Correlation between NetFlow System and Network Views for Intrusion Detection

Cristina Abad, Yifan Li*, Kiran Lakkaraju, Xiaoxin Yin and William Yurcik

Presented by
Yifan Li

National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign
On Intrusion Detection

• IDSs are important to protect networked systems

• However, intrusion detection is difficult:
  – many attacks, new attacks, changing all the time
  – poor performance (false positives)
  – information overload to human users
  – scalability (huge data volume, data management)
  – many logs, each with different purposes and formats
Information Visualization for Intrusion Detection

• Leverage human cognitive abilities
• Promotes quick mental connections between security events
• Help reduce the amount of time spent tracing attacks
• Allows less experienced users to better understand the security events
Visualizing NetFlows

• NetFlows: obtained by hardware (Cisco) or software (Argus)
• Contain summarized traffic information
• We visually represent them in two views:
  – System
    • NVisionIP
  – Network
    • VisFlowConnect
• Correlating information presented in both enhances the intrusion detection process
NVisionIP System Views

• Built within D2K (Data-to-Knowledge)
• Three main views:
  – Galaxy View
  – Small Multiple View
  – Machine View
• Statistical information is collected for each host
• Extensive filtering capabilities
Galaxy View

[Diagram of Galaxy View software interface with labeled components]

National Center for Supercomputing Applications
Small Multiple View and Machine View
VisFlowConnect Network Views

• Visualize information between hosts:
  – Internal – External
  – Internal – Internal
• A point in each axes represents a host or a subnet
• Displays to and from traffic
• Extensive filtering capabilities
• Traffic pattern changes can be easily identified
• Animation
VisFlowConnect
Main View and Domain View

Parallel Axes View
- Open file
- Show domain
- Host IP: 128.17.0.0

Domain View
- Outside host: 215.60.30.14
- NCSA host: 237.169.41.00

Sun Aug 03 01:21:39 CDT 2003

National Center for Supercomputing Applications
Enhancing the Intrusion Detection Process

**NVisionIP**
- Visualize pattern changes
- Filter anomalous IP/subnet
- Filter particular port
- Visualize activity on unusual ports

**VisFlowConnect**
- One-to-many
- Many-to-one
- Increased bandwidth consumption
- Asymmetry
- Pattern changes
One-to-Many Pattern
Combination of the Tools

• What can we say about the figure?
  – Malicious scan?
  – Known software to help find vulnerabilities of the system?

• Use NVisionIP
  – Filter out those known ports

• More in the paper …
Link Analysis & Our Work

• Reveals complex patterns of correlations between individual values
  – understand the hidden structure of investigated data
  – isolate interested patterns for further investigation

• NVisionIP and VisFlowConnect
  – only significant links shown
  – interesting patterns identified
Future Work

Network -> Logs

Security Events -> Network

Logs -> Aggregate

Security Events -> Network

Aggregate -> Views

Views -> Machine Learning Techniques

Views -> Profiler

Machine Learning Techniques -> Correlate

Profiler -> Correlate

Correlate -> Filter/Mine

Correlate -> Human Feedback

Filter/Mine -> Unique Views

Unique Views -> New Knowledge

New Knowledge -> Human Feedback

Human Feedback -> Filter/Mine

Filter/Mine -> New Knowledge

Human Feedback -> Filter/Mine

NCSA

National Center for Supercomputing Applications
Questions?

http://www.ncassr.org