Estimating the Time-To-Compromise of Cyberattacks in Industrial Control Systems

Engla Rencelj Ling (KTH) englal@kth.se

Abstract for the 21st Seminar within the Framework of a Swedish IT Security Network for PhD students (SWITS 2021)

The metric Time-To-Compromise is used for estimating the time taken for an attacker to compromise a component or a system. The TTC helps to evaluate the critical attacks, which is useful when allocating resources for strengthening the cyber security of a system. In this presentation we describe our updated version of the original definition of Time-To-Compromise. The updated version is specifically developed for the Industrial Control Systems domain. The Industrial Control Systems are essential for our modern society that relies heavily on, for example, electricity and the Internet. Therefore, it is crucial that we keep these systems secure from cyberattacks. We align the method of estimating the Time-To-Compromise to Industrial Control Systems by updating the original definition's parameters and use a specific vulnerability dataset for the domain. The new definition is evaluated by comparing estimated Time-To-Compromise values to previous research results.

Keywords: Time-To-Compromise, cyberattack, industrial control system