

# MÚLTIPLOS CERTIFICADOS NO CLIENTE PARA ACESSO A WEBSITES COMERCIAIS

Marcelo Iorino<sup>1</sup>, Flávio Arnaldo Braga da Silva<sup>2</sup>

Especialização em Desenvolvimento para a WEB, Depto. de Informática, Universidade Estadual de Maringá, contato@marinforma.com

<sup>2</sup> Professor Orientador, Depto. de Informática, Universidade Estadual de Maringá, flavio@din.uem.br

**Resumo.** *A segurança para a realização de transações via Internet deve ser redobrada, pois o ambiente de redes e inter-redes é, por definição, inseguro. A realização de transações exige que as partes tenham confiança entre si, o que só é possível de alcançar via mecanismos de autenticação. O sistema usual de autenticação que se encontra na maior parte dos sites é feito por meio de nomes de usuários e senhas. Infelizmente, esse mecanismo é passível de falhas e ataques por meios variados, alguns difíceis de detectar. Este artigo trata do uso de múltiplos certificados para clientes para acesso a Web sites organizados em múltiplas regiões.*

## 1. Introdução

O setor de comércio eletrônico, ou *e-business*, e alguns ramos especializados como bancos, financeiras e corretoras de valores apresentam um crescimento bastante elevado de alguns anos para cá, tanto no Brasil como no mundo. Isso se deve a diversos fatores: aumento do uso da Internet em todas as regiões do país; uso de lojas Web como forma de atender melhor os fregueses, incluindo aqueles que residem em locais distantes dos pontos de venda; redução de custos; possibilidade de oferecer uma gama maior de produtos; redução do número de empregados; maior escala e possibilidade de negociar melhor com os fornecedores; etc.

Infelizmente, com essas vantagens vem o registro do aumento do número de fraudes, principalmente pelo ataque aos clientes, que apresentam pouca cultura e treinamento para uso seguro de computadores e navegadores para a Internet.

## 2. Autenticação por usuário e senha

A autenticação de usuários é uma tarefa crítica para qualquer sistema e sujeita a diversas falhas que podem atingir tanto usuários quanto servidores.

Por exemplo, para *sites* que utilizam páginas dinâmicas montadas a partir de um banco de dados, invasores podem usar o ataque de injeção de SQL (SPI, 2002) (Macoratti, 2009) (Anley, 2002) (Cerrudo, 2003). Mesmo havendo técnicas para testar os valores que o usuário digita em campos de formulários, como, por exemplo, nas telas de *login*, os autores afirmam que o ataque por injeção de SQL é de difícil tratamento, pois o uso de bancos de dados associados a *Web sites* é muito difundido, o que torna os comandos de SQL um alvo importante. Além disso, há diversas técnicas que podem ser utilizadas nesse ataque e eventualmente surgem outras novas, o que obriga os administradores a se atualizarem constantemente.

---

<sup>1</sup> Tecnólogo em Tecnologia de Informática pela Universidade Estadual do Paraná -UNIPAR- Cianorte – PR

<sup>2</sup> Mestre em Ciência da Computação, ICMC – USP São Carlos

Por outro lado, o uso de senhas por si só pode representar uma vulnerabilidade. O Instituto SANS dos EUA, ligado ao FBI, afirma que o costume de se permitir acesso a determinados sites sem necessidade de passwords, ou sem exigir dos usuários que suas senhas sejam fortes (no sentido de resistir a ataques por parte de invasores), é uma das vinte principais vulnerabilidades da Internet (SANS, 2002). Senhas fracas podem ser quebradas, por exemplo, usando-se o ataque do dicionário (Pinkas, 2002) (CISCO, 2003), usuários podem fornecer suas senhas de boa fé em ataques de engenharia social (Granger, 2001) (Mitnick, 2003), computadores pessoais podem ser vítimas de ataques (vírus, rootkits, etc.), servidores também podem sofrer ataques ou ser clonados, etc. (Tanenbaum, 2007).

Isso faz com que ataques de personificação atinjam tanto clientes quanto servidores (ver Figura 1).

Para resolver esses problemas, a alternativa mais interessante é usar certificados digitais para substituir nomes de usuários e senhas como forma de autenticação.

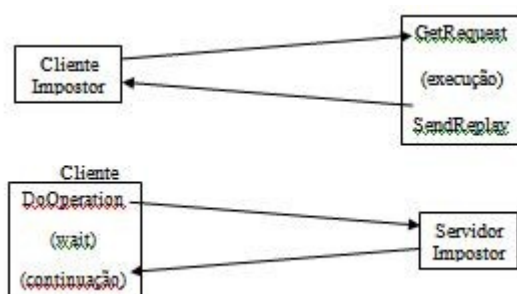


Figura 1. Personificação de clientes e servidores.

### 3. Certificado Digital

Uma questão central para o usuário é ter certeza de que ele está transacionando com o *site* correto, ou seja, que ele não está trocando informações com um *site* que poderá lhe prejudicar. Para domínios na Internet de instituições que fazem transações comerciais ou financeiras, exige-se a utilização do protocolo SSL<sup>3</sup> (OpenSSL, 2009). Para um servidor estabelecer uma conexão via SSL, ele precisa ter instalado um certificado digital associado ao domínio que o usuário pretende acessar. Por exemplo, o Banco Itaú utiliza certificados do padrão SSL 3.0 (Banco Itaú, 2009).

A geração e utilização de certificados digitais no Brasil são regulados pela ICP-Brasil (ICP-Brasil, 2009). O padrão internacional utilizado atualmente para certificados digitais é o X.509 (Cooper, 2008).

O uso de certificados digitais nos servidores torna mais segura a prática de atividades *online*, como o uso de Internet *banking*, sites de compras, etc. Notícias veiculadas na mídia especializada afirmam que o prejuízo dos consumidores americanos entre 2005 e 2006 com fraudes na Internet, vírus, spywares e phishing chegam a US\$ 7 bilhões, sendo que o risco calculado de um consumidor se tornar uma vítima pode chegar a 25% (Claburn,, 2007).

O certificado de um domínio permite usar o protocolo SSL, o protocolo usado para estabelecer comunicação segura na Internet. Com ele, toda a comunicação entre clientes e o servidor é criptografada, o que permite trocar informações sigilosas e críticas entre as partes, como números de cartão de crédito, contas bancárias, realizar compras, etc. (ver Figura 2) (Morimoto, 2008) (Mendes, 2003).

Todo certificado criado por uma autoridade certificadora (AC) apresenta um número de série. Uma consulta à AC por este número permite identificar o domínio real deste certificado e sua finalidade. O próprio certificado informa sua validade, portanto os usuários de um domínio têm

<sup>3</sup> Secure Socket Layer

condições de verificar se estão acessando o site correto (ver Figuras 3 e 4). Além disso, as ACs emitem relações de certificados revogados, as CRLs<sup>4</sup>. Por meio delas, é possível determinar se um certificado ainda é válido ou não. Domínios importantes procuram gerar seus certificados em ACs reconhecidas pelo mercado, como SertiSign, VeriSign e outras. Para atividades específicas, órgãos reguladores emitem certificados para seus usuários, como, por exemplo, a Receita Federal e a OAB.

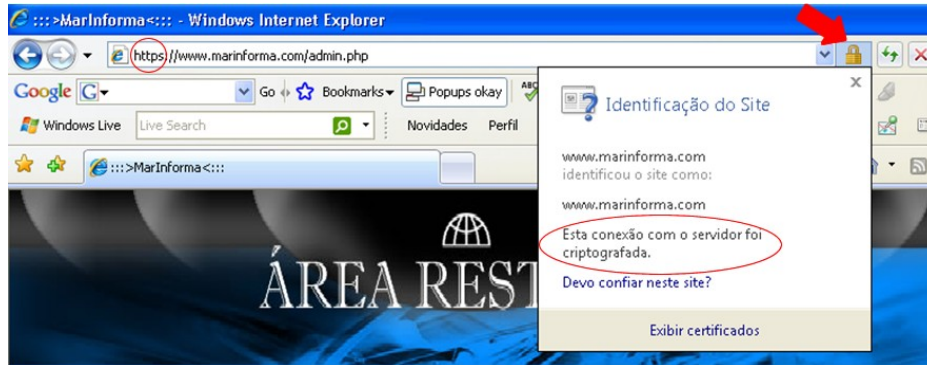


Figura 2. Identificação de um site seguro no navegador.

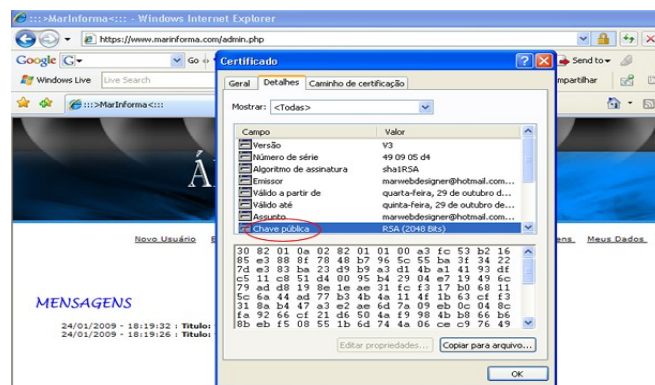


Figura 3. Informações detalhadas de um certificado.

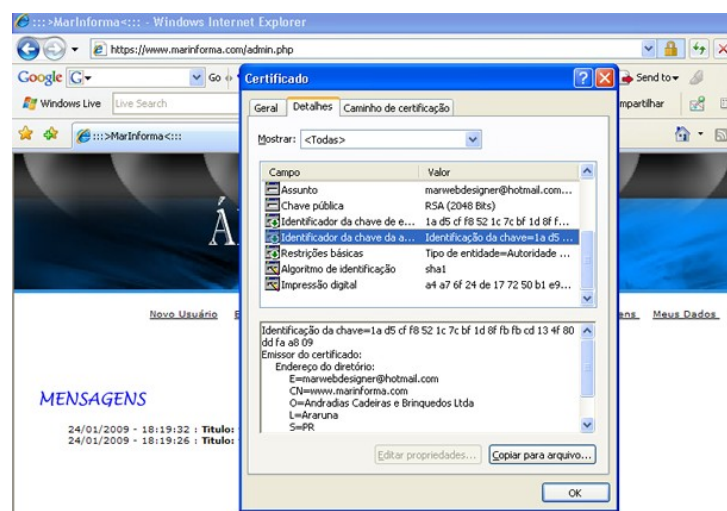


Figura 4. Dados de um certificado (identificação da chave pública).

<sup>4</sup> Certificate Revocation List

### 3.1 Certificados no Servidor

A organização que tem necessidade de estabelecer conexões seguras com seus clientes, ou porque os dados trocados entre as partes são sigilosos (por exemplo, a Receita Federal) ou porque pretende realizar transações comerciais ou financeiras, primeiro precisa ter um domínio registrado para o *site* que deseja tornar disponível. Precisa hospedá-lo em um provedor, que deve fornecer um número IP dedicado. O primeiro passo para emitir um certificado é solicitar do servidor um CSR<sup>5</sup>, um arquivo texto que contém as informações para solicitar seu certificado.

O CSR contém as seguintes informações:

- Informações de identificação da empresa que está solicitando o certificado digital;
- Chave pública;
- O tipo de servidor onde o certificado será instalado. (NetHorizontes, 2009)

Exemplo do CSR enviado pelo servidor:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB5DCCAU0CAQAwwgaMxCzAJBgNVBAYTAkJSMQswCQYDVQQIEwJQUjEJQMA4GA1UE
BxMHQXJhcnVuYTEtMCsGA1UEChMkQW5kcmFkaWFzIENhZGVpcmFzIGUgQnJpbnF1
ZWRvcyBMcGRhMRswGQYDVQQDExJ3d3cubWFyaW5mb3JtYS5jb20xKTAnBgkqhkiG
9w0BCQEWGm1hcndlYmRlc2lnbmVvYQGhvdG1haWwuY29tMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQCnSxQVVPqP459mowx3wkY3rIob6azPQOXdO+OiYRnmPXUx
XLkxOAmvAEtKyNwNxrXgOEEP2Px+H/IdkaZbhSQ5h7jEVGRTxizLJjiRZWWVix9x
kRuTqQGZ1MKG1oy8Ba6alZpHnKQN5mwXGH7glj2KFWtfz2BHDrxFZdnRGaBLEQID
AQABoAAAwDQYJKoZIhvcNAQEFBQADgYEAZ7XA6sqqqDuxsCz9gJnkQ/DHQpBuFMB
N/7HVekXfGV8R6kw3PI0x8MIqJOFnuUipiCsRdi6NXHhbgiklj5JahAP79JZRc4m
xnredEY2Sz/hzlxMcNXPgvb5D0YvqZE8riCDesDAZ7BKkEObk8kxkzBz/1e6kSiic
bKuXfgywCio=
-----END CERTIFICATE REQUEST-----
```

Private key

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCnSxQVVPqP459mowx3wkY3rIob6azPQOXdO+OiYRnmPXUxXLkx
OAmvAEtKyNwNxrXgOEEP2Px+H/IdkaZbhSQ5h7jEVGRTxizLJjiRZWWVix9xkRuT
qQGZ1MKG1oy8Ba6alZpHnKQN5mwXGH7glj2KFWtfz2BHDrxFZdnRGaBLEQIDAQAB
AoGBAITtSRXyIe23Je892yhFe9m9BThMon1DyeHSNnvNv/CMINSKIrSTHE6rYygX
FZLzaQBycnAPMAFfjNgl5ROPZUnvopgyT6uxzlcQ/CySeXOpXo6a5IR1qfh+eAf9
wSXQtM9c8nG7I9bd+1WXHwZtWlIbB5eGaf1CKZQjPfy8pAQBakEA3FP0wL8RIMlx
VzHksnDYsiR/avqkKMxM7+Yv2grXiZ295QQ0Rn1djpYSCBUxJ1RXhH8uXKLnio4i
2XHTAQyF4QJBAMJg96DmYwPuwqyqkIUePILTFiD0SQd1EiyVcBQ/GE0EEfEIKN76
RGCETomhahgZVCBgF4rcRPV7X/xQvfe6CzECQB65anESc+4tolnJcF3d1KoK4uXK
Mjfr3XK6w8OBLYtYPunXyz5Lw26KauM4PzeCxJD9gAfC3DL31o5QDZuO6ECQCI/
aYH89bcsqzo29y2tLSYzwPNfdzqMIv6d+dhnyYw4UNz3GiNnXwLobPQM7599Xvgx
VhSOSMwjx76yDzaFnhECQFyrQ5ygeqfbT2ib6Qdj50u+hSUOIB9avpQgDR/2nBWW
78kFPuTdASjzYwsdyKUGL0sWbkHy8alF3D1U6V0hTyQ=
-----END RSA PRIVATE KEY-----
```

O processo de geração da CSR e o processo de instalação final do certificado deve ser feito pelo administrador do servidor onde se encontra hospedado o domínio.

A organização deve criar uma conta em uma AC. Existem várias delas. Neste trabalho, foi utilizado a C O M O D O (Comodo, 2009).

Depois de preencher os dados solicitados pela empresa, ela envia um script do certificado para instalar no servidor do domínio. Acessando o *site* no seu domínio, o novo certificado é carregado em uma área própria para seu armazenamento. A Figura 5 apresenta a tela para adicionar um certificado, que pode ser diferente de servidor para servidor.

<sup>5</sup> Certificate Signing Request

Em *Add New Certificate*, abre-se a tela para informar os dados do certificado (ver Figura 6). A AC, então, pode, por exemplo, enviar o certificado por email. Recebendo o certificado, o administrador faz seu *upload* no servidor do domínio. O certificado instalado no servidor pode ser visto na Figura 7.

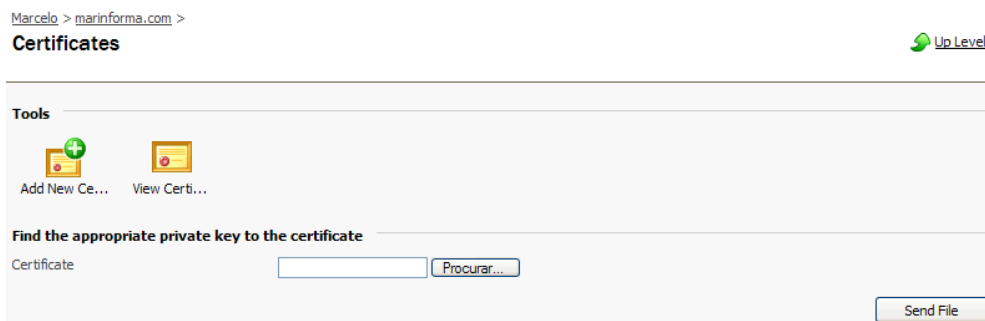


Figura 5. Tela para adicionar certificados no servidor de um domínio.

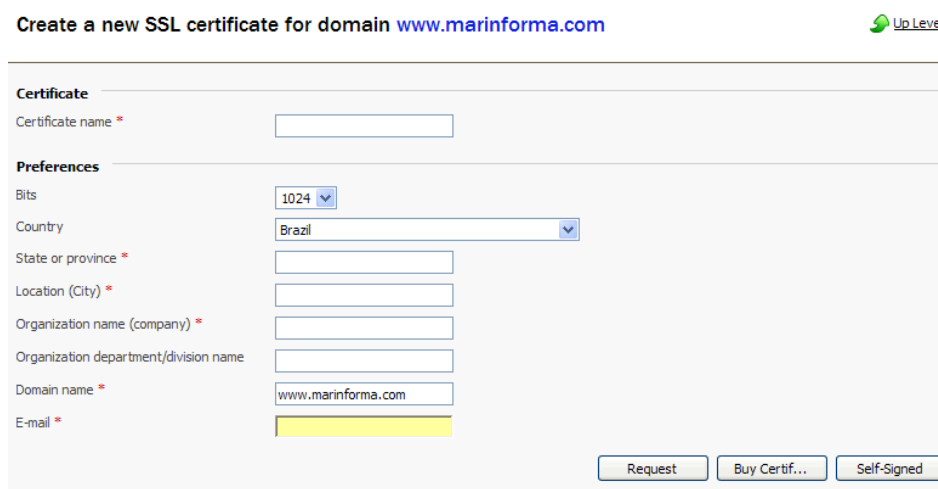


Figura 6. Dados do certificado informados para AC.

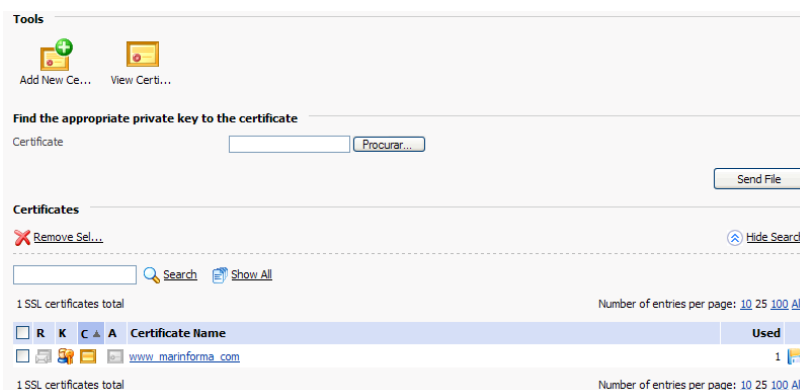


Figura 7 Certificados já instalados no servidor.

### 3.2 Certificados do lado do cliente

Se os consumidores, usuários e clientes de domínios na Internet sofrem grandes prejuízos com os ataques, da mesma forma os bancos, lojas e demais sites comerciais também são vítimas desse tipo de ataque. Por exemplo, a FFfebraban fez um levantamento e divulgou que, em 2006, os bancos tiveram prejuízos da ordem de R\$ 300 milhões (Manzoni Jr., 2006).

Antes que se pense que esses prejuízos devem ser assumidos pelos bancos ou por suas seguradoras, o STJ já decidiu em alguns casos que os clientes devem assumir esses prejuízos quando não tomam as medidas adequadas e necessárias para evitá-los, seja em suas ações ou por omissão. Assim, não se pode fazer uso do Código de Defesa do Consumidor e alegar defeitos na prestação do serviço quando a pessoa não toma os devidos cuidados na guarda de suas senhas e demais dados financeiros (Vainzof, 2004).

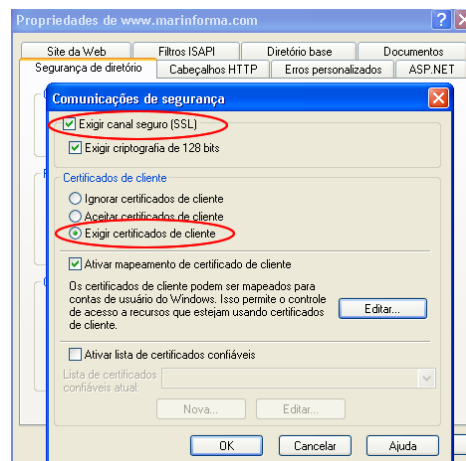
Portanto, é de interesse de ambos os lados que a autenticação dos clientes seja feita com a máxima segurança possível.

Vimos anteriormente que o mecanismo de usuário e senha é suscetível a uma série de problemas de segurança. Este trabalho propõe o uso de certificados digitais também do lado do cliente e, havendo necessidade, o uso de múltiplos certificados para garantir aos usuários diferentes direitos.

As vantagens do uso de certificados também pelos clientes são: ambos os lados (servidores e clientes) podem ter certeza de quem são seus pares; e os dados sigilosos podem trafegar por conexões criptografadas, ficando a salvo de espiões (Delgado, 2006).

Como desvantagens, podemos citar as seguintes: o uso de criptografia acrescenta uma carga extra pela necessidade de processamento para cifrar e decifrar as mensagens; e deve-se criar certificados únicos para todos os clientes cobrindo todos os direitos necessários para cada um (Delgado, 2006).

A exigência de certificados do lado do cliente é feita pelos servidores WWW. Na Figura 8, pode-se ver um servidor IIS<sup>6</sup> com a opção de exigir o certificado do cliente marcada. O certificado do cliente substitui a necessidade de fazer autenticação com usuário e senha. O certificado do cliente possui as informações do site para o qual ele é destinado. Alguns sites comerciais podem fazer uso de múltiplas regiões. Caso essas regiões sejam de acesso restrito, o usuário precisa identificar-se ou ter o certificado correspondente. Uma empresa pode ter um sistema Web controlando todo o seu funcionamento. Esse sistema tem regiões diferentes para, por exemplo, gerenciar as vendas, emissão de notas, cadastro de clientes e contas a pagar e receber.



**Figura 8.** Campo do IIS que exige certificados do cliente.

Um vendedor pode emitir um pedido. Para isso ele tem direitos específicos. Quando o cliente vai ao caixa e faz o pagamento, emite-se a nota fiscal. Se o cliente quer faturar a compra, ele precisa de um cadastro. O contas a receber faz o controle desses faturamentos emitidos.

<sup>6</sup> Internet Information Services

Para uma empresa com esse tipo de distribuição interna, pode-se ter uma organização da seguinte forma:

**Tabela 1 - Regiões de uma empresa**

Vendas	HTTPS://vendas.marinforma.com
Caixa	HTTPS://caixa.marinforma..com
Cadastro	HTTPS://cadastro.marinforma.com
Contas a receber	HTTPS://contas.marinforma.com

Cada uma dessas regiões necessita de um certificado diferente para dar os direitos de uso ao usuário. Caso uma pessoa tenha direito ou necessidade de fazer mais de uma dessas atividades, ela precisa ter todos os certificados correspondentes instalados em sua máquina.

Por exemplo, os dados de um certificado para o setor de emissão de notas poderiam ser os seguintes:

Identificação da chave de autoridade =

Identificação da chave=1a d5 cf f8 52 1c 7c bf 1d 8f fb fb cd 13 4f 80 dd fa a8 09

Emissor do certificado:

Endereço do diretório:

E=marwebdesigner@hotmail.com

CN=caixa.marinforma.com

O=Andradias Cadeiras e Brinquedos Ltda

L=Araruna

S=PR

C=BR

Número de série do certificado=49 09 05 d5

A instalação de qualquer certificado no computador do usuário pode ser feita pelo Painel de Controle em sistemas operacionais Windows. Opcionalmente, um usuário pode deixar seus certificados em um *smartcard* e conectá-lo a uma leitora de cartões quando necessário.

#### **4. Testes práticos**

Para a realização de um teste prático da proposta deste trabalho, foi criado um domínio ([HTTP://www.marinforma.com](http://www.marinforma.com)) e foi contratado um provedor para hospedá-lo.

Como servidor WWW, foi usado o IIS 6.0 da Microsoft. Sua configuração foi difícil, não tanto por causa do software em si, mas porque não foi possível encontrar suporte adequado. Descobrimos que, infelizmente, vários lugares que poderiam dar as informações necessárias não quiseram cooperar. Parece haver uma cultura de que o segredo é bom para alguns.

Felizmente, a configuração foi feita e o sistema funcionou.

Na prática, o funcionamento de um domínio com certificados é bastante simples. Havendo um certificado válido (ou mesmo vencido ou inválido, desde que o usuário o aceite), o navegador pode fazer uso de SSL para acessar suas páginas. Para isso, basta trocar o HTTP dos endereços pelo HTTPS.

Assim, o próprio usuário pode alterar os endereços das páginas que acessa para usar o HTTPS em lugares indevidos ou, o que é pior, tornar comum um acesso que deveria ser seguro.

Portanto, é de responsabilidade dos desenvolvedores colocar mecanismos em seus sistemas que impeçam os usuários de alterar os protocolos de acesso das páginas de um domínio.

Feito isso, o servidor IIS foi configurado para exigir certificados dos clientes. Na verdade, cada domínio deve ser configurado em separado para exigir do cliente um certificado correspondente.

A tentativa de um cliente acessar um domínio sem o certificado correspondente ou com um certificado inválido por qualquer motivo produz a seguinte mensagem de erro:

*HTTP 403.16 Forbidden: Client certificate untrusted or invalid.*

Com as várias regiões citadas na Tabela 1, um usuário com mais de um certificado consegue transitar de uma região para outra de forma transparente. O IIS simplesmente pede ao navegador os certificados correspondentes e autoriza o acesso caso esteja tudo certo. Se o usuário não possui o certificado de qualquer uma dessas regiões, a tentativa de acesso àquela parte do sistema produz o erro acima.

## **5. Conclusão**

Neste trabalho, foi verificado o uso de certificados em sites comerciais, tanto nos servidores como nos clientes. O uso de certificados aumenta a segurança dos sistemas Web, pois dá garantias para clientes e servidores da autenticidade de seus pares.

O sistema tradicional de autenticação baseado em usuários e senhas apresenta vários problemas associados e de difícil solução. Por outro lado, os certificados digitais representam uma solução viável para os problemas de autenticação de usuários e servidores.

No teste feito, pode-se verificar que o uso de múltiplos certificados substitui sistemas de controle mais complexos por parte dos desenvolvedores, principalmente nos casos em que um mesmo usuário deve possuir vários direitos diferentes, numa configuração que pode ser diferente dos demais usuários da instituição.

A segurança, nesse caso, é interessante porque se pode identificar cada pessoa com sua função, garantir o acesso de cada um às regiões que cada um precisa para poder realizar seu trabalho e acessar mais de uma região quando for o caso. O controle é realizado pela administração do site, portanto é possível fornecer a cada usuário apenas os certificados necessários para suas funções.

## **Referências Bibliográficas**

Anley, C., *Advanced SQL Injection in SQL Server Applications*, Publicação Interna, NGSSoftware, 2002.

Banco Itaú, *O que o Itaú faz pela sua segurança*, [http://www.itaubr.com.br/seguranca/itauseg\\_mecanismos.htm](http://www.itaubr.com.br/seguranca/itauseg_mecanismos.htm), acesso em /05/03/2009.

Cerrudo, C., *Manipulating Microsoft SQL Server Using SQL Injection*, Publicação Interna, Application Security, Inc., 2003.

CISCO Systems, Inc., *Dictionary Attack on Cisco LEAP Vulnerability*, Cisco Security Notice, 2003.

Claburn, T., *Viruses, Spyware, Phishing Cost U.S. Consumers \$7 Billion Over Two Years*, InformationWeek, 2007.

COMODO, *SSL Free Firewall Two Factor Authentication Products from Comodo*, <http://www.comodo.com>, acesso em 28/10/2008.

Cooper, D. et al., *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280)*, 2008.

- Delgado, G., *Advantages and Disadvantages of Client Side Certificates*, E-articles (2006), <http://e-articles.info/e/a/title/Advantages-and-Disadvantages-of-Client-Side-Certificates/>, acesso em 19/03/2009.
- Granger, Sarah, *Social Engineering Fundamentals, Part I: Hacker Tactics*, SecurityFocus Article, 2001.
- ICP-Brasil, “Portal ICP-Brasil” (2009), acesso em 19/03/2009.
- Macoratti, J. C., *Previna-se contra a Injeção SQL* (2009), [http://www.macoratti.net/sql\\_inj.htm](http://www.macoratti.net/sql_inj.htm), acesso em 09/03/2009.
- Manzonni Jr., R., *Febraban: fraudes eletrônicas somam R\$ 300 mi*, IDG Now, 2006.
- Mendes, H. das C., *Uma implementação livre do protocolo SSL*, <http://www.cic.unb.br/docentes/pedro/trabs/hammurabi.htm>, 2003, acesso em 28/10/2008.
- Mitnick, K., Simon, W. L., *A Arte de Enganar*, Editora Pearson, 2003.
- Morimoto, C. E., *Entendendo o mercado de certificados SSL*”, <http://www.guiadohardware.net/dicas/mercado-ssl.html>, acesso em 25/09/2008.
- NetHorizontes, *Serviços de Internet*, <http://www.nethorizontes.com.br/index.php?action=ssl>, acesso em 05/01/2009.
- Oliveira, J. N., Santos, L. e Amaral, L., *Guia de Boas Práticas na Construção de Web Sites da Administração Directa e Indirecta do Estado*”, <http://www.acesso.unic.pt/manuais/guiaboaspraticas.pdf>, acesso em 19/03/2008.
- OpenSSL, *OpenSSL: The Open Source toolkit for SSL/TLS*, 2009, <http://www.openssl.org/>. acesso em 02/03/2009.
- Pinkas, B., Sander, T., *Securing Passwords Against Dictionary Attacks*, em anais de ACM Computer and Communications Security Conference, 2002.
- SANS Institute, *The Top 10 Most Critical Internet Security Threats*, Publicação Interna, 2002.
- SPI Dynamics, Inc., *SQL Injection – Are Your Web Applications Vulnerable?*, White Paper, 2002.
- Tanenbaum, A. S., *Sistemas Operacionais Modernos*, 3ª. Edição, Prentice Hall Brasil, 2007.
- Vainzof, R., Cardoso, T. E., *STJ firmou entendimento sobre fraude na Internet*, Consultor Jurídico, 2004.