Visual Network Forensic Techniques and Processes

Robert F. Erbacher
Kim Christiansen, Amanda Sundberg
Department of Computer Science
Utah State University
Logan, UT 84322
Main Goals

• Create a good network forensic process
• Identify how visualization fits into process
• Identify needed and lacking capabilities
• Position our capabilities into these needs
• Create an effective process for the design of visualizations techniques to ensure goals are met
  – Design visualization techniques
Current Lackings

- **Interaction techniques**
  - Visualization techniques are not designed with the interaction in mind and only incorporate limited interaction capabilities

- **Analysis of the analysis**
  - Need to collect data on the analysis performed by experts and analyze this data to improve efficiency and identify legal validity
Current Lackings

• What does data duplication mean?
  – Encryption/attribution/validation

• What techniques are needed?
  – i.e., what capabilities do analysts need

• What is required for legal validity?
  – Conversely, what will prevent legal validity
Visualization Design Processes

- Visualizations designed for the data
- Visualization designed for interaction
  - Iterative process
- Do not forego other tools
  - Incorporate other tool capabilities/results
  - Improves capabilities/effectiveness/focus
- Repeated evaluation throughout process
Other Visualization Considerations

- **Cognitive task analysis (CTA)**
  - Done for network analysis
  - Deviations?
- **Human perception**
  - What improves/detracts visual comprehension
- **Scalability**
  - Need to enable analysis of terabytes of data
- **Current techniques result in data needing further analysis**
Example Visualization

- Designed for network forensics
- Design of visuals tightly integrated with design of interactions
- With forensics, interaction is primary goal
  - It empowers analysis
- Changing parameter mappings allows clustering of attacks
  - Based on attack type/characteristics
Visualization Example
Interaction: Filtering

Example: Remote IP: 10.7.1.12, Remote Port (nothing), Local IP (nothing), Local Port: 1500. This will filter all packets with remote IP, and Local port matching those given but with any Local IP or Remote Port.
Interaction: Direct Filtering
Interaction: Group Selection
Other Unanswered Questions

• Define network and computer forensics
  – Network forensics can incorporate computer forensics

• Who is target audience?
  – Law enforcement
  – Corporate analysts
  – Corporate legal
  – Home users???
Conclusions

• Identified needs of network forensics
  – Process has hardly been touched
• Identified requirements/processes for designing visualizations to meet needs
  – Focused on data analysis
  – Can be applied to analysis of analysis data
• Designed initial visualization techniques
Future Work

• Refine process
  – Finer granularity
• Attack remainder of process
• Examine multi-sensor data
• Resolve with computer forensics