



*Escola de Engenharia de São Carlos
Universidade de São Paulo*

Análise de vulnerabilidades em redes OPC UA industriais

Qualificação para mestrado em Engenharia Elétrica

Jonathan Tobias da Silva

Prof. Dr. Ivan Nunes da Silva
ORIENTADOR

Agenda

1 Introdução

- Motivação e Justificativa
- Objetivos

2 Referencial Teórico

- Protocolos IoT e IIoT
- *Cybersecurity*

3 Desenvolvimento

- Bancada Experimental
- Ataques em Redes Industriais OPC UA
- Metodologia

4 Resultados Esperados

5 Metas estabelecidas

- Cronograma proposto

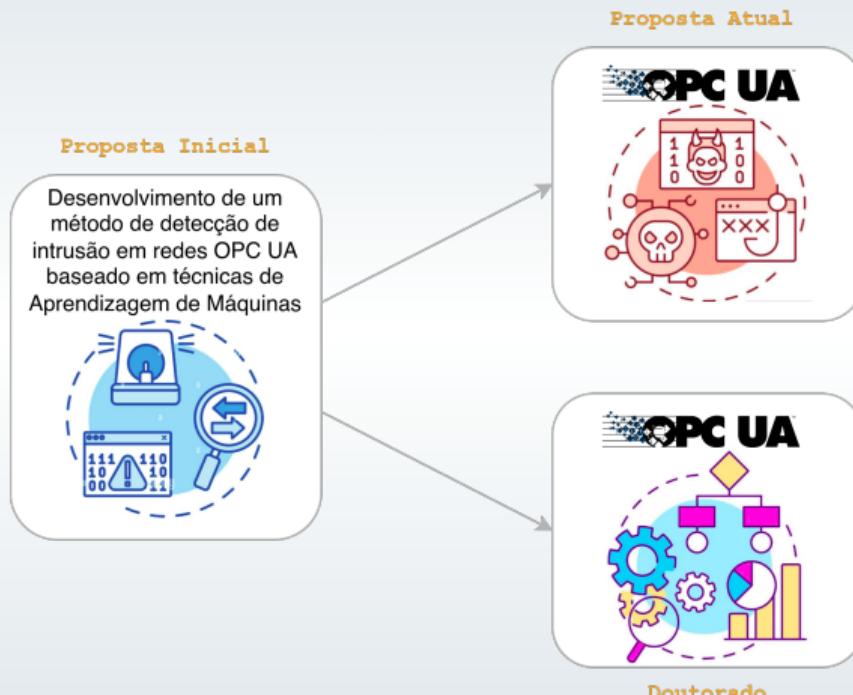
---- | Introdução | ---

Resumo

- Crescimento avançado da transformação digital
- Sistemas de Automação e Controle Industriais
- Protocolo OPC UA
- Preocupação com a segurança cibernética



Proposta inicial vs atual



Motivação

- Aumento nos casos de ataques cibernéticos em CPPSs

- *Industrial Internet of Things*

- Sistemas de Controle e Automação Industrial

- *Service Orientated Architecture* (SOA)

- *Open Process Automation Standards* (O-PAS)

- Baseado na IEC 62443
- Possui 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

Hackers 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

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



Pesquisa bibliográfica

OPC UA

■ Base de dados

- IEEEXplore

■ Termos de pesquisa

- OPC UA ou
- OPC Unified Architecture ou
- OPC:UA ou
- OPC-UA

■ Filtros de pesquisa

- Idioma: Inglês
- Data: 2018 - 2023

■ Critérios de exclusão:

- OPC UA aplicado na indústria ou IoT não é o foco principal da publicação;
- O OPC UA é referenciado na publicação, mas não é um tópico relevante da mesma;
- Publicações que se concentram em *marketing* de produtos e não priorizam o OPC UA como protocolo central ou recurso.

■ Publicação: IEEE/IAS International Conference on Industry Applications

- *A survey on OPC UA protocol: overview, challenges and opportunities*

Pesquisa bibliográfica

OPC UA + Analise de Vulnerabilidades

■ Bases de dados

- IEEEXplore
- Scopus
- Web Of Science

■ Termos de pesquisa

- **OPC UA** (ou derivados) e
- **Vulnerabilities** ou
- **Vulnerabilities Analysis** ou
- **Vulnerabilities Assessment**

■ Filtros de pesquisa

- **Idioma:** Inglês
- **Data:** 2013 - 2023

■ Principais referências

- Simulating and Detecting Attacks of Untrusted Clients in OPC UA Networks [1]
- Vulnerabilities of the Open Platform Communication Unified Architecture Protocol in Industrial Internet of Things Operation [2]
- Security Analysis of OPC UA in Automation Systems for IIoT [3]

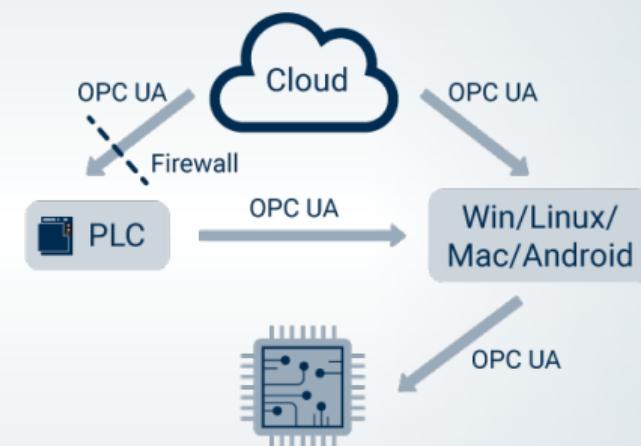
Investigação detalhada de ataques cibernéticos em redes OPC UA aplicadas nos sistemas de automação e controle industriais



--- | Referencial Teórico | ---

Principais aspectos do OPC UA

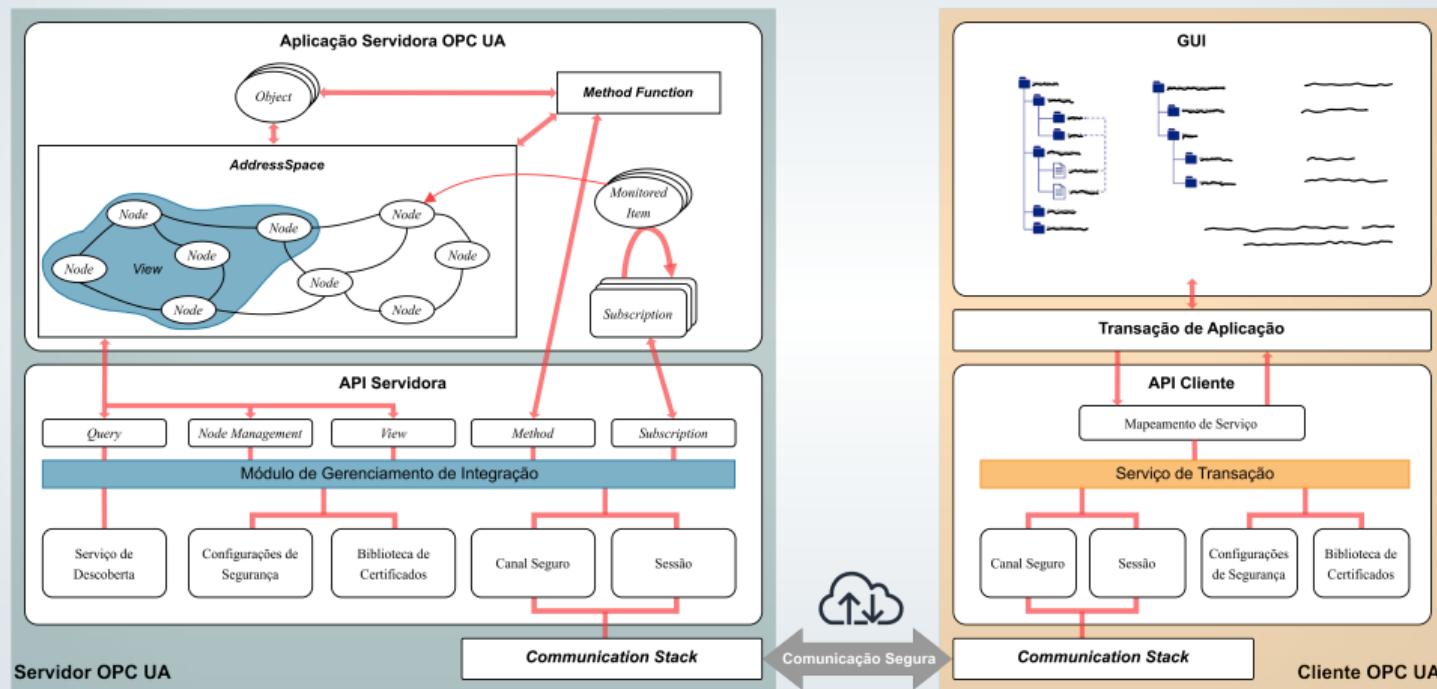
- Padrão de comunicação industrial interoperável
- Segurança integrada
- Plataforma agnóstica
- Modelo de informação unificado
- Arquitetura Orientada a Serviços (SOA)
- Robusto e confiável
- Suporte a dados complexos em tempo real
- Serviços Web



OPC Router - What is OPC UA?

OPC UA

Address Space e Information Model



OPC UA

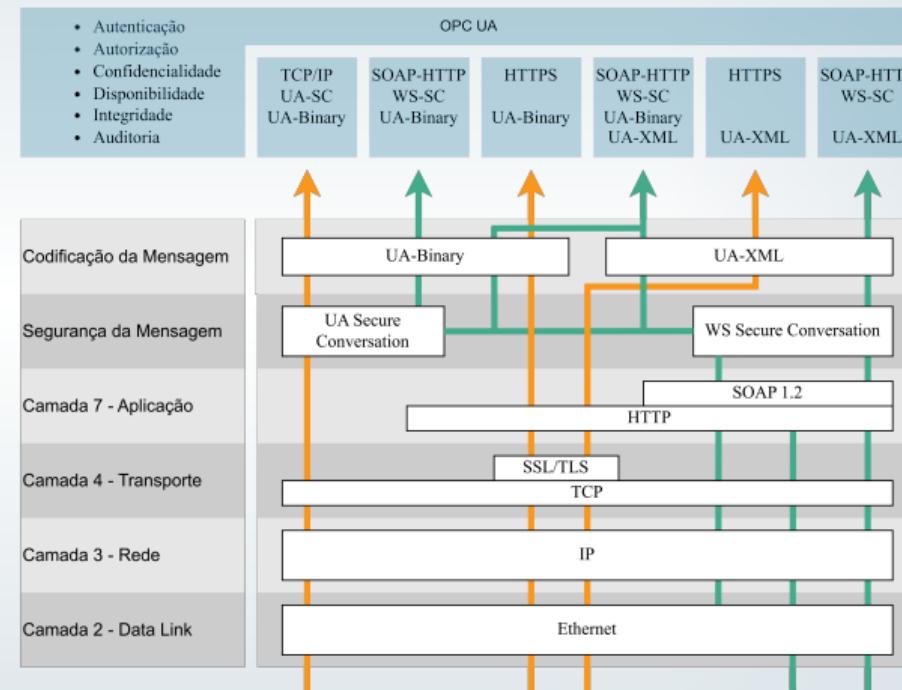
Escopo de proteção

■ Tríade CIA:

- Confidencialidade
 - Integridade
 - Disponibilidade

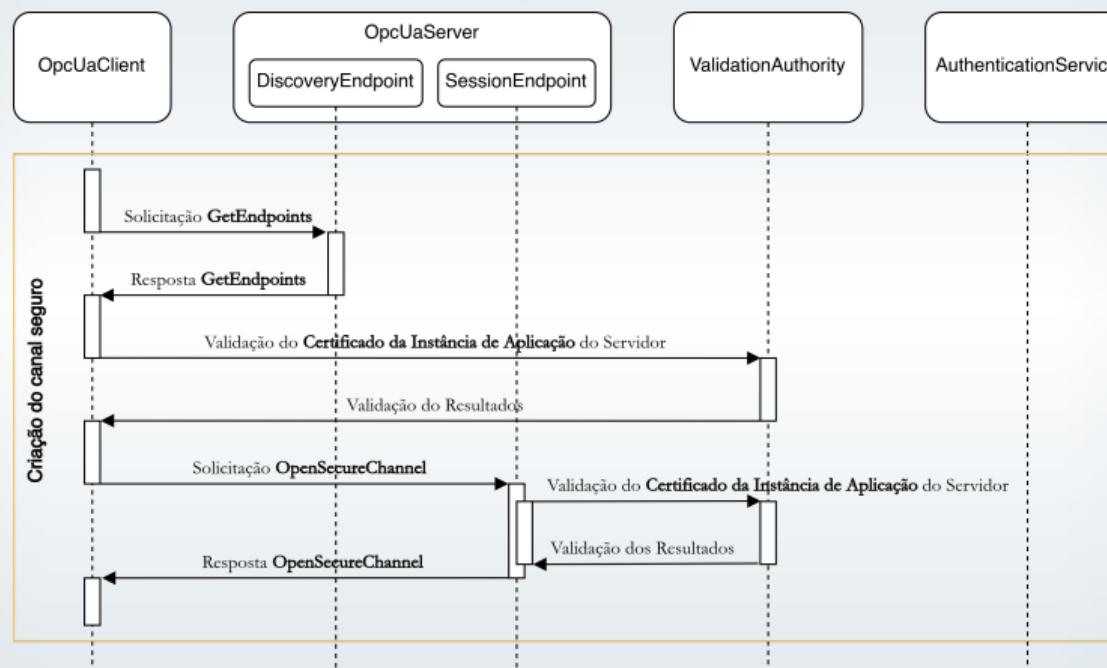
■ Framework AAA:

- Autenticação
 - Autorização
 - Auditoria



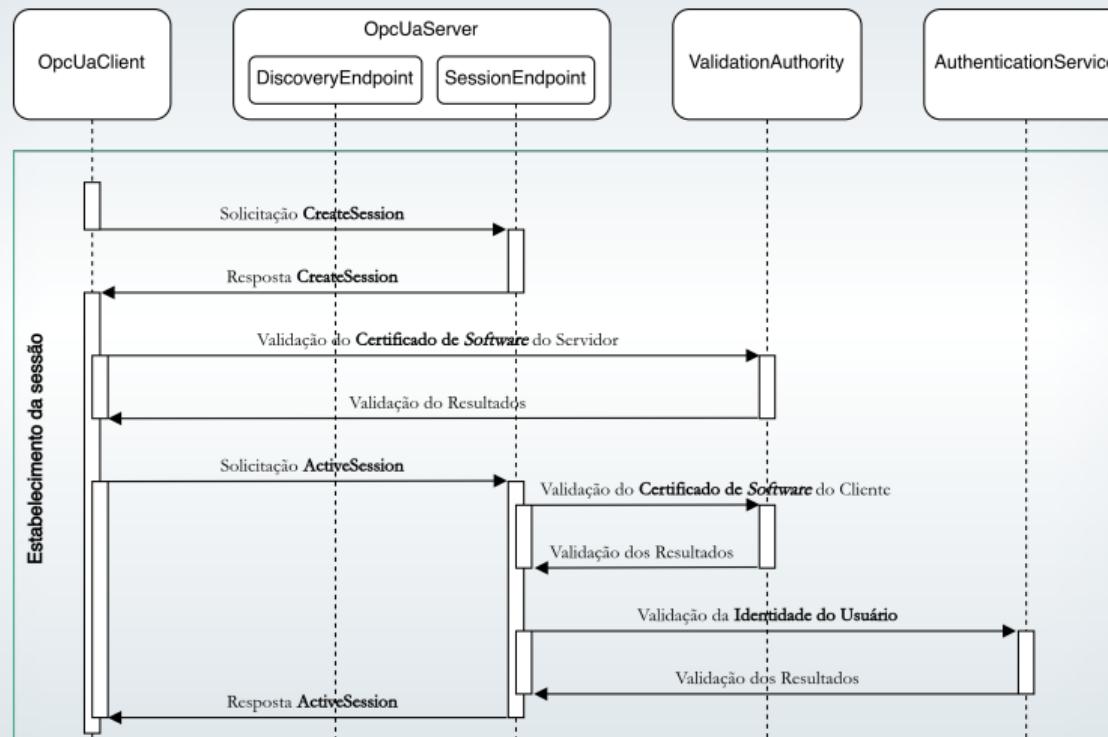
OPC UA

Processo de conexão segura



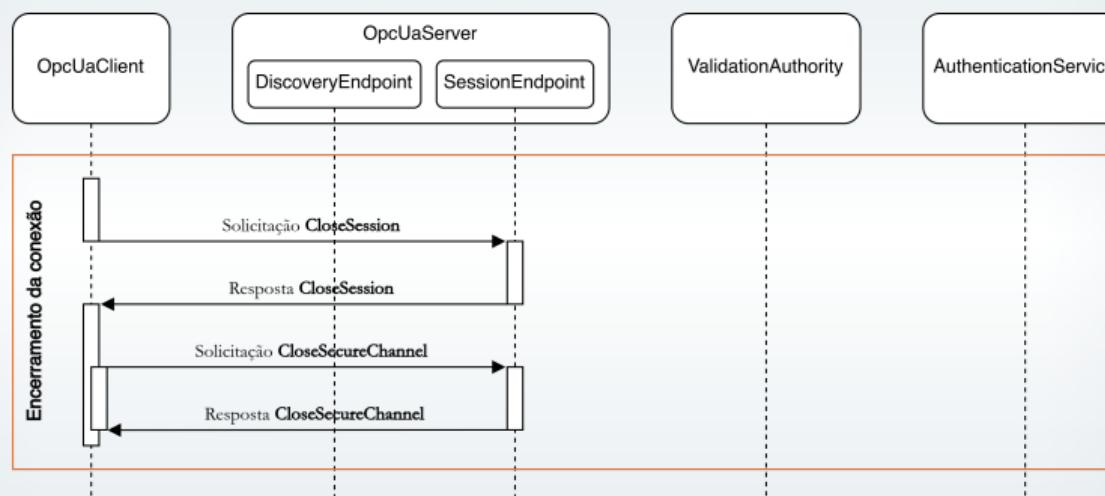
OPC UA

Processo de conexão segura



OPC UA

Processo de conexão segura

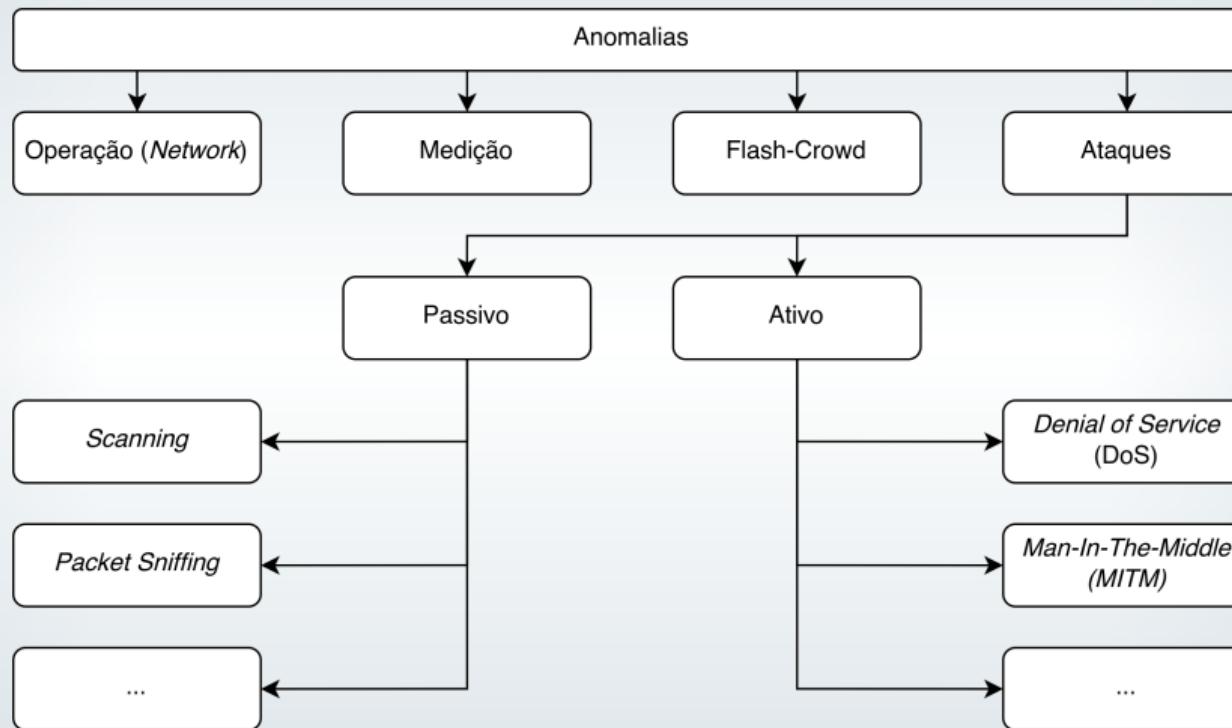


Convergência IT/OT



⁰Connection - Cisco IoT Manufacturing Solutions

Ataques cibernéticos



Análise e descoberta de vulnerabilidades

Análise de vulnerabilidade no âmbito de *software*:

- Estática
- Dinâmica
- Híbrida

Descoberta de vulnerabilidades:

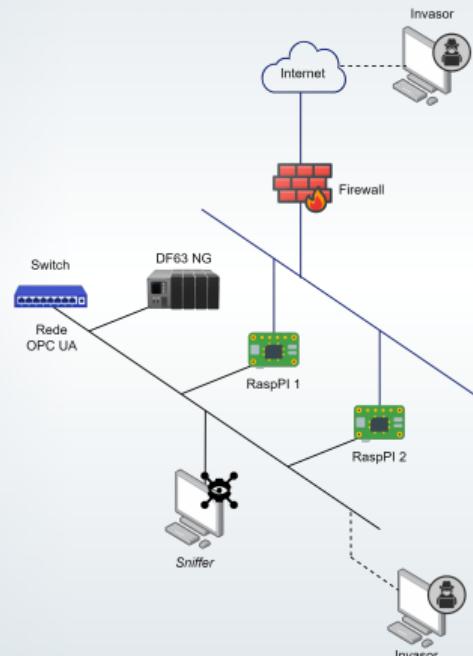
- Teste de Penetração
- *Fuzz-Testing*
- Análise Estática de Fluxo de Dados



---- | Desenvolvimento | ----

Bancada experimental

para testes de intrusões em redes OPC UA

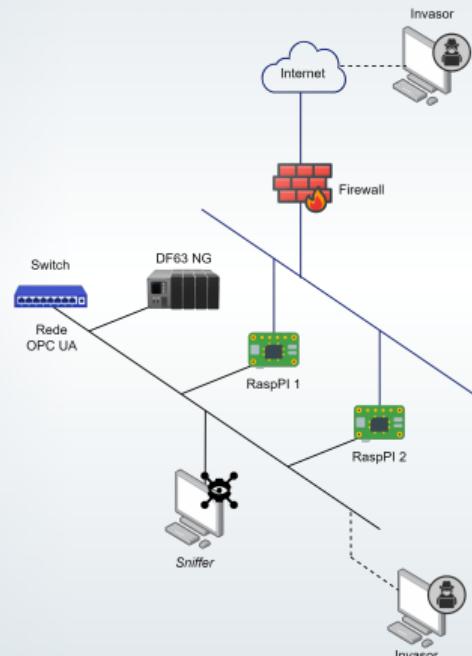


Hardware

- DF63 NG
- Raspberry Pi 4 Modelo B
- Ethernet Switch
- Elemento Invasor

Bancada experimental

para testes de intrusões em redes OPC UA

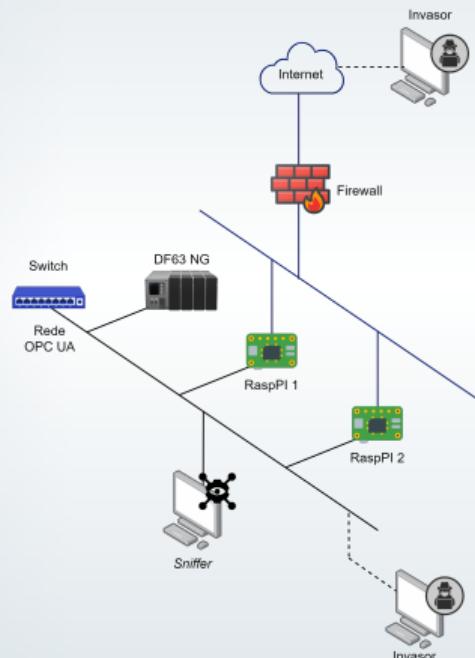


Software

- Smar OPC UA server
- opcua-asyncio
- OPC UA Exploit Framework
- Ettercap
- Hping3
- Wireshark
- Nmap

Bancada experimental

para testes de intrusões em redes OPC UA

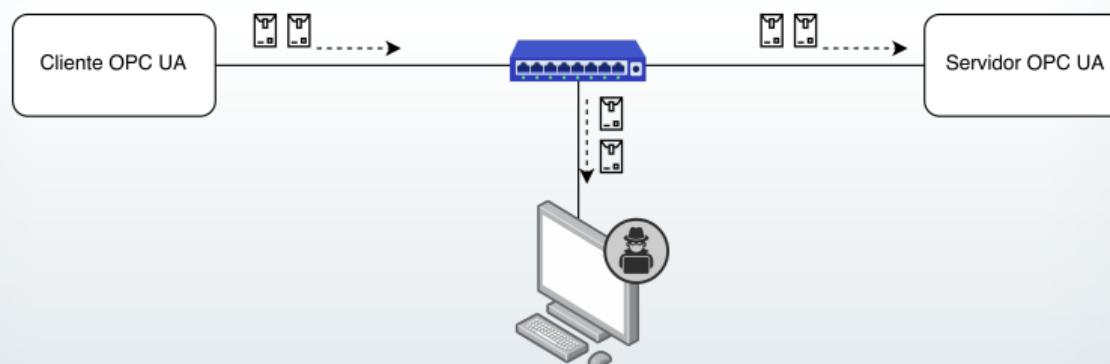


Packet Sniffing

- Monitorar comunicação OPC UA
- Roubar dados sigilosos (caso rede OPC UA não seja configurada corretamente)
- Ataque de entrada para outros

Execução:

- Ettercap
- Wireshark

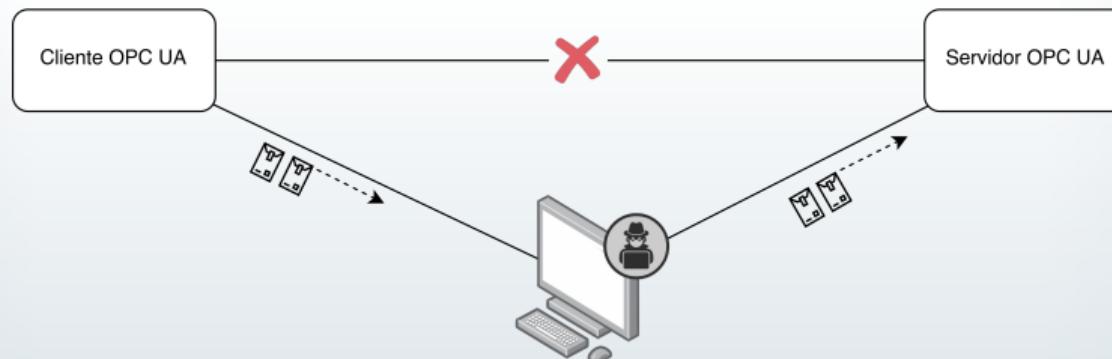


Man-in-The-Middle (MITM)

- Interceptação das informações do *SecureChannel*
- Inserção de elementos não confiáveis na rede OPC UA ao trocar os endereços MAC, pelo ARP
Spoofing
- Concede ao Elemento Invasor o poder de visualizar e/ou alterar informações da comunicação

Execução:

- Ettercap
- Wireshark

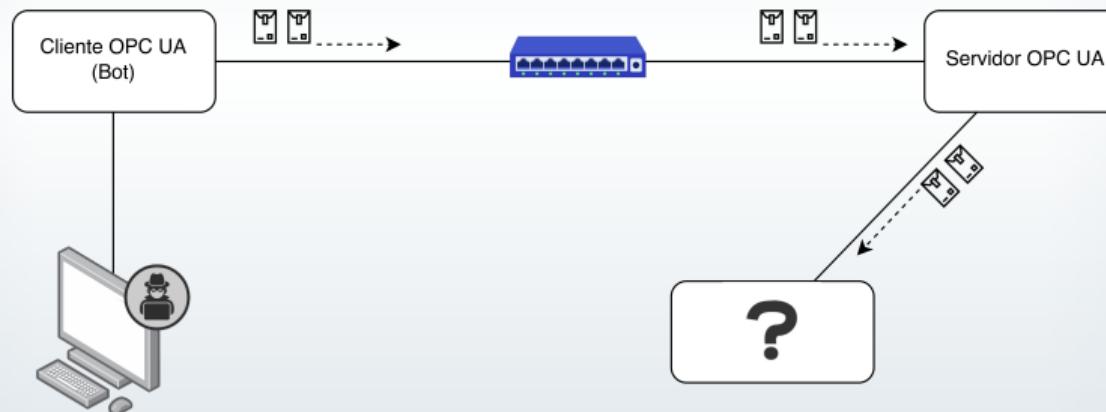


Denial of Service (DoS)

- Inundação da rede e do servidor ao enviar mensagens específicas continuamente
- Concede ao Elemento Invasor o poder de visualizar e/ou alterar informações da comunicação

Execução:

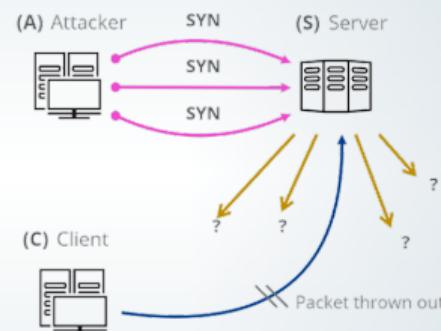
- Nmap
- OPC UA Exploit Framework
- Hping3
- Wireshark



Denial of Service (DoS)

SYN Flooding:

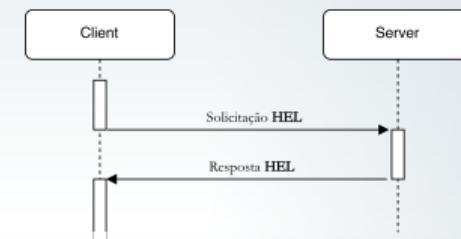
- Utilização do Nmap para a varredura da rede
- Uma vez mapeada, aplica-se o Hping3 para realizar este ataque



Denial of Service (DoS)

HEL Flooding:

- No caso do OPC UA, envio de mensagens contínuas HE (Hello message) para o servidor
 - Endpoint URL: `opc.tcp://192.168.164.102:4840/opcua/`
 - *Scheme*: `opc.tcp` ou `opc.https`
 - *Endereço do servidor*
 - *Porta*
 - *DiscoveryEndpoint*



Denial of Service (DoS)

Chunk Flooding:

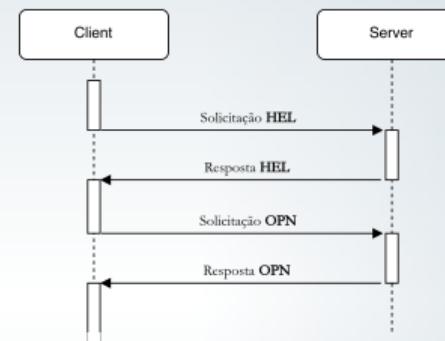
- *Chunk* refere-se a uma unidade de dados que pode ser transmitida entre um cliente e um servidor OPC UA
- Caso ocorra um erro na criação de um destes fragmentos, um *Chunk* final deve ser enviado
- A inundação por *Chunk* envolve o envio de uma quantidade abundante de fragmentos de dados ao servidor sem o envio do fragmento final correspondente



Denial of Service (DoS)

Abertura de múltiplos canais seguros:

- Solicitações OPN (OpenSecureChannel) são enviadas continuamente ao servidor.
 - Recursos substanciais são consumidos durante a validação do certificado, na solicitação e no processo de criptografia da mensagem
 - Pode ser ainda mais eficaz quando a Autoridade de Certificação está localizada em um sistema diferente

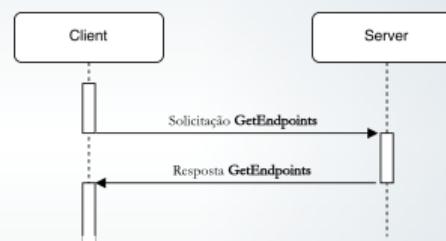


```
> Frame 47: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interface enp4s0
> Ethernet II, Src: Raspberry_2e:1a:b6 (e4:5f:01:2e:1a:b6), Dst: Raspberry_2e:1b:c1 (e4:5f:01:2e:1b:c1)
> Internet Protocol Version 4, Src: 192.168.164.101, Dst: 192.168.164.102
> Transmission Control Protocol, Src Port: 37738, Dst Port: 4840, Seq: 70, Ack: 29, Len: 138
> Opca Binary Protocol
  Message Type: OPEN
  Chunk Type: F
  Message Size: 132
  SequenceNumber: 0
  SecurityPolicyUri: http://opcfoundation.org/UA/SecurityPolicy#None
  SenderCertificate: <MISSING>[OpcUa Null ByteString]
  ReceiverCertificateThumbprint: <MISSING>[OpcUa Null ByteString]
  SequenceNumber: 1
  RequestId: 1
- Message: Encoded Object
  > Type: ExtendedObject
  > OpenSecureChannelRequest
    > RequestHeader: RequestHeader
    ClientProtocolVersion: 8
    SecurityTokenInRequestType: Issue (0x0000000000)
  
```

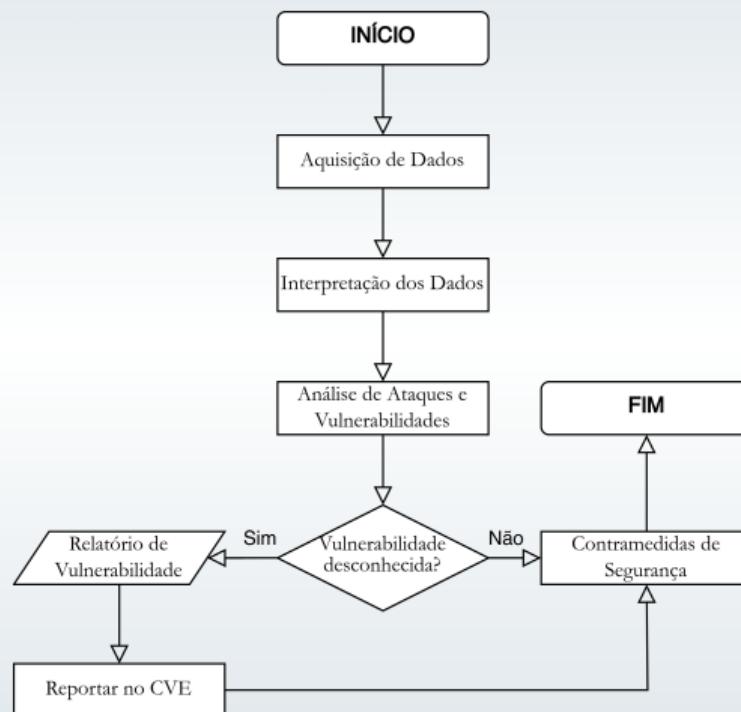
Denial of Service (DoS)

Tradução do caminho de navegação:

- São enviadas ao servidor requisições de traduções de *browse path* complexas que exploram a falta de limites adequados na resolução destes caminhos



Fluxo de atividades



---| Resultados Esperados |---

Sniffing:

- Alto nível de resistência à interceptação não autorizada de pacotes, dependendo do nível de segurança aplicado
- Segurança garantida no modo Sign&Encrypt
- Comprometimento da confidencialidade dos dados nos demais modos de segurança

MITM:

- Dependência significativa da configuração aplicada na comunicação
- Caso nível mais alto de segurança, o OPC UA não deve permitir a quebra de algum pilar de segurança
- No entanto, a integridade dos dados pode ser comprometida nos demais níveis
- Contramedidas devem ser propostas para as falhas encontradas

DoS:

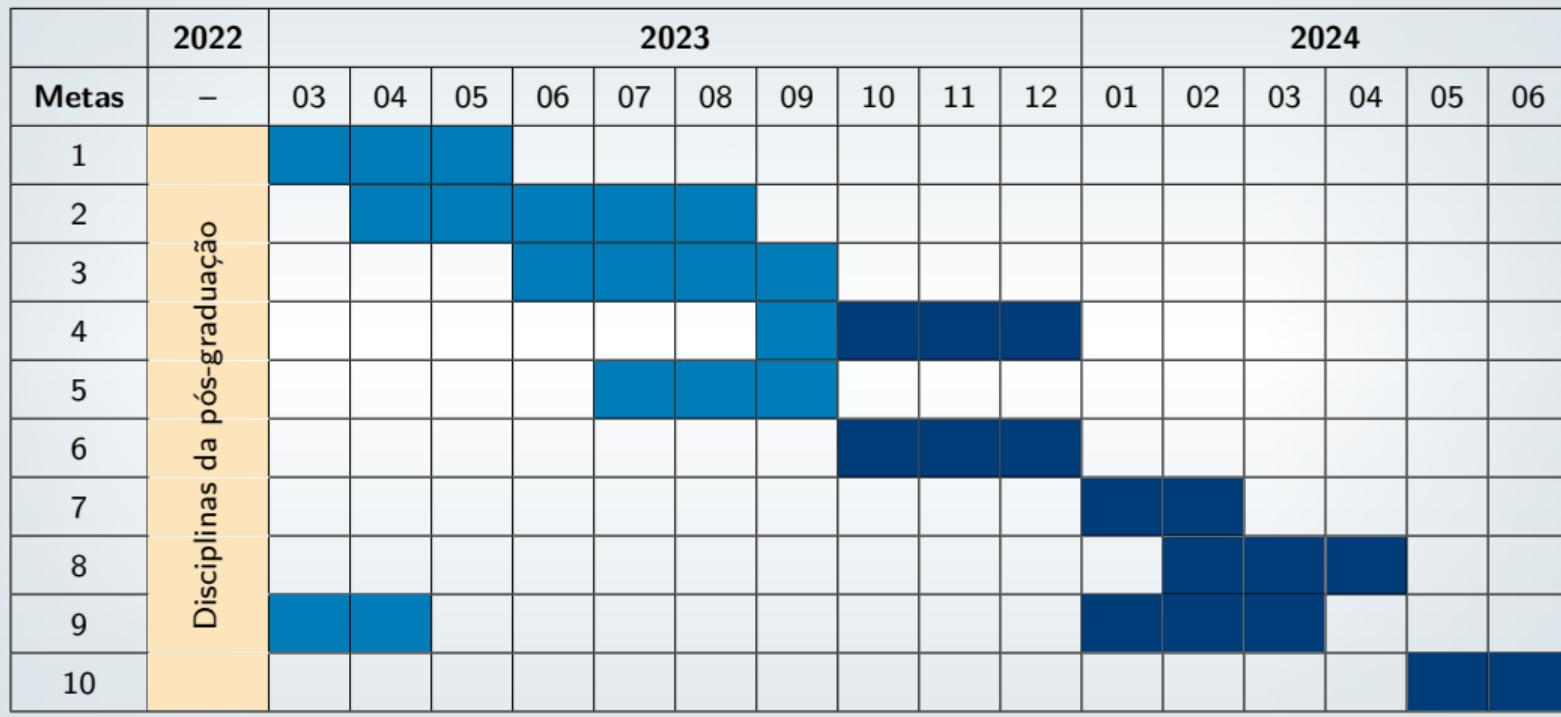
- Depende da capacidade da rede e do processamento dos hospedeiros
- Em redes reais, os efeitos devem ser potencializados devido à quantidade de equipamentos
- Esgotamento de recursos em alguns tipos de ataques de negação de serviço, comprometendo disponibilidade dos dados

---| Metas estabelecidas |---

Table: Metas estabelecidas para a projeto.

Metas	Descrição
1	Pesquisa bibliográfica
2	Projeto e implementação do ambiente de teste para coleta de dados
3	Análise e escolha dos ataques cibernéticos
4	Implementação dos ataques na bancada experimental
5	Dissertação para exame de qualificação
6	Coleta e interpretação dos dados
7	Análise dos ataques e vulnerabilidades em redes industriais OPC UA
8	Verificação de desempenho e validação dos resultados
9	Escrita e submissão de artigo científico
10	Entrega final e defesa da dissertação

Table: Cronograma proposto para cumprimento das metas.



■ Itens realizados

■ Itens propostos

Referências

- [1] Charles Varlei Neu, Ina Schiering, and Avelino Zorzo. Simulating and detecting attacks of untrusted clients in opc ua networks. In *Proceedings of the Third Central European Cybersecurity Conference*, CECC 2019, New York, NY, USA, 2019. Association for Computing Machinery.
- [2] Dong-Hyuk Shin, Ga-Yeong Kim, and Ick-Chae Euom. Vulnerabilities of the open platform communication unified architecture protocol in industrial internet of things operation. *Sensors (Basel)*, 22(17), August 2022.
- [3] Vaishnavi Varadarajan. Security analysis of opc ua in automation systems for iiot, 2022.



EESC • USP

www.eesc.usp.br