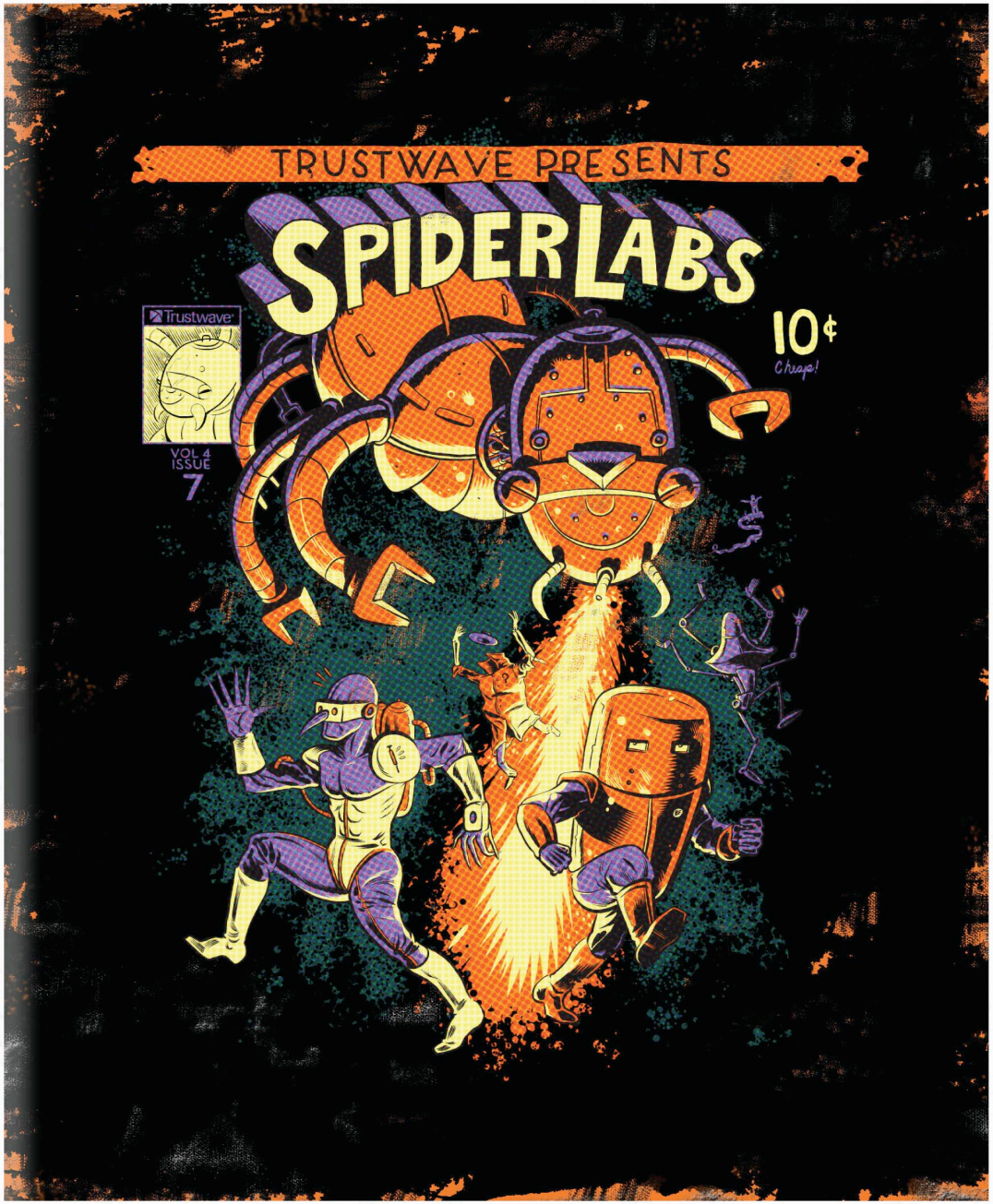


SpiderLabs 2009

Long Term Sessions: This is why we can't have Nice Things

Trustwave®

Steve Ocepek
Senior Security Consultant

Agenda

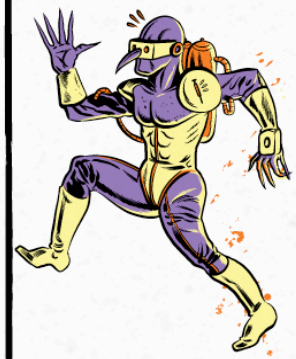
- Long-Term Sessions: What they are
- How to Differentiate
- ackack: A Proof of Concept
- Fun Games the Whole IEEE 802 Family can Play

About me

- Wholepoint, 2001
  - or, how I ARP Poisoned my 20's
  - Internal network security (huh?)
- Mirage Networks
  - From the mind of Gartner sprang NAC
  - Combined pre- and post-admission, full cycle
- Trustwave SpiderLabs
  - Bought Mirage, and me
  - I bugged Nick until he let me in

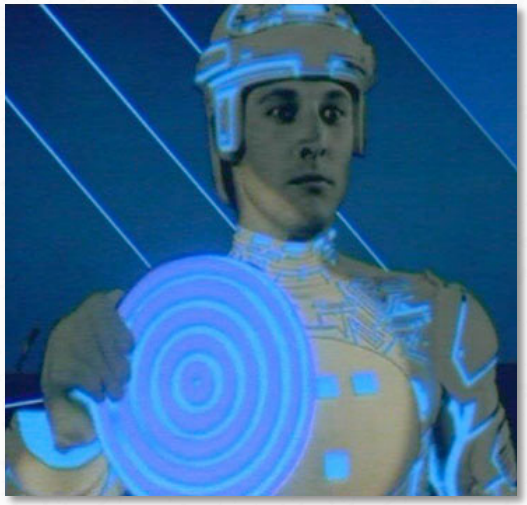
Long-term Sessions

So what?

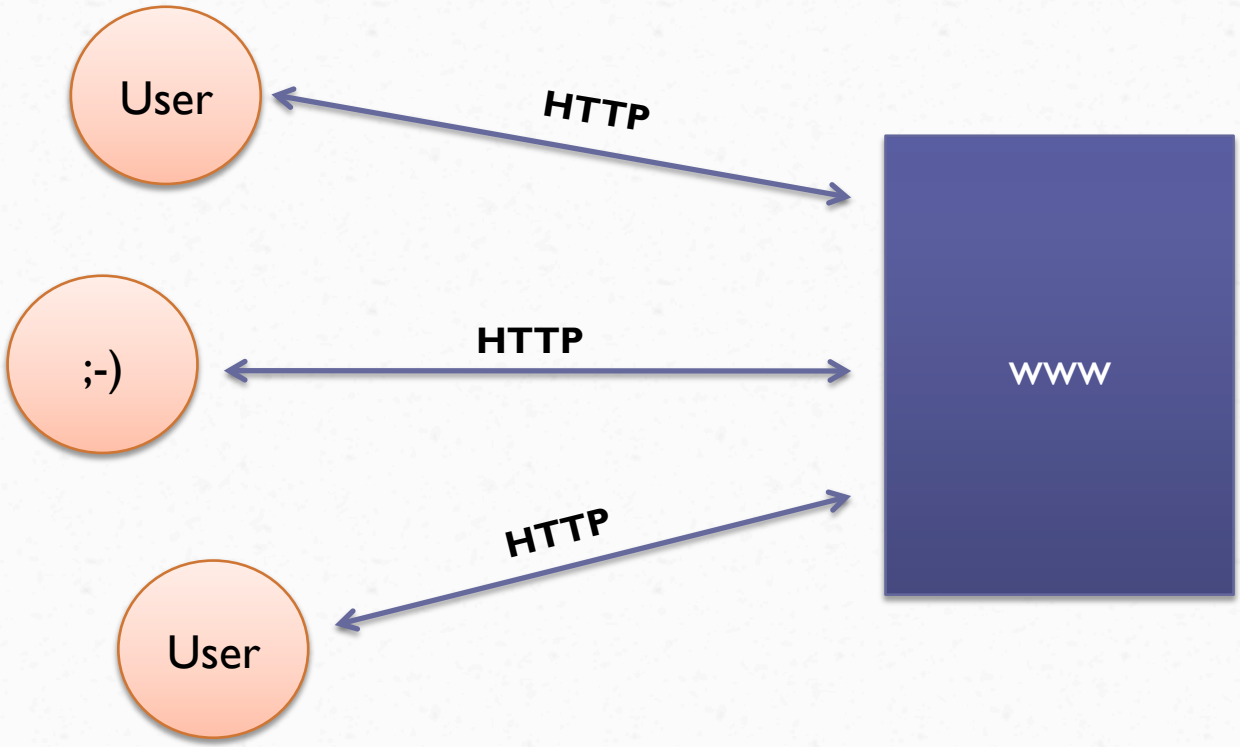


Long-Term Sessions You Don't Want

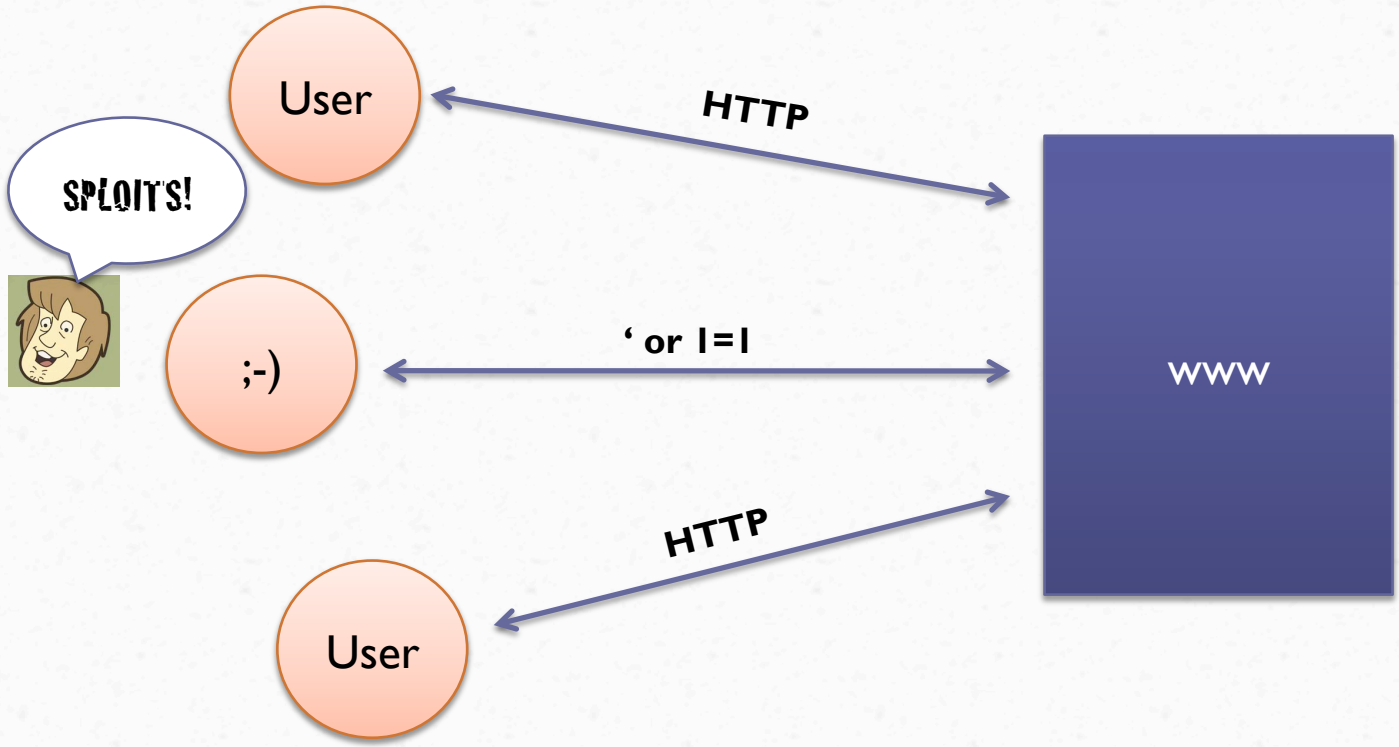
- Bind shells
- Sniffers
- Remote Control
- Virtual Reality connection into your mainframe that allows the kid you fired last month to meet up with his malware and show it how to exploit a timing flaw in the MCP, I mean kernel



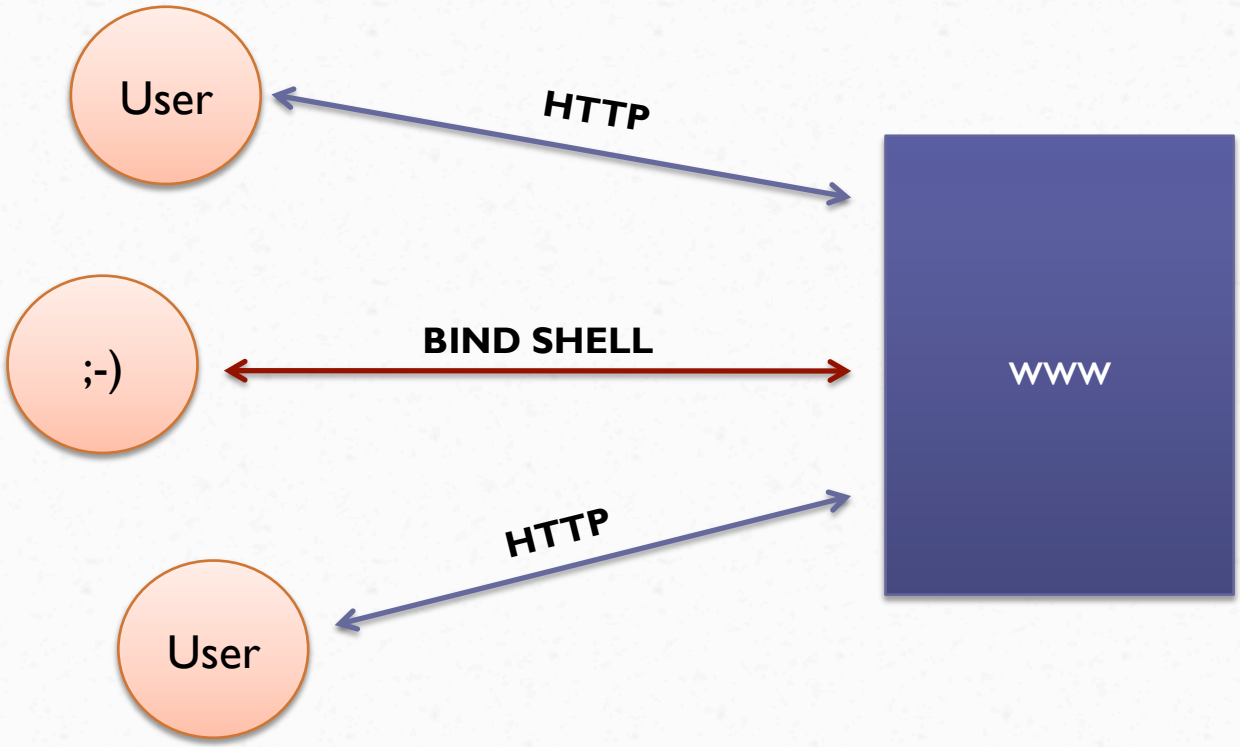
Example



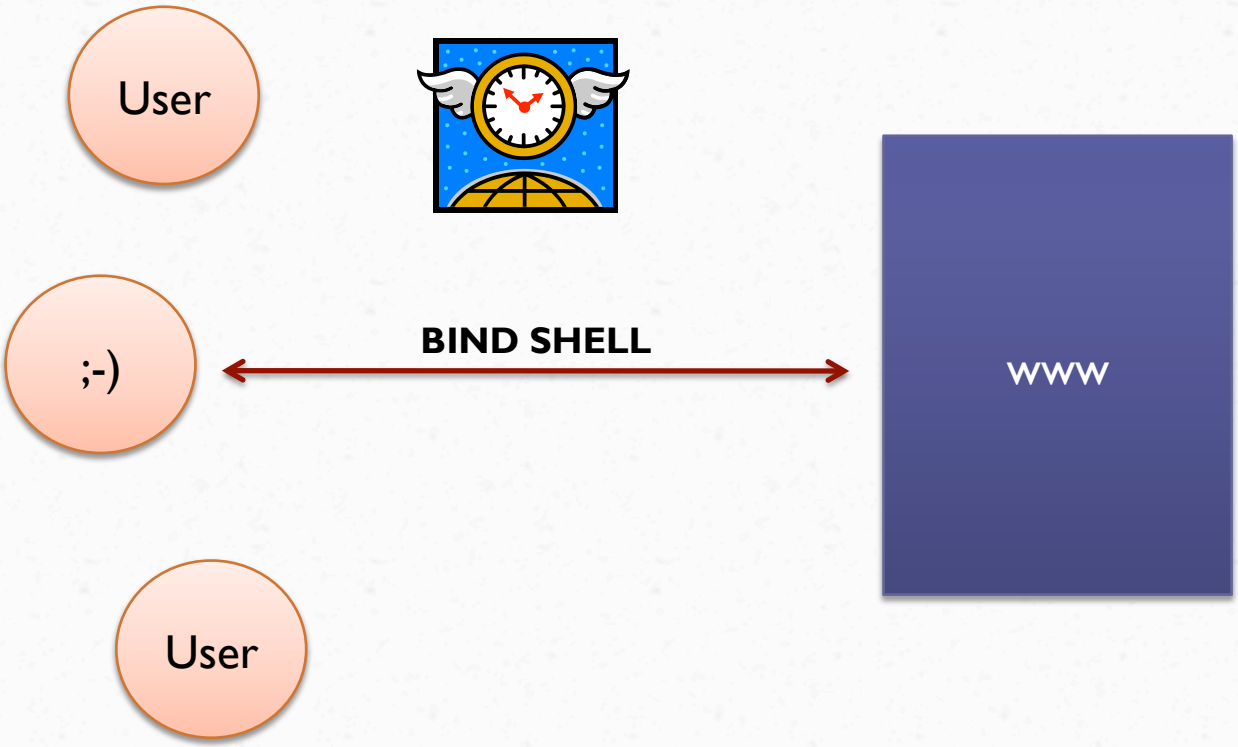
Example



Example



Example

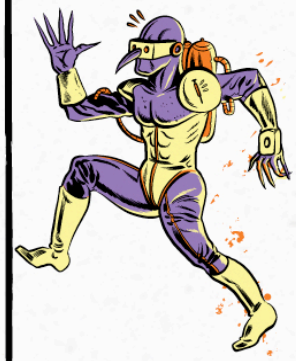


Long-Term Sessions You Might Want

- Instant Messaging
- Large File Downloads
- Streaming Media
- Rich Web Apps (Comet)
- Multi-User Dungeon

But How Do You Tell the Difference?

Differentiating Sessions



Trustwave®

Web App Eat World

"In just one decade, the Web has evolved from being a repository of pages used primarily for accessing static, mostly scientific, information to a powerful platform for application development and deployment."

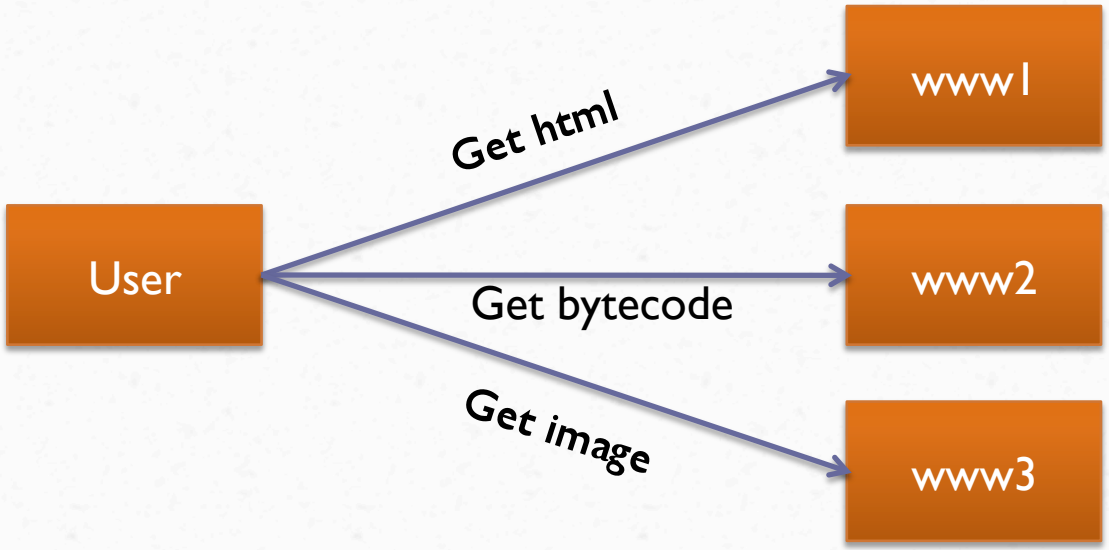
M. Jazayeri, 2007
Future of Software Engineering
IEEE Digital Library

"After more than four years during which peer-to-peer (P2P) applications have overwhelmingly consumed the largest percentage of bandwidth on the network, HTTP (Web) traffic has overtaken P2P and continues to grow. Presently, as a result of streaming audio and video in Web downloads, HTTP is approximately 46% of all traffic on the network. P2P continues as a strong second place at 37% of total traffic.

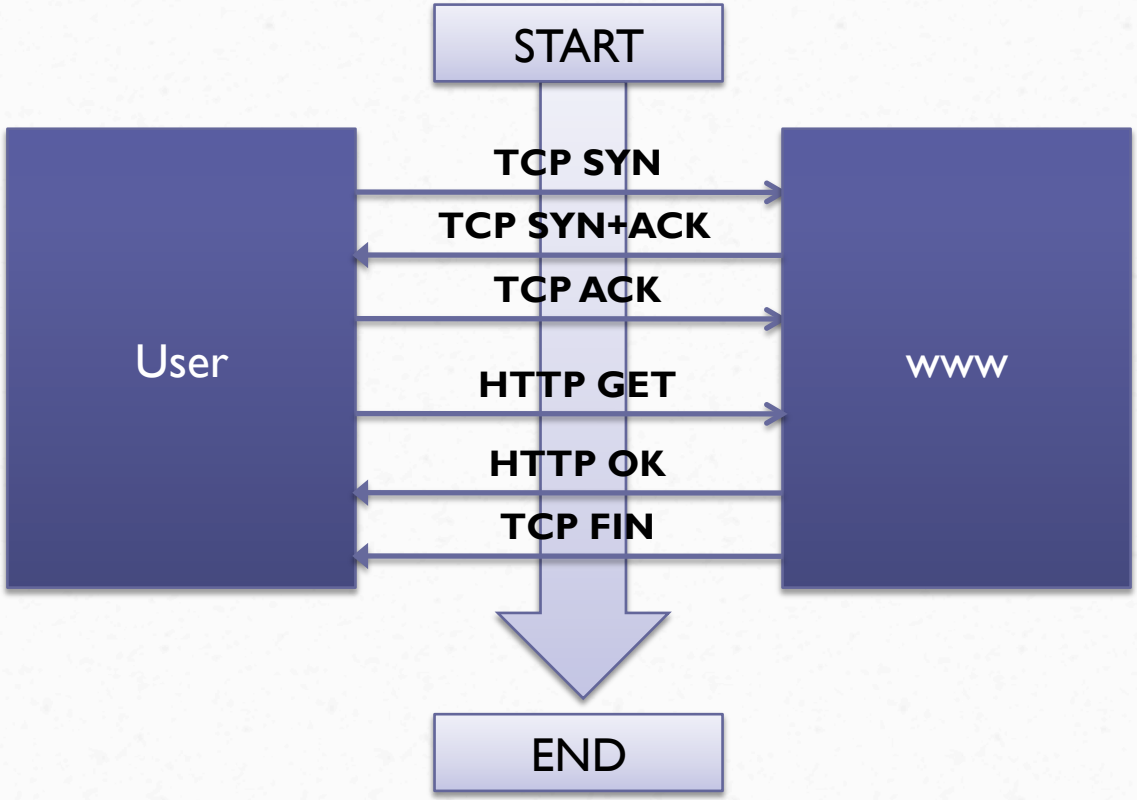
Ellacoya (now Arbor Networks), 2007

Short-Term Sessions

- Majority of Web sessions are terminated within short duration
- Session established, data transferred, session closed



HTTP Session

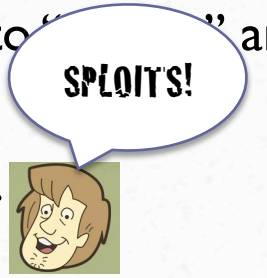


Duration and Source

- Definition of long-term session: "Duration"
  - Could be different for each scenario
    - Web servers ~ 5 minutes
    - File servers ~ 1 hour
    - From Internal to Internet server ~ 10 minutes
  - Helps with signal-to-noise ratio
- Session Source – who started it?
  - Each session needs to be broken down into "Server" and "Source"
  - Normal source: internal user PC's
  - Not-so-normal source: your web server…

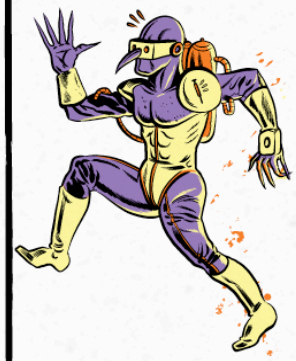
Duration and Source

- Definition of long-term session: "Duration"
  - Could be different for each scenario
    - Web servers ~ 5 minutes
    - File servers ~ 1 hour
    - From Internal to Internet server ~ 10 minutes
  - Helps with signal-to-noise ratio
- Session Source – who started it?
  - Each session needs to be broken down into "[illegible]" and "Source"
  - Normal source: internal user PC's
  - Not-so-normal source: your web server…



Whitelists

- Need to define "OK" long-term sessions
- Common for internal user PC's
- Instant Messaging
- Comet web apps
  - Loose term to describe new ways to do long-term web apps
  - Some use long-term sessions
  - Some use long-polling, unique hybrid approach
- Whitelisting apps can be challenging
  - IM, Comet apps don't use one server, they use clusters
  - IP addresses may change between sessions



Proof of Concept

ackack

Trustwave®

ackack

- Network Sniffer
- Detects new and *existing* sessions
- Allows creation of Policies using Duration and Source criteria

- Groups hosts by IP subnet, range, or WHOIS query
- It calls you "Commander"

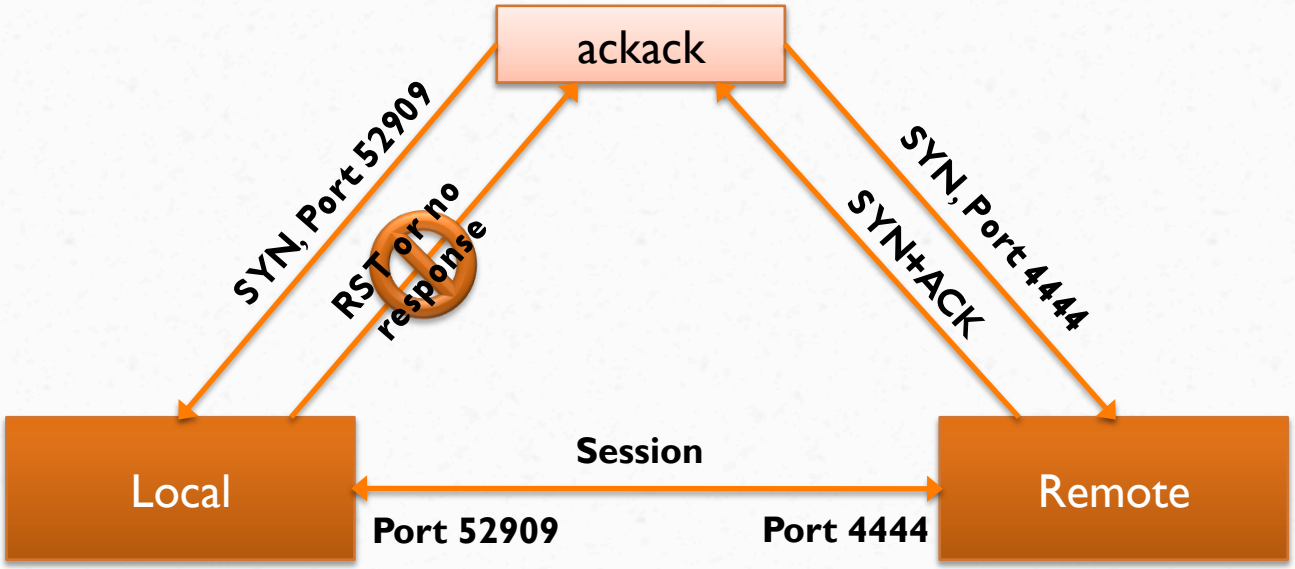
```
-=SESSION MANAGER REPORTING COMMANDER=-
```

Source Detection

- Who started it?
- Only needed for existing sessions (ack, ack)
- Source: initiator of the session
- Server: um, the server
- Port guessing
  - Lower port is the server
  - Actually works most of the time
  - Gets confused on P2P
  - Good last resort
- Port List
  - Checks specific list of ports for server
  - Ports listed in precedence order in case of double-match
  - Still might miss out on P2P, ports picked somewhat at random

Source Detection

- Port Validation
  - Connects to each port (low-to-high order), uses first SYN+ACK as server
  - Pretty darn reliable
  - Adds one packet on the wire for each session guess



Groups

- Used to classify hosts, networks
- Important for Whitelisting
  - "Local PC's can create long-term sessions with AOL IM servers, alert on anything else"
- WHOIS used to include large networks
  - Q: How do you enumerate AIM servers?
  - A: Watch network traffic, use WHOIS feature of ackack to use the net block that contains that IP
  - Q: AOL is an ISP – did I just allow my network to get hacked by AOL users?
  - A: *Generally speaking*, net blocks that support apps such as AIM do not intermingle with IP's given to users.
  - Do your own WHOIS query for more info about business unit associated with IP before plugging into ackack

Policies

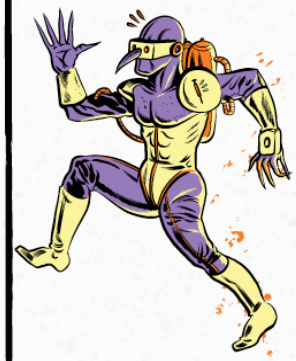
- Define "interesting"
- Format:

```
Source: {Server: Duration, Server: Duration …}
```

- For each Source, sessions with these Servers for this Duration should generate alerts
- Source and Server are both Groups
- Use "X" to specify "undefined"

Usage Examples

What do I do with it?



Trustwave®

As a counter-measure

- Can be used to watch network for abnormal sessions
- Connect to mirror port, monitor session, network tap, etc. for more visibility
  - Proof-of-concept code, please send performance numbers ☺
  - Uses a really cool C event loop (EV), but it's slacker Perl code nonetheless
  - Packet drops reported by Session Manager
- Use Policies, Groups to report interesting sessions
- As valid sessions are discovered, tweak policy and repeat

Example

- Goals
  - Servers
    - Alert each time a session is established for more than 5 minutes
    - Alert each time a Server initiates a session
  - Inside
    - Alert when a session is established more than 10 minutes
    - Exclude sessions with AIM
- Groups
  - Servers: 169.254.20.5-169.254.20.10
  - Inside: 192.168.1.0/24

Example Groups

group.yml

```
---
Inside:
  - 192.168.1.0/24
Servers:
  - 169.254.20.5-169.254.20.10
# WHOIS queries
AIM:
  - (64.12.24.218)
  - (205.188.248.151)
```

Example Policy

policy.yml

```
---
# Alert when somebody inside opens session with unknown host
# more than 10 mins
Inside: {X: 10}
# Alert when unknown host opens session with server > 5 mins
X: {Servers: 5}
# Servers shouldn't initiate sessions
# It smells of sploits
Servers: {X: 0, AIM: 0}
```

As a pentesting tool

- It's a sniffer, can be used with ettercap, etc.
  - ARP Poison and run to see sessions
- Set "report_all" to 1 in config.yml
  - Shows all connections, not just alerts
- Look for connections being made to the PCI zone, setup alerts
- Use Groups to organize Source and Servers

Example Groups

group.yml

```
---
PCI:
  - 10.10.1.0/24
  - 10.10.2.1-10.10.2.10
Local:
  - 192.168.1.100-192.168.1.254
# These are just labels for visual cues
Printers:
  - 192.168.1.10-192.168.1.20
Mail:
  - 192.168.1.5
```

Example Policy

policy.yml

```
---
# Alert when Local talks to PCI environment
#
# Also when Local makes long-term connection to outside
# Might be interesting IM, webmail, or something
# (Or someone's already been here!)
Local: {PCI: 0, X: 10}
# This would be wrongish
PCI: {Local: 0}
```

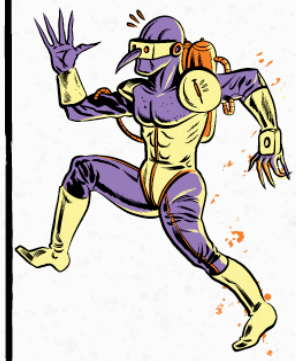
Notes / Bugs / Excuses

- It's Perl, but there are PAR binaries in bin/ for Win32, Linux, MacOS
  - Should work on other platforms if you can compile modules
  - Most exotic is EV, used by AnyEvent for event loop
- Groups shouldn't overlap yet
  - Hash order is like a box of chocolates…
- Source guessing in place, validation is soon
  - Lowest port is server, might suck at P2P
- I was drunk about 50% of the time

Did I run over?

Thanks guys

Steve Ocepek
glassjoe@fastmail.net
socepek@trustwave.com
http://www.trustwave.com/spiderlabs



Trustwave®