Beyond Ethereal: Crafting A Tivo for Security Datastreams

Gregory Conti
www.cc.gatech.edu/~conti
conti@cc.gatech.edu

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.
SecVis Demo
(one possible window)

- Sven Krasser design and implementation lead
- Code on CD
  - Caveats
  - Thanks to NETI@Home
  - Released under GPL
- See the research paper for more information

---

Gartner's Hype Cycle

Where are we now?

- Gartner Group

Thanks go to Kirsten Whitely for the Gartner curve idea
Potential DataStreams

- **Traditional**
  - pcap
  - snort
  - syslog
  - firewall logs
  - anti-virus
  - reconstruct streams
  - ...

- **Less traditional**
  - p0f
  - IANA data (illegal IP's)
  - reverse DNS
  - local data (unassigned local IPs)
  - inverted snort
  - active tools (e.g. nmap)
  - ...

- packet length (from Winpcap)
- Ethertype
- IP Transport Protocol
- Source/Destination IP
- TTL
- IP Header Len
- IP Version
- IP Diff Services
- IP Total Length
- IP Identification
- IP Flags
- IP Fragment Offset
- IP Header Checksum
- UDP Source/Destination Port
- TCP Source/Destination Port

---

RUMINT Main Screen

- Provide quick overview with minimal clutter
- Thumbnails act as menu
- Why “RUMINT”
Filtering, Encoding & Interaction

Filtering, Encoding & Interaction
Filtering, Encoding & Interaction

For More Information...

- **Dynamic Queries**

- **Requirements and Tasks**
  - Goodall. User Requirements and Design of a Visualization for Intrusion Detection Analysis

- **Semantic Zoom**

- **Noise in Internet Data**
  - Grizzard, Simpson, Krasser, Owen and Riley. Flow Based Observations from NETI@home and Honeynet Data. www.ece.gatech.edu/research/labs/nsa/papers/neti-honey.pdf

- **Automatic Filter Generation**

- **Human in the Loop Systems**
### Binary Rainfall Visualization

**(single packet)**

**Bits on wire...**

| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 |

**View as a 1:1 relationship (1 bit per pixel)...**

| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 |

24 Pixels
Network packets over time

Encode by Protocol

Bit 0, Bit 1, Bit 2 → Length of packet - 1
Encoding Headers

Navigation
Binary Rainfall Visualization
(single packet)

Bits on wire...
011011100101010010111110

View as a 1:1 relationship (1 bit per pixel)...
011011100101010010111110

View as a 8:1 relationship (1 byte per pixel)...
011011100101010010111110

3 Pixels

Binary Rainfall Visualization
(single packet)

Bits on wire...
011011100101010010111110

View as a 1:1 relationship (1 bit per pixel)...
011011100101010010111110

View as a 8:1 relationship (1 byte per pixel)...
011011100101010010111110

View as a 24:1 relationship (3 bytes per pixel)...
011011100101010010111110

1 Pixel
On the fly *strings*

![Rainfall strings](image1)

On the fly *disassembly?*

![Memory hex dump](image2)

---

1. Dataset: Defcon 11 CTF
2. Dataset: Honeynet Project Scan of the Month 21
A Variant:
Visual Exploration of Binary Objects

Textual vs. Visual Exploration
Comparing Executable Binaries

(1 bit per pixel)
Comparing Image Files
(1 bit per pixel)

image.jpg  image.bmp  image.zip  image.pae
(encrypted)

Comparing mp3 files
(1 bit per pixel)

the.mp3  pash.mp3  disguises.mp3

binary explorer demo
Byte Visualization

Byte Presence

dictionary file via HTTP  ssh  SSL
Byte Frequency

- dictionary file over HTTP
- ssh
- SSL
- streaming audio

byte frequency demo

Parallel Coordinates

- goal: plot any data fields
- dynamic columns
- change order for different insight
- intelligent lookup and translation of fields
  - e.g. IP transport protocol
Parallel Coordinates

Parallel Coordinates
(Streaming Audio)
Parallel Coordinates
(SOTM 21)

Scatterplot
(TCP destination port, Source IP, SOTM 21)
Krasser Visualization (secvis)

Routine Honeynet Traffic (baseline)
Slammer Worm

At a Glance Measurement

(Constant Bitrate UDP Traffic)
Port Sweep

Compromised Honeypot
Attacker Transfers Three Files...

Inbound botnet Traffic
Outbound botnet Traffic

Combined botnet/honeynet traffic
For more information...

Bit Rainfall (email me...)

Parallel Coordinate Plots
- Multidimensional Detective by Alfred Inselberg
  http://www.sims.berkeley.edu/academics/courses/is247/s04/resources/inselberg97.pdf

Byte Frequency Analysis

Krasser Visualization (see www.cc.gatech.edu/~conti)
- S. Krasser, G. Conti, J. Grizzard, J. Gribschaw and H. Owen; "Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization;" IEEE Information Assurance Workshop (IAW); June 2005.

Raffael Marty @ DEFCON

Open GL System Performance (secvis)

![Graph showing Open GL System Performance](image)
Win32 Performance
(SOTM 21, 3389 packets, rumint v1.60)

System Requirements

- IP over Ethernet
- Tested on Windows XP
- ~256+ MB Ram
- Processor 300MHZ (minimum)
- The more screen real estate the better
- Requires winpcap (I’ve used 3.0)

Development
  - Visual Studio 6
  - port to GCC and Open GL
  - PacketX for now
    - Go direct to (win)pcap

SOTM 21, AMD2800+, 1GB RAM
all visualizations at 1280x1024 except
byte frequency and presences which are fixed at 256x418
Inbound Campus Traffic
(5 seconds)

Campus Network Traffic
(10 msec capture)

inbound  outbound
Directions for the Future...

We are only scratching the surface of the possibilities

- **attack specific community needs**
- **plug-ins**
- launch network packets?
- **protocol specific visualizations**
  - including application layer (e.g. VoIP, HTTP)
- Open GL
- graph visualization+
- screensaver/wallpaper snapshot?
- work out GUI issues
- database of filters / smart books
- stress testing
- evaluate effectiveness

---

**Library of Tool Fingerprints**

- 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)
For more information...


--Talk PPT Slides

G. Conti; "Network Attack Visualization;" DEFCON 12; August 2004.

--Talk PPT Slides
--Classical InfoVis Survey PPT Slides
--Security InfoVis Survey PPT Slides

see www.cc.gatech.edu/~conti

Demo
Attacking the Analyst...

G. Conti, M. Ahamad and J. Stasko; "Attacking Information Visualization System Usability: Overloading and Deceiving the Human;" Symposium on Usable Privacy and Security (SOUPS); July 2005. On the CD...

G. Conti and M. Ahamad; "A Taxonomy and Framework for Countering Denial of Information Attacks;" IEEE Security and Privacy. (accepted, to be published) Email me...

DEFCON CTF DoI vs. DOS...

On the CD...

- Talk slides (extended version)
- Code
  - rumint
  - secvis
  - rumint file conversion tool (pcap to rumint)
- Papers
  - SOUPS Malicious Visualization paper
  - Hacker conventions article
- Data
  - SOTM 21.rum .pcap

See also: www.cc.gatech.edu/~conti and www.rumint.org CACM
Feedback Requested...

- Tasks
- Usage
  - provide feedback on GUI
  - needed improvements
  - multiple monitor machines
  - performance under stress
  - bug reports
- Data
  - interesting packet traces
  - screenshots
    - with supporting .rum and .pcap files, if possible
- Pointers to interesting related tools (viz or not)
- New viz and other analysis ideas

Volunteers to participate in user study

Acknowledgements

404.se2600, Kulsoom Abdullah, Sandip Agarwala, Mustaque Ahamad, Bill Cheswick, Chad, Clint, Tom Cross, David Dagon, DEFCON, Ron Dodge, EliO, Emma, Mr. Fuzzy, Jeff Gribschaw, Julian Grizzard, GTISC, Hacker Japan, Mike Hamelin, Hendrick, Honeynet Project, Interz0ne, Jinsuk Jun, Kenshoto, Oleg Kolesnikov, Sven Krasser, Chris Lee, Wenke Lee, John Levine, Michael Lynn, David Maynor, Neel Mehta, Jeff Moss, NETI@home, Henry Owen, Dan Ragsdale, Rockit, Byung-Uk Roho, Charles Robert Simpson, Ashish Soni, SOUPS, Jason Spence, John Stasko, StricK, Susan, USMA ITOC, IEEE IAW, VizSEC 2004, Grant Wagner and the Yak.
• 100+ Graduate Level InfoSec Researchers
• Multiple InfoSec degree and certificate programs

• Representative Research
  – User-centric Security
  – Adaptive Intrusion Detection Models
  – Defensive Measures Against Network Denial of Service Attacks
  – Exploring the Power of Safe Areas of Computation
  – Denial of Information Attacks (Semantic Hacking)
  – Enterprise Information Security

• Looking for new strategic partners, particularly in industry and government

www.gtisc.gatech.edu

Questions?

Greg Conti
conti@cc.gatech.edu
www.cc.gatech.edu/~conti
www.rumint.org