Preocupações a Respeito de Invasões em Controladores de Acesso Remoto Instalados em Subestações e Sistemas SCADA

Paul Oman e Edmund O. Schweitzer, III
Schweitzer Engineering Laboratories, Inc.

Deborah Frincke
University of Idaho

Apresentado na
55th Annual Georgia Tech Protective Relaying Conference
Atlanta, Georgia
2–4 de maio de 2001

Apresentado previamente na
V Simposio Iberoamericano Sobre Proteccion de Sistemas Electricos de Potencia,
novembro de 2000

Originalmente apresentado na
27th Annual Western Protective Relay Conference, outobro de 2000

Traduzido para o português em agosto de 2017

PREOCUPAÇÕES A RESPEITO DE INVASÕES EM CONTROLADORES DE ACESSO REMOTO INSTALADOS EM SUBESTAÇÕES E SISTEMAS SCADA

Paul Oman and Edmund O. Schweitzer, III
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

Deborah Frincke
University of Idaho,
Moscow, ID USA

RESUMO

Neste artigo, identificamos as ameaças a controladores de subestações e sistemas SCADA e discutimos mecanismos de mitigação para reduzir a vulnerabilidade às invasões eletrônicas maliciosas. O Instituto Nacional de Padrões e Tecnologia dos Estados Unidos relaciona nove ameaças ao comércio eletrônico na América do Norte. Seis dessas ameaças são pertinentes particularmente aos sistemas SCADA e pelo menos quatro são relevantes para os controladores de subestações elétricas. A maior dependência em relação aos sistemas de controle automáticos com acesso remoto (via telefone ou internet) e a crescente economia mundial têm expandido o número de atacantes potenciais com acesso a controladores de subestação e sistemas SCADA e, portanto, ampliado o risco a que as concessionárias de energia elétrica estão expostas em termos de sabotagem e espionagem. Estima-se que a espionagem industrial e estrangeira na América do Norte tenha aumentado em mais de 260% na última década e o governo americano tem reconhecido que outros países têm nacionalmente patrocinado esforços de guerra de informação dirigidos contra o comércio norte-americano.

A indústria das concessionárias precisa estar ciente dessas ameaças aos seus sistemas e tomar providências para reduzir o risco e mitigar as vulnerabilidades. Os projetistas de relés de proteção e provedores de serviços auxiliares devem usar mecanismos que minimizem a probabilidade de que pessoas com intenções hostis possam degradar ou destruir os sistemas de potência. As políticas de produto, projeto e segurança no âmbito corporativo são ferramentas para identificar as vulnerabilidades, avaliar o risco e implementar mecanismos de mitigação. Muitos dos riscos envolvendo controladores em rede e sistemas SCADA são similares aos que afetam os tradicionais sistemas de computadores baseados em redes. Daí, a implementação de políticas de segurança para controladores de subestações e sistemas SCADA pode tirar proveito de lições aprendidas com a segurança de computadores e redes comerciais. As tradicionais soluções para reduzir a vulnerabilidade incluem técnicas tais como proteção de senha, registro de auditagem, níveis de acesso em diferentes camadas, condições de alarme, configuração e autenticação automáticas de IED, controladores redundantes, parâmetros de comunicação de tempo espera, proteção contra vírus, paredes corta-fogo e sistemas de detecção de intrusos. Esses e outros mecanismos para salvaguarda dos controladores de subestação e sistemas SCADA são discutidos neste artigo.

1. INTRODUÇÃO

Embora a destruição física ainda seja a grande ameaça à rede de energia elétrica da América do Norte, a ameaça de invasões e ataques a sistemas de computadores eletrônicos é crescente e precisa ser enfrentada pela indústria de energia elétrica [1, 2, 3]. Em um relatório para a Casa Branca, intitulado "Avaliação dos Riscos à Energia Elétrica", o Comitê de Assessoramento de Telecomunicações da Segurança Nacional (NSTAC) constatou que os desastres naturais e os ataques físicos constituem o principal dano à rede de energia elétrica, porém que a "segurança das redes de controle de energia elétrica representa um risco emergente importante para a rede de energia elétrica" [2]. Os fatores que influenciam a

probabilidade de invasões físicas e eletrônicas são variados e incluem parâmetros tão diversos quanto condições econômicas, localização da subestação, estéticas da edificação e paisagísticos, conflitos trabalhistas, usos de propriedades adjacentes, curiosidade e ignorância, instabilidade civil e política e o uso conjunto de instalações [1]. A literatura recente é consistente na alegação de que a ameaça de invasão por meios eletrônicos está aumentando devido a diversos fatores sociais, políticos e tecnológicos:

1. A mudança de sistema de controle de computadores baseados em *mainframe* patenteados para sistemas distribuídos, utilizando protocolos e padrões abertos e a expansão da utilização de protocolos públicos para interconectar redes que anteriormente eram isoladas.
2. As pressões dentro da indústria visando "downsize", eficiência, automação e corte de custos para manutenção de margens de lucros.
3. Requisitos FERC 888 e 889 para proporcionar acesso livre a informações do sistema de transmissão.
4. Maior acesso e interconectividade a locais remotos através da utilização de modems de discagem e da Internet.
5. Instabilidade no mercado de trabalho das concessionárias de energia elétrica, causado por competição e desregulamentação.
6. Aumento de incidentes de terrorismo internacional e doméstico dirigidos contra a América do Norte.
7. Aumento do número de países com iniciativas de guerra de informação patrocinadas por governos estrangeiros.
8. Rápido aumento de população treinada para utilizar computadores.
9. Larga disponibilidade de bibliotecas de ferramentas para hackers.

Na comunicação da Casa Branca sobre a proteção à infra-estrutura crítica [3], os fatores acima foram identificados como uma nova mistura poderosa, capaz de prejudicar a rede elétrica porque "enquanto os recursos necessários para conduzir um ataque físico não se alteraram muito recentemente, os recursos necessários para conduzir um cyber-ataque são agora lugar comum".

Quando vistos como um todo, esses fatores aumentam dramaticamente o risco de invasões das redes de energia elétrica de todas das nações industrializadas através de computadores. Além disso, esses mesmos fatores, combinados com crescentes demandas globais e maior necessidade de energia de qualidade mais elevada, têm criado uma rede de energia elétrica mais frágil, ao invés do sistema robusto e confiável que é necessário para proteger as infra-estruturas críticas [4, 5]. Felizmente, (e infelizmente) muito dos riscos envolvendo IEDs em rede, Controladores e sistemas SCADA são similares aos que afetam os sistemas de computadores tradicionais baseados em redes. Neste artigo, identificamos ameaças específicas e discutimos mecanismos de mitigação para redução da vulnerabilidade diante das ações maliciosas. Utilizamos definições e fraseologia nominais da literatura de segurança da computação, sendo que a única diferença é que são utilizados os termos "invasão eletrônica" e "ataque eletrônico" ao invés dos termos mais comuns "cyber invasão" e "cyber ataque". Fazemos isso para manter consistência com a Norma IEEE que regula a segurança nas subestações [1], a qual define a *invasão eletrônica* como:

> *"Entrada na subestação através de linhas telefônicas ou de outros meios baseados na eletrônica, visando a manipulação ou perturbação de dispositivos eletrônicos. Esses dispositivos incluem relés digitais, registradores de perturbações, equipamentos de diagnóstico, equipamentos automáticos, computadores, PLC e interfaces de comunicações."*

Até esta data, não há registro de qualquer caso documentado de invasões eletrônicas ou ataques, causando desligamentos ou danos à rede de energia elétrica, porém tem havido casos onde os hackers visavam as concessionárias elétricas [2, 6]. O relatório do NSTAC cita três desses incidentes:

1. Hackers atacaram os sistemas de negócios e informação de concessionárias de energia elétrica.
2. Um grupo ambiental radical foi pego tentando invadir o sistema de informação de uma concessionária.
3. No Texas, um ex-empregado insatisfeito colocou uma nota num jornal de *Hackers* informando que tinha suficiente informação para atacar eletronicamente a rede de energia elétrica.

A extensão do problema de invasão eletrônica, até o momento, é desconhecida porque poucas empresas estão operando sistemas de detecção de invasão e um número menor ainda está reportando as invasões. Um estudo citado pelo relatório NSTAC constatou que apenas 25% das empresas concessionárias utilizam qualquer tipo de sistema de detecção de invasão eletrônica e um estudo do FBI citado no mesmo relatório constatou que menos de 17% de um grupo de 428 empresas pesquisadas disseram que reportariam incidentes de invasão. Essa falta de interesse em reportar é consistente com a rede bancária e as empresas de telecomunicações, onde a maioria das empresas não informa sobre invasões por temor de publicidade negativa e de perder a confiança dos clientes.

Essas conclusões sugerem que IEDs, Controladores e sistemas SCADA, remotamente acessíveis – e mais importante, subestações controladas por esses dispositivos – são vulneráveis a ataques eletrônicos. Os invasores físicos costumam "abrir válvulas, apertar botões, e operar disjuntores, religadores e chaves" [1], de modo que se julga que os invasores eletrônicos fossem fazer a mesma coisa. Por causa da natureza das atividades e sistemas controlados por dispositivos eletrônicos nas subestações, a utilização incorreta desses dispositivos poderia apresentar conseqüências desastrosas, capazes de levar à perda de vidas e/ou patrimônio. A indústria da energia elétrica precisa enfrentar e minorar esses riscos.

Em resposta à avaliação de riscos de 1997, documentos da Casa Branca pediram aumento da vigilância e financiamento de pesquisas e desenvolvimento de soluções tecnológicas para o problema [2, 3]. Mais recentemente, a IEEE e o FBI entraram em ação para atender a este desafio. A Norma IEEE 1402-2000, "*Guide for Electric Power Substation Physical and Electronic Security*", discute mecanismos para aliviar os riscos e pede maior vigilância e o treinamento em segurança de redes [1]. Ela conclui:

> *"A introdução de sistemas de computadores com acesso on line à informação da subestação é significativa no aspecto em que os sistemas de proteção, controle e coleta de dados de relés da subestação podem ficar expostos às mesmas vulnerabilidades como todos os outros sistemas de computadores. Na medida que aumenta a utilização de equipamentos de computação no ambienta da subestação, a necessidade de sistemas de segurança para prevenir invasões eletrônicas poderá se tornar ainda mais importante."*

Em outra frente, o FBI e o North American Electric Reliability Council (NERC) trabalhariam em conjunto para formar o "Sistema de Indicações e Advertência de Energia Elétrica" do Centro Nacional de Proteção à Infra-estrutura (NIPC) para ajudar as concessionárias com queixas sobre incidentes e ações legais [7]. Em seu testemunho perante a audiência do Comitê Judiciário do Senado sobre cyber crimes, Michael Vatis, Diretor do NIPC, disse que a sua organização seria o "portal de uma rede nacional de alerta projetada para reagir rapidamente contra cyber ataques visando os controles informatizados do sistema elétrico de potência da América do Norte."

Todas as organizações empenhadas no estudo do problema concluem que uma maior conscientização e que mais treinamento são necessários dentro da indústria para mitigar o problema, evitando que a rede de energia elétrica possa ser comprometida. Neste artigo, respondemos à chamada para maior conscientização e capacitação, enumerando os riscos para os IEDs, Controladores e Sistemas SCADA, remotamente acessáveis, utilizados pelas empresas de energia elétrica, e discutindo como mitigar esses riscos. A seção seguinte relaciona ameaças para as empresas de energia elétrica. Na Seção 3, apresentamos um exemplo de cenário de ataque. Seção 4 demonstra o valor de forte proteção de senhas. As Seções 5, 6 e 7 proporcionam mecanismos de alívio e sugestões para salvaguardar equipamentos de computação das subestações, estações de controle e ambientes de TI. E, finalmente, as conclusões pedindo uma atitude proativa da parte das empresas de energia elétrica são apresentadas na Seção 8.

2. AMEAÇAS A IEDS, CONTROLADORES, SISTEMAS SCADA E REDES CORPORATIVAS

As comunicações da Casa Branca sobre proteção à infra-estrutura crítica relacionam dez ameaças a concessionárias [3], enquanto o manual NIST sobre segurança na informática identifica nove ameaças ao Comércio Americano [8] e a norma da IEEE sobre proteção a subestações relaciona nove ameaças de invasão [1]. A Tabela 1 é um compêndio dos tipos de ameaças identificadas em cada documento.

Tabela 1. Ameaças a Subestações e Redes de Computadores

NIST 1994	Casa Branca 1997	IEEE 2000
Física e Infra-estrutura	Eventos e Acidentes Naturais	Desastres Naturais
Ameaças à Privacidade Pessoal	Danos Físicos Acidentais	Condições Econômicas
Erros e Omissões	Equívocos, Erros e Omissões	Curiosidade e Ignorância
Empregados Insatisfeitos	"Insiders"	Conflitos Trabalhistas
Hackers Maliciosos	Hackers Recreativos	Agitação Civil/Política
Código Malicioso	Atividade Criminosa	Localização
Espionagem Industrial	Espionagem Industrial	Uso de Propriedade Adjacente
Espionagem Estrangeira	Terrorismo	Estética
Fraude e Roubo	Inteligência Nacional (Estrangeira)	Instalações de Uso Comum
	Guerra de Informação	

Enquanto todas as ameaças listadas na Tabela 1 são de preocupação para os ambientes informatizados das concessionárias de energia elétrica ao nível empresarial, diversos desses itens são de preocupação específica para os ataques eletrônicos contra IEDs, Controladores e sistemas SCADA:

- *Equívocos, Erros e Omissões* – Esses incluem a configuração/reconfiguração acidental de dispositivos de proteção, e manutenção incorreta ou negligente de dispositivo ou rede que introduza vulnerabilidades significativas na segurança.
- *Fraude e Roubo, Atividade Criminosa* – Fraude e roubo eletrônicos estão crescendo em todo o país, com as perdas excedendo $123 milhões anualmente.
- *Empregados e "Insiders" insatisfeitos* – Esses podem inserir configurações erradas, plantas bombas lógicas, inserir dados incorretos, travar sistemas, alterar ou apagar dados e seqüestrar dados.

- *Curiosidade e Ignorância, Hackers Recreativos e Maliciosos* – embora os prejuízos correntes devidos a ataques de hackers sejam significativamente menores do que as perdas devidas aos "insiders", o problema com os hackers é indiscriminado e crescente.

- *Espionagem Industrial* – Informação roubada inclui dados sobre preços, processos de fabricação, especificações de desenvolvimento de produtos, pesquisa básica, planos estratégicos, posições de negociação e dados de contratos. Em 1999, as perdas por espionagem na informática excederam $60 milhões [9].

- *Código Malicioso* – O número de vírus conhecidos está crescente exponencialmente, incluindo vírus, worms, cavalos de Tróia e bombas lógicas.

- *Espionagem Estrangeira e Guerra da Informação* – Numerosos países dispõem de capacidade de guerra da informação patrocinada nacionalmente, algumas delas explicitamente dirigidas contra o governo e o comércio americanos.

Uso indevido envolvendo um IED, Controlador ou Sistema SCADA pode ocorrer em muitos recintos: na empresa, em trânsito ou *in situ*. Por exemplo, *Erros e Omissões* comprometeriam a estabilidade de TI na empresa, *Empregados e Insiders Insatisfeitos* poderiam violar produtos em trânsito e *Hackers Maliciosos* podem invadir um IED, Controlador ou sistema SCADA in loco. Todas essas ameaças são riscos distintos para a confiabilidade e integridade da empresa de energia elétrica. Além do mais, com maior automação vem a crescente interdependência de infra-estruturas críticas. Por exemplo, o ataque de um hacker adolescente ao sistema telefônico de Worcester, MA, em 1997, não somente cortou o serviço telefônico de 600 residências, porém efetivamente fechou a torre de controle do aeroporto local, serviço de meteorologia, rádio transmissores, e luzes de balizamento da pista do aeroporto, que são comandadas por aqueles transmissores [10]. Daí, a grande preocupação quanto ao dano potencial que poderia ser causado pelos indivíduos mais profissionais, mais maliciosos e melhor treinados que a gente sabe que existem por aí.

Embora o mau uso pode certamente ocorrer por acidente, neste artigo enfocamos situações envolvendo um indivíduo ou indivíduos que possam se sentir motivados para "atacar" ou utilizar indevidamente um relé de proteção, controlador ou dispositivo SCADA. As motivações desses indivíduos são variáveis:

- **Hacking**: alguns intrusos entram em sistemas *simplesmente porque podem entrar*. O "hacker" relativamente benigno é muitas vezes motivado pela curiosidade ou pelo desafio da exploração, sem uma intenção aberta e maliciosa. Outros são vândalos por natureza, com a intenção de adquirir notoriedade ou causar danos. Os hackers de uma ou outra variedade podem ser "insiders" ou estranhos.

- **Espionagem**: A possibilidade de adquirir vantagem industrial ou política é um grande incentivo para coleta de informações, através de meios tanto legais quanto ilegais. Os "insiders" – e estranhos que ganham acesso ao interior – podem estar envolvidos em espionagem ilegal, mediante a aquisição e distribuição de informação confidencial. Porém, os estranhos também podem ganhar informação valiosa através do exame de informação pública tal como páginas da Internet, descrições de produtos e literatura promocional. Portanto, mesmo quando uma organização não está preocupada com a espionagem interna, é importante tomar precauções com relação aos tipos de informação que são publicadas.

- **Sabotagem**: Os motivos para sabotagem freqüentemente estão enraizados nos desejos de ganho pessoal, econômico ou político. dependendo da causa da raiz e das oportunidades disponíveis para o sabotador, as conseqüências da sabotagem podem ser a destruição da estrutura organizacional inteira e/ou perda de fração de mercado. "Hactivismo" é uma emergente forma de sabotagem onde os hackers violam e

descaracterizam recursos de TI corporativos (por exemplo, páginas na Web) em nome de alguma causa radical.

- **Vandalismo**: Há muitas motivações possíveis para o vandalismo – a destruição de patrimônio valioso sem o ganho pessoal – e algumas delas são similares a aquelas de outras categorias (particularmente sabotagem). No entanto, o vandalismo deve ser tratado separadamente da espionagem e da sabotagem, porque é tipicamente indiscriminado, aleatório e relativamente localizado. Ou seja, as conseqüências de longo prazo do vandalismo são usualmente muito menos severas do que as espionagem e sabotagem. O vandalismo é primariamente associado a estranhos.

3. VULNERABILIDADES, AMEAÇAS, ATAQUES E RISCOS

O relatório de avaliação de riscos do NSTAC concluiu que as subestações de energia elétrica constituíam "a vulnerabilidade de segurança da informação mais significativa dentro da rede de energia elétrica", principalmente porque os dispositivos remotamente acessíveis utilizados dentro das subestações são em grande parte desprotegidos contra invasão. Os autores do relatório também reconheceram que ataques eletrônicos poderiam resultar em perturbação em larga escala do abastecimento de energia em níveis regionais e mesmo nacionais durante até 24 horas. O elo fraco que permite esses resultados são as linhas de comunicações publicamente acessíveis existentes entre subestações, centros de controle e redes de computadores corporativas. E não são apenas os Controladores e Sistemas SCADA que estão sob risco – todos os dispositivos eletrônicos utilizados para monitorar e controlar sistemas de potência são suscetíveis a invasões eletrônicas, incluindo IEDs, PLCs e RTUs. O relatório do NSTAC declara:

> *"Tanto as RTUs como os novos dispositivos automáticos (IEDs) estão sujeitos a ataque eletrônico. Discando para uma porta de um disjuntor digital, um engenheiro da concessionária pode reconfigurar o dispositivo ou selecionar qualquer dos seis níveis de proteção. Um invasor eletrônico ... poderia discar para uma porta não protegida e reconfigurar o disjuntor para um nível de tolerância mais alto do que o dispositivo a ser protegido pode suportar. Fazendo isso, seria possível fisicamente destruir um determinado item de equipamento dentro de uma subestação. O invasor também poderia ajustar o dispositivo para que se tornasse mais sensível do que as condições para operação normal e fazer o sistema desligar para auto proteção."*

Para fins ilustrativos, agora faremos um breve exame de um exemplo de subestação com acesso remoto via modem discado ou conexão LAN/WAN através das linhas de comunicações públicas. Figura 1 mostra os pontos de acesso eletrônico (vulnerabilidades) na configuração de uma subestação hipotética.

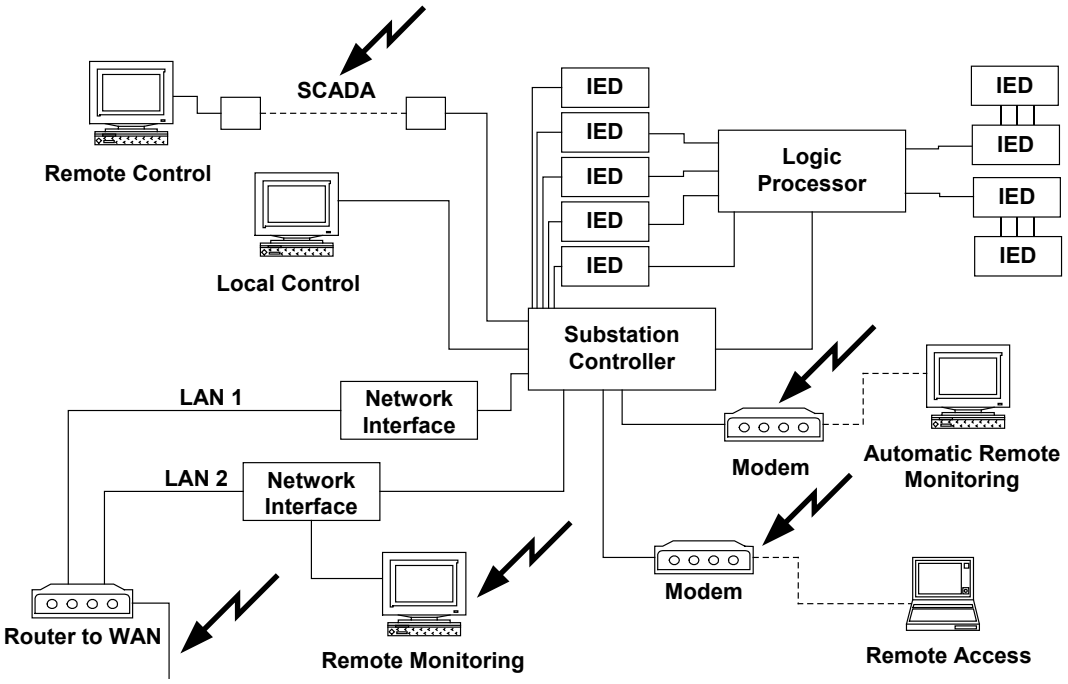

Figura 1. Pontos de Vulnerabilidade a Invasão Eletrônica

A *vulnerabilidade* neste cenário é o acesso público às linhas de comunicação que entram e saem da Subestação. A *ameaça* é a invasão maliciosa e/ou espionagem. O *ataque* se desenvolve aproximadamente deste modo:

1. Utilizando um discador especial, o invasor potencial escaneia centenas de números de telefone acima e abaixo dos números de telefone publicamente disponíveis da empresa, procurando modems que atendem a ligações.

2. Alternativamente, o invasor poderia utilizar um programa "ping sweep" para varrer vários milhares de endereços IP acima e abaixo do endereço IP publicamente disponível da concessionária.

3. Quando uma conexão provável é encontrada, múltiplos retornos, pontos de interrogação, "HELP" e "HELLO" (Alô) são inseridos para testar a conexão e procurar pistas sobre o tipo de conexão.

4. Assim que um diálogo é estabelecido, o invasor utiliza a *engenharia social* para determinar a informação de login, ou lança um ataque de senha *baseado em dicionário* ou em *força bruta*.

5. Quando a conexão é completada e o invasor está "dentro" do IED, Controlador ou sistema SCADA, qualquer das seguintes atividades poderia ser realizada:

    a. Desligar a subestação ou qualquer parte do subsistema controlado pelo dispositivo comprometido, tanto imediatamente quanto de maneira retardada.

    b. Alterar configurações para inibir ou degradar a funcionalidade de qualquer parte do subsistema controlado pelo dispositivo de modo tal a comprometer a confiabilidade da SE.

    c. Coletar dados que possam ser utilizados posteriormente para lançar ataques subseqüentes com intenção de executar o desligamento ou degradação mencionado acima.

d. Alterar (perturbar ou poluir) os dados de modo tal a acionar uma ação imprópria pelo dispositivo.

e. Plantar instruções (código malicioso) que poderia posteriormente ser utilizado em um ataque retardado e coordenado.

Deste modo, os invasores eletrônicos podem ganhar acesso, alterar ajustes para causar degradação ou danos, e desaparecer – enquanto isto, mantendo um alto grau de anonimidade e não deixando virtualmente qualquer sinal quanto à natureza e a extensão do ataque.

4. A IMPORTÂNCIA DE SENHAS "DURAS"

É fato comum que a proteção através de senhas é falha e suscetível a ataques automáticos, porém a proteção de dispositivos através de senhas "duras" ainda é eficaz, porque serve para retardar o atacante, desta forma aumentando a probabilidade de que o ataque possa ser detectado e/ou o invasor desista do ataque e procure alvos mais fáceis. Isso é especialmente verdadeiro quando a proteção de senha é apenas um componente de um sistema integrado de proteção incluindo autenticação, restrição de acesso, detecção de intrusos, etc. Técnicas específicas para proteger sistemas de computadores são discutidas na seção seguinte; aqui nós demonstramos o valor da implementação de senhas "duras."

Definimos uma senha "dura" como a que contém seis ou mais caracteres, com pelo menos um caractere ou dígito especial e sensível à mistura de caixa de letras e que não forme um nome, data, acrônimo ou palavra pronunciável. As senhas formadas desta maneira são menos suscetíveis de ataques de dicionário, onde uma lista comum de palavras, siglas e nomes é utilizada em um ataque automático contra o controle de acesso. As ferramentas utilizadas para rodar esses ataques são facilmente disponíveis na Internet e são bastante fáceis de se utilizar. Não é incomum para os decifradores de senha rodar testes offline utilizando dicionários completos em diversas línguas diferentes – de modo que a utilização de uma palavra estrangeira não é adequado para proteção. A "advinhação", executada deste modo, tipicamente começa através da verificação de todas as palavras; em seguida, adicionando-se prefixos ou sufixos às palavras e depois combinando palavras curtas. Mesmo "duras" ou "endurecidas", as senhas continuam sujeitas a serem decifradas através das técnicas de "força bruta" e decodificação, porém esses processos exigem mais tempo e mais esforço do que os ataques com dicionário, assim reduzindo a probabilidade de um ataque bem sucedido.

A Tabela 2 mostra as diferenças entre os tempos de conclusão previstos para ataques de dicionário e ataques de "força bruta" contra senhas de 4, 6, e 8 caracteres em extensão. Os dados para o ataque de dicionário são baseados no dicionário de verificação de grafia Unix, de 25.143 palavras, contendo palavras, números acrônimos e nomes comuns. Senhas singulares de 4, 6, ou 8 caracteres eram geradas a partir do dicionário e lançadas em um script automático contra um Controlador típico de Subestação. O tempo para concluir o ataque é mostrado para cada uma das cinco velocidades de conexão, variando da velocidade de discagem comumente utilizada em Subestações, de 2400 bps até a velocidade nominal de acesso da Internet, de 10 Mbs. A 9600 bps, o ataque de 20.721 palavras pode ser lançado e completado em 3,5 horas – um tempo muito curto para deter um invasor eletrônico. Mesmo a 2400 bps, o ataque de dicionário contra uma senha de oito caracteres leva apenas 5,3 horas, o que ainda não constitui obstáculo sério para um hacker determinado.

Tabela 2. Diferenças de tempo entre Ataques a Senha com Métodos Dicionário e Força Bruta

Ataque	No palavras	2400 bps	9600 bps	19200 bps	38400 bps	10 Mbs
Dicionário						
4 caracteres	11.022	2,4 horas	1,9 horas	1,4 horas	1,3 horas	0,9 horas
6 caracteres	20.721	4,6 horas	3,5 horas	2,7 horas	2,5 horas	1,7 horas
8 caracteres	23.955	5,3 horas	4,0 horas	3,1 horas	2,9 horas	2,0 horas
Força Bruta						
4 caracteres	66.347.190	14.707 horas	11.168 horas	8.625 horas	7.961 horas	5.528 horas
6 caracteres	$5{,}3741 \times 10^{11}$	13.598 anos	10.326 anos	7.975 anos	7.361 anos	5.112 anos
8 caracteres	$4{,}3530 \times 10^{15}$	110.150.114 anos	83.647.831 anos	64.599.315 anos	59.630.136 anos	41.409.817 anos

Nota: As velocidades de ataque não são linearmente proporcionais às velocidades de comunicação devido aos estados de espera do processo de autenticação.

Dados para ataque "força bruta" são baseados nos cálculos do Departamento de Defesa (DOD) dos Estados Unidos sobre vulnerabilidades das senhas [11]. Embora mais antigos, os princípios incorporados nas diretrizes de gerenciamento de senhas do DOD são facilmente atualizados para as atuais velocidades de comunicação. O número de senhas possíveis com extensão de n caracteres é a permutação de caracteres C no conjunto total de caracteres tomados n de cada vez com a repetição permitida (por exemplo, "aaaa"):

$$P(C.n) = C^n$$

Por exemplo, alguns relés de proteção e controladores utilizam senhas de seis caracteres construídas a partir de um conjunto de caracteres do teclado típico. Este conjunto consiste de 52 caracteres de caixa alta e caixa baixa, mais 10 dígitos e 28 caracteres especiais. Assim, C = 90 e n = 6; assim para senhas de estritamente seis caracteres, há

$$P(90.6) = 90^6 = 531.440.000.000$$

possíveis permutações da senha. No entanto, mesmo a proteção de senha mais forte pode ser obtida permitindo *até seis* caracteres, dando permutações adicionais do conjunto da senha, especificamente

$$(C.1)+P(C.2)+P(C.3)+P(C.4)+P(C.5)+P(C.6)$$

$$= C^1+C^2+C^3+C^4+C^5+C^6$$

$$= \sum_{i=1.6} C^i = 537.410.000.000$$

Assim, há mais de 537 bilhões de senhas possíveis quando se permite uma extensão de um a seis caracteres em um conjunto de 90 caracteres. Utilizando os cálculos do DOD para o tempo previsto para "abrir" uma senha "dura" de extensões com quatro, seis e oito caracteres em um conjunto de 90 caracteres chega-se aos tempos mostrados na Tabela 2. Os dados mostram claramente que mesmo as senhas "duras" de quatro caracteres são significativamente mais fortes do que um nome, palavra, data ou acrônimo comum que tenha 8 caracteres.

5. MATRIZ DE VULNERABILIDADE DA SUBESTAÇÃO

Estabelecemos que o equipamento de proteção e controladores dentro das subestações, que os sistemas SCADA que conectam as subestações aos centros de controle, e que as redes de processamento de informações das concessionárias encontram-se sob risco de invasões eletrônicas. A vulnerabilidade, daí o risco, aumenta com a conectividade. Dessa forma, os dispositivos conectados às redes de comunicações públicas são os mais acessíveis para o maior grupo de pessoas e são, portanto, os que estão mais "em risco". Por exemplo, o uso de uma LAN/WAN Ethernet tem vulnerabilidades tradicionais inerentes para acesso e uso não autorizados (quando comparado com as conexões de linha privada, acesso discado e *wireless*); contudo, também existem mitigações tecnológicas conhecidas para estes mesmos problemas. A Tabela 3 mostra uma listagem de vulnerabilidades, riscos e estratégias de mitigação para dispositivos variando desde relés de proteção até redes de computadores.

Tabela 3. Matriz de Vulnerabilidade da Subestação e Rede de Computadores

Dispositivo	Vulnerabilidade	Risco	Mecanismo de Mitigação
Relés, IEDs, PLCs	• Acesso físico por pessoal autorizado ou não autorizado	• Equipamento de proteção acidentalmente configurado/reconfigurado • Equipamento de proteção deliberadamente configurado/reconfigurado por pessoa não autorizada	• Implementar controle de acesso via senha ou PIN IDs • Instruir engenheiros sobre importância de gerencia-mento de senha / PIN • Advogar uso de senhas "duras" na documentação e materiais de treinamento • Implementar controle de acesso de duas camadas "mostrar" vs. "configurar" • Confundir a extensão da senha[1]
Controladores não conectados às redes	• Acesso físico por pessoal autorizado ou não autorizado • Subsequente acesso ao equipamento de proteção conectado	• Controlador configurarado/reconfigurado acidentalmente ou deliberadamente • Equipamento de proteção configurarado/reconfigurado acidentalmente ou deliberadamente	*Os mecanismos de mitigação acima se aplicam.*
Controladores, RTUs, PCs e sistemas SCADA *conectados a linhas privativas*	• Acesso físico e eletrôni-co por pessoal autorizado ou não autorizado • Acesso subseqüente ao equipamento de proteção conectado	• Dispositivos de controle configurados/reconfigurados acidentalmente ou deliberadamente • Equipamentos de proteção configurados/reconfigurados acidentalmente ou deliberadamente	*Os mecanismos de mitigação acima se aplicam, mais:* • Emitir avisos de advertência de acesso[2] • Implementar funções de relatório automático para detectar quando as linhas estão sendo perturbadas

[1] Caracteres de máscara da senha devem exceder o comprimento máximo das senhas de modo que os invasores potenciais não possam limitar o seu esforço de deciframento de senhas a uma extensão conhecida.

[2] Declarações de advertência de acesso devem ser emitidos em cada tentativa de acesso; por exemplo, "Advertência: Uso não autorizado deste dispositivo é proibido por lei"

Tabela 3. Matriz de Vulnerabilidade da Subestação e Rede de Computadores - continuação

Dispositivo	Vulnerabilidade	Risco	Mecanismo de Mitigação
IEDs, PLCs, RTUs, Controladores e sistemas SCADA *conectados a modems*	• Número discado acessível via engenharia social ou "war dialer" • Controle de acesso driblado por ataque de senha • Acesso eletrônico por pessoal autorizado ou não autorizado • Acesso subseqüente ao equipamento de proteção associado	• Dispositivos de controle configurados /reconfigurados acidentalmente ou deliberadamente pelo invasor • Equipamento de proteção configurado /reconfigurado acidentalmente ou deliberadamente pelo invasor • Acesso não autorizado aos Controladores e SCADA	*As medidas de mitigação básicas são aplicáveis, mais:* • Emitir avisos de advertência sobre acesso[2] • Emitir desligamento após três tentativas com senha errada[3] • Usar modems "dial-back"[4] • Usar modems com codificação[5] • Usar cartões de autenticação com modems[6] • Criar hierarquia de acesso multicamadas (multi-sign-on)[7]
IEDs, PLCs, RTUs, Controladores e sistemas SCADA *conetados à rede pública*	• Endereço da rede acessável via engenharia social ou varredura automática (por exemplo, ping-scan) • Controle de acesso driblado pelo ataque à senha • Acesso eletrônico por pessoal autorizado ou não autorizado • Acesso subseqüente ao equipamento de proteção associado • Pacotes de dados não seguros • Endereço vulnerável a ataques "Serviço Negado" (DOS)	• Dispositivo de controle configurado/reconfigurado acidentalmente ou deliberadamente pelo invasor • Equipamento de proteção configurado/reconfigurado acidentalmente ou deliberadamente pelo invasor • Acesso não autorizado aos Controladores e SCADA • Pacotes de dados visíveis via Network Sniffer • Perda de funcionalidade causada por sobrecarga de solicitação de serviço (ataque DOS)	*As medidas de mitigação básicas são aplicáveis, mais:* • Emitir avisos de advertência sobre acesso[2] • Emitir desligamento após três tentativas com senha errada[3] • Implementar a autenticação do dispositivo de nível de aplicação[6] • Criar hierarquia de acesso multi-camadas (multi-sign-on)[7] • Implementar codificação dos dados em nível de pacote[8] • Implementar COTS IPSec[9] • Implementar Certificados PKI[10] *Sem mitigação para os ataques DOS.*

[3] As conexões devem ser encerradas na terceira tentativa de uso de senha errada no acesso.

[4] Modems do tipo "dial-back" (discar de volta) não são seguros, porém são menos inseguros do que os modems de simples resposta.

[5] Pelo menos até agora, não se sabe se os modems codificadores estão seguros contra intrusão de "dial back".

[6] Dispositivos de autenticação de hardware são fortes na segurança de discagem, onde IPSec ou PKI não forem seguros.

[7] Implementar diferentes senhas para cada nível de hierarquia do dispositivo.

[8] Implementar codificação de dados do software ou firmware entre os dispositivos de envio e recepção da rede.

[9] Implementar segurança de software/hardware do tipo COTS - Commercial Off the Shelf em cada extremidade da linha pública (por exemplo, SSL, VPN).

[10] Certificados Public Key Infrastructure (PKI) corretamente implementados permitem a autenticação, codificação e não rejeição da transmissão de dados.

Tabela 3. Matriz de Vulnerabilidade da Subestação e Rede de Computadores - continuação

Dispositivo	Vulnerabilidade	Risco	Mecanismo de Mitigação
Redes em nível corporativo conectadas a *redes públicas*	• Todas as vulnerabilidades tradicionais dos sistemas de computação são aplicáveis	*Todos os riscos acima são aplicáveis, mais:* • Roubo de informação e dados exclusivos • Roubo de informação e identificação pessoais • Roubo de números de cartões de crédito e informação de contas • Roubo de planejamento estratégico e especificações de desenvolvimento de produto	*As medidas de mitigação básicas são aplicáveis, mais mitigação para conexões à rede pública (diretamente acima), mais:* • Usar senhas vencidas pré-ajustadas para novas instalações[11] • Mudar senhas 3 a 4 vezes por ano[12] • Usar verificadores ativos de senhas para identificar e eliminar senhas fracas[13] • Implementar programas anti-vírus e atualiza-los regularmente • Implementar Sistemas de Firewall e de Detecção de Intrusos • Analisar logs de acesso e outros arquivos relevantes à segurança regularmente • Manter uma política definida de segurança de rede de computação em nível da Empresa

[11] Senhas com data de vencimento pré-definida, de modo a obrigar o cliente a ajustar as suas próprias senhas, dessa forma lhe atribuindo responsabilidade (e ônus) pelo gerenciamento de senhas.

[12] A Agência de Segurança Nacional dos Estados Unidos recomenda mudar senhas mensalmente ou trimestralmente.

[13] Programas que varrem arquivos de senhas no nível de sistema procurando se há senhas fracas (ou seja, "decifráveis") são facilmente disponíveis através da Internet.

6. SEGURANÇA DA REDE, PAREDES CORTA-FOGO (FIREWALLS) E SISTEMAS DE DETECÇÃO DE INTRUSOS

As modernas configurações de controladores de subestações e sistemas SCADA são essencialmente sistemas de dispositivos inteligentes distribuídos que se assemelham aos tradicionais sistemas de computação conectados em rede. Por causa do aumento da interconectividade das subestações e sistemas SCADA, e do crescente risco de acesso externo indesejado, é importante abordar todas as ameaças à rede tradicional associadas às comunicações remotas. Maneiras típicas de administrar essas ameaças envolvem a autenticação de parceiros de comunicação, uma maior segurança da conexão entre sites, a proteção da periferia virtual de um site e a identificação dos ataques, caso os mesmos passem pela periferia e penetrem na rede.

A autenticação de parceiros de comunicação para sistemas distribuídos ainda é primariamente baseada na sede, algumas vezes incrementada pela utilização de cartões inteligentes (geradores de senha de uma vez), ou tecnologias de Public Key Infrastructure (PKI). Os cartões inteligentes podem ser utilizados para fornecer diretamente informação de autenticação, e também como um meio de aumentar a informação de autenticação digitada por um usuário (por exemplo, chaves aleatórias ou "swipes" magnéticos). Uma grande vantagem da utilização da tecnologia do cartão inteligente para aumentar as senhas do usuário

é que a autenticação automática é válida somente durante um curto período de tempo antes que uma nova chave seja gerada. Normalmente, as senhas são transmitidas diretamente através de uma rede e podem ser capturadas por hardware ou software que estejam "ouvindo" na linha, e em seguida, reutilizadas posteriormente. As chaves de autenticação geradas pelos cartões inteligentes não são válidas durante por muito tempo após a transmissão original, o que torna improvável a reutilização subseqüente por um invasor.

Uma extensa discussão a respeito da codificação de chave publica PKI está fora do escopo deste trabalho, porém há muitos artigos e livros excelentes que descrevem o assunto [12]. Através da utilização apropriada de criptografia e de algoritmos criptográficos, é possível conseguir comunicação privada com maior certeza de identidade do parceiro comunicante. Os projetistas de soluções integradas para subestações e sistemas SCADA podem constatar que as tecnologias de chave publica são úteis para acrescentar uma camada adicional de segurança de rede aos seus sistemas.

"Firewalls" (paredes corta-fogo) frequentemente são utilizadas para defender um site contra ameaças externas, enquanto um sistema de Detecção de Intrusos (IDS) bem administrado pode ser um modo útil para identificar tanto o mau uso interno, quando atacantes externos que conseguem ganhar acesso interno. A "firewall" é um portal protegido que se situa entre os recursos que necessitam de proteção e o "mundo externo". A "firewall" pode ser implementada através de roteador que filtra o tráfego indesejável, ou através de combinações mais complicadas de soluções de hardware e software. Para ser eficaz, uma "firewall" deve guardar todo acesso à rede interna, incluindo as conexões de modem, além do acesso remoto à rede. Internet Protocol Security (IPSec) e Virtual Private Works (VPNs) são tecnologias estreitamente aliadas que proporcionam o meio de proteger as comunicações entre sites fisicamente distantes. IPSec utiliza a codificação para salvaguardar dados e informação de autenticação embutida nos pacotes TCP/IP. VPNs combinam tecnologia IPSec e firewalls para formar uma conexão ponto a ponto segura, através das redes públicas, de modo que do ponto de vista da privacidade ela apareça como uma rede interna simples.

Um IDS é uma boa defesa complementar de um sistema de firewall que focaliza sobre o lado interno da parede (embora alguns examinem o tráfego recebido da rede). A intenção é determinar se os usuários internos ou externos estão utilizando mal o sistema. As invasões freqüentemente têm assinaturas de ataque (similares às assinaturas de vírus), que são padrões associados à utilização imprópria do sistema. A missão do IDS é reconhecer as assinaturas de ataque à medida que vão se desenvolvendo e cortar o ataque ou notificar o administrador do sistema de que está ocorrendo um ataque. Outra implementação comum envolve a perfilagem, onde um IDS tem um modelo interno do que é atividade nominal (versus atividade anormal). Por exemplo, um IDS pode procurar atividade durante um tempo anormal do dia, ou durante acesso prolongado e alta utilização a partir de usuários externos de outros países.

7. RECOMENDAÇÕES

As recomendações para o "reforço" de dispositivos de subestações, sistemas SCADA e redes de computadores das concessionárias contra as invasões eletrônicas são muitas e variadas. Cada empresa envolvida com a produção e distribuição de energia elétrica precisa realizar a sua própria avaliação de risco. Embora não haja nenhuma sensação de uma crise nacional ou ameaça imediata, o relatório da Casa Branca efetivamente expressou um certo grau de urgência na seguinte declaração (ênfase acrescida):

> *"Sugerimos consideração dessas ações imediatas antes da conclusão de uma avaliação formal de risco:*
>
> 1. *Isolar os sistemas de controle críticos das redes inseguras, desligando ou utilizando firewalls adequadas.*

2. *Adotar práticas melhores para controle e proteção de senhas, ou instalar mecanismos de autenticação de modems.*
3. *Proporcionar responsabilidade individual através de registros de ações protegidos ou equivalente."*

A seguir é fornecido um compêndio de recomendações úteis de [1, 2, 3, 8, 11] e da nossa própria experiência na proteção de sistemas de redes de computadores. Organizamos essas recomendações pela categoria de utilização de modo que os relacionamentos se tornem mais aparentes.

Administração de Senhas:

- Utilize senhas "duras" de seis ou mais caracteres com mistura de caixa da fonte e caracteres especiais.
- Não utilize palavras comuns, acrônimos, ou informação pessoal como datas de nascimento, nomes, etc.
- Memorize as senhas, não anote em papel.
- Troque de senhas periodicamente (a Agência de Segurança Nacional dos Estados Unidos recomenda mensalmente ou trimestralmente).
- Mude as senhas imediatamente após casos de instalação e manutenção feitas por empreiteiras, suspeitas de invasão e quando giro de pessoal ou desentendimentos aumentarem o risco relativo a "insiders".
- Utilize diferentes senhas em diferentes locais, equipamentos e sistema; não caia na tentação da utilização de senhas únicas para entrada no sistema para facilidade de uso.
- Assegure-se de que as senhas sejam emitidas e controladas localmente (e não distribuídas largamente).
- Dê treinamento sobre segurança de senhas e monitore o cumprimento das regras – force a troca periódica de senhas, utilize verificadores de senhas para identificar e eliminar senhas fracas.
- Evite utilizar dispositivos com proteção de senhas inadequadas (por exemplo, senhas apenas numéricas com menos de oito dígitos).

Eventos de Alarme:

- Emita contatos de alarme para eventos de acesso, senha e configuração.
- Monitore os contatos de alarme e eventos diligentemente – não somente para detecção de invasão, porém para verificar a funcionalidade de dispositivos.
- Registre eventos de alarmes e atividades suspeitas (por exemplo, tentativas com senhas erradas) em memória não volátil.
- Faça varredura de logs de acesso e auditagem de arquivos regularmente.
- Automatize a resposta a condições de alarme com desligamentos pré-programados, advertências de auto-dial e mais alarmes sonoros e visuais.

Conexões de Rede:

- Utilizar linhas de comunicação privativas sempre que possível para limiar a possibilidade de grampos públicos e invasões em potencial.

- Implementar hierarquias de acesso com diferentes níveis de permissão para visualizar e configurar dispositivos.
- Utilize topologias estrela ponto a ponto (por exemplo, linhas "home-run") a partir dos IEDs para o controlador com o objetivo de aumentar a sobrevivência e a vulnerabilidade "cai um, caem todos."
- Utilize senhas, restrições de acesso e autenticação de usuário para proteger contra acesso não autorizado.
- Proteja os sistemas SCADA e IT utilizando scanners de vírus, firewalls e sistemas de detecção de invasão.
- Limite o acesso ao projeto de sistemas e informação de acesso à rede.

Conectividade:

- Utilize "banners de advertência" para desestimular invasões eletrônicas e habilitar a monitoração eletrônica e processar invasores.
- Utilize modems seguros tipo "dial-back", de codificação ou autenticação, e dispositivos de rede seguros.
- Encerre as sessões interativas após longos períodos de inatividade – assegure-se de que a porta aberta seja devidamente fechada de modo que o usuário seguinte não adquira os privilégios de acesso desautorizado.
- Limite o número de tentativas fracassadas de inserir uma senha – desconecte e faça time-out da linha após um limite ajustado.

8. CONCLUSÕES

Está claro que o risco de uma invasão eletrônica em um IED, Controlador ou Sistema SCADA é possível, o que pede a necessidade da adoção de medidas de segurança mais fortes. A determinação final relacionada a quanto esforço deve ser investido no sentido de adotar procedimentos mais fortes – e as respectivas mudanças empresariais – deve ser determinada por uma avaliação formal de risco conduzida pela empresa ou concessionárias.

Temos documentado a crescente ameaça de ataque eletrônico contra dispositivos de subestações, sistemas SCADA e redes de computadores das concessionárias, além de enumeramos e discutimos as ações sanadoras visando reduzir o risco de invasões. A literatura é consistente com o clamor para maior conscientização e capacitação sobre todos os aspectos da segurança de computadores e redes, assim repetimos esse clamor aqui. As concessionárias de energia elétricas precisam enfrentar o desafio de salvaguardar o seu negócio em um mundo de computadores interconectados, no qual se aumenta a ameaça de ataque eletrônico. Através do estabelecimento de mecanismos para prevenção, detecção, resposta e restauração de sistemas de computação seguros podemos prover a confiabilidade continuada da infra-estrutura dos sistemas elétricos de potência.

REFERÊNCIAS

[1] IEEE Power Engineering Society, *IEEE Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE, New York, NY, Apr. 4, 2000.

[2] National Security Telecommunications Advisory Committee Information Assurance Task Force, *Electric Power Risk Assessment*, March, 1997: http://www.ncs.gov/n5_hp/Reports/EPRA/electric.html

[3] The White House Office of the Press Secretary, *White House Communications on Critical Infrastructure Protection*, Oct. 22, 1997: http://www.pub.whitehouse.gov/urires/I2R?urn:pdi://oma.eop.gov.us/1997/11/17/3.text.1

[4] M. Amin, "Toward Self-Healing Infrastructure Systems," IEEE Computer, *IEEE Computer*, Vol 33(8), Aug. 2000, pp. 44-53.

[5] A. Jones, "The Challenge of Building Survivable Information Intensive Systems," *IEEE Computer*, Vol 33(8), Aug. 2000, pp. 39-43.

[6] K. Poulsen, "Lights Out: NIPC Unveils Plan to Monitor Cyber Attacks on the Power Grid," an *InfoSec News* article ported to *Security Focus* web page, May 25, 2000: http://www.securityfocus.com/news/41

[7] U.S. Federal Bureau of Investigation, National Infrastructure Protection Center web page, 2000: http://www.nipc.gov

[8] U.S. National Institute of Standards and Technology, *Introduction to Computer Security: The NIST Handbook*, NIST, Dept. of Commerce, July 20, 1994.

[9] B. Sullivan, "NetEspionage Costs Firms Millions," MSNBC, Sept 12, 2000: http://www.zdnet.com/zdnn/stories/news/0,4586,2626931,00.html

[10] CNN, "Teen Hacker Faces Federal Charges," Mar. 19, 1998: http://www.compugraf.com.br/hackers.html

[11] U.S. Department of Defense, *Department of Defense Password Management Guideline*, CSC-STD-002-85, DOD Computer Security Center, Fort Meade, MD 20755, Apr. 12, 1985.

[12] W. Stallings, *Cryptography and Network Security*, Prentice Hall, New York, NY, 1999.

BIOGRAFIAS

Dr. Paul W. Oman é Engenheiro Sênior de Pesquisas na Schweitzer Engineering Laboratories em Pullman, WA. Antes de ingressar na SEL, ele foi Professor e Chefe do Departamento de Ciência da Computação na *University of Idaho* e foi premiado com a distinção da *Hewlett-Packard Engineering Chair* durante seus últimos sete anos de trabalho neste local. Dr. Oman publicou mais de 100 artigos e relatórios técnicos sobre tópicos de engenharia de software. Ele foi editor dos periódicos *IEEE Computer* e *IEEE Software*. Ele tem Ph.D. em Ciência da Computação pela *Oregon State University* e é membro ativo do IEEE, *IEEE Computer Society* e ACM.

Dr. Edmund O. Schweitzer, III recebeu seus diplomas de Bacharel e Máster em Engenharia Elétrica da *Purdue University*, e seu Ph.D da *Washington State University*, com uma dissertação sobre relés de proteção digitais. Dr. Schweitzer continuou sua pesquisa em relés de proteção digitais, atendendo ao mesmo tempo as faculdades de engenharia elétrica da *Ohio University* e *Washington State University*. Em 1982, Dr. Schweitzer fundou a Schweitzer Engineering Laboratories, em Pullman, Washington, para desenvolver e fabricar relés de proteção digitais e produtos e serviços relacionados. Dr. Schweitzer é reconhecido como um pioneiro na proteção digital e detém o título de *Fellow* do *Institute of Electrical and Electronic Engineers* (IEEE), um título concedido para menos de 1% dos membros do IEEE. Escreveu dezenas de artigos técnicos nas áreas de projeto de relés de distância, filtragem de relés de proteção, testes e confiabilidade de relés de proteção, localização de faltas em linhas de transmissão aéreas, proteção de motores de indução, projeto de elementos direcionais, dinâmicas dos elementos de sobrecorrente e relés de proteção de alta sensibilidade. Dr.

Schweitzer detém mais de 20 patentes relativas à proteção, medição, monitoramento e controle de sistemas de potência.

Dra. Deborah Frincke concluiu seu Ph.D. em Ciência da Computação na *University of California*, Davis, EUA, em 1992. Ela atualmente trabalha na *University of Idaho*, onde é membro ativo (co-diretora e co-fundadora) do *Center for Secure and Dependable Software* (CSDS). Os principais interesses de pesquisa da Dra. Frincke incluem sistemas de detecção de intrusão, particularmente os aspectos da colaboração entre sites remotos e técnicas de investigação. A Dra. Frincke tem estado ativamente envolvida na promoção tanto de pesquisa quanto de educação na área de segurança. Ela participou de programas e comitês técnicos para diversas conferências de segurança nacionais e internacionais e tem recebido convites para efetuar palestras para grupos que vão desde o FBI até a *Inland Northwest Technology Alliance*.

© 2000 University of Idaho e
Schweitzer Engineering Laboratories, Inc.
Todos os direcitos reservados.
20001004 • TP6111-01