Proposing a Multi-touch Interface for Intrusion Detection Environments

Jeffrey Guenther, Fred Volk, and Mark Shaneck
The Problem

- Huge text-based network logs with more being created every second
- Context is difficult to acquire from detail level tools
- And only Jim knows what is really going on
Analysts need tools which:

• Handle LARGE datasets
• Provide context
• Afford exploration
• Manage cognitive load

Essentially, the **Fundamental Problem** of Visual Analytics
Current Visualizations

- Consensus on the need for more interactivity
  - Access to both detail and contextual information

- See Section 2.1 for a more detailed discussion
Getting to Know Analysts

• Need more than a CTA
• Activity Theory
  – provides a theoretical basis
  – need a multi-methods approach
Applying Activity Theory Example

- Activities – keeping the network
- Actions – reviewing logs
- Operations – changing the configuration of a network sensor
A New Design Approach
A look at requirements:

- Monitoring
- Analysis
- Response
- Knowledge Management
Monitoring

- Identify network state at a glance
- Use pre-attentive visual properties to control the amount required attention
Analysis

• Goal: to develop understanding
• Multiple views at different levels of data abstraction
Response

- Network management
- Parts of response:
  - Record the happening of an event
  - Affect network changes
Knowledge Management

• Capture Jim’s experience
• Provides a library of case studies for future training
• Must be a by product of using the tool, not an extra step
Our Design
Multi-touch based network analytics tool
Affordances

• Physical (embodied) interaction with interface
• Gestures
• Faster interaction than with a mouse
Zoomable, Spatial Exploration
Time

devcomponents.com
Using Metadata

• To learn context
• To describe interactions -> create knowledge base
ActionLine

1. Select start of action segment
2. Select end of action segment
3. Touch selected segment. Action menu shown
User-refined Alert Correlation

• Make alert correlation interactive
  – Guided exploration of data

• Allow addition/removal of events from attack
• Correlation computation updated
Wrapping Up

• Exposed the need for a multi-method research
• List of Requirements:
  – Monitoring
  – Analysis
  – Response
  – Knowledge Management
• Argued for a new mode of interaction
Questions?