
Using Geographic Information Systems for Enhanced Security Visualization



Matthew Dunlop
David Shelly

Agenda

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

Purpose

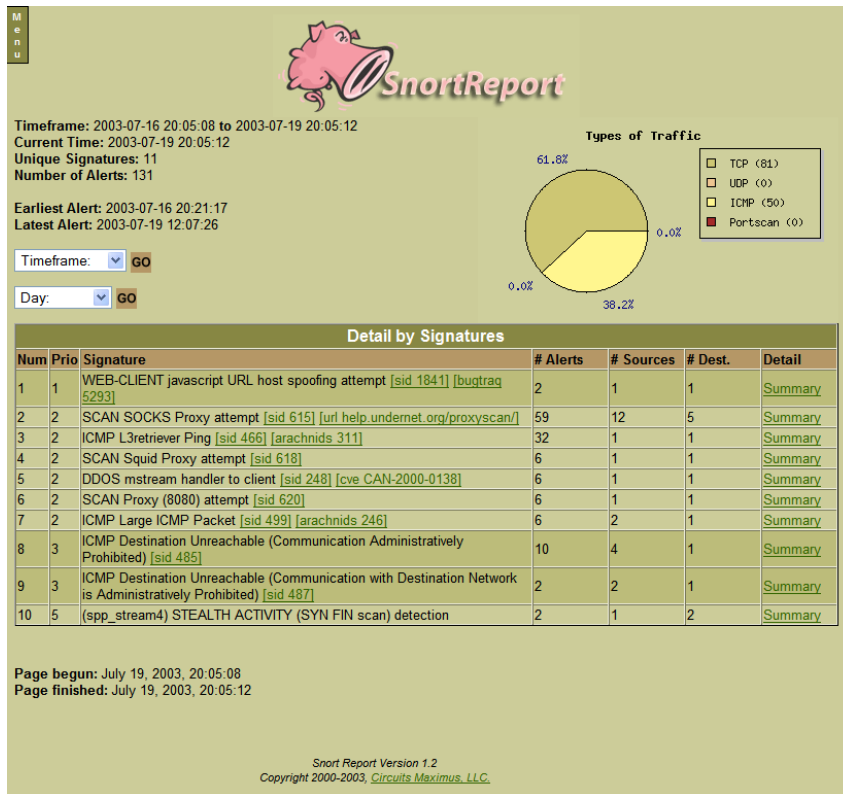
- To design a usable security visualization prototype tool that leverages global information systems (GIS)
 - Present security information more clearly
 - Facilitate rapid identification of network security shortcomings
 - Allow better protection of critical network assets

Problem

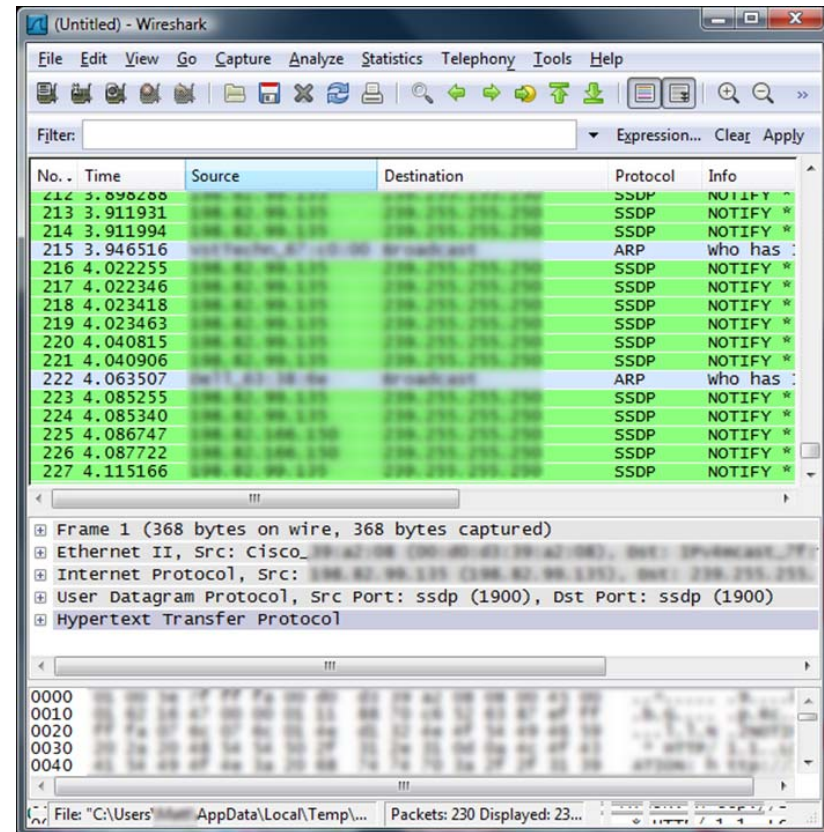
- Information overload
 - VT processes over 5 million emails per day
 - Manages over 500 SMTP & 3500 HTTP servers
- Analysts rely on multiple tools
 - Analysis takes more time
- Popular tools are not very *usable*
 - Primarily text based
 - Do not scale well for large networks
 - Graphical representations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

Current Security Tools – Text-based

Snort

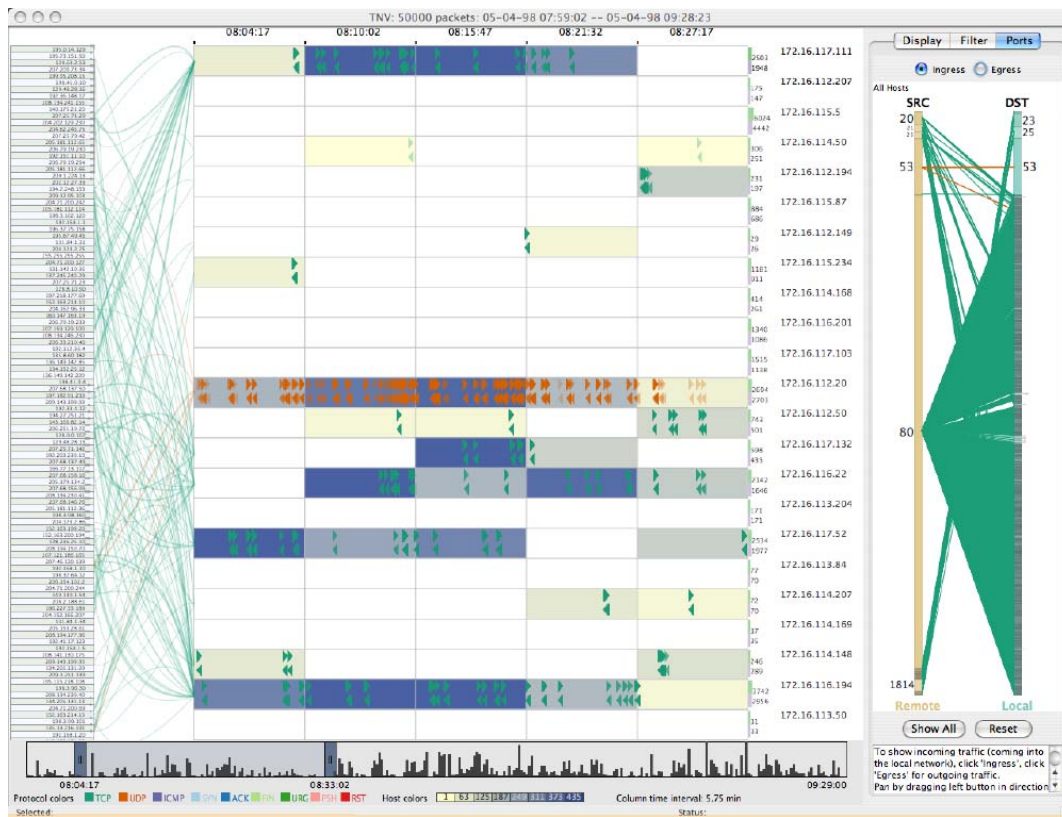


Wireshark

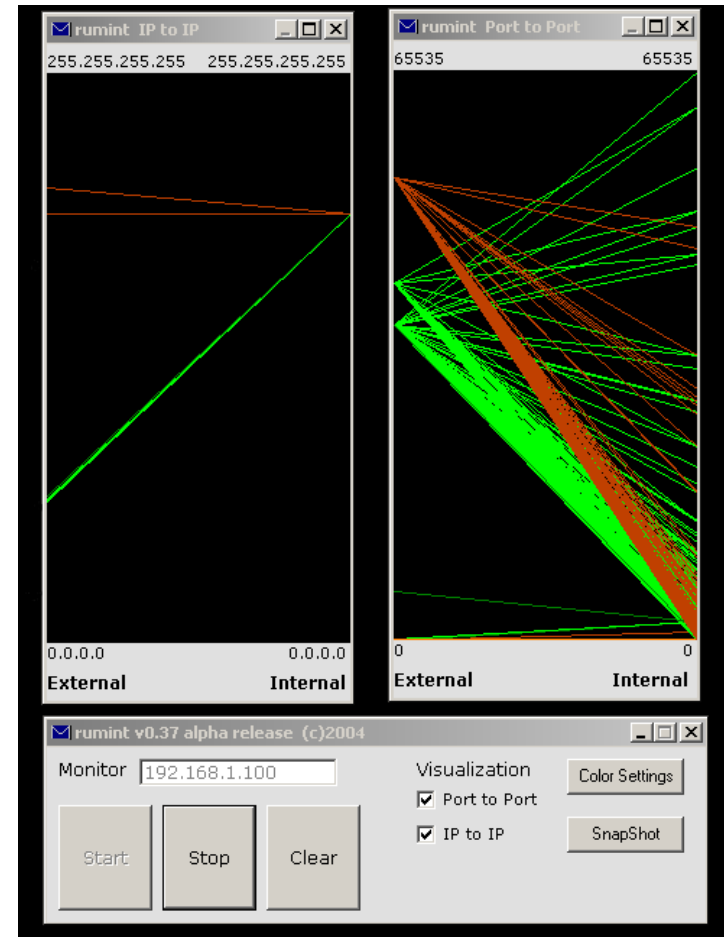


Current Security Tools – Graphical

The Network Visualizer



Rumint



Study Design - Participants

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

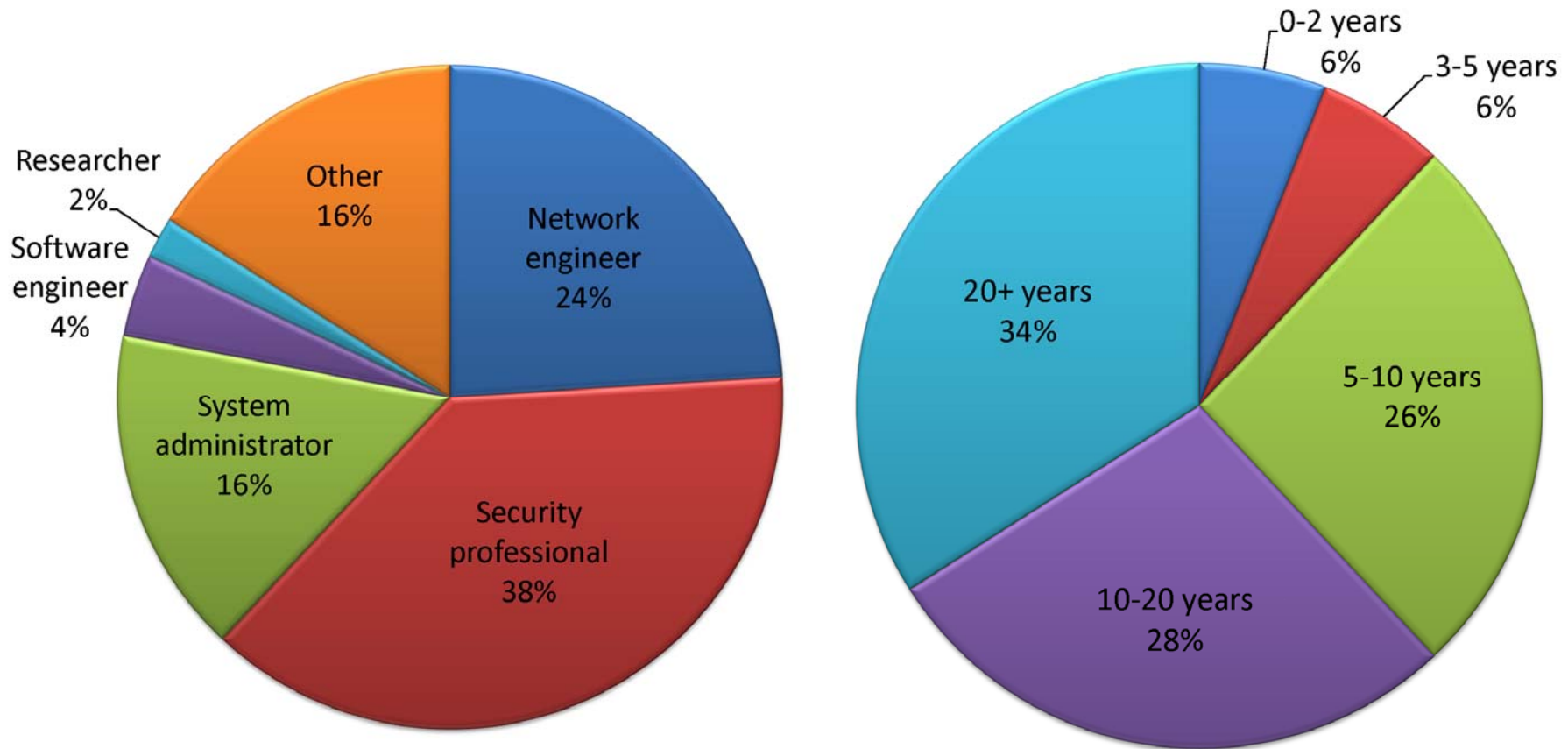


50 respondents

Study Design – Question Areas

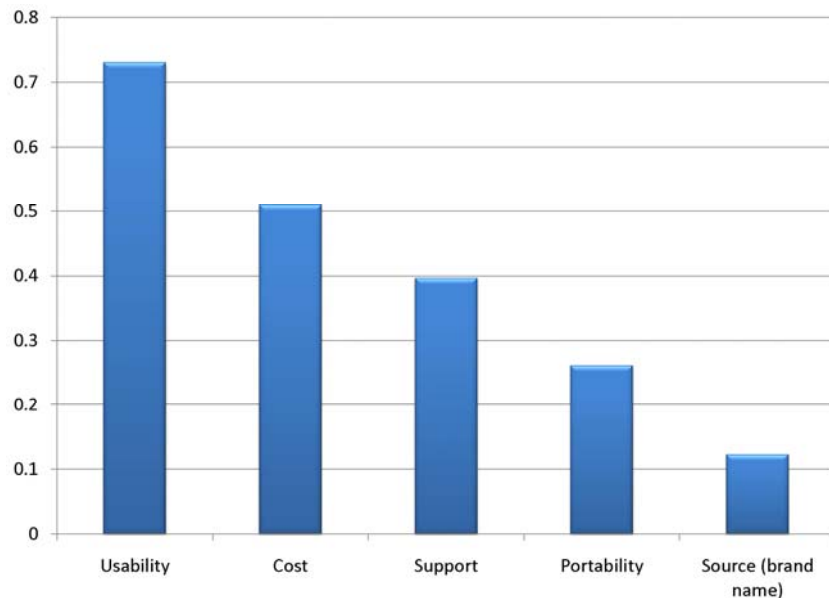
- Background Information
- System Information
- Security Information
- Security Tools
- GIS Information

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

VirginiaTech
Invent the Future

Information Technology

VT Web VT People
Enter your search here GO

CyberSecurity Operations Center

Information Technology Homepage IT Security Homepage About Us IT Security Lab IMS

IP Address	BLDNUM	BLDNAME	Domain Name	Hostname	Lat	Lon
138.0.79.26.29	2190	MATH EMPORIUM	emporium.vt.edu	emporium.emporium.vt.edu	37.213421	-80.43
138.0.79.128.94	177	CAROL M. NEWMAN LIBRARY	lib.vt.edu	lib.vt.vt.edu	37.22876234	37.22
138.0.79.128.17	191	MCCOMAS HALL - Schiefel Health Center	shs.vt.edu	shs.vt.vt.edu	37.2206893	-80.42
138.0.79.128.103	177	SCAROL M. NEWMAN LIBRARY	lib.vt.edu	lib.vt.vt.edu	37.22876234	-80.41
138.0.342.106	623	ISB	iwa.vt.edu	hwshd.iwa.vt.edu	37.20383439	-80.41
138.0.342.130	623	ISB	db.vt.edu	db.vt.vt.edu	37.20383439	-80.41
138.0.342.131	623	ISB	db.vt.edu	db.vt.vt.edu	37.20383439	-80.41
138.0.342.132	623	ISB	db.vt.edu	db.vt.vt.edu	37.20383439	-80.41
138.0.342.133	155	DERRING HALL	geos.vt.edu	geos.vt.vt.edu	37.2250603	-80.42
138.0.342.134	623	ISB	cc.vt.edu	cc.vt.vt.edu	37.20383439	-80.41
138.0.342.135	623	ISB	iwa.vt.edu	hwshd.iwa.vt.edu	37.20383439	-80.41
138.0.342.137	623	ISB	iwa.vt.edu	hwshd.iwa.vt.edu	37.20383439	-80.41
138.0.342.138	623	ISB	cms.vt.edu	hwshd.cms.vt.edu	37.20383439	-80.41
138.0.342.139	623	ISB	iwa.vt.edu	hwshd.iwa.vt.edu	37.20383439	-80.41
138.0.79.97.28	119	BIOINFORMATICS FACILITY PHASE 1	bioinformatics.vt.edu	bioinformatics.vt.edu	37.22080196	-80.42
138.0.79.203.77	102	PRICE HALL	ento.vt.edu	ento.vt.vt.edu	37.22573661	-80.42
138.0.79.203.80	102	PRICE HALL	ento.vt.edu	ento.vt.vt.edu	37.22573661	-80.42
138.0.79.97.89	119	BIOINFORMATICS FACILITY PHASE 1	bioinformatics.vt.edu	bioinformatics.vt.edu	37.22080196	-80.42
138.0.79.97.100	119	BIOINFORMATICS FACILITY PHASE 1	bioinformatics.vt.edu	bioinformatics.vt.edu	37.22080196	-80.42
138.0.79.203.107	102	PRICE HALL	ento.vt.edu	ento.vt.vt.edu	37.22573661	-80.42
138.0.79.97.149	119	BIOINFORMATICS FACILITY PHASE 1	bioinformatics.vt.edu	bioinformatics.vt.edu	37.22080196	-80.42
138.0.79.203.148	119	BIOINFORMATICS FACILITY PHASE 1	bioinformatics.vt.edu	bioinformatics.vt.edu	37.22080196	-80.42
138.0.79.203.149	119	BIOINFORMATICS FACILITY PHASE 1	bioinformatics.vt.edu	bioinformatics.vt.edu	37.22080196	-80.42
138.0.342.204	623	ISB	cc.vt.edu	cc.vt.vt.edu	37.20383439	-80.41
138.0.79.97.176	119	BIOINFORMATICS FACILITY PHASE 1	bioinformatics.vt.edu	bioinformatics.vt.edu	37.22080196	-80.42

Virginia Tech Home | Information Technology | IT Security
Last updated Fall, 2009

Usable Security -

a Tech

Detailed View



Future Work

- Build working model of prototype
- Conduct usability study

Questions

