Gestão de Identidades em Redes de Automação de Subestações

Yona Lopes[1], **Natalia Castro Fernandes**[1], **Débora C. Muchaluat Saade**[1]

[1]Universidade Federal Fluminense (UFF) – Niterói – RJ – Brazil *

Resumo. *Este trabalho discute a segurança e gestão de identidade em redes de comunicação em subestações elétricas. Apesar de ser um tema de grande criticidade, ele foi negligenciado durante um longo período, resultando em ataques recentes de grande severidade. Trata-se de um tema complexo com várias oportunidades para pesquisa, pois explora característica de um sistema que foi concebido isolado e que agora converge com a tecnologia da informação.*

1. Introdução

Os ambientes de subestações têm passado por uma forte evolução. Inicialmente a comunicação era feita de forma serial, com protocolos proprietários e apenas para controle e supervisão. Com a evolução e modernização deste ambiente, a comunicação serial foi substituída por redes de comunicação baseadas em Ethernet aumentando a eficiência e amplitude da comunicação em subestações. Tal modificação traz amplas possibilidades de inovação, permitindo a sofisticação de sistemas de monitoração e controle (como o SCADA (*Supervisory Control and Data Acquisition*)), para análise em tempo real, sendo possível o uso de grandes quantidades de dados para suas análises e otimização. As funções críticas realizadas através de cabo rígido, como abertura de disjuntores, ganharam a opção de serem realizadas via rede de comunicação, permitindo também a sofisticação de sistemas de proteção e controle.

No entanto, em um sistema de automação de subestações não existe margem para erros. Um erro – ou um ataque – pode danificar equipamentos críticos e até mesmo colocar a vida de trabalhadores em risco. Existe, inclusive, risco de explosão. Os protocolos industriais foram concebidos quando a segurança não era uma grande preocupação industrial, já que os ambientes eram isolados. Como consequência, mecanismos de segurança não faziam parte dos sistemas e protocolos industriais. Com isso, apesar da criticidade, padrões e iniciativas para avanço da segurança desses ambientes são recentes.

Outro ponto de atenção é que esses ambientes têm passado por uma forte convergência da *Information Technology* (IT) e *Operational Technology* (OT), com redes de controle conectadas à infraestrutura de comunicação corporativa das empresas e da Internet. Esta convergência, muitas vezes é justificada pela redução de custos e a absorção das funcionalidades de IT, como interoperabilidade e acesso remoto. Contudo, devido a essa convergência e evolução, os sistemas de automação de subestações têm se tornado alvo de ataques cibernéticos. A DRAGOS, empresa focada em segurança cibernética no setor elétrico, fez um relatório[1] sobre ataques e vulnerabilidades ressaltando a preocupação relacionada à segurança de rede destes sistemas. O relatório mostrou, dentre outros dados, que um dos últimos ataques levantados – subestação na Ucrânia – foi realizado explorando vulnerabilidades básicas. Enquanto os ataques mais antigos, como o Stuxnet 2010,

*As autoras agradecem ao apoio financeiro da CAPES, INERGE, FAPESP, FAPERJ, e TAESA.

[1]https://dragos.com/wp-content/uploads/CrashOverride-01.pdf

supostamente usavam pen drives USB maliciosos para entrar na rede, os ataques mais modernos, como os ataques de 2015 e 2016 na rede elétrica da Ucrânia ou o ataque de 2017 da planta petroquímica da Arábia Saudita, supostamente utilizam técnicas de acesso e propagação bastante semelhantes às vistas em redes corporativas. Isso mostra uma relação maior entre conectividade e aumento de ataques a subestações.

2. Gestão de Identidade em Redes de Automação de Subestações

A gestão de identidade pode ser definida como métodos que fornecem um nível adequado de segurança para os recursos de uma organização através de políticas impostas aos usuários, focando nos requisitos de autenticação, autorização e auditoria [Almulla and Chan Yeob Yeun 2010]. Nos ambientes de subestação, o processo de autenticação deve identificar também, além de usuários, os dispositivos da rede de comunicação da subestação.

O padrão IEC 62351 [IEC62351 2018] foi desenvolvido pelo Comitê Técnico 57 da IEC, a fim de fornecer os requisitos de segurança em redes de automação de energia. Ele emprega métodos de segurança a fim de preservar a integridade das mensagens com base em um esquema forte de gestão de identidade. Além disso, propõe o uso de *Role-Based Access Control* (RBAC). Os objetivos do padrão também incluem integridade, confidencialidade, prevenção de falsificação, detecção de intrusão, autenticação por meio de certificados digitais, e assim por diante. O conjunto de padrões NERC CIP (*North American Electric Reliability Corporation Critical Infrastructure Protection*)[2] visa garantir a segurança geral dos sistemas que gerenciam diretamente as redes de energia. Para cobrir as diretrizes gerais, possui nove padrões para impor a governança dos sistemas. Esses padrões incorporam os princípios básicos de identificação de ativos críticos, criando mecanismos de controle e segurança lógica e física desses sistemas para recuperação em caso de um incidente.

Neste sentido, a proposta de métodos de autenticação e integridade mais seguros para a comunicação, sem incorrer nos requisitos de alto poder de processamento ou elevados atrasos de comunicação é de especial importância nesse ambiente [Lopes et al. 2015]. Um dos maiores desafios é a inclusão de mecanismos de gestão de identidade em equipamentos utilizados em subestações. É importante ressaltar que os atuadores e sensores de subestação, mesmo que comuniquem via rede, apresentam desafios e considerações de segurança únicos. Portanto, a cooperação entre IT e OT é de suma importância para evolução dos ambientes de subestações. Esse trabalho vai discutir as principais vulnerabilidades de gestão de identidade deste cenário, apresentando seus aspectos, soluções atuais e apresentando as oportunidades de pesquisa e desenvolvimento nesta área.

Referências

Almulla, S. A. and Chan Yeob Yeun (2010). Cloud computing security management. In *International Conf. on Engineering System Management and Applications*, pages 1–7.

IEC62351 (2018). Power systems management and associated information exchange - data and communications security. Technical report, IEC.

Lopes, Y., Fernandes, N. C., Castro, T. B., and Muchaluat-Saade, V. S. F. D. C. (2015). Desafios de Segurança e Confiabilidade na Comunicação para Smart Grids. In *Minicursos do SBSeg*, pages 55–109. SBC.

[2]https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx