DOI: 10.48011/asba.v2i1.1196

Análise da segurança de redes em sistemas de automação e controle industriais: estudo de caso com a planta MecatrIME

Christiana Couto, Gustavo Claudio Karl Couto, Antonio Eduardo Carrilho da Cunha

Instituto Militar de Engenharia
Praça General Tibúrcio, 80, 22290-270, Praia Vermelha, Rio de Janeiro, RJ, Brasil.
(christianacouto,gustavokcouto,carrilho@ime.eb.br).

Abstract: The growing concern about cyber attacks, motivated researchers to seek security solutions for networks of industrial automation and control systems. This work carried out a data capture of the local network of the MecatrIME plant of the Mechatronics Laboratory of the Military Engineering Institute (IME) in order to elaborate a solution to increase its security. The results indicated that the main protocols of the network are: ARP, TCP, UDP and SMB2. An architecture that allows the secure connection of the plant to the Internet, based on the creation of a demilitarized zone and an intrusion detection system was proposed, in order to protect the network from these cyber attacks.

Resumo: A crescente preocupação com ataques cibernéticos motivou pesquisadores a buscarem soluções de segurança para redes de sistemas de automação e controle industriais. Por isso, este trabalho realizou uma captura de dados na rede local da planta MecatrIME, do Laboratório de Mecatrônica do Instituto Militar de Engenharia (IME), a fim de elaborar uma solução para aumentar a sua segurança. Os resultados indicaram que os principais protocolos da rede são: ARP, TCP, UDP e SMB2. Então, foi proposta uma arquitetura que permite a conexão segura da planta à Internet, baseada na criação de uma zona desmilitarizada e de um sistema de detecção de intrusão, a fim de proteger a rede desses ataques cibernéticos.

Keywords: Industrial automation and control systems; cyber-physical systems; information security; electric networks; wireshark; demilitarized zone

Palavras-chaves: Sistemas de automação e controle industriais; sistemas ciber-físicos; segurança da Informação; redes elétricas; wireshark, zona desmilitarizada

1. INTRODUÇÃO

Inicialmente, as redes dos sistemas de automação e controle industriais (*Industrial automation and control systems* - IACS) eram isoladas e dedicadas, por isso foram elaboradas sem focos específicos para as ameaças cibernéticas. Mas com a atualização tecnológica para à Indústria 4.0 (Popkova et al., 2018), esses sistemas foram conectados à rede externas.

Essa conexão permite o monitoramento remoto da produção em tempo real e a transmissão dos dados para o setor corporativo, que poderá utilizá-los nas decisões estratégicas a fim de aumentar a produtividade das empresas. Técnicas modernas de inteligência de negócios e ciências de dados são utilizadas no tratamento desses dados.

Por outro lado, a conexão com à Internet expõe os IACS às ameças do ambiente cibernético. Ao contrário dos casos nos sistemas de tecnologia da informação tradicionais, esses ataques aos IACS podem causar danos físicos às pessoas, ao meio ambiente e aos ativos físicos dos sistemas como as máquinas de produção.

Por exemplo, no Irã, em 2010, um ataque ciber-físico a uma usina nuclear, com o *worm* Stuxnet, conseguiu controlar um atuador em um sistema SCADA, enquanto fazia parecer que a operação estava normal aos operadores da usina (Langner, 2011).

Em outro caso famoso, Garcia et al. (2008) descobriram o funcionamento do protocolo de criptografia de cartões de identificação por radiofrequência do tipo MIFARE. Infelizmente, isso permitiu que atacantes desenvolvessem ataques como o de clonagem desses cartões.

Nesse contexto, a crescente preocupação com ataques cibernéticos motivou diversas entidades a criarem soluções para a segurança cibernética de IACS, como sistemas de detecção de intrusão (*intrusion detection system* - IDS) e

⋆ O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, utilizou infraestrutura computacional financiada com recursos do subprojeto Pesquisa cibernética do Projeto Estratégico do Exército Brasileiro e da Financiadora de Estudos e Projetos (FINEP).

de prevenção de intrusão (*intrusion prevention system* - IPS).

Este trabalho apresenta uma análise da rede da planta MecatrIME [1] do Laboratório de Mecatrônica do Instituto Militar de Engenharia (IME), a fim de estudar e propor melhorias para a sua segurança. Para isso, foi feita uma captura e análise do tráfego dos pacotes transmitidos com a ferramenta *wireshark*.

Os principais protocolos dessa rede foram descobertos, organizados e analisados quanto ao seu funcionamento na rede e vulnerabilidades de segurança. Com base nessa análise, elaborou-se uma solução para conectar a planta à Internet durante a operação da linha de montagem, superando o requisito de segurança baseado no isolamento. A arquitetura criada utiliza uma zona desmilitarizada e um sistema de detecção de intrusão para detectar ataques que almejam alterar a produção da planta.

Este trabalho está dividido em cinco seções, além desta introdução: a seção 2 discute os trabalhos relacionados; a seção 3 descreve a planta utilizada; na seção 4, são apresentados e discutidos os resultados da análise de rede com o *wireshark*; na seção 5 é apresentada a solução proposta; e, por fim, na seção 6 são apresentadas as conclusões do trabalho.

2. TRABALHOS RELACIONADOS

Considera-se que o estudo e análise dos dados que trafegam em uma rede são importantes na detecção de ameaças e no desenvolvimento de ferramentas para proteger todo o sistema. As unidades básicas da comunicação em redes de computadores são os pacotes de dados (Tanenbaum and Wetherall, 2010). Os segmentos de dados que encapsulam esses pacotes contém informações como protocolos, endereços de origem e destino, horário de transmissão e etc. Com essas informações, é possível identificar se o conteúdo de um pacote pode ser prejudicial ao sistema e deduzir a ocorrência de um ataque cibernético.

Couto et al. (2020) fizeram um estudo sobre a segurança cibernética da plataforma MecatrIME através de uma simulação. Foi realizada uma análise de risco e uma estratégia de defesa para a proteção da planta foi elaborada.

Iii (2016) sugeriu a utilização do *wireshark* para a captura e análise de pacotes em sistemas de controle industriais. Isso é conveniente visto que as informação de controle são encapsulada dentro dos protocolos da camada de transporte e, por isso, requerem uma análise de rede mais profunda.

Os IACS utilizam sistemas, como o sistema de gerenciamento de redes e os sistemas de supervisão e aquisição de dados (*Supervisory Control and Data Acquisition - SCADA*), que são implementados via *software* para controlar e monitorar dispositivos dispersados espacialmente (Stouffer et al., 2015). A comunicação com o sistema SCADA é feita através de uma interface gráfica, que permite aos operadores monitorar e controlar esse sistema em tempo real.

Segundo Zhu et al. (2011), no contexto de sistemas SCADA, a injeção de pacotes mal formados pode levar os equipamentos de destino, como atuadores, a se comunicarem erroneamente. Isso pode causar a perda de controle e monitoramento dos operadores.

Segundo Pramod and Sunitha (2018), as taxas de transmissão de pacotes são periódicas em sistemas SCADA. Ao observar o tempo de resposta entre esses pacotes, pode-se classificá-los em: normal, retransmissão, perdido ou anormal. Além disso, os sistemas SCADA são estáticos, então os endereços IP designados não mudam com frequência.

Por isso, essa informação pode ser incluída na definição dos padrões de normalidade, junto ao tamanho dos pacotes, os protocolos usados e as identidades. A definição de um padrão de normalidade pode ser usado para comparação com o monitoramento em tempo real, a fim de detectar desvios que possam indicar falhas acidentais ou advindas de ataques.

Carvalho and Santos (2015) identificaram ameaças e vulnerabilidades que surgiram nos sistemas SCADA, após o fim dos isolamentos, e propuseram uma arquitetura denominada honeySCADA. Essa solução coleta ataques cibernéticos a esses sistemas, por meio da simulação da interação entre um *honeypot*, que simula um CLP, e um equipamento do operador.

Andrade et al. (2018) abordaram a segurança da informação em sistemas SCADA. Analisou-se as principais diferenças entre os ambientes de TI tradicional e o ambiente industrial. Além disso, foram analisados os tipos de atacantes, as ferramentas de segurança e as aplicações de técnicas de segurança disponíveis para sistemas SCADA. Em seguida, foram apresentados vinte e um passos para aumentar a segurança desses sistemas. Por fim, foi feito um teste, como exemplo, de estudo do grau de vulnerabilidade resultante da conexão de um sistema SCADA à Internet.

Vários pesquisadores utilizaram o *wireshark* em seus trabalhos para detectar ataques em redes de computadores como Iqbal and Naaz (2019), McDonald et al. (2008) e Banerjee et al. (2010).

Alguns sugeriram a utilização do *wireshark* como base para a criação de sistemas de detecção de intrusão (Banerjee et al., 2010). Um IDS armazena um banco de dados dos padrões de ataques conhecidos. Esses são, então, comparados aos *logs* que estão sendo monitorados na rede para detectar a ocorrência de semelhanças que possam significar um ataque.

Em outro trabalho, Iqbal and Naaz (2019) realizaram um teste mostrando que, quando uma comunicação sob ataque é observada com o *wireshark*, muitos pacotes de ARP *reply* são enviados da máquina que simula o atacante. Esses pacotes fornecem o endereço MAC do atacante para as máquinas legítimas e vinculam-no a dois endereços IP diferentes.

Eckhart and Ekelhart (2018) utilizaram o *wireshark* para identificar ataques do tipo *ARP cache poisoning* (Zhu et al., 2011), em um módulo de segurança, como parte da elaboração de um Gêmeo digital para a sistemas ciberfísicos.

[1] `https://sites.google.com/ime.eb.br/mecatrime`

Utilizando-se o *wireshark*, pode-se estabelecer filtros de pacotes pré-configurados, dentro de padrões considerados perigosos para proteger um sistema de possíveis ataques. No entanto, essa ferramenta não é capaz de gerar um alarme ou implementar uma ação de segurança. Ainda assim, pode-se utilizá-la junto a outras ferramentas para alcançar esses objetivos.

Outra solução existente para esse cenário é a chamada zona desmilitarizada, ou DMZ (DeMilitarized Zone), a parte da rede de uma empresa que não está na região de segurança (Tanenbaum and Wetherall, 2010). Pode-se incluir nela máquinas, como um servidor Web ou de banco de dados, e através dela, conectar os computadores da rede corporativa à Internet de modo seguro .

3. A PLANTA MECATRIME

Neste estudo de caso, foi utilizada a plataforma MecatrIME, do Laboratório de Mecatrônica do Instituto Militar de Engenharia (IME), ilustrada na Figura 1. A planta é composta por uma estação de gerenciamento (P9), seis estações de produção (P2-P7), uma estação de controle do transporte de peças pela esteira (P8) e uma estação de armazenagem (P1), totalizando assim nove estações interligadas por uma esteira. As estações de produção ilustram alguns dos principais processos de fabricação industriais como torneamento (P2), fresamento (P3), soldagem (P4), metrologia (P5), montagem e inspeção visual (P6) e gravação a laser (P7).

A ligação entre elas é feita por cabos formando uma rede local (*Local Access Network* - LAN) Ethernet utilizando a pilha de protocolos de comunicação TCP/IP. A comunicação entre os computadores nas estações e a rede do IME é realizada por meio de um ponto de acesso à Internet e a comunicação entre os dispositivos e os computadores nas estações é feita utilizando o protocolo RS232.

O *software* utilizado para o controle da planta é o OpenCIM (IntelitekInc., 2019), que controla, monitora e opera a produção conforme a abordagem CIM. O *software* é composto pelo módulo CIM *Manager* e os módulos *Station Manager*. O CIM *Manager* é o módulo instalado na estação de gerenciamento que coordena a funcionalidade de todos os dispositivos da planta através da LAN. Os *Station Manager* são os módulos instalados em cada estação, que as controlam e se comunicam com o CIM *Manager*.

As estações podem ser utilizadas de forma isolada, sem o controle da estação de gerenciamento. Então, caso aconteça algum problema com essa estação, ou o usuário só necessite de um único processo, pode-se utilizá-lo separadamente. Essa rede pode ser considerada como uma rede ponto-a-ponto (*peer-to-peer*) já que todas as estações podem enviar e receber mensagens entre si.

Os computadores conectados à rede da MecatrIME não podem se conectar à rede sem fio do IME, ao mesmo tempo em que a linha de operação está em execução, por motivos de segurança, mas podem ser utilizados normalmente quando a planta não está em execução.

A planta é utilizada regularmente no ensino de áreas como controle de sistemas, computação, robótica e mecatrônica.

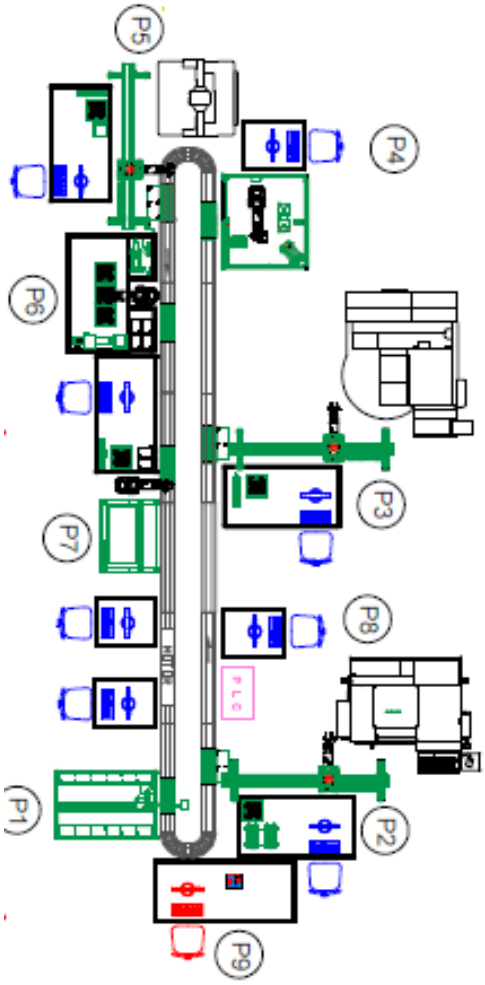

Figura 1. Planta da MecatrIME

Como o OpenCIM possui código fechado, não é possível saber o seu comportamento exatamente, mas pode-se estudá-lo, a partir da captura de informações com um analisador de rede, como o *wireshark*.

4. ANÁLISE DA REDE DA MECATRIME

Como os IACS são compostos por equipamentos heterogêneos, criados por diferentes fabricantes, a ferramenta selecionada para a sua análise precisa ser versátil.

O analisador de pacotes *wireshark* [2], de código aberto, identifica diferentes tipos de protocolos e funciona em muitos equipamentos com diferentes tipos de sistemas operacionais (Iqbal and Naaz, 2019). Além disso, essa ferramenta permite a criação de regras de *firewalls*, com base nos dados capturados, para vários sistemas operacionais.

Então, neste trabalho, utilizou-se o *wireshark* para capturar pacotes, interceptar e registrar o tráfego, na planta MecatrIME, a fim de analisar o funcionamento da sua rede. A metodologia utilizada foi baseada na criada por Iqbal and Naaz (2019).

[2] Ferramenta disponível em `https://www.wireshark.org/docs/`

A captura ocorreu, na estação de gerenciamento e na estação do torno, em duas situações. Primeiramente, foi feito o processamento de uma peça na estação do torno, como exemplo de uma etapa do processo de produção. A outra análise foi realizada com a linha de montagem parada.

É importante frisar que a estação de fresamento estava desligada da rede, nos dois ensaios, por motivos técnicos. Para comprovar isso, foi feita um busca por seu IP nas amostras de dados coletadas, utilizando-se os filtros "ip.dst" e "ip.src" no *wireshark*, que não retornou resultados.

No total, no primeiro caso, na estação de gerenciamento, foram recuperados 55.922 pacotes, durante aproximadamente quatro horas. No segundo caso, foram capturados 305 pacotes na estação de gerenciamento e 4891 no torno.

Como a hierarquia da arquitetura do OpenCIM não mostra as conexões dos dispositivos internos para a estação de gerenciamento, não houve detalhamento dos pacotes nesse nível mais baixo.

Os protocolos identificados foram os seguintes:

- ARP - *Address Resolution Protocol*;
- *Microsoft Windows BROWSER Protocol*;
- DHCPv6 - *Dynamic Host Configuration Protocol* para o IPv6;
- DNS - *Domain Name System*;
- ETHERNET;
- HTTP - Hypertext Transfer Protocol;
- ICMPv6 - *Internet Control Message Protocol* ver. 6;
- IP - *Internet Protocol* versões 4 e 6;
- IGMPv3 - *Internet Group Management Protocol* versão 3;
- LANMAN - *Microsoft Windows Lanman remote API protocol*;
- LLMNR - *Link-Local Multicast Name Resolution*;
- MDNS - *Multicast Domain Name System*;
- NBNS - *NetBIOS Name Service*;
- SMB - *Server Message Block* versões 1 e 2;
- SSDP - *Simple Service Discovery Protocol*;
- TCP - *Transmission Control Protocol*;
- UDP - *User Datagram Protocol*; e
- TLS - *Transport Layer Security* versões 1 e 1.2.

4.1 Análise do primeiro caso

A Figura 2 ilustra o resultado da captura de dados com a linha de produção parada.

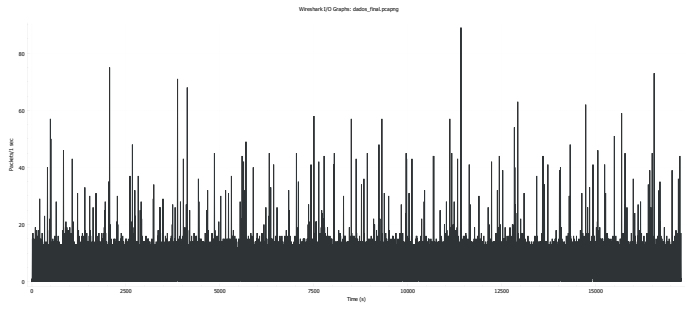

Figura 2. Captura de pacotes na estação de gerenciamento no primeiro caso

As parcelas de pacotes, em relação ao total, e a velocidade de transmissão média para os protocolos UDP, TCP, ICMPv6, IGMP e ARP, no primeiro caso, são apresentadas na Tabela 1.

Tabela 1. Parcelas dos pacotes por protocolo e velocidade de transmissão no primeiro caso

Protocolo	**Pacotes** (%)	**velocidade (bits/s)**
ARP	7,8	79
IPv6 - UDP	9,6	19
IPv6 - TCP	41,5	5582
IPv6 - ICMP	8,1	66
IPv4 - UDP	25,4	52
IPv4 - TCP	6,8	433
IPv4 - ICMP	0,1	1
IPv4 - IGMP	0,7	2

Observa-se, a partir da Tabela 1, que a maioria dos pacotes transmitidos utilizam o protocolo TCP e o IP versão 6, que é relativamente rápido. Por outro lado, a parcela de dados transmitida pelo protocolo UDP e o IP versão 4 é relativamente baixa e menos rápida.

Ressalta-se que analisar a velocidade de transmissão em IACS é importante porque, como esses sistemas operam em tempo real, o tráfego dos dados deve ser o mais rápido possível.

4.2 Análise do caso de requisição

As parcelas de pacotes, em relação ao total, e a velocidade de transmissão média para o caso da requisição, capturadas na estação de gerenciamento são apresentadas na Tabela 2, e, as capturadas na estação do torno, na Tabela 3 .

Tabela 2. Parcelas dos pacotes por protocolo e velocidade de transmissão média na estação de gerenciamento

Protocolo	**Pacotes** (%)	**velocidade (bits/s)**
ARP	12,5	10
IPv6 - UDP	12,1	2
IPv6 - ICMP	3,6	2
IPv4 - UDP	38,7	7
IPv4 - TCP	30,5	296
IPv4 - ICMP	0,7	0
IPv4 - IGMP	2,0	0

Observa-se, a partir da Tabela 2, que a maioria dos pacotes transmitidos utilizam o protocolo TCP e o IP versão 4, diferentemente do caso geral, no qual a versão 6 é mais utilizada.

A Figura 3 ilustra as parcelas dos pacotes que utilizam os protocolos: TCP (em amarelo), UDP (em preto), SSDP (em laranja), TLS (em vermelho), ARP (em rosa) e IPv6 (em verde), em relação ao total de pacotes capturados na estação de gerenciamento.

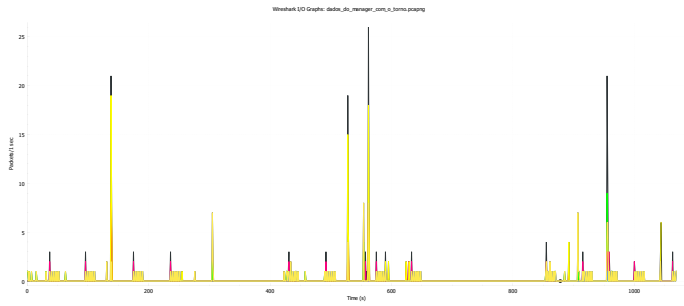

Figura 3. Filtro de pacotes nos dados da estação de gerenciamento

Observa-se que os picos são formados, em maioria, pelos protocolos TCP e UDP, como era de se esperar, já que a maioria dos pacotes são transmitidos por esses protocolos.

Nota-se também, que são expressivos os picos nos quais o protocolo TLS compõe uma parcela alta. Deduz-se que representam os momentos de estabelecimento das sessões, quando trafega uma quantidade alta de bits.

Tabela 3. Parcela dos pacotes por protocolo e velocidade de transmissão média na estação do torno

Protocolo	**Pacotes** (%)	**velocidade (bits/s)**
ARP	3,9	78
IPv6 - UDP	5,6	21
IPv6 - TCP	53,4	7317
IPv6 - ICMP	3,5	51
IPv4 - UDP	27,4	103
IPv4 - TCP	5,7	467
IPv4 - IGMP	0,6	4

A Figura 4 ilustra as parcelas dos pacotes que utilizam os protocolos TCP (em amarelo), UDP (em preto) e SMB2 (em verde), em relação ao total de pacotes capturados na estação do torno.

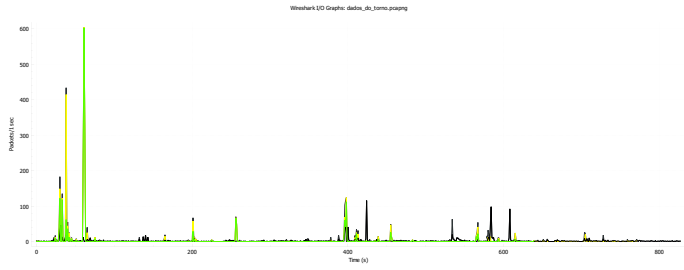

Figura 4. Filtro nos pacotes capturados na estação do torno

Observa-se, a partir da Tabela 3, que a maioria dos dados transmitidos pelo protocolo TCP é encapsulada na versão 6, como no primeiro caso. Isso é corroborado pelos dados da Figura 4, a partir do que infere-se que os picos na transmissão dos pacotes representam os pacotes que utilizam o protocolo TCP (em amarelo).

O maior desses pico deve-se ao grande número de erros de conexão na execução do protocolo SMB2, como será explicado na subseção 4.6. Observa-se que os pacotes que utilizam o protocolo SMB2 formam uma parcela expressiva do total, influenciando significativamente nos picos encontrados na Figura 4.

As próximas subseções irão analisar os resultados, considerando, individualmente, os protocolos ARP, ICMP, TCP, UDP e SMB2 focando na sua segurança.

4.3 Protocolo ARP

O protocolo ARP é responsável por correlacionar os endereços IP e MAC em uma rede, através do envio de perguntas (*request*) e respostas (*reply*), para todas as máquinas (Tanenbaum and Wetherall, 2010). Alguns exemplos dos pacotes de *request* e *reply* do protocolo ARP, coletados neste trabalho, estão detalhados na Tabela 4.

Tabela 4. Mensagens do protocolo ARP

Origem	**Destino**	**bits**	**Informação**
HP_X:X:b4	HP_X:X:5f	42	X.X.1.1 is at X:X:X:X:X:b4
HP_X:X:d3	Broadcast	60	Who has X.X.1.16? Tell X.X.1.15
HP_X:X:c0	Broadcast	60	Who has X.X.1.15? Tell X.X.1.16
HP_X:X:7a	Broadcast	60	Who has X.X.1.16? Tell X.X.1.12
HP_X:X:7d	Broadcast	60	Who has X.X.1.16? Tell X.X.1.14
HP_X:X:c0	Broadcast	60	Who has X.X.1.12? Tell X.X.1.16
HP_X:X:c0	Broadcast	60	Who has X.X.1.14? Tell X.X.1.16
HP_X:X:b4	Broadcast	42	Who has X.X.1.16? Tell X.X.1.1
HP_X:X:c0	HP_X:X:b4	60	X.X.1.16 is at X:X:X:X:X:c0
HP_X:X:d3	HP_X:X:b4	60	X.X.1.15 is at X:X:X:X:X:d3

A partir da análise da Tabela 4, conclui-se que as estações da planta MecatrIME enviam mensagens em *broadcast* para se identificarem mutuamente. A mensagem "XXX.XXX.1.1 *is at* X:X:X:X:X:b4", que identifica o endereço MAC da estação de gerenciamento para as outras máquinas na rede, apareceu na amostra coletada 1325 vezes.

Considerando que no total foram coletadas 3387 mensagens do protocolo ARP, isso significa que quase um terço dessas mensagens buscam garantir que todas as máquinas consigam se corresponder com a estação de gerenciamento. Isso pode ser explicado pela importância dada a essa estação na arquitetura da rede.

Por outro lado, as outras máquinas só transmitiram pacotes de ARP *reply*, com seus endereços MAC, 14 vezes cada em média.

Um tipo de ataque a esse protocolo é o *ARP cache poisoning* (Zhu et al., 2011), que pode ser evitado utilizando tabelas estáticas com os endereços da planta MecatrIME. Essas tabelas podem ser criadas e armazenadas facilmente, considerando que utilizam-se algumas dezenas de endereços.

4.4 Protocolo TCP

O protocolo de controle de transmissão é um dos principais protocolos de rede da Internet e complementa o UDP (Tanenbaum and Wetherall, 2010). Sua implementação oferece controle de fluxo e de congestionamento dando mais confiabilidade as aplicações.

Para iniciar uma conexão TCP, entre um cliente e um servidor, é feito um procedimento padrão chamado *SYN/ACK handshake*, que consiste na troca de pacotes específicos para tal.

Primeiramente, o cliente envia um pacote SYN para o servidor, que responde, em seguida, com um pacote SYN/ACK confirmando o recebimento. Por último, o cliente também envia outro pacote ACK confirmando esse recebimento (Tanenbaum and Wetherall, 2010).

O protocolo TCP foi o mais utilizado na capturada de dados realizada, como está apresentado nas Tabelas 2 e 3.

Um exemplo de ataque a esse protocolo é descrito no trabalho de Iqbal and Naaz (2019). Observou-se, no teste realizado, uma grande quantidade de pacotes TCP, com as *flags* SYN ativadas geradas por um único endereço IP, mas sem recebimento de nenhuma confirmação do servidor. Isso indica um ataque de Inundação SYN, do tipo DoS, (Tanenbaum and Wetherall, 2010) que pode sobrecarregar uma máquina alvo e, consequentemente, desabilitá-la.

Algumas contra-medidas a esse ataque são: o bloqueio do envio de pacotes por endereços de origem que não pertençam à rede local, o bloqueio do recebimento de pacotes, oriundos da Internet, que contenham endereço de origem igual ao de um endereço IP da rede local ou a utilização de criptografia e autenticação na comunicação.

4.5 Protocolo ICMP

O ICMP é a parte do IP que fornece relatórios de erros à fonte de origem. Quando ocorre um evento fora do padrão, como um pacote IP não chegar ao seu destino, uma mensagem ICMP é enviada automaticamente ao transmissor (Tanenbaum and Wetherall, 2010).

O protocolo ICMP também pode ser usado para testar a conectividade entre máquinas. O método chamado *ping* consiste no envio de pacotes para um dado equipamento de destino e no agrupamento das respostas recebidas. Para isso, mensagens do tipo "ECHO" e "ECHO REPLY" são utilizadas pelos transmissores para verificar se os destinatários estão ativos (Tanenbaum and Wetherall, 2010).

Na amostra de dados coletada neste trabalho, foram capturados quarenta e oito pacotes do tipo "Echo (ping) request id=0x0001, seq=1/256, ttl=32 (no response found!)", da estação de gerenciamento para a estação do torno, durante o caso de requisição. Isso significa que houve erros de conexão e, portanto, deve-se buscar soluções para otimizar esse processo.

4.6 Protocolo SMB2

O protocolo SMB2[3] é utilizado para acesso a sistemas de arquivos, nos quais clientes realizam pedidos para um servidor de arquivos.

Do total de 4891 pacotes recuperados na estação do torno, durante a execução do pedido para a estação do torno, 2130 utilizaram o protocolo SMB2 com destino à estação de torno.

Mas nenhum pacote desse tipo de protocolo foi capturado na estação de gerenciamento.

Um exemplo da amostra desses pacotes está apresentado na Tabela 5.

Tabela 5. Pacotes do protocolo SMB2

Origem	Destino	bits	Info
X:X:X:94ce	X:X:X:4985	358	Create Request File:X
X:X:X:4985	X:X:X:94ce	350	Create Response File:X
X:X:X:94ce	X:X:X:4985	238	Write Request Len:48 Off:0 File:X
X:X:X:4985	X:X:X:94ce	158	Write Response
X:X:X:94ce	X:X:X:4985	286	GetInfo Request File:X
X:X:X:4985	X:X:X:94ce	270	GetInfo Response;GetInfo Response
X:X:X:4985	X:X:X:94ce	186	Break Response
X:X:X:94ce	X:X:X:4985	178	Break Request
X:X:X:4985	X:X:X:94ce	202	Close Response
X:X:X:94ce	X:X:X:4985	166	Close Request File:
X:X:X:94ce	X:X:X:4985	240	Session Setup Request, NTLMSSP_NEGOTIATE
X:X:X:4985	X:X:X:94ce	179	Session Setup Response
X:X:X:94ce	X:X:X:4985	186	Tree Connect Request Tree: ||-MANAGER|IPC
X:X:X:4985	X:X:X:94ce	158	Tree Connect Response
X:X:X:94ce	X:X:X:4985	146	Tree Disconnect Request
X:X:X:4985	X:X:X:94ce	151	Tree Disconnect Response
X:X:X:94ce	X:X:X:4985	146	Session Logoff Request
X:X:X:4985	X:X:X:94ce	146	Session Logoff Response
X:X:X:94ce	X:X:X:4985	182	Negotiate Protocol Request
X:X:X:4985	X:X:X:94ce	248	Negotiate Protocol Response

Deduz-se, a partir da análise dos pacotes da Tabela 5, que a estação do torno está requisitando a criação de arquivos para a estação de gerenciamento, durante uma sessão.

Um ataque famoso, que se aproveitou de uma vulnerabilidade do protocolo SMB, foi o *Wannacry*, que abalou mais de 150 países, em 2017. Os atacantes utilizaram um *ransomware*, que foi analisado por Akbanov et al. (2018), utilizando o *wireshark*.

4.7 Protocolo UDP

O UDP é um dos principais protocolos de rede da Internet e complementa o TCP (Tanenbaum and Wetherall, 2010). Sua implementação permite que aplicações enviem mensagens de tamanho fixo, chamadas de datagramas, encapsuladas em pacotes IPv4 ou IPv6, a um dado destino sem precisar criar conexões.

Apesar de não garantir a chegada dos pacotes aos seus destinos, o protocolo UDP possui uma grande vantagem, quando se trata de serviços nos quais a velocidade é fundamental e uma perda mínima de dados não é muito desvantajosa (Tanenbaum and Wetherall, 2010).

Quase todos os pacotes desse tipo de protocolo capturados na planta MecatrIME partiram da estação de gerenciamento, como por exemplo "63202 -> 49546 Len=319".

[3] `https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/5606ad47-5ee0-437a-817e-70c366052962`

Durante o processo de requisição para o torno, nenhum pacote desse tipo foi identificado na estação de gerenciamento, somente no torno. Deduz-se, então, que é importante para a estação de gerenciamento confirmar o recebimento da sua requisição, mas as mensagens enviadas a partir da estação do torno não são essenciais para a operação.

5. SOLUÇÃO DE SEGURANÇA CIBERNÉTICA PARA A PLANTA MECATRIME

Esta seção apresenta uma solução para a segurança cibernética da planta MecatrIME, composta por uma DMZ, para a proteger a conexão com a a rede privada virtual (*Virtual Private Network* - VPN) do IME, e um sistema de detecção de intrusão na rede interna. Além disso, propõe-se uma forma segura para monitoramento remoto da planta.

5.1 Proposta de uma zona desmilitarizada

Partindo-se dos resultados apresentados nas seções anteriores, elaborou-se uma arquitetura para a planta MecatrIME, que permitirá o senvio dados em tempo real à Internet de modo seguro, superando o requisito de isolamento. Dessa forma, poderá se monitorar a rede à distância.

Essa arquitetura se baseia na criação de uma DMZ, seguindo a metodologia de Young (2003).

Considera-se a LAN da planta MecatrIME como a rede interna da DMZ e a VPN do IME como a rede externa. Isso está ilustrado na Figura 5.

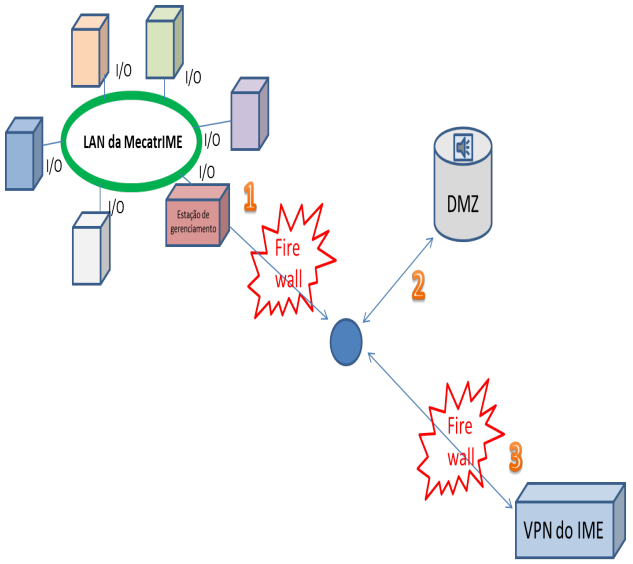

Figura 5. Zona desmilitarizada para a planta MecatrIME

O ponto de conexão entre a DMZ e a LAN deve ser a estação de gerenciamento, porque é a partir dela que se pode obter acesso direto a todas as informações da planta.

Entre a DMZ e a rede interna (conexão 1 na Figura 5), deve-se instalar um *firewall* independente, de forma *offline* da rede. Também deve bloquear tudo o que vá para a rede interna, de maneira que o tráfego nessa conexão se torne unidirecional. Isso protegerá a planta mesmo no caso eventual de um ataque a partir de uma máquina na DMZ.

Entre a DMZ e a VPN do IME, será configurado um outro *firewall*, de um fabricante diferente do primeiro, que permitirá o fluxo bidirecional de acordo com regras de segurança.

Nas máquinas dentro da DMZ não deverão operar programas, recursos ou utilitários que não sejam essenciais. Além disso, o conjunto de usuários e senhas dessas máquinas deve ser diferente do utilizado nas redes interna e externa, para garantir que, no caso de descoberta dessas informações, um atacante não as utilize em outra subrede. Esses procedimentos seguem as recomendações de Young (2003).

5.2 Sistema de detecção de intrusão

Os sistemas de detecção de intrusão podem detectar atividades maliciosas através da correlação entre o monitoramento de dados e um padrão pré-definido de comportamento benigno (Mitchell and Chen, 2014). Pode-se detectar inclusões de dispositivos desconhecidos, conexões não especificadas, alterações nas conexões e etc. (Eckhart and Ekelhart, 2018). Caso ocorra que um ataque interno na LAN, por exemplo, por um meio físico, como uma *pen-drive*, uma DMZ não seria suficiente para proteger a planta, então precisa-se de outro método auxiliar.

A partir da análise realizada na seção 3, pode-se desenvolver um padrão de comportamento benigno para a MecatrIME. Com esse levantamento, é possível criar uma *whitelist* dos protocolos e códigos aceitáveis na rede.

Deduz-se que, devido a intensa utilização do protocolo SMB2 para a requisição dos pedidos entre as máquinas, durante a operação da planta, deve-se utilizá-lo como filtro.

Portanto, sugere-se a criação de uma nova conexão na planta MecatrIME, exclusivamente para monitorar os pacotes SMB2 nas entradas e saídas de todas as estações, utilizando o *wireshark*.

Esses dados serão enviados, com criptografia, para uma outra máquina na DMZ que irá correlacioná-los para garantir a sua coerência. Caso haja uma discordância, será concluído que há interferências externas, como um ataque cibernético, e será acionado um alarme integrado aos dispositivos já existentes na planta para interromper a linha de produção. Uma metodologia semelhante foi utilizada por Banerjee et al. (2010).

Além disso, o *wireshark* pode ser utilizado para criar as regras de controle de acesso em *firewalls* no sistema operacional *Windows*. Com base na captura de pacotes realizada, sugere-se utilizar regras do tipo: “Source port- add portopening tcp 445 Wireshark ENABLE”, e “Destination port- add portopening tcp 49170 Wireshark ENABLE”. Isso permitiria o tráfego dos pacotes SMB2 já conhecidos, pelas portas normalmente utilizadas, mas bloquearia aqueles fora desse padrão.

5.3 Monitoramento remoto da planta

A utilização de uma DMZ também pode contribuir para monitorar remotamente a planta de forma segura. Pode-se criar um programa que gere um arquivo com o *log* da operação do OpenCIM *manager* na estação de gerenciamento.

Esse *log* deve ser enviado para uma rede externa de forma a monitorar a operação.

Assim, um conjunto desses *logs* poderão ser armazenados em um servidor de banco de dados, dentro da DMZ, em intervalos de tempo definidos. Então, um cliente com acesso à VPN do IME poderá requisitar acesso a esse *log*. Essa operação é pode ser resumida nas seguintes etapas:

- Criação do *log* na estação de gerenciamento;
- Envio do *log* para a DMZ;
- Armazenamento do *log* no servidor de banco de dados na DMZ;
- Um cliente solicita o *log* através da VPN do IME; e
- O servidor de banco de dados envia o *log* para o cliente.

6. CONCLUSÃO

Este trabalho apresentou uma abordagem para avaliar a segurança da rede em IACS e propor soluções.

Neste estudo de caso, foi proposta uma arquitetura para a rede da planta MecatrIME. Analisou-se a sua rede local, através da captura de pacotes com a ferramenta *wireshark*. Isso permitiu o mapeamento dos protocolos encontrados, sua organização segundo o modelo de referência TCP/IP e sua análise a fim de avaliar a segurança da rede.

Dois casos foram analisados: um com a linha de produção parada e um caso de requisição da estação de gerenciamento para a estação do torno, como exemplo dos processos da linha de produção.

Foram encontrados muitos pacotes utilizando o protocolo SMB2, o que indica seu destaque no funcionamento da rede. Na análise do protocolo ARP conclui-se que quase um terço das mensagens visam garantir que todas as máquinas consigam se corresponder com a estação de gerenciamento. Além disso, identificou-se tanto a utilização de protocolos TCP, quanto UDP nas versões 4 e 6 do protocolo IP.

Então, foi elaborada uma proposta para uma arquitetura que permitirá conectar a planta à Internet, de modo seguro, baseada na criação de uma zona desmilitarizada e de um sistema de detecção de intrusão. Essa solução contribuirá também para o monitoramento remoto da planta de forma segura.

Além disso, pode-se utilizar a DMZ para a atualização de *softwares* instalados nas estações na planta, ao invés de expô-las diretamente à Internet, como é feito atualmente. Para isso, o *firewall* deverá ser liberado temporariamente para conectá-las a um *proxy* configurado na DMZ, com as atualizações mais recentes do sistema da planta. A segurança dessas atualizações deverá ser checada.

Como trabalhos futuros estão o aprofundamento e implementação da solução elaborada. Sugere-se para outros pesquisadores a utilização dessa metodologia de análise em sistemas mais complexos.

REFERÊNCIAS

Akbanov, M., Vassilakis, V., and Moscholios, I. (2018). Static and dynamic analysis of wannacry ransomware.

Andrade, A., Becker, L., Quintino, L., and Dias, J. (2018). CritÉrios de seguranÇa para sistemas scada em rede corporativa. doi:10.20906/CPS/CBA2018-0528.

Banerjee, U., Ashutosh, V., and Mukul, S. (2010). Evaluation of the capabilities of wireshark as a tool for intrusion detection. *International Journal of Computer Applications*, 6. doi:10.5120/1092-1427.

Carvalho, R.S. and Santos, A. (2015). Honeypots e sua importância na defesa cibernética das infraestruturas críticas do setor elétrico. *EletroEvolução - Sistemas de Potência*, 81, 30–35.

Couto, C., Couto, G.C.K., and Cunha, A.E.C. (2020). Modelagem da segurança da informação em sistemas de automação e controle industriais: estudo de caso com a planta mecatrime. In *VIII Simpósio Brasileiro de Sistemas Elétricos*.

Eckhart, M. and Ekelhart, A. (2018). Towards security-aware virtual environments for digital twins. 61–72. doi: 10.1145/3198458.3198464.

Garcia, F., Gans, G., Muijrers, R., van Rossum, P., Verdult, R., Schreur, R., and Jacobs, B. (2008). Dismantling mifare classic. volume 5283, 97–114. doi:10.1007/978-3-540-88313-5_7.

Iii, G. (2016). Towards an in-depth understanding of deep packet inspection using a suite of industrial control systems protocol packets.

IntelitekInc. (2019). *OpenCIM 5 User Manual*.

Iqbal, H. and Naaz, S. (2019). Wireshark as a tool for detection of various lan attacks. *International Journal of Computer Sciences and Engineering*, 7, 833–837. doi: 10.26438/ijcse/v7i5.833837.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9, 49–51. doi:10.1109/MSP.2011.67.

McDonald, M.J., Conrad, G.N., Service, T.C., and Cassidy, R.H. (2008). Cyber effects analysis using vcse promoting control system reliability.

Mitchell, R. and Chen, I.R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Comput. Surv.*, 46(4). doi:10.1145/2542049. URL `https://doi.org/10.1145/2542049`.

Popkova, E.G., Ragulina, Y.V., and Bogoviz, A.V. (2018). *Industry 4.0: Industrial Revolution of the 21st Century*. Studies in Systems, Decision and Control. Springer International Publishing. URL `https://books.google.com.br/books?id=Q\_xlDwAAQBAJ`.

Pramod, T. and Sunitha, N.R. (2018). *SCADA: Analysis of Attacks on Communication Protocols*, 219–234. doi: 10.1007/978-3-319-75683-7_17.

Stouffer, K., Falco, J., and Scarfone, K. (2015). Guide to industrial control systems (ics) security. Technical report.

Tanenbaum, A.S. and Wetherall, D.J. (2010). *Computer networks*, volume 13. pearson, 5 edition. 25-05-2020.

Young, S. (2003). Designing a dmz.

Zhu, B., Joseph, A.D., and Sastry, S. (2011). A taxonomy of cyber attacks on scada systems. In *iThings/CPSCom*, 380–388. IEEE Computer Society. URL `http://dblp.uni-trier.de/db/conf/ithings/ithings2011.html#ZhuJS11`.