SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA

GTL - 12
16 a 21 Outubro de 2005
Curitiba - Paraná

GRUPO XVI

GRUPO DE ESTUDOS DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO

SEGURANÇA DE DADOS NAS SUBESTAÇÕES

Juliano da SantAnna Bahia
Schweitzer Engineering Laboratories, Brasil LTDA

RESUMO

O grande crescimento do uso da internet nas últimas décadas abriu uma larga porta de entrada para os crimes cibernéticos. As companhias energéticas também se tornaram um alvo para estes crimes, já que hoje o sistema elétrico é muito semelhante as redes de computadores. Em face destes eminentes riscos o sistema elétrico tem usado, ainda de forma muito modesta, técnicas para se prevenir destes ataques.

PALAVRAS CHAVE
Hacker, Ethernet, SCADA, Vulnerabilidade, Segurança.

1.0 INTRODUÇÃO

Não é difícil de se notar a vulnerabilidade dos sistemas de potência com relação aos hackers. O centro de toda essa fraqueza do sistema está na capacidade de obter acesso remoto aos equipamentos de controle e proteção das subestações de transmissão, distribuição, geração e industriais. Tem-se na verdade um cobertor curto. Ao passo que crescem as facilidades de interação com os equipamentos pelos meios de comunicações diversos, crescem também os pontos fracos dos sistemas. Apesar de historicamente o acesso remoto fique restrito a redes privadas e proprietária existe uma grande tendência em se usar os meios públicos de comunicação para trafegar dados diminuindo muito os custos na implantação da integração do sistema.
A vulnerabilidade de uma subestação pode trazer conseqüências pouco agradáveis como fortuitamente ou maliciosamente operar disjuntores, religadores, mudar ajustes de equipamentos gerando desde um simples desligamento pontual a um “apagão” de toda uma região.
Diversas ferramentas baseadas em computadores são utilizadas para ataques. Muitas destas ferramentas são facilmente encontradas gratuitamente na Internet. Sites e livros oferecem verdadeiras aulas de como ser um hacker. Porém existem também inúmeros sites disponibilizando softwares voltados para a proteção e combate destes infelizes intrusos. É importante salientar que a telefonia pública e a rede pública de computadores podem se citadas como as principais portas de entrada dos hachers.
Este artigo descreve estas técnicas ofensivas e as correspondentes ferramentas e procedimentos para minimizar as perturbações e salvaguardar a continuidade no fornecimento de energia elétrica. É importante saber que o sistema nunca será totalmente seguro, então a constante vigilância é necessária para se obter uma maior confiabilidade o sistema.
São analisados os ataques e defesas para proteção da rede e dos equipamentos inerentes ao sistema. É dado ênfase principalmente principalmente nas posturas de defesa, conhecendo melhor as ferramentas e técnicas de ataque (softwares e hardwares) para assegurar um acesso confiável. Autenticação de usuário, encriptamento, modems seguros, firewalls, VPN (Virtual Private Network) são alguns dos métodos empregados para tornar o sistema seguro e confiável.
Imagine o que um invasor pode fazer se conseguir acesso aos equipamentos de proteção, controle e até mesmo ao SCADA (Supervisory Control and Data Acquisition), imagine o prejuízo que pode ser dado por estes “usuários” maliciosos.
Trata-se sim de mais uma preocupação que os administradores destes sistemas tem que ter e saber combatê-las.
As facilidades de ferramentas para os hackers tornam as subestações ainda mais vulneráveis. Na própria Internet não é necessário gastar muito esforço para encontrá-las. Felizmente existem também muitas ferramentas e técnicas para combater os ataques corriqueiros, porém é preciso usá-las e implantá-las antes que o caos chegue.

Muitas medidas para diminuir esta vulnerabilidade são disponibilizadas nos próprios equipamentos e muitas vezes sem nenhum custo para a empresa, basta ativá-las. Técnicas como senhas fortes de proteção; verificação de loggin; níveis de acessos nos relés, processadores de comunicação, UTR`s (Unidades Terminais Remotas), IHM (Interface Homem Máquina) e o próprio SCADA; condições de alarmes; controles redundantes; time-out, anti-virus, firewalls e sistemas de detecção de intrusos são um dos exemplos de técnicas e ferramentas muitas vezes disponíveis e não utilizadas pelo usuário.

2.0 VULNERABILIDADE NO ACESSO REMOTO A SUBESTAÇÕES

A configuração do sistema e seus pontos de acesso remotos criam vulnerabilidades que podem ser alvos para acessos ilegais. Na FIGURA 1 notamos uma variedade de acessos, tanto locais quanto remotos. Vejamos seus pontos fracos:

- Acesso ao modem via provedor de serviço de telecomunicação;
- Rede pública de computadores – Internet;
- Redes sem fio - Wireless;
- Rede privativa;
- Redes arrendadas – ATM e Frame relay.

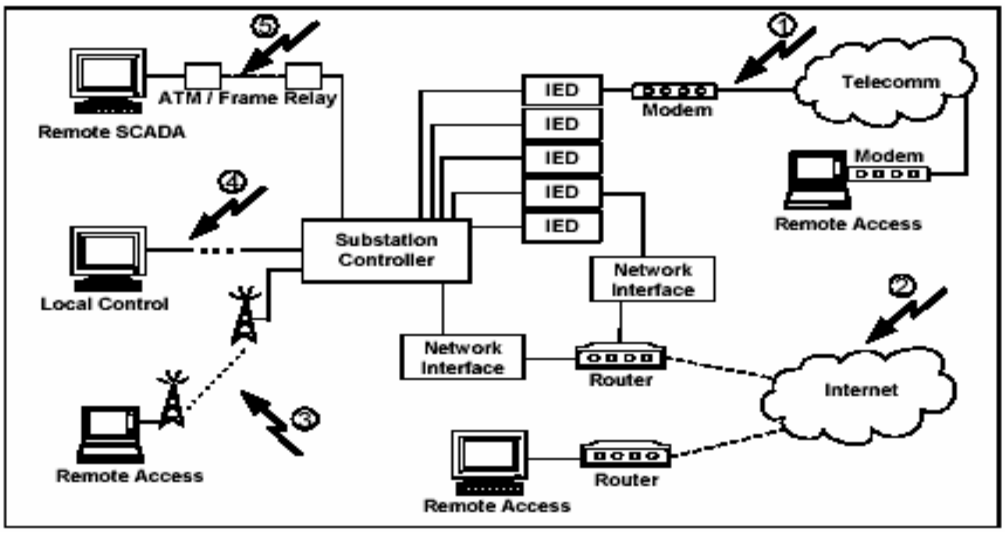

FIGURA 1 – Vulnerabilidades no Acesso Remoto em subestações

De fato, muitos IED`s (Intelligent Electronics Devices), controladores e o SCADA possuem características para gerenciar o acesso local e remoto através de senhas. Pensando nisto iremos iniciar nossa discussão com as tecnologias para autenticação e controle de acesso.

2.1 Restrição de Acesso e Autenticação de Usuário

A restrição de acesso e autenticação do usuário é a base de toda a segurança do sistema. A senha e a identificação pessoal são os meios mais comuns de restrição e de atribuição de responsabilidade ao acesso da rede. A senha é a primeira segurança e por isso deve ser bem escolhida. O nível ou camada de segurança é definido pelo software ou firmware, implementando a senha de controle. Se vários usuários possuem a mesma senha, então foi implantada uma técnica simples de restrição de acesso, perdendo a responsabilidade do usuário, pois seria impossível distinguí-lo precisamente. O ideal é que para cada usuário seja implantada uma senha.
As senhas não devem ser consideradas como único método de limitar acessos e autenticação de usuários. Autenticações eletrônicas via chaves de codificação pode ser também uma boa maneira de restringir acessos.
Muitos são os modelos de equipamentos de identificação de acesso e autenticação de usuários como distintivos (identifica sinais característicos), SmartCards, faixas magnéticas, código de barras, chips, impressão digital, scan de retina, voz, modelamento da face humana, dentre outras.
Três fatores são relevantes para autenticação:

1- Alguma coisa você sabe;
2- Alguma coisa você tem;
3- Alguma coisa você é.

Para o acesso remoto, o equipamento local envia a autenticação para um servidor remoto de autenticação, verificando a legitimidade do acesso, habilitando ou não o suposto usuário.
Segue abaixo alguns equipamentos de autenticação:

- Aproximação de distintivo
- Gerador aleatório de números
- Botões inseridos ao vestuário
- Scaner

Os preços destes equipamentos podem variar de poucas centenas a milhares de dólares.

2.2 Senhas

A senha é uma ferramenta primordial para segurança do sistema. Um grande esforço é despendido pelo hacker para descobrir uma suposta senha. E eles contam com diversos programas de computadores capazes de gerar milhares de senhas comumente usadas.
As senhas geralmente são descobertas de duas formas: por hackeamento ou por crackeamento. Senhas hackeadas são litaralmente roubadas fisicamente ou eletronicamente. Muitos são os artifícios usados pelos hachers como a engenharia social onde tais criminosos se disfarçam desde consultores de redes a faxineiros para conseguirem informações a respeito do sistema operacional e até mesmo obter senhas em latas de lixo. Um outro método utilizado é através de e-mails atrativos que exigem cadastramento do indivíduo. Existe uma estatística mostrando que 10% das pessoas que recebem estes e-mails realmente se cadastram e 10% dos que se cadastram usam o mesmo loggin e senha para tudo. Um outro meio de se obter tais senhas é através de funcionários e ex-funcionários insatisfeitos. As senhas crackeadas são obtidas através da decodificação das mensagens onde o cracker utiliza de programas específicos para tais finalidades.
A FIGURA 2 mostra um software típico de crackeamento.

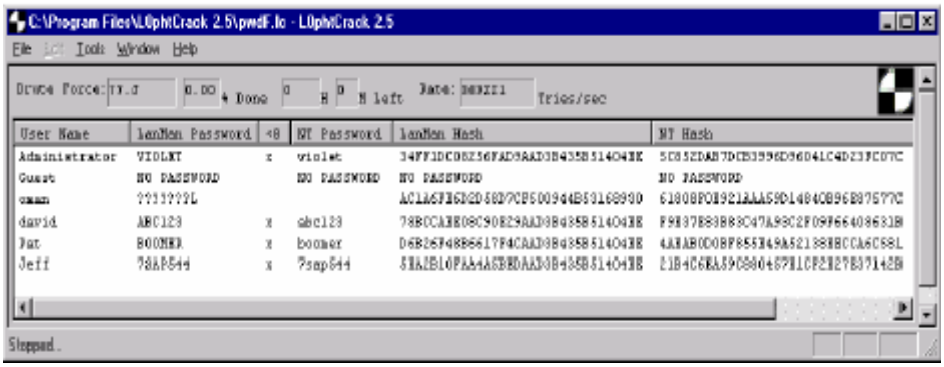

FIGURA 2 - Software de Crackeamento

Todo expert em segurança de rede concorda que uma senha segura é a melhor forma de defesa contra invasores de todas as formas. Uma boa senha assegura a integridade do sistema e aumenta a confiabilidade nas operações do SCADA. Por este motivo as senhas defalt dos equipamentos devem ser trocadas e estas não devem ser baseadas em fatos comuns à comunidade, datas ou relacionados a cultura popular. Uma senha forte consiste de seis ou mais caracteres, mesclando numerais e alfabéticos sem que formem nome, data, acrônimos etc.
Exemplos de senhas fortes:

H1g54Ua 4Pvf6C S1b5t8 C1ePr7E

Porém apenas uma senha forte não é razão para se descuidar do sistema. Estas senhas devem ser mudadas periodicamente.
Vários equipamentos presentes nas subestações estão implementados com funções de desconexão automática para um certo número de tentativas de senhas erradas ou ainda time-outs onde após um certo período de inatividade entre o usuário e equipamento será necessário entrar novamente com a senha de acesso para ter condições de operações ou modificação no IED. Certas medidas como estas podem proteger em até 100 anos contra constantes ataques.
Segue abaixo uma lista de recomendações para manter uma senha segura:

- Senha de seis ou mais caracteres (Case-sensitive);
- Teste o sistema com os softwares utilizados para crackeamento;
- Troque periodicamente as senhas;
- Mantenha a senha em lugar seguro. De preferência, na mente;
- Limite o número de senhas incorrtetas;
- Estabeleça um time-out por inatividade da comunicação.

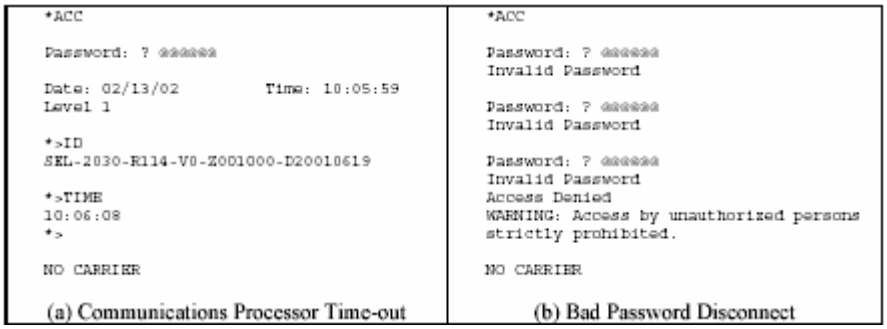

FIGURA 3 – Time-outs e Desconexão de Acesso em Processadores de Comunicação

2.3 Modem

Os hackers utilizam programas específicos que discam automaticamente para centenas ou milhares de números telefônicos observando se algum modem atende. Quando tal software consegue a resposta de algum dos modems discado o hacker é notificado ou simplesmente armazena o número em uma lista de possíveis alvos para futuros ataques.
Para evitar possíveis transtornos, algumas atitudes podem ser bastante oportunas:

- Escolha modems que exijam autenticação e controle de acesso;
- Use senhas fortes e seguras nos modems;
- Use time-outs de comunicação e desconexão por número de senhas erradas;
- Prefira modems que possam criptografar as mensagens;
- Teste o sistema com softwares de ataque.

2.4 Redes Públicas

Um dos pontos mais importantes a se lembrar quando se abre uma seção na Internet é que estamos abrindo uma porta de entrada para possíveis invasores, a menos que sejam criadas barreiras restringindo o acesso e codificando as mensagens.
A rede pública -Internet- não foi criada com a pretensão de oferecer o mínimo de segurança nos dados e também não se cogitava em utilizá-la como meio para intercambiar dados entre SCADA e subestações. Felizmente existem ferramentas para salvaguardar o sistema elétrico de controle, proteção e supervisão.
Hackers experientes raramente atacam diretamente de seus próprios computadores. São utilizados servidores de e-mails anônimos com sites obscuros e redes onde os endereços IP's permanecem dissimulados ficando difícil de identificar o invasor. Os hackers camuflam seus rastros através de varias camadas do computador invadido. Uma vez escondido o rastro dar-se-á início ao ataque com:

Ping Sweep - onde vários pings são enviados para vários computadores aguardando a resposta de um endereço ativo;
Trace Router – ferramenta que mostra o roteamento desde o computador de origem até o computador de destino;
Port Scan - determina o tipo de porta, em determinado micro-computador, está vulnerável para ser atacado. Algumas destas ferramentas mensuram até o nível de dificuldade de invasão;

Após determinar a rota do alvo, o sistema operacional e alista de portas vulneráveis, basta definir o melhor ataque. Hoje algumas ferramentas são utilizadas para suprir a deficiência de segurança da Internet tais como SDI (Sistema de detecção de intruso), vírus scanners, firewalls e VPN's (Virtual Private Networks).
Abaixo segue algumas recomendações para assegurar a continuidade do sistema de supervisão e controle:

- Use senhas fortes e seguras;
- Use time-outs de comunicação e desconexão por número de senhas erradas;
- Troque a senha padrão dos equipamentos;
- Use Port Scanners para verificar a vulnerabilidade das portas;
- Use Ping Sweepers para encontrar endereços IP's não autorizados ou esquecidos dentro do domínio do sistema;
- Use farejadores (Sniffers) ou trace routers para verificar a facilidade de localização do SCADA na rede pública;

- Utilizar sempre que possível Switches ao invés de Hub. As mensagens nos Switches são direcionadas a uma porta específica, já no hub, todos que estão conectados nele “escutam” as mensagens trocadas entre dois equipamentos na rede;
- Eliminar portas não utilizadas na rede, bem como contas de usuários;
- Habilite na rede a segurança de sites e as restrições através de firewalls;
- Use VPN’s para encriptar as mensagens;
- Use IDS, vírus scanners;
- Adote níveis de responsabilidade para o usuário, identificando todo o log de operações exercidas a cada acesso diário.

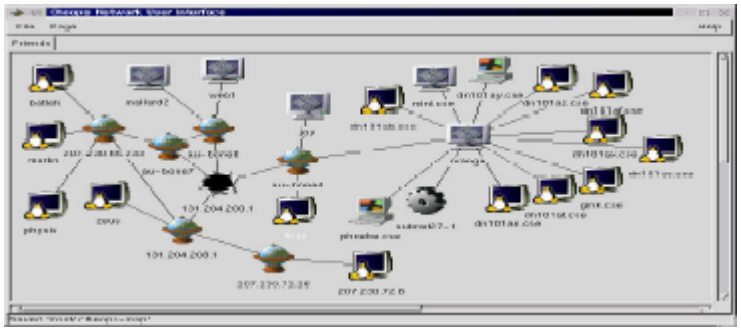

FIGURA 4 – Software de Roteamento

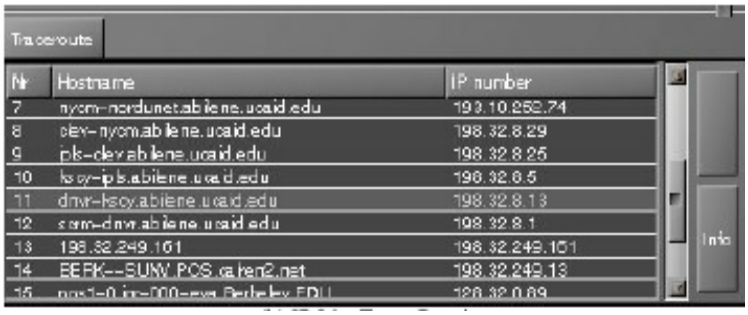

FIGURA 5 – Lista de Endereços Rastreados por Software Trace Router

2.5 Redes sem Fio (Wireless)

O nível de segurança das redes sem fio em relação as públicas é maior, pois os fabricantes incorporam aos seus equipamentos características de segurança. Os padrões wireless mais utilizados hoje são bluetooth e IEEE802.11. Ambos trabalham com speed-spectrum. Satélite e microondas são tipicamente os meios de transmissão mais seguras que os rádios. A maioria dos fabricantes comercializa wireless roteadores e modems com firewalls e VPN’s. Entretanto estas funções de segurança são desativadas por defalt e necessitam ser ativada logo que inseridas ao sistema.
Recomendações para salvaguardar uma rede wireless:
- Assuma que sua rede wireless é uma rede publicas, pois então siga todas os cuidados de uma rede Internet;
- Habilite todos as características de segurança do equipamento;
- Use ferramentas como o sniffer para verificar se o encriptamento está sendo otimizado e se as contas e senhas estão obscuros para a rede;
- Use firewalls e VPN’s sempre que possível.

2.6 Redes Privadas

Redes privativas são as mais seguras das redes citadas, porém não possui 100% de segurança e devemos tomar os devidos cuidados citados neste paper. As vezes o inimigo faz parte da rede como os próprios funcionários ou usuários de empresas terceirizadas e visitantes. Todas as considerações com relação a segurança devem ser utilizadas, não subestimando as ações internas.

- Tenha em foco que eventualmente pode-se ter problemas com intrusos. Implemente controle de acesso;

3.0 CONCLUSÃO

As modernas arquiteturas dos sistemas de controle e proteção das subestações assemelham-se bastante com as rede de computadores tanto em suas facilidades quanto em seus problemas. E é justamente com os problemas que devemos nos preocupar. A vulnerabilidade do sistema do sistema pode ser minimizada com técnicas, muitas vezes simples e ferramentas disponíveis no mercado. A FIGURA 6 mostra um exemplo de um sistema de comunicações seguro para uma suposta subestação.

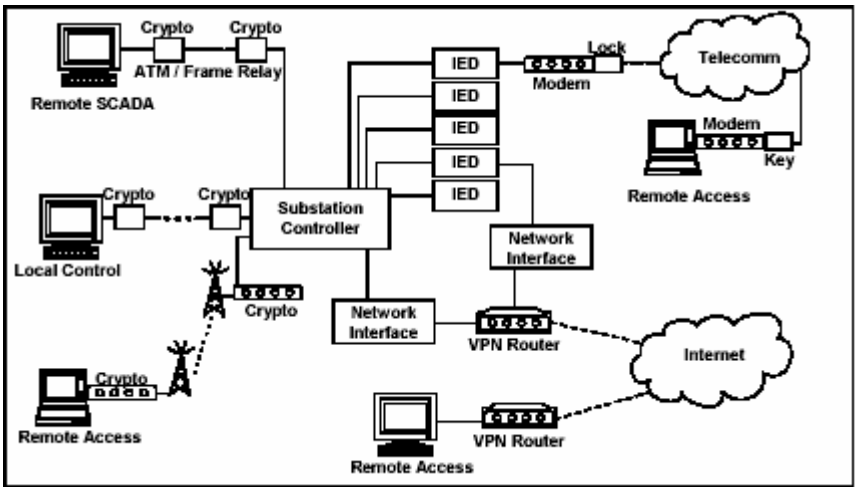

FIGURA 6 – Segurança na Comunicação em Subestações

No Brasil ainda se dá pouca importância à segurança do sistema elétrico. As senhas defalts dos equipamentos, na maioria das vezes, não são trocadas; SCADA's sem autenticação.
Um sistema seguro é um sistema onde temos boas técnicas, ferramentas e não podemos esquecer de um ótimo especialista em segurança.
Devemos nos antecipar, sempre que possível, aos ataques. De que adianta equipamentos com altíssima tecnologia, grandes MTBF's se o sistema está susceptível a invasões em vários pontos.

4.0 Referências Bibliográficas

(1) Paul W. Oman. Tools for Protecting Electric Power Systems from Electronic Intrusion. Pullman, WA USA.

(2) Dave Dolezelek, Secure SCADA and Engineering Access Communication. Pullman, WA USA.

(3) Ulbrich, Henrique Cesar, Universidade do Hacker. Brasil