Flow Analysis for Network Situational Awareness

Tim Shimeall

January 2010

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

What We Will Cover

Introduction

Your Network

- Fundamentals of networks, flow, and protocols
- Malicious traffic

External Events & Trends

- Malware
- Networks in the Broad

Working Together

- Network dependencies
- Analysis

Summary

What this class is

Approaches, methods, trends of interest in building network situational awareness

Big picture view of analysis

Assumes you have good handle on analysis tool suites

What this class is not

Cool tricks with SiLK

Installing and using SiLK

Everything you need to do analysis

Bits and bytes on the wire

A couple of rules…

ASK!

No smoking/chewing

Cell phones on stun

No smelly food

Recognition Stances

Definition

The systematic gathering, analysis and interpretation of data from local and remote networks regarding structure, applications, traffic and resources to produce actionable information for decision making in network operations and defense. *(Shimeall, 2008)*

Network Situational Awareness

Alternate Definitions

Situation Awareness (SA): “The perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future." (Endsley, 1988)

Network SA: “the operational picture that consolidates all available information that is actually needed for identifying attacks and for selecting and applying appropriate countermeasures.” (Kemmerer et. al., 2008)

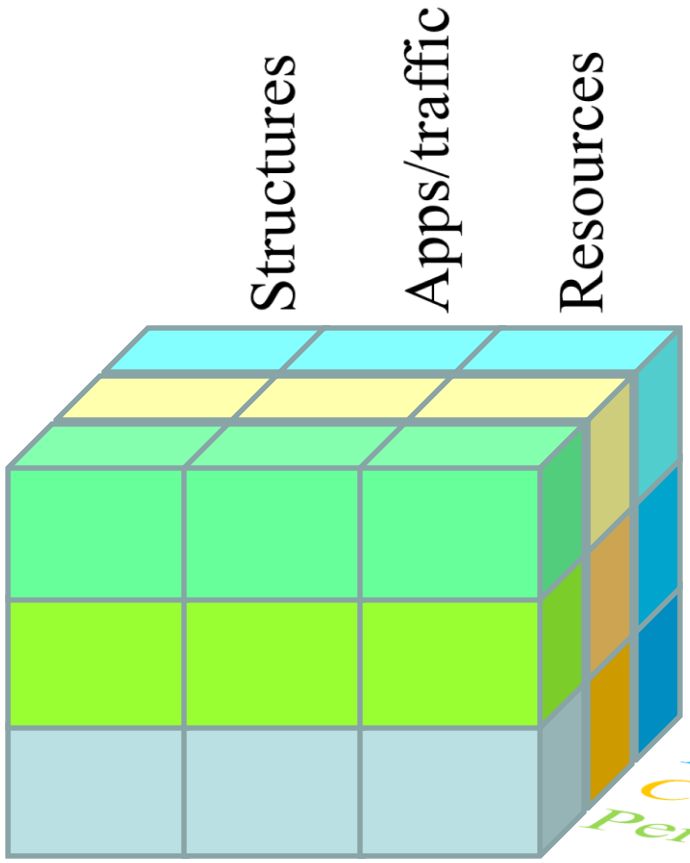
Network Situational Awareness Practice

Know your network

Know current external events and trends

Know how they fit together

How these Definitions Apply



Know Network

Know Events/Trends

Know How They Fit

Predict
Comprehend
Perceive

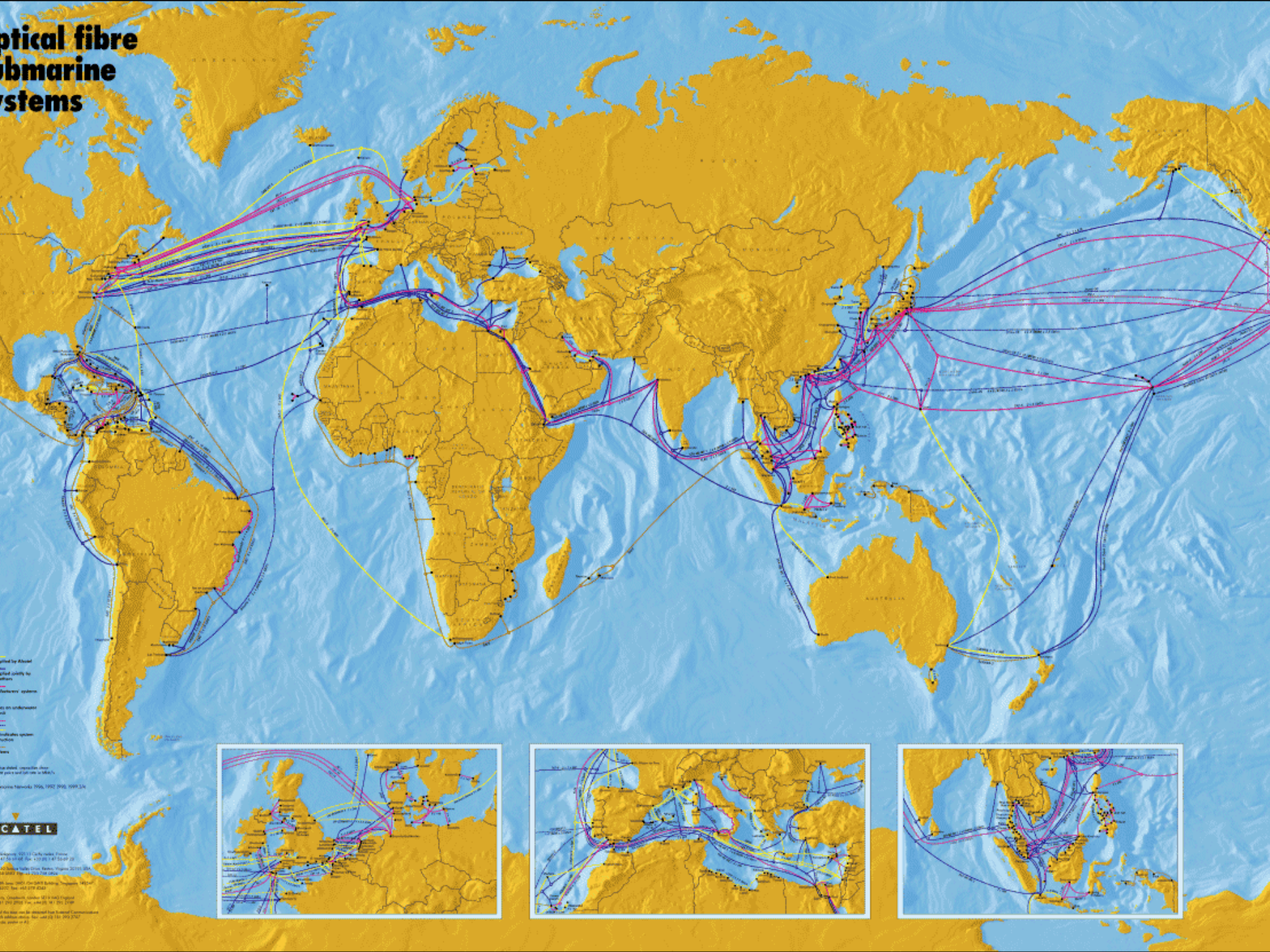
Vulnerability Note VU#800113

Multiple DNS implementations vulnerable to cache poisoning

- http://www.youtube.com/watch?v=XDKw8ny6IcM#

July 2008

ptical fibre
ubmarine
ystems



CATEL

Estonia, April 2007

The 2008 Olympics

USA TODAY Home News Travel Money Sports Life Tech

News » World ▪ Troop deaths in Iraq

Internet sites still blocked for Olympic reporters

Updated 7/30/2008 10:34 PM | Comments 45 | Recommend 8

E-mail | Save | Print | RSS

Enlarge By Oded Balilty, AP

A foreign journalist uses Internet services provided at the Main Press Center Tuesday in Beijing. After promising the Internet will be uncensored for journalists during the Olympics, the IOC delivered a stark clarification on Tuesday, saying many Internet sites will be blocked under controls applied by China's communist government.

BEIJING (AP) — Olympic organizers are backtracking on another promise about coverage of the Beijing Games, keeping in place blocks on Internet sites in the Main Press Center and venues where reporters will work.

STORY CORRECTION: Ebersol's comments mischaracterized

The blocked sites will make it difficult for journalists to retrieve information, particularly on political and human rights stories the government dislikes. On Tuesday, sites such as Amnesty International or any search for a site with Tibet in the address could not be opened at the Main Press Center, which will house about 5,000 print journalists when the games open Aug. 8.

"This type of censorship would have been unthinkable in Athens, but China seems to have more formalities," said Mihai Mironica, a journalist with ProTV in Romania. "If journalists

Mixx it

Other ways to share:

Yahoo! Buzz

Digg

Newsvine

Reddit

Facebook

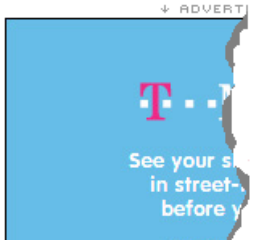
What's this?

uly 30, 2008 2:01PM; Updated: Wednesday July 30, 2008 7:18PM

es still blocked for reporters

lympic organizers are backtracking on
about coverage of the Beijing Games,
blocks on Internet sites in the Main
venues where reporters will work.

The blocked sites will make it difficult for journalists to retrieve information, particularly on political and human rights stories the government dislikes. On Tuesday, sites such as Amnesty International or any search for a site with Tibet in the address could not be opened at



Questions of Interest

Is my bandwidth increasing from business-related activity, or from non-work related activity?

How will my business be impacted by implantation of more stringent security policy?

If my backbone Internet Service Provider chooses to de-peer with another backbone provider, how will I be affected?

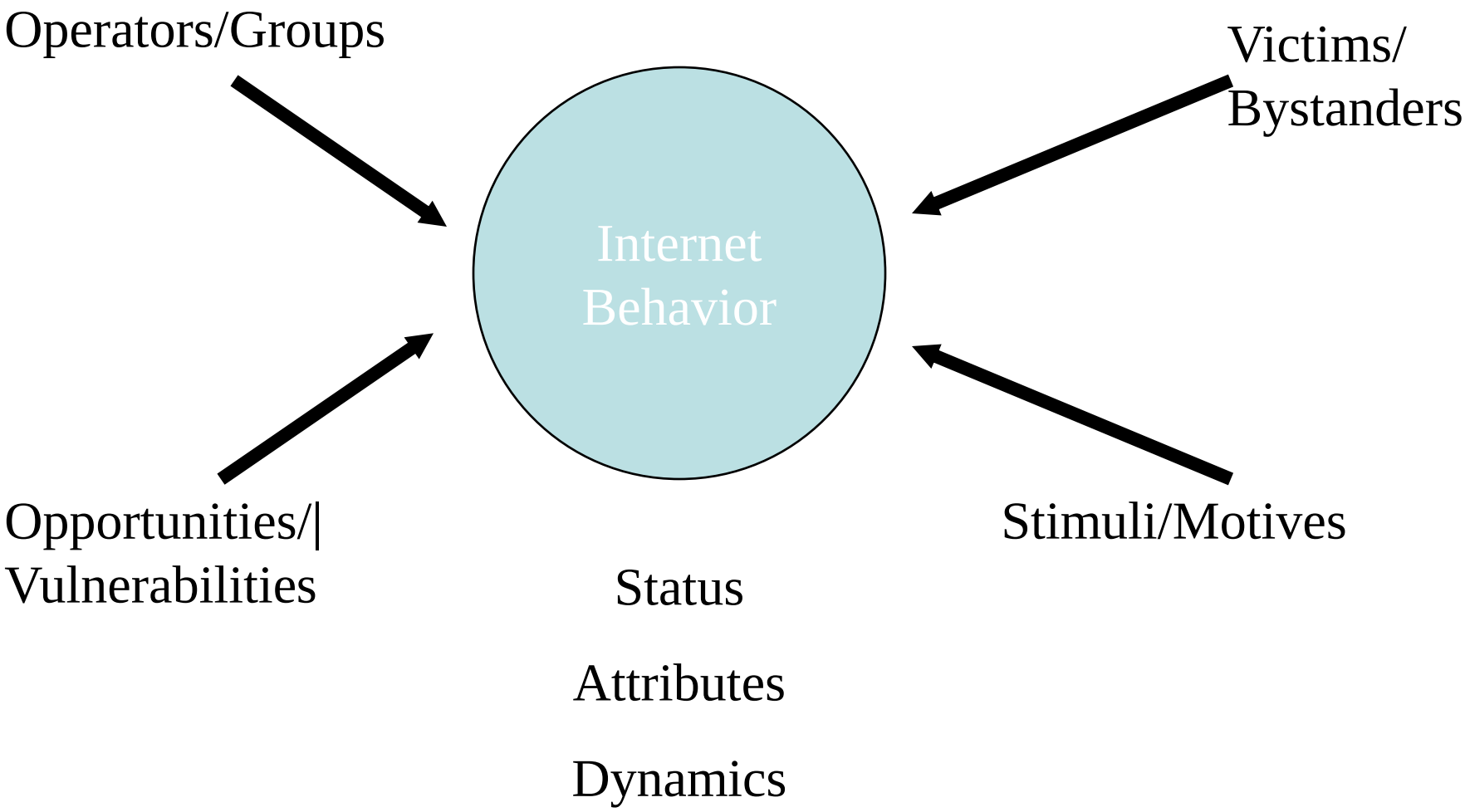
How will socio-political uprisings impact my network?

What are the most important dependencies my network has with external resources?

Do computers on my network follow policy?

Can my network survive a distributed denial-of-service attack? How can I prioritize resources during a bandwidth-limiting attack?

Building Understanding



Challenges to Analysis

- Gathering sufficient datasets to make statistically valid judgments
- Developing automated technical analysis tools
- Developing a reliable methodology for cyber-analysis
- Overcoming organizational bias against sharing information

Network Fundamentals

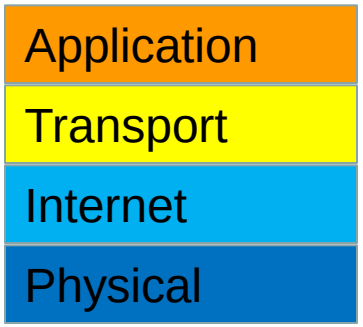
What We Will Cover

- Introduction
- Your Network
  - Fundamentals of networks, flow, and protocols
  - Malicious traffic
- External Events & Trends
  - Malware
  - Networks in the Broad
- Working Together
  - Network dependencies
  - Analysis
- Summary

The Internet

Internet: Network of Networks

- Connected by routers, no central control
- Using common set of protocols



Internet Protocol (IP)

- flexible routing of information from source to destination

Transmission Control Protocol (TCP)

- Sequencing of series of packets to transmit data reliably over Internet

Other protocols running on top of IP:

- UDP – one-directional burst of packets
- ICMP – network management protocol
- BGP – Router protocol
- IPSEC – VPN traffic

How IP Works

Packet switched:

- Flow of information broken into chunks
- Each routed independently by best route to destination
- Destination must reassemble into correct order (offset)

Internet Address:

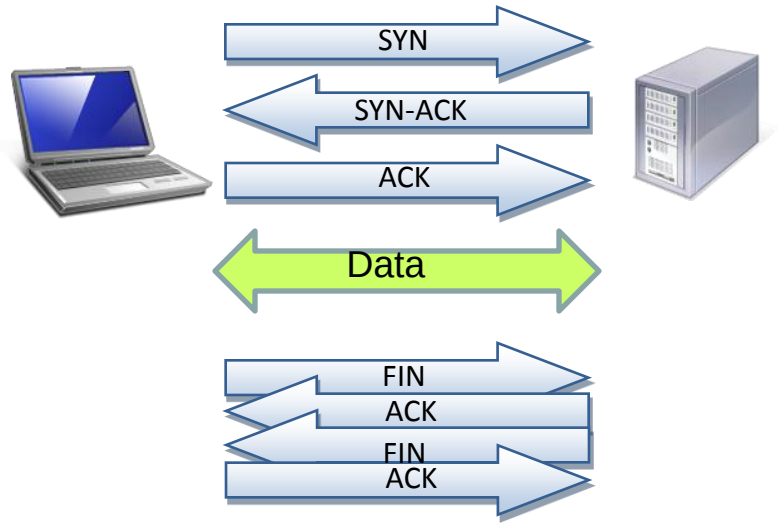
- Logical network (location) & Logical host (identity)
  - Subnet masking & CIDR blocks
- V4 (1982) -- current version (32 bit addresses)
- V6 (1999) -- forthcoming version (128 bit addresses)

How TCP Works

Header added to packets

Connection: IPs and ports

- Service port
- Dynamic port



Initial handshake

- SYNch sequence numbers (assembly/retransmit)
- ACKnowledge SYNch
- ACK (with data)

Termination

- FINalize/ ACK FIN
- ReSeT/ no ack

Application Protocols

On top of TCP and UDP (mostly)

Sequences of packets to support common applications

- SMTP
- HTTP
- HTTPS / TLS
- DNS
- Others?

Simple Mail Transfer Protocol

- TCP/25 by default
- Transfer-agent based
- Text Protocol
- Single connection, multiple messages (maybe)
- Easily forged

S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: Alice Example <alice@example.com>
C: Date: Tue, 15 Jan 2008 16:02:43 -0500
C: Subject: Test message
C: Hello Alice.
C: Your friend, Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye {The server closes the connection}

Example from wikipaedia.org

HyberText Transfer Protocol

TCP/80 or TCP/8080

Vast bulk of traffic

Request/Response

Stateless (almost)

Requests:

request-line
headers (host)
empty line
optional message

Request-line:

- GET url
- PUT url
- HEAD url
- DELETE url
- TRACE url
- OPTIONS
- POST url
- CONNECT

Response:

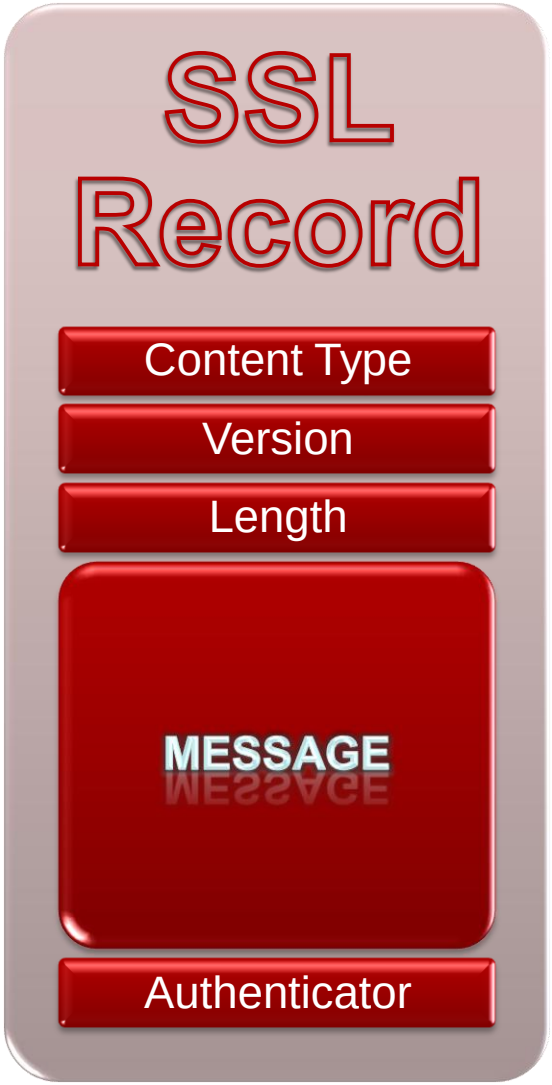
Status line (404, 200)
Message (data)

SSL Record Format

There are four content types:

- Handshake, 0x16
  - Negotiate encryption capabilities
- ChangeCipherSpec, 0x14
  - Flag the recipient that the encryption scheme has changed
  - Prereq is a successful handshake
- Application, 0x17
  - The bulk of the data transfer
- Alert, 0x15
  - Errors and warnings

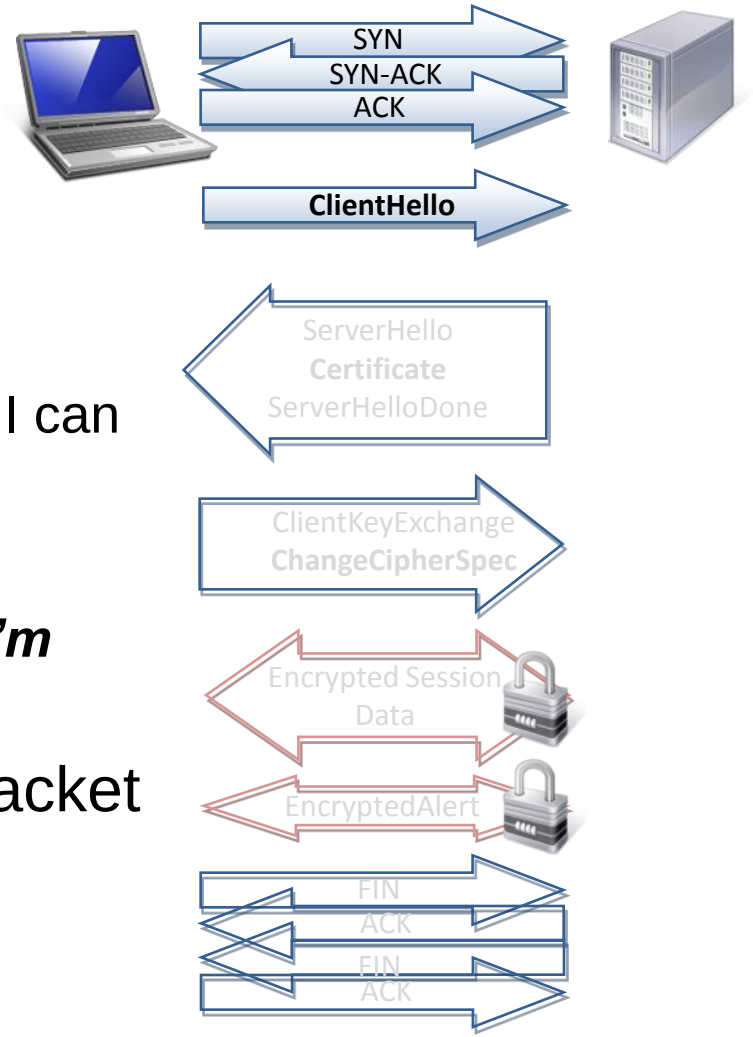
Regardless of content type, the ***message*** is always encrypted with the current session state



SSL Client Hello

What happens when a client connects to an SSL server?

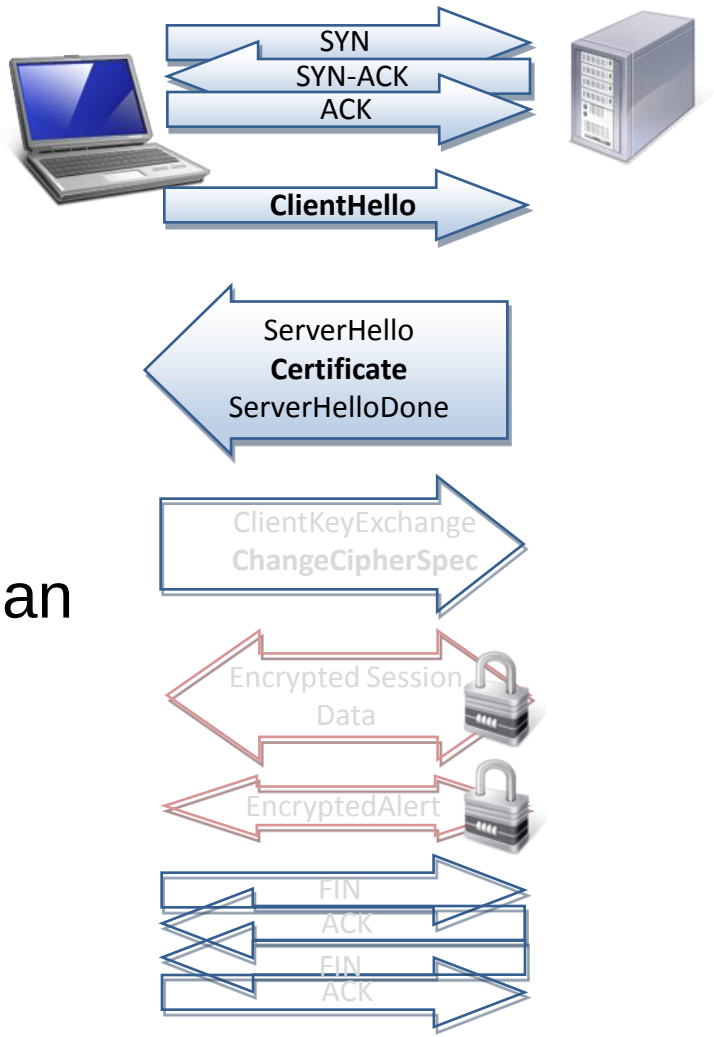
- 3-way handshake
- Client sends hello
  - These are the encryption ciphers I can handle
  - Here's a random seed number
  - ***Here's the name of the server I'm trying to connect to***
- The client hello all fits in one packet



SSL Server Response

Server replies to the client

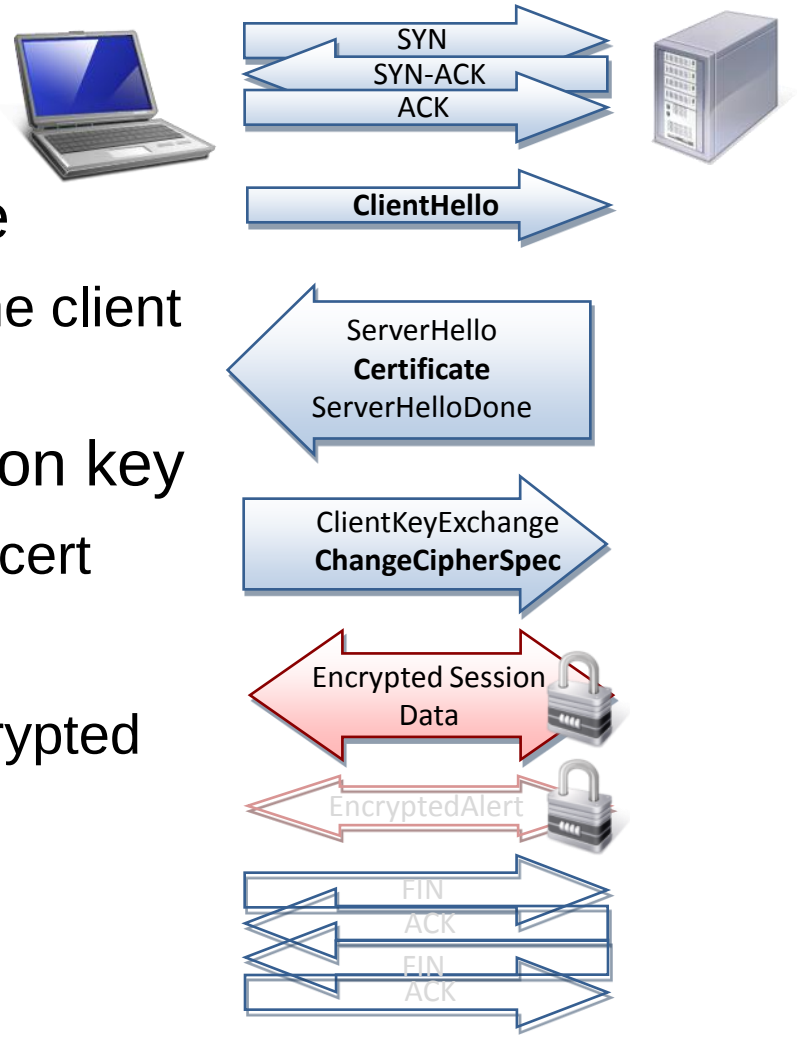
- Server sends “Hello”
  - Encryption and seed
- Server sends its certificate
  - public key and usually cert chain
- Server sends “Done”
- Response usually takes more than one packet



SSL Client Response

After the server is done:

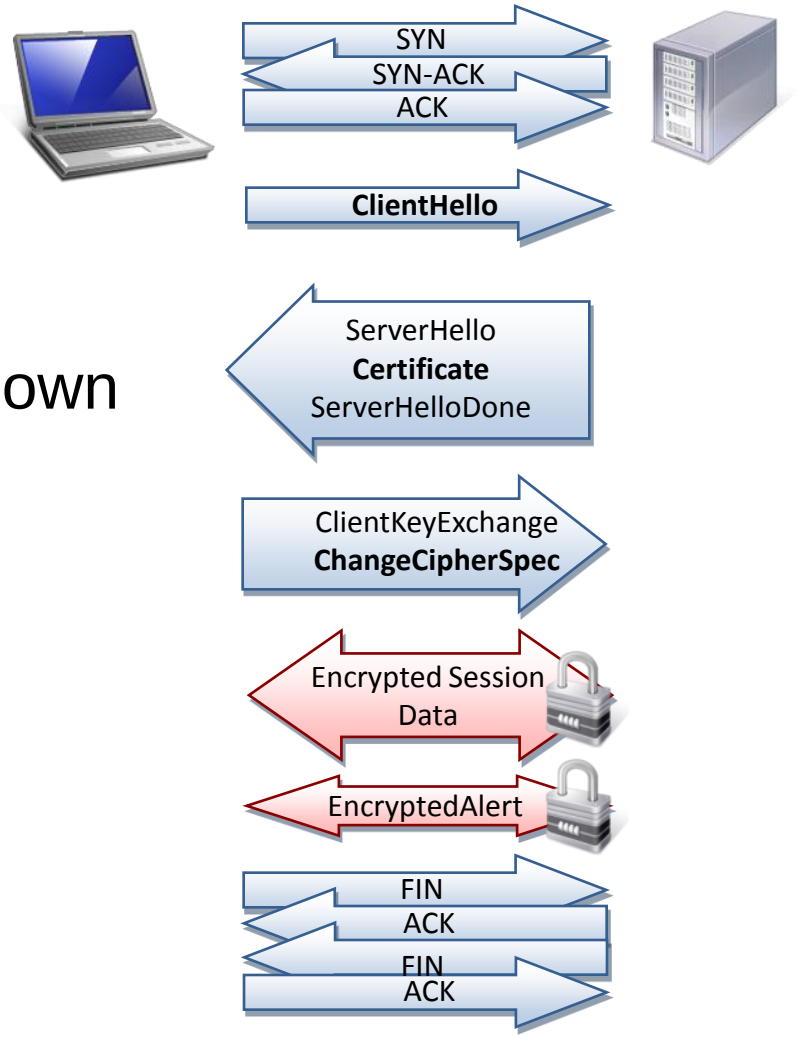
- Behind-the-scenes, the client validates the certificate
  - This only generates traffic if the client needs an updated CRL
- The client exchanges a session key
  - The key is encrypted with the cert
- `ChangeCipherSpec`
  - From now on, all traffic is encrypted



SSL Session Teardown

When they're done

- Someone issues an alert
  - It's encrypted, so we can't tell anything about it
- The TCP connection is torn down



Domain Name System

More than just hostname → IP

Query hierarchy of nameservers

- Local nameserver (resolver): answer from cache or preloaded resolutions, may do recursive queries
- Authoritative nameserver: answer based on domains it covers, or recurse
- Root nameserver: answer top-level, delegate, or generate errors

DNS protocol

UDP/53 or TCP/53

Client queries local (address, ptr, mx, ns, hinfo, any)

Local responds from cache or queries to root

Root responds with referral to TLD or error

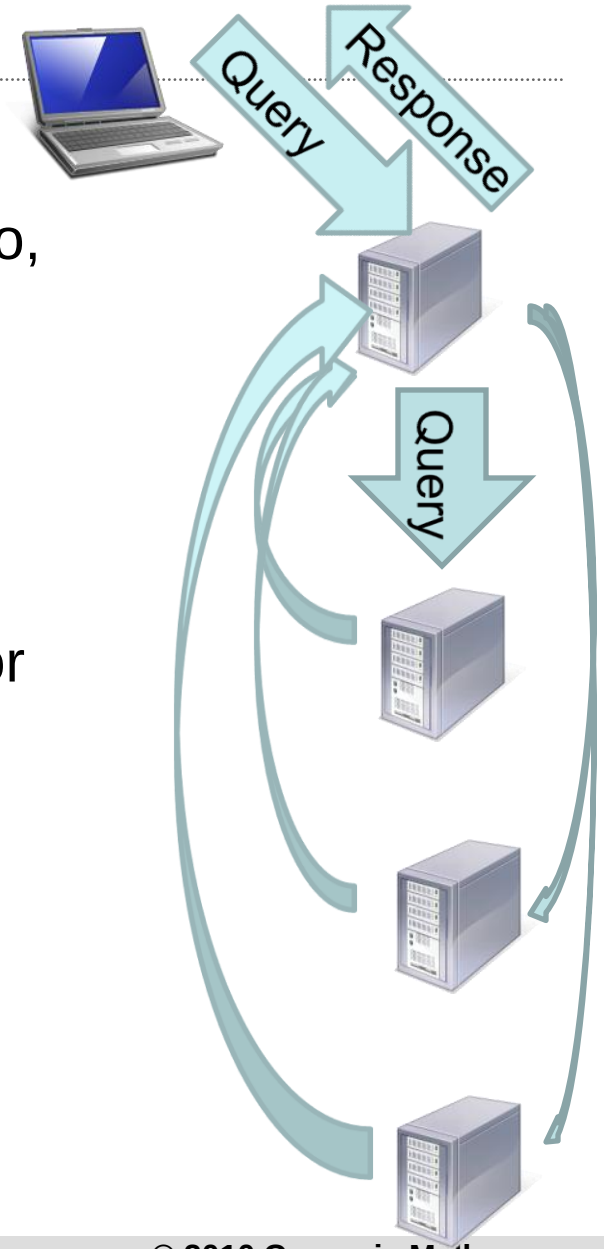
Local queries TLD

TLD responds with referral to authority or error

Local queries authority

Authority sends answer

Local sends answer



Other Protocols

Wikipaedia is your friend!

Want to know:

- Sequence of messages
- Packets/message
- Size range of packets
- Service ports/protocols
- Other application protocol characteristics

Peer to Peer

Cloud discovery

- Fumble (past sites)
- Service ports
- Registered sites

Join

Export data (often stream)

Import data (often slow)

Why do We Care?

Know your network

- Services, servers
- Dependencies

Know your threats

- Open vectors
- Non-protocol on service ports
- Signalling/Beaconing

Malware and Malicious Traffic

What We Will Cover

- Introduction
- Your Network
  - Fundamentals of networks, flow, and protocols
  - Malicious traffic
- External Events & Trends
  - Malware
  - Networks in the Broad
- Working Together
  - Network dependencies
  - Analysis
- Summary

Malicious Traffic

Scanners

Worms/Viruses

DDos/Backscatter

Spam/Response

Backdoors

A taxonomy of Attributes

Backscatter: Few sources, scattered evenly across network, generally contains RST or ACK flags.

Scans: Single source, usually strikes the same port on many machines, or different ports on the same machine

DoS: Multiple sources, single target, usually homogenous (but no requirement). May be oddly sized

Worms: Scanning from a steadily increasing number of hosts

Key Servers: Identifiable by IP addresses (e.g. Hotmail)

Step 1: What does scanning look like?

Scanning generates a lot of flows, if there is any scanning, the noisiest is probably the scanner.

So, we want to find the noisiest IP, refilter (or count by IP and/or port)

Use what we know about how the protocol behaves as well. (TCP, for example)

How many packets in TCP prior to sending data?

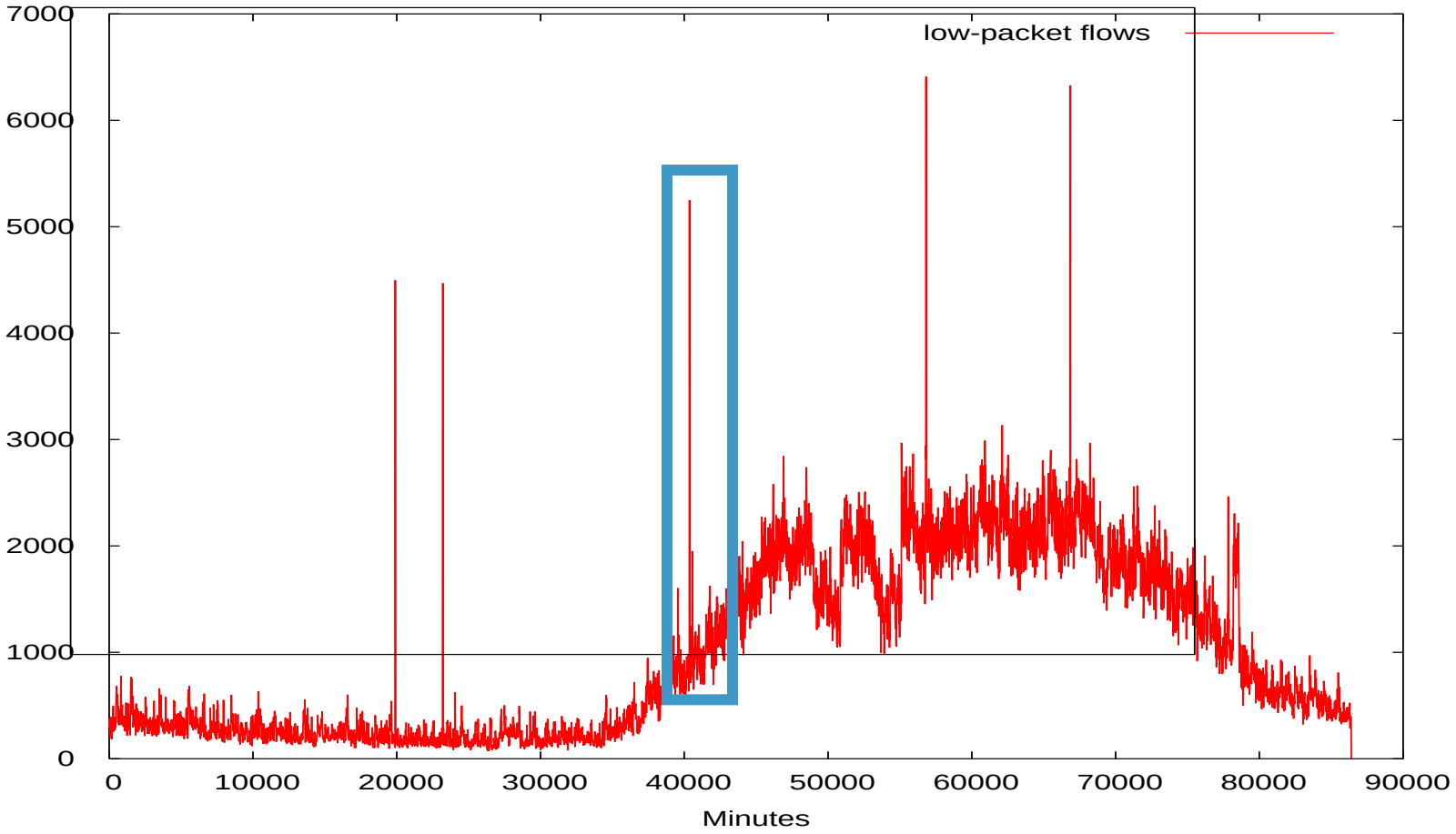
How many bytes in a TCP packet if there's no data?

What's TCP do if it can't connect the first try?

What SiLK tools can count by IP?

What traffic goes to addresses with no host?

Find the Scan



Step 2: Discerning what spikes are

Use rwstats and look at the busiest source IP addresses

In general, there will be a small number of addresses with a large number of packets

- Those are usually scanning, or worms, or similar
- Although it could be hotmail

Step 3: Checking vulnerabilities

In general, you are looking at scan data after the fact.

Next step is to determine what the scanner found.

Reverse the query using IP Sets

Step 3: Checking Vulnerabilities (ii)

Build a set of all the targets that the scanner visits

Use this set as the source IP's and the scanner's IP as the destination IP on the opposite direction of traffic

Profile the flags and the responses

- Who SYN|ACK'd?
- Who RST?

Measuring Worm Propagation

When looking for a worm you'll usually have a profile

- Target ports hit, packet size, etc.

In those cases, you can use tools like rwfilter and rwstats for accounting rather than discovery

- Worms usually result in an increase in service activity, especially if the service is relatively low-traffic (I.e., not web)

DDoS Analysis

DDoS = **D**istributed **D**enial **O**f **S**ervice

Crude, mechanical attack where some number of subverted clients overwhelm a target

- Does *not* have to be spoofed
- Does *not* have to be a SYN Flood
- Does *not* have to involve garbage traffic

Can strike at different layers of the stack

- SYN Floods: hit TCP
- Other floods will affect router, IP traffic

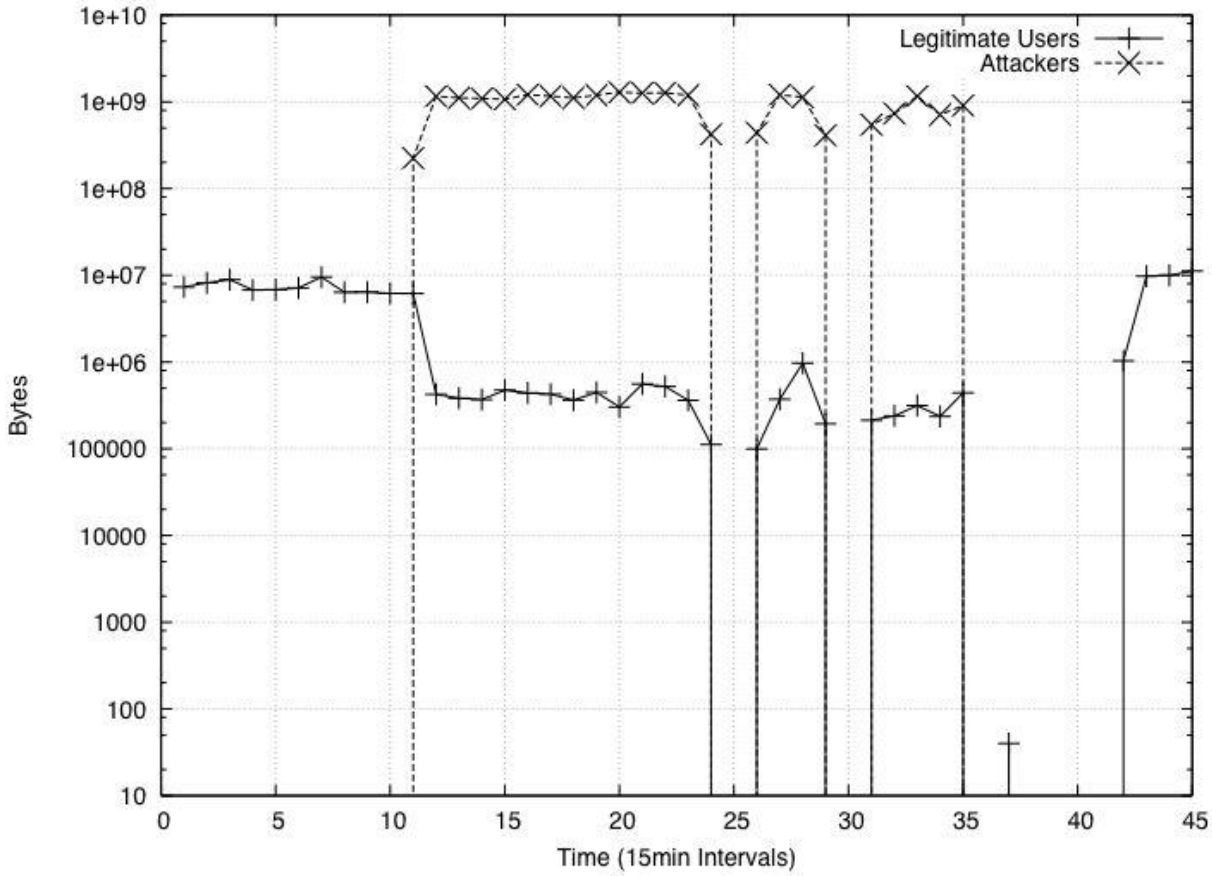
DDoS Analysis

First step will involve identifying and plotting the traffic

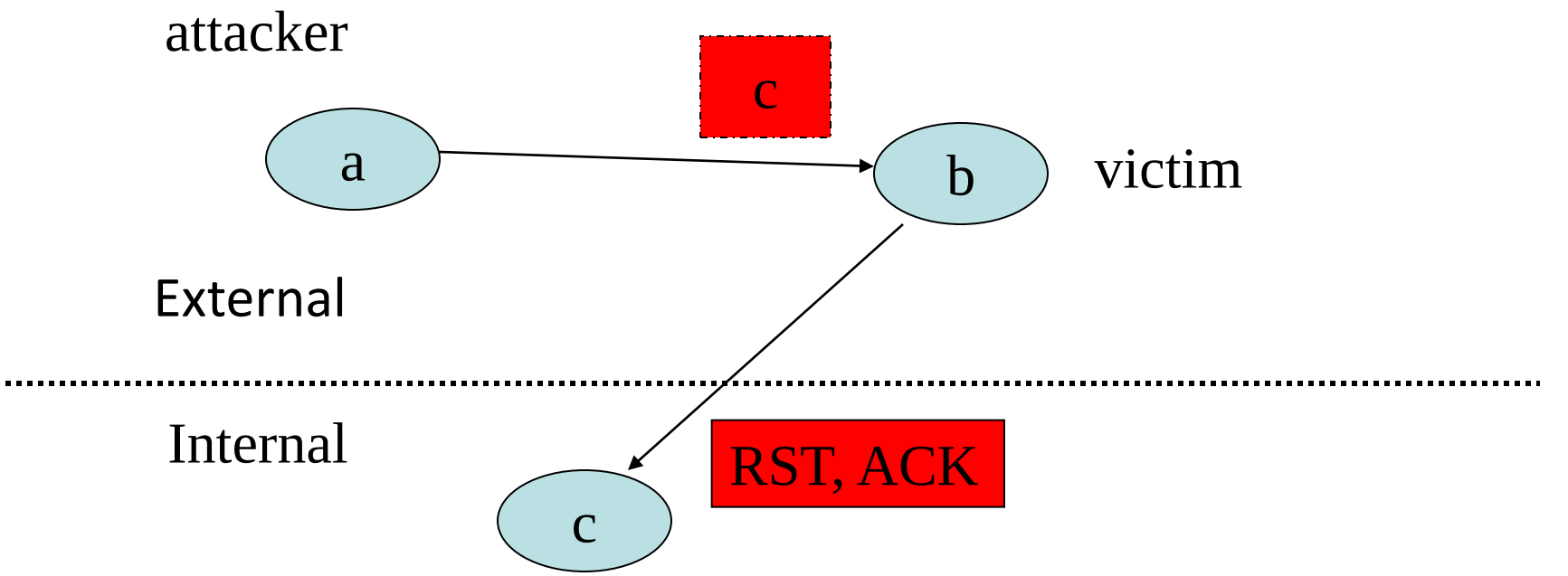
- DoS generally is not subtle (can't afford to be in several cases)
- Various plots are useful:
  - Traffic volume over time
  - Number of clients visiting target over time

In an ideal world, should be obvious

DDos



Backscatter

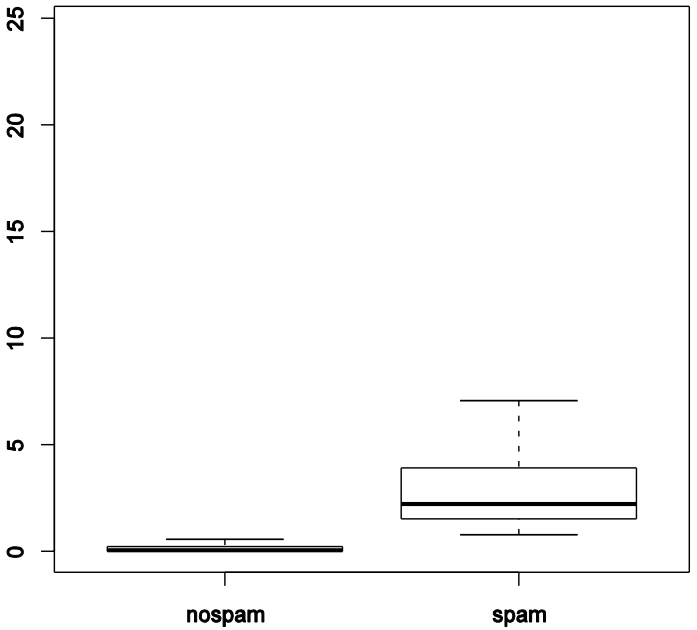


Spam

Rate (the main one)

Locality

Exclusivity



Responses to Spam

About 0.1% of spam gets response

Most spam responses not email

Can detect spam flows, then look for non-automated replies to spam flows

Suspicious destinations

- Alleged criminal connections
- DHCP pools
- ADSL pools

What We Will Cover

- Introduction
- Your Network
  - Fundamentals of networks, flow, and protocols
  - Malicious traffic
- External Events & Trends
  - Malware
  - Networks in the Broad
- Working Together
  - Network dependencies
  - Analysis
- Summary

Purpose of Modern Malware

Steal information (key logging, screen scraping, DNS redirection, etc.)

Commandeer system resources (launch DOS, relay network traffic, spam, etc.)

Propagate

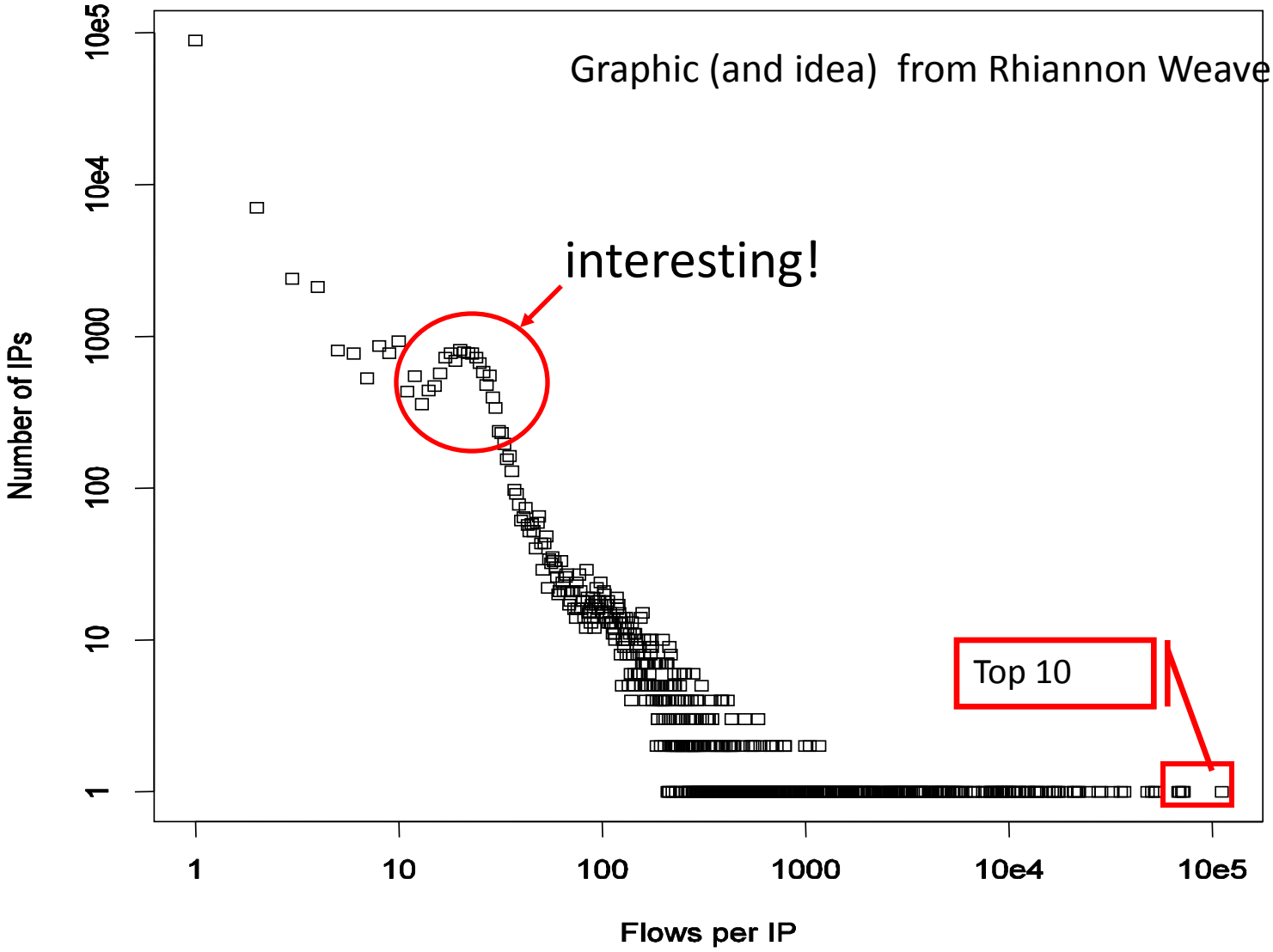
Locate and kill security programs and competing malware

Hide

Methods of Modern Malware

- Most not novel
  - Derived from base of existing code
    - Borrow from other malware
    - Borrow from tutorial examples
  - Change command and control channel
  - Slightly adjust obfuscation scheme
- Where novel, closely held
  - Avoid antivirus
  - Block competitors

Top N isn't everything



Malware and the Internet

- Propagation (dealt with previously – violations of locality; finding scans)
- Receiving commands
  - C&C site
  - C&C channel
  - Downloads (loading more malware)
- Executing commands
  - DOS detection
  - Data exfiltration drop site
  - Fraud artifacts

C&C Site

- Beaconing
  - Regular contact
  - Outside of expected port range
  - Not otherwise explained
- Violations of locality
  - C&C site is a compromised host; not regular contact
- Violations of rationality
  - Not in customer/user area
  - Unexpected server location
  - Warning: Porn, low-end commerce, tourism sites
  - Peer-to-Peer overuse

C&C Channel

- IRC – not human-originated chat
  - Very short contacts (1-2 packets)
  - Somewhat regular contacts
  - Malware authors rely on encryption and obfuscation
- DNS – no follow-on contact activity
  - Disguise beacon as lookup
  - Disguise C&C message in body of response
  - But domain doesn't actually exist, so follow-on contact doesn't happen

Downloads

Not usually assorted with normal mechanisms

- Web, ftp, etc.

High-port to high-port connections

- Above 10,000
- With content
- Short duration
- From unusual contact

Executing Commands

- Outbound scanning
- Outbound Ddos
  - Frequency of contact
  - Diversity of ports/protocols
  - Site outside of locality
- Data exfiltration is file transfer
  - High-to-High ports
  - HTTP outbound data from client
- Fraud artifacts
  - Pay-per-view
  - Pay-per-click
  - Pay-per-install

External Sources of Situational Information

- CERT: http://www.cert.org
- CVE Database - http://www.cve.mitre.org/
- Internet Storm Center - http://isc.sans.org/
- SecureWorks Research & Threats - http://www.secureworks.com/research/
- DefCon - http://www.defcon.org/
- Microsoft Security - http://www.microsoft.com/security/default.mspx

Leading Questions

What service is being hit?

What protocol is being used?

Are there several protocols in use?

How many packets?

How large are the packets?

How long is a session?

Any beaconing?

Spreading phase vs. Quiet phase Vs. Active phase?

Networks in the Broad

What We Will Cover

- Introduction
- Your Network
  - Fundamentals of networks, flow, and protocols
  - Malicious traffic
- External Events & Trends
  - Malware
  - Networks in the Broad
- Working Together
  - Network dependencies
  - Analysis
- Summary

Why the Internet Works

Peering and Hosting

Partial compliance with standards

Partial trust

What this all means to network situational awareness (and your network)

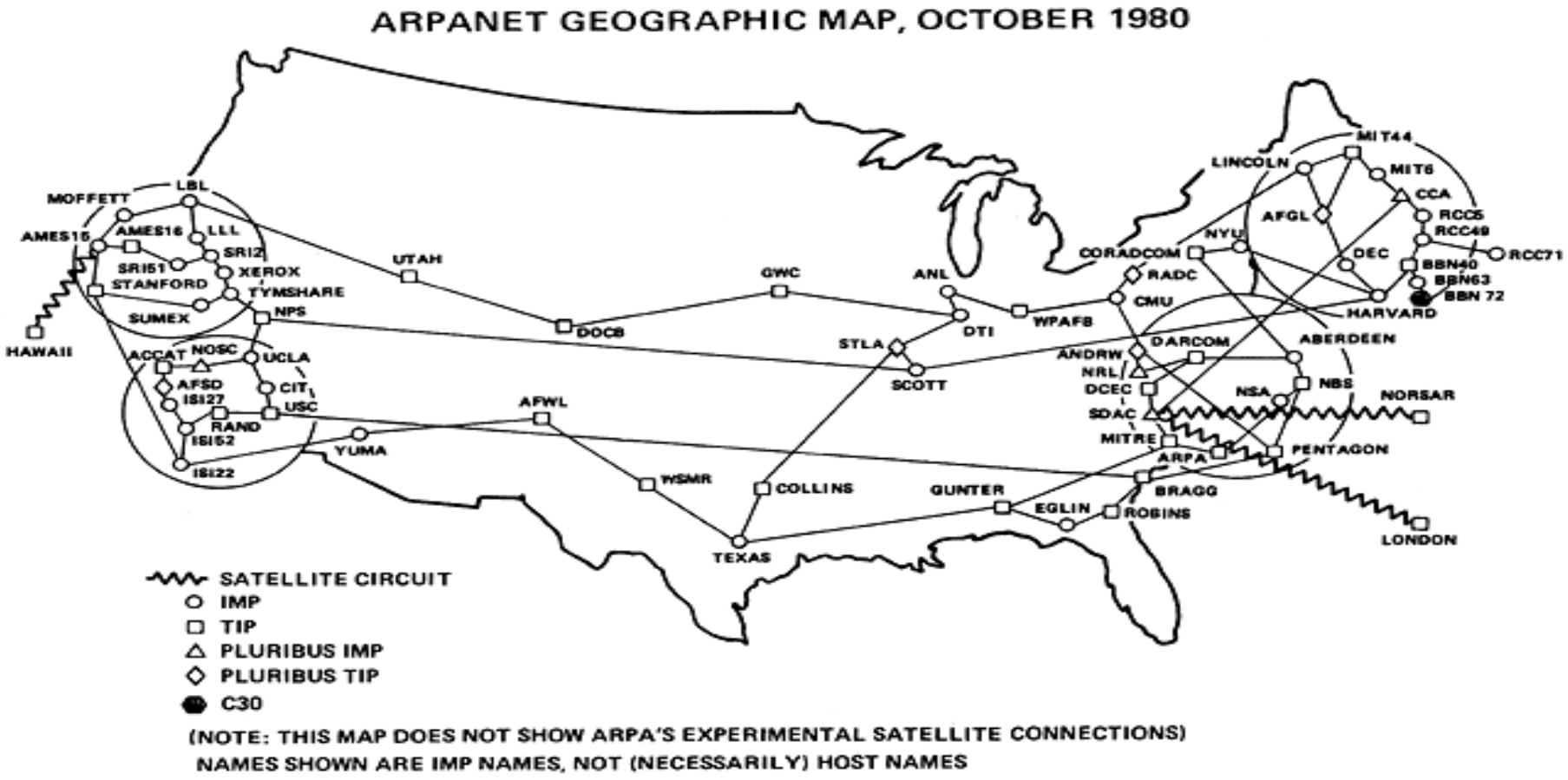
Peering and Hosting

Hosting – contractual agreement to provide access

Peering – voluntary agreement to exchange access

How you contract is largely independent of how your information is routed.

The Old Net



Arpanet to Internet

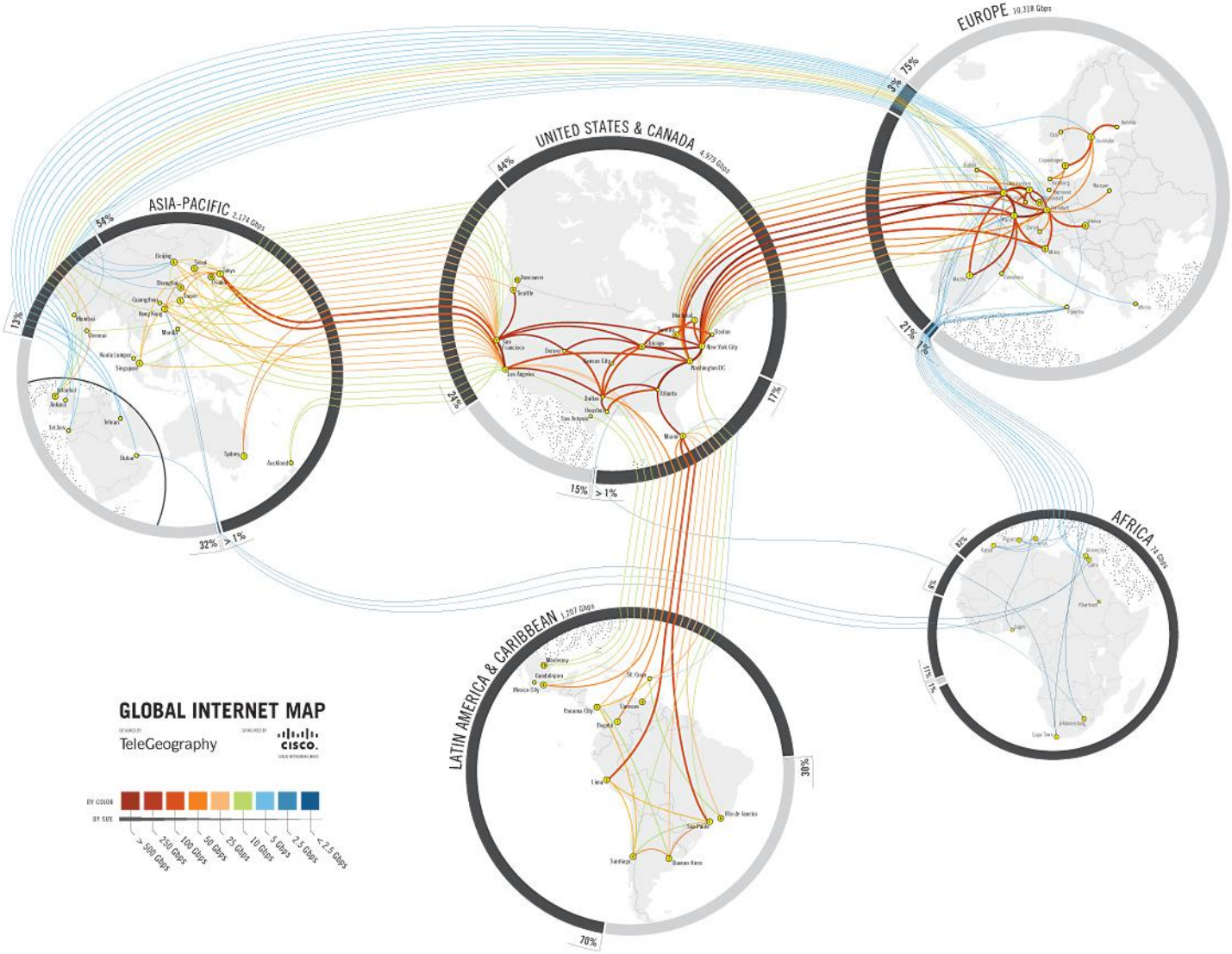
Arpanet: Defense-related institutions and research universities ($$$)

NSFNet: science-related institutions and research universities ($)

Usenet: peer-based institutions

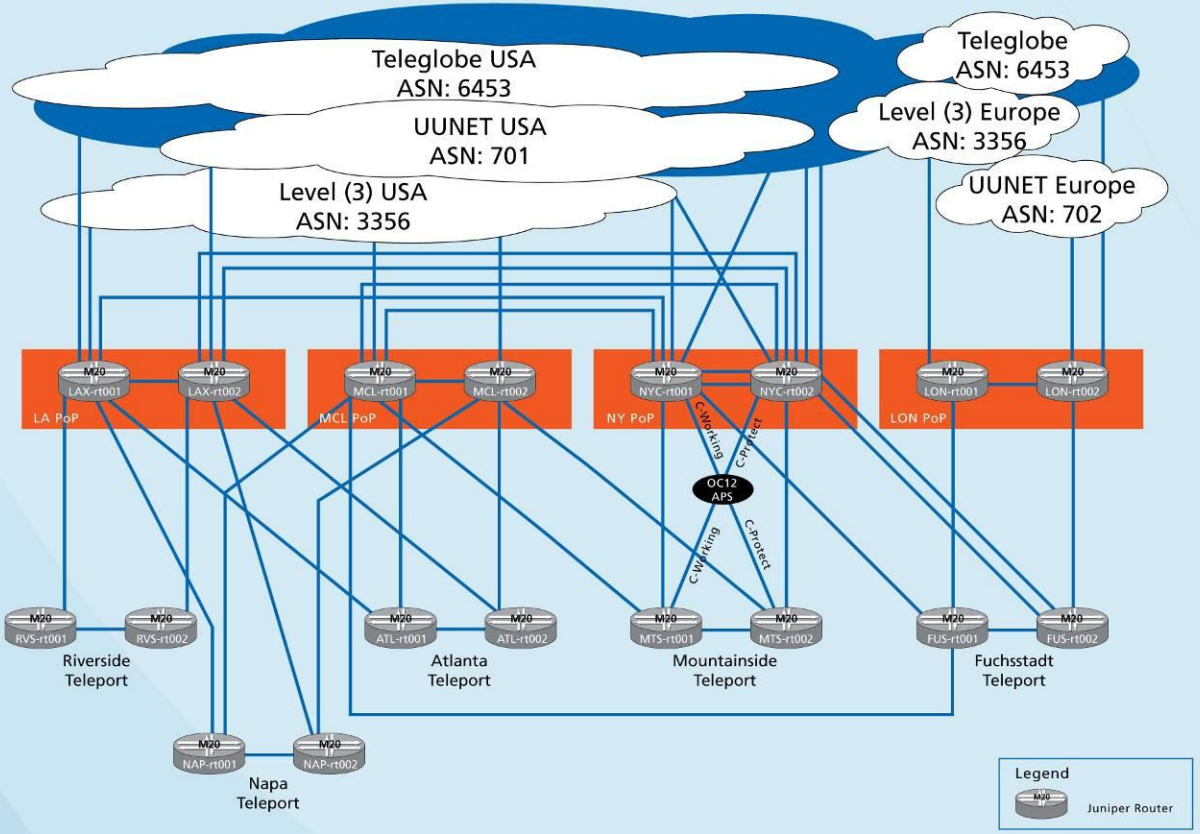
Fleemco!ucvax!berkvax!gateway@berkley.arpa

Addressing schemes still referenced in RFCs



Intelsat GXS® IP Network

Source: Intelsat satellite guide



Partial Compliance with Standards

RFCs are NOT binding documents

- Descriptions of suggested practice
- Acceptance varies widely

NO authoritative body over users

- IANA can pull accreditation to offer names
- But institutions involved readily find other hosting
- NO standardization of host or network configuration

Partial Trust

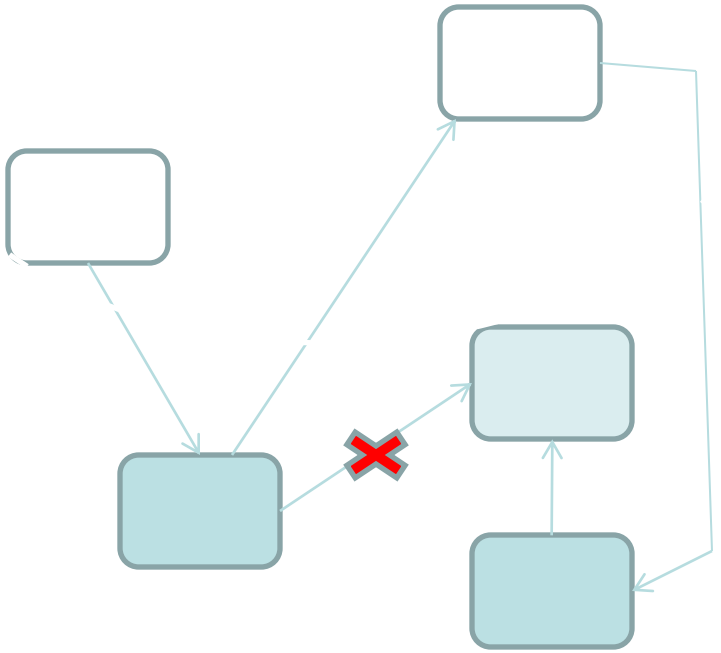
Tom trust Freda, and Freda trusts Harry, but Tom doesn't need to trust Harry

If a host uses an address, it is presumed to have the authority to use that address

Some of this is changing with VPNs, and with IPv6

What this means for Situational Awareness

- Weird traffic artifacts are common
- Weird routing behavior is common
- Routes change
- Redundant routing is the rule, not the exception
- How A talks to B isn't how B talks to A



Geolocation of IP Addresses

- “technique of determining a user's geographic latitude, longitude and, by inference, city, region and nation by comparing the user's public Internet IP address with known locations of other electronically neighboring servers and routers” (http://www.linuxjournal.com/article/7856)
- Series of Inference rules
- On-line database
- Registration information

Rules

Where is this address routed to?

Where is this address routed from?

What is the physical location of those routers?

Where have other hosts on the same network been sited?

Is there location-specific information available on that host? For how large a set of locations?

Geolocation Methods

- Database lookup
  - http://www.caida.org/tools/utilities/netgeo/ -- OLD
  - http://www.ip2location.com/
  - http://www.ipligence.com/geolocation/
- DNS lookup
  - host -t LOC yahoo.com
    yahoo.com LOC 37 23 30.900 N 121 59 19.000 W 7.00m 100m 100m 2m
- Traceroute, then look at where nearby routers are

86.140.13.8

(Thoughtfully sent to me by a spammer)

Netgeo: IANA reserved

Ip2location.com: British Telecom home office in London

Ipligence: Somewhere in the United Kingdom

No LOC record in DNS

- host86-140-13-8.range86-140.btcentralplus.com

Traceroute 86.140.13.8

```
. . .
 7  equinixexchange2.bt.com (206.223.115.140)  6.951 ms  7.176 ms  7.596 ms
 8  t2c1-p5-0-0.uk-eal.eu.bt.net (166.49.164.226)  88.313 ms  87.844 ms  87.264 ms
 9  166-49-168-22.eu.bt.net (166.49.168.22)  88.093 ms  87.684 ms  87.949 ms
10  core1-te0-10-0-0.ealing.ukcore.bt.net (62.6.200.109)  81.990 ms  81.976 ms  82.344 ms
11  core1-pos5-1.reading.ukcore.bt.net (194.74.65.190)  91.785 ms  90.783 ms  91.475 ms
    MPLS Label=23 CoS=5 TTL=1 S=0
12  core1-pos5-4.birmingham.ukcore.bt.net (62.6.204.1)  85.324 ms  85.857 ms  85.146 ms
13  bar4-pos8-0.birmingham2.broadband.bt.net (195.99.120.42)  85.313 ms  85.997 ms  84.909 ms
14  217.47.249.115 (217.47.249.115)  90.754 ms  90.986 ms  90.884 ms
15  217.41.172.45 (217.41.172.45)  85.263 ms  84.725 ms  86.857 ms
16  217.41.172.69 (217.41.172.69)  91.118 ms  90.829 ms  90.920 ms
17  217.41.172.73 (217.41.172.73)  92.357 ms  91.154 ms  91.784 ms
18  217.41.172.10 (217.41.172.10)  90.673 ms  92.228 ms  91.226 ms
19   * * *
```

Birmingham, England -> Hertfordshire England

30 miles to London, 90 miles to Birmingham

Case Studies

Dependencies are clearest when systems fail

Looking at a variety of causes

- Natural events
- Business decisions
- Nationalism/Political

What are the imlications for network situational awareness?

Natural Events

Storms

Disasters

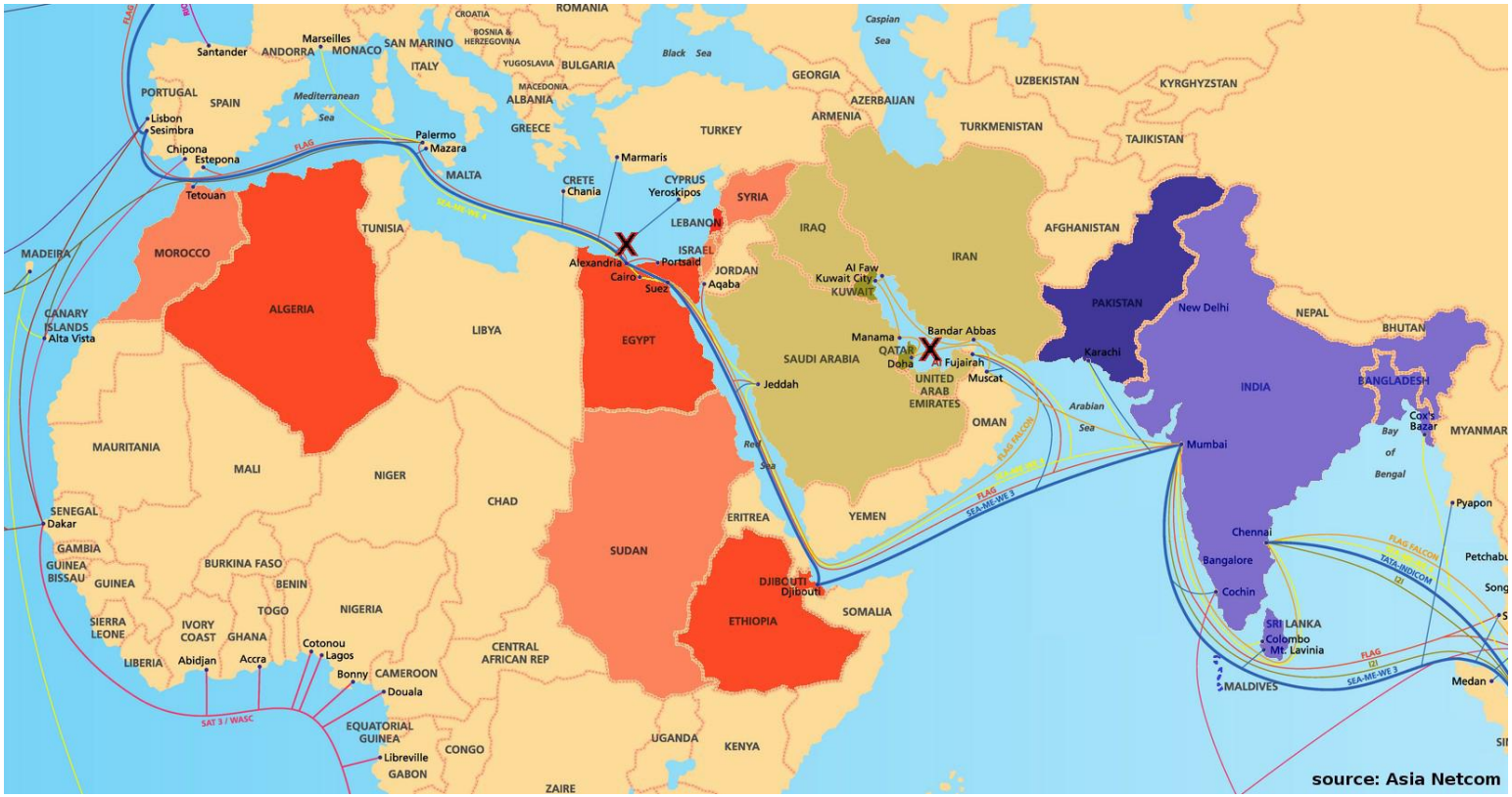
Wear/Corrosion

Frequency is not uncommon

Most common defense is redundancy

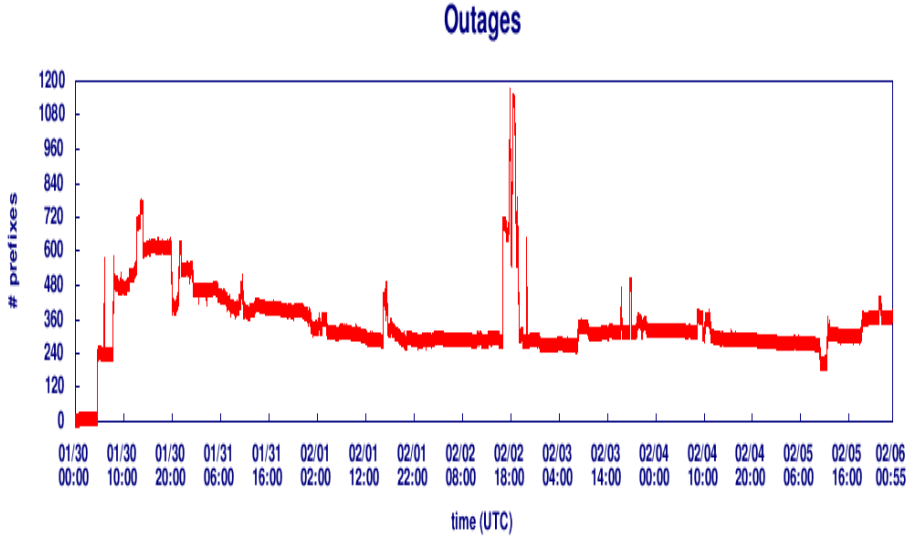
Cable Cut

http://www.renesys.com/tech/presentations/pdf/menog3-cablebreaks.pdf

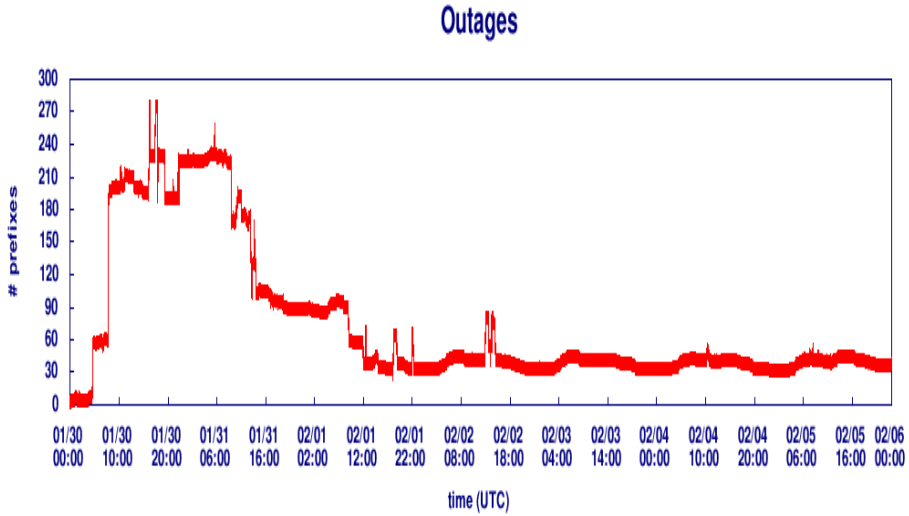


Impacts

Egypt



Kuwait



Egypt: 96% of prefixes suffered some outage (loss of routing on Internet)

- New Service providers
- Traffic Sharing among providers

Kuwait: 70% of prefixes suffered some outage

Business Decisions

Does loss of connectivity benefit anyone?

How do the business relationships work?

Where are business relationships most vulnerable?

How is redundancy a business asset?

How is redundancy a business liability?

What does this mean for network situational awareness?

De-Peering

http://www.renesys.com/tech/presentations/pdf/nanog43-peeringwars.pdf

- Internet is a voluntary network
  - Transit: For-cost service
  - Peering: Voluntary interconnection
  - Tier 1: No transit providers, only peering providers and customers
    - All Tier 1's have to peer, or Internet is divided
- What is volunteered can be withdrawn
  - March 13: Cogent de-peers Telia (restored March 28)
  - Several thousand prefixes affected in multiple nations

Cyber-Attacks

- Cyber War vs. Net War
- Advantages: Cost, effectiveness, deniability, recoverability
- Disadvantages: Escalation, retaliation, collateral damage
- Examples:
  - Chechnya: Russian hacker groups
  - Estonia: Nationalist gone cyber
  - Georgia: Mentored hackers

Cyber War Evaluation

- Where does awareness end?
- How does an organization manage its vulnerability?
- Can the organization manipulate the cost model for the attackers?
- Can the attackers manipulate the cost model for the organization?
- What does this mean for situational awareness?

Mission and Internet Dependencies

What We Will Cover

- Introduction
- Your Network
  - Fundamentals of networks, flow, and protocols
  - Malicious traffic
- External Events & Trends
  - Malware
  - Networks in the Broad
- Working Together
  - Network dependencies
  - Analysis
- Summary

What is Mission?

What is the reason your organization exists?

What are the values that motivate your organization?

What activities does your organization need to perform?

What services does your organization need to exhibit?

Mission and Network Design

Services

Servers

Quality of service

Points of presence

Access points

Acceptable degradation of services

Mission and Internet Usage

Strategy of Internet usage

Point of presence sizing

External firewall / Proxies

Mission and Situational Awareness

What do you need to watch?

- Host vs. Network
- Key Servers
- Key Clients
- Key Routers

How do you need to watch?

- Real-time
- Retrospective

Case Study

Large meeting, held at intervals greater than one year

Involves numerous individuals of national prominence

- Public presentations and votes
- Private meetings / decision-making sessions

Strong social impact at national level

High degree of visibility

Always held in large metropolitan area

Always draws strong protest events

Disruption/failure of event has social, political, and economic impacts

Event operations dependent on local infrastructures (telecomm, transportation, energy)

Heavily IT dependent

Event Production

Local organizers (task force for event only)

- Staff-up / Set-up / Event / Teardown / Staff-down over 1+ year span
- Little or no contact with previous event task force

Contractors/Consultants/Vendors

Venue (infrastructure owners -- assume Major Event Center)

- operations staff
- Access control
- Security Policy
- Additional contractors/vendors

National Organization

- Staff
- Participant source (event attendees and speakers)
- Funding Sponsors: extra services, priority access, no interest in security
- No IT Security Policy for event
- Views event as source of key decisions, important publicity

Event Protesters

Opposition/protest activity can be significant and possibly violent

Awareness by opposition groups of the impact of IT as a means of disruption

Violence against supporting infrastructures

Non-violent interference with event (shouting, physical intrusion, computer mischief, dramatics)

Identification of “single points of failure”

Right to peaceful protest must be respected

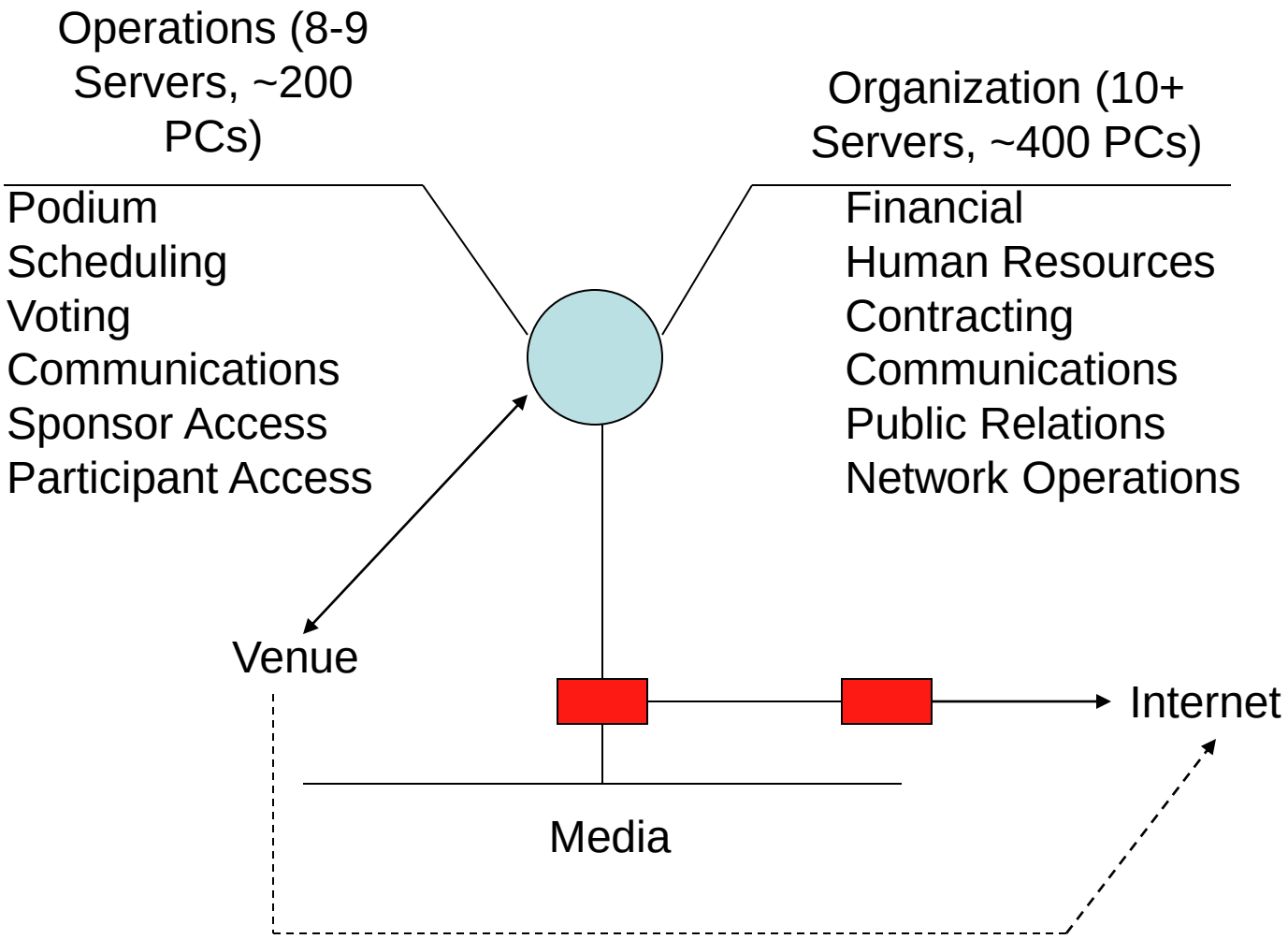
Media

print/radio/television

local/national/international

- Access to event (limited screening: Press freedom)
- Access to information
  - Deadline pressure
  - Privacy compromise
- Source of valued publicity

Event Network



High Concern Risks (1)

Loss of Event/Critical time

- Time at event is short, highly contended
- Loss of infrastructure
- Loss of communications

Loss of Critical personnel

- Physical threat
- Embarrassment / Compromise
- Lack of respect for stakeholders

Loss of trust in decisions made at event

- Can include public exposure of sensitive data
- Compromise of voting systems

High Concern Risks (2)

Loss of privacy, yielding decreased impact on event, decreased participation with organization

- Individuals of prominence can lose privacy – can include a physical security risk (schedules, timetables, etc.)
- Such a loss may not directly impact event – impact delayed
- Can result in loss of Sponsorship, financial support, public perception of competence

Loss of control of convention flow due to disruption (schedule trust loss)

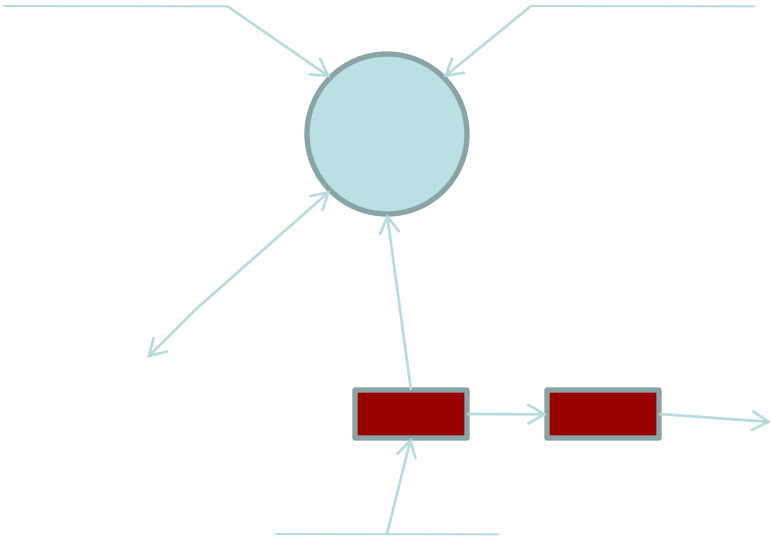
- DDOS can result in loss of critical services – can impact success of meetings
- Intrusion can result in false scheduling, loss of public confidence, loss of trust in IT integrity

Loss of financial control of convention

- Intrusion or DDOS can result in loss of critical financial sponsorship
- Result can include additional financial loss to recover from malicious intrusion or attack
- Loss of public confidence can limit economic/financial support which is considered critical to ultimate success of meetings

Situational Awareness

- What is the mission?
- What is the need for situational awareness?
- What needs to be monitored?
- How does it need to be monitored?



Internet Dependencies

Insourcing

- What don't we use the Internet for?
- What situational awareness needs for internal connectivity?

Outsourcing

- VPN
- Trust relationships
- Exposures

Exporting and Importing Services

What do we need the Internet for?

What should we make someone else's problem?

When should we take on someone else's problem?

What does this imply for Situational Awareness?

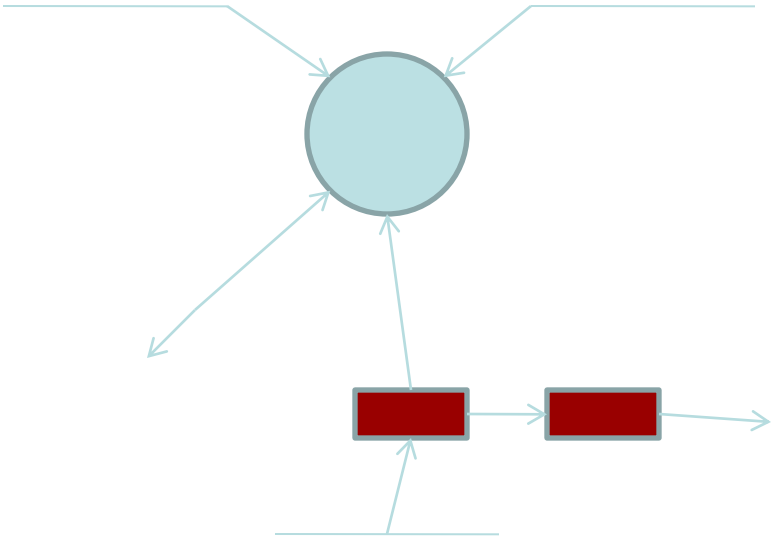
Case Study

What do they need from the Internet?

What does the Internet need from them?

What should they outsource?

What mustn't they outsource?



Doing Analysis

What We Will Cover

- Introduction
- Your Network
  - Fundamentals of networks, flow, and protocols
  - Malicious traffic
- External Events & Trends
  - Malware
  - Networks in the Broad
- Working Together
  - Network dependencies
  - Analysis
- Summary

Building an Analysis Team

Define your mission

- Develop network situational awareness
  - Security
  - Availability
  - Non-traditional threat scenarios
- Know your network,
  Know external events & trends,
  Know how they work together

Building an Analysis Team (2)

Define your needed skill sets

- Layer 2: Networking
- Layer 3 & 4: Ports and Protocols
- Layer 5 - 7: Applications
- Layer 9: Management

Also remember soft skills

- Team building & Communications
- Research & Record Keeping

How would they help?

- Security Architect
- Network Engineer
- Programmer
- Statistician
- Tech Writer
- Mathematician
- Manager
- Team Leader
- Mentor

Performance Metrics

Are they just a management nightmare?

Why do you need metrics?

- Justify existing staff (and staff increases)
- Keep the threat visible
- Senior management sound bites
- Justify expenditures

Good Performance Metrics

Baseline Inventory ("Know your network")

- Services Offered
- Services Consumed

Noise Level

- High volume events that can be quantified, normalized and compared
- Scan counts; vuln sweeps; brute force attempts
  - Compare with open source metrics for the same event
  - Do not combine discrete event types

Good Performance Metrics (2)

- Near misses
  - Evaluate your defense-in-depth architecture
  - Virus hits; drive-by-download misses; policy violations
- Hits
  - Should be rare
  - List, but avoid summarizing
    - individual hits can not be compared with each other
- Work load
  - Overtime hours for team members

Calibrating Your Infrastructure

Can an alarm tell you if a theft has occurred?

Rely on out-of-band management

- Leverage existing solutions built for other needs

What will you never know?

Total ground truth on a network of any size

How often is bad considered good? (false negative)

What is the next attack?

Why did they attack you?

What are your competitors seeing?

Inherently Partial Data

Technology shifts

Attacker actions

Defender actions

Managerial decisions

Network bandwidth

Correlation and Causation

Baseline in dynamic environment

Correlation vs. Causation

Implications

- Need to be cautious in kinds of conclusions
- Consider strategies for dealing with analysis gone wrong

Indication and Proof

Indication: There is reason to believe

Proof: There is no other logically defensible explanation

How much confidence do you need?

Cost of false positive?

Cost of false negative?

Clustering and Extrapolation

- Clustering groups reports into meaningful classes
- Similarity metric applied to common features
  - Cohesion function calculates degree of similarity
  - Clustering generates overlapping clusters (clumps)
    - Minimizes cohesion function betweens incident sets
- Extrapolation fills in the reporting gaps
  - Extrapolation criterion establishes when and how
- Generates extrapolated incidents (x-incidents)

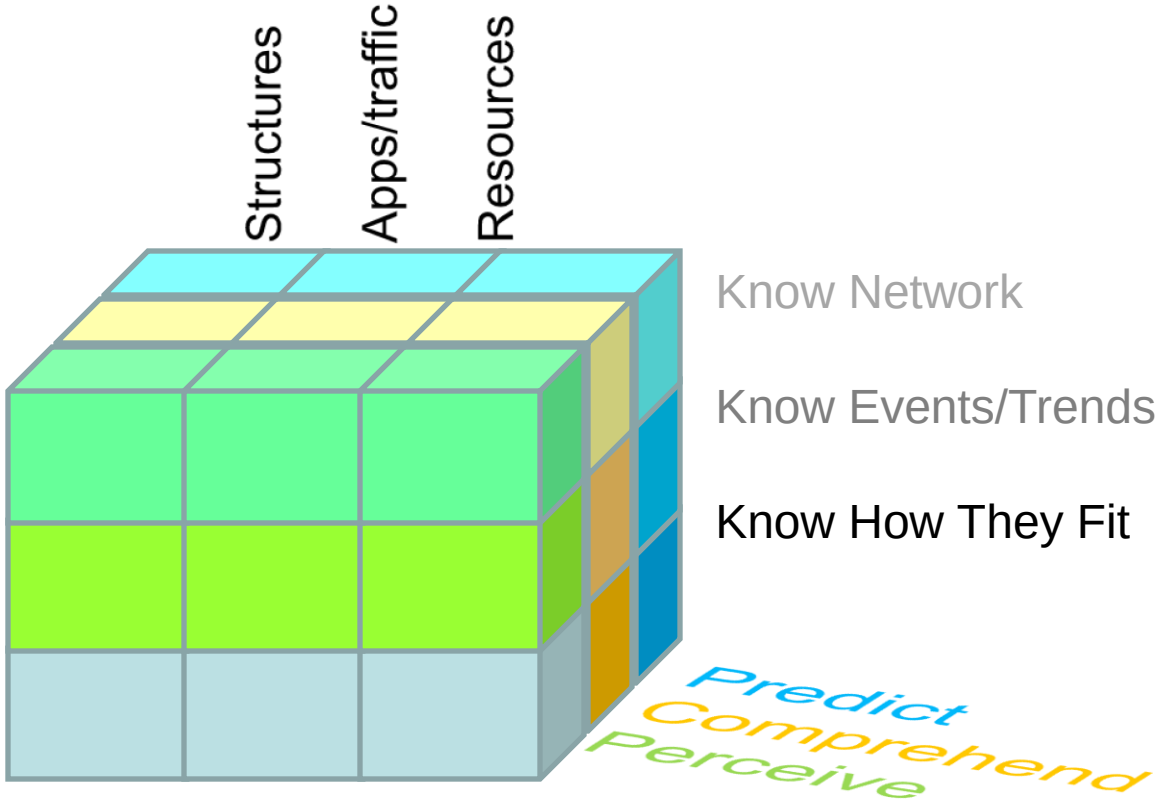
Correlation and Abduction

- Identifies sequences that constitute staged attack
  - Generates x-incident chains
  - Starting context establishes understanding of initial system/network configuration
- Causal relationships through pre-/post-condition chaining
  - Precondition of first incident must satisfy starting context
  - Postcondition of each incident must satisfy precondition of the subsequent incident
- Techniques available (abduction) for filling in gaps
  - Strings together x-incident chains using attack patterns
  - Abduction criterion establishes when and how

What We Will Cover

- Introduction
- Your Network
  - Fundamentals of networks, flow, and protocols
  - Malicious traffic
- External Events & Trends
  - Malware
  - Networks in the Broad
- Working Together
  - Network dependencies
  - Analysis
- Summary

Where we have been



Governance Questions

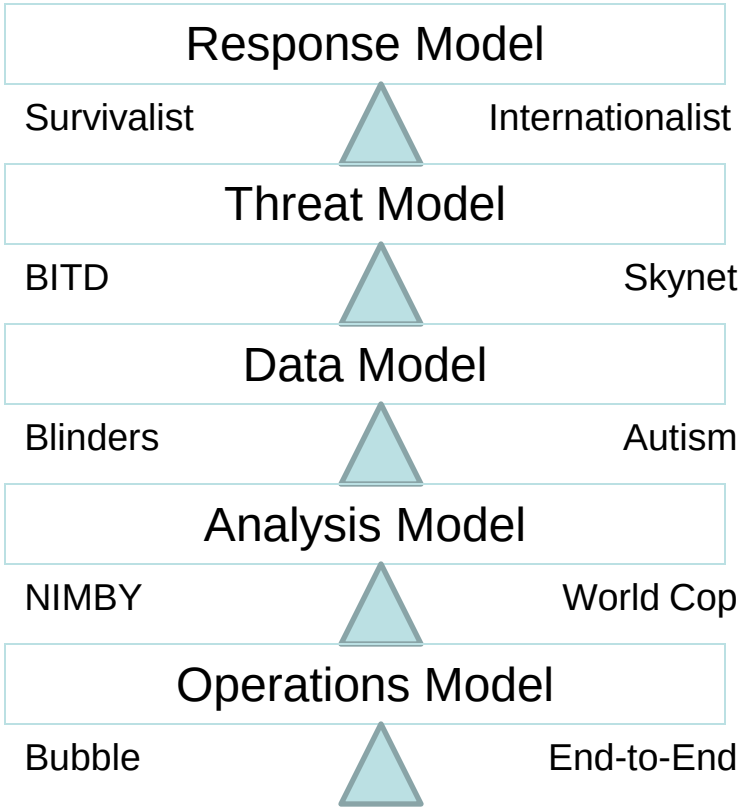
How do I know what I'm looking for?

How do I know why I'm looking?

How do I know where to look?

How do I know when it's found?

NetSA Governance



Future of NetSA

- Analysis coalitions (FloCon on steroids)
- NetSA as a service
- Diversity of specializations
  - Malware vs. Inventory vs. Architecture
  - Diagnose vs. Track/Trace vs. Profile
  - Packet level vs. Trace level vs. Flow level vs. Organizational
- More approachable formalisms
  - Visualizations with meaning
  - Drill down with extensibility
  - Better handling of time

Conclusions

NetSA is new as a systematic approach at scale

NetSA is changing (arms race, technology)

- Need awareness WITHOUT total information
- Need awareness WITH confidence and timeliness
- Need awareness WITHOUT global state
- Need awareness WITH extensibility

We live in interesting times…