Using Geographic Information Systems for Enhanced Security Visualization

Matthew Dunlop

David Shelly

Agenda

- Purpose
- Problem
- Study
  - Design
  - Results
- Prototype
- Future

Purpose

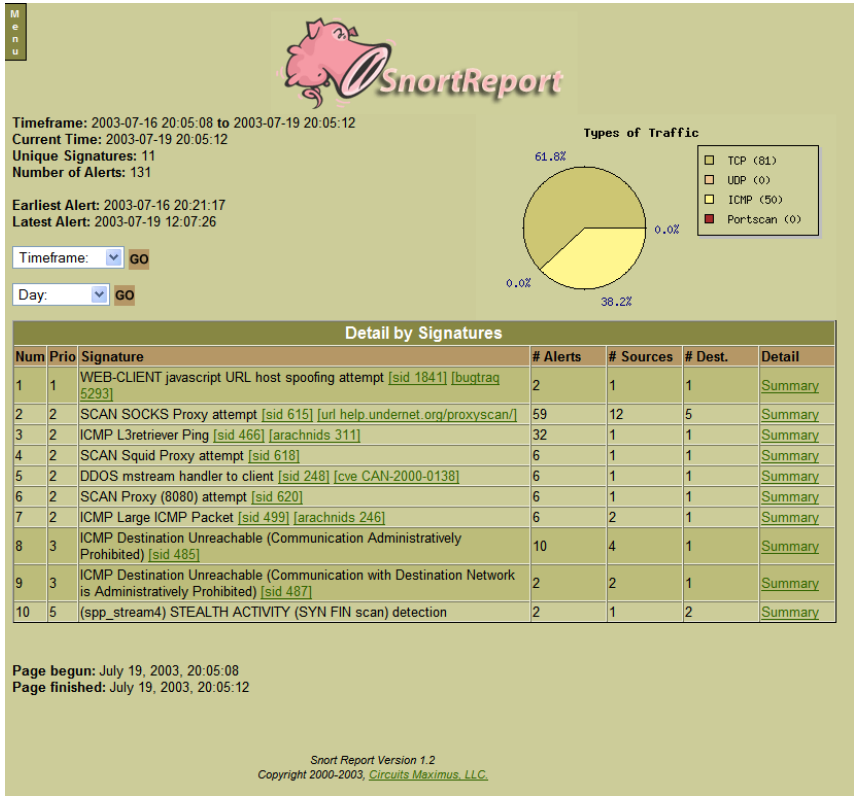
- To design a usable security visualization prototype tool that leverages global information systems (GIS)
  - Present security information more clearly
  - Facilitate rapid identification of network security shortcomings
  - Allow better protection of critical network assets

Problem

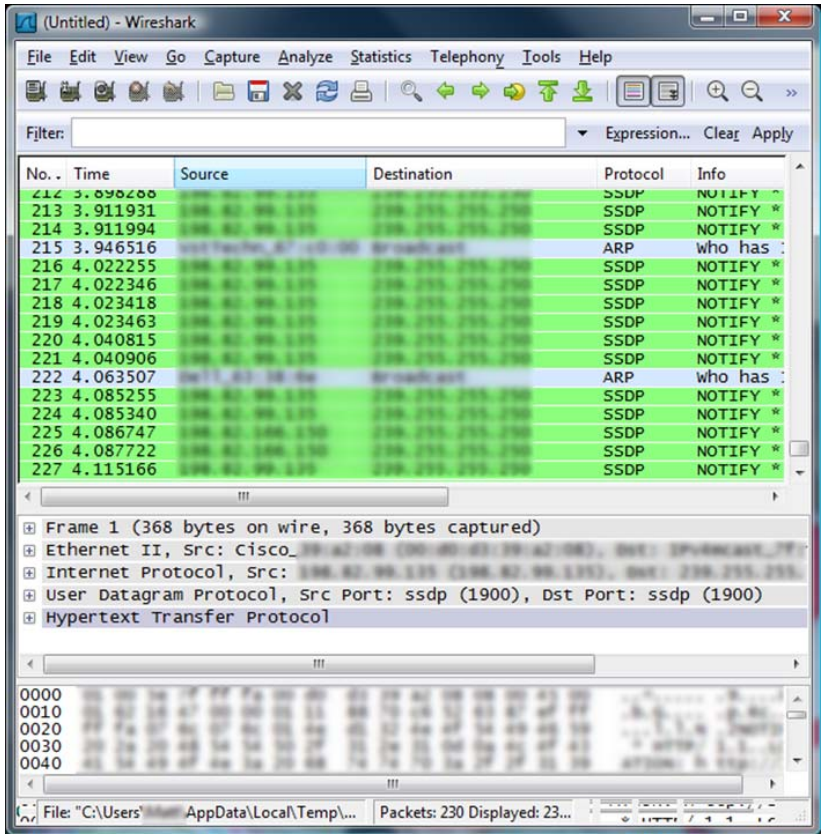
- Information overload
  - VT processes over 5 million emails per day
  - Manages over 500 SMTP & 3500 HTTP servers
- Analysts rely on multiple tools
  - Analysis takes more time
- Popular tools are not very *usable*
  - Primarily text based
  - Do not scale well for large networks
  - Graphical representations are not intuitive
- *GIS adds context as well as scalability*

Current Security Tools – Text-based

Snort

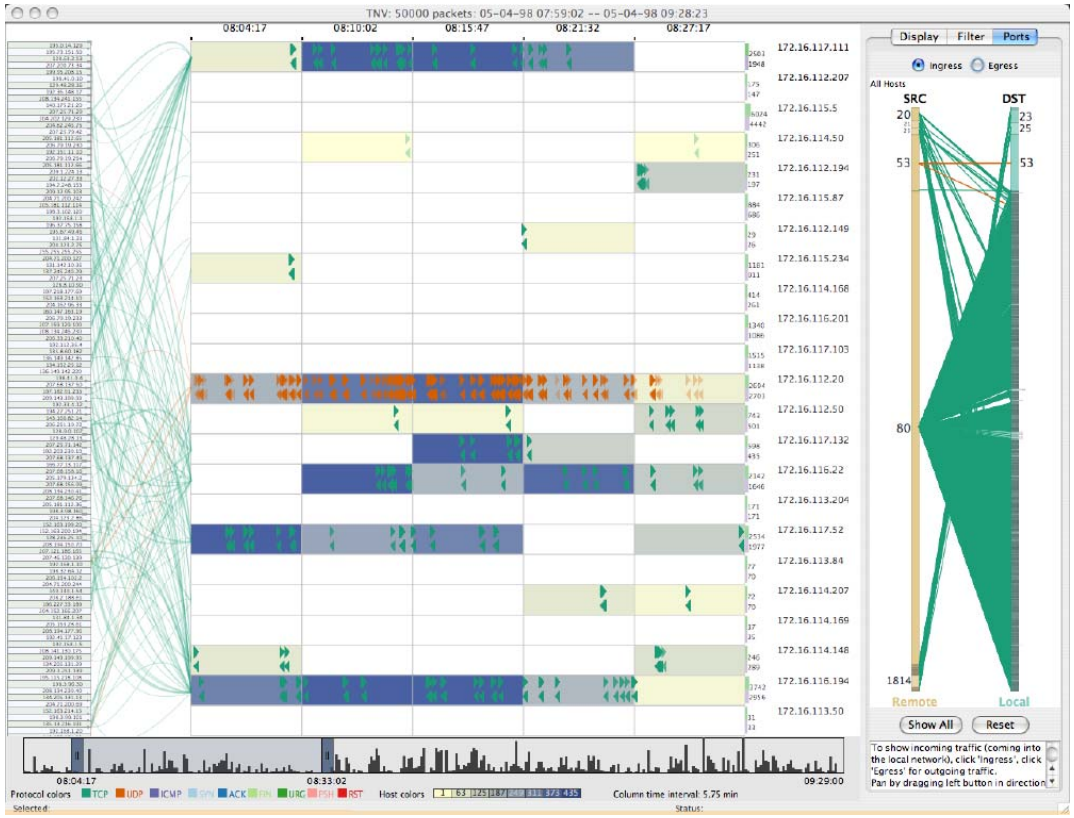


Wireshark

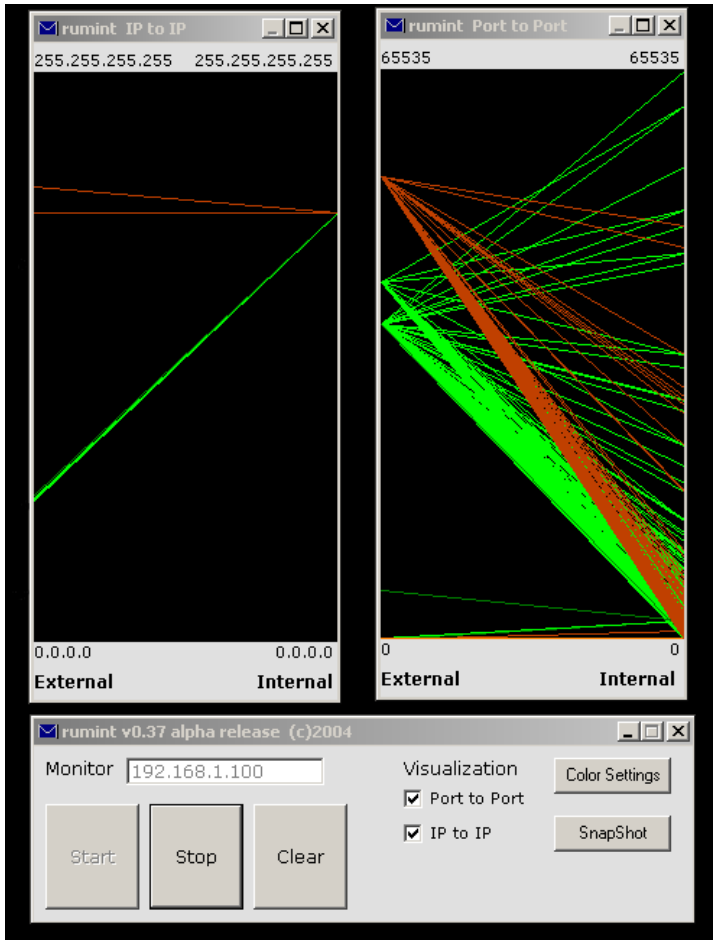


Current Security Tools – Graphical

The Network Visualizer



Rumint



Study Design - Participants

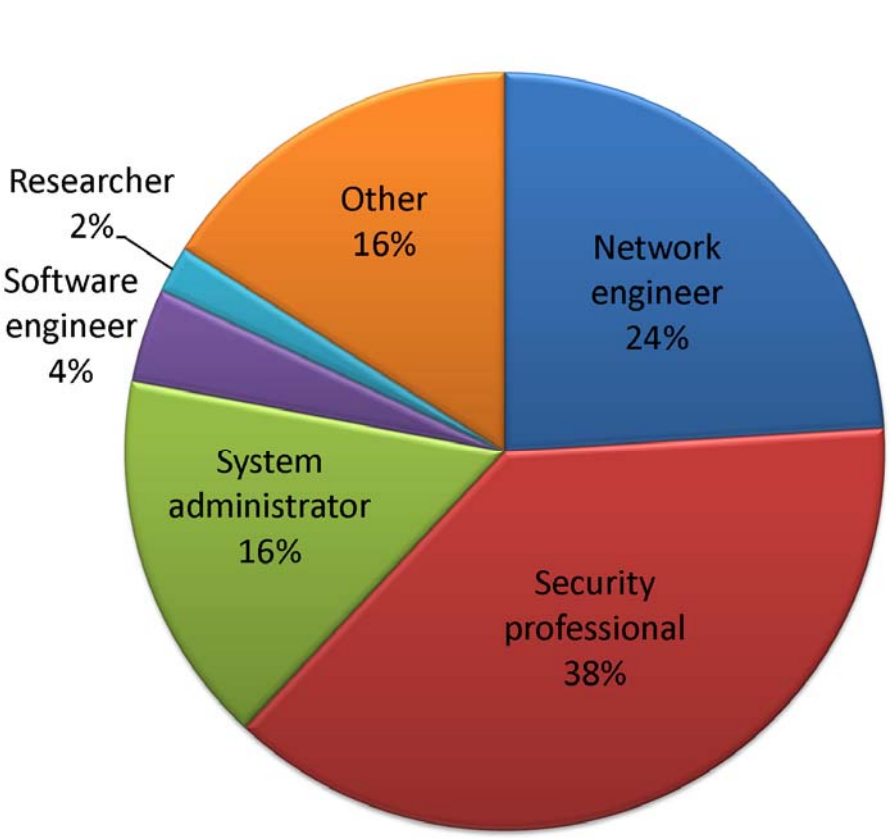
- Virginia Tech system administrators
- SANS IT professionals
- U.S. Army network engineers

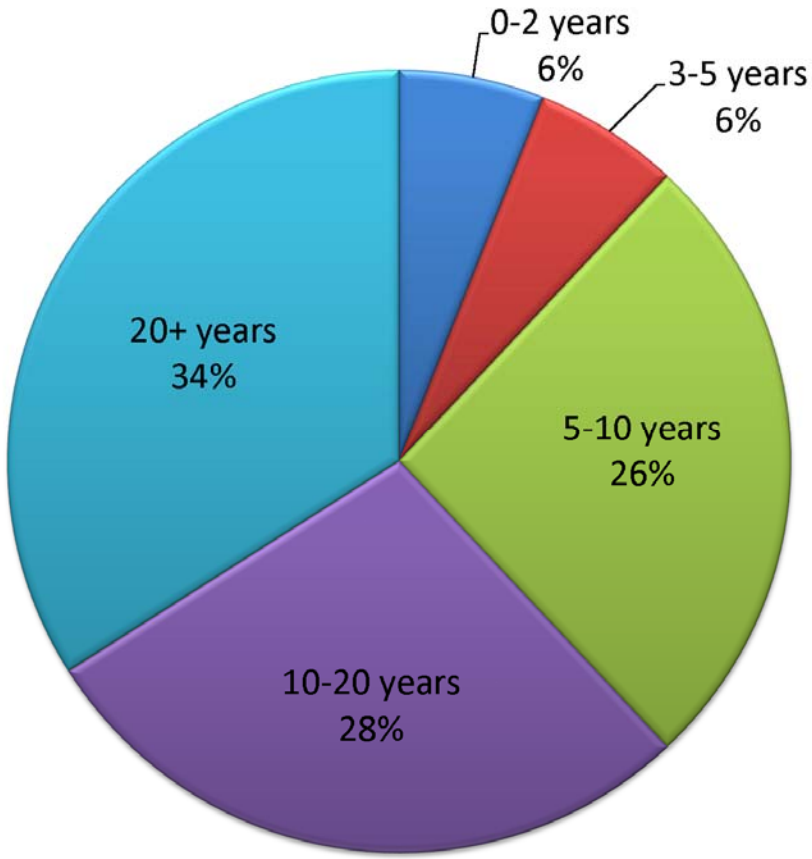
50 respondents

Study Design – Question Areas

- Background Information
- System Information
- Security Information
- Security Tools
- GIS Information

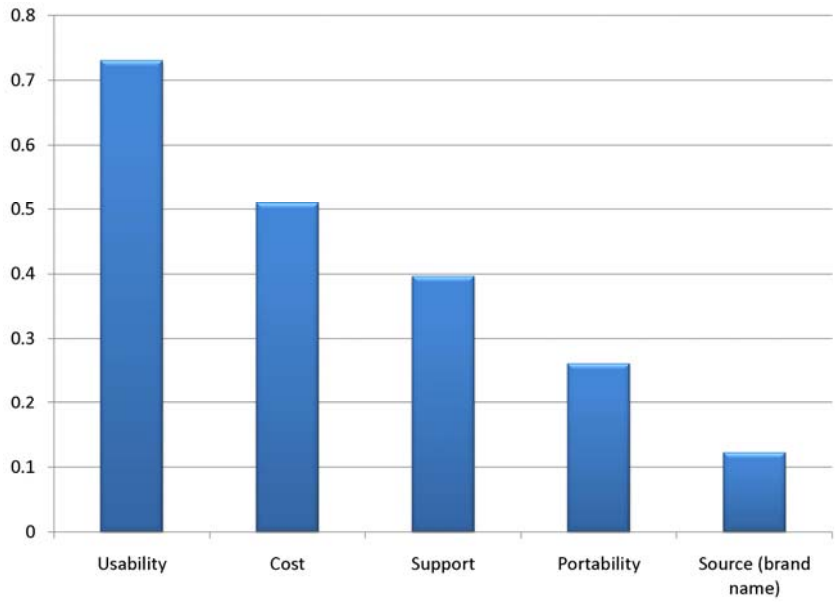
Study Results – Background





Study Results - Preferences

Most important aspects of security tools



- Top usability improvements
  - Improved user interface
  - Better summary of information
  - Improved visual representation
- Other findings
  - Prefer customizability
  - Multiple tools = longer time to isolate threats

Study Results - Visualization

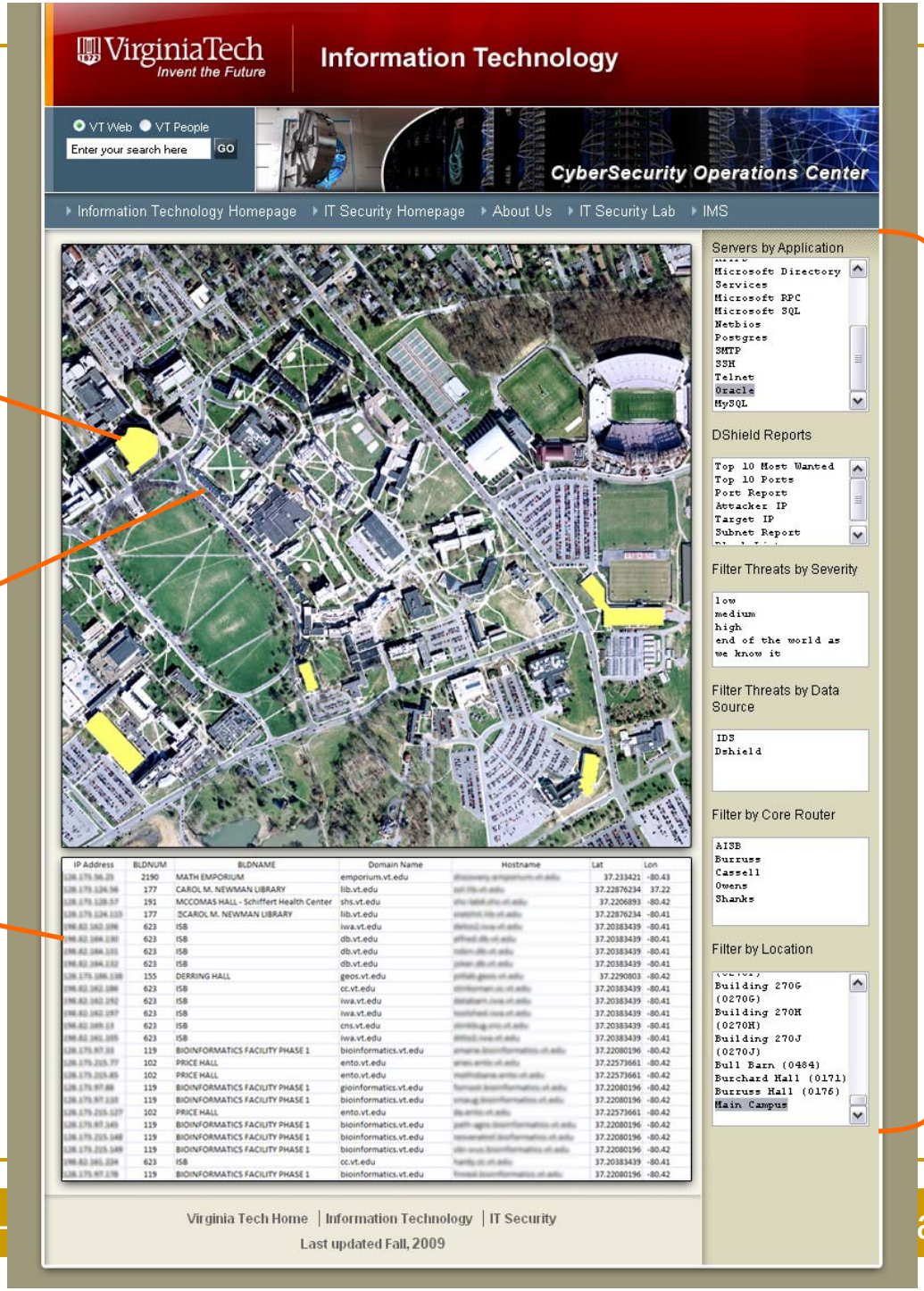
- Visualization not widely used
  - 50% never used it to visualize networks
  - 76% never used it to visualize security
- Openness to GIS visualization
  - 76% feel GIS tool would be useful for network visualization
  - 50% envision using it for security visualization
- Helpful in explaining security to technical and nontechnical audiences

Prototype Design

Color-coded security status

Ability to drill down

Device details



Filtering options

Detailed View

Future Work

- Build working model of prototype
- Conduct usability study

Questions