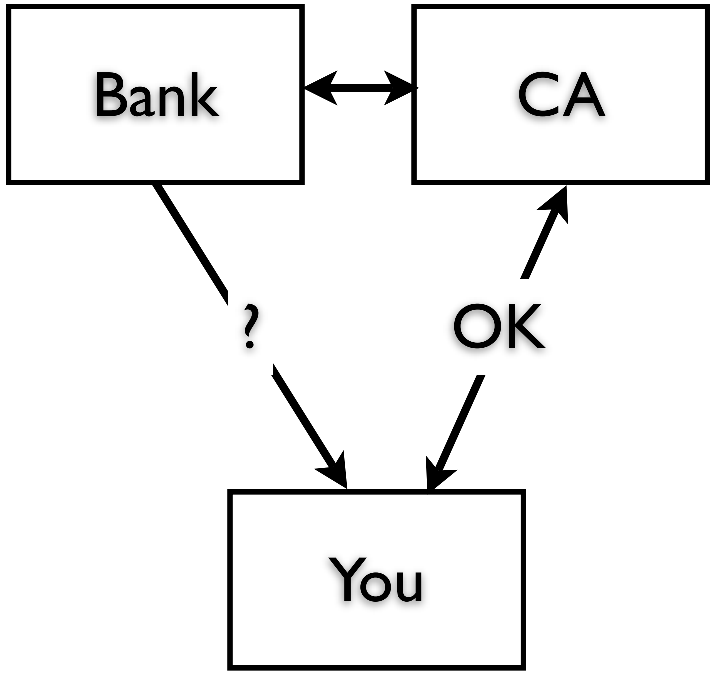
Public Key Cryptography

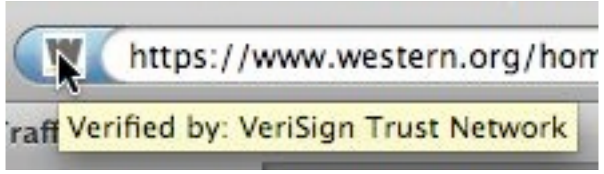
- Bank decrypts it using it’s private key
- Now you and bank have the session key
- An evesdropper can’t get it

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"





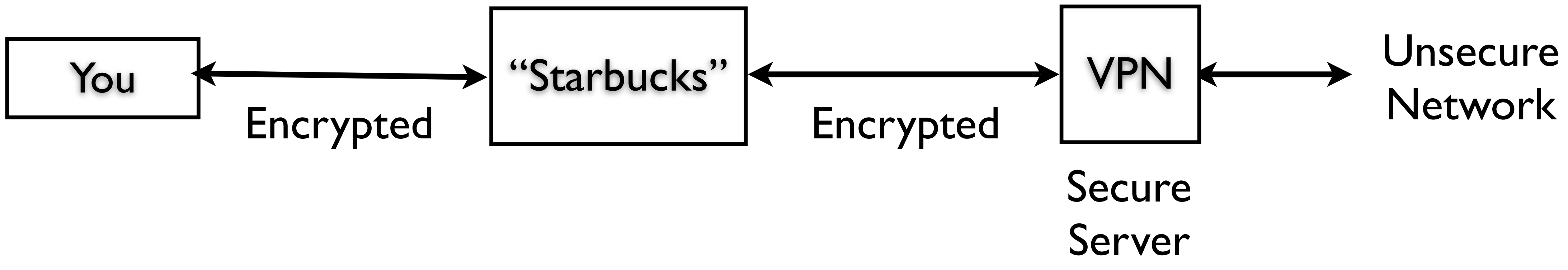
Verified by: VeriSign Trust Network

Verisign is the CA

Bob Brooks, 8-27-08

Virtual Private Networks (VPN)

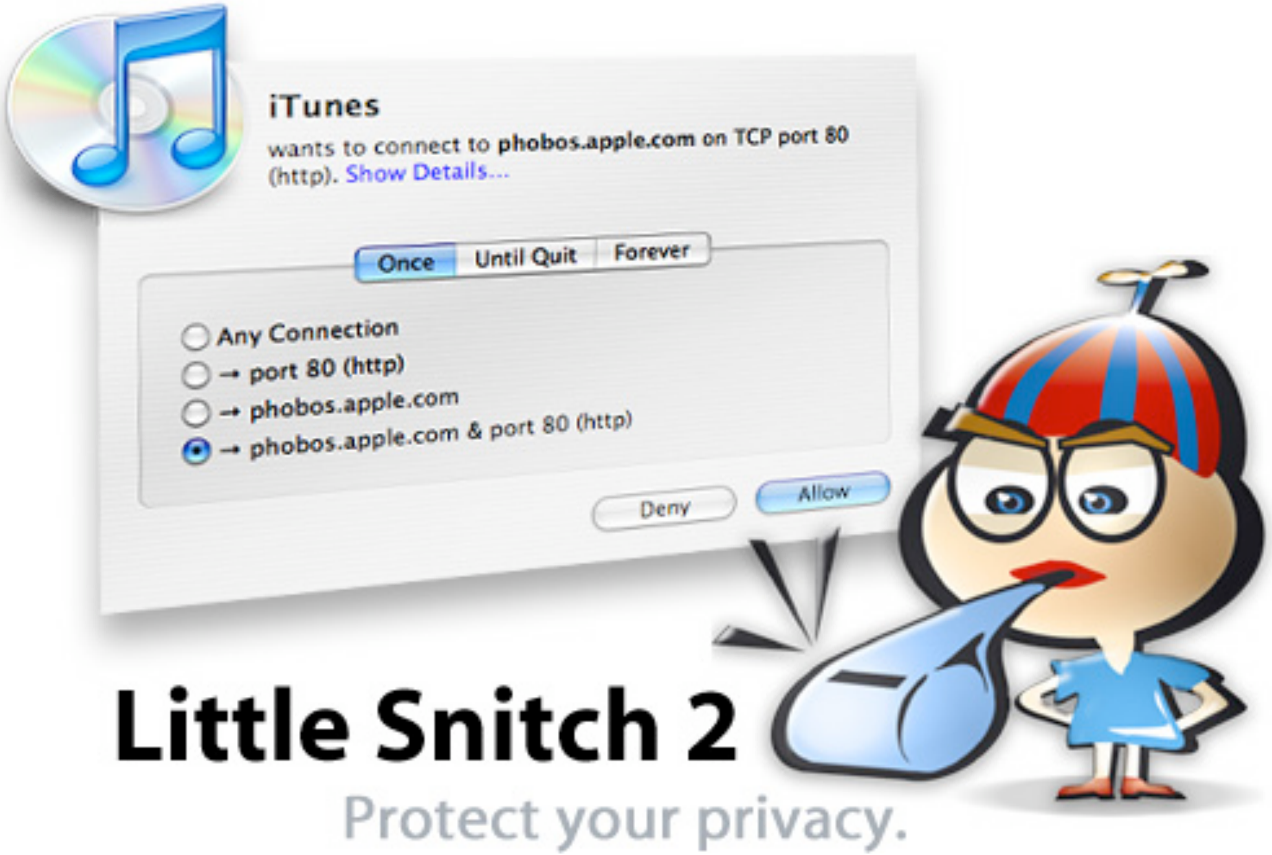
For communicating with unsecured networks
A secure intermediary



Little Snitch

Alert: when applications want to phone out

- Firewall blocks intruders
- Apps can phone out
- Little Snitch tells you
- It’s usually benign:
  e.g. software update



iTunes

wants to connect to **phobos.apple.com** on TCP port 80 (http). Show Details...

[✓ Once] Until Quit Forever

○ Any Connection
○ → port 80 (http)
○ → phobos.apple.com
● → phobos.apple.com & port 80 (http)

Little Snitch 2

Protect your privacy.

Bob Brooks, 8-27-08

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