



**XXIII SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA**

FI/GTL/12
18 a 21 de Outubro de 2015
Foz do Iguaçu - PR

GRUPO – XV

GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS ELÉTRICOS - GTL

SEGURANÇA CIBERNÉTICA E CONTROLE DE ACESSO EM SISTEMAS ELÉTRICOS DE POTÊNCIA

**Rafael Argachof Cervev(*)
SEL**

RESUMO

Os sistemas de automação têm contribuído para uma maior visibilidade, melhorias na operação e confiabilidade do sistema elétrico de potência. Esse contexto tem criado as bases para as chamadas redes inteligentes. Aliado a esses avanços nos recursos operativos é igualmente importante que o sistema seja seguro contra ataques e uso mal intencionado dos seus recursos. Neste contexto, o controle de acesso aos equipamentos e a utilização de protocolos de comunicação seguros cumprem um papel importante na segurança do sistema.

PALAVRAS-CHAVE

Controle de Acesso, LDAP, Segurança Cibernética, Redes Inteligentes

1.0 INTRODUÇÃO

Atualmente existe um grande apelo ao conceito de redes elétricas inteligentes, denominadas de “Smart Grids”. Estas redes inteligentes, de forma bastante simplificada, podem ser definidas como sistemas baseados em tecnologia digital de comunicação e automação visando o consumo otimizado de energia elétrica, com redução de custos e aumento da confiabilidade do sistema. A base para a implantação de um sistema de rede inteligente reside na quantidade de informações disponíveis do sistema elétrico, na possibilidade de transitar essas informações através de meios de comunicação e no tratamento correto das mesmas.

Este conceito de redes inteligentes tem contribuído para um novo cenário na automação de sistemas elétricos. Até o final de década de 90, a realidade era diferente, o sistema era composto por “Ilhas de Automação”[1],[2]. Existiam subestações com certos níveis de supervisão e controle, algumas vezes telecomandadas, mas elas eram pequenas ilhas que não se interconectavam. “O cenário da automação de subestações nesta época era, em sua grande maioria, baseada em comunicações totalmente isoladas e normalmente utilizando canais seriais” [3].

A evolução dos sistemas de comunicação contribuiu com a interconexão dos sistemas de automação, atuando como o pano de fundo para o desenvolvimento das redes ao proporcionar a visibilidade e os dados necessários para a inteligência da rede.

Os sistemas de comunicação, sejam eles de propriedade da concessionária ou contratados de operadoras, possibilitam que os dados necessários às redes inteligentes estejam disponíveis aos sistemas, operadores e à engenharia. Adicionalmente, o acesso remoto através desses meios de comunicação aos equipamentos e subestações tem contribuído com a otimização de recursos e na solução de problemas com maior agilidade.

“Os avanços nos sistemas de controle e comunicação, voltados para o sistema elétrico de potência, apresentam novos desafios relacionados à segurança cibernética que devem ser tratados antes de iniciar a implantação dessas tecnologias no desenvolvimento de redes inteligentes” [4].

(*) Rodovia Campinas-Mogi Mirim (SP-340), km 118.5. Condomínio Pólis de Tecnologia (CPqD) – Prédio 11
CEP 13086-902 Campinas, SP – Brasil Tel: (+55 19) 3515-2000 – Fax: (+55 19) 3515-2011 – Email: suporte@selinc.com

Com a popularização dos sistemas digitais também foram registrados diversos casos de uso mal intencionado da tecnologia, gerando prejuízos para pessoas e instituições. Como o suprimento de energia é extremamente importante para a economia, segurança e até mesmo saúde das pessoas, é necessário que as redes inteligentes de distribuição sejam seguras e confiáveis.

Conhecendo as vantagens que um sistema interconectado pode proporcionar e sabendo das ameaças que podem surgir, órgãos governamentais e privados tem se mobilizado para estudar e propor soluções para proteger as redes inteligentes contra ameaças cibernéticas [8]. Nos Estados Unidos as resoluções do NERC-CIP (North American Reliability Corporation – Critical Infrastructure Protection) exercem grande influência nas empresas do setor de energia elétrica e no sistema básico de geração e transmissão de energia elétrica. Nas aplicações de redes inteligentes, também existe uma grande influência das recomendações do NIST (National Institute of Standards and Technology).

Recentemente a Mandiant, uma empresa especializada em segurança da informação, publicou um relatório apresentando evidências de um sistema de operações na China com o objetivo de espionar e roubar informações de diversas companhias ao redor do mundo [5]. A McAfee, outra empresa voltada à segurança da informação, também publicou diversos relatórios produzidos juntamente com o governo americano, apontando diversas tentativas de ataques a empresas de energia elétrica, gás e óleo [6]. Além dessas publicações recentes, existem registros amplamente divulgados de casos como o Stuxnet, que traçam o pano de fundo para a necessidade de uma observação mais criteriosa das questões relacionadas com a segurança cibernética em sistemas de energia elétrica. O Stuxnet foi um vírus de computador descoberto em plantas de beneficiamento de urânio no Irã com o objetivo específico de atacar os sistemas de controle e gerar danos físicos às instalações [14].

Além da necessidade de proteção dos canais de comunicação contra invasões e interceptações, uma rede segura deve impôr mecanismos que regulamentem os direitos de acesso aos seus recursos.

2.0 CONTROLE DE ACESSO

A proteção de um sistema contra ataques cibernéticos é um assunto complexo, pois é necessário atuar em diversas frentes de trabalho, sejam elas técnicas ou no gerenciamento de pessoas, no intuito de garantir altos níveis de segurança. Adicionalmente à atuação nesses níveis, a literatura sobre segurança sugere a utilização da técnica de defesa em profundidade, com o objetivo de propor uma solução integral, baseada em várias camadas de defesa [3]. Dentro desse conceito, o controle de acesso seria uma das camadas necessárias para a defesa de uma instalação ou sistema.

Sob o ponto de vista de segurança de redes, o controle de acesso visa limitar e controlar o acesso aos sistemas por meio dos enlaces de comunicação [9].

Nos Estados Unidos, o NIST desenvolveu uma série de guias com políticas e procedimentos de segurança para os sistemas de controle industriais, envolvendo sistemas de supervisão e controle (SCADA), sistemas de controle distribuído (DCS) e outros dispositivos como controladores lógicos programáveis (PLC). Estas políticas e procedimentos visam estabelecer diretrizes de segurança para um sistema industrial, e traçam os requisitos mínimos para controle de acesso nesses sistemas.

Apenas sob o aspecto técnico, no nível dos equipamentos, softwares e produtos empregados com a finalidade de proteger o sistema, não é possível atingir níveis satisfatórios de segurança. Segundo o NIST, para assegurar a confidencialidade, integridade e disponibilidade das informações em determinado sistema é necessário atuar de forma gerencial, operacional e técnica [10].

No primeiro nível definido pelo NIST, as ações são focadas no gerenciamento de risco e no gerenciamento da segurança das informações. Nesta classe são definidas medidas que visam a elaboração de políticas e procedimentos de segurança, além de métodos para medir e certificar a segurança de determinada instalação.

No nível operacional são definidas as medidas de controle focadas nas pessoas da organização, por exemplo: segurança pessoal, planos de contingência, resposta a incidentes e medidas para conscientização e treinamento de pessoal. Dentro do nível operacional se encontram as primeiras recomendações do NIST relacionadas ao controle de acesso voltadas para o aspecto da segurança física das instalações.

Segundo o NIST, os sistemas de controle de acesso devem assegurar que somente pessoas autorizadas possam obter acesso a determinados espaços controlados como, por exemplo, as subestações, incluindo o pátio e sala de controle. Os sistemas de controle de acesso devem ser flexíveis. A necessidade de acesso deve ser baseada no horário (turno), nível de treinamento, nível hierárquico do funcionário, atribuições da função do funcionário e diversos outros fatores. O sistema deve ser capaz de identificar que a pessoa a quem será liberado o acesso é realmente quem deveria ser.

Sob o olhar técnico do NIST na classificação das medidas de segurança, são definidas as medidas que são embarcadas em mecanismos de hardware, software e firmware. Dentro deste nível de atuação, são definidas pelo NIST quatro famílias principais: Identificação e Autenticação, Controle de Acesso, Auditoria e Responsabilidade, Proteção do sistema de comunicação.

2.1 Identificação e Autenticação

Autenticação consiste no processo de identificação positiva de potenciais usuários, aplicações, serviços e recursos, utilizando uma combinação de fatores ou credenciais [10]. Existem diversas formas de se confirmar a autenticação de uma pessoa, dispositivo ou sistema. Sob o ponto de vista corporativo, as pessoas usualmente possuem senhas específicas para acesso ao sistema e computadores da empresa. Igualmente no contexto de automação, os equipamentos e sistemas muitas vezes disponibilizam senhas e níveis de usuário para acesso as suas funções.

Sob o aspecto de rede, o NIST recomenda que as autenticações de serviços utilizem técnicas mais seguras do que o emprego de senhas, como, por exemplo, a Autenticação por desafio-resposta ou por certificados de chave pública. O método de desafio-resposta é uma técnica em que as duas partes da comunicação devem conhecer um código secreto. No momento da conexão, o solicitante, envia um número ou string randômico. O receptor deve então utilizar a informação recebida para gerar uma resposta única com o código secreto. Se for enviada a resposta esperada, a conexão é estabelecida. O método de certificação será abordado oportunamente, no item sobre criptografia.

2.2 Controle de Acesso

O controle de acesso possui uma série de mecanismos com a finalidade de possibilitar o uso dos recursos e sistemas somente para usuários, programas e sistemas autorizados. Neste nível são definidos os direitos e as permissões que determinado usuário tem para acessar informações e atuar sobre o sistema.

Existem diversas técnicas de controle de acesso, sendo recomendada pelo NIST a utilização do controle de acesso baseado em papéis. Nesta técnica os direitos e permissões de determinado indivíduo são estabelecidos frente ao papel que ele desempenha dentro da organização e estes papéis são associados aos tipos de usuários. Os papéis são criados de acordo com as diferentes funções e cargos existentes na organização e os usuários são associados aos papéis de acordo com as suas responsabilidades e qualificações.

Trazendo este conceito para os sistemas de proteção e controle, temos diversos usuários que atuam diretamente no sistema como: equipes de engenharia, manutenção, operadores, etc. O acesso aos equipamentos e sistemas deve ser restringido frente aos papéis que cada um desses grupos desempenha dentro da organização. Por exemplo, os operadores podem ter acesso aos equipamentos para visualização de grandezas elétricas e estado, contudo, não devem ter permissão para alterar ajustes ou parâmetros dos relés de proteção. Em contrapartida, a equipe de manutenção deve ter acesso aos ajustes e parâmetros para atuar no sistema conforme a necessidade de intervir ou modificar as configurações dos equipamentos. Porém, sem uma política de controle de acesso é impossível garantir essa condição.

Dentro de ambientes corporativos o controle de acesso já é vastamente empregado, em sua maioria baseado em senhas e cartões, contudo, continua renegado dentro dos sistemas de automação e proteção do sistema elétrico. Geralmente não são utilizados os recursos de autenticação disponíveis nos equipamentos do sistema elétrico. Muitos equipamentos possuem senhas, contudo, muitas vezes é utilizada a senha padrão definida pelo fabricante ou a senha é compartilhada. Tais práticas não garante nenhum nível de segurança.

2.3 Auditoria e Responsabilidade

A auditoria tem como objetivo possibilitar o rastreamento de todos os usuários e ações realizadas no sistema. O NIST recomenda que as organizações devem estabelecer políticas e procedimentos para o registro de ações.

No contexto de sistemas de proteção e controle de sistemas elétricos, os ajustes e parâmetros dos equipamentos que compõem o sistema são dados vulneráveis a alterações. Por exemplo, a alteração inadvertida de um ajuste de um relé de proteção pode ocasionar a atuação indevida ou a descoordenação do relé, culminando possivelmente no desligamento do sistema. Os sistemas de controle de acesso nesse contexto devem permitir que tais ajustes e parâmetros utilizados durante a validação e comissionamento do sistema continuem em operação e, quando alterados, sejam registrados de forma a possibilitar a auditoria e rastreamento das alterações.

2.4 Proteção do Sistema de Comunicação

Os sistemas de comunicação podem ser submetidos a diversos tipos de ameaças, tais como: invasões, ataques e interceptações. Portanto, é necessário que além de políticas de controle de acesso o sistema de comunicação utilizado na subestação e em seu enlace externo seja seguro.

“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, [...]” [3]

De forma a proteger os sistemas de comunicação são indicadas a utilização de técnicas como criptografia, VPN (Virtual Private Networks), protocolos seguros, firewalls e filtragem de pacotes. Por exemplo, uma conexão VPN pode ser estabelecida na borda de uma subestação para conexão com um centro remoto de forma a criar um canal de comunicação criptografado e com autenticação sobre a rede insegura, além disso, a utilização de Firewalls também é importante, pois permite criar uma barreira com o propósito de controlar a comunicação entre a subestação e o mundo exterior.

Em alguns locais, a comunicação com subestações ou IED's (Intelligent Electronic Device) ainda é realizada através de canais de comunicação seriais. Estes canais também podem ser protegidos através de autenticação e criptografia de forma a assegurar que a mensagem foi enviada por quem realmente deveria enviar e, que não houve alteração em seu conteúdo.

Além da proteção do sistema de comunicação com a utilização de protocolos seguros, também é importante observar como é controlado o acesso aos dados e informações disponíveis nos equipamentos e sistemas.

3.0 LDAP – Lightweight Directory Access Protocol.

O LDAP é um protocolo de comunicação que define um formato de mensagens utilizadas por um determinado cliente para acessar dados em um diretório. Um serviço de diretório é uma coleção de software, hardware, processos, políticas e procedimentos administrativos destinados a fazer com que a informação do diretório esteja disponível aos usuários que o acessam [7].

Através do LDAP, usuários de uma determinada rede podem ser gerenciados através de um servidor centralizado. Dentro de uma concessionária de energia elétrica já existe um diretório com os usuários que acessam a rede corporativa da empresa, esta estrutura também pode ser utilizada como o servidor central para os usuários acessarem o sistema de proteção e controle. Os equipamentos utilizados para proteção e controle do sistema elétrico tradicionalmente não possuem o recurso de autenticação junto a um diretório via LDAP, dessa forma é necessário utilizar, por exemplo, nas subestações, uma Central de Autenticação Cliente para interface entre o Servidor de Acesso Centralizado e os IED's.

Quando um usuário necessita ter acesso a um determinado equipamento ou sistema, a solicitação será através da Central de Autenticação Cliente. Essa central irá consultar o Servidor de Acesso Centralizado que, por sua vez, irá verificar a autenticação do usuário. Se as credenciais do usuário forem válidas o acesso ao IED será liberado a partir da Central de Autenticação Cliente. Caso não seja um usuário conhecido ou este não possua as permissões necessárias para acessar o determinado IED o acesso não será liberado. Esse processo pode ser vista na Figura 1.

A autenticação em um servidor centralizado também permite que o acesso aos IED's seja baseado em regras relacionadas às funções e privilégios de cada usuário. Por exemplo, os usuários de manutenção podem acessar os IED's e alterar os parâmetros, contudo, usuários da operação podem somente visualizar dados e requisitar relatórios.

Este gerenciamento centralizado traz diversos outros benefícios, por exemplo: se determinado colaborador é desligado, a exclusão do usuário no servidor já indisponibiliza o usuário e senha que ele utilizava para acessar os dispositivos da rede bloqueando seu acesso aos equipamentos e sistemas. Da mesma forma, se o colaborador possui um novo cargo e este permite um nível de acesso diferente aos recursos do sistema, o gerenciamento centralizado facilita o processo de atualização dos privilégios desse usuário.

De forma a tornar seguro esse processo de acesso às informações, o LDAP requer uma autenticação no estabelecimento da conexão entre o cliente e o servidor. Essa autenticação visa proteger o sistema contra pessoas ou serviços mal intencionados que busquem obter acesso ilícito. Assim como ilustrado na Figura 2, é utilizado certificado padrão X.509 para autenticar o servidor LDAP na interação do cliente com o servidor para confirmar as credenciais de um usuário solicitando acesso.

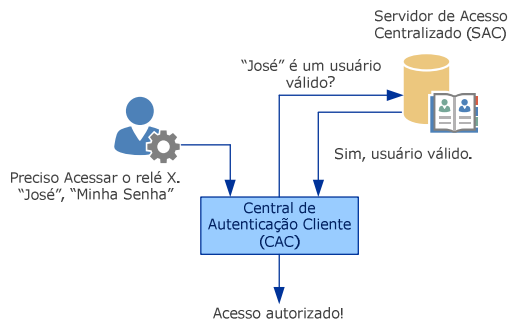


Figura 1 – Autenticação no Servidor de Acesso Centralizado (SAC).

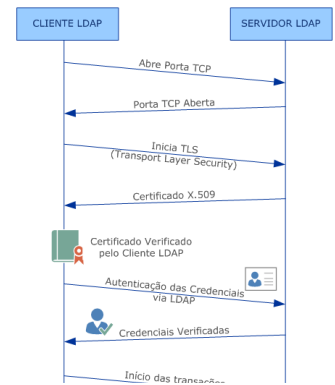


Figura 2 – Autenticação via LDAP

Com o objetivo de tornar a comunicação segura, os certificados trocados entre o cliente e servidor LDAP no processo de autenticação utilizam técnicas de criptografia.

4.0 CRIPTOGRAFIA

Uma das ferramentas mais importantes para proteção da informação que trafega em um meio de comunicação é a criptografia dos dados. A criptografia consiste na transformação de uma mensagem em um formato que não seja prontamente decifrável, permitindo que esta seja conhecida somente pelo transmissor e receptor. A transformação e a recuperação dos dados dependem de uma "chave". Nas aplicações modernas de criptografia essa chave é gerada a partir de algoritmos matemáticos. "Criptografia é o estudo de sistemas matemáticos com o objetivo de tratar dois problemas de segurança: privacidade e autenticação" [13].

Existem duas formas de criptografia: simétrica, também chamada de convencional, e a criptografia assimétrica, conhecida também como chave pública.

4.1 Criptografia Simétrica

Na criptografia simétrica a cifragem e decifragem da mensagem são realizadas utilizando a mesma chave [9]. A cifragem da mensagem é realizada utilizando uma chave secreta e um algoritmo de criptografia. Utilizando a mesma chave e um algoritmo de decifragem é recuperado o texto claro a partir do texto cifrado.

O algoritmo de criptografia realiza diversas substituições e transformações no texto claro baseado na chave secreta. A chave é um valor independente do texto claro e do algoritmo.

De acordo com Stallings [9], é impraticável decifrar uma mensagem com base no texto cifrado e com o conhecimento dos algoritmos de cifragem/decifragem. Dessa forma na criptografia simétrica não é necessário manter o algoritmo secreto, o importante e essencial para manter a confidencialidade da mensagem é preservar a chave protegida. Essa característica da criptografia simétrica a torna de implementação mais simples e de menor custo [3]. Existem dois padrões principais de criptografia simétrica, o DES (Data Encryption Standard) e o AES (Advanced Encryption Standard).

4.2 Criptografia Assimétrica

Na criptografia assimétrica a cifragem e decifragem são realizadas utilizando chaves diferentes, uma pública e outra privada. Nesta forma de criptossistema o texto claro é transformado em texto cifrado através de uma das chaves e do algoritmo de criptografia. Usando a outra chave e os algoritmos de decifragem o texto claro é recuperado a partir do texto cifrado [9]. O criptossistema de chave pública mais aceito e utilizado é o RSA (Rivest Shamir Adleman) [9].

4.3 Autenticação de Mensagens

A autenticação das mensagens visa assegurar que a integridade de uma mensagem, ou seja, que os seus dados, são realmente aqueles enviados pelo remetente e que a identidade do emissor é válida.

"Um sistema de autenticação previne que mensagens não autorizadas sejam inseridas em um canal público, garantindo ao receptor de uma mensagem a legitimidade do emissor" [13].

As duas técnicas mais utilizadas para autenticação de mensagens são: MAC (Message Authentication Code) e a função de Hash.

O MAC atua como uma função da mensagem e de uma chave secreta. Através da chave secreta é gerado um bloco de dados de tamanho fixo que é anexado à mensagem. Esse bloco de dados é conhecido como o código de autenticação MAC. Se considerarmos que somente o emissor e o receptor tem conhecimento da chave secreta, o receptor da mensagem tem a garantia de que ela não foi alterada e que ela provém realmente do emissor conhecido. Se for realizada alguma alteração indevida na mensagem, sem o conhecimento da chave secreta, o cálculo do código de autenticação MAC do receptor será diferente do emissor, indicando que houve uma alteração na mensagem. Exemplos do código de autenticação de mensagem são: HMAC e o CMAC.

A função de Hash relaciona uma mensagem, que pode ser de tamanho variável, a um valor de hash com tamanho fixo. A função de hash não utiliza uma chave assim como no código MAC. O código gerado é uma função de todos os bits da mensagem, atuando como autenticador da mensagem. Qualquer alteração na mensagem resulta em uma mudança no código de hash. Como exemplo, duas das implementações mais importantes do algoritmo de hash são: o SHA (Secure Hash Algorithm) e o MD5 (Message-Digest algorithm 5).

4.4 Assinatura Digital

A assinatura digital possui uma filosofia similar aos antigos selos de cera que eram aplicados para fechar e identificar as correspondências reais. Através dessa técnica um determinado emissor “assina” a mensagem ao incluir um código gerado através de um algoritmo criptográfico. Uma assinatura digital pode ser criada ao se definir um código de hash para a mensagem e então criptografar esse código com a chave privada do emissor. Com a assinatura digital é possível proteger duas partes que trocam mensagens contra uma terceira [9]. O DSS (Digital Signature Standard) é um padrão adotado pelo NIST que utiliza o algoritmo SHA [9].

4.5 Certificação Digital

Certificados digitais, também denominados de certificados de chave pública, proporcionam um método formal para vincular uma determinada chave pública a seu respectivo dono. O certificado permite verificar a identidade do autor de uma assinatura. Usualmente os certificados digitais são utilizados em três formas: Infraestrutura de chave pública (PKI – Public-Key Infrastructure), Teia de Confiança (Web of Trust) e Simple Public Key Infrastructure (SPKI).

A certificação por infraestrutura de chave pública é o mais formal, pois ele é emitido por uma Autoridade Certificadora (AC).

A Teia de Confiança é um método descentralizado. Assim como infraestrutura de chave pública a certificação é fornecida por um terceiro, contudo, não uma Autoridade Certificadora formal.

No modelo de Simple Public Key Infrastructure, a certificação não é emitida por um terceiro, o dono e o emissor do certificado é a mesma entidade. Os certificados são distribuídos antecipadamente entre os dispositivos que farão parte de um enlace de comunicação.

O padrão mais comum para os certificados digitais é o X.509, ele descreve o modelo e os passos para autenticação. O X.509 foi definido pelo ITU-T (International Telecommunication Union standard).

Como indicado na Figura 2, no início da comunicação o servidor apresenta o seu certificado X.509 para autenticação junto aos cliente. Tal medida visa proteger o sistema contra um terceiro que tente se mascarar para obter acesso.

5.0 EXEMPLO DE UM SISTEMA SEGURO

Diante dos conceitos, funções e recursos analisados nesse trabalho sob o aspecto da segurança cibernética, é necessário identificarmos alguns exemplos de como eles podem ser aplicados dentro do contexto de uma subestação de energia elétrica.

5.1 Controle de Acesso

Os equipamentos e sistemas utilizados para proteção e automação de sistemas elétricos geralmente possuem senhas para acesso às suas funções. Alguns permitem até a criação de mais de um nível de usuário com permissões distintas. Apesar de possuírem esse recurso, dentro do contexto de uma empresa do setor elétrico o gerenciamento das senhas de todos os equipamentos de forma isolada se torna uma tarefa impossível: Em função

da quantidade de equipamentos existentes, diversas equipes e profissionais que necessitam acessá-los e o fato do compartilhamento de senhas contrariar os princípios de segurança cibernética. Outro fator complicador, o qual podemos citar, é a amplitude geográfica e a distância entre subestações, regionais e equipamentos instalados ao longo da rede.

Portanto, atuar no controle de acesso aos equipamentos e sistemas é praticamente impossível sem que este seja realizado de forma centralizado. Como os IED's para proteção e automação de sistemas elétricos normalmente não possuem funções ou recursos que permitam a autenticação e autorização centralizados, é necessário incluir nas arquiteturas de automação dispositivos com o intuito de adicionar esta função dentro do contexto das subestações de energia elétrica.

Uma possível solução é a utilização de um gateway de segurança na subestação (Figura 3 e 4). Este gateway deve ter acesso ao servidor centralizado através da rede. O gateway irá atuar como uma central de autenticação cliente buscando validar no servidor através do protocolo LDAP as credências de determinado usuário no momento da requisição de acesso a um determinado IED da subestação. Tal gerenciamento também permite que o controle de acesso seja baseado nos papéis que os usuários exercem, definindo os privilégios e funções que cada usuário pode realizar.

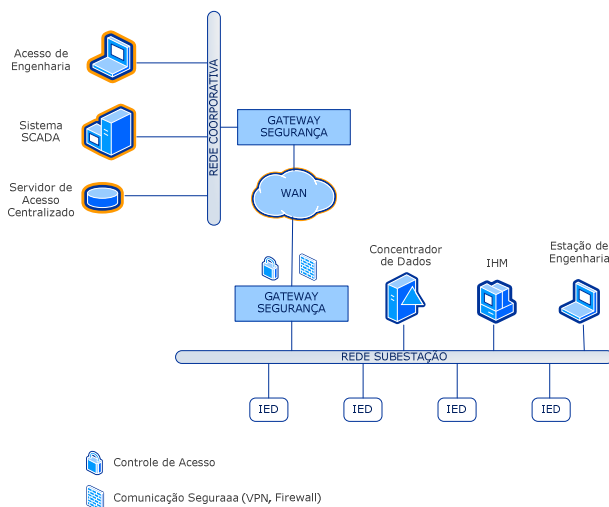


Figura 3 – Arquitetura de subestação com gateway de segurança

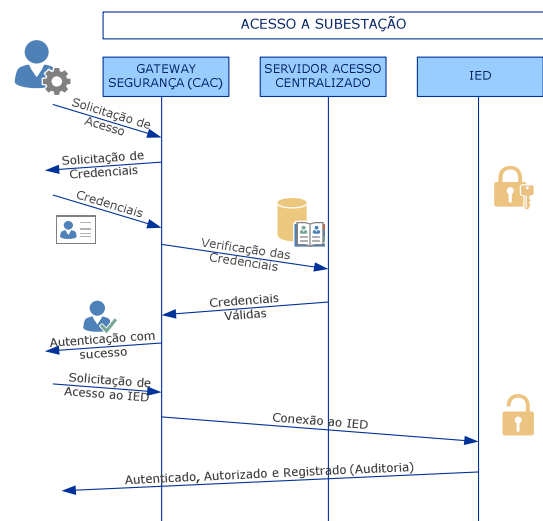


Figura 4 – Controle de acesso

Também há vantagens no gerenciamento corporativo, por exemplo, caso um colaborador seja desligado da empresa a exclusão do usuário do sistema é realizado a partir do Servidor Central e o acesso é automaticamente bloqueado a todos os IED's. Por exemplo, nas resoluções do NERC-CIP é determinado que após o desligamento de um colaborador as senhas sejam trocadas em um período de 24 horas.

O gateway de segurança, além de buscar a autenticação dos usuários que solicitam acesso aos IED's no servidor centralizado também deve atuar no gerenciamento das senhas dos IED's da subestação. As senhas dos IED's devem ser alteradas pelo gateway de segurança. Se forem utilizadas senhas conhecidas nos IED's, a autenticação centralizada se torna inútil. Um determinado usuário, localmente ou remotamente, poderia acessar o IED através da senha do equipamento ao invés de utilizar a sua senha corporativa e a autenticação centralizada. O gerenciamento das senhas por parte do gateway de segurança deve utilizar senhas complexas e trocas periódicas de forma a elevar os níveis de segurança.

5.2 Auditoria

Além de proporcionar o controle de acesso de forma centralizada, a utilização de um gateway de segurança também pode permitir a auditoria através dos registros de acesso aos equipamentos. Um questionamento recorrente entre as empresas do meio diz respeito à garantia de que os equipamentos, após certo tempo, estarão com os ajustes e configuração conforme o comissionamento e start-up. Igualmente, se forem realizadas intervenções e alterações, quando e por quem elas foram realizadas? Tais questionamentos podem ser respondidos com a utilização de um gateway de segurança que permita o registro de acesso e de intervenções nos equipamentos de forma a fornecer os recursos necessários para a auditoria do sistema.

5.3 Comunicação Segura

Os meios de comunicação devem proporcionar um caminho seguro para os dados que trafegam para a subestação. Nesse sentido, o gateway de segurança, na borda da subestação, pode além de atuar no controle de

acesso, estabelecer uma conexão segura, por exemplo, via VPN com o gateway do centro de controle.

A certificação e a criptografia também cumprem um papel importante na segurança da comunicação, pois asseguram a integridade da informação e autenticidade das partes.

6.0 CONCLUSÕES

Atualmente, as empresas de energia elétrica vêm buscando tornar a rede cada vez mais inteligente, com o intuito de melhorar a confiabilidade e qualidade do suprimento de energia elétrica a seus consumidores. O desenvolvimento dos equipamentos, com a inclusão de recursos voltados a comunicação e integração, aliado a evolução dos meios de comunicação proporcionam a base para a maior visibilidade e inteligência da rede.

Além das facilidades e recursos proporcionada pela interligação dos equipamentos e sistemas, é importante observar as questões de segurança cibernética de forma a proteger a rede e garantir a confiabilidade de um sistema inteligente. Nesse contexto, o controle de acesso ocupa um papel de suma importância. O acesso aos equipamentos deve ser controlado de forma que somente pessoas autorizadas possam acessar suas funções e alterar parâmetros. Como os equipamentos de proteção e automação atualmente utilizados geralmente não possuem recursos que garantam um sistema seguro de controle de acesso é necessário incluir dentro do sistema das subestações equipamentos com esta finalidade.

Igualmente é importante que os canais de comunicação e os protocolos utilizados no acesso aos equipamentos sejam seguros. Nesse sentido, a utilização criptografia, VPN, protocolos seguros, firewalls e filtragem de pacotes são importantes para proteger o conteúdo dos dados. A autenticação também é necessária para garantir a legitimidade das partes em um sistema de comunicação.

Por fim também é importante que sejam observados, além dos aspectos técnicos, os procedimentos e políticas das empresas no controle de acesso aos recursos e equipamentos, para garantir níveis satisfatórios de segurança cibernética.

7.0 REFERÊNCIAS BIBLIOGRÁFICAS

- (1) TORSTEN, Cegrell. Power System Control-Technology. Englewood Cliffs, Prentice-Hall, 1986.
- (2) ERICSSON, Göran N.. Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure, IEEE Transactions on Power Delivery, vol. 23, no. 3, pp 1501-1507, Abril 2010.
- (3) OLIVEIRA, Carlos e ABOUD, Ricardo. Desafios da Segurança nas Subestações de Energia Elétrica. In: XI Seminário Técnico de Proteção e Controle. Florianópolis. 2012.
- (4) AMIN, S.M. e GIACOMONI, A.M. Smart Grid, Safe Grid, IEEE Power and Energy Magazine, vol. 10, no. 1, pp. 33-40, Janeiro/Fevereiro 2012.
- (5) MANDIANT. Mandiant Intelligence Center Report APT1: Exposing One of China's Cyber Espionage Units. Disponível na internet. URL: <http://intelreport.mandiant.com/> (acesso em 2013).
- (6) McAfee, Inc.. Global Energy Cyberattacks: "Night Dragon". Disponível na internet. URL: <http://www.mcafee.com/au/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf> (acesso em 2013).
- (7) HOWES, Timothy A., SMITH, Mark C. e GOOD, Gordon S.. Understanding and Deploying LDAP Directory Services. Estados Unidos, Addison-Wesley Professional, 2003.
- (8) DOLEZILEK, David e HUSSEY, Laura. Requirements or Recommendations? Sorting Out NERC CIP, NIST, and DOE Cybersecurity. In: 2011 64th Annual Conference for Protective Relay Engineers. Texas, 2011. pp. 328-333.
- (9) STALLINGS, William. Criptografia e segurança de redes: Princípios e Práticas. São Paulo, Pearson Prentice Hall, 2008
- (10) NIST. Guide to Industrial Control Systems (ICS) Security. Disponível na internet. URL: <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf> (acesso em 2013).
- (11) NIST. Guideline for Implementing Cryptography In the Federal Government. Disponível na internet. URL: http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf (acesso em 2013)

- (12) DENNING, Dorothy E..Cryptography and data security. EstadosUnidos,Addison-Wesley Publishing Company, 1982.
- (13) DIFFIE, Whitfield. e HELLMAN, Martin. E. New directions in cryptography. IEEE Transactions on Information Theory. vol. 22, no. 6, pp. 644-654, Novembro, 1976.
- (14) LANGNER, R.Stuxnet: Dissecting a Cyberwarfare Weapon.Security & Privacy, IEEE.vol. 9 , no.3, pp. 49-51, Maio/Junho, 2011.
- (15) RAUSCHER, Karl. It's Time to Write the Rules of Cyberwar. Disponível na internet:<http://spectrum.ieee.org/telecom/security/its-time-to-write-the-rules-of-cyberwar>(acesso em 2013).