Segurança de transações contra dois tipos de ataque

Danton Nunes, InterNexo Ltda.
danton.nunes@inexo.com.br

Motivação

Recente discussão na lista GTS−L sobre a questão de segurança de transações bancárias pela Web.

Método

Análise teórica com um mínimo de simulações de apoio. (até mesmo pela falta de tempo para coisa melhor),

Neutralidade em relação a sistema operacional e navegador

Cenários idealizados com boa dose de realismo.

Intrusos considerados

Man−in−the−middle (MIM): um agente intruso em um "proxy", capaz de:

*** Oferecer ao cliente certificado falso porém plausível,**

*** Executar procedimentos "client side" que tenham sido enviados pelo servidor do banco,**

*** Interceptar a conversa entre cliente e servidor em texto claro.**

porém não pode:

*** Executar procedimentos em dispositivos externos no lado do cliente.**

Intrusos considerados

Man−in−the−browser (MIB) um agente infiltrado no computador do cliente, capaz de:

*** Simular as ações do usuário de forma indistinguível do ponto de vista do navegador ou do SO,**

*** Submeter formulários clandestinamente,**

*** Executar procedimentos "client−side" quer tenham sido enviados pelo servidor ou já presentes.**

Não considerei o caso de um MIB cooperando com um MIM, por ser mais complexo, e desnecessário, pois separados já fazem estrago suficiente!

Defesas consideradas

Estes procedimentos foram escolhidos por serem usados por bancos dos quais o autor é cliente.

*** Identificação do computador,**

*** Senha variável de 4 dígitos em cartão,**

*** Senha variável de 6 dígitos em "token" eletrônico.**

O uso de senhas variáveis seria seguro contra o MIM se fosse usado corretamente, nenhum método resiste à presença do MIB!

Identificação do computador

Consiste em obter uma assinatura a partir de vários dados "únicos" da máquina (ex. endereço MAC, /proc)

Minha maior crítica a este processo é que basicamente se pergunta ao Lobo Mau se ele é a Vovozinha!

A resposta nunca será confiável, por mais artifícios que se apliquem. No fim sempre se depende de /proc (ou equivalente) e "system calls" que podem estar comprometidos.

Finalmente o autor conseguiu criar uma máquina virtual com o mesmo endereço MAC de seu portátil que alegremente passou pelo teste.

Identificação do computador

Conclusão

DETONADO!

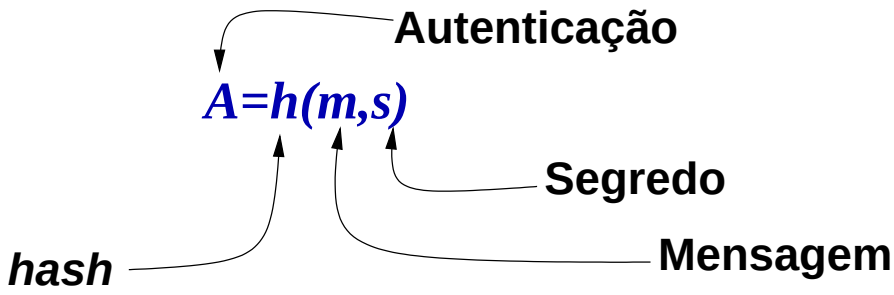
Senhas de uso único

Trata−se de um segredo compartilhado entre cliente e servidor, concebido especialmente para derrotar o MIM

Senhas de uso único

Procedimento

Dados a mensagem e o segredo compartilhado calcula−se:



Transmite−se a autenticação junto com a mensagem.

Do lado do servidor a autenticação é verificada.

O segredo deve ser usado uma única vez por mensagem (e é aqui que mora o problema!)

Senhas de uso único

Resistência ao MIM

Conclusão

Sabendo usar, FUNCIONA!

Infelizmente, porém, os sítios Web de bancos não usam este procedimento corretamente, mantendo a mesma chave para várias transações.

Senhas de uso único

Resistência ao MIB

Aqui a situação é crítica pois o MIB:

* tem acesso à senha do cartão ou token pois o usuário a entrou em um campo de formulário,

* tem acesso ao procedimento de cálculo do hash, mesmo que este seja feito por dispositivo externo, pois o SO ou o browser não distinguem suas ações das do usuário.

Conclusão

O intruso pode falsificar uma transação!

Resumo da ópera

Ataque	Identificação	Cartão (4díg)	Token(6díg)
MIM	interceptável e falsificável	risco de com−prometimento por criptanálise se usado em mais de uma transação.	bem mais duro, mas pode ser comprometido se usado em mais de uma transação.
MIB	resposta não confiável.	o intruso tem acesso ao segredo e pode falsificar transações que passam por legítimas.	o intruso tem acesso ao segredo e pode falsificar transações que passam por legítimas.

Conclusões

Se o computador do cliente estiver tomado, nada do que foi analisado permitirá uma transação segura.

Identificação do computador é história da carochinha.

Senhas únicas só são seguras se forem realmente únicas por transação, e não por sessão.

Referências

Schneier, B.: Secrets & Lies − Digital Security in a Networked World, John Wiley & Sons, 2000

http://www.schneier.com/blog/archives/2005/03/the_failure_of.html