Security

Keeping Them Out

Almost all networks are extremely vulnerable

Bruce Schneier

(he’s right)

General Concepts

What should we expect, and whats our role?

Who are we keeping out?

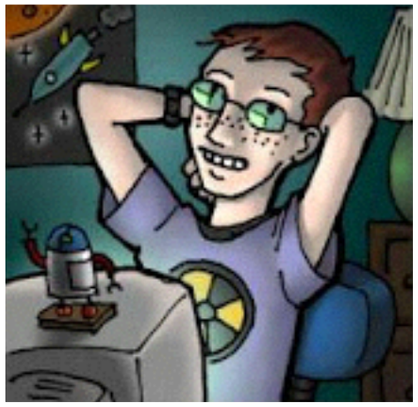
Automated Threats

Easy to Predict

Not Sophisticated

Easy to Block

Low Level Data Threat



Script Kiddies

Easy to Predict; Not Creative

Depends on Tools

Easy to Block

Medium Level Data Threat

Targeted Attacks

Hard to Predict

Range of Sophistication

~

High Level Data Threat

NSA Level Threat

Impossible to Predict

Incredibly Sophisticated

Impossible to Block

~

Known vs Unknown

Known

Most anti-threat systems work on the known (signatures, known heuristics)

Unknown

Unknown harder to protect against, and requires a different level of paranoia

Policy

- Removes the human element
- Creates a security checklist
- Ensures easy, secure provision of devices

Trust is built with consistency.
Lincoln Chafee

Our Role

Post Intrusion

- Preserving Data
- Removing Threats
- Securing Holes

Prevention

- Analyze Weaknesses
- Setup Safeguards
- Educate Users

Ongoing

- Keep Abreast of News
- Monitor Logs
- Software Upgrades

Keep In Mind

Clients are often willing to pay more for security expenses - news markets for us

It’s our job to make security as easy as we can

Attackers take the easiest route

Assume nothing is secure

Low Hanging Fruit

- Software Updates
  - 10.8+ includes ASLR, NX

    (10.6+ kinda does)
- Passwords
  - Use 2factor
- Uninstall Flash & Reader
- Consider Managed Services
- Network Security Appliances
  - Makes network security much easier

The Human Element

- Educate users
- Build systems that are easy to use
  - They're hiring you to be the expert
- They WILL write passwords down
  - Not always bad, but push a password manager

UPPER LAYERS

7 **Application Layer**
✓ Message format, Human-Machine Interfaces

6 **Presentation Layer**
✓ Coding into 1s and 0s; encryption, compression

5 **Session Layer**
✓ Authentication, permissions, session restoration

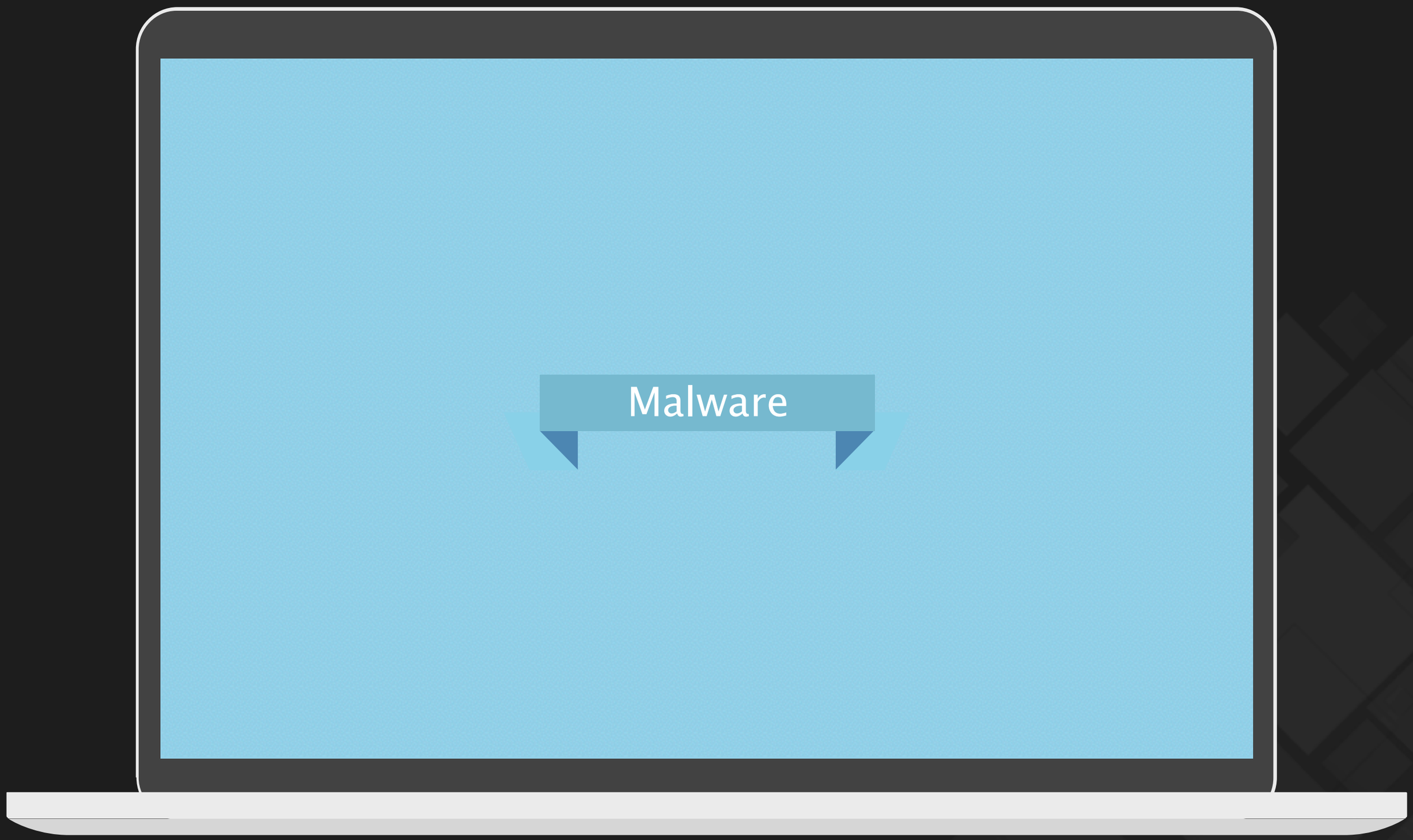
TRANSPORT SERVICE

4 **Transport Layer**
✓ End-to-end error control

3 **Network Layer**
✓ Network addressing; routing or switching

2 **Data Link Layer**
✓ Error detection, flow control on physical link

1 **Physical Layer**
✓ Bit stream: physical medium, method of representing bits


Malware

Malware

Identification and Protection

Identification

- http://www.thesafemac.com/
- Infection Routes
  - Drive by download
  - Pirated Software
  - Infected USB/media

AV

Built In

- xprotect
  - limited scope; known popular malware only
- Gatekeeper

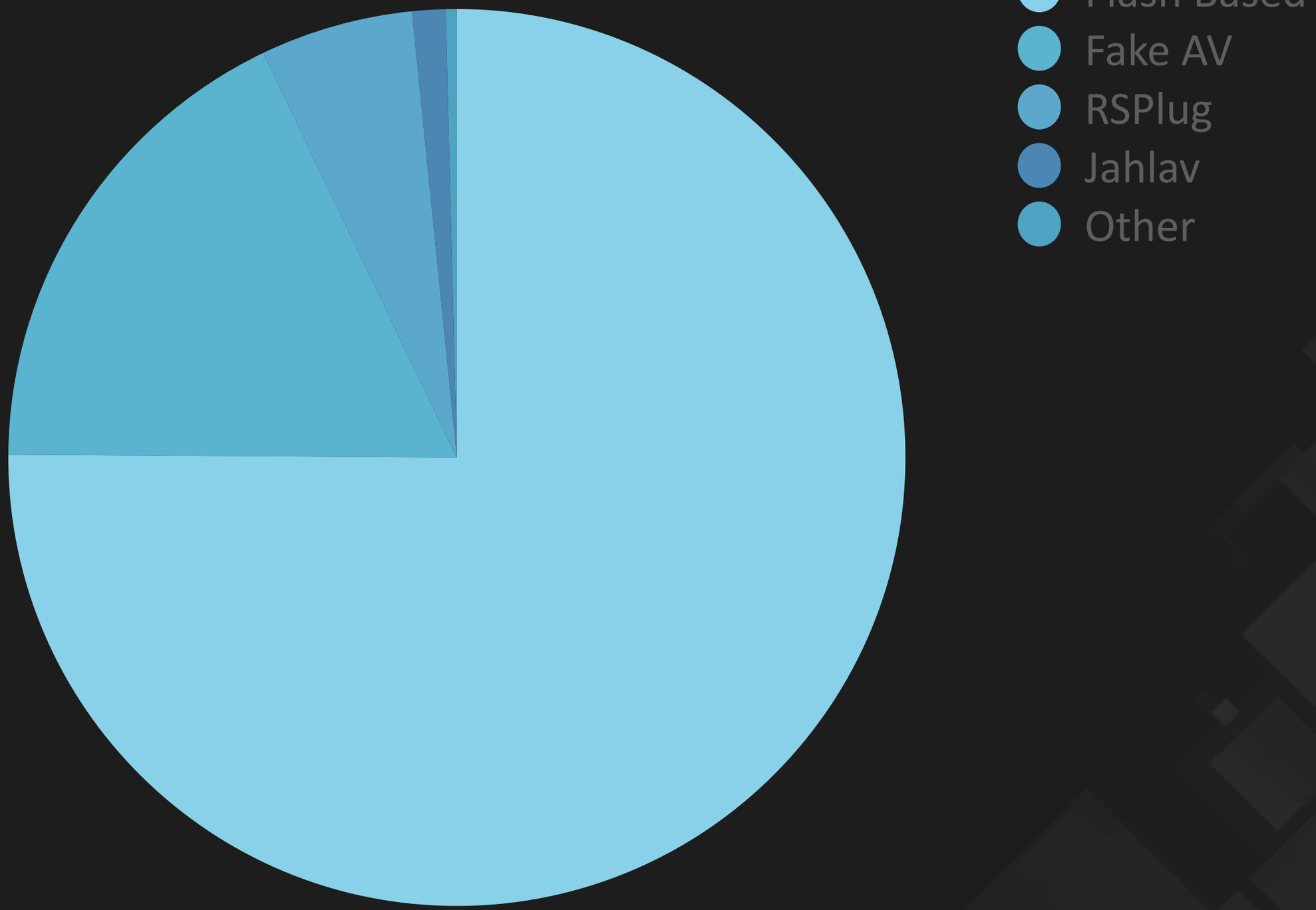
Free

- Clam AV
- Avast
- Sophos

Numerous Paid

1 in 5 Macs Infected

Sophos, 2012

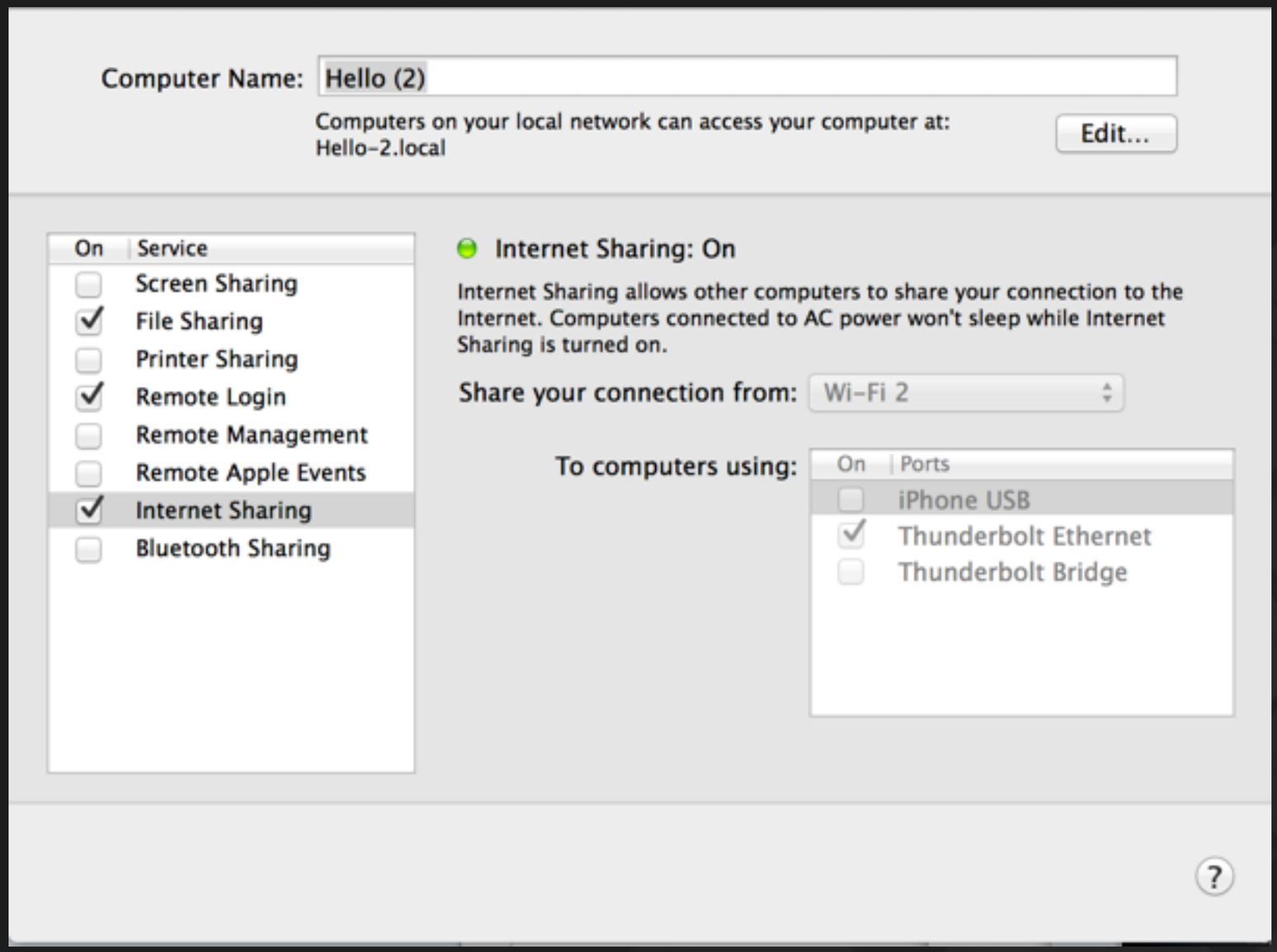


App Whitelisting

- Profile Manager/Parental Controls
  - Limits user to allowed apps
  - Valid on iOS/Mac OS/Android
- Useful for kiosks and extra sensitive environments

Disabling Services & Launch Apps

- Sharing PrefPane
- StartItems



Disabling Services & Launch Apps

/System/Library/LaunchDaemons/

System-wide daemons provided by Mac OS X

/System/Library/LaunchAgents/

Per-user agents provided by Mac OS X.

~/Library/LaunchAgents/

Per-user agents provided by the user.

/Library/LaunchAgents/

Per-user agents provided by the administrator.

/Library/LaunchDaemons/

System-wide daemons provided by the administrator.

Encryption

…and signing too!

Encryption vs Authentication

Encryption

Used to obscure data in a reversible manor

eg:

- FileVault
- Zip Password

Authentication

Used to verify identity and source

eg:

- PGP
- App Signatures
- Certificates

SSL

- Can be stripped
  - Make sure lock is there
  - Certificate Pinning
- Disable broken cyphers
- Force PFS with plugin

Certificate Management

- Built in
  - Mail
  - Apple ID/iMessage
  - Safari (and other browsers)
- You can be your own Certificate Authority!
  - Free with some limits
- Tools
  - GUI: Keychain
  - CLI: OpenSSL

Authentication

- Certificates
  - PKI: Public Key Infrastructure
    http://en.wikipedia.org/wiki/Public_key_infrastructure
    - Centralized
    - Pay $ for privilege to use well-known root certificate
    - Or install your own!
  - PGP
    http://en.wikipedia.org/wiki/Web_of_trust
    - Web of Trust
    - Non-centralized
    - Key signing parties; sign your friends
- Root certificates for major players pre-installed

Checksums

- UUID (v4+ only)
- File Checksums
  - Use SHA2+ (256+ output bits)
  - MD5/SHA-0 broken, SHA1 theoretical
  - CLI utilities or 3rd party GUI

Digital Signatures

- Prevalent
  - Applications
  - Packages
    - GUI: no
    - CLI: spctl

http://krypted.com/mac-os-x/signing-installation-packages/

- Gatekeeper
  - GUI: System Preferences
  - CLI: spctl
    link

Types of Encryption

Symmetric

Shared Key

eg:

Zip Password

Asymmetric

Key Split Into Public & Private

eg:

PGP

Message Encryption on Mac OS X

- Not default in OS X
  - GPG Tools
    - Free; gpgtools.org
    - GUI:
      - GPG For Mail; 10.6 – 10.9
      - GPG Keychain
      - GPG Services
        - Files, signing, verification of keys, etc
  - CLI: gnupg port

Message Encryption on iOS

- Not built in
  - App Store
  - iPGMail
  - Symantec Mobile Encryption
  - oPenGP

Data Encryption on Mac OS X

Folder & Volume Level Encryption

Folder Level

Disk Images

- 128 or 256bit AES
- Created With:
  - Disk Utility
  - Finder
  - CLI
    - diskutil
    - hdiutil
- Legacy FileVault
- 3rd Party (Tao, TrueCrypt, etc)

Volume Level

CoreStorage

- Logical Volume Groups
- Created With:
  - Disk Utility
  - FileVault 2
  - CLI
    - diskutil

TrueCrypt/PGP/3rd Party

FileVault: Old and New

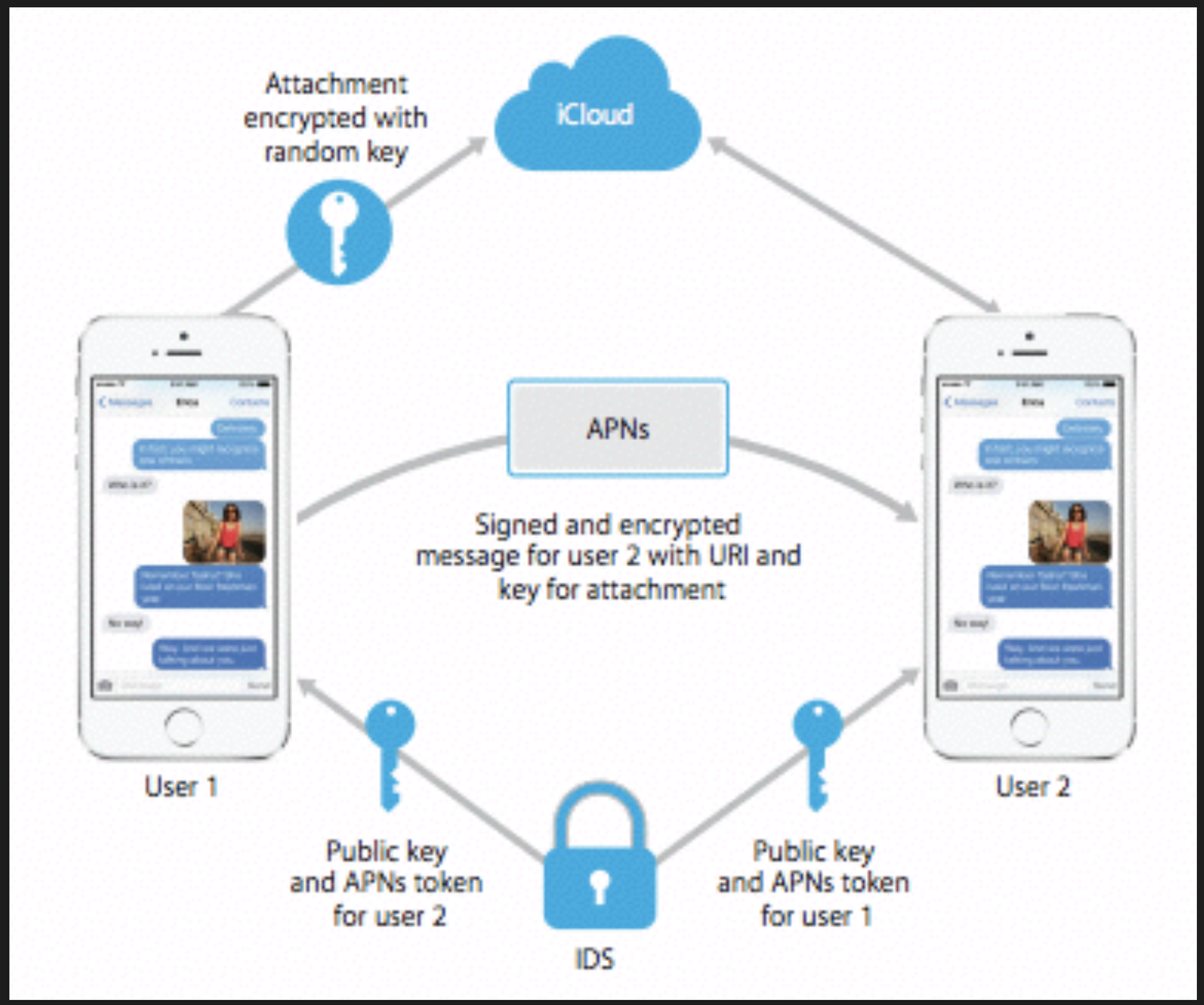
- FileVault 2
  - Uses AES 128 or 256
  - CoreStorage
  - ~20% performance loss
  - Encrypts entire user folder until after login
- Key Escrow with Cauliflowervest
  - Forces Encryption
  - Stores keys on a private server
  - Delegate access
- Legacy FileVault
  - Master Password
  - Horrible for Backups

Encryption on iOS

Mostly Automatic

- Not 100% secure
- Initial wipe does not wipe the memory, just the keys
- Be sure to encrypt your backups

Digital Signatures on iOS



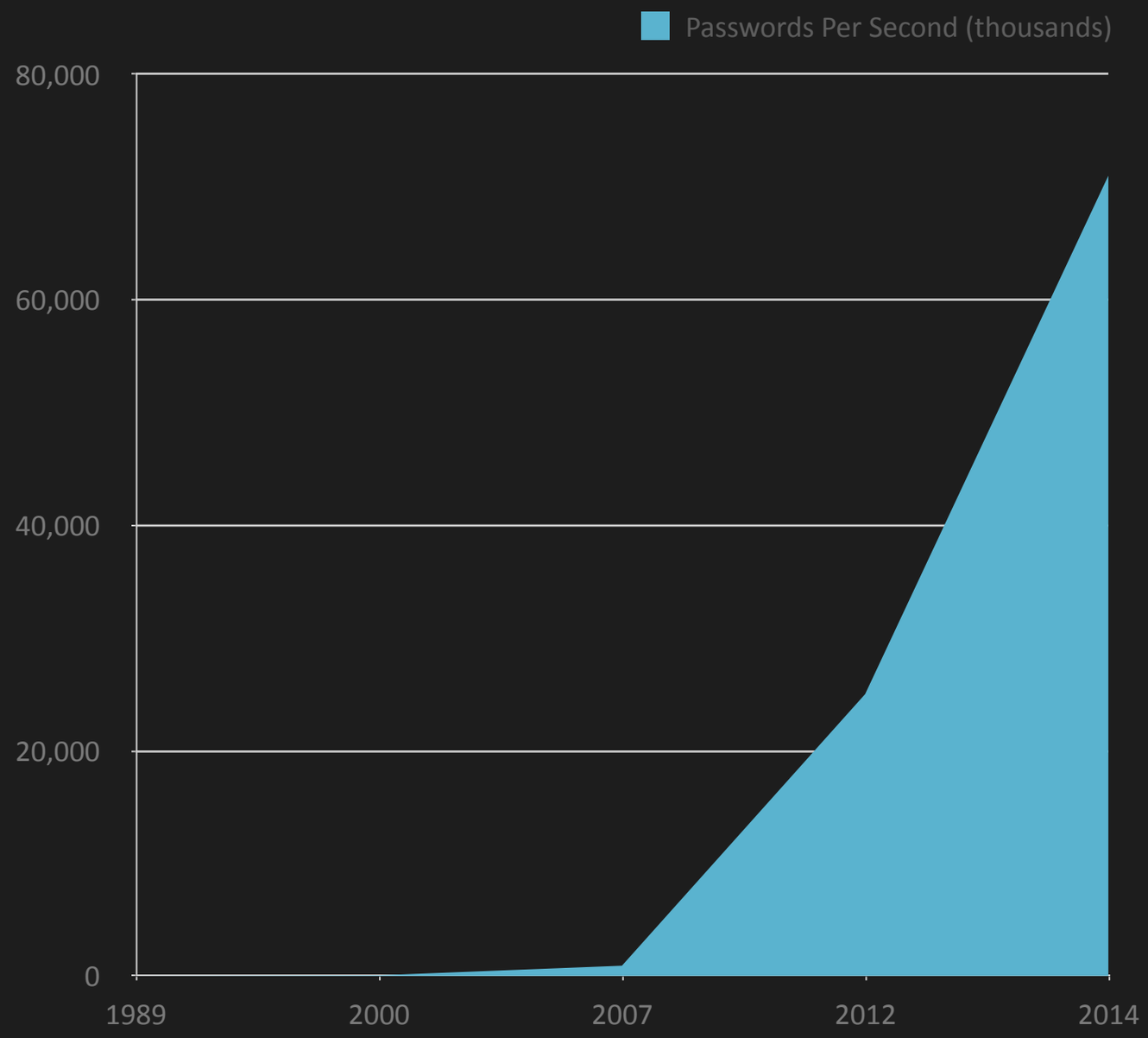
App Signatures

iMessage Encryption


Passwords

Password Cracking Speed

2000-2014



GPU

Access to GPU pipelines optimized for math has dramatically increased the amount of password tries

OS Matters

10.8+ Use a new hashing scheme, PBKDF2 that takes longer to crack

Certificates

For added security, use certificates when possible

Password Tips

KISS Password Policies

1. Expiring passwords does more harm than good
2. Your password is only as strong as your reset mechanism
3. Phrases turned into words and acronyms are best
4. Real words strung together are NOT secure

1

Wow...doestcst

Wow, does that couch smell terrible.

2

tlpWENT2m

his little piggy went to market

https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

MACTECH

Password Storage

- Keychain
  - OS X
    - Pervasive
    - Multiple Keychain Support
    - GUI: keychain access
    - CLI: security
  - iOS
    - Pervasive; no cli
  - iCloud Keychain syncs both
- Third Party Apps
  - 1password, lasspass,

    built into browsers, etc


Networks

Port Management

- TCP vs UDP
  - What are they?
  - How are they different?
- Who has access?
  - 0–1024 root only
    - prevents service spoofing

Firewalls are your friend. Use them.

Christian Woodward

(he’s right)

Firewalls

- Network Firewall: inbound/outbound
  - Router/Switch Level
    - Vendor Hardware
    - pfSense/m0n0wall
      - m0n0 better for OS X knowledge
  - OS Level
    - Built in cli: ipfw
    - 3rd party vendors

Firewalls Cont.

- Application Level Firewall: only inbound
  - OS X (server and regular)
    - Only singed packages can communicate
    - GUI: System Preferences
    - CLI:
      - socketfilterfw / defaults / launchd / config files
- http://krypted.com/mac-security/the-os-x-application-layer-firewall-part-3-lion/

Common Ports

22

SSH

80
443

Web

993
143
110
25

Mail

53

DNS

Well known TCP & UDP ports used by Apple

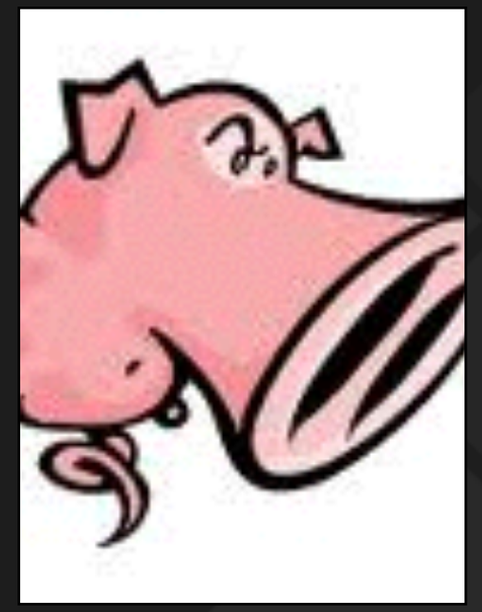
http://support.apple.com/kb/ts1629

/etc/services

IDS Life

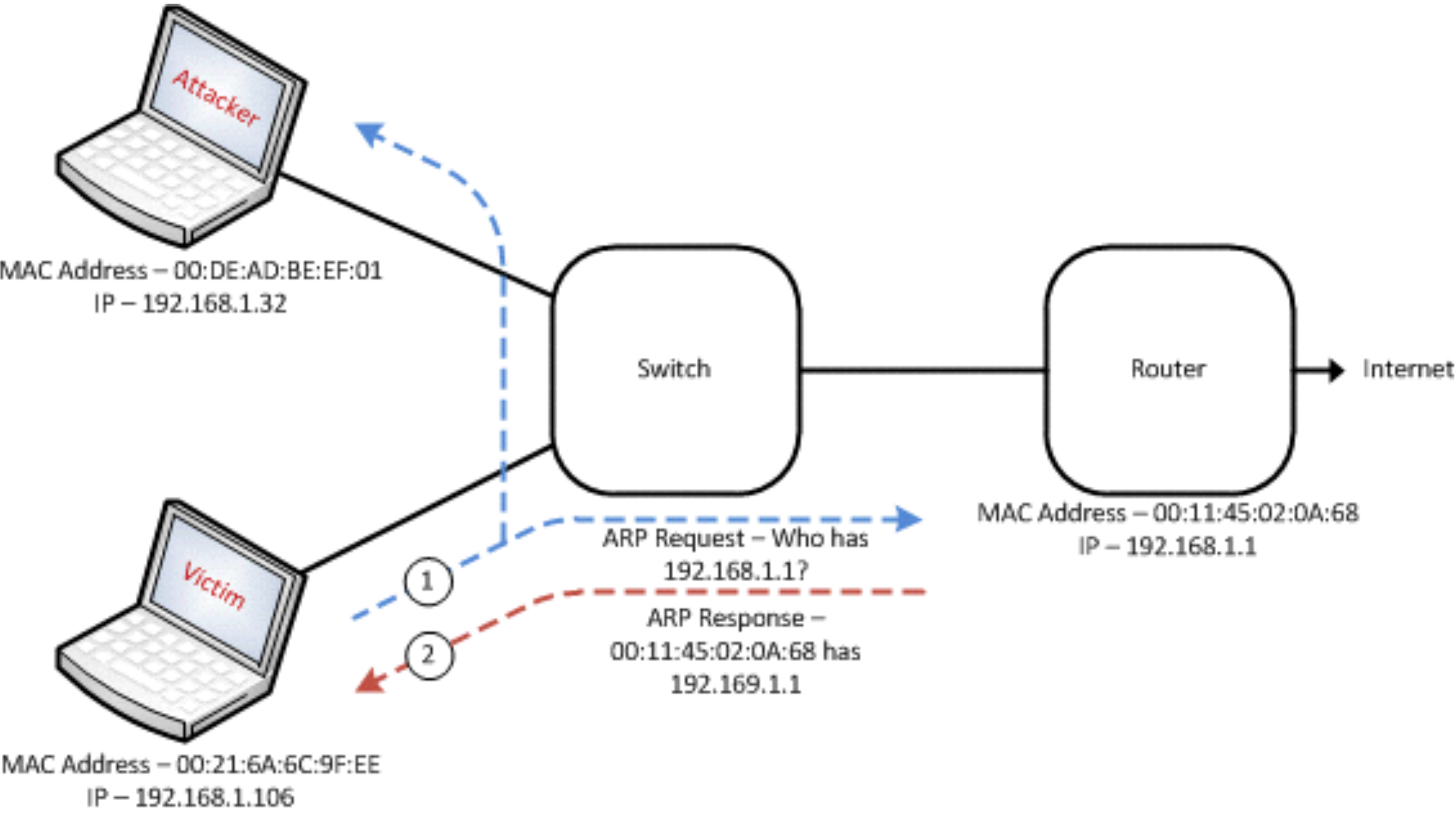
…or how I learned to stop worrying and love the snort

- Detects attacks and can integrate to block in realtime
  - Signature based
    - Must be maintained/updated
    - Requires someone to monitor to be effective
  - Vendor hardware
  - Software: SNORT, 4shadow, MIDAS, etc



Man in the Middle

- Some AV vendors protect
- Best protection at network level
- Techniques
  - ARP Cache
  - DHCP Spoof/Race
  - IPv6 Neighbor Discovery
  - Others


Attacker
MAC Address – 00:DE:AD:BE:EF:01
IP – 192.168.1.32
Switch
Router
Internet
MAC Address – 00:11:45:02:0A:68
IP – 192.168.1.1
ARP Request – Who has 192.168.1.1?
1
ARP Response – 00:11:45:02:0A:68 has 192.169.1.1
2
Victim
MAC Address – 00:21:6A:6C:9F:EE
IP – 192.168.1.106

VPNs

- Dont use PPTP!
- IPSec or SSL VPN preferred
  - OS X Server, OpenVPN, vendor appliances
  - l2tp over ipsec if you must
- **VPN as much as possible**

Environmental Obfuscation

- Security by Obscurity
  - Server and Service Identification.
    - How are you naming your server?
    - How are you advertising it?
  - Some believe it makes it harder to find.

Environmental Obfuscation

DONT DO THIS

- Security by Obscurity
  - Server and Service Identification.
    - How are you naming your server?
    - How are you advertising it?
  - Some believe it makes it harder to find.

Minimizing Threat Surface

- Obfuscation does not work, but minimizing your threat service can eliminate risk.
- Leave open what you need, use appropriate protocols, and run everything that does not NEED to be public facing over a VPN.
- Limit post-intrusion risk by limiting cross-machine access
- No password re-use
- Dont trust internal devices


Questions?

Thank You

christianwoodward@gmail.com

I respect myself. That's why I refuse to use `sprintf`.
Using `sprintf` is a decision you can never take back.
That's why I'm waiting until I'm older and there's a string handling function that's right for me

Forget `sprintf`!

natashenka.ca/sprintf