

Desafios da Segurança Cibernética Nas Subestações de Energia

Carlos Oliveira e Ricardo Abboud, *Schweitzer Engineering Laboratories, Inc.*

Resumo—O avanço da aplicação da norma IEC 61850 nos projetos de subestações, a presença de redes Ethernet na área de energia elétrica cresceu exponencialmente na última década. Contudo em termos de segurança cibernética, os projetos de subestações normalmente empregam apenas medidas perimetrais como roteadores e firewalls. Tais equipamentos não garantem totalmente a segurança da rede uma vez que estes podem ser configurados erroneamente e apresentam pouca, quando nenhuma, eficácia para detectar e impedir invasões originadas internamente. Um controle rigoroso de controle de acesso é necessário, porém tal abordagem requer uma metodologia dinâmica e integrada a um sistema de autenticação centralizado.

I. INTRODUÇÃO

Ao escutarmos a expressão “ameaça cibernética” é comum a relacionarmos à figura de um hacker, ou seja, um adolescente que domina sistemas computacionais com intuito de invadir sites e redes de grandes corporações por diversão. Porém esta não é mais uma realidade no mundo atual. As invasões atuais são arquitetadas por grupos organizados, geralmente patrocinados por governos ou empresas com o intuito de causar danos materiais, roubo de informações sigilosas ou até mesmo, ações terroristas.

Até o final da década de 90, os sistemas de automação de energia elétrica não compartilhavam da preocupação com tal ameaça. O cenário da automação de subestações nesta época era, em sua grande maioria, baseada em comunicações totalmente isoladas e normalmente utilizando canais seriais. Atualmente vivemos uma realidade totalmente diferente. Com o avanço da aplicação da norma IEC 61850, os sistemas de automação de subestações de energia elétrica estão cada vez mais interligados. A falta de formação técnica especializada aliada à farta informação disponível sobre os sistemas elétricos na Internet faz com que os profissionais desta área comecem a se preocupar cada vez mais com possíveis ameaças cibernéticas.

Em 2007, uma pesquisa realizada com diversas empresas em todo o mundo, apontou que no Brasil, aproximadamente 80% destas já haviam sido vítimas de pelo menos um ataque ao ano [1]. Em 2011, a empresa McAfee publicou um relatório intitulado de “*Global Energy Cyber Attacks: Night Dragon*” que alertava para diversas tentativas de ataques a empresas de energia elétrica, gás e óleo utilizando ferramentas de administração remota [2]. Mais recentemente, a McAfee conduziu um estudo por solicitação do Departamento de Energia (DOE) dos Estados Unidos que apontou uma tendência de crescimento destas ameaças [3]. Isto seria justificado pelo aumento da exposição, da interconexão e da complexidade das

redes de comunicação juntamente com o uso de tecnologias computacionais existentes e a necessidade emergente de cada vez mais automação dos processos.

II. ANÁLISE DE UM PROJETO: AMEAÇAS E RECOMENDAÇÕES

O conceito de segurança dentro de um projeto de subestação normalmente nos remete ao conceito de cercas, cadeados, CFTV, sistemas de alarme e vigias [4]. De certo modo esta associação não está errada. Em segurança cibernética existe o termo “defesa em profundidade”. Esta designação tem origem em uma técnica militar utilizada desde a antiguidade. A base principal é o emprego de várias camadas de defesa. Um castelo medieval é um bom exemplo, aonde para uma invasão, era necessário primeiro atravessar um fosso, no caso de sucesso, ainda existiam muralhas altas a se transpor e no topo dessas, soldados armados. Se estas barreiras fossem vencidas ainda existiam vários muros e portões até que a invasão alcançasse finalmente a sala do trono real. Abstraindo este conceito para o ambiente da tecnologia de informação, defesa em profundidade é o emprego de várias técnicas de proteção dispostas em múltiplas camadas. No caso de um projeto de subestação de energia elétrica, a camada mais interna de proteção seria justamente a segurança patrimonial ou física. Ver Fig. 1.

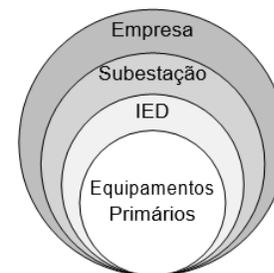


Fig. 1. Múltiplas camadas de proteção em um projeto de subestação

A Fig. 2 descreve um sistema de comunicação desde o controle e supervisão local de uma subestação até ao centro de controle remoto e engenharia de uma empresa. Esta é uma arquitetura fictícia, porém representa a realidade em vários projetos modernos de subestações utilizando a norma IEC 61850. Temos todos os IEDs conectados à rede Ethernet através de switches gerenciáveis.

Neste projeto podemos identificar vários níveis de proteção e seus principais focos de possíveis falhas de segurança. Eles estão assinalados com círculos numerados de 1 a 4 que serão abordados nos itens de 2.1 a 2.4 respectivamente.

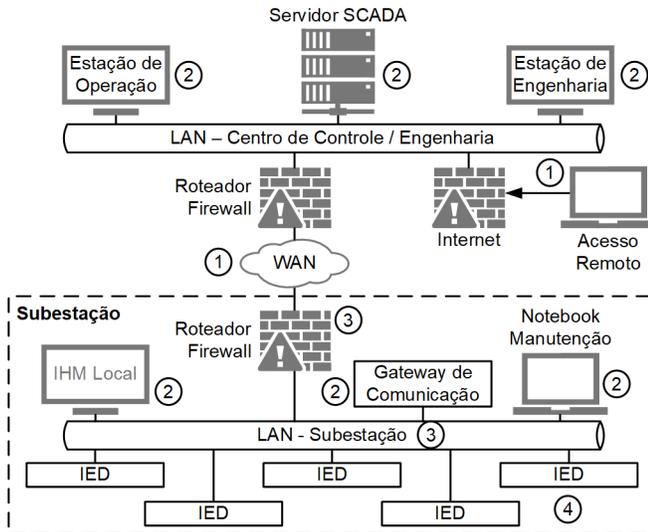


Fig. 2. Arquitetura exemplo de projeto de automação de subestação

A. Enlaces de Comunicação Externa

Os enlaces de comunicação externa são todos os canais disponíveis para entrada e saída de informações de uma subestação. Eles podem ser infraestruturas de comunicação pertencentes a própria empresa ou a provedoras de serviços de telecomunicações. Estes enlaces possuem uma exposição física e lógica sendo a porta de entrada de diversos ataques, alguns principais serão mostrados a seguir.

1) Invasões e Ataques

A proteção mais utilizada contra invasões de uma rede é o controle de acesso aos recursos e serviços da mesma. Para prover este controle de acesso é utilizado o firewall. Uma das origens do nome recorre ao meio automobilístico onde é usado como designação do isolamento utilizado para separar um possível incêndio no motor do compartimento dos passageiros [5]. A segurança do usuário do automóvel deve ser priorizada, porém alguns acessos nesta barreira de proteção devem ser abertos para integração do controles do carro, tais como, volante, acelerador, freio, etc. Assim é o firewall em uma rede Ethernet, ele deve bloquear todos os pacotes nocivos ao sistema e liberar somente os pacotes confiáveis à aplicação. Este controle é realizado através de regras programadas no firewall, baseadas no fluxo de entrada e saída da comunicação. A principal regra a configurar em um firewall empregado em uma subestação de energia elétrica é, por padrão, negar todos os pacotes. Em seguida serão adicionadas regras para cada serviço necessário de acordo com o projeto de automação.

2) Intercepções

Uma vez invadida uma rede de comunicação, é possível interceptar os pacotes de dados que trafegam nesta. O ataque denominado de “*Man-in-the-middle*”, como o próprio nome sugere, consiste no invasor alocado justamente dentro do fluxo de informações entre dois pontos. Por exemplo, em um sistema de automação de energia elétrica poderia ser entre um IED da subestação e uma estação de engenharia remota. A Fig. 3 mostra uma interceptação de pacotes e como informações importantes com a senha de acesso do IED são expostas neste caso.

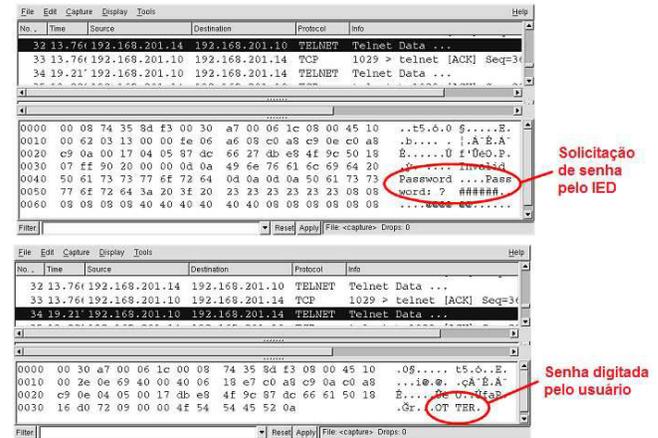


Fig. 3. Exemplo de interceptação de pacotes em um sistema de automação de energia elétrica

A descentralização das tarefas nas empresas e a necessidade de uma rápida resolução de problemas traz a necessidade do acesso de colaboradores aos recursos da rede mesmo quando estes estão fora das alocações físicas da empresa. O risco de interceptação neste tipo de acesso remoto é muito grande, já que é comum o uso da Internet para este fim devido à fácil implantação de uma solução baseada na comunicação através da mesma.

A principal medida preventiva contra a interceptação de informações em uma linha de comunicação é a criptografia de dados. Criptografia é uma palavra de origem grega para “escrita escondida”. Sua ideia principal é codificar uma mensagem utilizando regras ou símbolos que somente serão conhecidos pelo transmissor e pelo receptor como ilustrado na Fig. 4. Na área da tecnologia da informação, estas regras ou símbolos são chamadas de “chave”.

Em um projeto moderno de automação de subestação é aconselhável o uso de VPN (*Virtual Private Network*) em todos os acessos remotos à rede. VPN é utilizada para prover uma extensão de uma rede local para outros pontos de acesso de maneira segura mesmo utilizando meios como a Internet para realizar tal conexão. Existem dois tipos de VPN: *Security* e *Trusted*. A VPN do tipo *Security* se utiliza de técnicas de criptografia para criar um canal de comunicação blindado. Esta técnica é chamada de “tunelamento” e normalmente emprega protocolos seguros de rede como o IPsec (*Internet Protocol Security*). Este protocolo é derivado do IP (*Internet Protocol*), largamente utilizado nas redes Ethernet, porém pode embaralhar as informações contidas em seu pacote. A VPN do tipo Confiável não possui a funcionalidade de criptografia incorporada, mas estabelece que a rota de comunicação é conhecida e controlada.

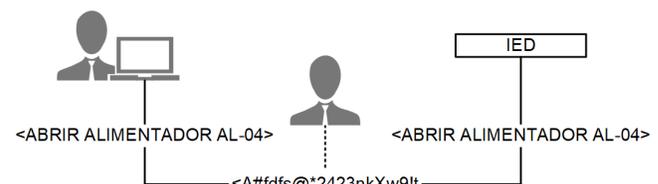


Fig. 4. O invasor não possui a chave de decodificação, logo não consegue interpretar ou modificar de maneira válida o comando enviado pelo operador do sistema

B. Plataformas Computacionais

Computadores sempre foram utilizados dentro dos centros de controle de subestações em ambientes climatizados, livres de interferências eletromagnéticas ou surtos elétricos. Com a popularização destes equipamentos, seu custo tornou-se cada vez mais baixo propiciando o desenvolvimento de computadores mais robustos que poderiam ser aplicados nos mesmos ambientes agressivos a que os IEDs eram expostos nas subestações.

Atualmente, os projetos de automação de subestações consideram o uso de computadores nos diversos níveis da aplicação. A flexibilidade de desenvolvimento e compartilhamento de funções em plataformas computacionais são indubitavelmente as grandes vantagens da utilização das mesmas, porém estas facilidades baseiam-se em sistemas operacionais de mercado, devido a isto, as mesmas ameaças que convivemos operando computadores pessoais no ambiente corporativo ou doméstico, são passíveis nestas plataformas computacionais, descritas a seguir, mas não limitadas a estas.

1) Vírus

Em um sistema de automação de subestação as principais preocupações em se utilizar softwares antivírus residem basicamente em:

- Impacto no desempenho da plataforma computacional diante de funções críticas de controle da subestação. Imagine se uma rotina de autoexame a procura de vírus é inicializada no momento de uma manobra de um circuito impedindo que o operador a concretize;
- Não existem informações largamente disseminadas sobre a utilização de softwares antivírus em sistemas dedicados de automação. As empresas desenvolvedoras de software antivírus possuem seu foco em usuários domésticos e corporativos;
- Dificuldade de atualização constante do software em computadores alocados dispersamente nas subestações.

A publicação especial do NIST de número 1508 [6] apresenta algumas orientações sobre o uso deste tipo de softwares no ambiente de automação de processos. Algumas conclusões interessantes neste estudo que podem ser abstraídas para a automação de subestações são:

- O exame para verificação de vírus sob demanda, ou seja, disparado pelo usuário, tem o maior impacto sobre o desempenho das tarefas de automação muitas vezes ocupando 100% dos recursos disponíveis de processamento;
- Por outro lado, o exame para verificação de vírus de tempo-real tem pouco ou nenhum impacto;
- É possível utilizar softwares antivírus de mercado em plataformas computacionais de automação desde que as parametrizações sejam feitas com um foco diferente do comumente utilizado na área de TI.

2) Dispositivos Móveis de Memória USB

Dispositivos de memória USB são largamente utilizadas em todos os níveis de um sistema de automação de subestações. Genericamente chamadas de Pendrive ou Flashdrive, estes dispositivos são empregados para troca de arquivos entre

plataformas computacionais, atualização de softwares, etc. Porém são grandes responsáveis pela propagação dos vírus [7]. Outra ameaça relacionada é o vazamento de informações confidenciais por parte de colaboradores mal-intencionados ou no caso de perda ou roubo destas memórias.

É muito importante no projeto de um sistema de automação de subestações de energia elétrica a adoção de restrições ao uso destes dispositivos. Algumas ações preventivas são o bloqueio de uso das interfaces USB nas plataformas computacionais responsáveis pelas tarefas de tempo-real do sistema e adoção de políticas de uso de Pendrives. Quando o uso destes dispositivos é indispensável, empregar Pendrives dotadas de criptografia, antivírus embarcados e sistemas de proteção por senha dos dados gravados.

3) Vulnerabilidades Instantâneas

Os softwares antivírus baseiam suas defesas em sintomas e trechos de programação dos vírus conhecidos até o momento e registrados em uma base de dados interna. Seu comportamento pode ser comparado com uma lista-negra (*blacklist*). Se a solicitação de um determinado aplicativo possui características similares as presentes nesta lista, é julgada como possível ameaça. Porém em alguns casos os vírus podem sofrer mutações, ou seja, adotar outro modo de operação desconhecido pelo software antivírus e conseguir se inocular no sistema. Isto é considerada uma vulnerabilidade instantânea que é denominada de uma ameaça zero-hour (hora zero), também conhecida como zero-day (dia zero) [8]. Além de novos tipos ou mutações de vírus, também se enquadram nesta classificação as falhas de desenvolvimento de sistemas operacionais ou aplicativos.

Uma ação defensiva contra esta ameaça é o emprego de *Whitelists*. Como o nome sugere, enquanto uma *blacklist* é uma lista de restrições, uma *whitelist* é um conjunto de permissões. Somente as ações, aplicativos e arquivos definidos nela são passíveis de execução [8]. Tudo que não se encontra permitido, por padrão, é vetado de execução.

Outra ação defensiva neste caso é o emprego de versões de sistemas operacionais e aplicativos com uma certa maturidade de mercado, onde todas as vulnerabilidades já foram encontradas e sanadas e que o desenvolvedor possua um “Ciclo de desenvolvimento do sistema” (SDLC) bem estruturado. A publicação especial do NIST de número 800-64 [9] apresenta um guia para adequação deste ciclo às necessidades de segurança de sistemas de automação e controle. Basicamente ele apresenta orientações relativas à prevenção de vulnerabilidades na etapa de desenvolvimento e de como o fornecedor do software deve proceder para mitigar os impactos de alguma falha detectada quando a versão do produto já foi fornecida aos clientes.

4) Controle de Acesso

Apesar de serem dotados de sistemas operacionais compatíveis com os controladores de acesso presentes no ambiente corporativo, as plataformas computacionais empregadas no interior das subestações, normalmente estão isoladas deste sistema. Ou seja, um colaborador quando deseja alterar uma planilha de custos compartilhada na sua rede

corporativa, tem a sua identidade (*login* de rede) conferida por um servidor de acesso, porém quando este mesmo colaborador altera uma configuração em uma IHM ou gateway de comunicação na subestação, ele utiliza um usuário e senha compartilhado entre vários colaboradores.

Uma identidade compartilhada viola um dos princípios básicos do controle de acesso seguro: a Autenticação. Basicamente a ação preventiva neste caso é a integração de um servidor de acesso e todas as plataformas computacionais em todos os níveis do sistema de automação de subestações. Este artigo abordará com mais detalhes a questão do controle de acesso mais adiante.

C. Enlaces de Comunicação Interna

O alicerce de uma rede de comunicação dentro de uma subestação de energia elétrica de acordo com a IEC 61850 são os switches. Estes equipamentos são elementos concentradores das conexões Ethernet dos diversos dispositivos da instalação. Existem duas categorias de switches: Gerenciáveis e Não-Gerenciáveis. O primeiro tipo é o mais utilizado nos projetos modernos, pois fornece ao usuário uma série de funcionalidades e possibilidades que o segundo tipo não possui. Em um primeiro momento da implantação de projetos de subestação baseados na norma IEC 61850, muito se preocupou com funcionalidades como VLAN (*Virtual LAN*) e RSTP (*Rapid Spanning Tree Protocol*). Utiliza-se VLAN normalmente para segregar o tráfego de pacotes IEC 61850 GOOSE, evitando o impacto do multicast sobre IEDs que não compartilham do mesmo grupo de automação. Já o RSTP é importante à medida que temos configurações que utilizam vários switches para atender ao número total de pontos de redes solicitados pela aplicação. Novamente, a preocupação com a segurança cibernética, normalmente não é um requisito do projeto neste nível.

1) Configurações Básicas

Apesar da principal diferença entre switches gerenciáveis e não-gerenciáveis ser justamente a capacidade de configurar diversos aspectos deste equipamento, é muito comum encontrar switches em operação nas subestações sem qualquer configuração realizada. No caso de uma invasão através dos enlaces externos de comunicação, o invasor utilizará justamente usuário e senha padrões para interceptação dos pacotes trafegados ou até mesmo degradar o desempenho da rede ao ponto de inviabilizar a comunicação na subestação.

A ação defensiva básica neste caso é a configuração de usuários e senhas com diversos níveis hierárquicos de acesso. É muito importante garantir que configurações sejam criptografadas evitando a quebra de confidencialidade em possíveis interceptações. Muitos switches gerenciáveis fornecem interfaces WEB seguras (HTTPS) para realizar a configuração dos mesmos, para esta sessão de comunicação são utilizadas técnicas de criptografia, é importante que as chaves de criptografia possam ser alteradas pelo usuário. Caso a chave de criptografia seja de conhecimento público e não possa ser alterada, ataques podem ser realizados através da interface de

configuração do switch, permitindo que toda parametrização do mesmo seja alterada, abrindo assim outras possibilidades de ataque.

2) Redes com Topologia Plana

Para comunicação interna em uma subestação, geralmente não existe a preocupação de se utilizar uma topologia com níveis hierárquicos, ou seja, todos os dispositivos com interface de rede fazem parte da mesma rede lógica independente das suas funcionalidades. Este arranjo é chamado de topologia plana. Esta topologia pode propiciar algumas falhas de segurança. Na Fig. 5, por exemplo, um notebook da equipe de manutenção é ligado ao switch para configuração de um IED, uma IHM ou um concentrador de dados. Porém como o notebook possui um endereço IP dentro da mesma rede lógica dos demais equipamentos, além dos aplicativos da manutenção, se o computador estiver contaminado com algum vírus, este poderá se proliferar para os demais elementos da rede.

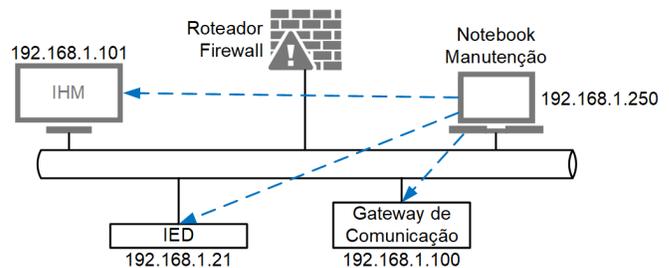


Fig. 5. Em uma rede com topologia plana não existe nível hierárquico de acesso

Como normalmente existe um roteador de borda e um firewall para interligação com o enlace externo do sistema de automação da subestação, é interessante criar também rotas e regras para a rede interna de comunicação. Desta forma somente as portas realmente necessárias aos aplicativos da manutenção serão disponibilizadas na rede. Na Fig. 6, tomando como base a rede mostrada na Fig. 5, temos liberadas somente as portas de serviços realmente utilizados na aplicação. Por exemplo, SSH (porta 22), HTTPS (porta 443) e RDP (porta 3389). O notebook obrigatoriamente será configurado para uma rede lógica diferente das dos demais dispositivos da rede, o acesso não ocorre mais de maneira direta e não supervisionada. Caso um software mal-intencionado esteja instalado no notebook de manutenção, ele será bloqueado pelas regras do firewall e pelas rotas.

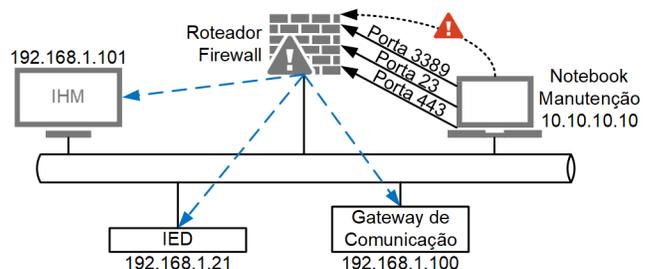


Fig. 6. Uma rede com topologia não plana confere um maior nível de segurança

D. IED: Controle de Acesso

O IED é o dispositivo mais próximo dos equipamentos de pátio de uma subestação. Este pode ser um relé de proteção multifuncional ou um controlador de bay por exemplo. Em uma concepção de defesa em profundidade, esta seria a última camada para evitar que uma ameaça cibernética evolua para uma atuação catastrófica no sistema elétrico. Em uma primeira análise, os projetos modernos de subestação não se preocupam com os aspectos de segurança da informação neste nível.

Senhas de acesso são uma importante medida de segurança. Uma senha bem estruturada é a melhor defesa contra invasões de sistemas [11]. A Tabela I mostra a comparação do tempo necessário para se decodificar uma senha baseado em uma comunicação serial de 57600 bps para diferentes IEDs. A regulamentação NERC-CIP requer que as senhas utilizadas em todos os dispositivos e sistemas envolvidos na automação de subestações possuam pelo menos seis caracteres combinando letras, números e caracteres especiais (por exemplo, @, #, ?, etc.) e que esta senha seja modificada anualmente ou com menor frequência [11]. Contudo a senha é apenas uma parte quando discutimos a questão de controle de acesso que possui três princípios básicos: Autenticação, Autorização e Auditoria.

Autenticação é a validação do usuário, isto é, uma conferência de sua identidade dentro do sistema. Normalmente protegida por uma senha, cartões criptografados, leituras biométricas, etc. Autorização é um conjunto de permissões que uma dada identidade recebe no sistema, ou seja, o que o usuário pode fazer no sistema. Finalizando, a auditoria é a possibilidade de rastreamento de todas as ações do usuário assim que autenticado no sistema. Nos sistemas de automação de subestações de energia elétrica, estes conceitos são ausentes ou deficitários. A autenticação até existe, porém as senhas são compartilhadas entre vários colaboradores o que prejudica ou até mesmo invalida a auditoria. A autorização é presente em alguns modelos de IEDs, diferenciando vários níveis de acesso. Porém como a senha foi compartilhada, a autorização também será.

TABELA I
COMPARAÇÃO DOS PADRÕES DE SENHA DE DIFERENTES IEDS E QUAL O TEMPO NECESSÁRIO PARA DESCOBRIR A SENHA UTILIZADA

	Caracteres Possíveis	Tamanho da Senha	Número de Combinações	Tempo Para Descobrir a Senha
Dispositivo 1	90	6	537 Bi	18 anos
Dispositivo 2	10	10	11 Bi	201 dias
Dispositivo 3	10	6	1 M	17 minutos
Dispositivo 4	26	4	475 K	5 minutos
Dispositivo 5	14	4	41 K	27 segundos
Dispositivo 6	2	3	14	4 milissegundos

Exigir um sistema complexo de controle de acesso no nível dos IEDs pode ser desproporcional, em função da aplicação totalmente dedicada destes dispositivos. Outro empecilho na implantação deste sistema é que os enlaces externos nem sempre dispõem de grandes larguras de banda. Existem alguns dispositivos que atuam como gerenciadores de acesso aos IEDs e empregam o protocolo LDAP (*Lightweight Directory Access Protocol*) para conexão com os servidores de autenticação centralizado. O LDAP é implementado na maioria dos sistemas operacionais utilizados em servidores de autenticação.

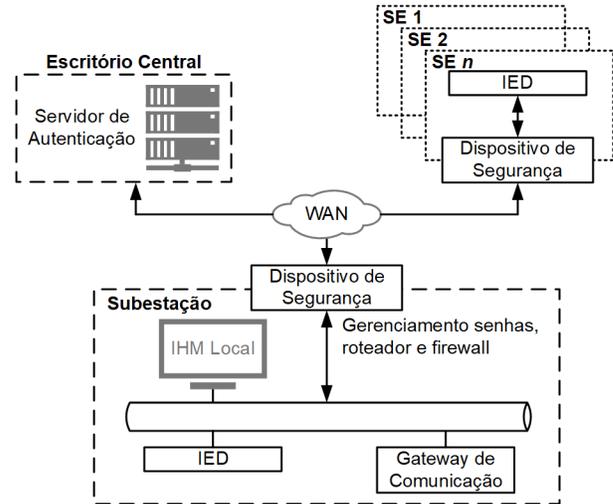


Fig. 7. Conceito de gerenciamento de senhas centralizado

Deste modo o colaborador pode utilizar a sua mesma identidade requerida quando acessa seu computador pessoal no escritório para, por exemplo, trocar um ajuste de um relé de proteção na subestação. Adicionalmente existem dispositivos capazes de realizar simultaneamente as funções de gerenciamento de senhas, roteador e firewall, a Fig. 7 ilustra a utilização de tais dispositivos e o conceito do gerenciamento de senhas centralizado.

Estes dispositivos são capazes de gerenciar e controlar as senhas de acesso corrente aos IEDs utilizando requisitos de segurança como senhas complexas e alterações periódicas das mesmas, a Fig. 8 exemplifica o processo. As alterações de senhas são comunicados ao administrador do sistema através de relatórios.

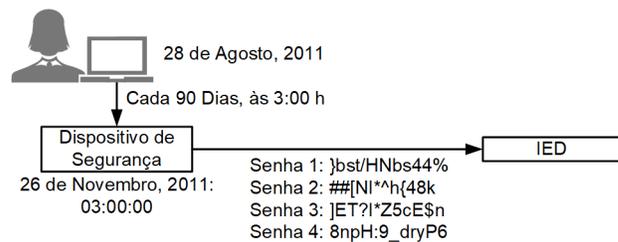


Fig. 8. Mecanismo de alteração automática de senhas

Além de o colaborador necessitar da memorização de apenas uma senha para vários tipos de atividade, existem outras vantagens como:

- Restrição de acesso a determinados IEDs baseado em regras de grupos de acesso. Por exemplo, integrantes do grupo de manutenção poderiam acessar integralmente a parametrização dos IEDs enquanto que um grupo de monitoramento seria permitido apenas a leitura de relatórios;
- Controle de todas as ações dos colaboradores no sistema de automação de subestações, uma vez que para qualquer ação, estes devem ser autenticados no servidor centralizado;
- Aumento da segurança no nível dos IEDs, já que a senha de acesso a estes não precisa ser compartilhada entre todos os colaboradores.

III. CONCLUSÃO

Questões de segurança cibernética não atingem mais somente o ambiente TI. Os resultados de uma invasão cibernética em sistemas de automação de subestações podem ser catastróficos. Regulamentações existentes nos Estados Unidos e tendências de adoção na União Europeia enfatizam a importância de adoção de medidas preventivas nos projetos de subestações modernas. Algumas ações abordadas foram:

- Utilização de criptografia em todos os enlaces externos;
- Emprego de roteadores e firewalls tanto para enlaces externo quanto para internos, evitando assim o emprego de redes de topologia plana;
- Software antivírus também são necessários em todas as plataformas computacionais porém suas configurações devem ser readequadas para este fim;
- Políticas de uso de memórias USB e emprego de whitelist em computadores com tarefas de tempo-real;
- Desabilitação de portas ociosas nos switches;
- Sempre utilizar senhas com pelo menos 6 caracteres contendo letras, números e caracteres especiais para todos os dispositivos no sistema;
- Utilização de sistemas de controle de acesso centralizado propiciando autorização, autenticação e auditoria de maneira abrangente, incorporando funcionalidades de roteador e firewall.

IV. REFERÊNCIAS BIBLIOGRÁFICAS

- [1] A. Massoud e A. M. Giacomoni. Smart Grid – Safe, Secure, Self-Healing, artigo publicado pela revista IEEE Power & Energy de janeiro/fevereiro de 2012.
- [2] C-C Liu e outros. Intruders in the Grid, artigo publicado pela revista IEEE Power & Energy de janeiro/fevereiro de 2012.
- [3] P. A. Craig Jr., e T. P. McKenna Jr. Technology Security Assessment for Capabilities and Applicability in Energy Sector Industrial Control Systems, relatório publicado pela McAfee em março de 2012.
- [4] C. Ewing. Engineering Defense-in-Depth Cybersecurity for the Modern Substation, artigo publicado pela Schweitzer Engineering Laboratories, Inc. em 2010.
- [5] D. Anderson e N. Kipp. Implementing Firewalls for Modern Substation Cybersecurity, artigo publicado pela Schweitzer Engineering Laboratories, Inc. em 2010.
- [6] J. Falco e outros. Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts, NIST Special Publication 1058 em setembro de 2006.
- [7] E. O. Schweitzer, III, e outros. How Would We Know?, artigo publicado pela Schweitzer Engineering Laboratories, Inc. em 2011.
- [8] D. Anderson. Increase Security Posture With Application Whitelisting, artigo publicado pela Schweitzer Engineering Laboratories, Inc. em 2011.
- [9] R. Kisseld e outros. Security Considerations in the System Development Life Cycle, NIST Special Publication 800-64 em outubro de 2008.
- [10] CSSP (Control Systems Security Program) ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) endereço eletrônico http://www.us-cert.gov/control_systems/ics-cert/.
- [11] D. Anderson e G. Leischner. Cybersecurity as Part of Modern Substations, artigo publicado pela Schweitzer Engineering Laboratories, Inc. em 2007.