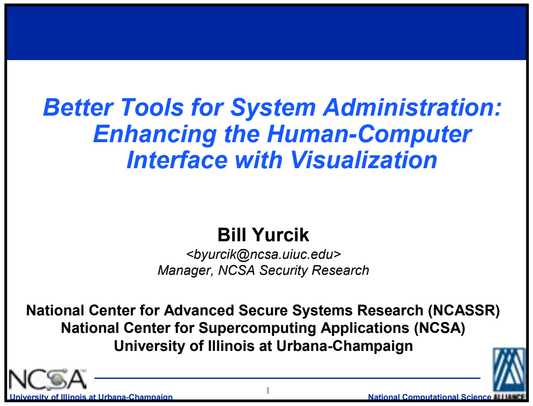
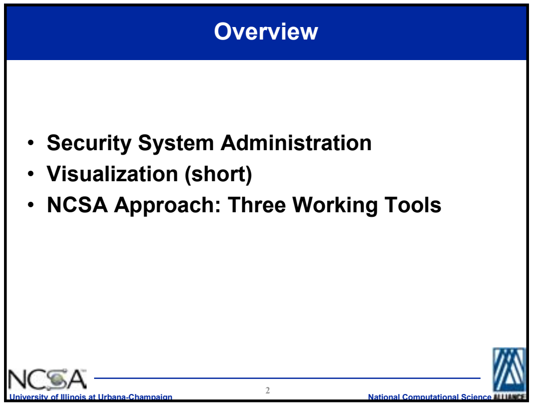


Better Tools for System Administration: Enhancing the Human-Computer Interface with Visualization

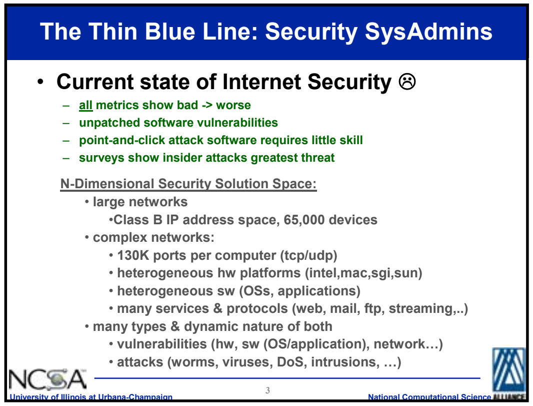
Bill Yurcik
<byurcik@ncsa.uiuc.edu>
Manager, NCSA Security Research

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



Overview

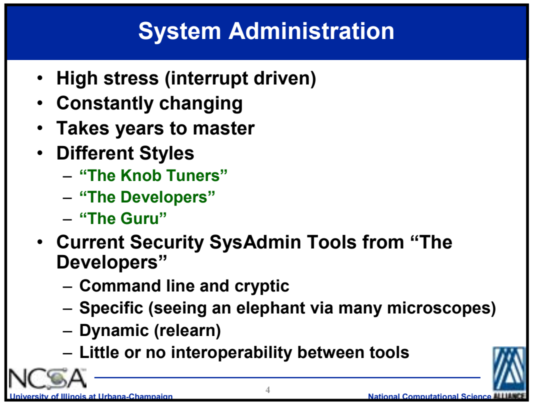
- **Security System Administration**
- **Visualization (short)**
- **NCSA Approach: Three Working Tools**



The Thin Blue Line: Security SysAdmins

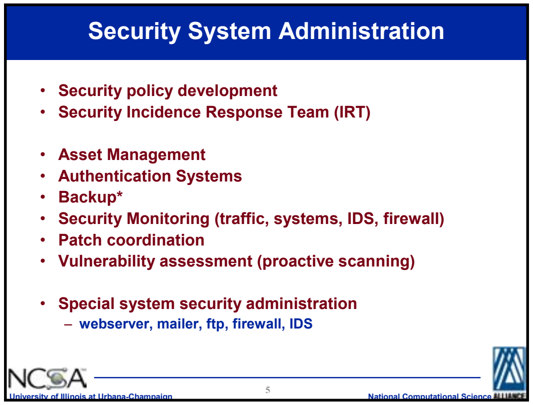
- **Current state of Internet Security ☹**
  - **all metrics show bad -> worse**
  - **unpatched software vulnerabilities**
  - **point-and-click attack software requires little skill**
  - **surveys show insider attacks greatest threat**

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**

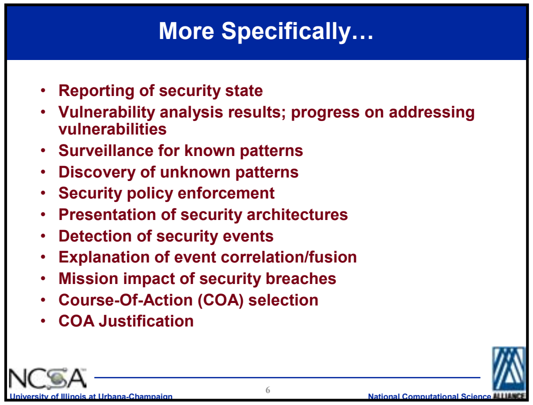


Security System Administration

- **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**



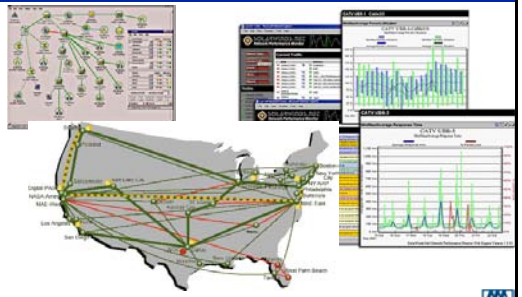
More Specifically…

- **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

Probe Followed by Attack (Attack Pattern)

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

Visual Tool Design

“overview, zoom & filter, details-on-demand”

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

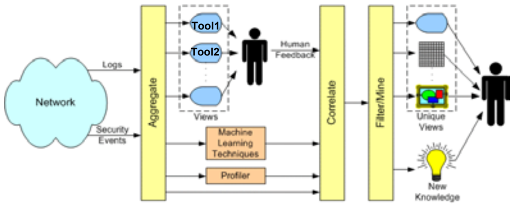
NCSA Approach

“Know Thy Network”

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

The SIFT Approach

Improved intrusion detection process and visualization



Three Working Security SysAdmin Tools

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!

Tool 1

High Performance Cluster Security

"NVisionCC"

The Specific Cluster Security Problem

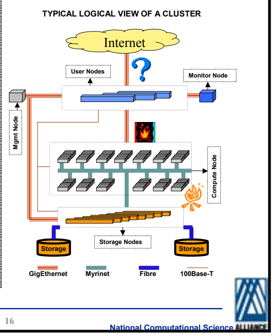
- Cluster becomes larger and thus harder to control
  - Titan (160 Nodes)
  - Mercury (256 Nodes)
  - Platinum (512 Nodes)
  - Tungsten (1450 Nodes)
- Current state of protecting cluster is dangerous
  - Most of cluster nodes are publicly accessible
  - Limited protection from border router
  - IDS not 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?

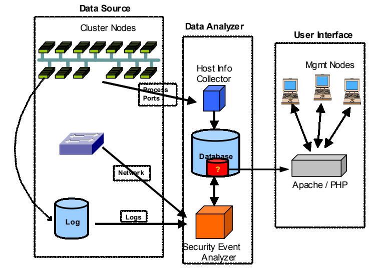
🔥 One or more compute nodes could be compromised from Internet directly. (Public accessible)

🔥 Cluster node is compromised from internal network. (Without even passing router)

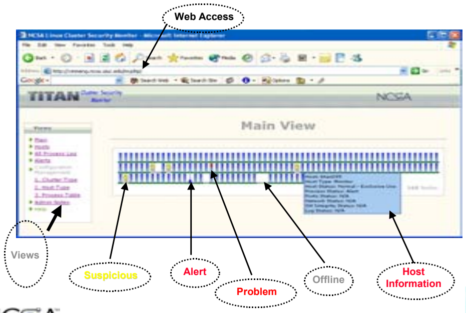
? Some nodes communicate with machines outside cluster. (Is it suspicious?)



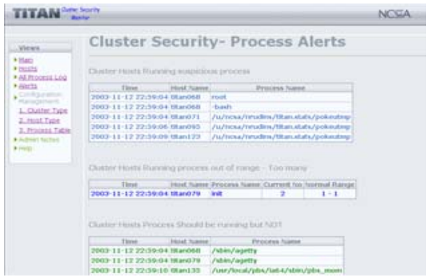
A Backend Cluster Security Systems



NVisionCC



Prioritized GUI



TITAN Cluster Security Monitor

NCSA

Views

- Main
- Hosts
- All Process Log
- Alerts
- Configuration Management
  - 1. Cluster Type
  - 2. Host Type
  - 3. Process Table
- Admin Notes
- Help

Cluster Security- Process Alerts

Cluster Hosts Running suspicious process

Time	Host Name	Process Name
2003-11-12 22:39:04	titan068	root
2003-11-12 22:39:04	titan068	-bash
2003-11-12 22:39:04	titan071	/u/ncsa/nrudins/titan.stats/pokeutmp
2003-11-12 22:39:06	titan095	/u/ncsa/nrudins/titan.stats/pokeutmp
2003-11-12 22:39:09	titan123	/u/ncsa/nrudins/titan.stats/pokeutmp

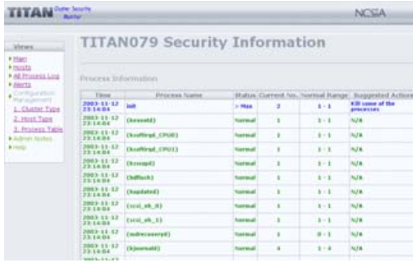
Cluster Hosts Running process out of range - Too many

Time	Host Name	Process Name	Current No.	Normal Range
2003-11-12 22:39:04	titan079	init	2	1 - 1

Cluster Hosts Process Should be running but NOT

Time	Host Name	Process Name
2003-11-12 22:39:04	titan068	/sbin/agetty
2003-11-12 22:39:04	titan079	/sbin/agetty
2003-11-12 22:39:10	titan133	/usr/local/pbs/ia64/sbin/pbs_mom

Individual Host Details



TITAN Cluster Security Monitor

NCSA

Views

- Main
- Hosts
- All Process Log
- Alerts
- Configuration Management
  - 1. Cluster Type
  - 2. Host Type
  - 3. Process Table
- Admin Notes
- Help

TITAN079 Security Information

Process Information

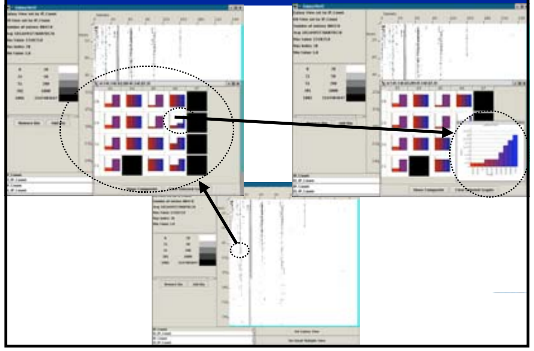
Time	Process Name	Status	Current No.	Normal Range	Suggested Action
2003-11-12 23:14:04	init	> Max	2	1 - 1	Kill some of the processes
2003-11-12 23:14:04	(keventd)	Normal	1	1 - 1	N/A
2003-11-12 23:14:04	(ksoftirqd_CPU0)	Normal	1	1 - 1	N/A
2003-11-12 23:14:04	(ksoftirqd_CPU1)	Normal	1	1 - 1	N/A
2003-11-12 23:14:04	(kswapd)	Normal	1	1 - 1	N/A
2003-11-12 23:14:04	(bdflush)	Normal	1	1 - 1	N/A
2003-11-12 23:14:04	(kupdated)	Normal	1	1 - 1	N/A
2003-11-12 23:14:04	(scsi_eh_0)	Normal	1	1 - 1	N/A
2003-11-12 23:14:04	(scsi_eh_1)	Normal	1	1 - 1	N/A
2003-11-12 23:14:04	(mdrecoveryd)	Normal	1	0 - 1	N/A
2003-11-12 23:14:04	(kjournald)	Normal	4	1 - 4	N/A

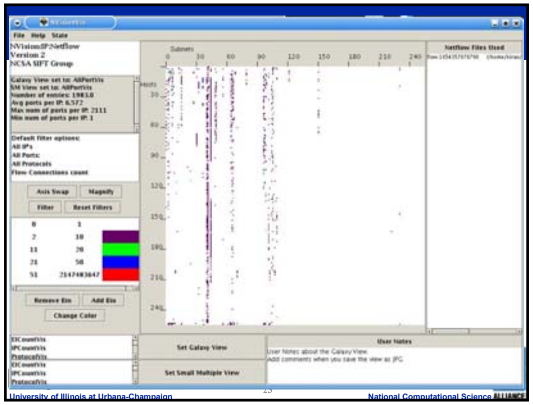
Tool 2

System State View

"NVisionIP"

NVisionIP Drill-Down Views





NVisionIP:Netflow
Version 2
NCSA SIFT Group

Galaxy View set to: AllPortVis
SM View set to: AllPortVis
Number of entries: 1983.0
Avg ports per IP: 6.572
Max num of ports per IP: 2111
Min num of ports per IP: 1

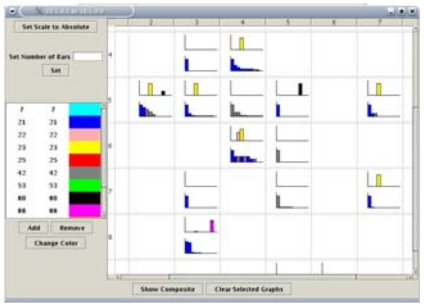
Default filter options:
All IP's
All Ports:
All Protocols
Flow Connections count

0	1	
2	10	🟪
11	20	🟩
21	50	🟦
51	2147483647	🟥

ElCountVis
IPCountVis
ProtocolVis
ElCountVis
IPCountVis
ProtocolVis

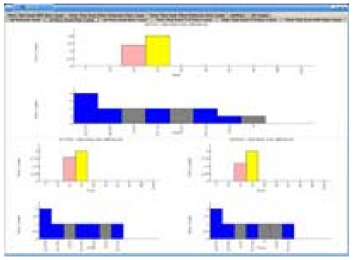
User Notes about the Galaxy View.
Add comments when you save the view as JPG

Small Multiple View

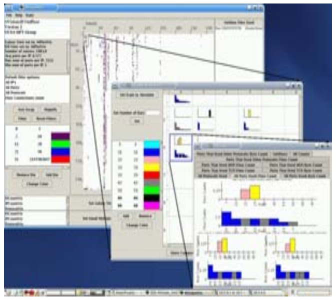


7	7	🟦
21	21	🟦
22	22	🟥
23	23	🟨
25	25	🟥
42	42	⬜
53	53	🟩
80	80	⬛
88	88	🟪

Our SIFT Approach



NVisionIP

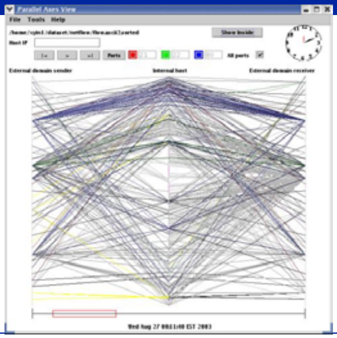


Tool 3

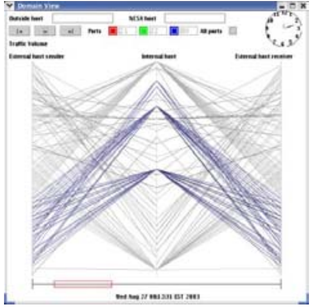
Link Analysis View

"VisFlowConnect"

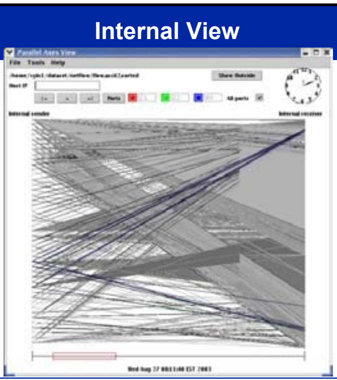
VisFlowConnect

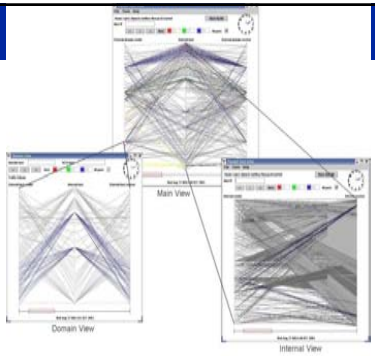


Domain View



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 <u>now</u>
- Visualization tools are hard to develop but can quickly become impossible to live without

URL

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

also Google “vizsec” for ACM CCS Workshop