Network Security
Data Visualization

Greg Conti
www.cc.gatech.edu/~conti

http://www.cybergeography.org/atlas/walrus1_large.gif
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.
Why InfoVis?

- Helps find patterns
- Helps reduce search space
- Aids efficient monitoring
- Enables interaction (what if)
- Help prevent overwhelming the user
So What?

- Go Beyond the Algorithm
- Help with detecting and understand some 0 day attacks
- Make Root Wars & CTF 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 image: http://www.bgnett.no/~giva/pcap/tcpdump.png
TCPDump can be found at http://www.tcpdump.org/

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/
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
Ethernet

Packet Capture

Parse

Process

Plot

tcpdump (pcap, winpcap, snort)
Perl (c/c++)
Perl (c/c++)
xmgrace (GNU plotutils gtk+/opengl html)

tcpdump capture files

Creativity
Information Visualization Mantra

Overview First,
Zoom & Filter,
Details on Demand

- Ben Shneiderman

http://www.cs.umd.edu/~ben/
Overview First...

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000000</td>
<td>10.1.3.1</td>
<td>10.1.100.3</td>
<td>FTP</td>
<td>Response: 530 Login</td>
</tr>
<tr>
<td>2</td>
<td>57.699660</td>
<td>10.1.3.1</td>
<td>10.1.100.3</td>
<td>FTP</td>
<td>Response: 530 Login</td>
</tr>
<tr>
<td>3</td>
<td>107.412280</td>
<td>10.1.3.1</td>
<td>10.1.100.3</td>
<td>FTP</td>
<td>Response: 530 Login</td>
</tr>
<tr>
<td>4</td>
<td>1417.537217</td>
<td>10.1.3.1</td>
<td>10.1.100.3</td>
<td>FTP</td>
<td>Response: 530 Login</td>
</tr>
<tr>
<td>5</td>
<td>1417.969338</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>6</td>
<td>1417.022253</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>7</td>
<td>1417.052157</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>8</td>
<td>1417.073243</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>9</td>
<td>1417.124019</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>10</td>
<td>1417.163392</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>11</td>
<td>1417.273972</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>12</td>
<td>1417.214781</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>13</td>
<td>1417.308916</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>14</td>
<td>1417.333711</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>15</td>
<td>1417.423149</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>16</td>
<td>1417.445194</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>17</td>
<td>1417.484148</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>18</td>
<td>1417.534217</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>19</td>
<td>1417.608517</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>20</td>
<td>1417.687446</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
<tr>
<td>21</td>
<td>1417.745307</td>
<td>10.6.1.251</td>
<td>10.1.4.4</td>
<td>TCP</td>
<td>[TCP ZeroWindow] ftp</td>
</tr>
</tbody>
</table>

Frame 11 (145 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:15:9a:50:70:09, Dst: 00:05:19:aa:30:70:09
Internet Protocol, src Addr: 10.6.1.251, Dst Addr: 10.1.4.4 (10.1.4.4)
Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: echo (7), Seq: 0, Ack: 0,
Zoom and Filter...
Details on Demand...
What Tools are at Your Disposal…

Tools
- Color
- Size
- Sequence
- Filtering
- Interactivity

What InfoVis can help you see
- Relationships between X & Y & Z…
- Extremes
- Comparisons and Differences
- Trends

http://www.netstumbler.com/
Image: http://images.webattack.com/screenfiles/netstumbler.gif
More tools
  – Shape
  – Orientation
  – Scale
  – Perspective

What InfoVis can help you see
  – Anomalies
  – Outliers
  – Patterns

http://scanmap3d.sourceforge.net/
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 GNUpplot

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
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 waves of the global communications networks and vast online information resources. The cybermaps, like maps of the real-world, help us navigate the new information landscapes, as well 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 anamolies
- 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
Example 2 - PortScan

Port Scan Against Single Host
Superscan w/ports 1-1024
Port Scan Against Single Host
Superscan w/ports 1-1024

Defender
Port Scan Against Single Host
Superscan w/ports 1-1024

Attacker
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
HELLO STEVENSON TESTS?
THIS IS DR. LAVSKY. I ORDERED A
SET OF RORSCHACH INK BLOTS.
BUT INSTEAD I RECEIVED
VARIOUS PICTURE OF ME RAPING AND
KILLING MY MOTHER. IS THIS SOME
KIND OF SICK JOKE?

http://www.wire-fu.com/adept/
Brian McLachlan
Used with permission
nmap 3 (RH8)
nmap 3 UDP (RH8)
scanline 1.01 (XP)
SuperScan 3.0 (XP)

NMapWin 3 (XP)
nmap 3.5 (XP)
nikto 1.32 (XP)
SuperScan 4.0 (XP)

Demo
SuperScan 4.0
WinNMap
Three Parallel Scans
Example 4: Vulnerability Scanner
Nessus 2.0.10
Sara 5.0.3

Light

Medium

Heavy
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)
Port 135

**CAN-2003-0605 tcp any 135**
The RPC DCOM interface in Windows 2000 SP3 and SP4 allows remote attackers to cause a denial of service (crash), and local attackers to use the DoS to hijack the epmapper pipe to gain privileges, via certain messages to the __RemoteGetClassObject interface that cause a NULL pointer to be passed to the PerformScmStage function.

**CAN-2003-0352 6 any 135**
Buffer overflow in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a malformed message, as exploited by the Blaster/MSblast/LovSAN worm.

Conclusions

• Limited fingerprinting of tools is possible
• Visualization can help drive better algorithms
• Some attacker techniques can be identified
• Some vulnerabilities can be identified
Where to go for files...

www.rumint.com/interz0ne3
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 10.1.3.0.1080 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)

```bash
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&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: DoD Red Team
- Defenders: US Service Academies

Defenders lock down network, but must provide certain services