Quantitative Model for Evaluating Security Products

Jacob Dulaney, Hyunjoon Kim, Benjamin Krause, Luis Gustavo Loayza, Shival Puri, Allen Shen
General Dynamics Information Technology; Robert Carey
SME: Richard Lord

BACKGROUND

- Current cyber security products are not based on any meaningful measures
- The security tools are advertised on their qualitative features rather than their quantitative measure on how much they improve the security. Sales revolve around these qualitative features
- Advantages: can effectively compare different security products with similar features quantitatively by comparing the percentage of improvement in security
- Challenges: complex to develop one model that fits different organizations due to different requirements of each organization

OBJECTIVE

- A model that can be used to determine the qualitative value of similar security products against a given set of risk mitigation security controls at a high confidence and is applicable to all security tools
- Because of our lack of data to work with, our model was to be developed to be flexible to work with any type of data that could be gathered

APPROACH

- In order to determine a minimum set of enterprise security controls applicable to cybersecurity devices, we researched standard logical controls related to business. Per the scope of our project, we did not review policy or physical controls
- Our research references previous work done by leaders in cybersecurity such as SANS Institute, the National Institute of Standards and Technology (NIST) and NSS Labs
- We broke up the Open Systems Interconnection (OSI) model into each of its 7 layers. We identified the most critical vulnerabilities of each layer to determine a minimum security control that could be measured in protecting against that vulnerability
- Rather than focus on the effectiveness of one type of cybersecurity device, we developed a controls matrix addressing the seven layer security stack. The controls matrix would allow for a global view of which combinations of devices can protect all seven layers
- After researching, we adopted the “rule of 5” to determine a minimum of 5 data points for reliable metrics
- We then developed tests for each metric setting benchmarks of 80% minimum for a tool to be deemed satisfactory. For highly critical controls, the tool had to pass the metric tests 100% of the time

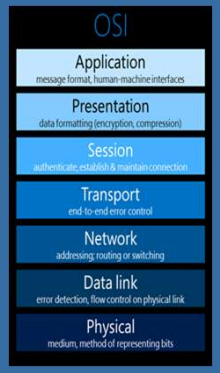

Figure 1. OSI Model

MODEL

Layer	Control	Security Device: Traditional Firewall	Application Firewall	Next Generation Firewall	Intrusion Detection System	Intrusion Prevention System	Web Proxy	Endpoint Protection	Network Access Control
Application	1. Monitor applications using signature based detection for known malware								
	2. Application level access controls to define and enforce access to application resources.								
	3. Monitor and block application inquiries and activity that deviates from normal behavior								

- Layer - Selected layers from Open Systems Interconnect model that were relevant
- Control - Chose security controls that can be implemented at selected layer
- Security Device - Selected most commonly used and effective security tools and determined effectiveness in implementing selected controls

Layer	Control	Metric	Test Methodology	Benchmark
Application	1. Monitor applications using signature based detection for known malware	1. How well the device can detect malware signatures	1. Test a set of malware with known signatures to determine if the tool detects them (estimated 20 unique malware to test)	At least 18/20
	2. Application level access controls to define and enforce access to application resources.	2. How well the device blocks access	2. Test whether users can access critical applications (estimate 5 applications to test)	At Least 4/5
	3. Monitor and block application inquiries and activity that deviates from normal behavior	3. How well the device blocks malware from executing	3. Test whether malware or code injection attacks can be executed (estimate 20 attacks)	At Least 18/20

- Metric - Determined attribute of security device when covering selected control
- Test Methodology - Selected way in which metric effectiveness could be tested with necessary equipment
- Benchmark - Determined number at which security device would “minimally secure” selected control

Model Uses:

- Organizations can compare current security controls to those we have defined
- Companies will have better knowledge of what security tools cover each control
- Easier to define which security tools are actually needed - reduces chances of overlapping controls

OUTCOME

- The overall approach failed due to being unable to obtain testing data. We were unable to test and refine the testing and evaluation methodology:
  - Declined by multiple organizations when approached about acquiring data
  - Without testing data, it was impossible to confirm what realistic benchmarks are or a defined testing methodology
- The initial approach of creating minimum security stack of controls fulfilled the criteria needed to develop the model:
  - Create measurable criteria for the model
  - Control the scope of of information that would be needed for testing
  - Process is replicable by any third party interested in customization of the model
- Based on the outcome of our research, the following improvements to our approach could solve the issues we faced:
  - Secure a data source before developing the model. The lack of testing data proved very difficult for our team
  - It would be beneficial to narrow the scope to a single tool/device and the role it plays in the network rather than attempt to include many devices for testing
  - Adjust the scope of the model to the data available if comprehensive testing data cannot be found

CONCLUSIONS

- Creating a quantitative model to measure the effectiveness of a cyber security product is very difficult
  - Various organizations have thrown a lot more resources at this problem and have yet to effectively solve the problem
- The approach to creating a quantitative model should be to create a general, broad model where organizations and individualize it themselves
  - We ended up just evaluating based on a single tool. Companies can use this model to match to certain cyber security products
- Future research can include a wide variations of uses everything from another potential risk management framework all the way from individual organization adopting the model for use for their own for things like auditing both internal and external systems for information assurance

ACKNOWLEDGEMENTS

We’d like to thank General Dynamics Information Technology for assistance with this project. We appreciate the support, time, and effect from our customer, Robert Carey, and our SME, Richard Lord. We would also like to thank Peggy Brouse for giving us this opportunity, and Gino Manzo for supporting us throughout the project. We’d also like to thank David Raymond from Virginia Tech for his professional advice.

References

Wilson, J. (2015, February 6). IOE/IOT KEY ENABLERS WILL BE UBIQUITOUS CONNECTIVITY & PREDICTIVE MAINTAINENCE. Retrieved April 23, 2018, from http://jimwilsonblog.com/?cat=176