UM NOVO PROTOCOLO DE AUTENTICAÇÃO

Adriana M.P. Léo

Banco do Brasil S/A
EDSED IV - SAIN 716
Brasília, DF, 70620-000
adrianaleo@bb.com.br

*Valdemar C. da Rocha Jr.**

Grupo de Pesquisa em Comunicações
Universidade Federalde Pernambuco
CP 7800, Recife, PE, 50711-970
vcr@npd.ufpe.br

RESUMO

Este trabalho considera um cenário onde um Servidor precisa estabelecer uma comunicação segura com um número finito de clientes remotos. Para que este objetivo seja alcançado, é introduzido um novo protocolo, simples e seguro, que baseia-se no uso de criptografia simétrica. Este protocolo possibilita a troca de informação de forma confidencial e autêntica, através de um canal inseguro. É mostrado que um eventual vazamento de informação não é, de uma forma geral, suficiente para que um criptoanalista inimigo possa fazer inferências sobre as senhas ou números de identificação pessoal (PINs) dos clientes, e é mostrado como proceder a fim de resistir ao chamado ataque por dicionário, usando este novo protocolo.

1. INTRODUÇÃO

Vários protocolos conhecidos [1, 2, 3, 4] autenticam os usuários através do conhecimento, compartilhado por ambas as partes, de uma informação secreta, na forma de senha (*password*) ou número de identificação pessoal (*Personal Identification Number*), ou PIN. Tais protocolos so conhecidos como *Encrypted Key Exchange* [1], *Secret Public-Key Methods* [2],*SPEKE* [3], e *Open Key Exchange* [4]. Embora vários dos protocolos disponíveis já façam uso de assinaturas digitais para autenticação dos usuários (clientes) [6], senhas e PINs permanecem em uso, seja em sistemas operacionais [7], seja em várias aplicações do dia a dia, por exemplo, operações de *homebanking* e operações com cartões de crédito [8] [9]. A seguir, iremos introduzir uma combinação de técnicas que empregam criptografia simétrica e procedimentos de identificação/autenticação baseados em senhas ou PINs, que irá permitir a troca de informações, de forma confidencial e autêntica, através de um canal inseguro, sem fazer uso das técnicas de criptografia assimétrica. Nas aplicações práticas do "mundo real", o uso das técnicas de criptografia assimétrica se restringem à troca de chaves de sistemas de criptografia simétrica, e assinaturas digitais [5, pág.216], devido ao elevado *overhead* e baixo desempenho, em comparação com as técnicas de criptografia simétrica.

Neste trabalho, introduziremos um novo protocolo para autenticar clientes remotos (usuários) que encontram-se conectados com um banco (servidor ou *host*), através de senhas ou PINs. Este protocolo possibilita a troca de chaves secretas, em sistemas criptográficos simétricos, resistindo inclusive ao chamado ataque por dicionário, no qual um intruso examina exaustivamente todas as possíveis senhas. Mostraremos que um eventual vazamento de informação não é, de uma forma geral, suficiente para que um criptoanalista possa fazer inferências sobre as senhas ou PINs dos clientes. Nosso protocolo pode vir a ser usado juntamente com qualquer sistema de criptografia simétrica, mas nós sugerimos o uso do SAFER+ [10], pois o mesmo apresenta as seguintes características de extrema relevância:

a) O SAFER+ é uma cifra de grupo, ou seja, é equivalente a uma cifra de bloco descartável (one-time pad) [5] se uma única rodada é feita, com uma chave usada uma única vez [10];

b) O SAFER+ pode operar com chaves de 128, 192 ou 256 *bits* de comprimento;

c) O SAFER+ é rápido em ambas as operações, de cifragem e de decifragem;

d) A família SAFER de cifras, possui um histórico de confiabilidade desde sua introdução em 1993.

Na Seção 2, descrevemos passo a passo, o protocolo proposto. Na Seção 3, discutiremos a segurança e limitações do mesmo. Finalmente na Seção 4 apresentaremos algumas aplicações do protocolo proposto.

*O trabalho deste autor foi financiado parcialmente pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Projeto 304214/77 – 9

2. DESCRIÇÃO DE PROTOCOLO

Na Tabela 1 apresentamos e definimos a notação a ser empregada. Vamos assumir que uma nova chave secreta de sessão é estabelecida toda vez que uma nova sessão tem início e, além disso, vamos assumir que o sistema de criptografia simétrico empregado é o SAFER+ [10]. A seguir, descrevermos as etapas envolvidas na implementação do protocolo.

1. Um(a) cliente C_i, $1 \leq i \leq n$, conecta seu terminal ao servidor H (banco) e envia sua identificação Id_i para o servidor H. Nenhuma senha é necessária nesta etapa.

2. O servidor H (banco) assume que o cliente é realmente C_i e utiliza a identificação Id_i para localizar o *hash* de 128 *bits* $h(p_i)$, correspondente a este cliente, que encontra-se armazenado em uma base dados contendo os arquivos de *hash* dos clientes.

3. O servidor H gera um número binário aleatório r, de 128 *bits*.

4. O servidor H cifra r utilizando a cifra SAFER+ tendo $h(p_i)$ como chave secreta, e envia o texto cifrado resultante para C_i, isto é, H calcula $E_{h(p_i)}(r)$, e envia o resultado para C_i.

5. O servidor H efetua a operação ou-exclusivo bit-a-bit dos números $h(p_i)$ e r, ambos com 128 *bits*, produzindo a chave secreta de sessão, Z, isto é, H calcula $h(p_i) \oplus r = Z$.

6. C_i calcula o *hash** de sua senha p_i, para obter $h(p_i)$, e então extrair r decifrando $E_{h(p_i)}(r)$, isto é, C_i efetua a operação de decifragem

$$D_{h(p_i)}(E_{h(p_i)}(r)) = r.$$

7. C_i efetua então a operação ou-exclusivo bit-a-bit dos números $h(p_i)$ e r, ambos com 128 *bits*, produzindo a chave secreta de sessão, Z, isto é, C_i calcula $h(p_i) \oplus r = Z$.

8. C_i então usa a chave secreta de sessão, Z, para cifrar/decifrar sua comunicação com o servidor H e vice-versa.

*Nós assumimos que o cliente está operando de um terminal de computador, que possui uma aplicação, a qual permite a ele/ela introduzir sua identificação Id (PIN ou senha) e obter o correspondente *hash* $h(p)$.

C_i	Cliente i, $1 \leq i \leq n$, onde n é um número inteiro positivo
Id_i	Identificação de cliente i
p_i	Senha do cliente i
H	servidor
$h(.)$	função de *hash* seguro, com 128 *bits*
r	número binário aleatório com 128 *bits*
Z	Chave-secreta de sessão
$E_Z(.)$	Operação de cifragem com a chave secreta Z
$D_Z(.)$	Operação de decifragem com a chave secreta Z
$a \oplus b$	Operação ou-exclusivo das quantidades binárias a e b

Tabela 1: Símbolos e notação.

3. ANÁLISE DE SEGURANÇA

A seguir, provaremos duas proposições relacionadas à robustez do protocolo proposto contra ataques às mensagens cifradas.

Lema 1 *O procedimento de estabelecimento da chave secreta de sessão é seguro, isto é, não é possível um intruso extrair nenhuma informação, qualquer que seja, sobre a senha ou PIN de um cliente, pela observação apenas da mensagem cifrada $E_{h(p_i)}(r)$, enviada pelo servidor para o usuário.*

Prova: Obter a senha pela observação apenas da mensagem cifrada $E_{h(p_i)}(r)$, é equivalente a quebrar uma cifra de bloco descartável (one-time pad), uma vez que a cifra simétrica SAFER+ com uma iteração é equivalente a uma cifra de bloco descartével, e portanto inquebrável [10]. □

Lema 2 *Não é viável um intruso extrair a chave secreta de sessão empregada, através de um ataque ao texto cifrado. Além disso, a complexidade de um ataque com texto claro conhecido é limitada superiormente pelo comprimento da senha do cliente.*

Prova: Extrair a chave secreta empregada pela observação apenas das mensagens cifradas é equivalente a quebrar a cifra simétrica SAFER+, e isto até a presente data tem se mostrado inviável. Para realizar um ataque com texto claro conhecido, o intruso dispõe de informação sobre o conteúdo de alguns campos de um formulário utilizado pelo banco/cliente. Este ataque consiste em exaustivamente testar os pares $(h'(p_i), r')$ como uma possível chave secreta de sessão $Z = h'(p_i) \oplus r'$,

até obter sucesso na decifragem de alguns campos conhecidos. O número de possibilidades a serem testadas é no máximo igual ao número de senhas distintas. □

Os lemas acima, mais o fato de que para toda sessão uma nova chave secreta de sessão é usada, permite-nos estabelecer as seguintes propriedades para o protocolo proposto.

Propriedade 1. O protocolo proposto evita a repetição sistemática de mensagens cifradas em sessões distintas.

Propriedade 2. A eventual exposição de uma das chaves secretas de sessão empregada, não comprometerá outra chave secreta de sessão (futura ou passada).

Propriedade 3. É impraticável para um intruso assumir o papel de um usuário legítimo do sistema sem o conhecimento prévio da senha ou do PIN deste usuário (vide comentário a seguir).

Comentários
Tipicamente a senha p_i do usuário i consiste de 6 dígitos decimais, que correspondem a aproximadamente 20 *bits*. Desta forma, embora $h(p_i)$ tenha 128 *bits*, na verdade apenas 20 *bits* são suficientes para determiná-lo. Considerando que um criptoanalista inimigo tem conhecimento do conteúdo de alguns campos específicos do documento cifrado, o trabalho de descobrir a chave de sessão pode ser simplificado concentrando atenção apenas nestes campos. Um ataque plausível consiste em:

1. Realizar a operação $D_{h'(p_i)}(E_{h(p_i)}(r)) = r'$, onde $h'(p_i)$ e r' são, respectivamente, as estimativas do criptoanalista sobre $h(p_i)$ e r. São gerados 2^{20} pares $(h'(p_i), r')$. Observamos que um destes pares será igual a $(h(p_i), r)$.

2. A cada novo par $(h'(p_i), r')$ gerado, o criptoanalista testa $h'(p_i) \oplus r'$ como uma possível chave de sessão. Daí concluímos que a probabilidade de quebrar este sistema é de 2^{-19}, considerando que em média cerca de metade das possibilidades (2^{19}) serão testadas para obter-se a quebra.

Caso 1000 pares $(h'(p_i), r')$ sejam testados por segundo, o valor esperado para o tempo de quebra é de apenas 17 minutos. Aumentando o comprimento da senha para 10 dígitos decimais, este valor esperado do tempo de quebra passa a ser de aproximadamente 116 dias.

4. APLICAÇÕES

O protocolo proposto pode ser usado em todas as aplicações de *electronic banking* empregando uma combinação de cartões magnéticos e PINs na identificação dos clientes. No momento, tais aplicações são usadas por bancos e outras instituições financeiras em todo o mundo. Estas aplicações permitem a comunicação entre um cliente em um teminal remoto e diversos sistemas da instituição financeira, fazendo uso de diversos tipos de canais de comunicação. Por oferecer um nível de segurança compatível com os requeridos por este tipo de aplicação, associado a eficientes taxas de transmissão, o nosso protocolo proposto mostra-se bastante promissor. Finalmente, qualquer intruso (que não conheça a senha p_i do cliente C_i) que tentar passar-se por C_i terá suas pretensões frustradas uma vez que, tomados alguns cuidados com o comprimento da senha, conforme observamos acima, será impraticável para este intruso gerar $h(p_i)$, e isto inclui um cripto-analista experiente.

5. REFERÊNCIAS

[1] S. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", Proceedings of the *IEEE Symposium on Research in Security an Privacy*, Oakland, May 1992, pp. 72-84.

[2] L. Gong, M. Lomas, R.Needham and J. Saltzer, "Protecting Poorly Chosen Secrets from Guessing Attacks", *IEEE Journal on Selected Areas in Communications*, Vol.11, No.5, June 1993, pp.648-656.

[3] D. Jablon, "Strong Password-Only Authenticated Key Exchange", *Computer Communication Review*, vol. 26, no. 5, October 1996, pp.5-26.

[4] S. Lucks, "Open Key Exchange; How to Defeat Dictionary Attacks Without Encrypting Public Keys", Proceedings of the *Security Protocol Workshop'97*, Spring Verlag, April 1997.

[5] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc. 1996.

[6] R. Smith, Internet Cryptography, Addison - Wesley, Inc. 1997, pp. 278-320.

[7] Microsoft TechNet, "Meeting Enterprise Security Needs MS Windows NT and UNIX", September 1998.

[8] ANSI Standard X9.8, Personal Identification Number (PIN) Management and Security, Washington, DC , American Bankers Association, 1982.

[9] ANSI Standard X9.9, Financial Institution Message Authentication (Wholesale), Washington, DC , American Bankers Association, 1986.

[10] J.L. Massey, G.H. Khachatrian and M.K. Kuregian, "Nomination of SAFER+ as candidate algorithm for the advanced encryption standard (AES)".
Internet: http://www.cylink.com/SAFER, June 1998.