Lee Brunovsky

CSCI 5120 Topics in Information Security

Week 2 & 3 Assignment

HW1_Science_of_Security

Due: Sep 9, 2021

Submitted: Sep 8, 2021

HW1Q1: Due an immense technical complexity across the various layers of computer science, as well as the rapidly dynamic environment that systems exist within, the JASON Program Office of the MITRE Corporation explained in a paper to the Department of Defense (DoD) that science of security (SoS) is an ever evolving holistic approach geared toward an increased understanding and execution of security agendas. Their work covered the applicable aspects of overlapping sciences such as Agriculture, Astronomy, Economics, Immunology, Medicine, and Meteorology in order to glean strategies to further define metrics and more effectively cultivate new strategies; Furthermore, this science based approach was largely focused on the establishment of trust via insights gathered from a concentration of cryptography, game theory, model checking, machine learning, obfuscation, response detection, sensing modalities, and scaling disciplines (2010). The JASON group predominantly leveraged existing techniques in these focus areas that included game theory 'Forwarder's Dilemma', model checking techniques such as Alloy, SPIN and Promela, and application specific methods such as the Needham-Schroeder Protocol to illustrate several widely accepted existing industry practices and shortfalls that lie within them. The underlying premise was that despite observations from implementing such techniques and focuses in the SoS, there remains a large need for a vast number of controlled experiments in the future in order to better define metrics, which are currently incapable of accurately assessing the complete picture; however, similar to the other sciences discussed, and improved but incomplete understanding is still a much better situation for society, and advancements spurred by a refined SoS will surely yield immense quality of life and security improvements.

HW1Q2: Science of Security and traditional cybersecurity differ in terms that the former is a higher level abstraction composed of universal laws that can be leveraged to more effectively guide security decisions based on projected outcomes, and thereby aide in the development of more secure

systems. Schneider elucidated on the ability of SoS to go beyond the defense and vulnerability of classical CIA (confidentiality, integrity, and availability) based assessments of specific systems by drawing correlations between non-apparent factors that comprise attacks, defenses, and policies in order to cultivate a systemic framework (2011). Therefore the more obtuse macro, and better defined micro view offered by SoS inherently provides a unique potential to develop more tailored and flexible strategies since more of the gray areas that exist currently would be better understood under such a framework. The ideology is well captured by Schneider (2011), where he mentioned Peter Nuemann's quote, "if you think cryptography is the answer to your problem, then you don't know what your problem is" (p.3). With this mindset, it becomes evident that SoS will have a branching foundation for which areas such as formal methods, improved Byzantine fault tolerance, and experimentation are sure to be included in the bedrock. For example, Schneider explained that formal methods are currently limited by their step-wise refinement approach, but SoS could eventually deliver a higher quality via inclusion of hyper-properties (2011). Therefore the potential advantages of SoS will be realized as the community continues to seek continuity in areas such as quantifiable definitions of CIA, obfuscation law enrichment, and prototype experimentation, which will undoubtedly improve upon the holistic understanding of SoS, and thereby arm developers with a more comprehensive framework and methodology for developing more secure systems.

HW1Q3: Arguably, the two most detrimental problems of traditional cybersecurity can essentially be stated as the inability to accurately establish a metrics based assessment of the level of security in a given system or network of systems, and that a stronger scientific foundation for computer security is still required. The two issues are by no means mutually exclusive. While all of the four readings for this assignment focused on both aspects, I found the paper *An Attack Surface Metric* written by

Manadhata & Wing to be the most informative in terms of tangible industry examples of assessing security levels. More specifically, the authors discussed potential vulnerabilities in terms of side channel exposure such as entry and exit points of I/O, non-trusted persistent data, damage potential to effort ratio, effectiveness of open source patches, and database vulnerabilities such as SQL fault injections: While deeper discussion of mapping concepts such as daemon privilege *setuid* system calls and attack surface area reductions via subsequent versions of new software are beyond the scope of this assignment, the key in the authors approach was that it was system centric opposed to attacker centric (Manadhata & Wing, 2011). Accordingly, despite the quality of such work, it really highlights the second issue of a need for a stronger scientific foundation for computer security. As previously alluded to in mentions from the JASON report and work from Schneider, attack surface reductions may mitigate some security issues, but fail to fully encompass the entire ecosystem of threat potentials, much less provide a systemic and well defined knowledge base of such vulnerabilities; however, all of the authors seemed aligned in the difficulties of establishing a holistic SoS foundation capable of addressing these two issues, but continued efforts to do so will undoubtedly continue to push SoS beyond specific use case cybersecurity cognizance.

References

Manadhata, P. K., & Wing, J. M. (2011). An attack surface metric. *IEEE Transactions on Software Engineering*, *37*(3), 371–386. https://doi.org/10.1109/tse.2010.60

Science of cyber-security. (2010). https://doi.org/10.21236/ada534220

Schneider, F. B. (2011). Blueprint for a Science of Cybersecurity. *Department of Computer Science Cornell University.*