

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

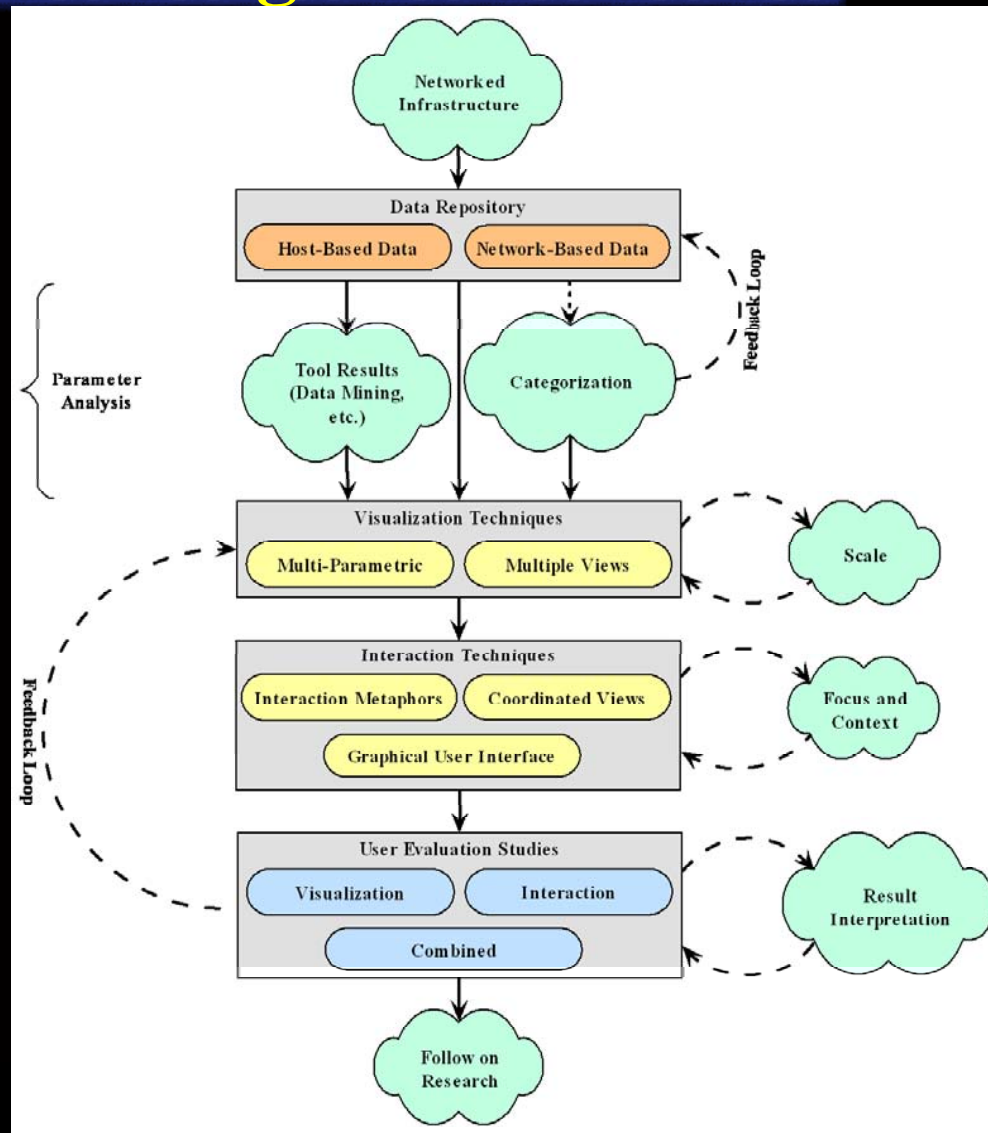


Current Lackings

- **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



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**

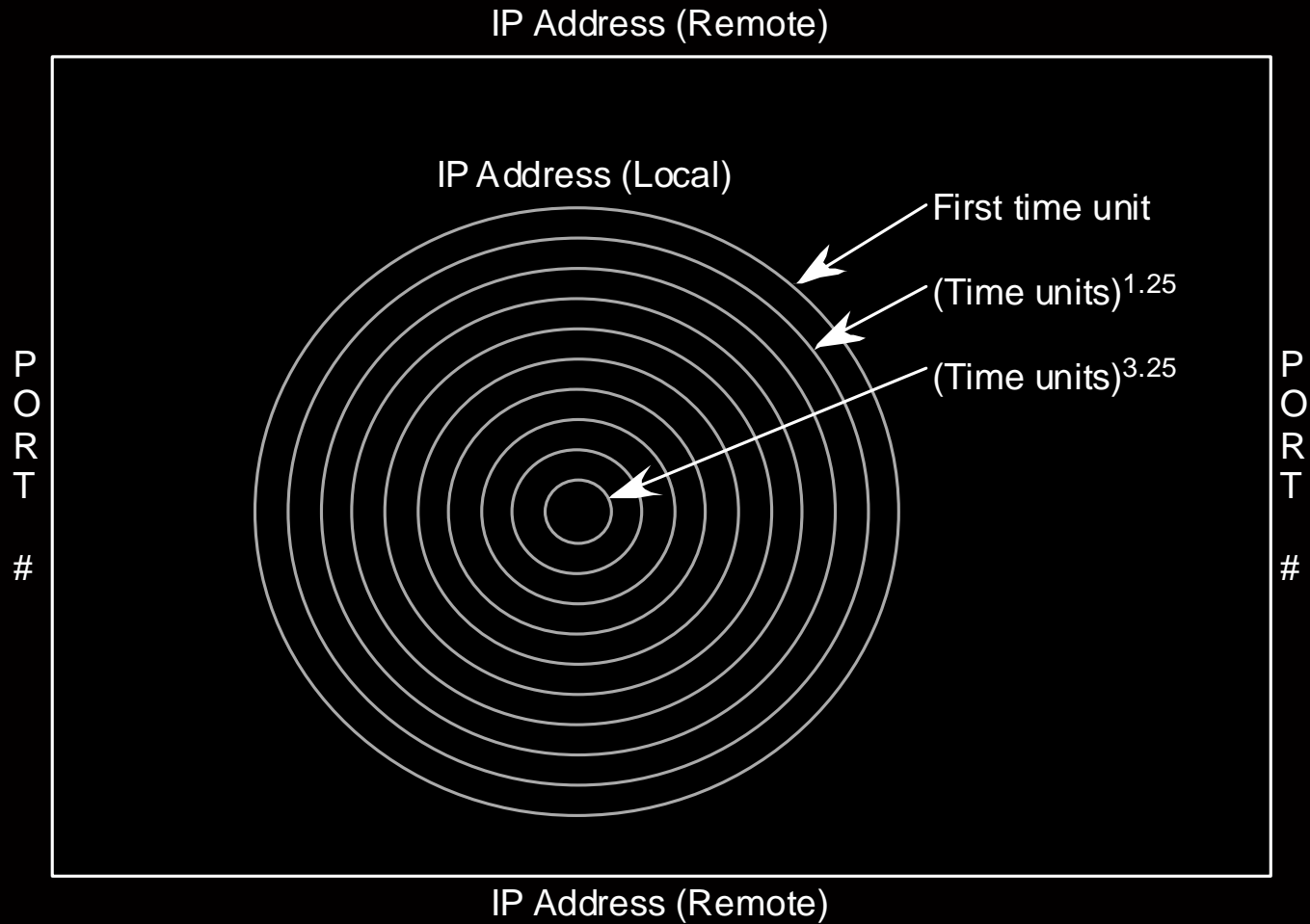


Example Visualization

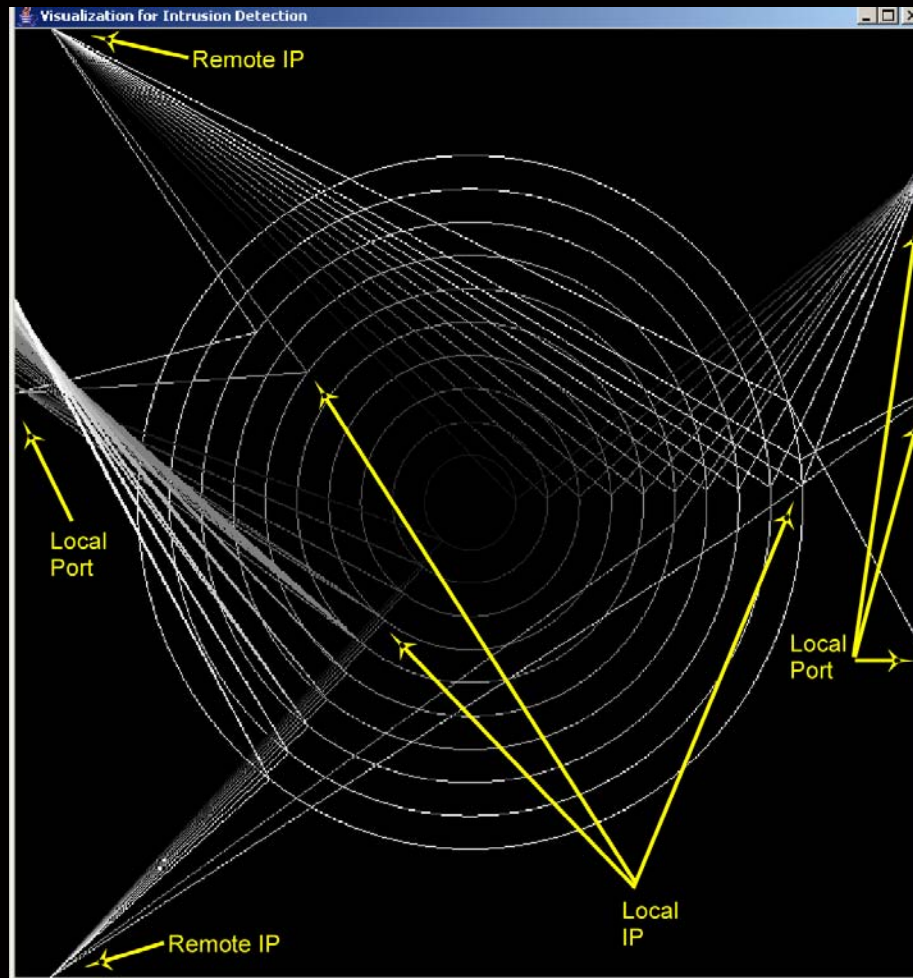
- Designed for network forensics
- Design of visuals tightly integrated with design of interactions
- With forensics, interaction is primary goal
 - It empowers analysis
- Changing parameter mappings allows clustering of attacks
 - Based on attack type/characteristics



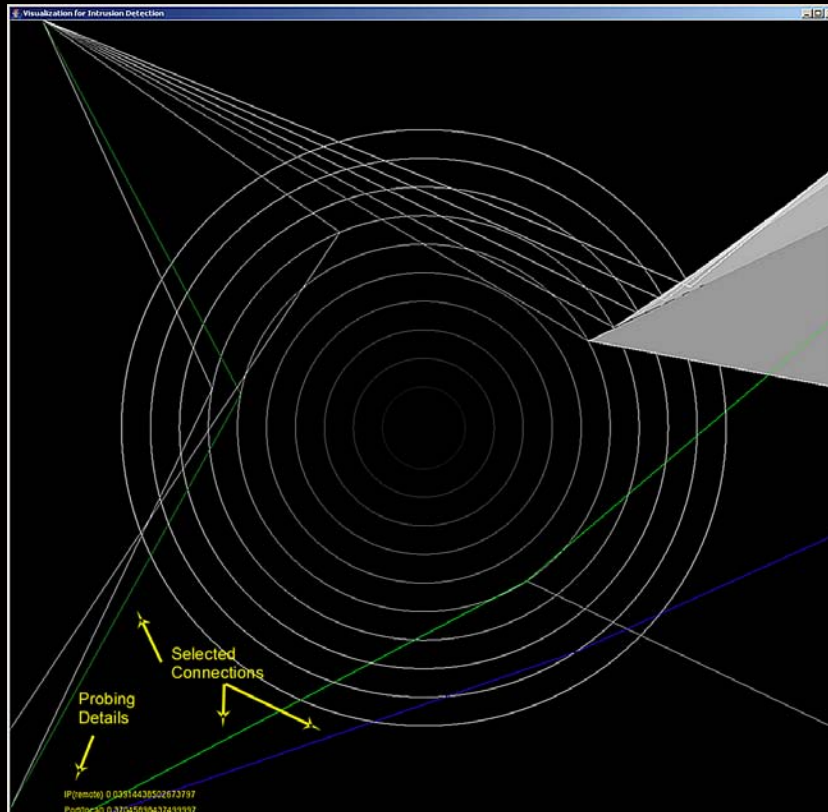
Visualization Design



Visualization Example



Basic Interaction: Probing



Main User Interface

File Filter Highlight Statistics

Run Vis. Mapping1 Edit Behavior Rate Control Packet Contents Misc. Help

8:43:52.354 8:44:1.892 8:45:49.784

```
Source IP: 10.100.1.101
Dest IP: 10.7.1.251
Source Port: 1598
Dest Port: 1505
Packet Length: 60
Time: 3/14/03 8:45:49.784
Type: 0
Flags: 0
Flags: 16
Remote Port Percent: 0.38408203124999996
Local IP Percentage: 0.039096850861556745
Local is the: Destination
Number of Packets: 92
```

The Color of this packet is: Remove

< << Stop Start >> >| stopped



Interaction: Filtering

Add a Filter

Filter by:

Remote IP (ex. 123.45.6.8)

Remote Port (ex. 1234)

Local IP (ex. 123.45.6.8)

Local Port (ex. 2345)

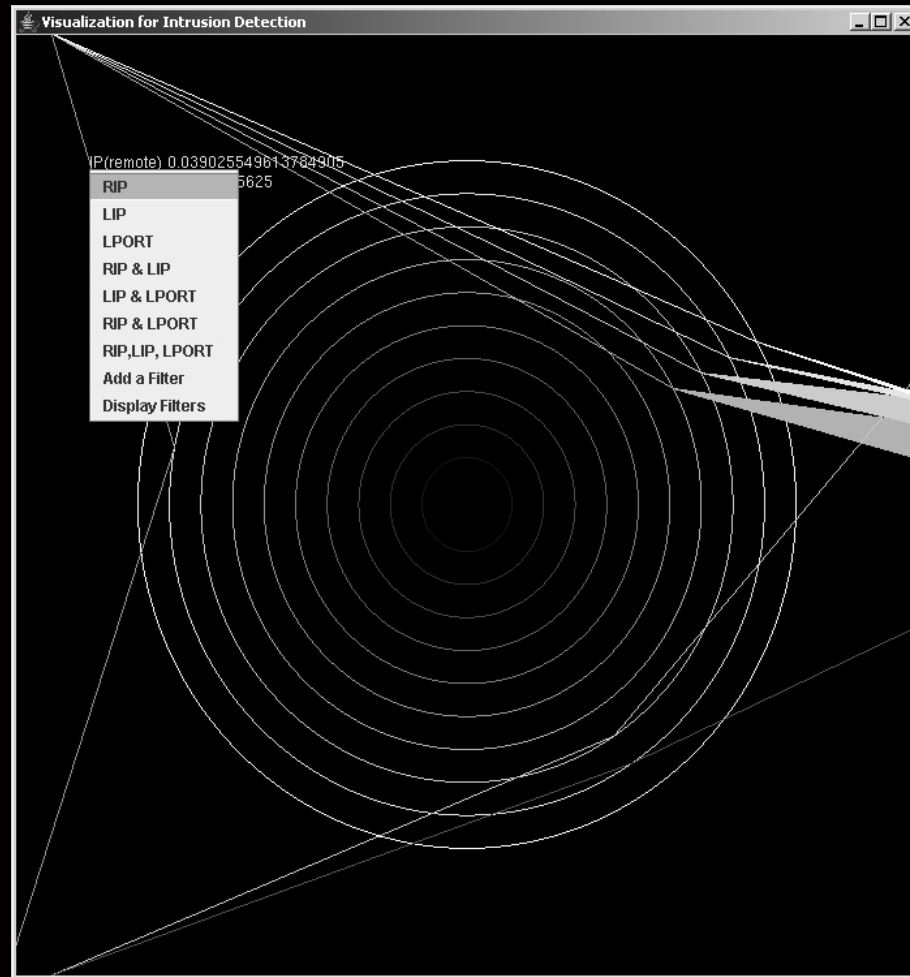
Example: Remote IP: 10.7.1.12, Remote Port(nothing), Local IP(nothing), Local Port: 1500. This will filter all packets with remote IP, and Local port matching those given but with any Local IP or Remote Port.

Display Filters

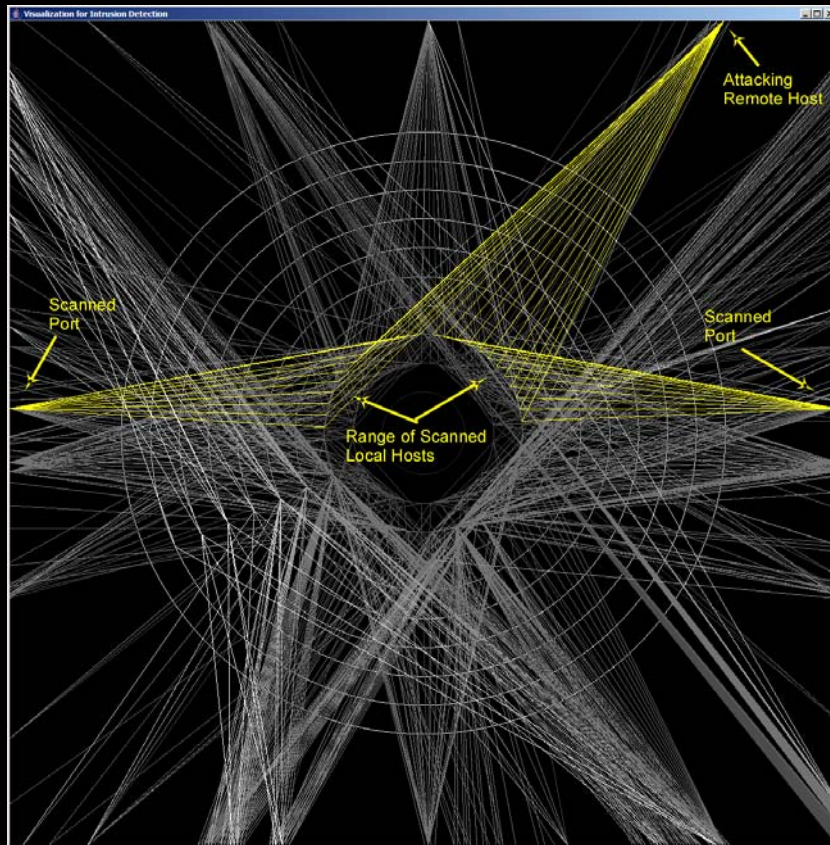
Checkboxes	Remote IP	Remote Port	Local IP	Local Port
<input type="checkbox"/>	-----	80	-----	-----
<input type="checkbox"/>	-----	-----	-----	80
<input type="checkbox"/>	-----	137	-----	-----
<input type="checkbox"/>	-----	-----	-----	137
<input type="checkbox"/>	-----	138	-----	-----
<input type="checkbox"/>	-----	-----	-----	138
<input type="checkbox"/>	-----	139	-----	-----
<input type="checkbox"/>	-----	-----	-----	139



Interaction: Direct Filtering



Interaction: Group Selection



Filter Based On Selected Packets

Remove	Show Params	TimeStamp	RIP	RPort	LIP	LPort	RIP	RPort	LIP	LPort
<input type="checkbox"/>	Show 1	6/1/05 17:5:43.540	220.70.105.55	1541	129.123.29.4	3306	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show 2	6/1/05 17:5:46.506	220.70.105.55	1541	129.123.29.4	3306	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show 3	6/1/05 17:5:47.49	220.70.105.55	1564	129.123.29.26	3306	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show 4	6/1/05 17:5:50.20	220.70.105.55	1564	129.123.29.26	3306	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show 5	6/1/05 17:5:47.50	220.70.105.55	1568	129.123.29.30	3306	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show 6	6/1/05 17:5:50.21	220.70.105.55	1568	129.123.29.30	3306	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Max To Display Remove Clear Checkboxes Set Up Default Apply Cancel



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**

