Escola de Engenharia de São Carlos
Universidade de São Paulo

Desenvolvimento de um método de detecção de intrusão em redes OPC UA baseado em técnicas de Aprendizagem de Máquinas

Proposta inicial de mestrado em Engenharia Elétrica

Jonathan Tobias da Silva

Prof. Dr. Ivan Nunes da Silva
Orientador

Prof. Dr. André Luis Dias
Coorientador

EESC · USP

March 10, 2023

Agenda

Apresentação

Trabalhos desenvolvidos

- Softwares WEB-based
- Diagnóstico de falhas
- *Machine Learning*
- Sistemas inteligentes
- *Cloud Computing*
- Publicações

Sobre o tema

Motivação e Justificativa

- Aumento nos casos de ataques cibernéticos em CPPSs
- *Industrial Internet of Things*
- *Artificial Intelligence*
- *Service Orientated Architecture* (SOA)
- *Open Process Automation Standards* (OPAS)
  - Baseado na IEC 62443
  - Possuí uma parte específica para Security
  - Comunicação baseada no OPC UA
- *Cybersecurity*
- Convergência IT/OT

Maroochy Shire - 2000

O sistema de controle da estação de tratamento de água, inundando o terreno do hotel com esgoto bruto

U.S. Federal Aviation Administration - 2009

Hackers invadiram várias vezes os sistemas de apoio à missão de controle de tráfego aéreo

Iran's nuclear system - 2011

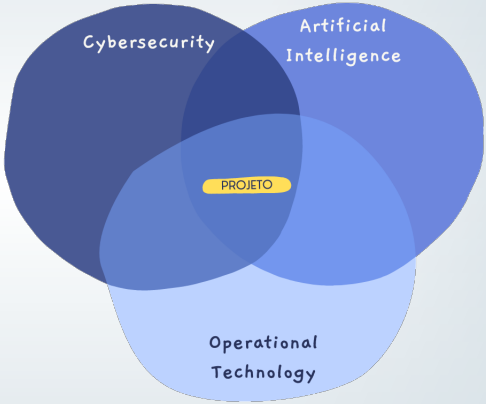
Hacker interromperam o sistema nuclear do Irã utilizando o worm Stuxnet

Ukrainian power grid - 2016

30 subestações de energia foram derrubadas por seis horas, afetando cerca de 80.000 pessoas

Motivação e Justificativa

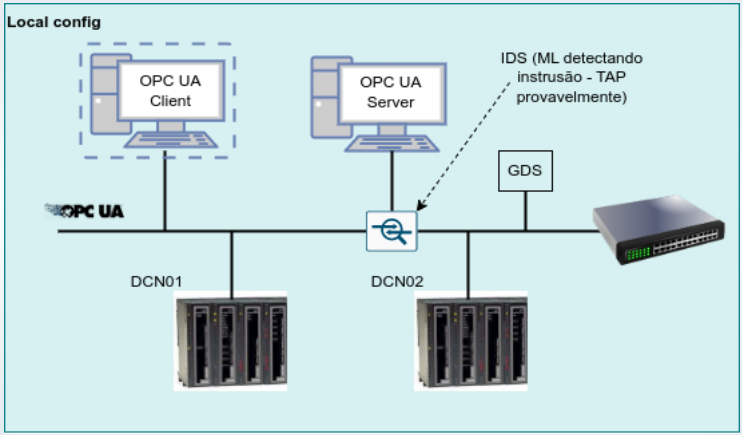
- Aumento nos casos de ataques cibernéticos em CPPSs
- *Industrial Internet of Things*
- *Artificial Intelligence*
- *Service Orientated Architecture* (SOA)
- *Open Process Automation Standards* (OPAS)
  - Baseado na IEC 62443
  - Possuí uma parte específica para Security
  - Comunicação baseada no OPC UA
- *Cybersecurity*
- Convergência IT/OT



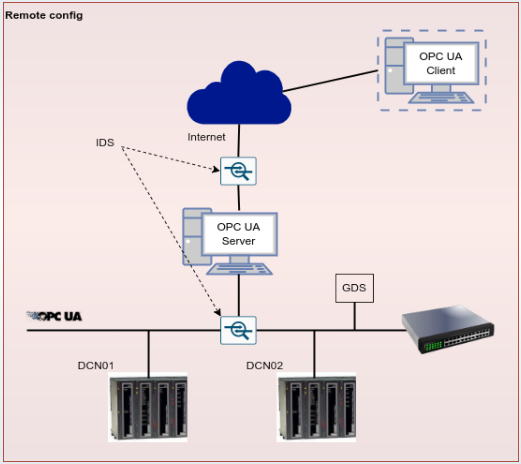
Pesquisa bibliográfica

- Bases de dados
  - IEEEXplore
  - Scopus
  - Web Of Science
- Termos de pesquisa
  - `OPC UA`
  - `Intrusion Detection System`
  - `Machine Learning`
  - `Anomaly Detection`
- Filtros de pesquisa
  - **Idioma:** Inglês
  - **Data:** 2016 - 2023
  - **Busca:** Obrigatório o termo `OPC UA`
- Principais referências
  - Desenvolvimento de método para detecção de intrusão em redes PROFINET baseado em técnicas de Aprendizado de Máquina [2]
  - Anomaly-based Intrusion Detection in Industrial Data with SVM and Random Forests [1]

Proposta


Local config
OPC UA Client
OPC UA Server
IDS (ML detectando instrusão - TAP provavelmente)
GDS
OPC UA
DCN01
DCN02

Proposta


Remote config
OPC UA Client
Internet
IDS
OPC UA Server
GDS
OPC UA
DCN01
DCN02

Metas estabelecidas

Table: Metas estabelecidas para a pesquisa.

METAS	DESCRIÇÃO
1	Pesquisa bibliográfica
2	Projeto e implementação do ambiente de teste para coleta de dados
3	Implementar ataques no ambiente proposto
4	Coleta e tratamento dos dados (*preprocessing*)
5	Apresentação para exame de qualificação
6	Análise das ferramentas de aprendizagem de máquinas
7	Desenvolvimento do método de detecção de intrusão
8	Verificação de desempenho e validação dos resultados
9	Escrita e submissão de artigo
10	Entrega final e defesa da dissertação

Table: Cronograma proposto para cumprimento das metas.

	2022	2023										2024							
METAS	–	03	04	05	06	07	08	09	10	11	12	01	02	03	04	05	06	07	08
1	Disciplinas da pós-graduação																		
2																			
3																			
4																			
5																			
6																			
7																			
8																			
9																			
10																			

Referências

[1] Simon D. Duque Anton, Sapna Sinha, and Hans Dieter Schotten. Anomaly-based intrusion detection in industrial data with svm and random forests. In *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–6, 2019.

[2] Afonso Celso Turcato. *Desenvolvimento de método para detecção de intrusão em redes PROFINET baseado em técnicas de Aprendizado de Máquina*. PhD thesis, Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2020. Tese (Doutorado em Sistemas Dinâmicos).

www.eesc.usp.br