産業用ロボットの潜在的脅威と対策

小山　千尋 <koyama.chihiro.jw6@is.naist.jp>

Abstract

- 本研究では産業用ロボットの要素・役割を列挙し、各要素への攻撃・脅威と対策をまとめた。
  また、現在の産業用ロボットに適用可能なセキュリティ対策を検討する。

Background & Motivation

- IFRの調査[1]では産業用ロボットの世界販売台数は毎年増加しており、「作業自動化」が様々な分野で期待されている。一方、産業用ロボットに関するセキュリティレポート[2]では攻撃シナリオとその検証結果が示され、人的・物的の観点からセキュリティ強化の必要性を主張している。
- 特に産業用ロボットは製造部門を支える重要な機器の１つであり、安全性・正確性・可用性が要求される。使用者の安全を確保する為のセキュリティ対策は不可欠である。

Result

- 産業用ロボットの構成をFig.1に示す。

Fig.1 Robot system loop

- センサを用いて外界の情報を取得し、その値を元に知能・制御系が次の動作を計算し、動作命令が駆動系に適用される。ループを形成するため、使用者の意図した動作の実現にはすべての要素が正しく機能することが必要である。以下に各要素への攻撃・脅威と対策をまとめる。

1. センサ[3]

物理量の計測原理に基づく”なりすまし・妨害信号”を攻撃回路から送信する。(Fig.2)

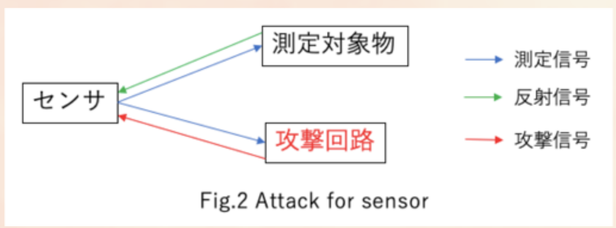

Fig.2 Attack for sensor

物理量を正確に測定できないため知能・制御系や駆動系で適切な動作が実施できない。
対策として「測定信号を複雑にし、信号の複製を困難にする」「測定値を相関・時系列で評価する」などが挙げられる。

(Result)

2. 知能・制御系

ロボットシステムに様々な機能を持たせるためにFig.4のような構成になることがある。ロボットソフトウェア開発に有用なROS(ミドルウェア)には認証の欠如による脆弱性が存在する[5]。

Layer
Software
Middleware
OS
Hardware

Fig.4 Controller

3. 駆動系

MTM※1(Fig.3) に基づき、攻撃者の目的・脅威に応じて各レイヤへ攻撃が実施された[4]。リモートGPIO設定上の脆弱性によるコマンド注入、サーボプログラマによる改変(フィジカル攻撃)などがある。

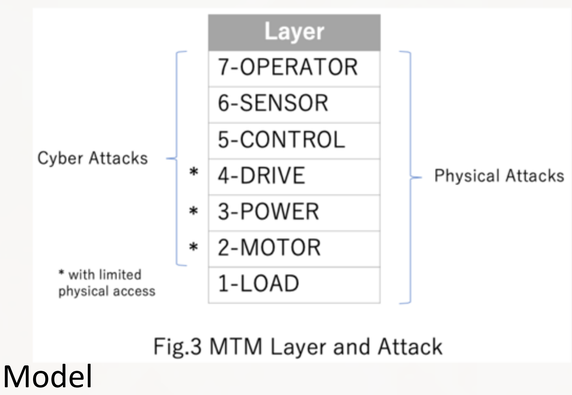

Fig.3 MTM Layer and Attack

※1 Motor Threat Model

Conclusion and Future Work

- 産業用ロボットの構成要素ごとに潜在的な脅威を俯瞰した。サイバー・フィジカル攻撃への対策は「技術:認証・検知」「物的:入退室の管理、SCM※2」「人的:従業員教育」など要因ごとに対処する必要がある。
- サイバー攻撃への技術的対策として制御理論に基づく攻撃検知機構を実装し、利用者のより安全な技術活用に貢献する。

※2 Supply Chain Management

Reference

[1] “Global Industrial Robot Sales Doubled over the Past Five Years.” IFR International Federation of Robotics. Accessed May 24, 2020. https://ifr.org/ifr-press-releases/news/global-industrial-robot-sales-doubled-over-the-past-five-years.
[2] “Rogue Robots: Testing the Limits of an Industrial Robot's Security.” Rogue Robots: Testing the Limits of an Industrial Robot's Security | トレンドマイクロ. Accessed May 24, 2020. https://resources.trendmicro.com/jp-docdownload-form-m176-web-rogue-robots.html.
[3] 藤本大介. センサの計測過程におけるセキュリティ. 電子情報通信学会, 2019, Vol.13 No.2, pp.142-150.
[4] Matthew Jablonski, Duminda Wijesekera. ATTACKING ELECTRIC MOTORS FOR FUN AND PROFIT. BlackHat USA 2019
[5] Bernhard Dieber et.al. Security for the Robot Operating System. Robotics and Autonomous Systems, 2017