Sharing Intelligence is our Best Defense:

Incentives That Work versus Disincentives That Can Be Solved

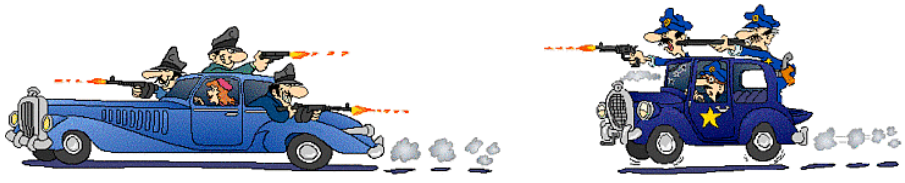
William Yurcik* Adam Slagell Jun Wang

NCSA Security Research
National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign

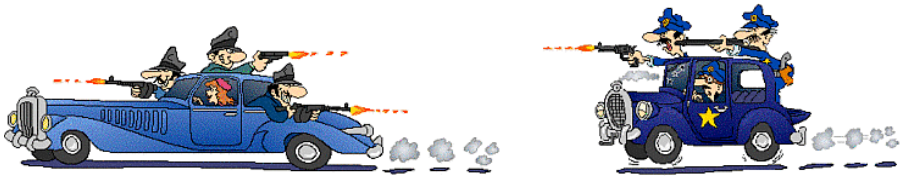
Data Sharing Panel

FloCon 2004

Cyber Security Today Is "a bit" Like the Keystone Cops

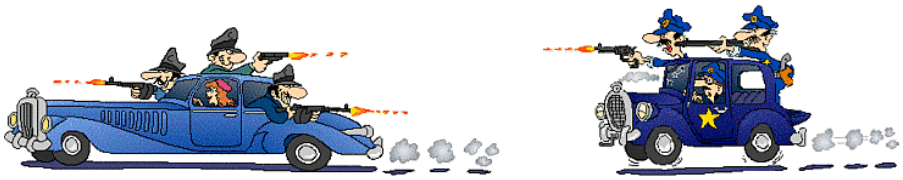


Cyber Security Today Is "a bit" Like the Keystone Cops



They do something really bad!

Cyber Security Today Is "a bit" Like the Keystone Cops

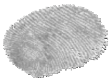


They do something really bad!

Then we chase them to the border.

Security Information Sharing

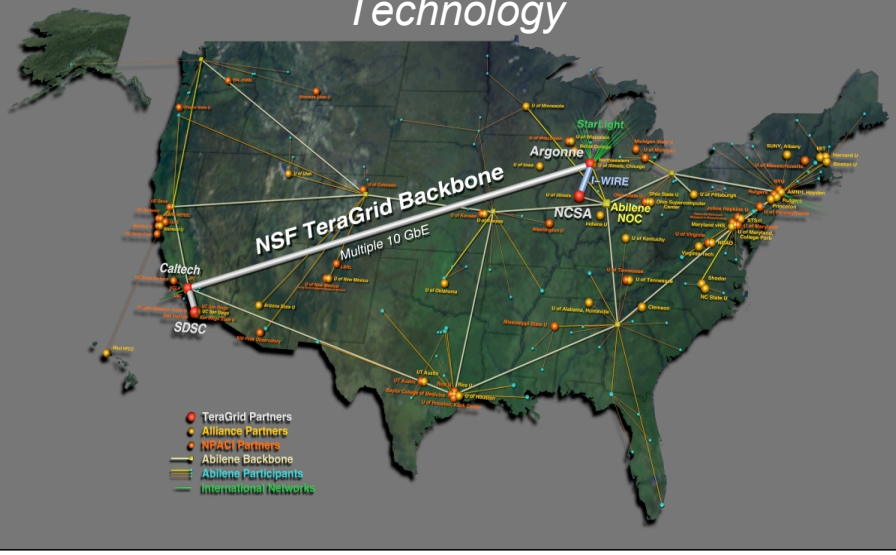
- Need to share information on attacks.
  - Fingerprints and attack profiles
  - Individual events
- Identify individuals



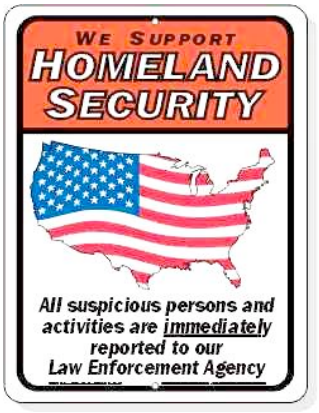
- We cannot continue to stop at the border, we need to cooperate with law enforcement and each other.
  - Security event repository
  - Event correlation across administrative domains
- “unfortunately, this country takes **body bags** and requires **body bags** sometimes to make really tough decisions about money and about governmental arrangements” - Richard Clarke 9/11 Testimony

The World is Rapidly Changing

Greater Dependency on Collaborations and Technology



Cooperation is Voluntary



The vast majority of incidents are never reported

Cooperation is Voluntary
Caveat - except in California!

Only state mandatory disclosure law currently on the books at state level.
Effective as of July 2003

Cooperation is Voluntary
Caveat - except in California!

Only state mandatory disclosure law currently on the books at state level. Effective as of July 2003

California Law has national effects:

California is home to many of the biggest technology companies in the country.

Law applies to all who "conduct business" in the state. Of course many companies route their information through servers housed in California.

Potential for litigation in California - many times companies will have no way of knowing whether a person is resident of California or not.

Computer Emergency Response Teams
CERTs

http://www.first.org/team-info/

Information Sharing and Analysis (ISACs)

- Gathering, analysis and sharing of information related to actual or unsuccessful attempts at computer security breeches.
- Presidential Decision Directive (PDD)-63
- Fee base membership

- Operational ISACs
  - Electric power
  - Telecommunications
  - Information technology
  - Financial services
  - Water supply
  - Surface transportation
  - Oil & gas
  - Emergency fire services
  - Food
  - Chemicals industry
  - Emergency law enforcement

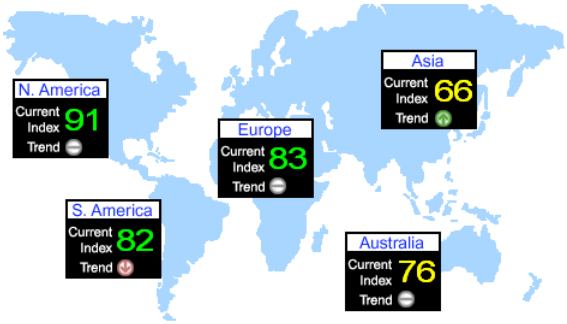
Question:

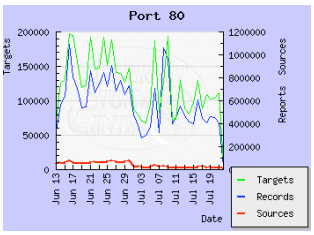
Can we share?

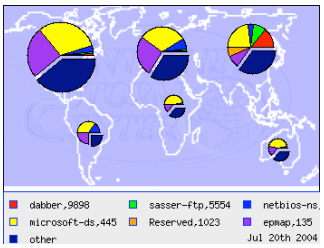
(1) SANS

INTERNET TRAFFIC REPORT

Last update (MST):
7/21/2004 20:20
Global Index 85
Trend





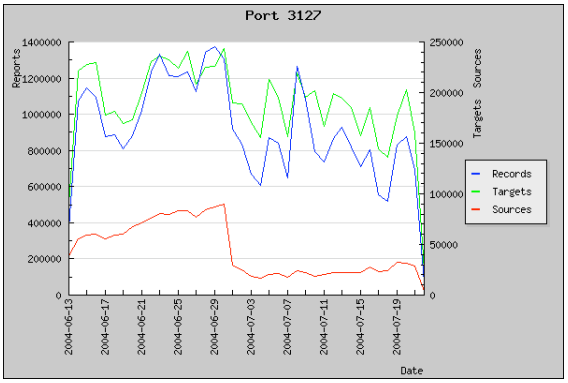


National Center for Supercomputing Applications

NCSA

(2) DShield.org

Distributed Intrusion Detection System



Services registered for this port
....

Vulnerabilities for this port
...

National Center for Supercomputing Applications

NCSA

<http://www.first.org/>

(3) Forum of Incident Response and Security Teams

(4) CIC-SWG

Committee on Institutional Cooperation
- IT Security Working Group
(Big Ten Universities plus the University of Chicago)
<http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/>

Incentives / Disincentives

Framing the Data Sharing Issues

- **Both an Internal / External Issue** (within before between)
- **Who should share externally?**
  - at what organizational levels (more/less bureaucracy)
  - flat or hierarchical (scalability)
- **What should be shared?**
  - raw data, processed data, known answers
- **How should it be shared?**
  - phone calls/Emails, reports, automation 

 **Significant time and effort to share**
  - payback? none/long-term  real-time 

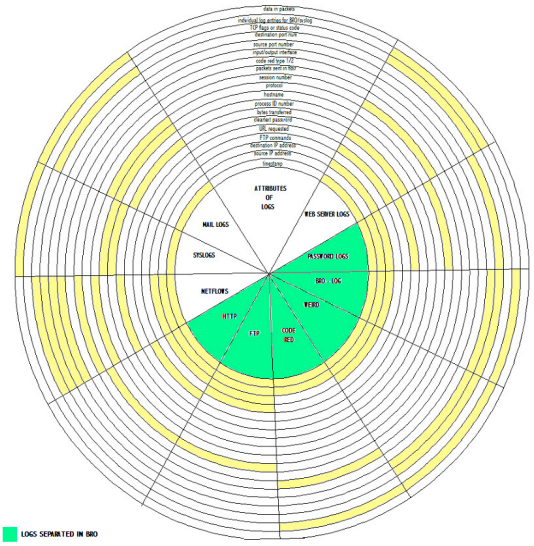
 **Does technology exist to share securely**
  - Will information I share come back to bite me?

Commonly Available Logs

1) **NetFlows Logs**
2) Packet Traces - tcpdump
3) Network IDS- BRO,Snort, etc.
4) Host IDS – Tripwire, etc.
5) Syslogs (general)
6) Authentication Logs
7) DHCP Server Logs
8) Firewall logs
9) Mail Server Logs
10) Backup Logs
11) AntiVirus Logs
12) Vulnerability Scan Logs
13) Nameserver DNS Cache
14) SNMP Logs
15) BGP Tables
16) Dial-Up Server Logs
17) ARP Cache
18) Workstation Logs
19) Process Accounting Logs
20) Trace Route Logs
21) “Homegrown” Logs

…..

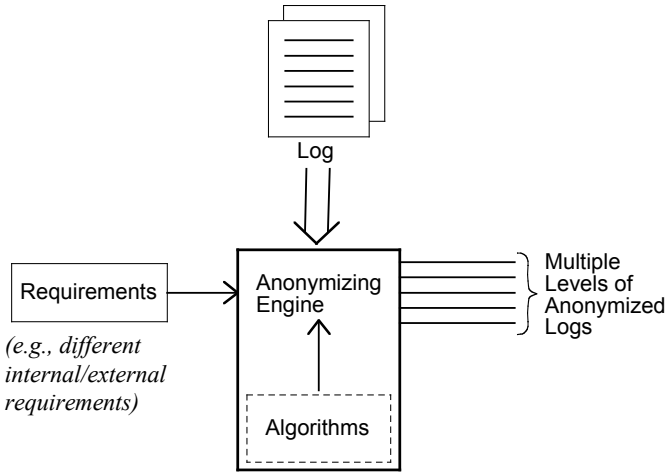
Attributes Across Logs



National Center for Supercomputing Applications

NCSA

Log Anonymization



National Center for Supercomputing Applications

NCSA

Known Plain-Text Attacks

Anonymized Prefix-Preserving IDS Log

unique scan of IP X at time T_1

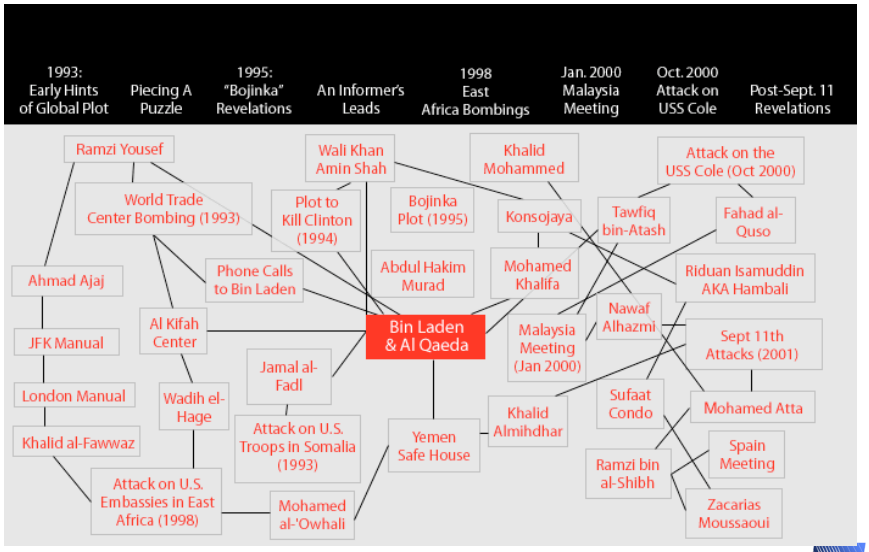
IP X with port activity at Time T_2

Statistical Inference

Anonymized Prefix-Preserving Syslog Log

unique ssh attempt on IP X at time T_1

IP X unique syslog messages at time T_2



NCSA SIFT Project

http://www.ncassr.org/projects/sift/

VizSEC Workshop Oct 29, 2004
ACM Computer and Communications Security Washington DC
http://www.cs.fit.edu/~pkc/vizdmsec04/

Discussion

- No *one-size-fits-all* solution exists for log sharing
- Solutions depend on the application
  - three major problems
    1) huge distributed data volumes
       - visualization is part of the solution here – next workshop
    2) security must be considered
       - CIA
       - may require re-design/re-architecture (I hope not!)
    3) Incentives
- Operational incentives may be the key
  - We have a counter-intuitive example that actually works:
    - sharing between very selfish sysadmins with very sensitive security information (go figure)
  - "only cooperation will make us less vulnerable"