Unit 3 - Seminar Preparation: Peer review activity

James Hines
RMPP

Paper 1: modeling cybersecurity risks: Proof of concept of a holistic approach for integrated risk quantification.

Purpose

To calculate cyber risk at various stages of a dynamic cyber attack.

Problem

Virtually all risk assessments are reactive and not using methods that follow a cyber attack, which is dynamic.

Objective or research question

To model risk in a complex system by carrying out a dynamic risk calculation (recalculated with each change of state) using risk metrics including and beyond probabilities that characterize the system.

Are they in line with your experience or thoughts on the topic?

They are far ahead of my understanding of dynamic risk modeling at this stage due to their approach of introducing a live SQL attack within their process. But, with less on-site file servers and more cloud based data centers, it may be good to see how this type of modeling complies with cloud based infrastructure and automated security.

Contributing to the collective body of knowledge in this area?

I think that the idea of calculating dynamically instead of a static analysis is of importance to the industry and a contribution to the discipline. The process and feeling of approach reminds me a little, of a bayesian type of markov chain.

Is the research methodology utilised in each paper appropriate for the stated purpose or question?

The methods section is broken down clearly, but lacks a clear mathematical formula/ image to show what and how they plan to carry out the research.

In terms of data collection and analysis, is this also appropriate for the stated purpose or question?

The paper outlines a section called: Statistical application, but does not have a results section. The statistical application section has very little data and is more focused on explaining the process of how they set it up and what is what.

Does the paper support its claims and conclusions with explicit arguments or evidence?
Yes, the paper supports what they set out to achieve and their conclusion does explain that the analysis can be run on a test-bed which will then allow for fault finding.

How would you enhance the work/paper?
I would include a flowchart to demonstrate what will happen at each process, what is included in each process and how each process is initiated. I would have included a results section and displayed results from at least several alternative analyses to check for accuracy and repeatability.

Reference
Henshel, D., Alexeev, A., Cains, M., Rowe, J., Cam, H., Hoffman, B. & Neamtiu, I. (2016) Modeling cybersecurity risks: Proof of concept of a holistic approach for integrated risk quantification. *IEEE Symposium on Technologies for Homeland Security (HST)*: 1-5. Available from: https://ieeexplore.ieee.org/abstract/document/7568937 [Accessed on 28th June 2023]

Paper 2: Semi-quantitative cybersecurity risk assessment by blockade and defense level analysis

Purpose
To establish a blockade and defense style approach of four areas of IT which are vulnerable and usually used for attack to systems and companies.

Problem
Current risk analysis focuses on mathematical probabilities

Objective or research question
To create a Blockade and defence level analysis which is a new intrinsic risk analysis consisting of a two step solution.

Are they in line with your experience or thoughts on the topic?
Yes, the researchers have covered the topic in question very well, they have critically discussed three types of risk analysis, the strengths and what they wish to see happen next.

Contributing to the collective body of knowledge in this area?
Yes, this is a very important topic which would be optimal for small businesses in my opinion.

Is the research methodology utilised in each paper appropriate for the stated purpose or question?
Yes, the methodology outlinesin this particular paper is very clearly presented.

In terms of data collection and analysis, is this also appropriate for the stated purpose or question?
Results are displayed clearly with good explanations.

Does each paper support its claims and conclusions with explicit arguments or evidence?
The researchers argue very clearly of what should be done for the four separate simulations. They claim that their BDLA (Blockade and defence level analysis) will be a great supporter to a company with 27001 certification. I have no doubt because the 27001 ISMS is a way to ensure that you have correct policies and procedures in place. Endpoint detection and response is widespread via microsoft products such as defender, this may be a challenger to BDLA in recent years and is usually integrated into many medium and large businesses. Where BDLA may have an advantage is in small businesses, it may be a more superior option.

How would you enhance the work/paper?
I would look at the Figure 2 design again, they claim to use HTTP and not HTTPS, no DMZ and only one firewall. They have separate IDS and IPS, where providers such as Fortinet provide IDS/IPS in a single device. But then again, it is just for demo purposes. The paper is very good, hard to enhance at this stage.

References
Han, C.H. and Han, C. (2021) Semi-quantitative cybersecurity risk assessment by blockade and defense level analysis. *Process Safety and Environmental Protection*, 155: 306-316. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0957582021004948 [Accessed on 28th June 2023]