産業制御システムに対するサイバー攻撃の調査

Survey on the cyber-attacks to industrial control systems

水沼　暁
Akira Mizunuma

概要

近年、主に重要インフラ業界で扱われる制御システムを標的としたサイバー攻撃によるインシデントが増加している。制御システムを情報系システムに接続することにより利便性向上およびコスト削減を実現しているが、制御システムと情報系システムそれぞれの脆弱性を考慮する必要がある。海外では、制御システムに対するインシデント報告件数は年々増加傾向にある。しかし、日本における報告件数及び事例の公開状況は海外と比較しても極端に少数であり、国内の制御システムインシデント状況が不透明である。そのため、制御システム事業者にサイバー攻撃の脅威が伝わらず、危機感が希薄になりがちである。しかし実際の攻撃者は、常に制御システムの脆弱性を狙っていると考えられる。そこで本研究では、SCADA HoneyNet Project のソースコードを用いて、制御システムを偽装したハニーポットを構築し、インターネットに公開することで第三者からのアクセス状況を調査した。その結果、特定のポートに対する異常アクセスが極めて多いことが判明した。

Abstract

Recently the incidents have increased due to the cyber-attack targeting for the control systems of important infrastructure. The improved convenience and cost reduction can be achieved by connecting the control systems to information system such as the internet. But their vulnerability must be considered more seriously than ever before. A lot of reports tell us that the incidents tend to increase overseas. However, the number of incidents reported in japan is relatively less than overseas, and sense of crisis for the cyber-attack tend to be scarce because its danger is not informed. But it is estimated that the attackers would be targeting the vulnerability of control system always. So, this study constructed a honeypot which impersonates the SCADA system using the source code of “SCADA HoneyNet Project”. And it investigated the access statistics from a third party. As a result, it found the rate of abnormal accesses to a specific port is extraordinarily high.