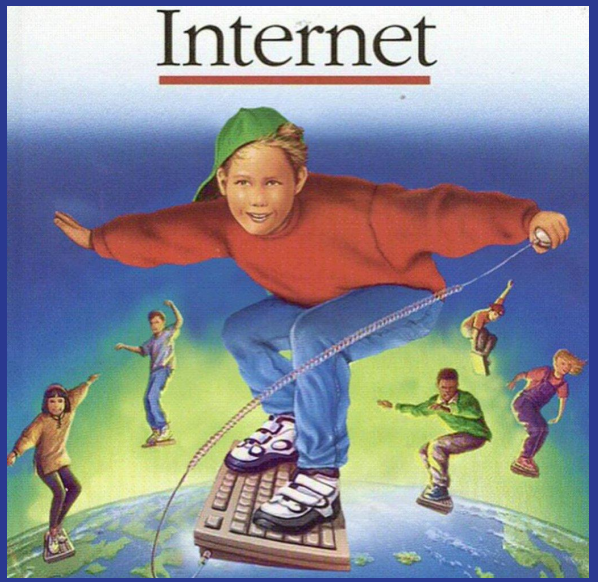
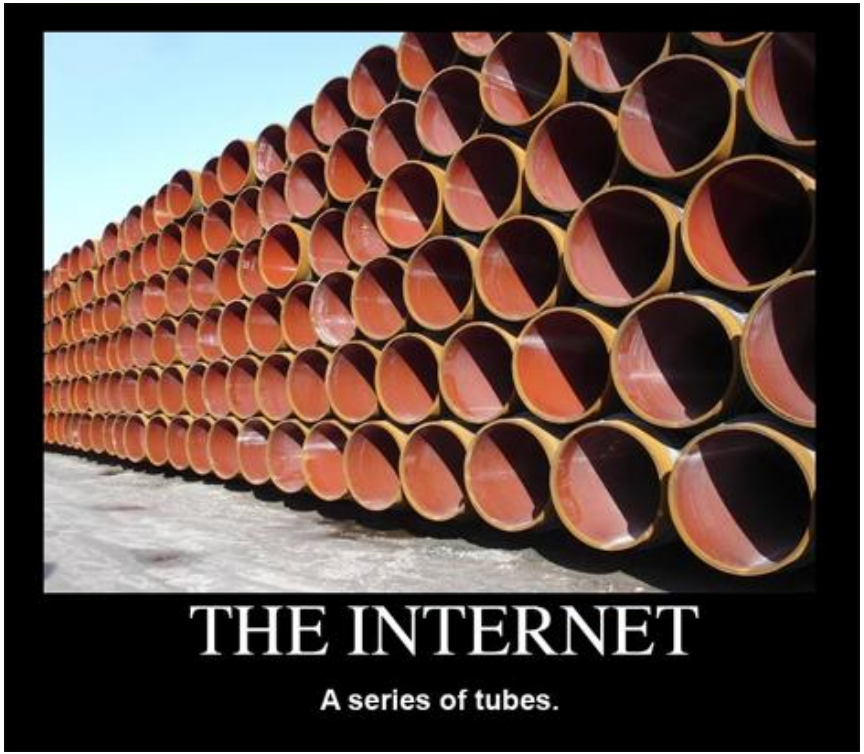
Secretly Surf Cyber-space



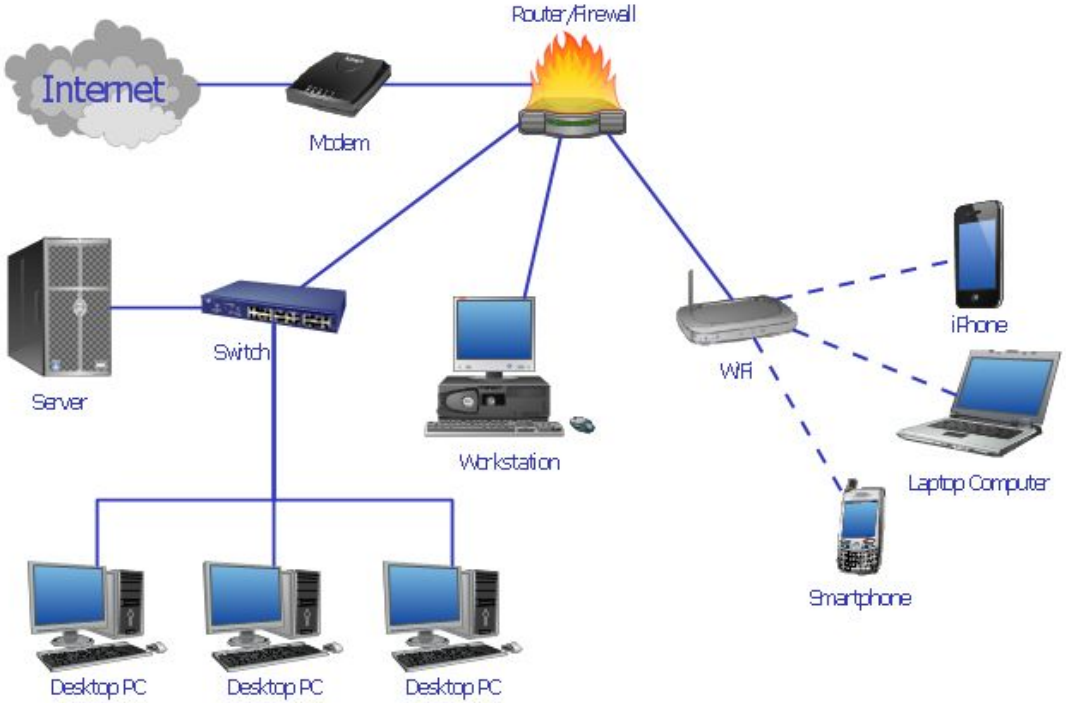
VP, Grey Hat UH Manoa

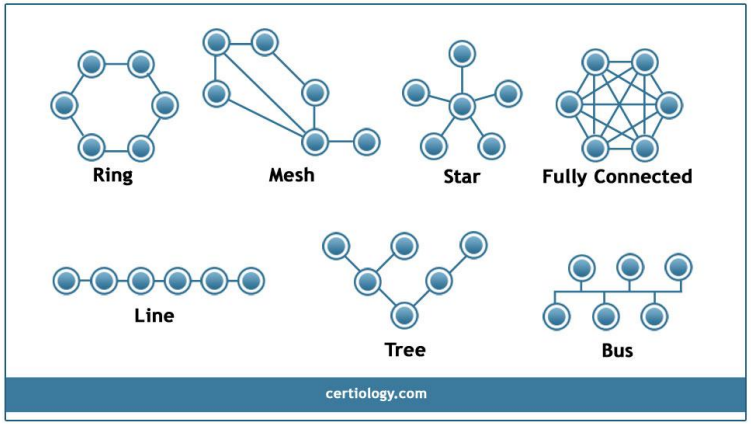
What is the Internet?



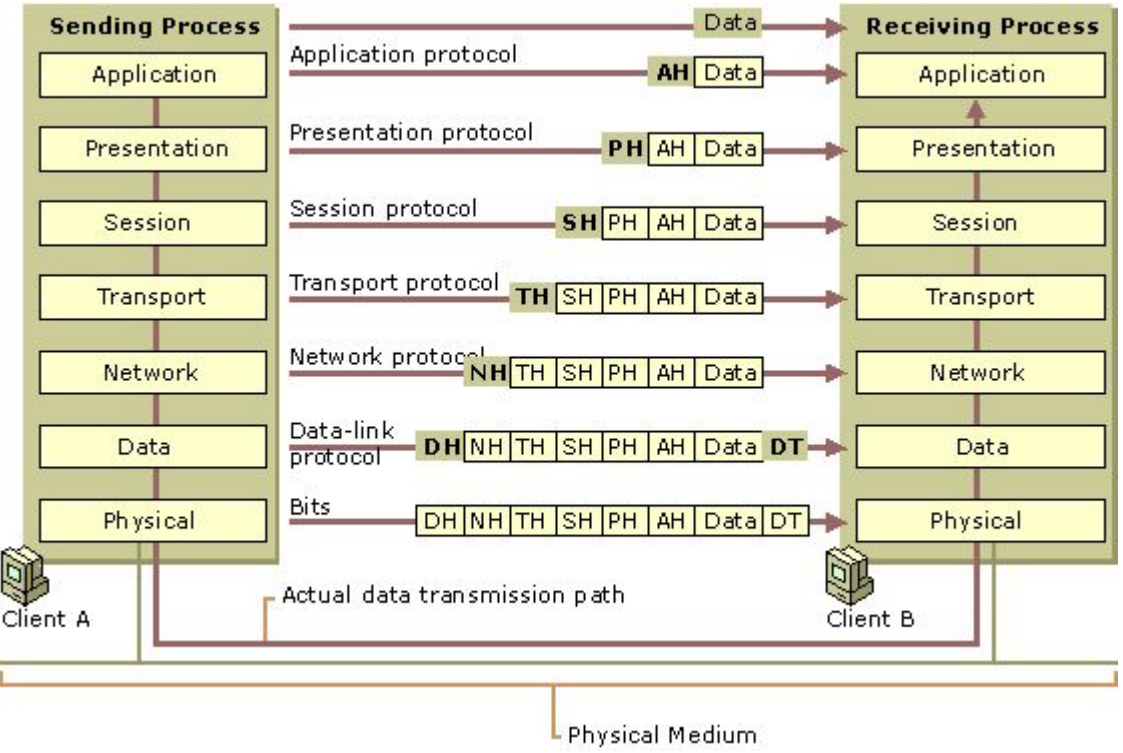
- In short, it’s a collection of tubes
- Two computers can make a two node network
- All computers can’t be connected
- Magic comes from devices connected to tubes able to route information
- World Wide Web is what we know as ‘the internet’
- Large organizations have intra-nets

How it looks


Router/Firewall
Internet
Modem
Server
Switch
Workstation
WiFi
iPhone
Laptop Computer
Smartphone
Desktop PC
Desktop PC
Desktop PC

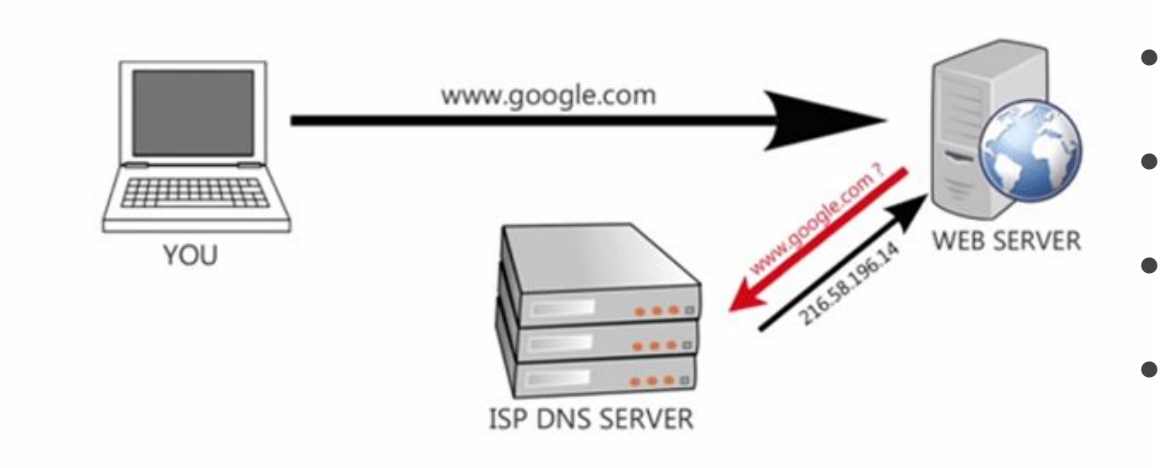

Ring
Mesh
Star
Fully Connected
Line
Tree
Bus
certiology.com

Layer Models



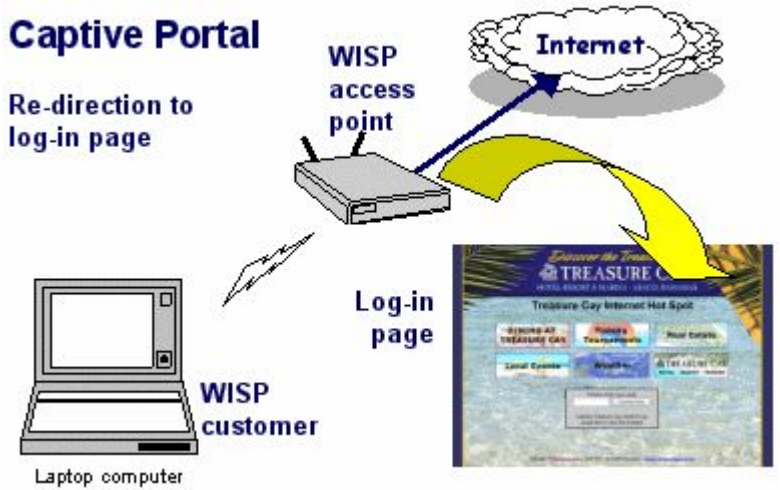
		OSI Model	Examples
Data	7	**Application Layer** Facilitates communiation between software applications like Outlook, IE	Web Application
Data	6	**Presentation Layer** Data representation and encryption	HTTP
Data	5	**Session Layer** Interhost communication	80
Segments	4	**Transport Layer** End to end connection and reliability	Transmission Control Protocol (TCP)
Packets	3	**Network Layer** Path determination and logical addressing	Internet Protocol (IP)
Frames	2	**Data Link Layer** Mac and LLC - Physical addressing	Ethernet
Bits	1	**Physical Layer** Media, signal and binary transmission	CAT5

Domain Name Server



- Computers use IP addresses, not URI/URL
- How to get 14.187.5.1 from www.porcupines.com
- Recursive i.e. if a device doesn't know, it'll ask the next highest up
- Rogue DNS could say facebook.com is 192.168.0.5 (i.e. my laptop)
- Https prevents this (out of scope)

Captive Portals



- Most paid internet uses captive portals
- Redirects DNS and HTTP to their server, which serves their page
- Can’t access get through to wide internet till authenticated
- Mostly uses MAC address since it doesn’t change
- What UH uses

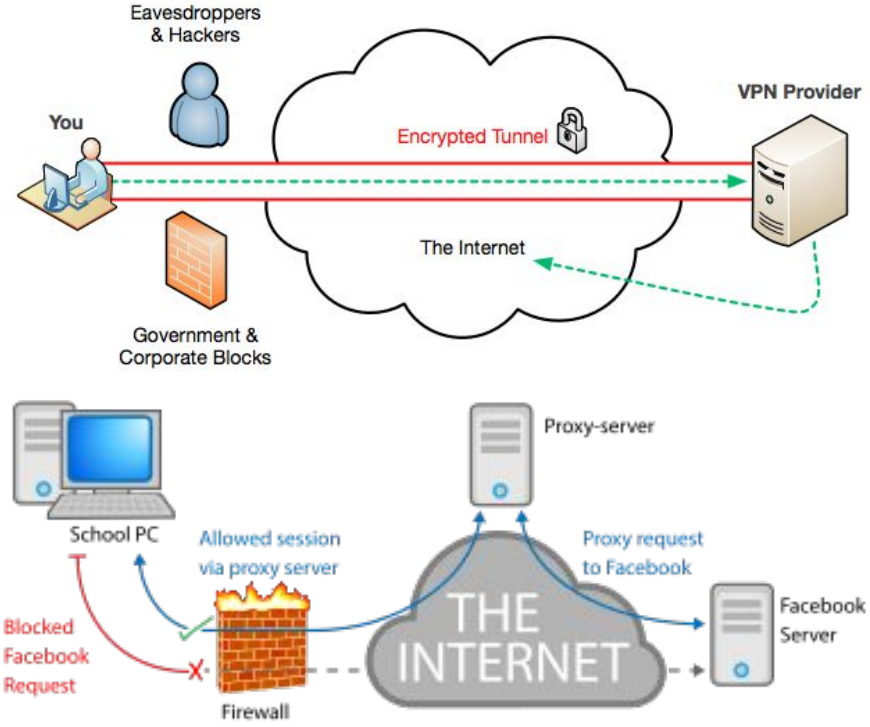
Disclaimer

- Doing these things can get you in trouble
- I’ve never done this, but heard it from a friend
- Ethical argument can be used i.e. all information should be readily available, but don’t bet on it
- Unauthorized usage violates ToS
- Network might count as property
- Unauthorized access is like ‘trespassing’
- But it’s cyber so everyone is 10x afraid

Manually Change Setting

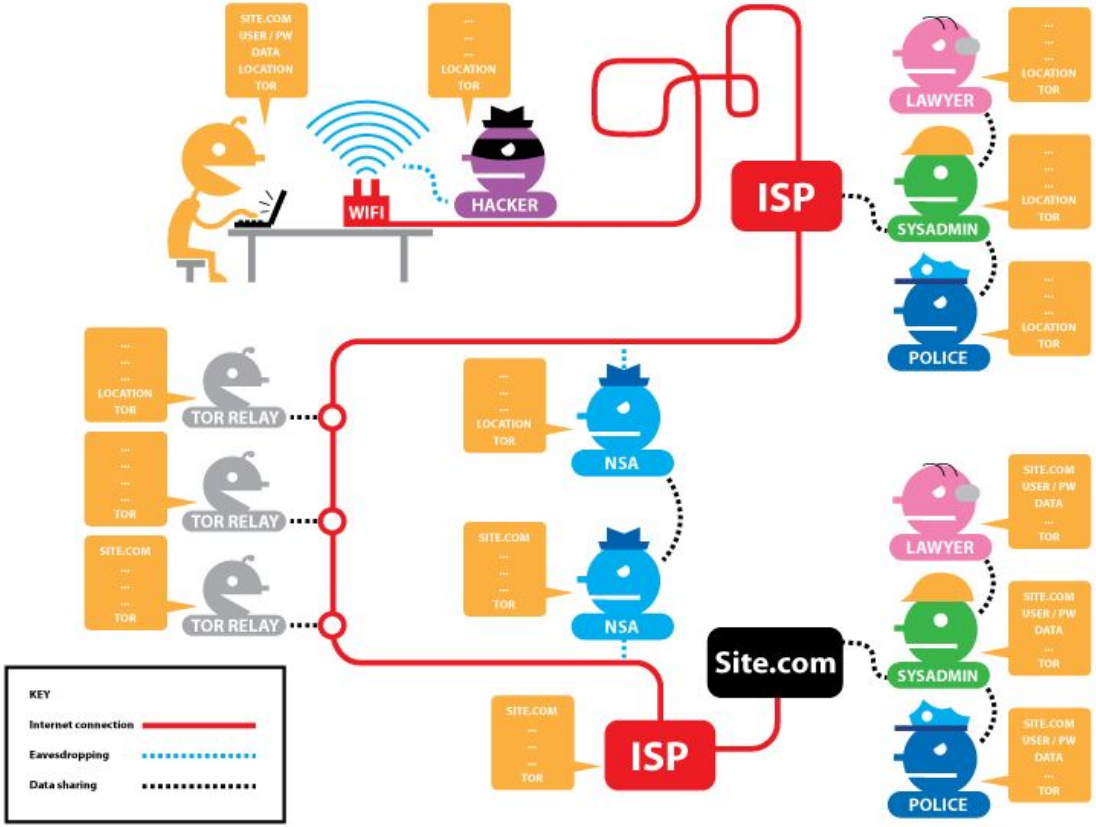
- DNS server set by DHCP request
- Just change DNS server 8.8.8.8
- Spoof MAC address
- ‘Baked’ into the silicone
- Read by software, then broadcast
- Just tell software to read something else
- Able to use arp-scan or wireshark
- Might use the ‘wrong’ MAC address
- “Why is the register making a http request to porcupines.com?”

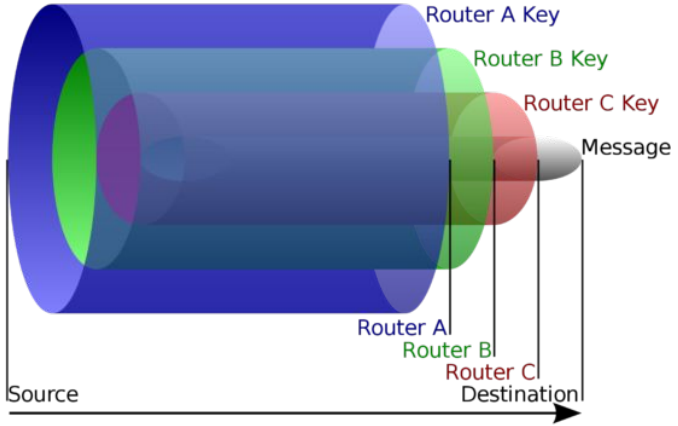
Secure Tunneling



- Also known as VPN
- Not the same as a proxy
- Not all proxies are VPNs, but all VPNs can be considered proxies
- Not bypassing firewall, tunneling through it
- Changes destination information
- Hides actual packet data

Tor Onion Network

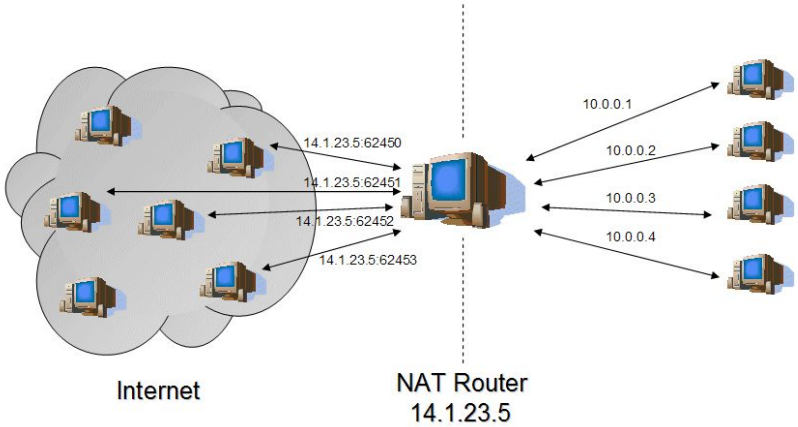




Paid/Free Proxy options

- Paid option: tunnel bear
- Free options available, DDG: ‘! free web proxy’
- Node sees all your traffic
- Always use with a grain of salt
- Best for media consumption to bypass location restrictions
- Again, might be legal where you are, but destination might say otherwise

Self Hosted



- Edge device needs to allows incoming traffic
- Able to use cloud hosting
- Tunneling to home hides traffic, but ISP still able to see
- Best when using public wifi
- Need cloud solution to ‘change location’
- OpenVPN for basic setup
- ICMP tunneling is the same concept
- Web doesn’t run on ICMP, proxy server ‘translates’ it to HTTP, etc.

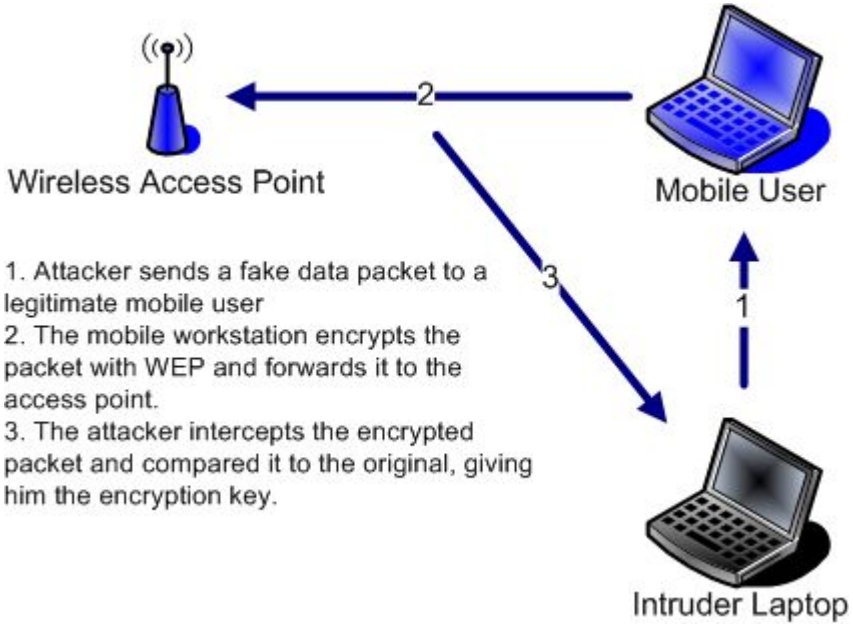
Detour: Deep web

- Deep web: anything not indexed by a search engine
- Your facebook login page is the deep web
- Able to find some stuff by ‘dorking’
- Google ‘targersite.com inurl:admin’
- Dark web is a park of the deep web
- Has bad stuff: drugs, porn (the bad stuff)
- Might only be able to access using a certain ‘network’
- Onion links is a well known example
- ‘Red Room’ game covers similar topics

Cracking Wifi

- Disclaimer: Can be considered ‘burglary’ since network is secure and forced way in
- Wanted to set up network and show in action but…
- WEP: Wired Equivalent Privacy is broken, don’t use it
- WPA2: Wi-Fi Protected Access 2, a lot better, but depends on password used

Cracking Wifi 2



- WEP is broken
- Might at well be open access point
- Able to crack in under 5 mins
- Did I say it sucks?
- <- check it

Cracking Wifi 3

- WPA2 is best
- Different from WPA in cryptographic algorithm used
- PSK: pre-shared key
- RADIUS: checks central server for access after some kind of authentication, biometric, user/pass, etc.
- Only as strong as password used
- Hawaiian Tel uses 10 digit number
- Tl;dr: deauth client(s), capture ‘handshake’, crack password

Dial-up

- Need telephone connection
- Land line isn’t free, but may be bundled with other services
- Major cell carriers provide unlimited minutes
- Did I mention it’s slow?
- Dial up often measured is kB per/sec
- Some cell carriers limit to 9600 baud i.e. bits per/sec
- Tl;dr: have computer connect to phone and use as modem

Wrapping Up

- Internet runs on hardware
- Software is free, but hardware isn't free
- Free isn't always best
- Be careful overseas; VPNs are illegal in China
- Proxies aren't bad, but bad people use them
- Bad people caught because they always used proxies
- If everyone uses them, then not automatically bad

Extra

VPNs
digitalocean.com/community/tags/vpn?type=tutorials
github.com/jlund/streisand

Wifi cracking
lmgtfy.com/?q=wifi cracking

Onion Links
lmgtfy.com/?q=onion%20links

How Tor users were caught
youtu.be/TQ2bk9kMneI
youtu.be/7G1LjQSYM5Q

Dorking (I contributed! :^D)
github.com/enaqx/awesome-pentest#osint-tools