Raghuveer Gummadi
CSC 6350
Fall 2020

Summary

The paper “An Effective Security Requirements Engineering Framework for Cyber-Physical Systems” discusses the complexities of securing systems on both a software and a hardware. The authors of the paper evalauate the weaknesses of several known approaches and propose a new approach. This could have implications in discussing computer security and in engineering processes.

The paper begins by the need for a security framework for what it calls “Cyber-Physical Systems” which are systems that are an amalgamation of software and physical machines that do real world functions. It expands on the variety of ways in which such systems were attacked, for example the hacking of the Iranian nuclear program and an attack on a U.S water filtration plant, and on the cost of fixing security flaws later.

The article continues by evaluating the various security frameworks that have sprung up over the years. SQUARE, UMLsec, CLASP, SREP CORAS, MS SDL, and Secure Tropos. The authors briefly go over the various differences and unique attributes of each type of framework and evaluate each frameworks respective effectiveness. The authors point out a common trope of each of them is the paucity of attention given to physical hardware and system security issues.

Each given security framework must be accompanied by a risk assessment, according to the authors of the paper. In the next section, the authors cover various types of risk any CPS might face and stress the importance of integrating such risk analysis early in the software process.

After giving background the paper introduces its proposal for a Security Requirements Engineering Framework (SRE) which seeks to provide a way to determine security requirements in the early part of the Requirements Engineering phase. The proposed framework has 8 activities: identify security goals, identify assets, identify threats, identify secure network communication, identify endpoint hardware, identify sensor data generation/communication, perform risk assessment, and finally to elicit security requirements.

The paper then presents a case study in which the framework was used, in a smart car parking system. After applying all 8 activities, the authors compared the various ways in which security issues were addressed and compared it with other frameworks and found the new system compared favorably. The authors end by indicating that such a framework could benefit researchers and software engineering teams further in the industry.

Critique

The authors of the paper are thorough and complete in the evaluation of security frameworks in the requirement engineering process. The case study with the smart car port was particularly illustrative, showing how basic security gaps can easily arise when security issues are not integrated in the process early. However, the authors when the author’s enumerate all the previous security frameworks that have sprouted over the years, their paper would’ve benefited in a more detailed examination of their weakness. The paper would have also benefited from a more direct comparision of their new framework and legacy frameworks.

Synthesis

The new software process that the authors propose looks promising, and replicating its results with more case studies could be a potentially useful line of inquiry. One idea of continuing research is by conducting a series of “red flag” exercises, where one team builds a software product using the proposed framework and another team attacks it. Such an exercise would vet the effectiveness of the

proposed framework in real world conditions. The results of the paper seem promising, and increasing the scale and reproducing these patterns seems to be a good way of testing it.

Paper Bibliography Information

1. Rehman, Shafiq Ur & Gruhn, Volker. (2018). An Effective Security Requirements Engineering Framework for Cyber-Physical Systems. Technologies. 6. 65. 10.3390/technologies6030065.