Setting the Standard for Automation™

América do Sul

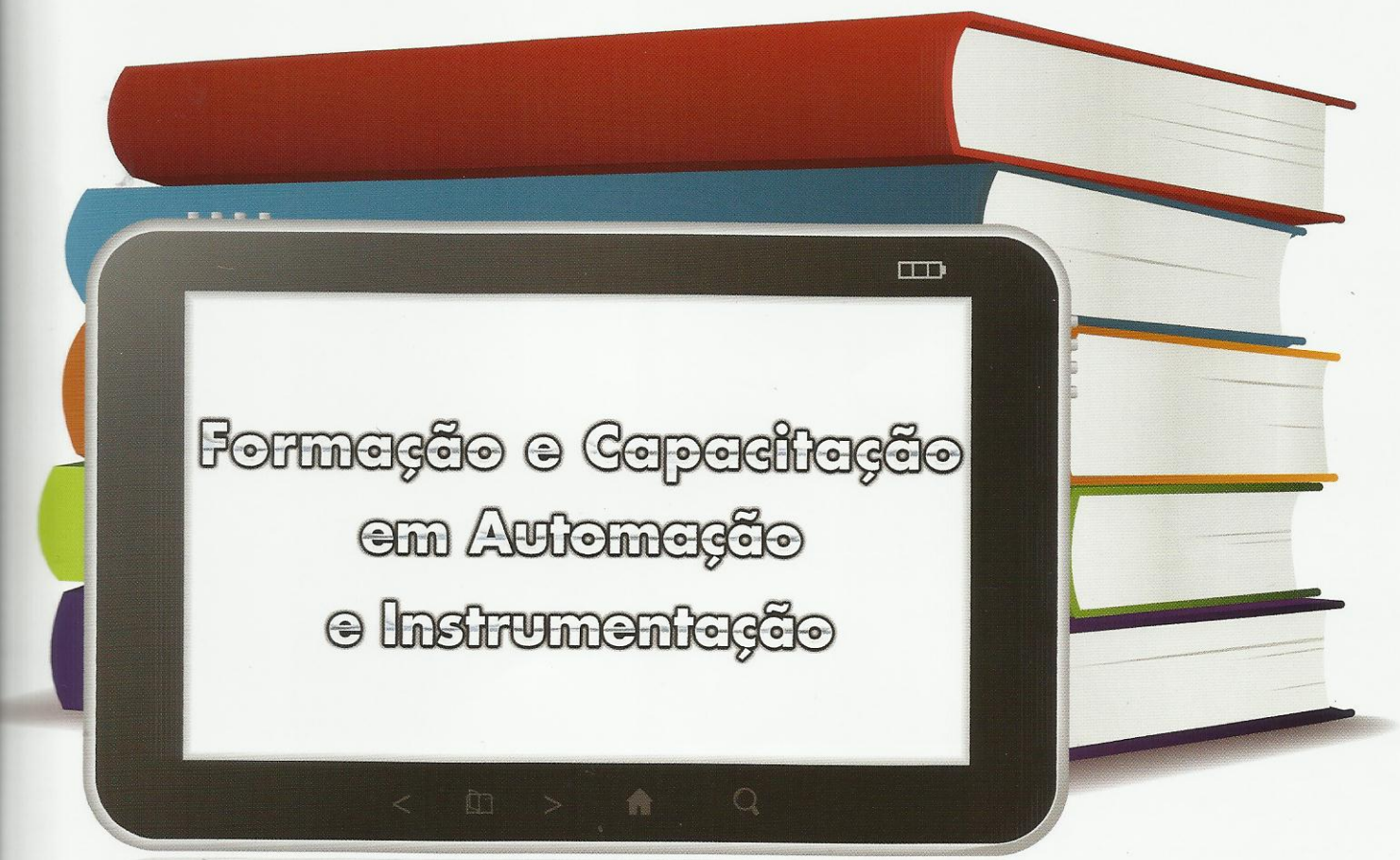
InTech

www.isadistrito4.org

Número 143

ISA Distrito 4

ISSN 2177-8906



GERENCIAMENTO DE RISCO EM AUTOMAÇÃO

MEDIÇÃO DE NÍVEL DE INTERFACE

PROCESSOS DE BATELADA

MEDIÇÃO DE PRESSÃO

■ REPORTAGEM

Mídias sociais: saudáveis ou viciantes?

■ ENTREVISTA

Ricardo Haetinger, Diretor Presidente da Elipse Software.

OS PERIGOS DO ACESSO REMOTO A SISTEMAS SCADA

Marcelo Branquinho (marcelo.branquinho@tisafe.com),
Diretor Executivo da TI Safe Segurança da Informação.

INTRODUÇÃO

Os sistemas de controle e supervisão possuem funcionalidades que permitem uma gestão mais flexível através do acesso remoto. Hoje em dia é possível supervisionar e controlar uma planta de automação, por exemplo, através de um *tablet* ou um celular utilizando uma rede sem fio gratuita.

O acesso remoto aos sistemas de controle permite a rápida atuação em casos urgentes, além da dramática redução de custos em viagens para reparos em equipamentos em localidades distantes.

Uma das principais funcionalidades da tecnologia de acesso remoto é tornar possível o acesso simultâneo de vários usuários a sistemas SCADA via redes locais ou pela internet sem a necessidade da instalação de programas nos dispositivos usados (o acesso é feito através de *browsers* como o Microsoft Internet Explorer, por exemplo).

Os celulares, *tablets* e computadores que não utilizam o sistema operacional Windows são dotados de aplicativos cliente do protocolo RDP que oferece suporte para acesso remoto a outros tipos de protocolos e sistemas operacionais [1].

Figura 1 – *Tablet* executando IHM SCADA.

OS RISCOS DO ACESSO REMOTO A SISTEMAS DE CONTROLE

Se por um lado o acesso remoto traz muitos benefícios em termos de produtividade e eficiência para as indústrias, por outro lado ele também abre portas para ataques externos, maliciosos ou não.

Existem alguns pontos críticos nas soluções de acesso remoto que devem ser observados:

- **Autenticação fraca**: a grande maioria dos aplicativos de mercado disponibiliza o acesso remoto com autenticação baseada na dupla "Usuário e Senha". Este tipo de autenticação é a mais fraca que existe e pode ser atacada de diversas formas que vão desde ataques de força bruta à instalação de *keyloggers* nas máquinas dos usuários remotos através de *malware* personalizado. Já imaginaram o que aconteceria se algum invasor conseguisse obter as credenciais de acesso remoto a um sistema SCADA?
- **Uso de máquinas não confiáveis**: é uma boa prática de segurança garantir que os computadores que acessam remotamente a rede de automação tenham atualizados os *patches* e soluções de antivírus. Dentro do perímetro de redes corporativas e de controle é relativamente simples estabelecer políticas que evitem que máquinas desatualizadas (vulneráveis) não tenham acesso à rede. Mas e se o usuário remoto utilizar máquinas que não estão cobertas pela política de segurança da rede da empresa? Quem pode garantir

que uma máquina remota está livre de *malware* que contaminará a rede de controle durante o acesso remoto ou roubará as credenciais de acesso do usuário?

- **Uso de redes não confiáveis**: a Internet e as redes Wi-Fi públicas são canais de transmissão de dados completamente promíscuos. Estas redes não possuem tráfego de dados criptografados e podem ser espionadas (através de *sniffers*) por atacantes que roubarão as credenciais de acesso.
- ***Modems* permanentemente habilitados**: muitos fabricantes de soluções de automação disponibilizam *modems* para comunicação direta com a planta de automação de seus clientes. Com isto conseguem atuar rapidamente em caso de falhas nos sistemas de controle e restabelecer sistemas com problemas. A boa prática manda que os *modems* sejam ligados somente durante o período de tempo em que o fabricante esteja atuando no sistema, e que sejam desligados logo após. O risco ocorre quando o cliente se esquece de desligar (ou desconectar) o *modem* após um acesso remoto deixando o equipamento pronto para receber chamadas externas. Os atacantes utilizam software para *war dialing* e realizam ataques fazendo uso destas conexões desprotegidas.

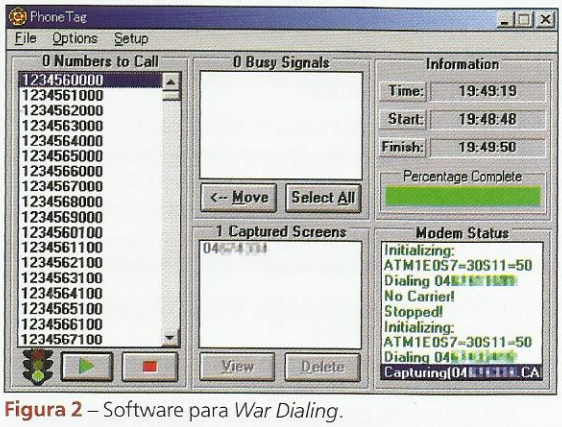


Figura 2 – Software para *War Dialing*.

- **Tecnologias vulneráveis**: o protocolo RDP usado em conexões remotas é extremamente vulnerável. Existem inúmeros ataques que exploram as vulnerabilidades do RDP [2], principalmente em versões mais antigas, sendo o mais comum deles o ataque do homem do meio (MITM – *Man In The Middle*). Além disso, o *Internet Explorer* é o browser mais vulnerável do mercado e um grande facilitador para a maioria dos ataques via *Metasploit* (ferramenta *open source* usada em análises de vulnerabilidades e testes de invasão, mas que em muitas vezes é utilizada como plataforma para ataques por *crackers*).
- **Baixo nível de detalhamento em trilhas de auditoria**: a falta de mecanismos de autenticação fortes baseados em múltiplos fatores faz com que a única trilha de auditoria gravada durante um acesso remoto seja a identificação do usuário que está acessando. Mas como garantir que a pessoa que está acessando a planta é quem realmente diz ser? E se tiver acontecido um roubo de identidade, que recursos teremos para descobrir a autoria de um ataque caso ele seja realizado por um acesso remoto?

ATAQUES DOCUMENTADOS

Nos dias atuais os ataques a sistemas SCADA são amplamente divulgados na internet, expondo ao mundo em tempo real o acontecimento de crimes cibernéticos. A base de dados pública mais completa sobre incidentes de segurança em sistemas de controle é o RISI (*Repository of Industrial Security Incidents* [3]). No RISI existem diversos casos de ataques que foram realizados através da exploração de mecanismos de acesso remoto a redes industriais. Existem diversos exemplos no livro "*Protecting Industrial Control Systems from Electronic Threats*" [4].

O caso mais recente que foi documentado ocorreu em novembro de 2011. O alvo do ataque foi o sistema de controle de águas [5] da cidade de Springfield, no estado do Illinois (EUA).

Este ataque começou com um roubo de credenciais de acesso através da invasão da rede corporativa do integrador do sistema de controle de águas. Depois de roubada a base de credenciais, os atacantes escolheram seu primeiro alvo e através do acesso remoto invadiram o sistema de controle e executaram comandos indevidos para desligar a estação principal do sistema de controle e destruir uma bomba na planta de automação.

A análise forense revelou que os atacantes já haviam acessado a planta por muitas vezes desde os três meses que antecederam o incidente com a bomba, somente para estudar o sistema. Os ataques parecem ter sido realizados através de computadores com endereços IP baseados na Rússia. Até o momento ainda é desconhecido se os atacantes conseguiram roubar as credenciais de acesso a outros sistemas de controle mantidos pelo mesmo fabricante e existe a possibilidade de que novos ataques semelhantes sejam realizados em outros sistemas de controle.

CONTROLES COMPENSATÓRIOS

Os benefícios que o acesso remoto traz às indústrias são tão grandes que é impensável abandonar esta tecnologia. Mas como utilizá-la de forma segura?

Os principais padrões de segurança de redes de automação detalham alguns controles compensatórios que podem aumentar bastante o nível global de segurança de sistemas de controle com acesso remoto. Os principais controles são os seguintes:

- **Senhas fortes para o acesso remoto**: as senhas utilizadas por usuários do acesso remoto devem ser fortes, possuindo pelo menos 8 caracteres e possuindo letras maiúsculas e minúsculas, números e caracteres especiais. Políticas de senha devem ser utilizadas e o acesso bloqueado em caso de muitas tentativas sem sucesso.
- **Uso de duplo fator de autenticação**: recomenda-se o uso de outros mecanismos de autenticação complementares à senha. Biometria e *tokens* OTP (*one time password*) são exemplos de mecanismos que fazem com que mesmo que um atacante consiga descobrir um usuário e senha válidos para um acesso remoto, ele não consiga estabelecer a conexão por não possuir o segundo fator de autenticação. Estes mecanismos também eliminam a possibilidade de um usuário negar a autoria de um ataque realizado com o uso suas credenciais de acesso.
- **Uso de máquinas confiáveis**: é recomendável estabelecer controles que garantam que somente máquinas com *patches* e soluções de antivírus atualizadas e de acordo com a política de segurança da empresa possam acessar os sistemas de controle remotamente. Uma boa prática é a empresa fornecer para os usuários remotos máquinas da empresa (preferencialmente *laptops*) já configuradas com as soluções de segurança especificadas na política de segurança corporativa e bloquear qualquer outro acesso remoto que não seja proveniente destas máquinas.
- **Uso de redes seguras**: uso de soluções de VPN (*Virtual Private Network*) para garantir a criptografia do canal de comunicação e evitar ataques por *sniffing*.
- **Regras rígidas para o uso de *modems* na rede de automação**: os *modems* da rede de automação deverão ser controlados através de autorizações por escrito. Sempre que um *modem* tiver que ser habilitado deverá existir um pedido associado, assinado pelo responsável pelo sistema de controle. Neste pedido deverão existir campos de data e hora para o momento em que o *modem* foi habilitado e a janela de tempo pelo qual ele poderá ser usado (ao término do uso o *modem* deverá ser desligado).

Existem algumas soluções de mercado que já incorporam muitos destes controles compensatórios com custo relativamente baixo.

CONCLUSÃO

Imagine o que aconteceria se um atacante atacasse um sistema de controle de uma estação de tratamento de águas e alterasse o *set point* responsável pela vazão dos reagentes químicos que são misturados para purificar a água que bebemos? Isto poderia potencialmente envenenar a água de regiões inteiras e comprometer a saúde de toda a população, causando o caos [6].

Eventos recentes como o aparecimento do Worm Stuxnet em 2010 mostram que os atacantes estão desenvolvendo ataques cada vez mais sofisticados contra sistemas de controle e supervisão. O acesso remoto é uma das vulnerabilidades mais interessantes sob o ponto de vista dos atacantes por permitir que eles realizem ataques sem sair de suas casas e causar destruição sem a necessidade de uma arriscada invasão física às instalações.

É ponto mandatório para empresas que possuam sistemas de controle a garantia da segurança no acesso remoto e controles compensatórios devem ser usados para este objetivo.

REFERÊNCIAS BIBLIOGRÁFICAS

1) Artigo "Operação Remota de Plantas de Mineração e Saneamento", escrito por Carlos Eduardo Gurgel Paiola, Alexandre Roberto Granito, Cláudia Souza de Oliveira e Diogo Lopes Gomes e publicado na revista InTech América do Sul, número 138, 2011.
2) Artigo sobre as vulnerabilidades do protocolo RDP, disponível em http://www.securiteam.com/windowsntfocus/5EP010KG0G.html.
3) Website do RISI (Repository of Industrial Security Incidents) - http://www.securityincidents.org.
4) Weiss, Joseph, Protecting Industrial Control Systems from Electronic Threats, ISBN: 978-1-60650-197-9, May 2010, Momentum Press.
5) Reportagem sobre a invasão na estação de águas nos EUA, disponível em http://www.techweekeurope.co.uk/news/us-water-utility-attacked-via-scada-network-46576.
6) Palestra Técnica "Cyber-Terrorismo e a Segurança das Infraestruturas críticas" disponível na seção de segurança da automação no site da TI Safe Segurança da Informação, link http://www.slideshare.net/tisafe/.

SOBRE O AUTOR

Marcelo Branquinho é Engenheiro de sistemas e computação formado pela UERJ com MBA em gestão de negócios. Especialista em segurança da automação é membro da ISA e integrante do comitê internacional da norma ANSI/ISA-99 que estabelece as melhores práticas de segurança para redes de automação e SCADA. ■