



SHARKFEST '13

Wireshark Developer and User Conference

I Can Hear You Tunneling

Alex Weber



About me

- Software developer at Tenable Network Security
- I fixed a typo in a comment in the FreeBSD kernel
- Contact info:
 - Twitter: **@AlexWebr**
 - Email: **AlexWebr@gmail.com**
 - FreeNode and Efnet: **AlexWebr**
 - I'm **AlexWebr** pretty much everywhere

Forewarning

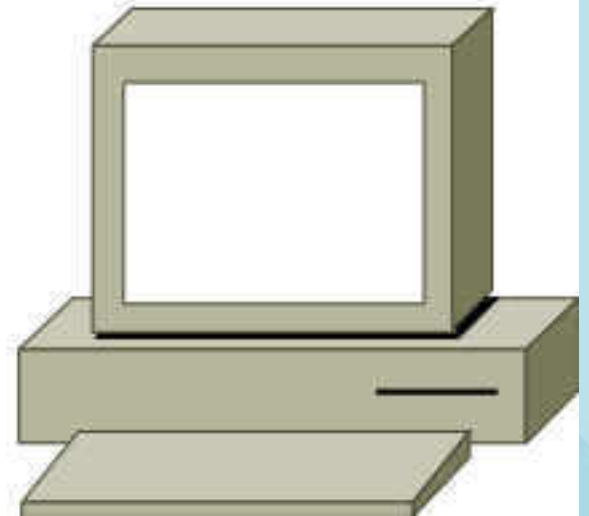
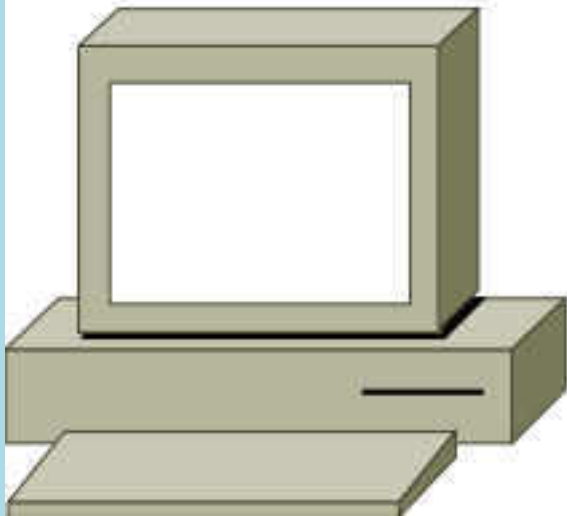
- I'm not here to show you how to break SSH
- SSH2 has a *really good* track record
- Warning: meandering ahead
- I intend to:
 - Explain what SSH is and convince you that it rocks
 - Explain why it can be dangerous
 - Bring you up to speed on previous research and current tools

What is SSH?

- Originally designed as a secure replacement for the infamous “r” commands (rsh, rexec, etc.)
- Uses strong encryption
- Allows for multiplexing many *channels* over a single encrypted TCP session
- The most popular implementation is OpenSSH
- PuTTY is a popular choice for Windows PCs

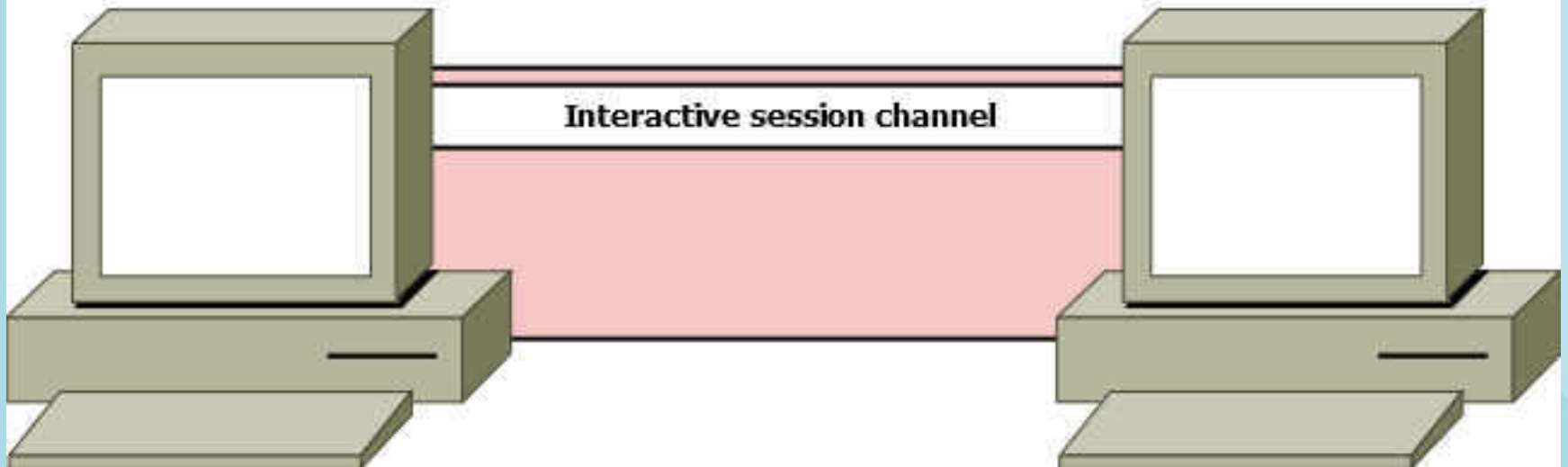
SSH Channels

```
$ ssh alex@example.com
```



SSH Channels

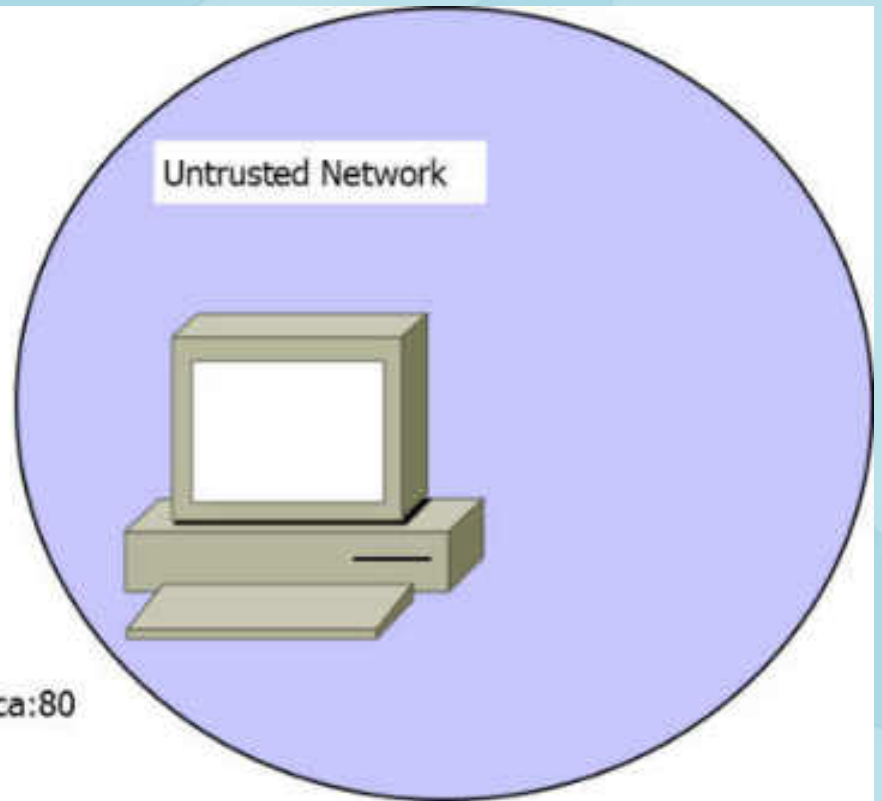
```
$ ssh alex@example.com
```



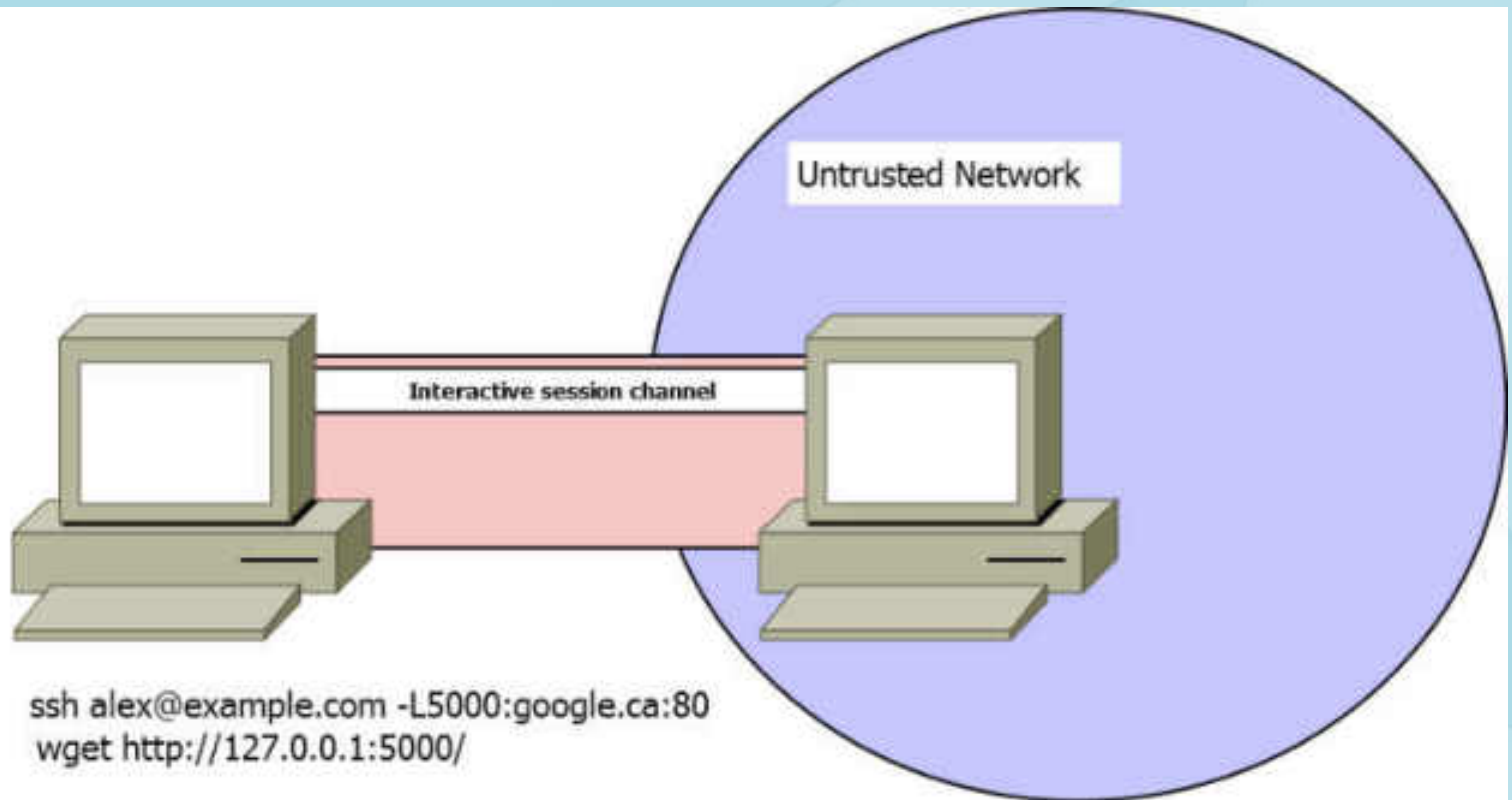
SSH Channels



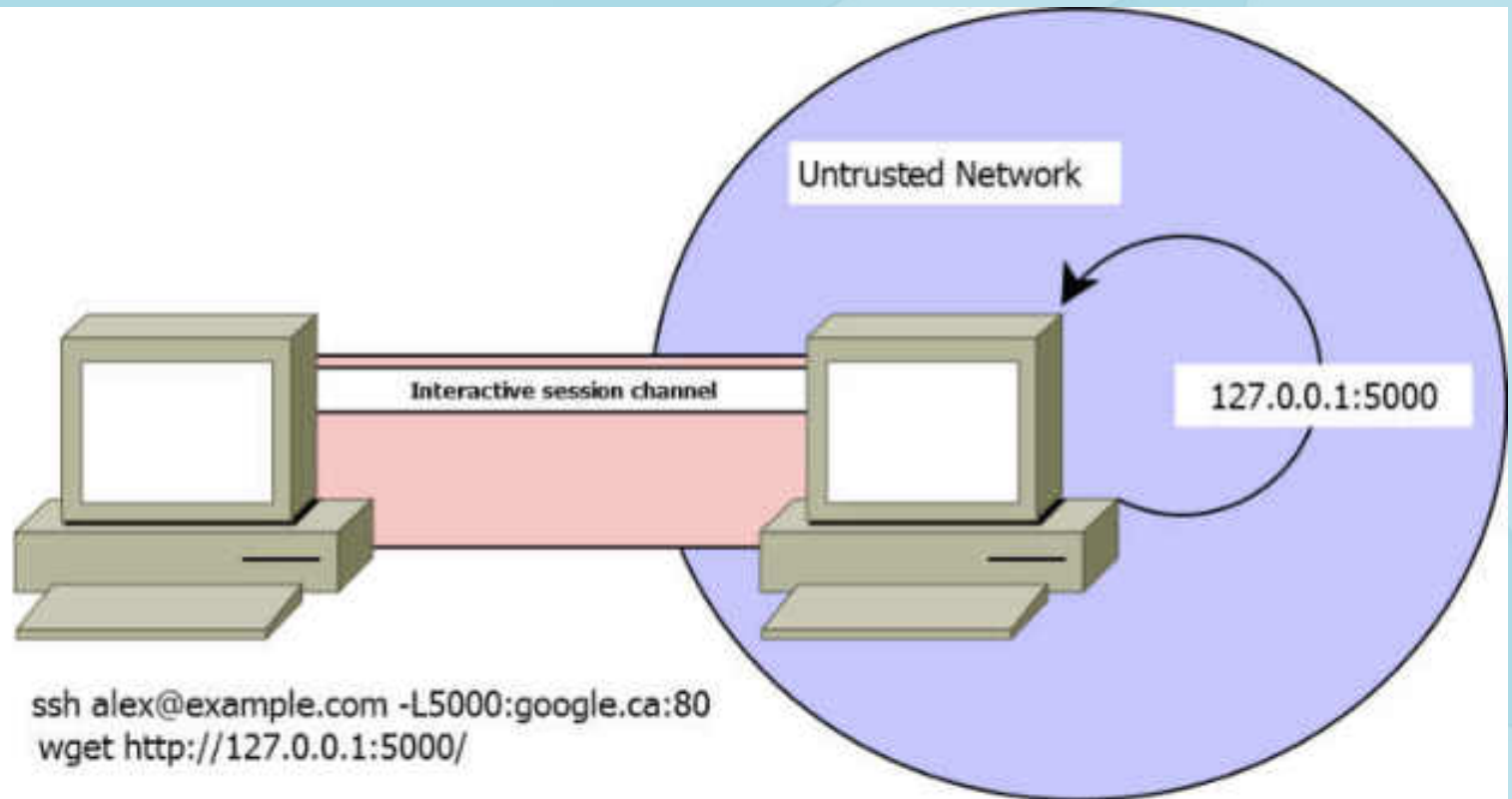
```
ssh alex@example.com -L5000:google.ca:80  
wget http://127.0.0.1:5000/
```



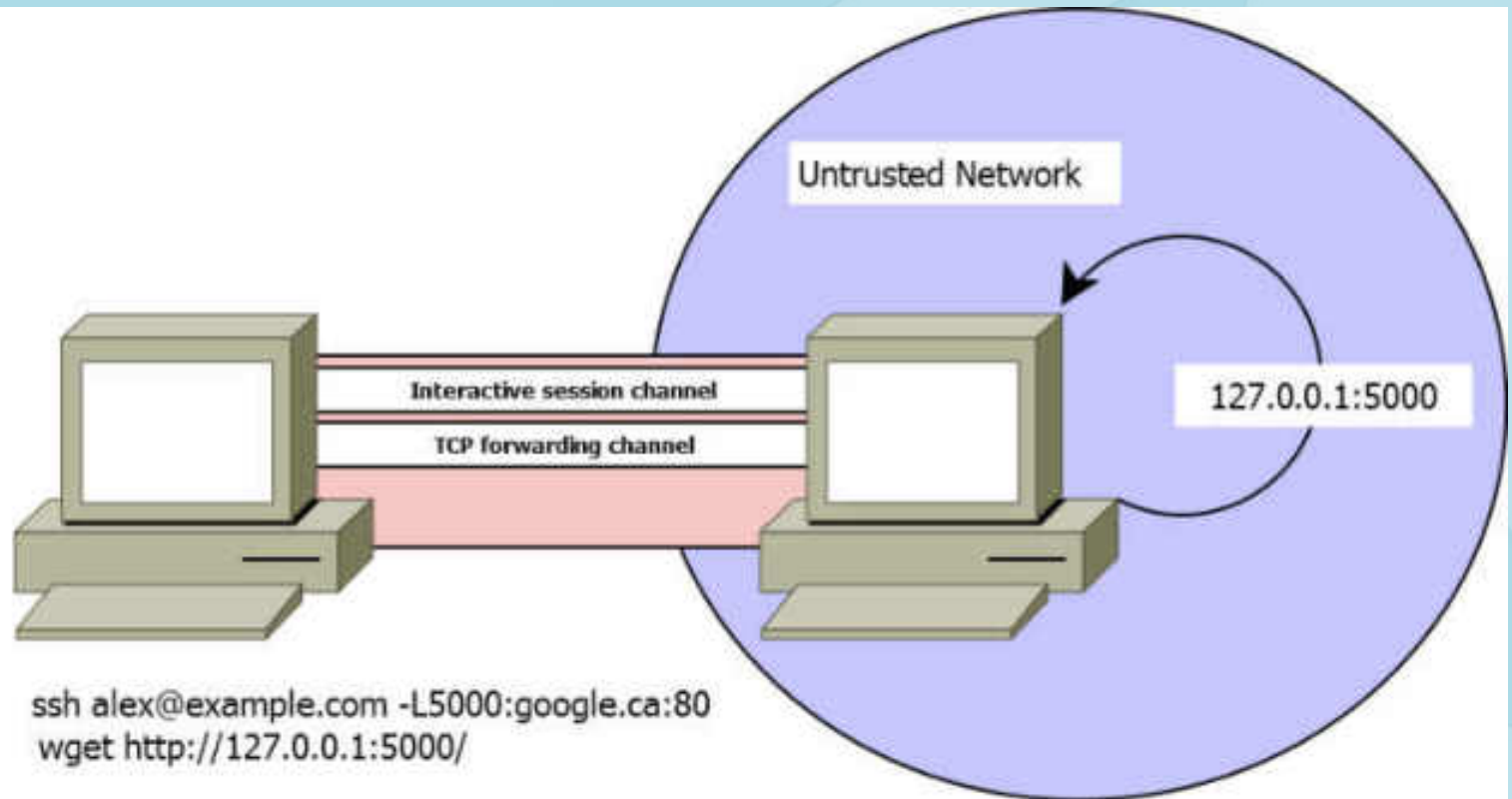
SSH Channels



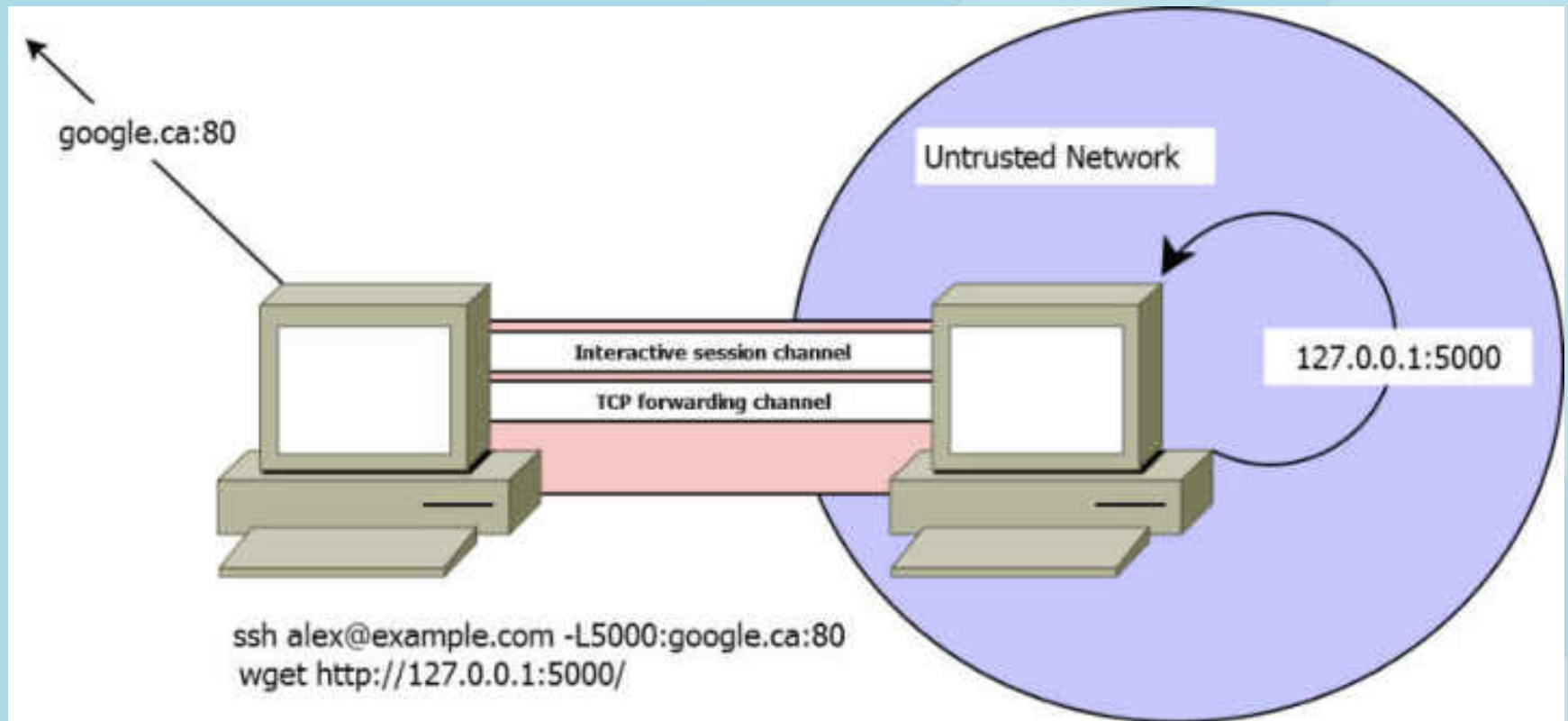
SSH Channels



SSH Channels



SSH Channels



SSH can do some awesome stuff

- Allows remote shell access to servers
- Choose-your-own authentication
- Permits file copies to and from a server
 - File system access (SSHFS)
 - Built-in compression
- Integrates with X11 – instant thin client!
- Can offer a SOCKS proxy (Firefox, Pidgin, etc.)
- Layer 3 and layer 2 VPN using **tun** devices

HOSTILE NETWORK?

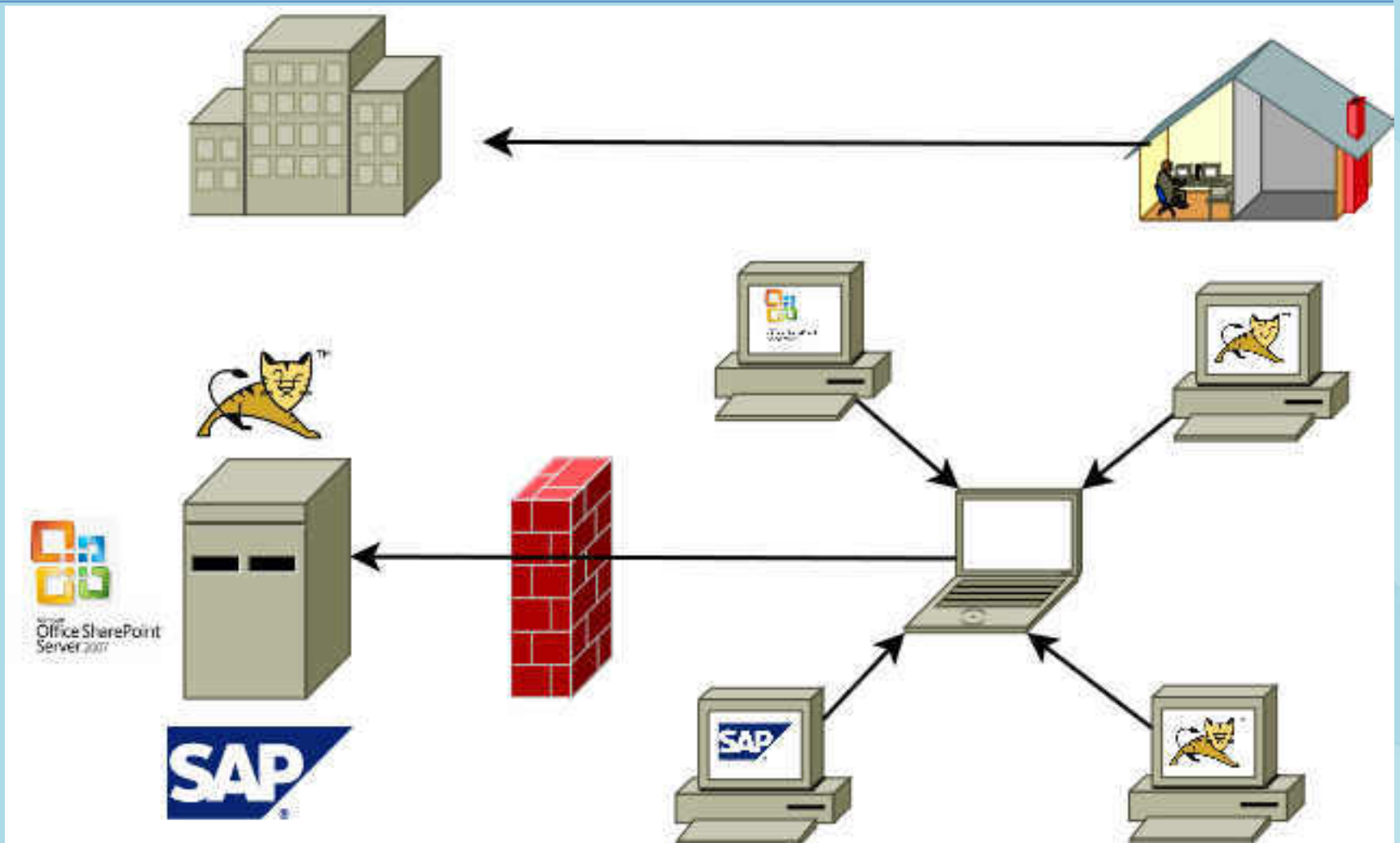


TUNNEL ALL THE THINGS!

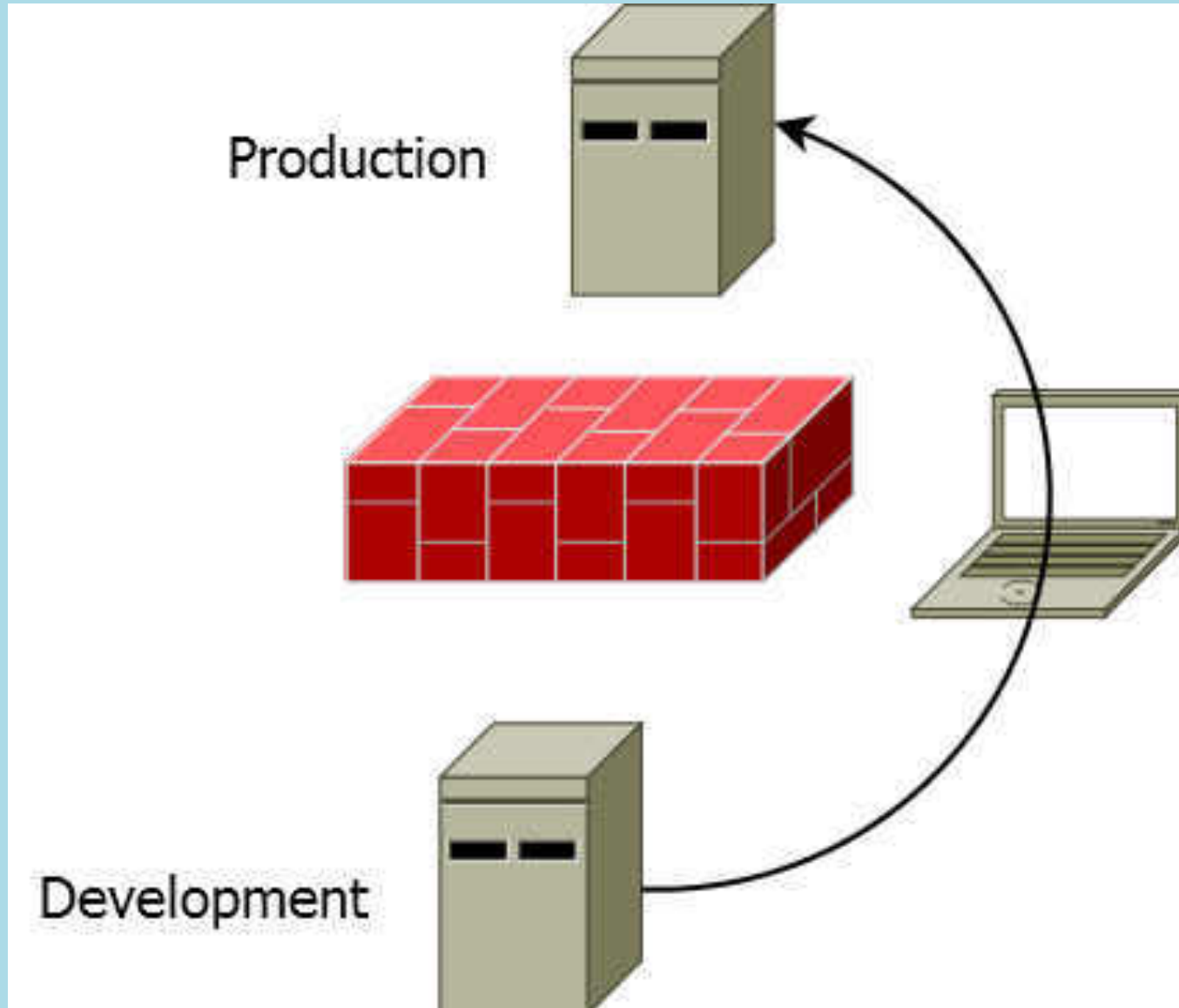
SSH can be dangerous!

- If you allow SSH traffic to travel all over the place, you are going to have a bad time
- We talked about channels already:
 - The client can forward ports to the server
 - The client can request that remote server ports be forwarded back to the client
 - Both remote- and local-forwarded ports can listen on external interfaces
- Let's look at a few examples...

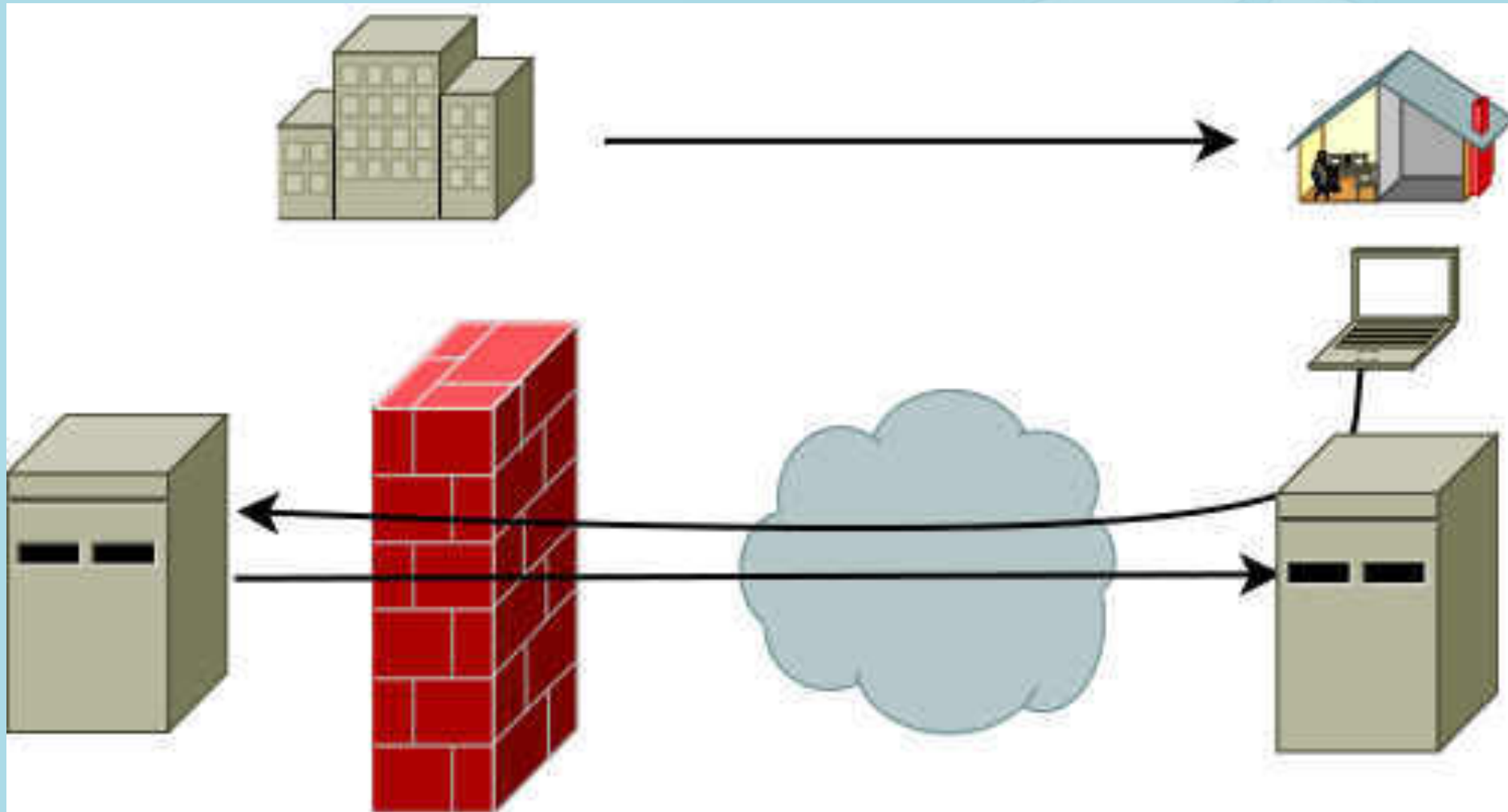
SSH can be dangerous!



SSH can be dangerous!



SSH can be dangerous!

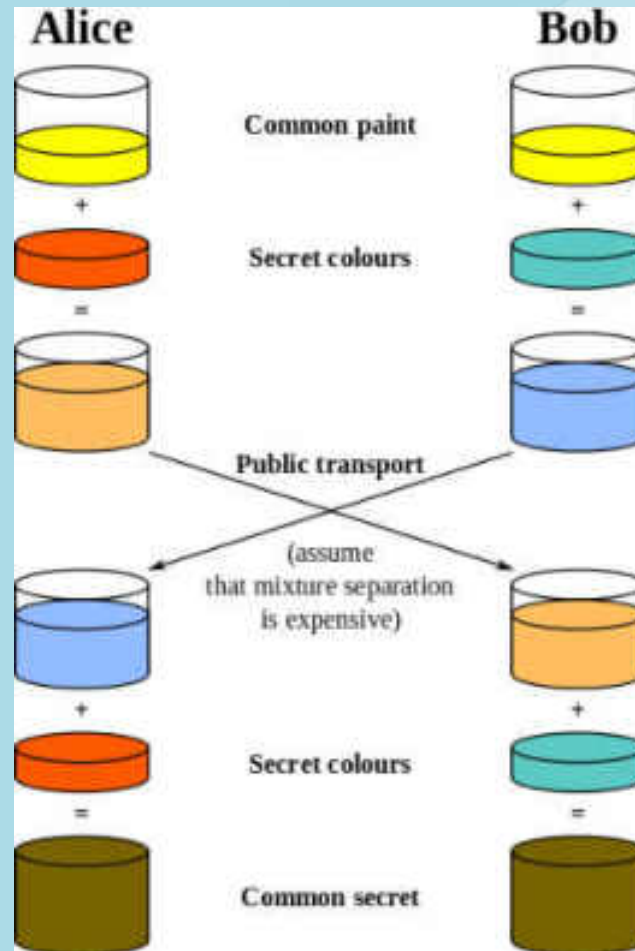


What's a network admin to do?

- SSH is hard to man-in-the-middle out of the box
- No X.509 certificate chain to transparently exploit

What's a network admin to do?

- Uses Diffie-Hellman (perfect forward secrecy)

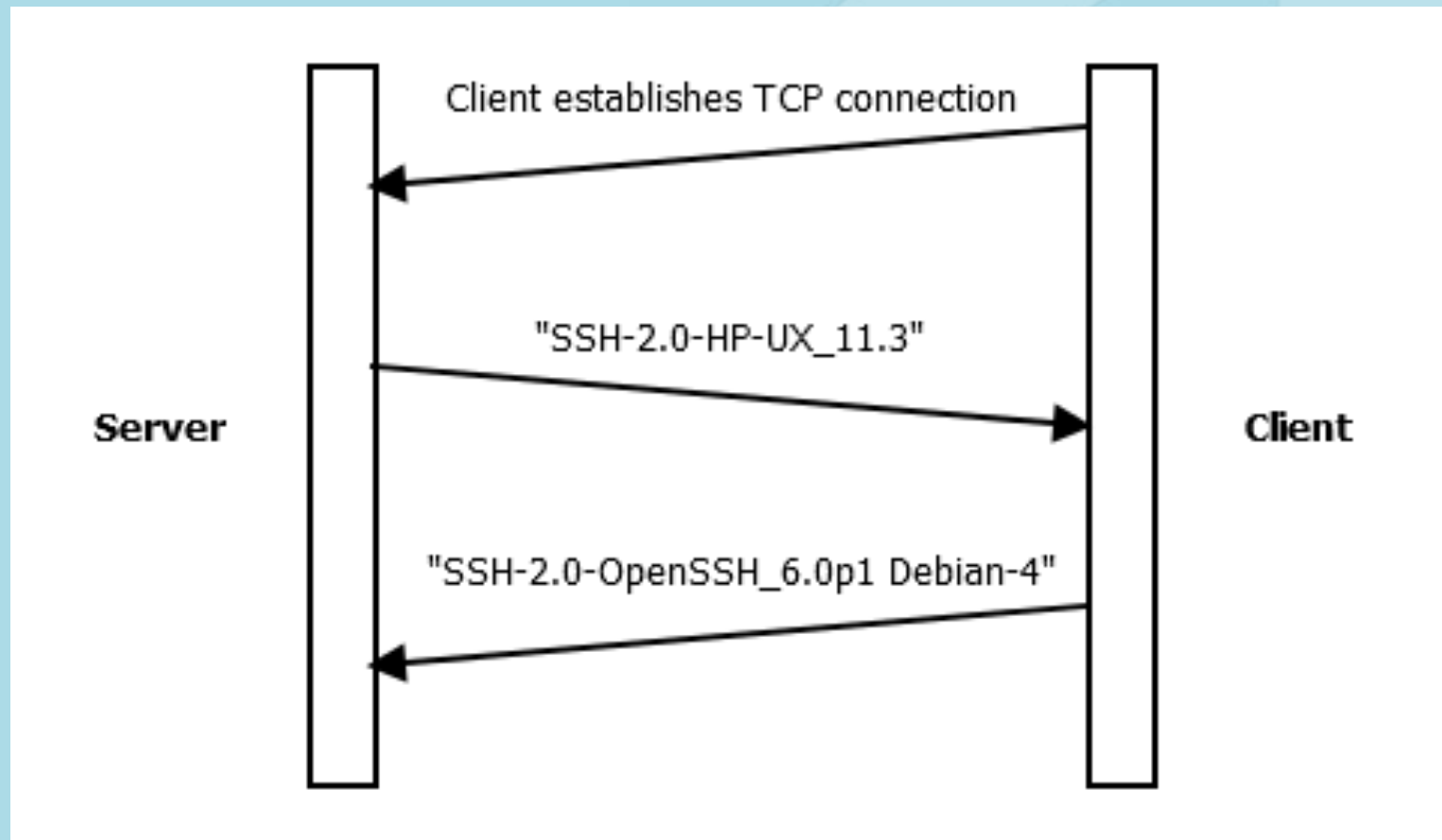


What's a network admin to do?

- In the real world, force all traffic through an SSH proxy - anything that doesn't cross the proxy is a policy violation
But, the real world is boring!

Analyzing the Handshake

- Let's look at the SSH handshake...



Analyzing the Handshake

- Look at version strings exchanged in the handshake because they can give away the operating system!
- Remember that a lack of explicit OS name is also information: likely **not** Debian, FreeBSD, etc.
- Examples:
 - SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1
 - SSH-2.0-OpenSSH_6.0p1 Debian-4
 - SSH-2.0-OpenSSH_5.5p1 Debian-6+squeeze2
 - SSH-2.0-HP-UX_11.3
 - SSH-2.0-OpenSSH_5.8p2_hpn13v11 FreeBSD-20110503

Analyzing the Handshake

- Look at negotiated cipher suites – can give away patch level if the version number is not present
- UMAC-64 support was added in 4.7
- CBC preferred before 5.2, CTR afterwards
- Elliptic Curve DSA support was added in 5.7
- Truncated SHA2 support added in 5.9 and removed in 6.1
- AES-GCM supported added in 6.2

Analyzing the Handshake

- Why should we care about version numbers?
- We can correlate operating system information with what's expected on the network:
“Why is there an Ubuntu machine on our network?”
- Can be used to look for vulnerabilities:
Tenable's Passive Vulnerability Scanner has over 90 passive checks that connect SSH version numbers to exploitable vulnerabilities

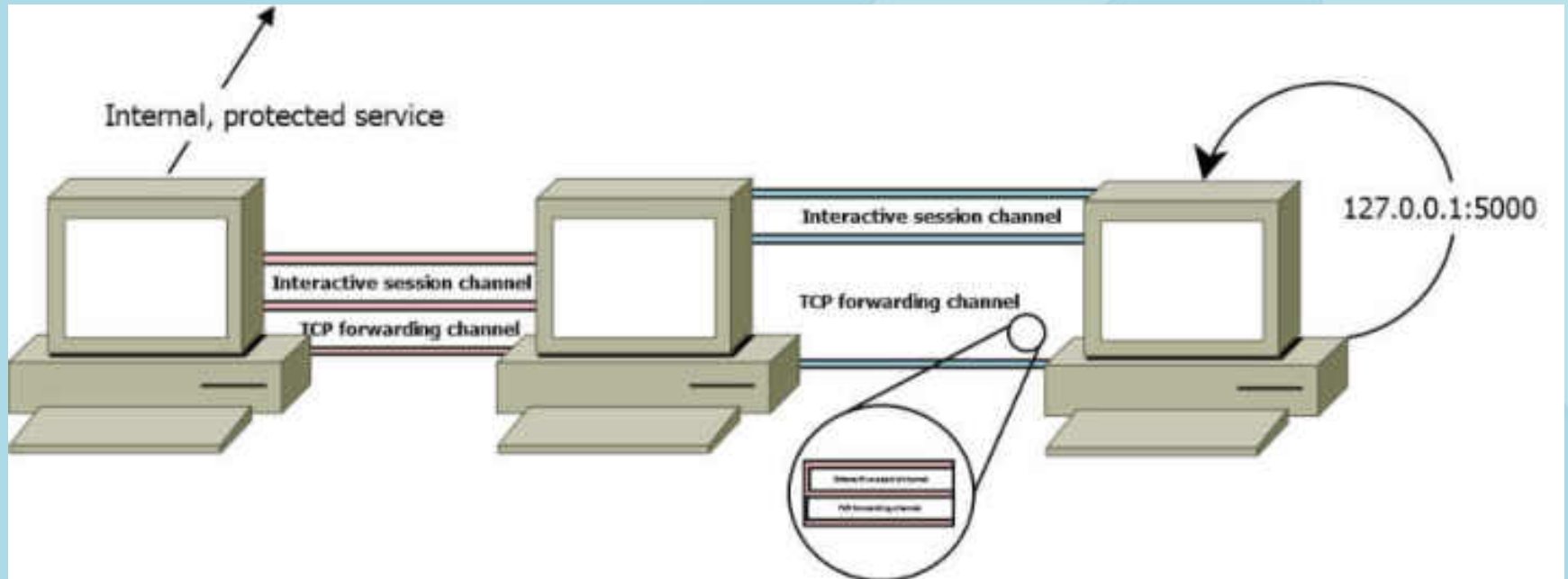
Detecting pivots

- Ingress and egress rules may be different depending on the network segment a device is in
- A user may route their traffic through one or more hops, so that their traffic is treated more favorably
- Penetration testers call this “pivoting”
- I’ve always wished I was cool enough to be a penetration tester, so I’ll call it pivoting too

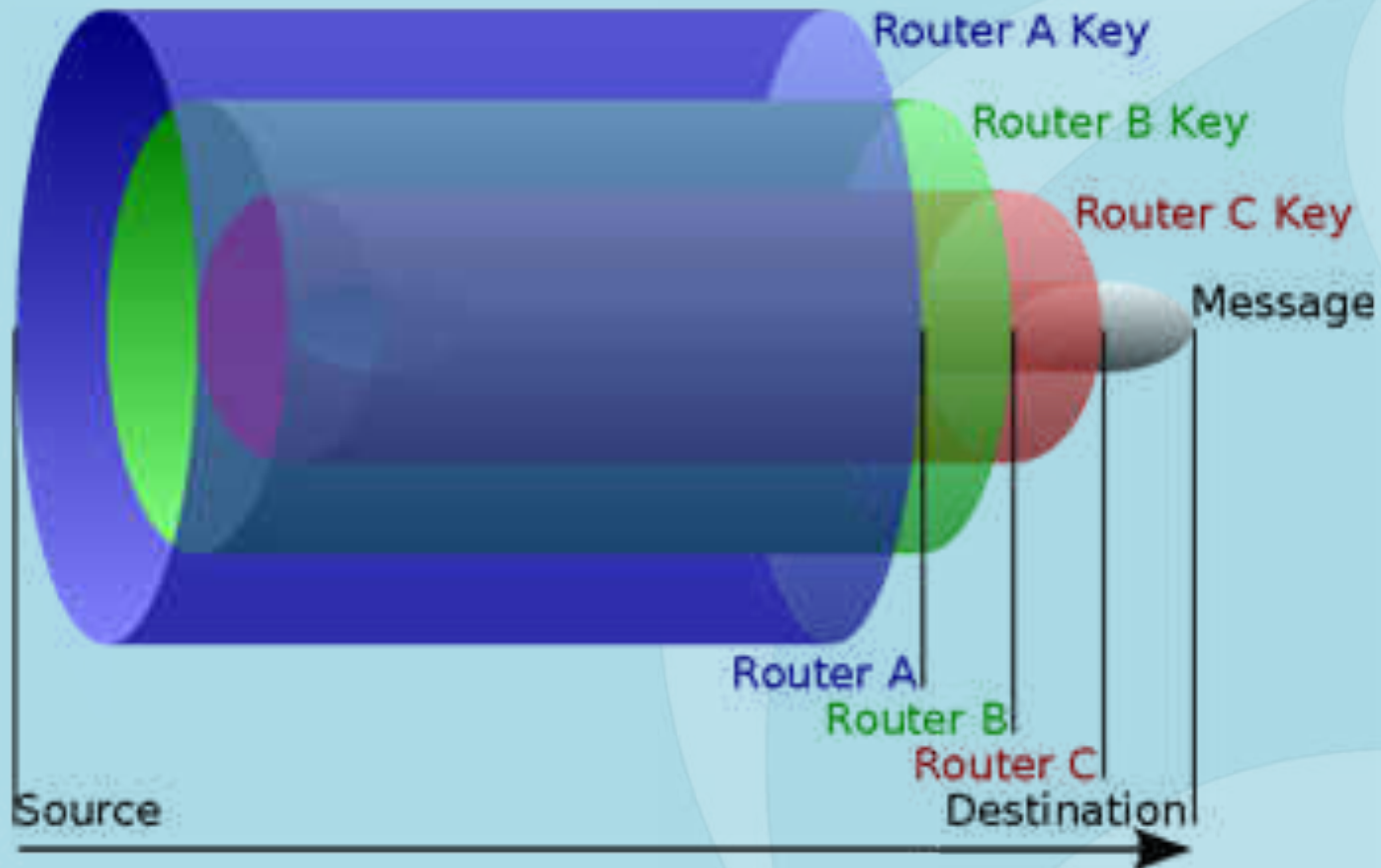
Detecting pivots

- The two kinds of pivots we'll talk about today:
 - Nesting SSH sessions
 - Using netcat, Ncat, or similar to relay

Detecting Nested SSH Sessions



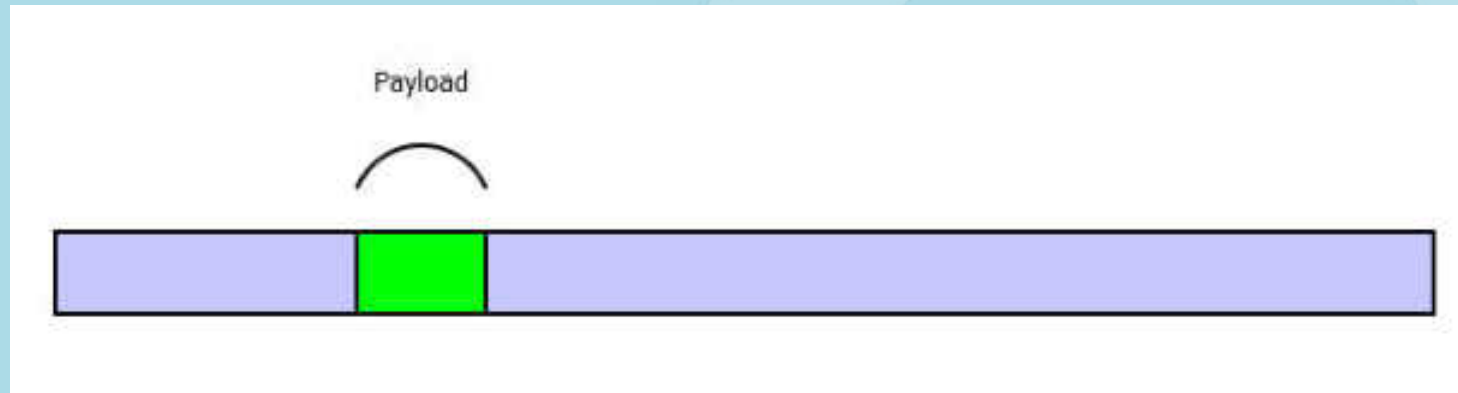
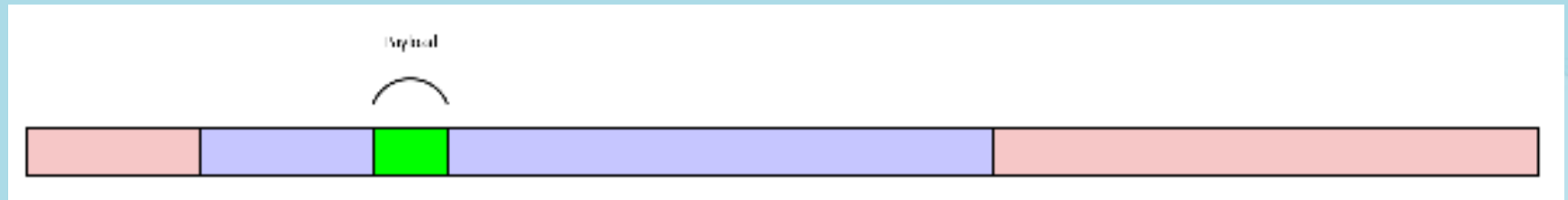
Detecting Nested SSH Sessions



Detecting Nested SSH Sessions

- In the case of nested tunnels, it's pretty easy to follow the flow through the network
- Look for SSH connections where the smallest packet is double/triple/etc. the size of the smallest possible packet for the chosen ciphersuite
- To find the next hop, look for packets egressing from the middle host that are “one layer smaller”

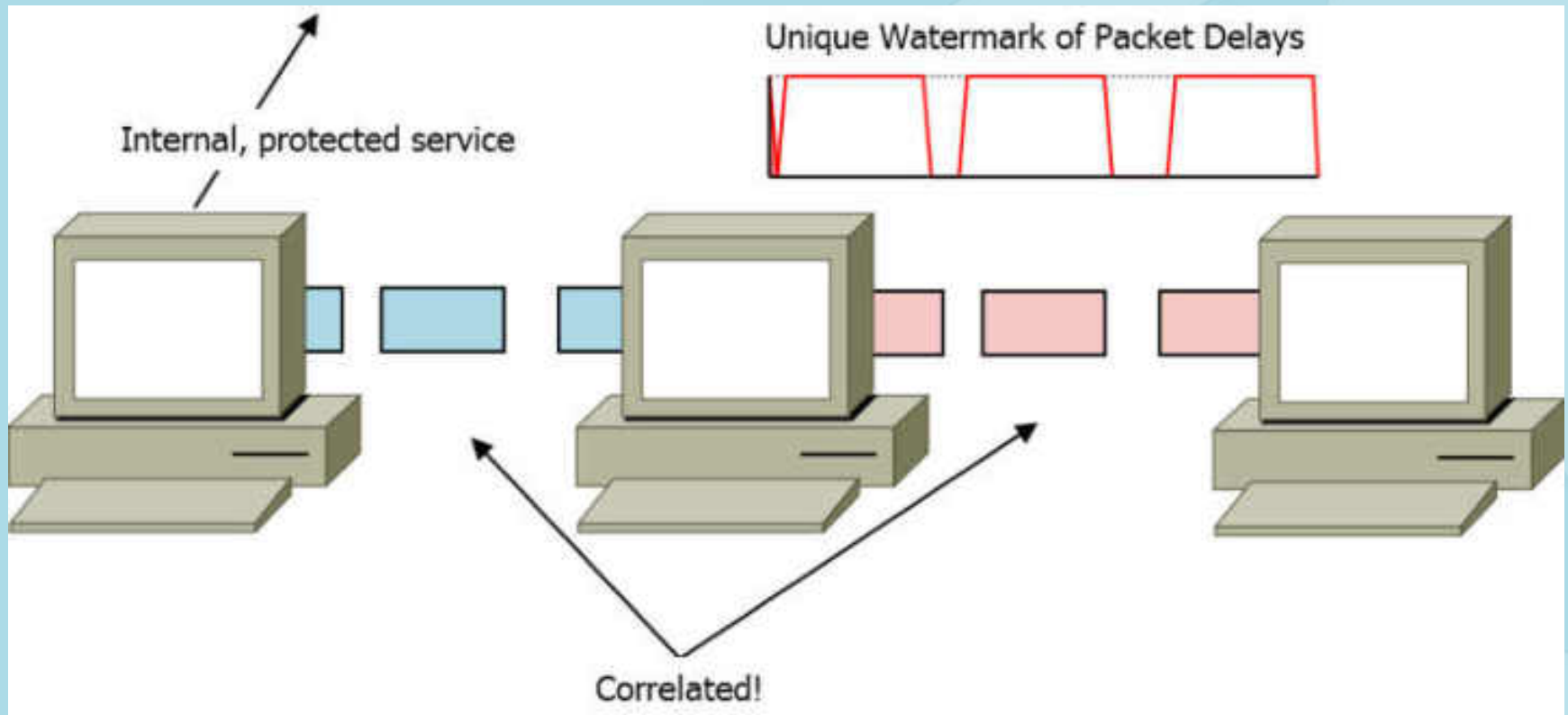
Detecting Nested SSH Sessions



Detecting netcat / Ncat relays

- “Active Timing-Based Correlation of Perturbed Traffic Flows with Chaff Packets”
Pai Peng, Peng Ning, Douglas S. Reeves,
Xinyuan Wang
North Carolina State U, George Mason U
- Not strictly passive, and not SSH, but interesting
- Watermark packets by introducing small, unique inter-packet delays
Any connection downstream with same inter-packet delay is likely ‘fed’ by the watermarked upstream connection

Detecting Pivots



Side Channel Attacks

- Definition: a side channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis)

- Wikipedia

Side Channel Attacks

- **Protocol for Securely Recording Information**
 - Write information down on a pad of paper
 - Don't allow anyone to see the paper
 - Easy!

Side Channel Attacks

- The act of writing requires visible movement
 - Can we reconstruct the text by monitoring movement of the arm, the eyes, or the pencil? How about all together?
- Writing causes friction heat in the writing surface
 - Can a thermal imaging camera reproduce the text by viewing the writing surface, post-recording?
- The act of writing generates noise
 - If recorded, can we determine the movement of the pencil?
 - What if there are many microphones?

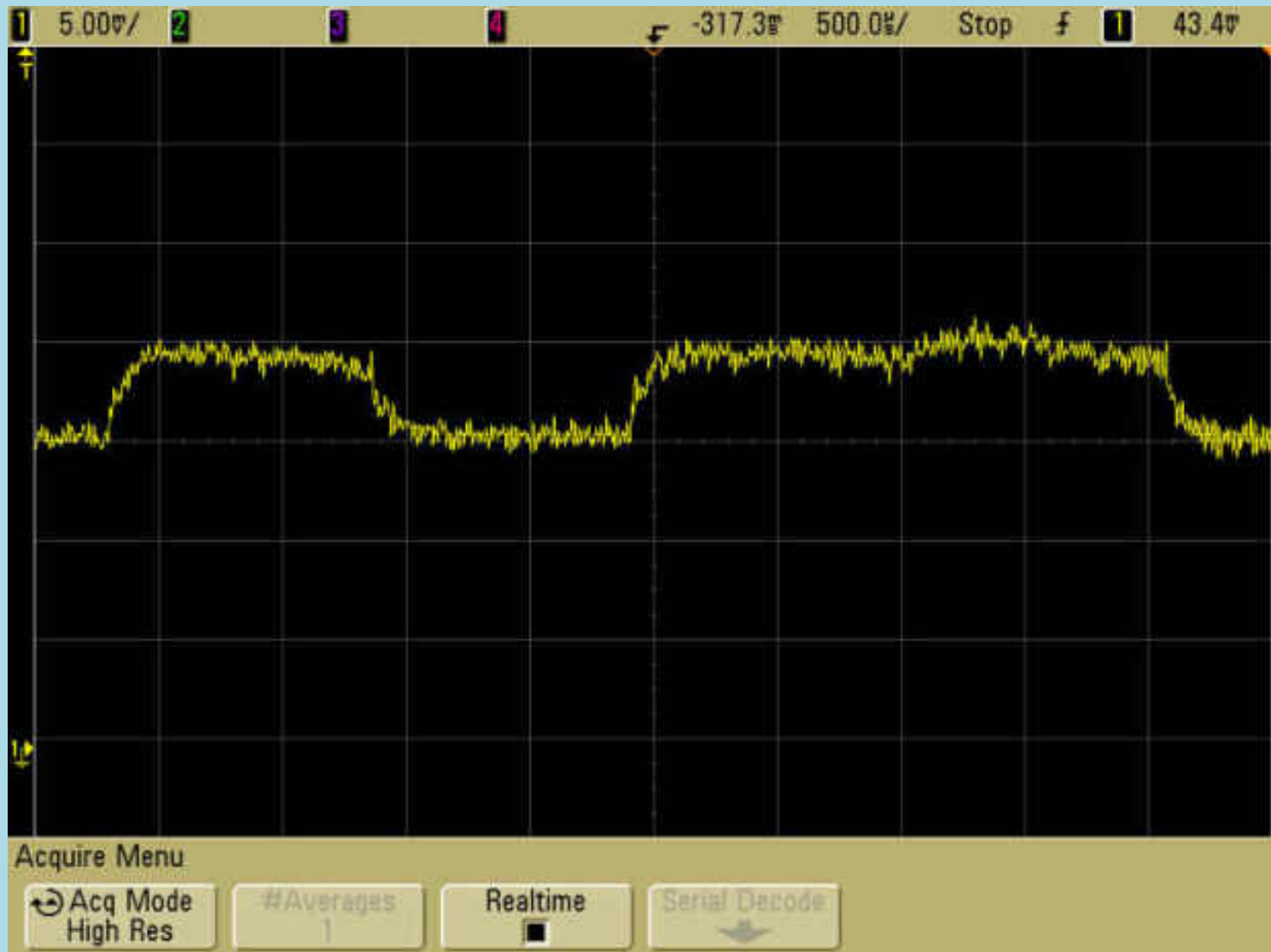
Side Channel Attacks – Real World

- Observable movement
 - Real-world equivalent: traffic flow analysis
- Residual heat in the writing surface
 - Real-world equivalent: cold-boot attacks
- Recordable noise from the writing process
 - Real-world equivalent: acoustic and power analysis
- Writing activity does not match information density
 - Real-world equivalent: CRIME (compression attacks)

Power Analysis

- Introduced by Cryptography Research in 1998
- Exactly what it sounds like:
Measuring the power consumption of a device as it performs a cryptographic operation
- Simple and Differential power analysis (SPA/DPA)
- FIPS 140-2 doesn't require SPA or DPA resistance

Power Analysis



Cold Boot Attacks

- Pioneered by J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten
- Contrary to popular assumption, RAM retains information for seconds to minutes after power is lost

Cold Boot Attacks

- Attack scenario:
 - Your laptop uses full-disk encryption
 - Your laptop is powered on, but locked
 - Your laptop is stolen
- If the attacker removes the harddrive, they get nothing
- We assume the lock screen cannot be bypassed (not always true, see “Inception” against Mac OS X)

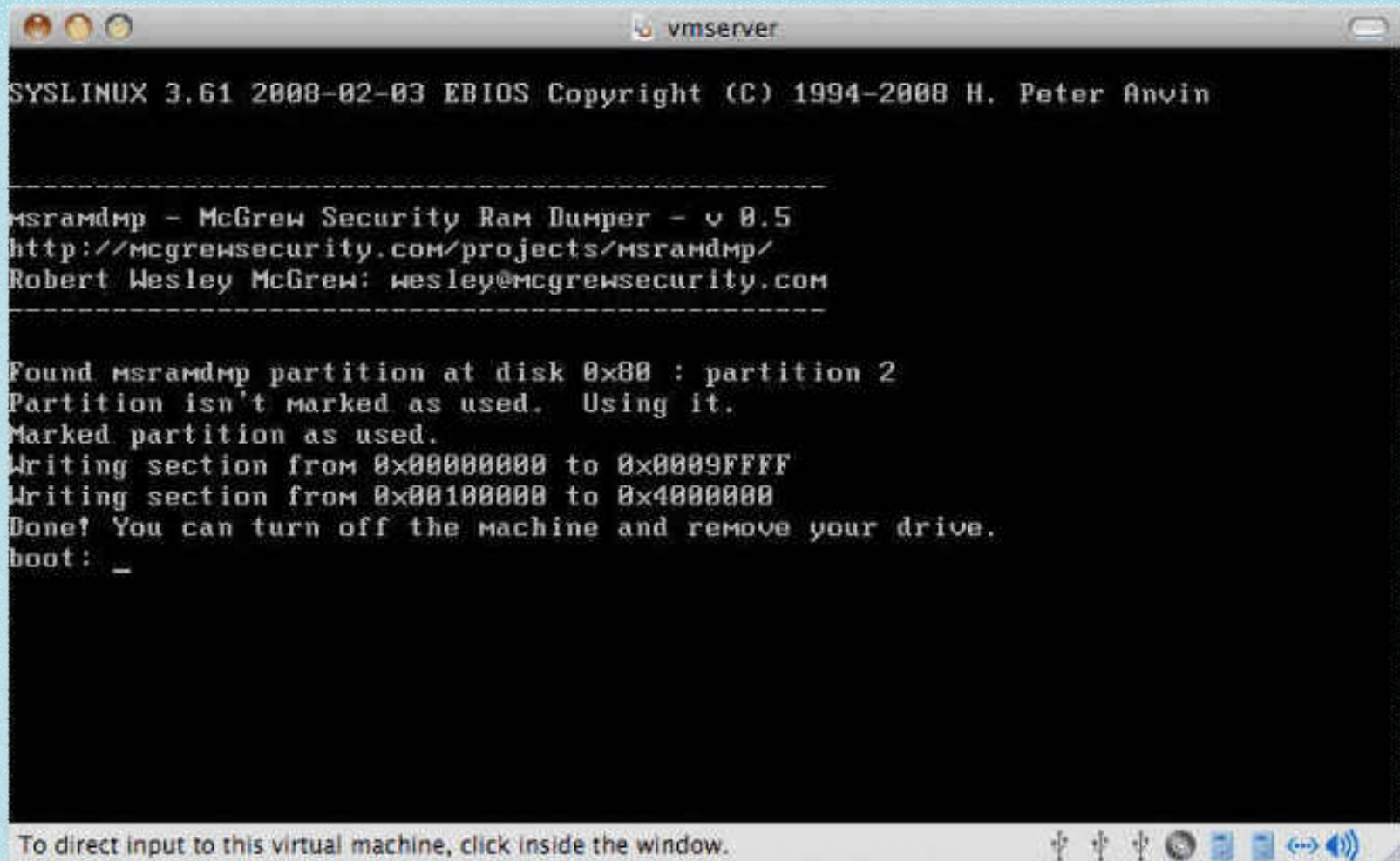
Cold Boot Attacks

- Cryptographic keys must stay in RAM
- RAM retains information for seconds to minutes after power loss
- As RAM is cooled, it retains information for longer
- Cool the RAM, hard reset, and dump all memory
- Apply a tool like **findaes** to the dumped memory to locate cryptographic keys

Cold Boot Attacks



Cold Boot Attacks



```
SYSLINUX 3.61 2008-02-03 EBIOS Copyright (C) 1994-2008 H. Peter Anvin

-----
msramdmp - McGrew Security Ram Dumper - v 0.5
http://mcgrewsecurity.com/projects/msramdmp/
Robert Wesley McGrew: wesley@mcgrewsecurity.com
-----

Found msramdmp partition at disk 0x80 : partition 2
Partition isn't marked as used. Using it.
Marked partition as used.
Writing section from 0x00000000 to 0x0009FFFF
Writing section from 0x00100000 to 0x40000000
Done! You can turn off the machine and remove your drive.
boot: _
```

To direct input to this virtual machine, click inside the window.

Side Channels and SSH

- Let's look at the previous information leaks SSH has had and how others have exploited them

Previous Research

- “Passive Analysis of SSH Traffic”
Solar Designer and Dug Song
March 19th, 2001
- Applies to SSH1, primarily
- Wrote a tool that:
 - Detects password length (login and sudo)
 - Detects RSA or DSA authentication
 - Determine the length of shell commands and in some cases, the commands themselves
 - If you have old Cisco devices with SSHv1, you’re still vulnerable!

Previous Research

- **sshkeydata**
Tool written by Brendan Gregg
Compares a packet capture from an SSH session and a Telnet session of the same user
Looks for timing similarities to guess commands
- 92% accuracy in an SSH session where 20 commands were executed

Previous Research

- First and foremost, SSH should protect the privacy of data being exchanged
- Ideally, SSH should also keep the user's behavior confidential.
- “A Preliminary Look at the Privacy of SSH Tunnels”
- “Tunnel Hunter: Detecting Application-Layer Tunnels with Statistical Fingerprinting”
- Uses big words like Gaussian Mixture Models and Hidden Markov Models

SSHFlow

- Written in Python, uses the dpkt library
- Examines a PCAP for SSH traffic
- Guesses what is being tunneled based on most common packet sizes
- Can distinguish file copies from X11 from interactive sessions
- Can detect nested tunnels
- It's not pretty – it's just a proof-of-concept

SSHFlow Demo 1

- I am going to demo using ASCII.IO
- If you have a smartphone or a laptop in front of you, you can watch this “asciicast” by browsing to this address:

asci.io/a/3442

SSHFlow Demo 2

- I am going to demo using ASCII.IO
- If you have a smartphone or a laptop in front of you, you can watch this “asciicast” by browsing to this address:

asci.io/a/3443

Recommended Reading

- Silence on the Wire
Michal Zalewski
- Cryptography Engineering
Ferguson, Schneier, Kohno

Hacker CTFs and Wargames

- PlaidCTF
- Ghost in the Shellcode
- Defcon Qualifiers
- PHDays
- PoliCTF
- Over the Wire
- Smash the Stack

Recap

- What SSH and why you should use it
- Why you should **not** let your users use SSH without careful monitoring
- Some pie-in-the-sky and some more practical techniques for following pivots through the network
- What side channel attacks are and how they affect SSHv1 with regards to password authentication

Recap

- SSHFlow, a proof-of-concept tool to detect the protocols being tunneled by an SSH connection
- Recommended reading
- CTF challenges and <http://ctftime.org>
- Recap
 - Recap
 - Recap
 - Oh my god what's going on!?!?!?

Thanks!

- Contact info:
 - Twitter: **@AlexWebr**
 - Email: AlexWebr@gmail.com
 - FreeNode and Efnet IRC: **AlexWebr**
- Demos: **ascii.io/~AlexWebr**
- <https://github.com/AlexWebr/sshflow>