Segurança na Internet: Estudo de Caso

Rafael Dueire Lins

(rdl@ee.ufpe.br)

Departamento de Eletrônica e Sistemas

Centro de Tecnologia e Geociências

Universidade Federal de Pernambuco

Av. **Prof. Luis Freire s/n**

Cidade Universitária
50740-540 - Recife - PE - Brasil

Sumário

Em fins de 1997, André Santos, brasileiro, aluno de doutorado em segurança de sistemas computacionais na Universidade da Califórnia em Santa Bárbara, tornou pública a sua invasão ao sistema de home-banking do Banco do Brasil S.A. Tal atitude denegriu a reputação da segurança do banco e trouxe prejuízos financeiros diretos e indiretos. Quase um ano mais tarde, sem conseguir traçar o cenário do ataque, o Banco do Brasil apresentou o problema e os elementos disponíveis ao autor deste artigo. Em outubro de 1998, foi formulada uma hipótese de explicação para o ataque, que desde então não foi refutada, tendo havido evidências que a corroboram. Neste trabalho, apresentamos tal solução para o ataque passo a passo, juntamente com as evidências que reforçam sua validade. São também apresentadas várias possibilidades para evitar reincidências de ataques da mesma natureza.

Abstract

By the end of 1997, André Santos, brazilian, doctoral student in computational system security in University of California at Santa Barbara, made public his attack to the home banking system of Banco do Brasil S.A. His attitude damaged the trust customers had in the service offered, causing direct and indirect finantial losses to the bank. Almost a year later, unable to explain the attack, Banco do Brasil presented the problem and the available information to the author of this paper. In October 1998, a hypotesis was formulated to explain the attack. Since then, no doubt has been cast upon it. On the contrary, evidences corroborate its validity. This paper presents the proposed solution to the attack step-by-step, together with evidences that strengthen its validity. Several ways of avoiding the same or similar attacks are presented

Introdução

Desde o surgimento da ARPANET no inicio dos anos 70 houve um aumento da conectividade das redes de computadores. Em pouco tempo mais redes foram se conectando a ARPANET, a principio redes locais (LANs - Local Area Networks) e pouco a pouco redes amplas (WANs - Wide Area Networks) até que surgiram as *internets.*
Hoje, a mais popular das *internets,* a Internet, é uma rede de dimensão planetária que interconecta mais de 15 milhões de máquinas, através de centenas de milhares de canais de comunicação que vão desde saté1ites, a fibras ópticas a pares trançados de fios de cobre. A Internet já é a peça central da infraestrutura de informação do planeta, permitindo o compartilhamento de dados, programas e recursos computacionais, além da troca de mensagem entre povos sem fronteiras geográficas, étnicas, culturais e econômicas. Uma vez que uma máquina esteja conectada a rede os seus usuários tem a possibilidade de executar programas em máquinas remotas e obter dados delas. Juntamente com essa abertura de possibilidades e há um preço a ser págo: a segurança do sistema torna-se vulnerável. Os especialistas em segurança de redes preocupam-se com aspectos tais como [6]:

•Quem tem permissão para usar determinada máquina.

•Como determinar se as credenciais de acesso apresentadas são legitímas.

•Como limitar o acesso de uma máquina ou usuário remoto a uma máquina hospedeira (host).
Os mecanismos de segurança desenvolvidos hoje vão muito além da verificação de senhas (passwords), de firewalls e das ferramentas de checagem de segurança tais como SATAN [2].

Uma das grandes propulsoras do desenvolvimento da Internet nos últimos anos foi a criação da World Wide Web por Tim Berners-Lee em 1992. Esta invenção introduziu a linguagem de marcação de hipertextos (html) e a navegação num grafo de informações interconectadas. Antes da invenção da WWW, o uso da Internet estava quase que inteiramente restrito a textos trocados via correio eletrônico e transferência de arquivos. Com a invenção da Web, tornou-se possível a troca de páginas Web realmente multimidia, incluindo figuras, sons, vídeos, bem como marcadores que dariarn acesso a novas páginas. De imediato, estavam abertas as portas para toda uma nova gama de serviços inclusive o comércio eletrônico e home banking.

Um outro conceito revolucionário veio alargar as fronteiras de uso da Web. Rompeu-se o modelo cliente-servidor onde o usuário solicitava páginas ao host e este devolviá páginas para se adotar um modelo dinâmico onde programas são cidadãos de primeira classe, podendo ser passados como resposta a um acesso. A linguagem Java, desenvolvida pela Sun Microsystems em 1995, foi a pioneira nessa nova filosofia de computação distribuida onde agora a máquina é a rede. 0 programa obtido em resposta ao acesso a um link escrito na linguagem Java é interpretado (executado passo-a-passo) pela máquina virtual Java (JVM - Java Virtual Machine). Os programas Java, conhecidos como Java applets, tornaram-se populares. Os navegadores para a Web, tais como o Netscape e o Internet Explorer, incorporaram versões da Java VM, permitindo a execução automática dos applets recebidos. Justamente na facilidade obtida residem os riscos de segurança [8]. Os applets Java são muito simples de serem obtidos, muitas vezes, inclusive de forma involuntária e sem o consentimento dos usuários.
Java possui três niveis de segurança :

- Acesso restrito a arquivos de sistema e a rede.

- Acesso restrito a partes intemas dos navegadores (browsers).
- Um conjunto de dispositivos de verificação em tempo de carreção e execução que exigem que os byte-codes sigam. as regras especificadas.

Embora Java seja talvez a mais segura dentre as linguagens da sua natureza, ela não é completamente segura. McGraw e Felten [6] salientam:
"Tenhá em mente que a máquina mais segura é uma máquina mantida desligada sempre e trancada num quarto. Obviamente uma máquina com tamanha segurança também é inútil".
Este artigo apresenta em detalhes a mais amplamente aceita explicação de como ocorreu o ataque ao sistema de Home Banking do Banco do Brasil S/A em fins de 1997,(largamente noticiado na imprensa. 0 atacante, o Sr. André Santos, estudante brasileiro em doutorado em segurança de sistemas na Universidade da California em Santa Barbara, atribuiu na revista Byte Brasil em Novembro de 1997 [10] as seguintes vulnerabilidades ao sistema:

"O Banco do Brasil errou na implementação do sistema de login, composto por muitas partes que podem falhar, como a linguagem JAVA e a criptografia proprietária utilizada. E um único ponto vulnerável acaba comprometendo todo o resto"...

Tendo também sido atribuída a Santos a seguinte frase:
"Tive acesso até a assinatura digital do banco ".

0 autor deste artigo foi contatado pelo Banco do Brasil a fim de esclarecer como havia sido processado tal ataque em Outubro de 1998, pois até então os especialistas do Banco não conseguiam detectar qualquer rastro do invasor, que continuava a penetrar no sistema, tendo acesso a informações confidênciais dos clientes do sistema de Home Banking, denegrindo tal sistema bancário e trazendo imensos prejuízos financeiros diretos e indiretos.

0 cenário do crime foi esclarecido pelo autor deste artigo, tendo também apontado ao Banco do Brasil várias maneiras de prevenir tal tipo de ataque. Na realidade, as vulnerabilidades apontadas pelo Sr. André Santos não refletiam a verdade dos fatos, ou a espelhava de maneira bastante distorcida.

0 tipo de ataque perpetrado por Santos apresenta uma nova faceta de redes como a Internet, onde não só a informação está distribuída, mas também a sua segurança como um todo.

Explicando o Ataque

A explicação de qualquer crime é, em geral, um processo não trivial. 0 trabalho do perito criminal é buscar elementos que expliquem o crime e levem ao culpado. Testemunhas são ouvidas, evidências circunstânciais e materiais são necessárias. É preciso ter cautela para a análise dos relatos testemunhais e da relevância das provas materiais, pois as pessoas mentem e evidências materiais podem ser propositalmente forjadas para desviár a atenção para a verdadeiras circunstâncias do crime.
0 crime eletrônico não é muito diferente de outros tipos de crimes. No caso especifico do ataque ao Banco do Brasil o culpado assumiu publicamente a culpa, mas como prevenir a reincidência do crime pelo culpado ou outros? As explicações oferecidas, seja pelo réu confesso ou pelas "testemunhas", não devem ser encaradas como verdades absolutas. Ainda mais comprometida fica a verdade dos fatos se existirem intermédiarios pouco conhecedores do assunto em questão reportando sensacionalisticamente o crime.

0 Banco do Brasil durante quase um ano tentou explicar sem sucesso o ataque de Santos ao sistema de Home banking, porém nenhum sinal da sua presença foi encontrado. 0 fato de informações particulares dos clientes terem sido divulgadas implica no fato de que o ataque efetivamente ocorreu. Seria o criminoso tão astuto ao ponto de ter entrado no sistema e ter eliminado todas as provas da sua presença? Partindo da suposição que não existe crime perfeito, em algum lugar alguma evidência deveria ser encontrada. 0 fato de ter sido atribuida a Santos o conhecimento a assinatura digital do banco [10], seria um indicativo que ele teria efetivamente penetrado o sistema do banco, e por isso o banco continuava a buscar de maneira infrutífera vestigios da sua indesejada visita.

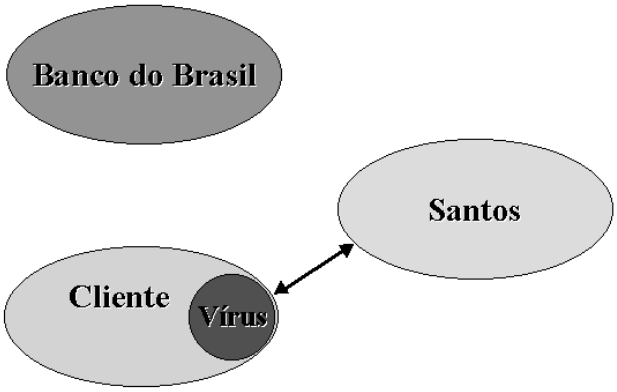
0 perito criminal busca a explicação mais plausível possível para crimes. A hipótese de simplicidade de um ataque deve ser levada em consideração. Por que um ladrão iria entrar pela janela trancada no primeiro andar de uma casa se os donos esquecerarn a porta da cozinhá aberta? A explicação oferecida pelo autor deste artigo para este episódio foi considerada plausivel pelo Banco do Brasil, e todas as outras hipóteses formuladas desde então mostraram-se menos viáveis. Na realidade, não há nenhuma evidência que Santos realmente tenhá obtido a assinatura digital do banco. Desta maneira, assumimos que a premissa da penetração direta ao sistema não teria sido efetuada. Então como explicar a obtenção das informações? Como será comentado mais adiante, as declarações atribuidas a Santos são pobres de conhecimento cientifico, seja na parte de segurança de sistemas de criptografia, ou de segurança de linguagens, havendo grande possibilidade de que ele efetivamente não ter dito o que a ele foi atribuido, uma vez que se espera que um doutorando em segurança de sistemas computacionais deve ter conhecimento mais aprofundado da matéria que o exibido. Mas o ataque existiu e necessita de ser explicado.

Ao nosso ver, o ataque perpetrado por Santos ao Banco do Brasil foi feito de maneira indireta, como é aqui explicado, passo a passo.

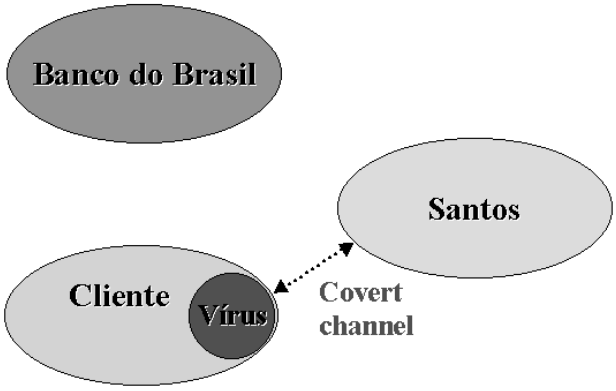
1) Em primeiro lugar o atacante atrai o usuário, neste caso o cliente de home-banking do Banco do Brasil, a visitar um site. Tal site, conhecido como honey-pot (pote de mel), pode ter sido catalogado em diversos mecanismos de busca como contendo a informação procurada pelo usuário.
   A figura seguinte apresenta a conexão estabelecida entre o cliente e o atacante.

2) Caso o usuário esteja navegado com o browser aberto, o atacante manda o applet atacante pela rede, ficando sujeito a segurança do browser que o usuário está usando freiar ou não o ataque.
   Caso o browser apresente falha de segurança ele poderd ser alterado deixando que o applet atacante contamine a máquina do usuário com um cavalo-de-tróia [5].

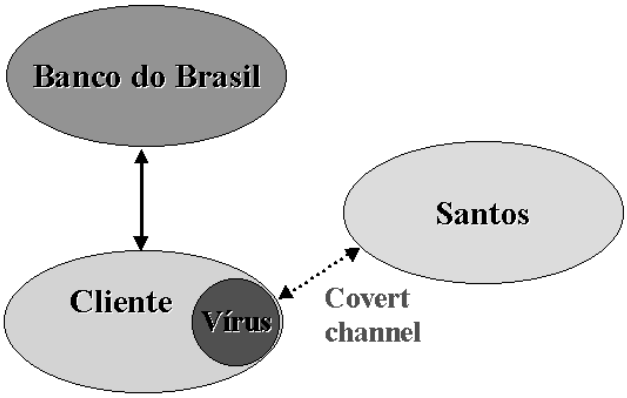
Porém um mecanismo, ainda mais simples de infecção do usuário deve ser observado. Com a falsa alegação que para ter acesso a informação que o usuário busca é necessário instalar um utilitário qualquer, o atacante que esteja com o browser fechado é induzido a receber *(download)* um applet atacante, na realidade um cavalo-de-tróia.
Em qualquer uma das duas situações apresentadas, teriamos a seguinte configuração de sistema:



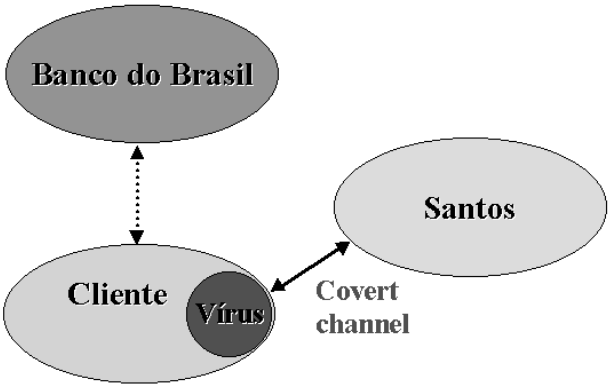
3) O vírus que infecta o usuário estabelece-se como um thread que monitora as atividades do usuário e por quais sites ele navega, como, mostrado, na figura a seguir.



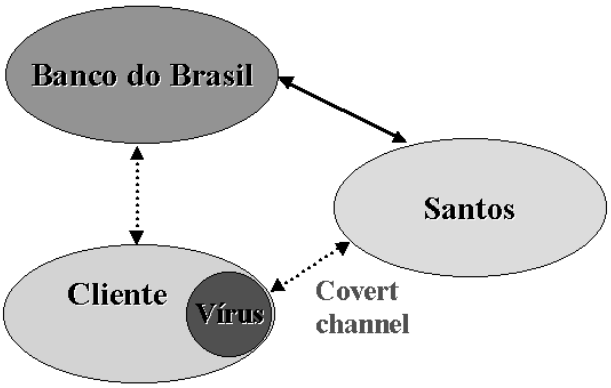
4) Na realidade o virus estabelece um canal encoberto (covert channel) espacial [5], que espera que o usuário acesse determinados sites de interesse do atacante, neste caso o site de home banking do Banco do Brasil.



5) Quando o usuário acessa o site de interesse o cavalo-de-tróia grava as informações do usuário (número da conta corrente, agência, senha, etc.) e no mesmo momento ou posteriormente, as envia via e-mail para o atacante, como apresentado, na figura abaixo.



6) Tendo obtido todas as informações confidenciais do cliente, o atacante acessa diretamente o banco, emulando ser o próprio cliente, como apresentado esquematicamente na figura a seguir,



7) O atacante dá ciência ao cliente e ao banco que obteve informações confidênciais do cliente, denegrindo a imagem pública da instituição e vulnerabilizando a confiança do cliente na segurança do serviço prestado.

É importânte salientar que:

- 0 Cavalo de Tróia está dentro da máquina do usuário e foi instalado por ele próprio ou pelo atacante utilizando-se da sua ingenuidade ou falhá do browser.
- Nenhuma linguagern está associada a tal falha. A id6ia de que tal tipo de ataque estária associado a linguagem Java, como atribuido a Santos pela revista Byte [1016 completamente improcedente, pois estando o cavalo de tróia instalado através do consentimento do próprio cliente ele passa a ter o comando da máquina do usuário.
- A utilização de código autenticado também é de nenhuma valia nessa caso de ataque, pois a autenticação serve apenas para se ter a procedência do código. 0 ataque não ocorre quando o usuário está acessando o sistema do banco, por exemplo, onde a sua máxima atenção para qualquer irregularidade no site está desperta. Na realidade, o ataque ocorre em episódio completamente não correlato, quando o usuário está ávido de obter outro tipo de informações e é atraído para o honey-pot.

Em dois artigos técnicos [7, 9], onde Santos aparece como co-autor, são analisadas falhas no navegador Netscape em linha semelhante ao trabalho de Dean, Felten e Wallach [1].

Também é analisado na referência [7] o tipo de ataque conhecido como "Man-in-the-Middle" [6], onde o usuário, semelhantemente a explicação proposta aqui, é atraído para uma página "falsa" (honey pot), que embora pareça ao usuário igual a página que o usuário deseja acessar

ela na realidade contamina a máquina do usuário com o cavalo-de-tróia. Da leitura dos trabalhos co-autorados por Santos pode-se tirar algumas conclusões:
1) 0 ataque do tipo "Man-in-the-Middle" embora semelhante ao aqui apresentado em mecanismo de ação é mais complexo, pois envolve o acesso a uma página (honey pot) cuja aparência seja igual ao site buscado.

2) A atração do usuário a um pote-de-mel completamente dissociado do sistema a ser atacado abre muito maiores possibilidades de ataque, pois na página do sistema o usuário estária com as "guardas levantadas". Um fato também a ser enfatizado é que o usuário contaminante pode ser distinto do usuário a ser atacado. Por exemplo, o filho adolescente quando atraído para uma página de sexo pode ser induzido a dar o download num cavalo de tróia ao mesmo tempo que o material pornográfico esteja senão recebido pela rede, infectando a máquina. Mais tarde, quando o seu pai tentar acessar o sistema de home banking do seu banco o cavalo-de-tróia entra em ação.

3) Pela natureza dos ataques descritos por Santos e seus colaboradores em [7, 9] fica corroborada a hipótese de que ele realmente não teria entrado diretamente no sistema do banco, mas sim indiretamente.

Na próxima seção veremos algumas estratégias capazes de evitar, ou diminuir a probabilidade de tal tipo de ataque.

Prevenindo Ataques Futuros

0 autor deste artigo indicou para o Banco do Brasil, em outubro de 1998, várias medidas que poderiam ser adotadas para evitar este tipo de ataque e seus semelhantes, dentre as quais salientamos:

0 usuário não deve ter outra janela aberta quando acessar o site do home-banking do Banco do Brasil.

Neste caso o cavalo de tróia pode estar monitorando a outra janela simultaneamente com operações completamentes inóqouas. A idéia básica de proteção ao usuário é que apenas os processos realmente necessários, conhecidos e confiáveis estejam ativos quando do acesso.

Embutir um monitor de processos no BB-browser (versão privada do browser configurada para o Banco do Brasil) para não permitir a conexão com processos suspeitos ativos.

0 browser configurado para o Banco do Brasil automaticamente veria quais os processos estão ativos na máquina do usuário e caso algum. deles seja suspeito (por não ser um dos programas padrão normalmente utilizados pelos usuários) o acesso seria negado.

Note-se que tal estratégia possui limitações grandes, uma vez que se o cavalo de tróia for batizado com o nome de um processo semelhante a processos padrão do Windows, por exemplo, ele passará despercebido. 0 fornecedor de serviço tal como home-banking deverá negar o acesso ao usuário sempre que julgar que o usuário esteja em risco de ter sua privacidade violada.

Rodar a cada n acessos ao BB um "anti-vírus", que extermine o cavalo de tróia.

A análise do código executável residente na máquina permite verificar se o código inclui primitivas que indiquem que o código está enviando e-mails ou fazendo ftp sem o consentimento explicito do usuário. Tal anti-virus possui. uma sobrecarga grande, não devendo ser executado no momento do acesso, mas em algum outro tempo quando o sistema se mostre ocioso ou após ter sido procedido um determinado número de acessos.

Gerar procedimentos extras de segurança.

0 sistema de cadastro de um. banco possui várias informações particulares de cada um dos seus clientes, tais como estado civil, nome dos pais, número da cédula de identidade (RG), número do cadastro geral de contribuintes do Ministério da Fazenda (CIC ou CGC), nome do(a) cônjuge, endereço, local de nascimento, etc.

A solicitação de um desses dados a cada acesso (início de sessão) escolhido aleatériamente reduz grandemente a probabilidade do atacante possuir todas as informações do usuário.

É importante salientar que a medida de segurança aqui proposta (apresentada ao Banco do Brasil em outubro de 1998) é de muito simples adoção, exigindo apenas modificação trivial da interface do browser para solicitar um dos dados disponíveis aleatoriamente. Em meados de 1999, o Banco Bradesco S.A. passou a adotar tal medida de segurança , e curiosamente alguns clientes externaram o seu protesto por ter que "preencher mais um campo", não dando a devida importância a sua própria segurança .

Traçar o perfill econômico dos usuários.

Cada correntista possui um perfil econômico. A mudança do perfil econômico dos usuários é rara e pode gerar medidas que possam ir desde a confirmação pessoal das operações até a suspensão de operações e crédito do usuário. Por exemplo, um funcionário público recebe o seu salário em determinada data, possui débitos pré-acertados (água, eletricidade, telefone, seguros, etc.) em dias e rubricas conhecidas. Créditos podem acontecer esporadicamente e em valores que sejam compativeis com o seu perfil econômico. Por outro lado, uma conta de doações de um hospital possui perfil econômico completamente distinto do funcionário público. Se subitamente o funciondrio público passar a receber créditos de R$ 1,00, R$ 2,00, R$ 5,00 ou R$ 10,00 de todo o estado ou o pais algo de muito estranho estária acontecendo, pois haveria uma quebra do seu perfil econômico. Neste caso, haveria grandes chances de por alguma razão não explicada o funcionário público estar obtendo créditos indevidos de doações do hospital. Também haveria a hipótese menos honrosa de tal funcionário púlico ter infectado com cavalos-de-tróia, como o aqui descrito, toda uma gama de usuários e estar fazendo transferência entre contas de maneira indevida.

Traçar o perfil psicológico dos ladrões/invasores.

0 perfil psicológico de vários tipos de criminosos é bastânte estudado, pois através do seu estudo pode-se prever quando e como o seu próximo ataque ocorrerá. Por exemplo, o perfil psicológico de estrupadores é geralmente de um homem de idade entre 18 e 35 anos, solteiro, de baixa renda ou desempregado, boa complexidade fisica, etc. Os ataques geralmente ocorrem em lugares pouco freqtientados e nos finais de

sernana. Dificilmente um senhor de mais de 50 anos, casado e de classe média iria cometer tal tipo de crime. 0 perfil psicológico dos criminosos eletrônicos já vem sendo estudado há mais de uma década, porém o rápido avanço da computação abre sempre novas oportunidades de crimes. 0 perfil psicológico de que o criminoso eletrônico seria um funcionário do próprio banco, que se sentia oprimido e não reconhecido pelos seus superiores não é mais válido. (Embora os bancos mantenham sempre em perspectiva o perfil econômico de seus funcionários e monitorem constantemente o saldo de suas contas correntes). A Internet abriu as portas do banco e de seus sistemas computacionais ao mundo, sem nenhuma fronteira. Antes se cometia o crime e se fugia com o dinheiro para um paraiso fiscal ou para a Suiça. Hoje de um desses lugares se pode roubar o mundo em plena segurança . Romper as barreiras de segurança de sistemas tais como sistemas bancários ou que possuem informações confidênciais tornam-se um desafio para adolescentes não adaptados ao ensino convencional, ociosos e com acesso a máquinas. É raro encontrarmos entre tal tipo de atacantes alunos de doutorado em busca de auto-promoção.

Vale salientar que a violação de privacidade por si só já constitui crime previsto em lei, sem falar que no caso especifico aqui apresentado o invasor ainda está passivo de processo por perdas financeiras ocasionadas pela má propaganda gerada ao banco pelos seus atos.

Instruir os usuários.

Na Internet, os usuários tornam-se co-responsáveis pela sua própria segurança nos sistemas acessados, podendo em alguns casos comprometer a segurança de outros usuários em caso dele mesmo servir como cavalo-de-tróia para o sistema todo. É fundamental que os usuários passem a compartilhar tal responsabilidade com as entidades que oferecem serviços na Internet.

Ser-se roubado com porta de casa arrombada é diferente de ter sido roubado porque a porta da casa ficou aberta. Os usuários de sistemas na Internet devem ser educados para conhecer os riscos que correm e para tomar medidas de segurança cabíveis.

Confidencialidade de Informações.

A divulgação de informações (implementação, configuração, softwares utilizados, algoritmos, etc.) de sistemas onde a segurança das informações é critica não deve ser feita em hipótese alguma. Tal conhecimento diminui grandemente o espaço das opções de busca e aumenta a vulnerabilidade do sistema a ataques.

Conclusões

Neste artigo vimos em detalhes um tipo de ataque perpetrado ao sistema de home banking do Banco do Brasil. Os fatores de vulnerabilidade apontados pelo atacante, como aqui apresentados, não correspondem fidedignamente a realidade. A linguagem JAVA, um dos pontos fracos apontado pelo invasor, é uma linguagem onde segurança foi pensada como aspecto prioritário, senão possivelmente a linguagem mais segura para tal tipo de aplicação. De forma semelhante, o uso da criptografia proprietária utilizada é erroneamente apontada como senão uma das deficiências do sistema. Neste ponto o atacante está duplamente errado. 0 sistema IDEA [3, 4] utilizado pelo Banco do Brasil é considerado um dos mais seguros do

mundo, não tendo sido noticiada a sua quebra desde o seu lançamento em 1990. Este artigo não só analisa o ataque, trazendo uma explicação geral para a sua natureza, como também apresenta uma série de sugestões para evitar tal ataque e seus semelhantes. Medidas gerais de precaução para aumentar a segurança de sistemas são formuladas. Tal ataque demonstra que na Internet não somente as informações estão distribuidas, mas que a sua segurança também é distribuida, senão, os usuários co-responsáveis pela segurança das suas informações nos sistemas acessados e in *extremis* pela vulnerabilidade do sistema como um todo.

Referências Bibliográficas

1. **D.Dean, E.W.Felten, and Dan S. Wallach,** "Java Security: From HotJava to Netscape and Beyond". *Proceedings of 1996 IEEE Symposium on Security and Privacy.*
2. **D.Farmer**. The SATAN website. **Web documents at URL** `http://www.fish.com/dan/satan.html.`
3. **X.Lai.** *On the Design and Security of Block Ciphers,* Konstanz, Germany :Hartung-Gorre, 1992.
4. **X.Lai and J.Massey**. A Proposal for a New Block Encryption Standard, *Advances in Cryptology--Eurocrypt'90 Proceedings*, New York: Springer Verlag, pp.389-404, 1990.
5. **C.E.Landwehr, A.R.Bull, J.P.McDermott, and W.S.Choi.** A Taxonomy of Computer Program Security Flaws, ACM Computing Surveys, pp. 211-254, March 1994.
6. **G.McGraw and E.W.Felten.** Java Security - Hostile Applets, Holes, and Antidotes, Wiley Computer Publishing, 1977.
7. **F. de Paoli, A. L. dos Santos and R.A.Kemmerer.** Vulnerability of "Secure" Web Browsers. Proceedings of 20th National Information Systems Security Conference, October 1997.
8. **A.D.Rubin, D.Geer and M.J.Ranum**. Web Security Sourcebook, John Wiley & Sons, 1997.
9. **A.L. dos Santos, R.A.Kemmerer, F. de Paoli.** Secure Browsers? (Draft), August 1997.
10. As suas informações estão seguras? Byte Brasil, pp. é6-74, Novembro 1997, Editora Globo.