Vulnerabilidades de Segurança Cibernética em Dispositivos de Medição Avançada de Energia Elétrica

Bruno M. Santos[1], Wesley H. Leite[2], Raphael C. S. Machado[1,3]

[1] Instituto de Computação Universidade Federal Fluminense (UFF),
[2] Departamento de Graduação, Faculdade Vincit
Niterói, RJ, Brasil

brunomacena@id.uff.br, wesley.leite@csflabs.seg.br, raphaelmachado@ic.uff.br

Abstract. *In this work, we assess the safety of Advanced Metering Devices for electric energy, critical elements in Advanced Metering Infrastructures (AMI). These devices, essential in energy distribution networks, record and transmit energy consumption data. We analyzed commercially available devices, addressing aspects from architectural to software security and their configurations. The vulnerabilities identified were classified according to the taxonomy of the Common Weakness Enumeration (CWE) and measured based on the methodology of the Common Vulnerability Scoring System (CVSS) 3.1. The analyses revealed high risks, especially in access and identity management.*

Resumo. *No presente trabalho investigamos como falhas de segurança cibernética em Dispositivos de Medição Avançada de energia elétrica introduzem riscos críticos em Infraestruturas de Medição Avançada. Avaliamos dispositivos disponíveis comercialmente, abordando desde aspectos arquiteturais até a segurança de software e suas configurações. Classificamos as vulnerabilidades identificadas conforme a taxonomia do Common Weakness Enumeration e propomos um critério de pontuação de risco com base na metodologia Common Vulnerability Scoring System. As análises revelaram que as mais relevantes vulnerabilidades identificadas seguem um padrão compatível com a lista OWASP IoT Top Ten.*

1. Introdução

Dispositivos de Medição Avançada de energia elétrica são componentes essenciais nas redes de distribuição, não apenas registrando e transmitindo dados de consumo energético, mas também servindo como interface para a interação com o consumidor final. Tais dispositivos desempenham um papel crucial no sucesso dos modernos processos de distribuição de energia elétrica e nas Smart Grids, incluindo a integração da geração distribuída de energia, tarifação dinâmica e monitoramento e gestão da demanda de energia. Alguns dispositivos de medição, ao permitirem a comunicação bidirecional entre o medidor e a concessionária, habilitam funções como o corte e a religação do fornecimento de energia para as unidades consumidoras. Sendo assim, são denominados de Medidores Inteligentes e servem como portas de entrada para as Infraestruturas de Medição Avançada (AMI), que são sistemas de informação fundamentais na gestão de recursos e constituem uma parte crítica das redes de distribuição.

As considerações de segurança cibernética para esses dispositivos e AMIs representam um desafio significativo, pois ataques cibernéticos originados a partir desses dispositivos têm o potencial de impactar serviços críticos para o bem-estar da sociedade. Eventos

históricos, como o ataque à infraestrutura elétrica da Ucrânia em 2015, evidenciam a realidade das ameaças cibernéticas às infraestruturas críticas, sublinhando a necessidade de reforçar a segurança cibernética em toda a infraestrutura energética para prevenir impactos significativos nos serviços essenciais à sociedade.

O objetivo deste trabalho é contribuir para a compreensão das fragilidades inerentes, identificando e classificando as vulnerabilidades cibernéticas presentes em dispositivos de medição avançada e na AMI, e avaliando a magnitude dos potenciais riscos à segurança da rede de distribuição de energia elétrica. Os resultados deste trabalho foram baseados em uma amostra selecionada de dispositivos de diferentes fabricantes e modelos, juntamente com suas plataformas de medição avançada. Embora esta amostra pareça limitada, ela abrange uma parte significativa da base instalada e em operação no território nacional. Esta constatação ressalta a importância da contribuição deste trabalho, evidenciando a necessidade de implementar medidas para reforçar a segurança das plataformas de medição avançada.

2. TRABALHOS RELACIONADOS

As contribuições anteriores sobre segurança em Medidores Inteligentes de energia elétrica e Infraestruturas de Medição Avançada foram cruciais para compreender o contexto e os desafios associados ao tema. Artigos como o de Ghosal e Conti [GHOSAL et al., 2019] destacam a relevância das técnicas de gerenciamento e segurança de chaves (Key Management System - KMS) para proteger a segurança cibernética das Infraestruturas de Medição Avançada (AMI). Sun, Cardenas, Hahn e Liu [Sun et al., 2020] abordam sistemas de Detecção de Intrusão para proteger a segurança dos Medidores Inteligentes. Foreman e Gurugubelli [FOREMAN et al., 2016] analisam a superfície de ataque cibernético em AMI. J. Chinnow, Bsufka, Schmidt, Bye, Camtepe e Albayrak [CHINNOW et al., 2011] apresentam um framework de simulação para avaliação de segurança nessas plataformas. Além disso, outros trabalhos, como os de Yi, Zhu, Zhang, Wu e Li [YI et al., 2014]; Tweneboah-Koduah, Tsetse, Azasoo e Endicott-Popovsky [TWENEBUAH-KODUAH et al., 2018]; e Khattak, Khanji e Khan [KHATTAK et al., 2019], abordam temas como ataques de Negação de Serviços (DoS) em AMI.

Nosso trabalho reconhece a importância dessas contribuições e avança adotando uma abordagem prática para analisar as ameaças e riscos em segurança cibernética, identificados em um contexto que reflete o estado atual da indústria. Além disso, consideramos essas contribuições ao longo do trabalho em cada uma das dimensões discutidas. Para isso, apoiamo-nos na analogia referencial de segurança cibernética da Internet das Coisas (IoT), utilizamos o Common Weakness Enumeration (CWE) para a taxonomia das vulnerabilidades identificadas e o Common Vulnerability Scoring System (CVSS) 3.1 para a pontuação de severidade. Trata-se de uma abordagem pragmática e sistemática para contribuir com a análise das ameaças cibernéticas neste contexto.

3. METODOLOGIA

Conduzimos testes de intrusão (pentest) em dispositivos de medição avançada e na infraestrutura relacionada de AMI, que inclui redes de comunicação e plataformas de software. Selecionamos seis dispositivos de medição e estabelecemos um ambiente de laboratório que replica as condições normais de operação, incluindo não apenas os próprios dispositivos de medição, mas também toda a infraestrutura de comunicação e a

camada de software necessária para sua operação. Cada dispositivo de medição foi configurado de acordo com suas especificações. Configuramos uma rede de comunicação com a topologia e os protocolos necessários para simular as condições operacionais reais.

O procedimento de teste seguiu um roteiro estruturado que incluiu planejamento, definição do escopo e objetivos. Iniciamos com uma análise detalhada dos softwares embarcados, acessando binários e manuais técnicos. As etapas de teste envolveram reconhecimento para compreender a arquitetura, as funcionalidades e os potenciais pontos de vulnerabilidade dos dispositivos. Em seguida, realizamos a varredura e a identificação de vulnerabilidades e falhas de segurança, explorando-as através de simulações de ambientes e monitoramento de tráfego. Adicionalmente, aplicamos técnicas de depuração para uma análise profunda e realizamos testes com a desativação de controles de segurança para avaliar seu impacto.

4. RESULTADOS

Constatamos que todos os medidores apresentam pelo menos uma vulnerabilidade considerada de alta severidade, com destaque para falhas no controle de acesso, conforme apresentado na Tabela 1. Também foram identificadas fragilidades relacionadas às interfaces usadas para configurar e administrar os dispositivos de medição.

A maioria dos impactos estava relacionada ao comprometimento da integridade dos dados de medição, o que poderia levar a manipulações e resultar em cobranças incorretas de consumo de energia.

Vulnerabilidades			Severidade	Medidor-001	Medidor-002	Medidor-003	Medidor-004	Medidor-005	Medidor-006
Categorização / Escopo	Controle de Acesso	CWE-521 CWE-1391	Médio	5.3					
		CWE-639	Alta	7.5	7.5	8.1			
		CWE-693			7.1		7.1		
		CWE-259						7.3	
		CWE-522		7.5	7.5			8.8	
	Outros	CWE-79							7.1

Tabela 1 - Tabulação das Vulnerabilidades

A exploração das vulnerabilidades exigia baixa complexidade e privilégios, aumentando a probabilidade de ocorrência de eventos cibernéticos relacionados.

4.1. Senhas e Credenciais Frágeis

Identificamos no 'Medidor-001' uma vulnerabilidade relacionada ao uso de senhas e credenciais fracas. Essa falha surgiu durante a ativação e configuração do medidor, realizada pelo operador responsável pela disponibilização do dispositivo, seguindo os procedimentos padrão para operação. A senha padrão foi mantida na configuração do dispositivo, mostrando-se insuficientemente segura devido à falta de conscientização sobre segurança por parte do operador e às limitações do sistema, que não exigem senhas robustas. Essas fragilidades são categorizadas como CWE-521 'Requisitos de Senhas Fracas' e CWE-1391 'Uso de Credenciais Fracas' [MITRE, 2022], e ocupam o primeiro lugar na lista do projeto TOP10 do OWASP Internet of Things [OWASP, 2018]. Essa ocorrência foi pontuada como de média severidade [AV:N, AC:L, PR:N, UI:N, S:U / C:L, I:N, A:N; CVSS Score 5.3], conforme representado na Tabela 2 abaixo.

Métricas de Explorabilidade		**Métricas de Impacto**	
Vetor de Ataque (AV):	Network/Rede (N)	**Impacto na Confidencialidade (C):**	Low/Baixo (L)
Complexidade do Ataque (AC):	Low/Baixo (L)	**Impacto na Integridade (I):**	None/Nenhum (N)
Privilégios Necessários (PR):	None/Nenhum (N)	**Impacto na Disponibilidade (A):**	None/Nenhum (N)
Interação do Usuário (UI):	None/Nenhum (N)		
Escopo (S):	Unchanged/Inalterado (U)		**CVSS Score:** 5.3

Tabela 2 - CVSS Score para ocorrência de requisitos fracos de senha

Durante os testes, ao analisar a rede sem fio, identificamos um padrão no Service Set Identifier (SSID) que faz referência ao número serial do medidor, frequentemente visível no painel frontal do equipamento, facilitando a identificação do alvo de nosso teste. Testes de autenticação revelaram uma vulnerabilidade na segurança das senhas, pois a autenticação bem-sucedida foi alcançada através de métodos como força bruta, utilizando uma sequência numérica de 8 dígitos..

4.2. Acesso não autorizado

Em nossos testes, investigamos a vulnerabilidade relacionada à evasão de autorização, conforme descrito no CWE-639, inicialmente identificada nos dispositivos 'Medidor-001' e 'Medidor-002'. Essa fragilidade estava presente em seus mecanismos de acesso sem fio. A mesma categoria de vulnerabilidade também foi encontrada no 'Medidor-003', por meio de um mecanismo diferente, que será apresentada na próxima seção. Essa vulnerabilidade é destacada como a segunda na lista do projeto TOP10 do OWASP Internet of Things. Agentes mal-intencionados podem explorá-la para obter acesso não autorizado aos dispositivos. Essa ocorrência foi classificada como de alta severidade, [AV:N, AC:L, PR:N, UI:N, S:U / C:H, I:N, A:N; CVSS Score 7.5].

Em cenários práticos, essa vulnerabilidade se manifesta quando um dispositivo permite que agentes mal-intencionados influenciem ou controlem as chaves de autenticação. No caso desses dispositivos, a autenticação é baseada em tokens facilmente interceptáveis, o que possibilita que atacantes ganhem acesso à plataforma.

Nos testes realizados, utilizamos engenharia reversa e monitoramento de tráfego para identificar falhas nos mecanismos de autenticação. A análise do processo de geração de senhas nos permitiu replicar e explorar esses mecanismos. O procedimento técnico envolveu a identificação do SSID e da área do código do aplicativo móvel responsável pela geração de senhas, utilizando ferramentas como DEX2JAR para converter o APK. A análise incluiu a identificação do endereço de rede, portas de conexão e uma função de envio de dados. Após a análise, desenvolvemos um código capaz de gerar senhas para ativar o acesso aos dispositivos. Esse processo depende do uso de um aplicativo que inicia a geração de senha com base no código serial do medidor, visível em uma função para gerar a senha do medidor pelo aplicativo móvel. O código desenvolvido replicou esse mecanismo, permitindo a geração de novas senhas para acesso mal-intencionado.

4.3. Escalada de privilégios

Nesta nova sessão de testes, identificamos a vulnerabilidade de evasão de autorização, classificada como CWE-639, também no dispositivo 'Medidor-003'. No entanto, neste caso, ela está associada à evasão de autorização nos controles de acesso do aplicativo móvel utilizado para interagir com o dispositivo de medição. Essa vulnerabilidade é listada como a terceira principal no TOP10 do OWASP Internet of Things 2018. Essa ocorrência foi avaliada como de alta severidade, considerando as métricas de explorabilidade e impacto obtidas nos testes. [AV:N, AC:L, PR:L, UI:N, S:U / C:H, I:H, A:N; CVSS Score 8.1].

A falha reside na validação dos 'roles' para a transmissão de dados, ocorrendo quando o aplicativo interage com sua API no Centro de Processamento de Dados, expondo parâmetros de acesso. Ao manipular esses parâmetros, conseguimos obter privilégios administrativos, o que possibilitou a reprogramação do medidor. A API

vulnerável foi identificada com o auxílio das ferramentas ADB e Frida. Tal falha expôs todos os 'roles' da plataforma, permitindo identificar aqueles com os maiores privilégios.

4.4. Falha no mecanismo de proteção

A vulnerabilidade observada, relacionada à falha nos mecanismos de proteção dos medidores 'Medidor-002' e 'Medidor-004', representa um risco significativo de subversão dos dados de medição. Essa falha permite que os atacantes manipulem os dados de leitura, utilizando técnicas como man-in-the-middle. Essa vulnerabilidade é mais adequadamente descrita pelo CWE-693 e foi destacada como a sétima na lista TOP10 do OWASP Internet of Things. Pontuamos essa falha como de alta severidade. [AV:N, AC:H, PR:L, UI:R, S:U / C:H, I:H, A:H; CVSS Score 7.1]

Em nossos testes, concentramos nossa análise no mecanismo de acesso e troca de informações entre o aplicativo de medição e o dispositivo medidor. Detectamos tentativas de ofuscação no código, incluindo chamadas para classes e métodos. Desde a definição do socket até a instância da classe, examinamos detalhes da comunicação. O processo de coleta começa com uma função de leitura. Analisamos o padrão de fluxo de dados em ASCII, semelhante ao encode base64, utilizando as ferramentas Wireshark e Frida. Apesar da conversão em base64, identificamos outra camada de codificação. No código-fonte, encontramos uma referência a uma classe de manipulação de trechos criptografados com AES. No entanto, não é necessário decifrar para criar um pacote de replay. Para simular o ataque, implementamos um medidor falso utilizando um arquivo TXT com o payload. A transmissão resultou em leituras idênticas, evidenciando um ataque de replay, onde o agente malicioso intercepta, armazena e retransmite os dados.

4.5. Uso de credenciais hard-coded

A vulnerabilidade identificada relacionada ao uso de credenciais hard-coded é mais apropriadamente descrita pela categorização do CWE-798 neste contexto. O cenário em questão envolve o aplicativo móvel utilizado para o 'Medidor-005'. Essa vulnerabilidade é destacada como a principal na lista TOP10 do OWASP Internet of Things 2018, sob a categoria 'Senhas Fracas, Previsíveis ou Hard-coded'. O dispositivo medidor em questão também possui capacidade de conectividade sem fio por rádio frequência. O aplicativo responsável por realizar esse acesso é instalado em um smartphone. Identificamos que o aplicativo móvel continha credenciais hard-coded, usadas para o primeiro acesso do medidor ao Centro de Processamento de Dados da AMI. Uma vez que a autenticação é bem-sucedida, um novo token é emitido para permitir a transmissão posterior dos dados de medição pelo dispositivo. Essa ocorrência foi classificada como de alta severidade. [AV:L, AC:L, PR:L, UI:N, S:U / C:H, I:H, A:L; CVSS Score 7.3]

Credenciais codificadas no APK apresentam riscos de segurança significativos. Os atacantes podem acessar o APK, extrair e utilizar essas credenciais codificadas para acessar o sistema, manipular dados de medição e comprometer a segurança do Centro de Processamento de Dados da AMI. Além disso, os atacantes podem imitar dispositivos legítimos e enviar medições forjadas, comprometendo a integridade do sistema.

4.6. Credenciais insuficientemente protegidas

Durante os testes, identificamos a vulnerabilidade de proteção insuficiente de credenciais em sistemas de medição, mais adequadamente descrita pelo CWE-522 neste contexto.

Esta vulnerabilidade é listada como a terceira na lista TOP10 do OWASP Internet of Things (OWASP, 2018), sob o título 'Interfaces Inseguras nos Ecossistemas'. O 'Medidor-005' mostrou-se suscetível a interceptações e recuperações indevidas de credenciais, transmitidas e armazenadas de forma insegura. Observamos uma vulnerabilidade em um APK usado para interação com o medidor. Essa ocorrência foi classificada como de alta severidade. [AV:N, AC:L, PR:L, UI:N, S:U / C:H, I:H, A:H; CVSS Score 8.8]

Ao analisar o fluxo de dados através de um endpoint do sistema utilizando as ferramentas ADB, FRIDA e Burp Suite, constatou-se a possibilidade de interceptar esses dados, incluindo credenciais, transmitidos em texto claro. As senhas dos medidores não estão apenas vulneráveis durante o fluxo de dados entre o aplicativo e a API; após a requisição do endpoint, essas senhas são armazenadas em uma tabela do sistema de gestão de arquivos SQL, mantido em um diretório no armazenamento local do dispositivo.

Assim, foi possível acessar este arquivo e expor dados sensíveis tratados por esta camada de software do Centro de Processamento de Dados da AMI, incluindo senhas de diversos dispositivos cadastrados na plataforma. Essas senhas possibilitam a reprogramação dos medidores e o acesso não autorizado. O uso inadequado desses dados pode resultar na indisponibilidade e no comprometimento das medições.

4.7. Ausência de higienização adequada de dados de entrada

A vulnerabilidade relacionada à inadequada neutralização de entradas em páginas web, que permite ataques de Cross-Site Scripting (XSS), é categorizada, no contexto deste trabalho, pelo CWE-79. Esta ameaça é amplamente reconhecida, ocupando a posição A03 na lista OWASP TOP 10 2021. Além disso, corresponde à terceira maior preocupação no projeto OWASP TOP 10 Internet of Things 2021. O XSS-Store, vulnerabilidade explorada em nossos testes, permite que o atacante injete código malicioso, resultando na execução de ações não autorizadas. Essa vulnerabilidade foi classificada como de alta severidade. [AV:N, AC:H, PR:L, UI:R, S:U / C:H, I:H, A:H; CVSS Score 7.1]

O laboratório montado para os testes baseou-se no uso do Ponto de Conexão do Cliente, onde a estação de teste compartilhava o mesmo meio de comunicação que o medidor analisado, replicando um cenário de operação normal. A análise com o suporte do Wireshark revelou que o equipamento de medição, identificado como 'Medidor-006', transmitia dados sem criptografia ao interagir com sua API no Centro de Processamento de Dados da AMI, tornando-os vulneráveis à interceptação e manipulação.

Após capturar e examinar o fluxo de dados na comunicação entre o medidor e o Centro de Processamento de Dados da AMI via Ponto de Conexão do Cliente, usamos um script para simular o comportamento do medidor e enviar dados falsos para o Centro de Processamento de Dados da AMI. Ao inserir uma string no protocolo, avaliamos o controle no sistema. Desenvolvemos um script, enviado para um socket usando o NETCAT e direcionado à API. A execução bem-sucedida do script resultou na localização do equipamento testado e na geração de mensagens inseridas de forma não autorizada no console. Identificamos a capacidade de enviar quantidades ilimitadas de dados (DoS), com potencial para causar indisponibilidade nos serviços da AMI.

5. Considerações Finais

A AMI enfrenta desafios significativos relacionados à segurança cibernética, decorrentes de sua natureza interconectada e arquitetura distribuída, que ampliam a superfície de

ataque - uma característica da Internet das Coisas (IoT) e diretamente associada aos dispositivos de medição avançada. Essa realidade aumenta a exposição aos riscos cibernéticos, tornando essencial a atenção à segurança desde o desenvolvimento até a operação da AMI. Assim, as fragilidades identificadas neste trabalho refletem as preocupações do projeto OWASP Internet of Things.

As ocorrências das vulnerabilidades, majoritariamente pontuadas como de alta severidade, estão ligadas a falhas na gestão de acesso e identidade (IAM) e a fragilidades em interfaces para configuração e gerenciamento dos dispositivos de medição. Abordagens viáveis de mitigação para as vulnerabilidades identificadas foram apresentadas por trabalhos anteriores citados neste artigo, incluindo mecanismos de criptografia forte nas comunicações, autenticação e proteção de dados, como RSA e funções físicas inalcançáveis (PUF), uso de mecanismos de gerenciamento de chaves, sistemas de Detecção de Intrusão, além de revisões e auditorias regulares de segurança.

Este trabalho lança um alerta sobre a importância de desenvolver ações sistemáticas para reforçar a segurança cibernética de medidores inteligentes e indica um caminho para pesquisas futuras, que podem fornecer uma compreensão mais abrangente das vulnerabilidades inerentes a esses elementos críticos e portas de entrada da AMI.

Referências

GHOSAL, Amrita; CONTI, M. Key Management Systems for Smart Grid Advanced Metering Infrastructure, IEEE Communications Surveys & Tutorials,2019. Disponível em: \<https://doi.org/10.1109/COMST.2019.2907650\>. Acesso em: Set. 2023.

SUN, Chih-Che; et Al.. Intrusion Detection for Cybersecurity of Smart Meters. IEEE Transactions on Smart Grid, 2020. Disponível em: \<https://doi.org/10.1109/TSG.2020.3010230\>. Acesso em: 07 Set. 2023

FOREMAN, J. C.; GURUGUBELLI, D. Cyber attack surface analysis of advanced metering infrastructure. arXiv preprint arXiv:1607.04811, 2016. Disponível em: \<https://arxiv.org/abs/1607.04811\>. Acesso em: 29 outubro 2023.

CHINNOW, J.; BSUFKA, K.; SCHMIDT, A. D.; BYE, R.; CAMTEPE, A.; ALBAYRAK, S. A simulation framework for smart meter security evaluation. , SMFG, 2011. Disponível em: \<https://doi.org/10.1109/SMFG.2011.6125758\>. Acesso em: 29 Out. 2023.

YI, P.; ZHU, T.; ZHANG, Q.; WU, Y.; LI, J. A denial-of-service attack in advanced metering infrastructure network. ICC, 2014. Disponível em: \<https://doi.org/10.1109/ICC.2014.6883456\>. Acesso em: 29 Out. 2023.

TWENEBOAH-KODUAH, S.; TSETSE, A.K.; AZASOO, J.; ENDICOTT-POPOVSKY, B. Evaluation of Cybersecurity Threats on Smart Metering System. In: Latifi, S. (eds) Information Technology, vol 558. Springer, Cham. Disponível em: \<https://doi.org/10.1007/978-3-319-54978-1_28\> . Acesso em: 29 Out. 2023.

KHATTAK, A. M.; KHANJI, S. I.; KHAN, W. A. Smart meter security: Vulnerabilities, threat impacts, and countermeasures. IMCOM, 2019. Disponível em: \<https://link.springer.com/chapter/10.1007/978-3-030-19063-7\>. Acesso em: 29 Out. 2023.