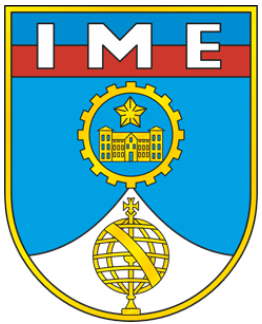

# PTP Flood: ataque cibernético de DoS em cliente PTP




Diego Piffaretti
Anderson Santos
Gabriela Dias

Instituto Militar de Engenharia (IME)

# Contextualização

Uso do PTP (Precision Time Protocol)

- Indústrias de Automação e Controle
- Data Centers
- Serviços Financeiros
- Redes de Telecomunicações
- Indústria de Energia
- Televisão e Radiodifusão

# Motivação

- Decreto nº 9.573/2018 do Brasil aprovou a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)
- Meta migrando seu datacenter para utilizar PTP

**Presidência da República**
**Secretaria-Geral**
**Subchefia para Assuntos Jurídicos**

**DECRETO Nº 9.573, DE 22 DE NOVEMBRO DE 2018**

Aprova a Política Nacional de Segurança de Infraestruturas Críticas.

**PRESIDENTE DA REPÚBLICA,** no uso da atribuição que lhe confere o art. 84, **caput** , inciso VI, alínea "a", da Constituição,

**DECRETA:**

Art. 1º Fica aprovada a Política Nacional de Segurança de Infraestruturas Críticas - PNSIC, nos termos do Anexo.

Art. 2º Compete ao Gabinete de Segurança Institucional da Presidência da República o acompanhamento dos assuntos pertinentes às infraestruturas críticas no âmbito da administração pública federal.

Art. 3º A administração pública federal direta, autárquica, fundacional e as empresas estatais dependentes de recursos do Tesouro Nacional para o custeio de despesas de pessoal ou para o custeio em geral considerarão, em seus planejamentos, ações que concorram para a segurança das infraestruturas críticas.

Meta

**Making Our Network Clocks More Precise for the Metaverse**

We're deploying Precision Time Protocol (PTP) across our data centers to sync our computer networks down to nanoseconds. PTP offers a new...

21 de nov. de 2022

Engineering at Meta

**PTP: Timing accuracy and precision for the future of computing**

Meta is deploying a timing protocol, Precision Time Protocol (PTP), that will offer new levels of accuracy and precision to our networks and...

21 de nov. de 2022

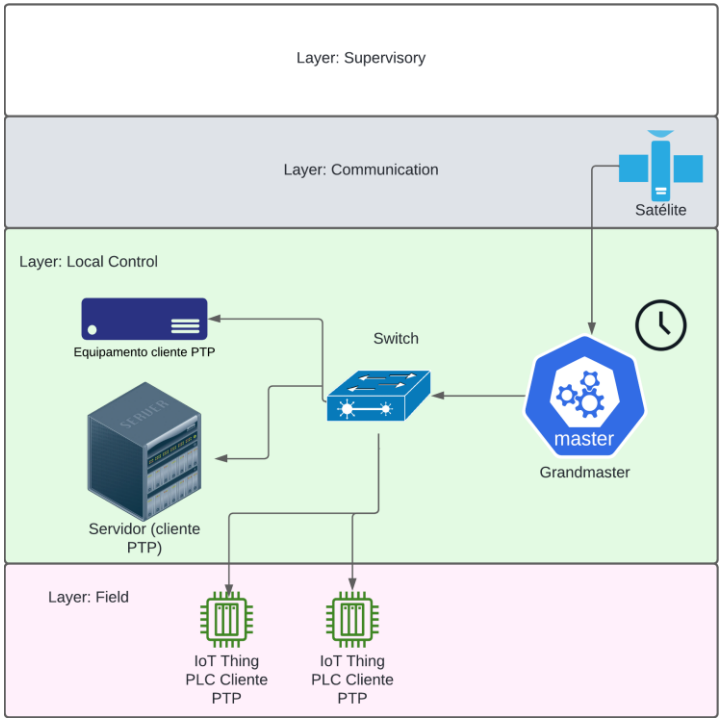
# Problema de pesquisa

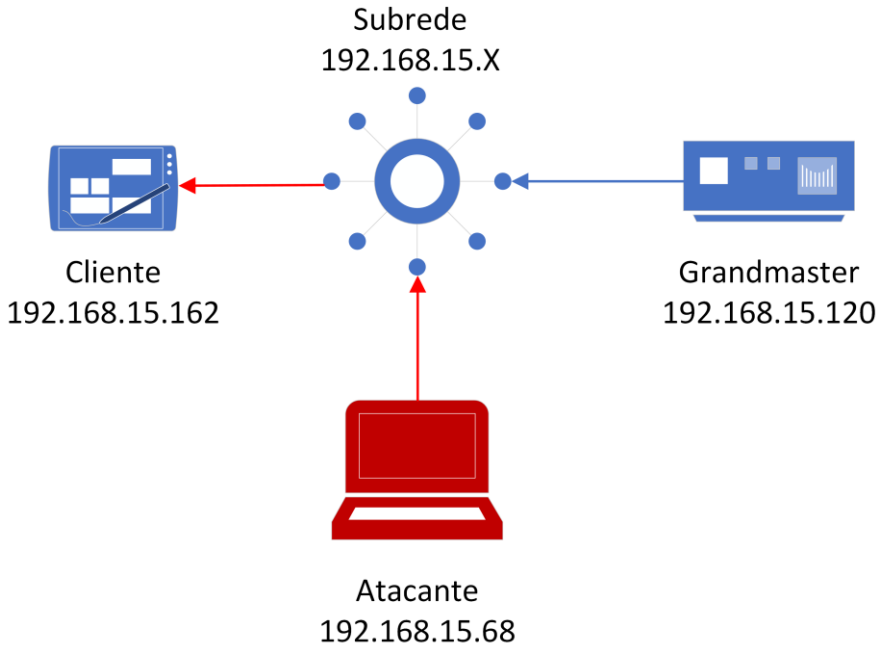
| | Ataques | | | Versão do PTP | |
|---|---|---|---|---|---|
| Artigo | DoS | Replay | Outros | PTP v2.0 (IEEE-2018) | PTP v2.1 (IEEE-2019) |
| Fotouhi [Fotouhi et al. 2023] | X | X | X | | X |
| Berardi [Berardi et al. 2023] | X | | X | | X |
| Rezabek [Rezabek et al. 2023] | | X | X | | X |
| Alghamdi [Alghamdi and Schukat 2022] | X | X | X | | X |
| Moradi [Moradi and Jahangir 2021] | | | X | X | |
| Alghamdi [Alghamdi and Schukat 2021] | | X | | | X |
| Alghamdi [Alghamdi 2021] | X | X | X | | X |
| Moussa [Moussa et al. 2020] | | | X | X | |
| Alghamdi [Alghamdi and Schukat 2020a] | | | X | X | |
| DeCusatis [DeCusatis et al. 2020] | X | | | X | |
| Alghamdi [Alghamdi and Schukat 2020c] | X | X | X | | X |
| Alghamdi [Alghamdi and Schukat 2020b] | | X | X | | X |
| Alghamdi [Alghamd and Schukat 2020] | | X | X | | X |
| Itkin [Itkin and Wool 2020] | | | X | X | |

## Trabalhos que usaram o TLV

# Solução Proposta

# Solução Proposta



# Solução Proposta

| Dados | Tempo de gravação | PPS | PPS Retransmitidos |
|---|---|---|---|
| Alpha | 1 minuto | 255,1 | 3743,57 |
| Beta | 3 Minutos | 254,7 | 3336,18 |

# Solução Proposta

| Minuto | MB | Porcentagem | MB | Porcentagem |
|---|---|---|---|---|
| 1 | 99 | 9,7% | 70 | 6,8% |
| 2 | 181 | 17,7% | 134 | 13,1% |
| 3 | 264 | 25,8% | 184 | 18,0% |
| 4 | 327 | 31,9% | 230 | 22,5% |
| 5 | 380 | 37,1% | 295 | 28,8% |
| 6 | 458 | 44,7% | 353 | 34,5% |
| 7 | 537 | 52,4% | 418 | 40,8% |
| 8 | 607 | | 466 | 45,5% |
| 9 | 654 | | 514 | 50,2% |
| 10 | 705 | | 591 | 57,7% |
| 11 | 775 | | 65 | |
| 12 | 822 | | 70 | |
| 13 | 886 | | 77 | |
| 14 | | | 82 | |
| 15 | 982 | 95,9% | | |
| 16 | 1024 | 100% | | |
| 17 | N/A | N/A | 98 | |
| 18 | N/A | N/A | 1024 | 100,0% |

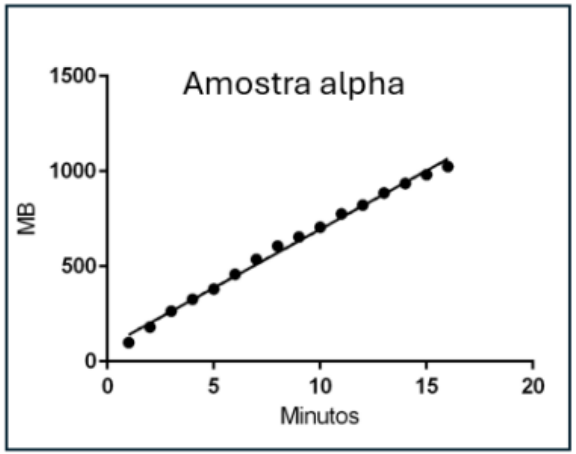
***Amostra alpha atinge 100% de uso de memória RAM aos 16 minutos***

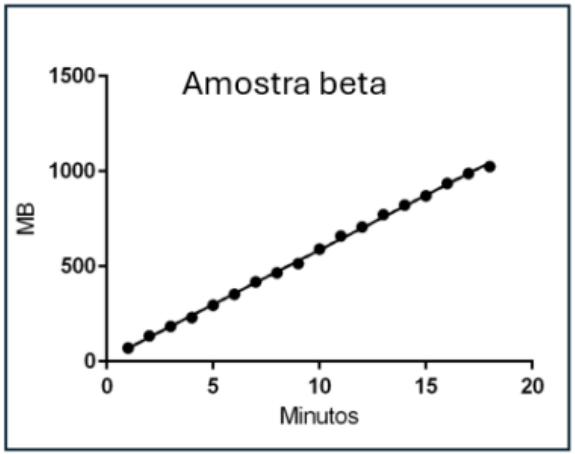
***Amostra beta atinge 100% de uso de memória RAM aos 18 minutos***

# Avaliação

Regressão linear das amostras

- Amostra alpha: y = 61.66176X + 78.125
- Amostra beta: y = 57.41176X + 12.03268



# Mitigações

- Anexar um marcador à primeira mensagem originada do mestre e incrementar esse valor para cada mensagem subsequente
- Estabelecimento de uma identidade digital para os nós mestres

# Considerações finais

- Análise dos resultados evidenciou que ataques de replay em um cliente PTP, mesmo com TLV habilitado, resultam em negação de serviço (PTP flood)
- O consumo de memória durante o ataque demonstrou um comportamento linear ao longo do tempo
- Identificação e prevenção desses ataques são fundamentais para garantir a integridade e disponibilidade dos sistemas de rede

# Trabalhos futuros

- Outras técnicas de ataques no PTP com requisitos de segurança disponíveis implementados
- Explorar as mitigações
- Análises mais avançadas da regressão linear com novas amostras

# OBRIGADO

Perguntas?

martins.diego@ime.eb.br
www.comp.ime.eb.br/pos/


# Patrocinadores do SBSeg 2024!

nic.br

cgi.br

Google

Tempest

CAPES

SiDi

FAPESP

zscaler™

BugHunt

CNPq

C.E.S.A.R

FACULDADE IBPTECH