Network Attack Visualization

Greg Conti

www.cc.gatech.edu/~conti
Disclaimer

The views expressed in this presentation are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense or the U.S. Government.
Information visualization is the use of interactive, sensory representations, typically visual, of abstract data to reinforce cognition.
An Art Survey…

A

B

C

http://www.clifford.at/cfun/progex/
http://www.muppetlabs.com/~breadbox/bf/
http://www.geocities.com/h2lee/ascii/monalisa.html
Why InfoVis?

• Helps find patterns
• Helps reduce search space
• Aids efficient monitoring
• Enables interaction (what if)
• Help prevent overwhelming the user
<table>
<thead>
<tr>
<th>Thread / Thread Starter</th>
<th>Rating</th>
<th>Last Post</th>
<th>Replies</th>
<th>Views</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sticky: DEF CON 12 Homebrew IP Appliance Contest Announced</td>
<td></td>
<td>04-23-2004 11:11 PM by Neural</td>
<td>8</td>
<td>235</td>
</tr>
<tr>
<td>Sticky: DEF CON 12 WarDriving Contest Announced</td>
<td></td>
<td>04-17-2004 03:58 PM by Thorn</td>
<td>5</td>
<td>214</td>
</tr>
<tr>
<td>Sticky: DEF CON 12 Slogan Contest</td>
<td></td>
<td>04-14-2004 03:55 PM by Chris</td>
<td>3</td>
<td>340</td>
</tr>
<tr>
<td>Sticky: All New Users: Read this BEFORE posting!</td>
<td></td>
<td>02-29-2004 08:10 PM by Gritter</td>
<td>0</td>
<td>455</td>
</tr>
<tr>
<td>need advice on getting company to send me</td>
<td></td>
<td>Yesterday 05:43 AM by phidal</td>
<td>9</td>
<td>126</td>
</tr>
<tr>
<td>AP sold out; chances of picking up cancellation?</td>
<td></td>
<td>05-08-2004 04:37 PM by Contrarian</td>
<td>11</td>
<td>126</td>
</tr>
<tr>
<td>Don't Forget Howard Johnson</td>
<td></td>
<td>05-08-2004 04:22 PM by Zhym</td>
<td>9</td>
<td>148</td>
</tr>
<tr>
<td>Anyone know the area?</td>
<td></td>
<td>05-09-2004 02:03 AM by HyperCityGirl</td>
<td>12</td>
<td>130</td>
</tr>
<tr>
<td>Who's bringing homebrews?</td>
<td></td>
<td>05-07-2004 05:07 PM by H3d Rush</td>
<td>12</td>
<td>128</td>
</tr>
<tr>
<td>Ironic timing for the &quot;Official Star Trek Con&quot; (123)</td>
<td></td>
<td>05-07-2004 04:43 AM by alk lloyd</td>
<td>26</td>
<td>453</td>
</tr>
</tbody>
</table>
So What?

- Go Beyond the Algorithm
- Help with detecting and understand some 0day attacks
- Make CTF and Root Wars a Spectator Sport
- Help find insider threats
- Stealth might not be so stealthy
- Help visually fingerprint attacks/tools

What tasks do you need help with?
Packet Capture Visualizations

TCP Dump

Ethereal image: http://www.linux-france.org/prj/edu/archinet/AMSI/index/images/ethereal.gif
Ethereal by Gerald Combs can be found at http://www.ethereal.com/

EtherApe image: http://www.solaris4you.dk/sniffersSS.html
EtherApe by Juan Toledo can be found at http://etherape.sourceforge.net/

TCPDump image: http://www.bgnnett.no/~giva/pcap/tcpdump.png
TCPDump can be found at http://www.tcpdump.org/
traceroute
Visualizations

3D TraceRoute

Xtraceroute

basic traceroute/tracert

3D TraceRoute Developer:  http://www.hlembke.de/prod/3dtraceroute/
XTraceRoute Developer:  http://www.dtek.chalmers.se/~d3august/xt/
Intrusion Detection System Types

- **Host-based intrusion-detection** is the art of detecting malicious activity within a single computer by using
  - host log information
  - system activity
  - virus scanners

- A **Network intrusion detection system** is a system that tries to detect malicious activity such as denial of service attacks, port-scans or other attempts to hack into computers by reading all the incoming packets and trying to find suspicious patterns.

http://en2.wikipedia.org/wiki/Host-based_intrusion-detection_system
http://en2.wikipedia.org/wiki/Network_intrusion_detection_system
System Architecture

Ethernet

Packet Capture

Parse

Process

Plot

tcpdump (pcap, snort)

winpcap

Perl

VB

Perl

VB

xmgrace (gnuplot)

服務或创意
Information Visualization Mantra

Overview First,
Zoom & Filter,
Details on Demand

- Ben Shneiderman

http://www.cs.umd.edu/~ben/
Overview First...
Zoom and Filter...
Representative Current Research
SequoiaView

Demo

http://www.win.tue.nl/sequoiaview/
Observing Intruder Behavior

Dr. Rob Erbacher

- Visual Summarizing and Analysis Techniques for Intrusion Data
- Multi-Dimensional Data Visualization
- A Component-Based Event-Driven Interactive Visualization Software Architecture

http://otherland.cs.usu.edu/~erbacher/
3 Line appearances and their relationships. (a) Telnet and rlogin connections as solid lines, (b) privileged FTPs as long dashed lines, (c) anonymous FTPs as short dashed lines, (d) Network file system (NFS) accesses as solid lines with many arrows, (e) initial inetd port connection, and (f) port scan.

Demo

2 Basic glyph organization. (a) The initial inetd connection to the system. (b) The resulting connection after authentication. (a) and (b) also represent the number of users with connections from the given remote host and the number of connections by said users through the use of the cross hatches. The monitored system, (c) showing number of users and load.

http://otherland.cs.usu.edu/~erbacher/
Operating System Fingerprinting

Dr. David Marchette

- Passive Fingerprinting
- Statistics for intrusion detection

http://www.mts.jhu.edu/~marchette/
Visualizing Internet Routing Data

Soon Tee Teoh

Demo

http://graphics.cs.ucdavis.edu/~steoh/

See also treemap basic research: http://www.cs.umd.edu/hcil/treemap-history/index.shtml
Worm Propagation

- CAIDA
- Young Hyun
- David Moore
- Colleen Shannon
- Bradley Huffaker

http://www.caida.org/tools/visualization/walrus/examples/codered/
Intrusion Detection and Visualization Using Perl

Jukka Juslin

3D plot of:
- Time
- SDP (Source-Destination-Port)
- Number of Packets

Data stored in Perl hashes
Output piped to GNUplot

http://www.cs.hut.fi/~jtjuslin/
TCP/IP Sequence Number Generation

Michal Zalewski

\[ x[n] = s[n-2] - s[n-3] \]
\[ y[n] = s[n-1] - s[n-2] \]
\[ z[n] = s[n] - s[n-1] \]

Follow-up paper - http://lcamtuf.coredump.cx/newtcp/
High Speed Data Flow Visualization

Therminator technology watches the data stream and illustrates categories of data as colored bars that are proportional in height to the quantity of data at a given time. The process is repeated to form a stacked bar graph that moves across a computer screen to show current and past data traffic composition.

Haptic and Visual Intrusion Detection

NIVA System
- Craig Scott
- Kofi Nyarko
- Tanya Capers
- Jumoke Ladeji-Osias

http://portal.acm.org/citation.cfm?id=952873&dl=ACM&coll=GUIDE
Scoreboard DC11

Team Name
Team Score
Hacking Rank
Count of services

Entire slide from: www.toorcon.org/slides/rootfu-toorcon.ppt
Atlas of Cyber Space

Welcome to the Atlas of Cyberspaces

This is an atlas of maps and graphic representations of the geographies of the new electronic territories of the Internet, the World-Wide Web and other emerging Cyberspaces.

These maps of Cyberspaces - cybermaps - help us visualize and comprehend the new digital landscapes beyond our computer screens, in the unseen communications networks and vast online information resources. The cybermaps, like maps of the real-world, help us navigate the new information landscapes, as well as being objects of aesthetic interest. They have been created by cyber-explorers of many different disciplines, and from all corners of the world.

Some of the maps you will see in the Atlas of Cyberspaces will appear familiar, using the cartographic conventions of real-world maps, however, many of the maps are much more abstract representations of electronic spaces, using new metrics and grids. The atlas comprises separate pages, covering different types of cybermaps.

http://www.cybergeography.org/atlas/atlas.html
Honeynets

John Levine

- The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks
- Interesting look at detecting zero-day attacks

Port 135 MS BLASTER scans

Date Public: 7/16/03   Date Attack: 8/11/03
Georgia Tech Honeynett
Source: John Levine, Georgia Tech
Hot Research Areas…

- visualizing vulnerabilities
- visualizing IDS alarms (NIDS/HIDS)
- visualizing worm/virus propagation
- visualizing routing anomalies
- visualizing large volume computer network logs
- visual correlations of security events
- visualizing network traffic for security
- visualizing attacks in near-real-time
- security visualization at line speeds
- dynamic attack tree creation (graphic)
- forensic visualization

http://www.cs.fit.edu/~pkc/vizdmsec04/
More Hot Research Areas…

- feature selection and construction
- incremental/online learning
- noise in the data
- skewed data distribution
- distributed mining
- correlating multiple models
- efficient processing of large amounts of data
- correlating alerts
- signature and anomaly detection
- forensic analysis

http://www.cs.fit.edu/~pkc/vizdmsec04/
One Approach…

- Look at TCP/IP Protocol Stack Data (particularly header information)
- Find interesting visualizations
- Throw some interesting traffic at them
- See what they can detect
- Refine
Information Available On and Off the Wire

- Levels of analysis
- External data
  - Time
  - Size
  - Protocol compliance
  - Real vs. Actual Values
- Matrices of options
- Header slides

http://ai3.asti.dost.gov.ph/sat/levels.jpg
Examining Available Data...

Link Layer (Ethernet)

Network Layer (IP)

Transport Layer (TCP)

Transport Layer (UDP)

IP: http://www.ietf.org/rfc/rfc0791.txt
UDP: http://www.ietf.org/rfc/rfc0768.txt
TCP: http://www.ietf.org/rfc/rfc793.txt
Ethernet: http://www.itec.suny.edu/scsys/vms/OVMSDOC073/V73/6136/ZK-3743A.gif
“Grace is a WYSIWYG 2D plotting tool for the X Window System and M*tif. Grace runs on practically any version of Unix-like OS. As well, it has been successfully ported to VMS, OS/2, and Win9*/NT/2000/XP”

http://plasma-gate.weizmann.ac.il/Grace/
Parallel Plot

Remote Machine’s Ports

Target Machine’s Ports
Results

Example 1 - Baseline with Normal Traffic
Example 2 - Port Scan
Example 3 - Port Scan “Fingerprinting”
Example 4 - Vulnerability Scanner
Example 5 - Wargame
Example 1: Baseline

<table>
<thead>
<tr>
<th>External Port</th>
<th>Internal Port</th>
<th>External IP</th>
<th>Internal IP</th>
</tr>
</thead>
</table>
Example 2 - PortScan
Port Scan Against Single Host

Superscan w/ports 1-1024

Defender
Example 3- PortScan “Fingerprinting”

nmap 3.00 default (RH 8.0)

nmap 3.00 udp scan (RH 8.0)

Superscan 3.0

Nmap Win 1.3.1
Exploring nmap 3.0 in depth
(port to IP to IP to port)

default (root)  
stealth FIN (-sF)  
NULL (-sN)  
UDP (-sU)  

SYN (-sS -O)  
stealth SYN (-sS)  
CONNECT (-sT)  
XMAS (-sX)
nmap within Nessus
(port to IP to IP to port)

CONNECT (-sT)

UDP (-sU)

Nessus 2.0.10
Codebase Evolution

SuperScan 3.0

scanline 1.01

SuperScan 4.0
Three Parallel Scans
WinNMap
Example 4: Vulnerability Scanner
Nessus 2.0.10
Example 5: Wargame

CDX 2003
10.100.X.X(left) 10.1.X.X(right) TCP & UDP  (dataset 1050588077)
CDX 2003
10.100.X.X(left) 10.1.X.X(right) Target and Source Sets (dataset 1050588077)

Demo
Findings (Strengths)

- Tools can be fingerprinted
- Threading / multiple processes visible
- OS/Application features visible
- Sequence of ports scanned visible
- Useful against slow scans
- Useful against distributed scans
Findings (Weaknesses)

- Spoofing
- Interaction with personal firewalls
- Countermeasures
- Scale / Labeling are issues
- Occlusion is a problem
- Greater interactivity required for forensics and less aggressive attacks
- Some tools are very flexible
- Source code not available for some tools
Future

- Active scanning, visualization of Nmap results
- Real-time vs. Offline
- Interesting datasets
- Honeypot Fingerprinting
- Other visualization techniques
- Visualization of protocol attacks
- Visualization of application layer attacks
- Visualization of physical layer attacks (?)
- Code up some stand-alone tools
Where to go for more information…

- www.rumint.com - for latest version of tool
- Course websites
  - http://www.cc.gatech.edu/classes/AY2004/cs7450_spring/detailref.html
  - http://people.cs.vt.edu/~north/infoviz/
  - http://graphics.stanford.edu/courses/cs448b-04-winter/
  - http://www.otal.umd.edu/Olive/
More Information

Information Visualization

• Envisioning Information by Tufte
• The Visual Display of Quantitative Information by Tufte
• Visual Explanations by Tufte
• Information Visualization by Spence
• Information Visualization: Using Vision to Think by Card

• See also the Tufte road show, details at www.edwardtufte.com
What’s on the CD

• rumint visualization tool
• tcpdump | perl | xmgrace
  – howto
  – sample scripts
• gallery of classic visualizations (w/links)
• webpage with security infovis links
• this talk
Acknowledgements

• 404.se2600
  – icer
  – StricK
  – Rockit
  – Hendrick
  – Clint

• Kulsoom Abdullah
  – http://www.prism.gatech.edu/~gte369k/csc/

• Dr. John Stasko
  – http://www.cc.gatech.edu/~john.stasko/

• Dr. Wenke Lee
  – http://www.cc.gatech.edu/~wenke/
Questions?

http://carcino.gen.nz/images/index.php/04980e0b/53c55ca5
Backup Slides
Data Format

- tcpdump outputs somewhat verbose output
  09:02:01.858240 0:6:5b:4:20:14 0:5:9a:50:70:9 62:
  10.100.1.120.4532 > 10.1.3.0.1080: tcp 0 (DF)

- parse.pl cleans up output
  09 02 01 858240 0:6:5b:4:20:14 0:5:9a:50:70:9
  10.100.1.120.4532 10.100.1.120 4532 10.1.3.0.1080 10.1.3.0
  1080 tcp

- analyze.pl extracts/formats for Grace.
  0 4532
  1 1080
  0 4537
  1 1080
  0 2370
  1 1080
Required Files

Perl, tcpdump and grace need to be installed.

- http://www.tcpdump.org/
- http://www.perl.org/
- http://plasma-gate.weizmann.ac.il/Grace/

to install grace...

Download RPMs (or source)
ftp://plasma-gate.weizmann.ac.il/pub/grace/contrib/RPMS

The files you want
grace-5.1.14-1.i386.rpm
pdflib-4.0.3-1.i386.rpm

Install
#rpm -i pdflib-4.0.3-1.i386.rpm
#rpm -i grace-5.1.14-1.i386.rpm
Hello World Example

# tcpdump -lnnq -c10 | perl parse.pl | perl analyze.pl | outfile.dat
# xmgrace outfile.dat &

Optionally you can run xmgrace with an external format language file…

# xmgrace outfile.dat -batch formatfile

See ppt file for more detailed howto information
Hello World Example (cont)

Optionally you can run xmgrace with an external format language file…

```
xmgrace outfile.dat -batch formatfile
```

formatfile is a text file that pre-configures Grace e.g.

```
title "Port Scan Against Single Host"
subtitle "Superscan w/ports 1-1024"
yaxis label "Port"
yaxis label place both
yaxis ticklabel place both
xaxis ticklabel off
xaxis tick major off
xaxis tick minor off
autoscale
```
To Run Demo

See readme.txt

Two demo scripts…
- runme.bat (uses sample dataset)
- runme_sniff.bat (performs live capture, must be root)

Note: you must modify the IP address variable in the Analyzer script. (See analyzer2.pl for example)
Example 1 - Baseline

- Normal network traffic
  - FTP, HTTP, SSH, ICMP...

- Command Line
  - Capture Raw Data
    - `tcpdump -l -nnqe -c 1000 tcp or udp | perl parse.pl > expl1_outfile.txt`
  - Run through Analysis Script
    - `cat expl1_outfile.txt | perl analyze_1a.pl > output1a.dat`
  - Open in Grace
    - `xmgrace output1a.dat &`
Example 1 - Baseline

Normal Network Traffic (SMTP, HTTP, SSH, FTP, ICMP)

TCP & UDP (Many Sources to Single Target)
Example 2 - PortScan

- Light “normal” network traffic (HTTP)
- Command Line
  - Run 2a.bat (chmod +x 2a.bat)

```
echo running experiment 2
echo 1-1024 port scan

tcpdump -l -nnqe -c 1200 tcp or udp > raw_outfile_2.txt
cat raw_outfile_2.txt | perl parse_2a.pl > exp2_outfile.txt
cat exp2_outfile.txt | perl analyze_2a.pl > output_2a.dat
xmgrace output_2a.dat &

echo experiment 2 completed
```
Example 3- PortScan “Fingerprinting”

Tools Examined:

• Nmap Win 1.3.1 (on top of Nmap 3.00)
  XP Attacker
  (http://www.insecure.org/nmap/)

• Nmap 3.00
  RH 8.0 Attacker
  (http://www.insecure.org/nmap/)

• Superscan 3.0
  RH 8.0 Attacker
  (http://www.foundstone.com/index.htm?subnav=resources/navigation.htm
m&subcontent=/resources/proddesc/superscan.htm)
Example 4: Vulnerability Scanner

• Attacker: RH 8.0 running Nessus 2.0.10
• Target: RH 9.0
Example 5: Wargame

- Attackers: NSA Red Team
- Defenders: US Service Academies

Defenders lock down network, but must provide certain services