

Evaluating Cyber Security Tools

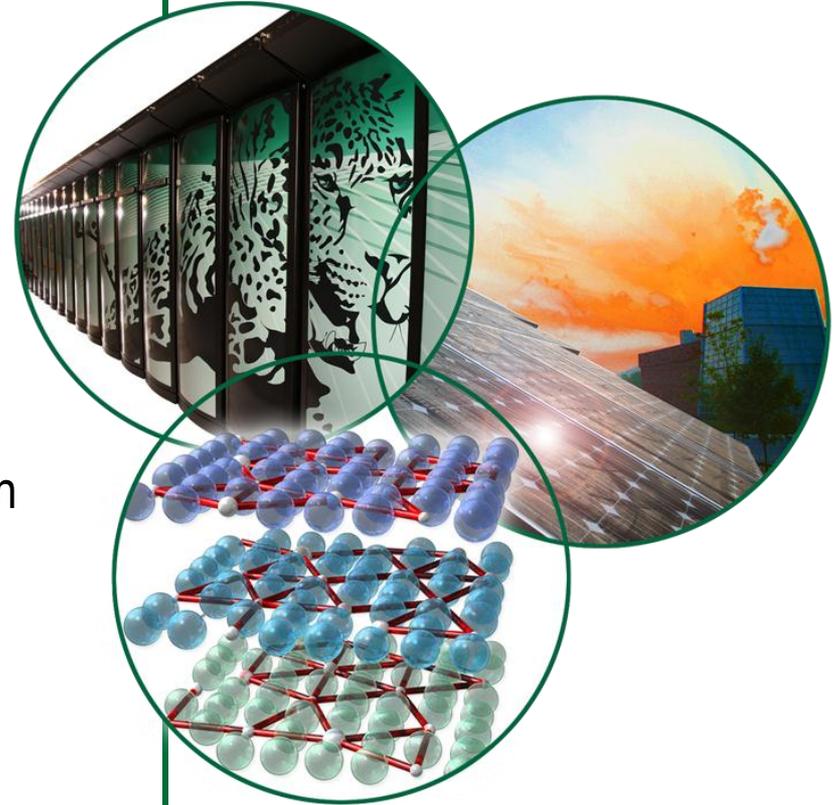
Katherine Victoria Williams

Research Alliance in Math and Science
Computing and Computational Sciences

Mentors: Kevin Kerr and Tina Heath
Information Technology Services Division
Risk Management Team

School: Saint Mary-of-the-Woods College
Saint Mary-of-the-Woods, Indiana

August 2012



Background of cyber security

- Every security tool has its own data repository – this way by design
- Know correlations between data repositories
- Know actual risk vs. industry-defined risk
- Better categorize risks – allows focus on actual critical risks
- Seeing data flow helps with understanding security
- Scoring vulnerabilities aids in determining risk to network



Project objectives

- Identify and list cyber security tools
- Create flow chart of interconnected security tools
- Determine specific data flowing between tools
- Create internal asset risk score
- Showcase uses for new tools being implemented
- Propose ideas for better security tool management



Resource for computer security information

Visit them at: <http://www.us-cert.gov/>

Methodology

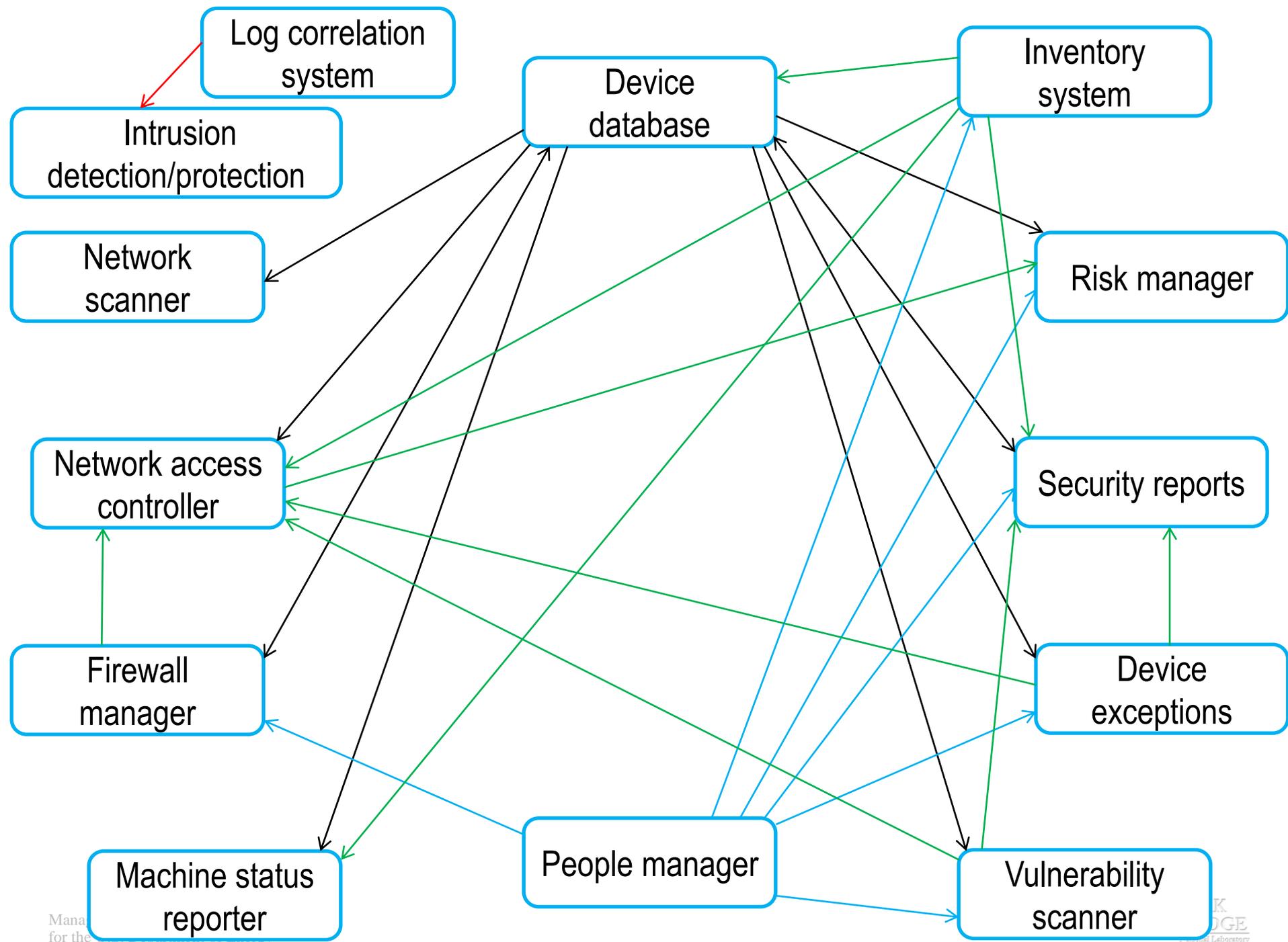
- Identify tools used within cyber security
 - Numerous tools at lab
 - Focus on approximately 30 tools
- Discuss with tool experts regarding cyber security tool use
- Create visual representation of data flow between tools
- Compile fact sheet with tool information
- Identify problems and inconsistencies
- Research scoring system which identifies vulnerabilities



Results

- Revelation of security tool gaps
 - Lack maxim efficiency
 - Tools gather only some aspects about data
- Revealed data not viewed the same among different tools
 - Tools provide different information about similar gathered data
 - Many ways to look at gathered data
- Uncovered problem of no single source of information
- Information sheet about Oak Ridge National Laboratory's tools
- Compiled data exchange sheet
- Risk index for internal systems (RIFIS) design and testing





From	To	Data being transferred
Tool A (Device database)	Tool B (Machine status reporter)	<ul style="list-style-type: none"> ▪ Device name ▪ IP address ▪ Location ▪ Mac address ▪ Operation system (OS)
Tool A (Device database)	Tool D (Network access controller)	<ul style="list-style-type: none"> ▪ Device type ▪ IP address ▪ Mac address ▪ Owner information ▪ Router
Tool A (Device database)	Tool E (Risk manager)	<ul style="list-style-type: none"> ▪ Alert flags ▪ Device type ▪ IP address ▪ Mac address ▪ Owner information
Tool C (People manager)	Tool D (Network access controller)	<ul style="list-style-type: none"> ▪ Department name ▪ Group name ▪ Owner contact ▪ Owner location ▪ Owner name/ID
Tool C (People manager)	Tool E (Risk manager)	<ul style="list-style-type: none"> ▪ Department name ▪ Owner contact ▪ Owner devices ▪ Owner location ▪ Owner name/ID
Tool D (Network access controller)	Tool E (Risk manager)	<ul style="list-style-type: none"> ▪ IP address ▪ Mac address ▪ Network exceptions ▪ Network location ▪ Time stamps

RIFIS test run

Name	Test Asset 1	Points
1. Vulnerabilites		
Mild	0	0
Medium	0	0
High/Critical	0	0
2. Asset Status		
Orange?	0	0
Red?	0	0
3. Sensitivity		
Low	0	0
Moderate	0	0
4. Firewall Rules		
Rules?	0	0
5. Alerts		
Number of alerts	0	0
6. Anti-Virus		
Number of flags	0	0
7. VIP Status		
VIP?	0	0
		0

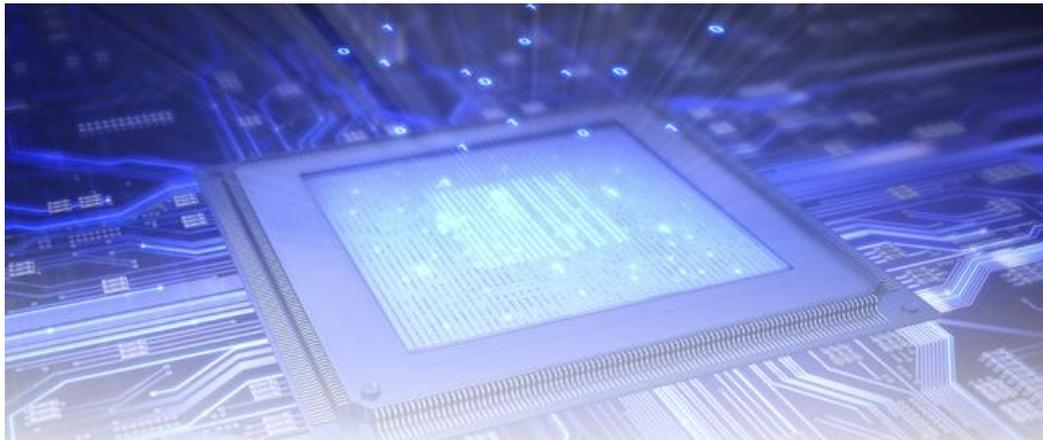
Non-vulnerable system

Name	Test Asset 2	Points
1. Vulnerabilites		
Mild	0	0
Medium	0	0
High/Critical	0	0
2. Asset Status		
Orange?	1	5
Red?	0	0
3. Sensitivity		
Low	0	0
Moderate	0	0
4. Firewall Rules		
Rules?	1	25
5. Alerts		
Number of alerts	30	150
6. Anti-Virus		
Number of flags	0	0
7. VIP Status		
VIP?	1	25
		205

Vulnerable system

Conclusions

- Large area of functionality
- Information not shared or viewed the same
- Identify vulnerabilities inside network to strengthen defenses
- Continuation of cyber security adaptability against new threats
- Current tools need evaluation for efficiency
- Evaluate current tools for better usage before purchase of new tools



Acknowledgements

There are many thanks to be given for the completion of this project. First would be to the mentors, Kevin Kerr and Tina Heath who helped support and encourage the growth of the project and its direction. Matt Disney also receives thanks for recommendations on next steps and help with completion of the project. Thanks also go to the rest of ORNL's ITSD, for all of the staff members who gave up time to answer questions and explain how tools functioned. Finally, thanks go to Debbie McCoy and the RAMS internship for the opportunity to work at Oak Ridge National Laboratory.

Questions?

History has taught us: never underestimate the amount of money, time, and effort someone will expend to thwart a security system. It's always better to assume the worst. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens, you'll be glad you did. — Bruce Schneier

