Better Tools for System Administration: Enhancing the Human-Computer Interface with Visualization

Bill Yurcik
<yurcik@ncsa.uiuc.edu>
Manager, NCSA Security Research

National Center for Advanced Secure Systems Research (NCASSR)
National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign

Overview

- Security System Administration
- Visualization (short)
- NCSA Approach: Three Working Tools

The Thin Blue Line: Security SysAdmins

- Current state of Internet Security
  - All metrics show bad -> worse
  - Unpatched software vulnerabilities
  - Point-and-click attack software requires little skill
  - Surveys show insider attacks greatest threat

N-Dimensional Security Solution Space:

- Large networks
  - Class B IP address space, 65,000 devices
- Complex networks:
  - 130K ports per computer (tcp/udp)
  - Heterogeneous hw platforms (intel,mac,sgi,sun)
  - Heterogeneous sw (OSs, applications)
  - Many services & protocols (web, mail, ftp, streaming...)
- Many types & dynamic nature of both
  - Vulnerabilities (hw, sw [OS/application], network...)
  - Attacks (worms, viruses, DoS, intrusions, ...)

System Administration

- High stress (interrupt driven)
- Constantly changing
- Takes years to master
- Different styles
  - "The Knob Tuners"
  - "The Developers"
  - "The Guru"
- Current Security SysAdmin Tools from "The Developers"
  - Command line and cryptic
  - Specific (seeing an elephant via many microscopes)
  - Dynamic (relearn)
  - Little or no interoperability between tools

Security System Administration

- Security policy development
- Security Incidence Response Team (IRT)
- Asset Management
- Authentication Systems
- Backup*
- Security Monitoring (traffic, systems, IDS, firewall)
- Patch coordination
- Vulnerability assessment (proactive scanning)
- Special system security administration
  - Webserver, mailer, ftp, firewall, IDS

More Specifically...

- Reporting of security state
- Vulnerability analysis results; progress on addressing vulnerabilities
- Surveillance for known patterns
- Discovery of unknown patterns
- Security policy enforcement
- Presentation of security architectures
- Detection of security events
- Explanation of event correlation/fusion
- Mission impact of security breaches
- Course-Of-Action (COA) selection
- COA Justification
Current Security Monitoring

Current Network Monitoring

Visualization

- Humans learn visually
  - 150 MB/sec
  - just-noticeable-difference
  - time dimension via animation “MTV generation”
  - leverage intuition “ecological design”
- Compact graphical representation
- Encourages exploration to make discoveries, decisions, explanations about
  - items
  - groups of items
  - patterns (trend, cluster, gap, outlier...)
- Direct manipulation strategies
  - immediate query with visual feedback, mouse pointing, reducing errors

Visualization

- Compact graphical representation
- Encourages exploration to make discoveries, decisions, explanations about
  - items
  - groups of items
  - patterns (trend, cluster, gap, outlier...)
- Direct manipulation strategies
  - immediate query with visual feedback, mouse pointing, reducing errors

Visual Tool Design

1) Overview
   Gain an overview of the entire collection
2) Zoom
   Zoom in on items of interest
3) Filter
   Filter out uninteresting items
4) Details-on-demand
   Select an item or group and get details when needed
5) Relate
   View relationships among items
6) History
   Keep a history of actions to support undo, replay, and progressive refinement
7) Extract
   Allow extraction of sub-collections and of the query parameters

NCSA Approach

“Know Thy Network”

- SIFT = Security Incident Fusion Tools
- Proposal – Increase Situational Awareness
  - How?
    - Visualization
    - Profiling
    - Data mining for discovery

The SIFT Approach
1. High Performance Cluster Computing: NVisionCC
2. System State View: NVisionIP
3. Link Analysis View: VisFlowConnect

Overview, zoom & filter, details-on-demand
Know Thy Network!

The Specific Cluster Security Problem

- Cluster becomes larger and thus harder to control
  - Titan (160 Nodes)
  - Mercury (256 Nodes)
  - Platinum (512 Nodes)
  - Tungsten (1450 Nodes)
- Current state of protecting cluster is dangerous
  - Most of cluster nodes are publicly accessible
  - Limited protection from border router
  - IDS not installed
  - Different hardware and software
- Little research on cluster security and no tool tailored for cluster security
  - all existing cluster monitor tools are focused on performance monitoring

What Could Go Wrong?

- One or more compute nodes could be compromised from Internet directly. (Public accessible)
- Cluster node is compromised from internal network. (Without even passing router)
- Some nodes communicate with machines outside cluster. (Is it suspicious?)

A Backend Cluster Security Systems

NVisionCC

Tool 1
High Performance Cluster Security
“NVisionCC”
Prioritized GUI

Individual Host Details

Tool 2
System State View
“NVisionIP”

NVisionIP Drill-Down Views

Small Multiple View
Our SIFT Approach

NVisionIP

Tool 3
Link Analysis View
“VisFlowConnect”

VisFlowConnect

Domain View

Internal View
Insights So Far…

• Humans are good at processing visual patterns (known)
• No expert knowledge required!
• Abstraction – finding the appropriate level of observation
• "Visual Debugging (problem-solving)
• Holistic Macro/Micro Views vs Divide-and-Conquer
• Though we think in pictures, we are no good at describing pictures (save functions)
• Capturing the time dimension of high-dimension data via animation is incredibly engaging to humans
• Success depends on effective HCI
  – Looking at new ways to augment systems administration in complex environments… (anti-autonomic)

Conclusions

• System Administrators are users too!
  (maybe more important to consider than end users)
• Security system administration is a natural application for better tools using visualization
  – Complex multi-dimensional space
  – Current security sysadmin tools are poorly designed
• Rough Consensus and Working Code
  – no more visualization design theory but rather lets bake-off and see what works best now
• Visualization tools are hard to develop but can quickly become impossible to live without

URL

http://www.ncassr.org/projects/sift/
also Google “vizsec” for ACM CCS Workshop