Jun Chen
CSC6350
Software Engineering
2020Fall

Summary of An Effective Security Requirements Engineering Framework for Cyber-Physical Systems

Problem Statement:

Nowadays, it is common to see that software, system hardware, and sensors work together by using the network. However, a lot of developers and the requirement analyst consider more about the software than hardware. Besides, the priority of the Cyber-Physical System is higher than other systems. It means that the Cyber-Physical System requires much higher security. However, the current security frame cannot satisfy all the requirements of the Cyber-Physical System. The developer and the requirement analyst seldom consider the security of the sensors.

Proposed Solution:

The authors provide an incremental security requirements evolution approach and apply and evaluate this approach. This approach can determine security requirements during the whole Requirements Engineering phase. This approach focuses on three significant parts of the CPS, such as security goals, risk assessment, and threats. This frame has eight activities, which are identify security goals, identify assets, identify threats, identify secure network communication, identify endpoint hardware, identify sensor data, perform risk assessment, and elicit security requirements.

Results:

By comparing different most used security requirements engineering frameworks, the authors find out that these frameworks cannot perform all required activities in the security system. By finding the weakness of these frameworks, the authors can use them to improve their provided security requirements engineering framework.

Evaluation:

The advantage of this framework is that this framework can minimize the weakness of the security requirements engineering framework. The framework can provide high security for the security system.

The disadvantage of this framework is that people need to compare a lot of common-used security requirements engineering frameworks and gather their weaknesses. This action will take a lot of time. Besides, this framework may have a lot of requirements to improve security, and it means that people may spend more budget on this security system.

Synthesis:

The authors should consider whether people or companies can use the limited budget to realize the system by satisfying the requirements of the security system. Besides, the authors should consider reducing the time of generating the security system. The authors also need to figure out and prove whether the system is more secure if the CPS has more requirements.

Reference:

Rehman, S., & Gruhn, V. (2018). An Effective Security Requirements Engineering Framework for Cyber-Physical Systems. Technologies, 6(3), 65. doi:10.3390/technologies6030065

.