RUDNEI SANTOS GUIMARÃES

Análise comparativa de "sistemas de autenticação" utilizados em *Internetbanking*

Dissertação apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo – IPT, para obtenção do título de mestre em Engenharia de Computação.
Área de concentração: Redes de Computadores.

Orientador: Prof. Dr. Volnys Borges Bernal

São Paulo
2006

Ficha Catalográfica
Elaborada pelo Centro de Informação Tecnológica do
Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT

G963a Guimarães, Rudnei Santos
Análise comparativa de "sistemas de autenticação" utilizados em Internetbanking. / Rudnei Santos Guimarães. São Paulo, 2006.
100p.

Dissertação (Mestrado em Engenharia de Computação) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Área de concentração: Redes de Computadores.

Orientador: Prof. Dr. Volnys Borges Bernal

1. Autenticação de usuário 2. Internet (redes de computadores) 3. Segurança de acesso 4. Operação bancária 5. Operação financeira 6. Internetbanking 7. Tese I. Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Centro de Aperfeiçoamento Tecnológico II.Título

06-75 CDU 004.056'738.52(043)

AGRADECIMENTOS

Agradeço a Deus, pelas oportunidades que me foram dadas.

À minha esposa Márcia, por seu amor, companheirismo, compreensão e apoio nas horas difíceis.

Aos meus pais Neide e Ney e aos meus irmãos Telma e Walmor, que sempre estiveram ao meu lado, incentivando-me.

Ao meu orientador Prof. Dr. Volnys, pela paciência, dedicação e orientação, por me incentivar e ajudar.

Aos componentes da banca de qualificação, Profs.dr. Adilson e Geraldo, por seus comentários a este trabalho.

Aos meus amigos da Divisão de Redes Corporativas do BANESPA (ano 2001), em especial à Lílian e Graça, com os quais muito aprendi.

Aos professores do mestrado do IPT e colegas do LSI-USP.

E a todos que de alguma forma me ajudaram na conclusão deste trabalho.

RESUMO

O sistema de autenticação tradicional de usuário usado normalmente pelos *sites* WEB, que utiliza senha, é um ponto explorado pelos "assaltantes cibernéticos". Os usuários de *sites* do setor financeiro são as vítimas preferenciais. Os fraudadores empregam desde a construção e divulgação de falsos *sites* até programas maliciosos para a obtenção não autorizada das senhas de acesso dos usuários.

Os bancos brasileiros mantêm *sites* de *Internetbanking* nos quais os clientes podem efetuar transações bancárias. Para agregar maior segurança, o processo de autenticação dos *sites* de *Internetbanking* passou a utilizar teclados virtuais e, em determinadas transações, utiliza-se também uma terceira autenticação de usuário baseada em senha, normalmente denominada pelos bancos de assinatura eletrônica.

Outros sistemas de autenticação de usuário possuem maior sofisticação, dificultando a ação dos criminosos em obter as senhas de acesso: *tokens* OTP (*One Time Password*) geram um único código de acesso, válido por determinado período; utilização de chaves assimétricas que são armazenadas em arquivos ou em *smart cards* e PIN, utilizado em conjunto com dispositivos como *token*.

Este trabalho tem o objetivo de comparar as características destes sistemas de autenticação de usuário, como o nível de segurança, facilidade de utilização, necessidade de dispositivos específicos e custos.

Como resultado, apresenta uma seleção de parâmetros e subsídios para que o tomador de decisões escolha o sistema de autenticação que melhor se encaixe no seu sistema.

Palavras-chave: redes de computadores; internet; autenticação; segurança de acesso.

ABSTRACT

The traditional user authentication system used normally by the WEB sites, based in passwords, is a point explored by the “cybernetic assailants” and the users of the financial sites are the preferential victims. The robbers employ since the construction and disclosure of fake sites until malicious programs to get the users' password.

The Brazilian banks maintain Internetbanking sites, which the clients can perform banking transactions. To add greater security, the authentication process of the Internetbanking sites started to use virtual keyboards and, in specific transactions, also uses a third user authentication based on passwords, called by the banks as electronic signature.

Others types of user authentication are more sophisticated, complicating the action of the criminals in obtain the access passwords: tokens OTP (One Time Password) generate only one access code, valid for a period of time; utilization of asymmetrical keys stored in files or smart cards and PIN, used together with devices as tokens.

This work has the objective of compare the characteristics of these types of user authentication, as the security level, easiness of use, necessity of specific devices and costs.

As result, it presents a selection of parameters and subsidies so that the administrator can choose the better authentication type for your Internet system.

Keywords: computers networks; internet; authentication; security access.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

AC	Autoridade Certificadora
AIDs	*Application Identifiers*
API	*Application Program Interface*
DCS	Dados Críticos de Segurança
DES	*Data Encryption Standard*
DNS	*Domain Name System*
ECC	*Elliptic Curve Cryptosystems*
EMV	Europay, Mastercard e VISA
FEBRABAN	Federação Brasileira dos Bancos
FQDN	*Full Qualified Domain Name*
GSM	*Global System for Mobile Communications*
HSM	*Hardware Module Security*
HTTP	*Hypertext Transfer Protocol*
ICP	Infra-Estrutura de Chaves Públicas
IEEE	*Institute of Electrical and Electronic Engineers*
IETF	*Internet Engineering Task Force*
IPSEC	IP *Security*
ISO	*International Standard Organization*
ITI	Instituto de Tecnologia da Informação
ITU	*International Telecommunications Union*
LEA	Laboratório de Ensaio e Auditoria
LCR	Lista de Certificados Revogados
MAC	*Message Authentication Code*
NTLM	Microsoft Windows NT LAN Manager
OCSP	*Online Certificate Status Protocol*
OTP	*One Time Password*
PCMCIA	*Personal Computer Memory Card International Association*
PKCS	*Public Key Cryptography Standards*
PKI	*Public Key Infrastructure*
PIN	*Personal Identification Number*
RFC	*Request for Comments*

RSA	Rivest, Shamir e Adleman
SCQL	*Structured Car Query Language*
SIM	*Subscriber Identify Module*
SSL	*Secure Socket Layer Protocol*
URL	*Uniform Resource Locator*
USB	*Universal Serial Bus*
WAP	*Wireless Application Protocol*
WTLS	*Wireless Transport Layer Security*

SUMÁRIO

1 INTRODUÇÃO

A autenticação em um sistema computacional pode ocorrer em diferentes níveis, atuando em conjunto ou separadamente:

- Autenticação do usuário: procura distinguir um indivíduo dos outros, seja por características físicas, algo que possua ou saiba;
- Autenticação do parceiro de comunicação: são utilizados outros mecanismos de autenticação para assegurar a origem da comunicação;
- Autenticação da mensagem: os dados transmitidos passam por um processo de verificação para validar sua autenticidade.

A autenticação do usuário é um dos itens mais centrais do ponto de vista de segurança nas infra-estruturas WEB computacionais, cujo acesso pode ser realizado remotamente. Os sistemas de autenticação reconhecem o usuário baseado nos dados enviados para a autenticação.

Existem três categorias de autenticação de usuário que podem ser utilizados em conjunto ou separadamente:

- "o que se sabe";
- "algo que se possui";
- "o que se é".

Os sistemas baseados no que "se sabe", conhecido como prova por conhecimento, utilizam algo que somente usuário sabe, por exemplo, a senha. Também se encaixam nesta categoria os PINs.

Os sistemas baseados no que "se possui", conhecido como prova por posse, utilizam algo físico como cartões magnéticos, *smart cards* ou *tokens*. Podem utilizar PINs como garantia contra perda ou roubo.

Os sistemas baseados no que "o indivíduo é", conhecido por prova por biometria, tentam autenticar o usuário distinguindo-o dos demais mediante algo que o torne único.

A mais conhecida e a mais comum forma de autenticação do usuário utilizada pelos sistemas de autenticação é a senha. Ela não é a melhor alternativa de autenticação já que os usuários podem esquecê-las, anotá-las ou utilizar senhas que podem ser facilmente adivinhadas. Deste modo, o sistema de autenticação lida com vários desafios:

- Como coletar os dados do usuário para autenticação;
- Como fazer a transmissão destes dados de forma segura;

- Como saber se o usuário que está se autenticando realmente é ele;
- Como provar que um usuário se autenticou no sistema.

Este capítulo apresentará a motivação, o objetivo e a organização da dissertação.

1.1 Formulação do problema

A sofisticação do sistema financeiro, aliado à agilidade e ao crescimento da utilização da Internet, resultou num grande crescimento das transações pelo *Internetbanking*. Segundo a FEBRABAN (2006), em 2005 foram executados 5,849 bilhões de transações e a quantidade de clientes que utilizaram a Internet para efetuar transações financeiras aumentou 271% desde 2001, alcançando 26,3 milhões do total de 95,1 milhões de clientes.

O *Internetbanking* é um sistema apoiado no protocolo HTTP que permite ao cliente, utilizando um navegador, acessar remotamente o banco no qual possui conta-corrente e executar transações bancárias como pagamento de contas, transferência de valores, aplicações financeiras, por meio da Internet sem a necessidade de deslocar-se até a agência.

O sistema de autenticação do usuário mais utilizado no *Internetbanking* tem como base o conhecimento de uma senha. A senha pode ser adivinhada, observada e apresenta outros problemas.

Segundo Schneier (2004), os criminosos seguem o dinheiro. Utilizando táticas como envio de e-mails falsos, que induzem o cliente a utilizar *sites* fraudulentos ou a efetuar *download* de programas maliciosos como *keyloggers*, os criminosos conseguem as senhas de acesso ao *Internetbanking*.

Para melhorar a segurança do sistema de autenticação de usuário utilizando senhas, adicionalmente passou-se a utilizar frases secretas e teclados virtuais. Alguns clientes utilizam *softwares* de segurança como antivírus, *firewall* e *antispy*. Entretanto, estes incrementos não estão sendo suficientes para diminuir os prejuízos causados pelos crimes eletrônicos. Não estão disponíveis estatísticas relacionadas somente às fraudes na autenticação do usuário do *Internetbanking*. Entretanto, segundo a FEBRABAN (2006), as fraudes eletrônicas causaram prejuízos de R$ 300 milhões em 2005. Logo, acredita-se que também houve crescimento das fraudes relacionadas à autenticação do usuário.

Em um sistema de automação bancária, em que vários serviços financeiros podem ser utilizados por meio da Internet, o cliente necessita estar autenticado por meio do serviço de autenticação de usuário para usufruir destes serviços. O acesso não autorizado às informações sensíveis de autenticação pode implicar em prejuízos financeiros e comprometimento da

imagem e seriedade da instituição financeira, além da perda da confiança na utilização do sistema *Internetbanking* por parte do cliente.

Uma das grandes ameaças relacionadas ao acesso não autorizado é conhecida como personificação, que é caracterizada por um usuário passar-se por outro com o objetivo de acessar o sistema.

O processo de autenticação de usuário que se utiliza de senha apresenta fragilidade para validar eficazmente o cliente, sendo alvo de vários ataques com objetivo de obter os dados de acesso à sessão *Internetbanking* do cliente.

1.2 Objetivo do trabalho

O objetivo deste trabalho é analisar o sistema de autenticação mais utilizado em *Internetbanking,* aquele baseado em senha, e compará-lo com outros sistemas de autenticação de usuário que podem ser utilizados no *Internetbanking*, fornecendo subsídios para o profissional selecionar o sistema de autenticação que melhor se encaixe no seu sistema.

A análise dos sistemas de autenticação será efetuada utilizando parâmetros de comparação representativos. Tais parâmetros auxiliam a identificar vantagens e desvantagens dos sistemas de autenticação analisados. Estes parâmetros estarão agrupados em 3 classes: segurança, conveniência e economia (menor custo). Por exemplo, avaliar na classe segurança questões atuais relacionadas às fraudes, como a irretratabilidade e a personificação.

Neste trabalho são considerados "sistemas de autenticação" os programas, infra-estruturas de rede, equipamentos e processos necessários para que a autenticação do usuário ocorra. Engloba, por exemplo, o navegador utilizado pelo usuário para acessar o sistema *Internetbanking*, o canal de comunicação, os servidores e os dispositivos de autenticação.

1.3 Escopo do trabalho

O escopo deste trabalho é analisar os sistemas de autenticação utilizados nos sistemas de autenticação do usuário em ambiente WEB, focado em sistemas *Internetbanking*. São analisadas senhas, *tokens*, chaves assimétricas, certificação digital e *smart cards*.

Este trabalho não analisa sistemas de autenticação que utilizam biometria. Segundo Smith (2002, p. 218), não se pode acreditar nestes sistemas quando utilizados em uma rede não confiável, como a Internet, a menos que exista uma autenticação e garantia de integridade no equipamento de biometria e do sistema ao qual está conectado.

1.3.1 Arquitetura de referência

Neste trabalho será utilizada uma arquitetura de referência composta por um navegador WEB, um servidor WEB e seus sistemas de apoio, e um canal SSL/TLS estabelecido entre o navegador e o servidor WEB. A Figura 1 ilustra esta arquitetura de referência.

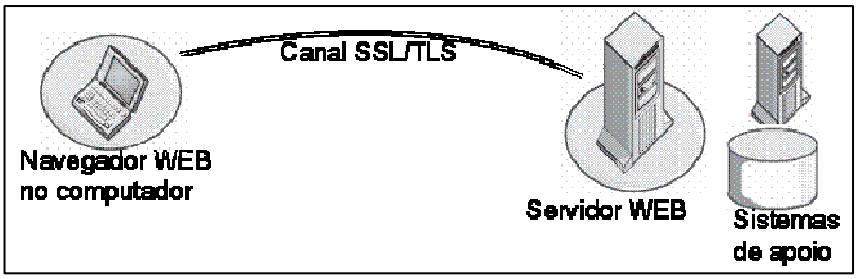


Figura 1: Arquitetura de referência

1.4 Levantamento da hipótese

De acordo com a verificação efetuada nos sites de *Internetbanking* dos cinco maiores bancos brasileiros em quantidade de agências em 2004, segundo o Banco Central do Brasil (BCB, 2005), a maioria dos sistemas de autenticação de usuário utiliza senha para autenticar o usuário.

Nesta forma de autenticação, o sistema de autenticação encontra dificuldades para evitar a personificação, tendo como conseqüência a dificuldade em provar que o usuário autenticado é realmente quem diz ser, anulando a irretratabilidade.

Os sistemas de autenticação de usuário que utilizam "prova por posse", se comparados aos sistemas de autenticação que utilizam senha ("prova por conhecimento"), possuem recursos para lidar com a personificação e, em alguns casos, garantir a irretratabilidade. Estes sistemas aproveitam o fato de que a identificação do usuário é feita com a apresentação de um dispositivo, difícil de copiar. A autenticação do usuário pode aproveitá-lo para validar suas credenciais, que podem ser requisitadas durante a utilização dos serviços disponíveis.

A utilização de sistemas de autenticação de usuário baseado em "prova por posse", em conjunto ou substituindo os sistemas baseados em "prova por conhecimento", poderá reduzir a personificação e garantir a irretratabilidade?

1.5 Justificativa da pesquisa

Anteriormente exploravam-se vulnerabilidades do sistema operacional, do servidor e do meio de comunicação. Entretanto, os investimentos em segurança feitos pelas instituições financeiras tornaram estes ambientes relativamente mais seguros, apesar de ainda estarem sujeitos a vulnerabilidades. Por outro lado, existe o aumento das fraudes financeiras, que exploram a ingenuidade ou a inabilidade dos clientes quanto aos requisitos de segurança a serem seguidos, tornando-as uma prática lucrativa.

Os clientes são alvos de várias vulnerabilidades que podem ser exploradas por criminosos. Pode-se citar a desinformação dos clientes sobre os conceitos de segurança, possibilitando a utilização de engenharia social contra eles; os provedores de Internet com problemas de segurança nos serviços disponibilizados, como DNS e *e-mails*; a facilidade de criação de *sites* fraudulentos; os computadores utilizados sem proteção; e o sistema de autenticação utilizado pelos bancos.

Trabalho relacionado com o tema autenticação, como "*Comparing Passwords, Tokens and Biometrics for User Authentication*" (O'Gorman, 2003), faz uma análise dos sistemas de autenticação, dividindo-os em três grandes grupos: senhas, *tokens* em biometria. Entretanto, a análise não é voltada para ambientes WEB e o trabalho não relaciona os possíveis controles que podem ser utilizados para reduzir o risco de exploração das vulnerabilidades. Em "*Securing Passwords Against Dictionary Attacks*" (Pinkas; Sander, 2002), "Autenticação Utilizando Senhas Descartáveis Baseadas em caos" (Santos; *et al.*, 2004), "Apresentação de senhas em máquinas hostis"(Lagares; Souza, 2005) e "*Improving The Diceware Memorable Passphrase Generation System*" (Carnut; Hora, 2005) propõem novas abordagens para autenticar o usuário por meio de senhas. No entanto, estas abordagens não são comparadas com outros sistemas de autenticação. Em "*Building Security and Trust in online banking*" (Nilsson; Adams; Herd, 2005), aborda somente a percepção do usuário do *Internetbanking*, com relação à segurança.

A contribuição deste trabalho foi estudar os sistemas de autenticação utilizados e os que podem ser utilizados pelos bancos, com o intuito de fornecer subsídios para a tomada de decisão sobre o sistema de autenticação que melhor se adapte às necessidades de negócio.

1.6 Metodologia

A metodologia utilizada na comparação tem como base o trabalho de O'Gorman (2003)

que avalia características como segurança, conveniência e custo. Segurança é mensurada pelas vulnerabilidades que podem ser exploradas e os controles utilizados. Conveniência é um fator subjetivo, associado à comodidade do usuário em lembrar uma senha complexa ou carregar um dispositivo para se autenticar. O custo engloba desde a infra-estrutura necessária, a logística de distribuição até o suporte ao usuário. Neste trabalho, esta característica será avaliada como economia. Quanto mais econômico um sistema de autenticação, menores são os custos.

Esta dissertação acrescenta, em relação ao trabalho de O'Gorman, novos parâmetros de comparação e outros sistemas de autenticação. Cada sistema de autenticação tem sua avaliação individual, para depois serem apresentados em conjunto, no formato de tabela. Este formato facilita a comparação entre os sistemas de autenticação e permite estimar vantagens em utilizar mais de um sistema de autenticação conjuntamente.

A condução da pesquisa consolidada neste trabalho compreendeu as seguintes atividades:

- Levantamentos bibliográficos;
- Pesquisas para identificar o sistema de autenticação de usuário mais utilizado pelos cinco maiores bancos no Brasil;
- Pesquisas de outros mecanismos de autenticação;
- Identificação das vulnerabilidades dos mecanismos de autenticação;
- Identificação dos controles utilizados pelos mecanismos de autenticação.
- Comparação das características.

1.7 Estrutura da dissertação

Este trabalho está dividido em 8 capítulos. O Capítulo 1 é esta introdução. O Capítulo 2 apresenta os principais serviços de segurança. O Capítulo 3 descreve o sistema de autenticação mais utilizado. O Capítulo 4 relaciona outros sistemas de autenticação pouco utilizados ou que podem ser utilizados. No Capítulo 5 são mostradas as vulnerabilidades e os controles dos sistemas de autenticação descritos anteriormente. O Capítulo 6 apresenta a comparação entre os sistemas de autenticação. No Capítulo 7, são apresentados dois estudos de caso. Finalmente no Capítulo 8, a conclusão do trabalho mostrando se o objetivo principal foi atingido.

2 SERVIÇOS DE SEGURANÇA

Os serviços de segurança são funcionalidades específicas de segurança oferecidas por procedimentos ou componentes (*software* e *hardware*) com a intenção de garantir segurança adequada aos sistemas ou à comunicação.

2.1 Principais serviços de segurança

A seguir serão descritos os principais serviços de segurança.

2.1.1 Identificação do usuário

A identificação do usuário é um serviço de individualização de usuário perante o ambiente. O método mais utilizado é exigir do usuário um código que o identifica no sistema (NIST,1995). Por exemplo, no *Internetbanking*, o cliente é identificado pelo número da conta-corrente, código do usuário ou ambos, atuando em conjunto

2.1.2 Controle de acesso

O serviço controle de acesso procura certificar que somente os usuários autorizados tenham acesso aos recursos do sistema (Smith, 2002).

2.1.3 Confidencialidade

O serviço de confidencialidade garante que os dados armazenados ou em trânsito são acessados exclusivamente pelos usuários autorizados (NIST,2001).

Por exemplo, nos sistemas baseados no protocolo HTTP, a confidencialidade no canal de comunicação de dados geralmente é mantida pelo protocolo SSL ou TLS.

2.1.4 Integridade

O serviço de integridade permite detectar quando uma informação foi alterada por uma entidade não autorizada ou por um erro de sistema (NIST,2001).

Por exemplo, a utilização de digesto (*hash*), gerado por meio de funções de espalhamento (funções *one-way hash*) ou assinatura digital[1], para assegurar que a mensagem não sofreu modificações.

2.1.5 Irretratabilidade

O serviço de irretratabilidade provê evidências em que o emissor e o recebedor dos dados não possam negar que tenham participado da comunicação.

A norma ISO 13888-1 (2004) especifica diferentes tipos de irretratabilidade:

a) Irretratabilidade da criação: garante que entidade criou o conteúdo da mensagem, não podendo negá-la;
b) Irretratabilidade da origem: garante a origem da mensagem, não podendo negar seu envio ou a inexistência de conteúdo;
c) Irretratabilidade da entrega: garante que a mensagem foi entregue, não podendo negar sua recepção ou a inexistência de conteúdo;
d) Irretratabilidade do conhecimento: garante que o recebedor da mensagem não possa negar o conhecimento do seu conteúdo;
e) Irretratabilidade da submissão: garante evidências que o responsável pelo envio da mensagem a tenha aceitado para transmissão;
f) Irretratabilidade do transporte: garante ao remetente que o responsável pelo envio tenha entregado a mensagem ao destinatário da mensagem.

A principal necessidade de irretratabilidade nos sistemas de *Internetbanking* é a irretratabilidade da criação de uma transação.

2.1.6 Autenticação de usuário

O serviço autenticação do usuário permite validar o usuário que está se identificando. Geralmente é utilizada uma chave de autenticação. A chave de autenticação é verificada perante o sistema nesta fase (NIST,2001).

O usuário é autenticado fornecendo algo que o torne único, algo que possua ou algo que apenas ele conheça como, por exemplo, a senha.

---

[1] Assinatura digital é comentada no Capítulo 4.

2.1.7 Autenticação da mensagem

O serviço autenticação da mensagem garante que a mensagem foi gerada por uma determinada entidade ou grupo (NIST,2001).

2.1.8 Autenticação do parceiro de comunicação

O serviço autenticação do parceiro de comunicação permite identificar a outra entidade envolvida em uma sessão de comunicação (NIST,2001).

Por exemplo, no sistema *internetbanking*, o servidor WEB é identificado utilizando processo de certificação digital[2], que comprova autenticidade do servidor.

2.1.9 Disponibilidade

O serviço disponibilidade possibilita garantir que os recursos que compõem o sistema estejam livres para as entidades autorizadas, no período de utilização. Também assegura que os recursos do sistema são usados somente para os propósitos a que foram designados (NIST, 1995).

2.2 Conclusão

Neste capítulo foram apresentados e definidos os principais serviços de segurança, importantes para as seções seguintes, com intuito de descrever os conceitos indispensáveis para a compreensão da segurança nos ambientes WEB e uniformizar a terminologia.

---

[2] Certificação digital é comentada no Capítulo 4.

3 SENHA: AUTENTICAÇÃO TRADICIONAL

Os bancos brasileiros na maioria das vezes utilizam senhas para autenticar seus clientes no sistema *internetbanking*.

3.1 Origem

Quando surgiram os primeiros computadores não havia a necessidade de autenticação. Segundo Smith (2002), o controle de acesso físico ao ambiente no qual se localizavam as gigantescas máquinas era o principal controle.

No início da década de 1960, com o surgimento dos computadores multi-usuários, surgiu a necessidade de identificar o usuário que estava utilizando o computador, para criar e manter ambientes privativos para cada usuário. Desta necessidade foram criados os primeiros programas de autenticação que foram aperfeiçoados ao longo do tempo.

O princípio deste modo de autenticação ainda é utilizado até os nossos dias: digita-se a identificação do usuário (também conhecida como *login* ou sigla) e uma senha. No entanto, a forma de armazenamento tem mudado constantemente. Os primeiros sistemas de autenticação armazenavam a sigla e senha em arquivos-texto, fáceis de serem lidos. Devido às vulnerabilidades deste tipo de armazenamento, pois as senhas podiam ser lidas facilmente, as senhas passaram a ser armazenadas de modo cifrado.

De acordo com Smith (2002), em seguida passou-se a utilizar funções *one-way cipher*, atualmente conhecidas como *one-way hash*, para armazenar as senhas, tendo como propriedade que o processo inverso não é possível. Entretanto, estes métodos são suscetíveis a ataques por força bruta[3] e ataques por dicionário de dados[4]. Para minimizar o risco de ataques, introduziu-se mais uma variável na geração do *hash*, conhecida como *salt*. *Salt* é um número aleatório, com tamanho de 12 *bits*, utilizado no processo de *hashing* como forma de possibilitar uma variação do resultado do código *hash*. Isto permite que a mesma senha tenha *hash* diferente toda vez que ela passar pela função.

O novo algoritmo fez com que ataques para descobrir a senha por força bruta se tornassem inviáveis nas décadas de 1960 e 1970 em decorrência do tempo para processar

[3] Método para descobrir a senha testando todas as combinações possíveis.
[4] Método para descobrir a senha utilizando uma relação das senhas mais prováveis.

todas as combinações possíveis. No entanto, ainda está suscetível contra tentativas de acesso utilizando ataques por dicionário de dados.

Os sistemas de codificação e armazenamento de senhas que não utilizam *salt* são também suscetíveis a ataques com base pré-compilada de codificação de senhas. Um exemplo deste ataque ocorre no NTLM[5] e NTLMv2.

3.2 Tipos de Senhas

No ambiente de *Internetbanking* as senhas são utilizadas para autenticar os clientes. A conta corrente e, em alguns casos, um nome de acesso são utilizados para a identificação.

O termo senha inclui palavras e frases que são mantidas em segredo pelo usuário e utilizadas para autenticação de usuário ou da transação eletrônica realizada por ele. Existem outros sistemas de autenticação baseados em senhas como frases secretas, assinaturas eletrônicas, desafio-resposta e lista de senhas.

Segundo Paine e Burnett (2002), a frase secreta é uma seqüência de caracteres utilizada como senha que é transformada em uma senha virtual com um tamanho padrão.

A assinatura eletrônica utilizada nos sistemas *Internetbanking* pelos bancos brasileiros é empregada para realizar uma nova autenticação do usuário. O usuário pode entender que a assinatura eletrônica é mais segura que a senha inicial usada para obter acesso ao ambiente *Internetbanking*.

O termo "assinatura eletrônica", utilizado pelos bancos brasileiros nos sistemas *Internetbanking*, não é adequado. De acordo com NIST-800-12 (1995, p.230), a assinatura eletrônica é um mecanismo criptográfico que possui função similar ao da assinatura em papel[6]: prover autenticidade e irretratabilidade. Este mecanismo pode ser implementado, por exemplo, utilizando chave simétrica (um segredo compartilhado pelo usuário e o sistema de autenticação) ou chaves assimétricas (assinatura digital[7]).

A assinatura eletrônica de uma mensagem utilizando chave simétrica é o resultado de uma função que produz um identificador conhecido como MAC (*Message Authentication Code*), utilizado para autenticar a mensagem. Esta função tem como característica que a alteração de pelo menos um bit da mensagem modifica o MAC. Para maiores informações sobre o MAC, consultar a referência RSA (2005).

---

[5] Protocolo de autenticação utilizado pelo sistema operacional Microsoft Windows NT.
[6] Assinatura com reconhecimento de "firma"em cartório.
[7] Chaves assimétricas e assinatura digital são comentadas no capítulo 4.

Logo, o usuário não poderia negar que executou a transação. No entanto, será visto neste trabalho que a senha e suas variações, como a assinatura eletrônica, não apresentam mecanismos que dificultem a personificação e não provêem irretratabilidade.

3.2.1 Senhas

A senha é uma seqüência de caracteres que deve ser mantida secreta e memorizada pelo usuário. Ela é um segredo conhecido pelo usuário e pelo sistema de autenticação. Para obter acesso o usuário deverá lembrá-la e utilizá-la. O sistema de autenticação permitirá o acesso se a senha informada for igual à armazenada.

Pode-se avaliar a qualidade da senha pela quantidade total de combinações possíveis. Este número de combinações é denominado espaço de chaves (*keyspace*). O *keyspace* de uma senha é descrito pela relação:

$$S=A^n,$$

no qual S é a quantidade de senhas possíveis, A é a quantidade de caracteres que podem ser utilizados para formar a senha e n é o tamanho da senha (Smith, 2002). Uma senha numérica de três dígitos tem o *keyspace* de 1.000. Já uma senha numérica com quatro dígitos tem o *keyspace* de 10.000.

Segundo Smith (2002), um outro modo de avaliar a senha é pela entropia. A entropia mostra a relação estatística de como os usuários selecionam a senha. Quanto maior a entropia, menor a chance de adivinhar a senha.

A entropia é o tamanho do *keyspace* em *bits.* É descrita pela relação:

$$B=log_2(S).$$

A Tabela 1 apresenta uma comparação entre *keyspace* e entropia, para senhas numéricas de 4 e 6 dígitos. Pode-se observar que quanto maior o tamanho (*N*) da senha, maior é o número de combinações possíveis (*keyspace*). Consequentemente, maior é a entropia.

Tabela 1: Comparação entre *keyspace* e entropia

N	***Keyspace***	**Entropia**
4	10.000	14
6	1.000.000	20

A entropia de uma senha é afetada pela tendência dos usuários de não escolherem senhas aleatórias ou pelo fato das senhas ficarem limitadas aos caracteres do teclado do computador (Smith, 2002). Por exemplo, considere uma senha cujo tamanho seja de 4

caracteres e somente possam ser utilizados números, e uma senha na qual, além de números, as letras também possam ser utilizadas.

A entropia do primeiro tipo de senha seria de 14 *bits*. A entropia do segundo tipo de senha seria:

$$S=36^4$$
$$B=log_2(36^4)$$
$$B=20,68\ ,$$

ou seja, aproximadamente 21 *bits*.

A quantidade de combinações possíveis para a senha formada por letras e números permite que ela seja mais resistente à adivinhação que a senha formada somente por números.

Smith (2002 p. 68) ainda descreve outro método para avaliar a qualidade das senhas, utilizando os conceitos de *keyspace* e entropia. Este método, chamado de "espaço médio de ataque", permite estimar a resistência da senha em relação às tentativas necessárias para descobri-la.

Assim como a entropia, o espaço médio de ataque pode ser influenciado pela tendência dos usuários em escolher senhas comuns. Seu valor pode ser calculado pela fórmula:

$$EMA = \log_2\left(\frac{S}{2 \text{ x } L}\right),$$

no qual S é a quantidade de combinações (o *keyspace*) e L é um coeficiente que indica a probabilidade de usuários propensos a escolher senhas triviais. O parâmetro L representa o conceito da entropia, descrito anteriormente. Segundo Smith (2002), o divisor 2 reflete a necessidade de pesquisar a metade das combinações, em média, para descobrir a senha. O espaço médio de ataque é representado na base 2, pois pode assumir valores muito altos.

Por exemplo, suponha um sistema de autenticação que utilize senha numérica, com tamanho de quatro dígitos. O valor de S seria 10.000 (o *keyspace*). Considere ainda que todos os usuários deste sistema de autenticação escolham a senha aleatoriamente. Neste caso, o valor do espaço médio de ataque seria aproximadamente de 13 *bits*.

Agora, suponha que, após uma pesquisa, descobriu-se que metade dos usuários do sistema de autenticação escolhe a senha tendenciosamente no formato MMDD. O valor de S seria 366; o valor de L seria 0,5. Neste exemplo, o valor do espaço médio de ataque seria aproximadamente de 9 *bits*. A tentativa em descobrir a senha caiu de aproximadamente 5.000 (2^{13}) combinações para em torno de 512 (2^9) combinações.

3.2.2 Frases secretas

A utilização de frases secretas aumenta a entropia e a aleatoriedade da senha em relação a uma senha escolhida pelo usuário. Possui a vantagem de ser facilmente memorizada pelo usuário se comparada a uma senha longa e complexa. É mais fácil para um usuário lembrar uma frase do que uma seqüência grande e aleatória de caracteres.

O valor da senha é obtido geralmente por um processo de *hashing* sobre a frase secreta escolhida pelo usuário.

A Tabela 2 apresenta a entropia aproximada de várias combinações, utilizando caracteres numéricos e alfabéticos e tamanhos variados de senhas (N).

Tabela 2: Comparação da entropia entre várias combinações

N	**26** (letras minúsculas)	**36** (letras minúsculas + números)	**62** (letras minúsculas e maiúsculas e números)	**95** (caracteres imprimíveis do teclado)
5	24	26	30	33
10	47	52	60	66
15	71	78	90	99
20	94	104	120	132
25	118	130	150	165
30	141	156	179	198

(Adaptado de MENEZES; OORSCHOT; VANSTONE, 1996, p. 392)

O grande tamanho (*N*) e uma maior quantidade de elementos para criar a senha permite que a frase secreta seja bastante resistente à adivinhação.

3.3 Protocolos de autenticação baseados em senha

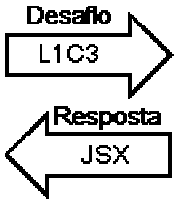
As senhas podem ser solicitadas ao usuário de vários modos pelos sistemas de autenticação baseados em senha. Os usuários podem responder a uma requisição ou serem desafiados, por exemplo. A seguir, serão descritos os principais protocolos de autenticação do usuário.

3.3.1 Requisição-resposta

O protocolo requisição-resposta é o mecanismo tradicional de autenticação de usuário no qual a senha é solicitada pelo sistema de autenticação para autenticar o usuário.

3.3.2 Desafio-resposta

Neste tipo de autenticação, o usuário responde a um desafio feito pelo servidor de autenticação. A resposta é selecionada a partir de uma matriz impressa[8] em papel, baseada no desafio. A Figura 2 mostra exemplo de desafio-resposta no formato de matriz impressa e a Figura 3 mostra exemplo no formato de tabela.



	C1	C2	C3
L1	KBC	GMA	JSX
L2	YHQ	RVT	TOD
L3	PEZ	UIW	CXF

Figura 2: Exemplo de matriz para desafio-resposta

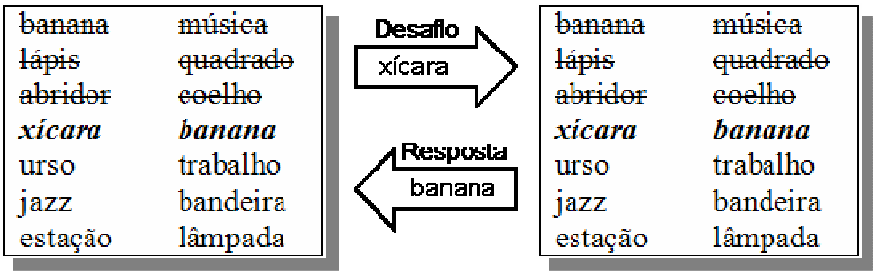


Figura 3: Exemplo de tabela para desafio-resposta

3.3.3 Lista de senhas

A lista de senhas é um conjunto de senhas que são utilizadas seqüencialmente pelo usuário para acessar o sistema de autenticação. A lista de senhas deve ser utilizada na ordem que é apresentada, caso contrário o sistema não conseguirá identificar corretamente o usuário. Figura 4 mostra exemplo de lista de senha.

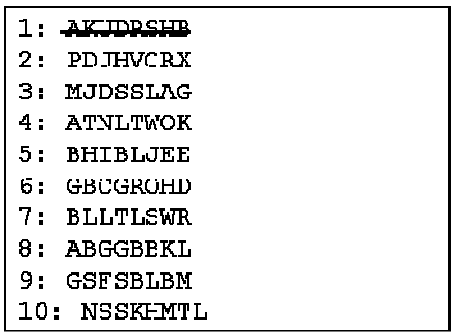


Figura 4: Exemplo de lista de senhas

[8] Termo utilizado para designar o cartão de papel nas quais as respostas estão impressas no formato de matriz ou tabela.

Existe um método desenvolvido por Lamport, conhecido como "protocolo *challenge-response*" (Smith, 2002) (Chapman; Zwicky, 1995), no qual o protocolo utiliza uma função *hash* "*one-way*" desenvolvida por Diffie-Hellman e uma seqüência de códigos *hashs*, sendo cada código *hash* derivado do código *hash* anterior (Lamport, 1981). Somente o último código *hash* é armazenado.

3.3.4 S/Key

O protocolo S/Key, criado pela Bellcore na década de 1990 é uma implementação do método desenvolvido por Lamport (Haller, 1994). Este protocolo opera com base em um valor "N" e na utilização de uma semente (*seed*). Segundo Haller (1994), o protocolo S/Key pode ser utilizado para gerar uma lista de senhas ou como protocolo desafio-resposta.

De acordo com Chapman e Zwicky (1995), o protocolo S/Key permite autenticar o usuário sem necessidade de armazenar dados sensíveis que possam comprometer a autenticação do usuário e possui a habilidade de validar o usuário, mas não possui a habilidade de predizer a próxima senha. A seguir será explicado o protocolo S/Key de acordo com (Chapman; Zwicky, 1995) e Smith (2002).

No protocolo S/Key o valor "N" é utilizado para gerar um conjunto de senhas por meio de um algoritmo *one-way hash*, tendo como base a senha anterior. No primeiro acesso deve-se utilizar a penúltima senha, no segundo, a antepenúltima e assim sucessivamente. A última senha nunca é utilizada pelo usuário.

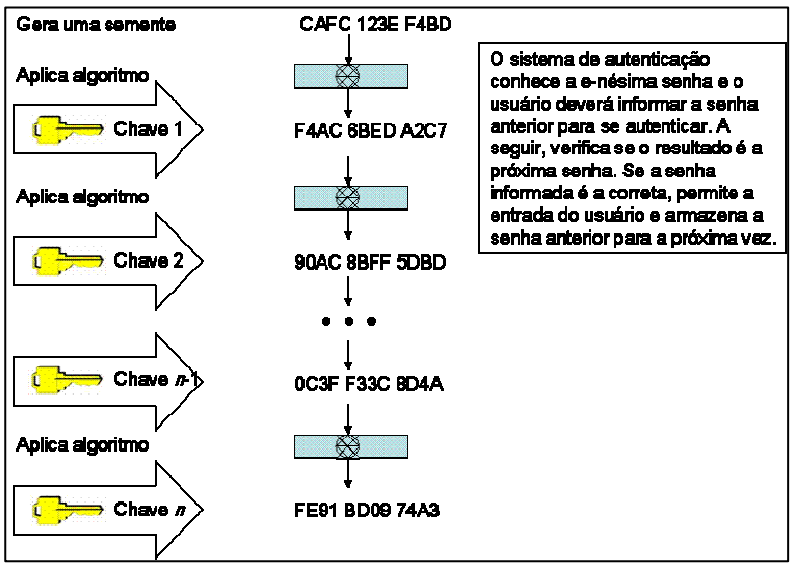


Figura 5: Funcionamento do protocolo S/Key
Fonte: Chapman; Zwiccky, 1995, p.361

O protocolo S/Key precisa de uma semente para gerar a primeira senha. A semente pode ser criada pelo usuário ou mediante a utilização de um algoritmo gerador, no qual o usuário digita uma parte da semente (um segredo) e a outra parte da semente é gerada aleatoriamente pelo algoritmo. A semente criada nesta forma tem a vantagem de que a utilização do mesmo segredo pelo usuário não produzirá o mesmo conjunto de senhas. A Figura 5 mostra o funcionamento do protocolo S/Key.

Quando o protocolo S/Key é utilizado como lista de senhas, o conjunto de senhas é impresso e entregue ao usuário.

Suponha, por exemplo, que o usuário deseja ter o direito de acessar um sistema 10 vezes. Utilizando um processo confiável, o usuário fornece seu segredo para compor a semente. Uma lista de senhas é gerada contendo 11 senhas a partir da semente. A última senha é guardada pelo sistema de autenticação (nunca será utilizada pelo usuário). O segredo fornecido pelo usuário ao sistema de autenticação não tem mais utilidade e é desprezado. O usuário utiliza a décima senha para se autenticar. Através desta senha, a décima primeira senha é calculada e verificada se está igual ao que está guardada. Sendo a senha válida, o sistema guarda a décima senha. O usuário deverá digitar a nona senha no próximo acesso e assim sucessivamente até terminar a quantidade de acessos.

Quando o protocolo S/Key é utilizado como desafio-resposta, o número da senha a ser informada e a parte da semente que o usuário não conhece são mostrados ao usuário. O usuário digita estes dados em um *software* que fornece a senha a ser respondida.

3.3.5 *Zero knowledge password*

Em um sistema de autenticação que utiliza senha, o usuário deve enviar a senha para se autenticar. No protocolo *zero knowledge password*, a senha não é enviada. A autenticação é realizada por meio de troca de mensagens (desafio-resposta) até que a entidade verificadora esteja convencida de que o usuário conhece a senha (Menezes; Oorschot; Vanstone, 1996).

Segundo Smith (2002), o protocolo *zero knowledge password* amplifica a entropia da senha mediante a geração de uma senha válida para uma sessão, com alta entropia. O protocolo *zero knowledge password* é uma implementação do protocolo *zero knowledge proof* para ser utilizado com senhas e efetuar autenticação mútua.

O protocolo *zero knowledge proof* permite ao usuário provar que conhece o segredo sem revelá-lo ao sistema de autenticação. Segundo Aronsson (1995), um modo de apresentar o protocolo *zero knowledge proof* é por meio da versão simplificada do protocolo Feige-Fiat-

Shamir. Este protocolo utiliza o conceito de chaves assimétricas, no qual dois números primos estão relacionados matematicamente. Uma terceira entidade, de confiança do usuário e do sistema de autenticação, é necessária no processo:

- Uma entidade de confiança (*T*) seleciona e publica o módulo *n*, no qual $n = p*q$. Os valores *p* e *q* são números primos grandes mantidos em segredo;
- O usuário (*A*) escolhe um segredo *s*, que atende a $1 \leq s \leq n$-1 e que seja um número primo grande; calcula sua chave pública $v=s^2 \bmod n$ e envia para *T*;
- *A* seleciona outro segredo *r*, que atende a $1 \leq r \leq n$-1 e que seja um número primo grande; calcula outra chave pública $x=r^2 \bmod n$ e envia *x* para o sistema de autenticação (*B*);
- *B* seleciona um desafio (um bit) $e = 0$ ou $e = 1$, e envia para *A*;
- *A* envia para *B* a resposta *y*, com base em *e*:
    - Se $e=0$, então $y=r$;
    - Se $e=1$, então $y=r * s \bmod n$;
- *B* obtém a chave pública *v* de *A* em *T*. *B* irá autenticar *A*:
    - Se $e=0$, então $x = y^2 \bmod n$;
    - Se $e=1$, então $x = y^2 * v \bmod n$.

As seções 3.3.5.1 e 3.3.5.2 mostram duas principais implementações do protocolo *zero knowledge password*. O protocolo *zero knowledge password* está em processo de padronização pelo IETF, IEEE e ISO.

3.3.5.1 *Encrypted Key Exchange* (EKE)

Segundo Perlman e Kaufman (1999), o protocolo EKE permite a utilização de senhas para efetuar autenticação mútua (do usuário e do sistema de autenticação), tornando-as um meio para a autenticação forte. Este protocolo utiliza uma versão do protocolo de troca de chaves Diffie-Hellman, em que cada comunicação é cifrada utilizando uma senha, conhecida pelo usuário e pelo sistema de autenticação.

O protocolo foi desenvolvido por Bellovin e Merrit (1992) e seu conceito é apresentado a seguir:

- Uma senha (*S*) é conhecida pelo usuário (*A*) e pelo sistema de autenticação (*B*);
- Dois números primos grandes *g* e *p* são conhecidos por *A* e *B*;
- A função $E_X(valor)$ é utilizada para cifrar *valor* com a chave *X*;
- A função $D_X(valor)$ é utilizada para decifrar *valor* com a chave *X*;

- *A* executa algumas tarefas:
    - Escolhe um número aleatório *a* e calcula (g^a mod *p*);
    - Cifra o resultado utilizando *S*: $E_S(g^a \bmod p)$;
- *A* envia para *B*: $E_S(g^a \bmod p)$;
- *B* executa algumas tarefas:
    - Utiliza a senha *S* para decifrar o que recebeu de A: $D_S(E_S(g^a \bmod p))$;
    - Escolhe um número aleatório *b* e calcula (g^b mod *p*);
    - Cifra o resultado utilizando *S*: $E_S(g^b \bmod p)$;
    - Cria uma chave de autenticação $K=(g^a \bmod p) * g^b$;
    - Escolhe um número aleatório $desafio_B$. Cifra o resultado utilizando *K*: $E_K(desafio_B)$;
- *B* transmite para *A*: $E_S(g^b \bmod p)$ e $E_K(desafio_B)$;
- *A* executa algumas tarefas:
    - Utiliza a senha *S* para decifrar $E_S(g^b \bmod p)$: $D_S(E_S(g^b \bmod p))$;
    - Calcula $K=(g^b \bmod p) * g^a$ e decifra $E_K(desafio_B)$: $D_K(E_K(desafio_B))$;
    - Escolhe número aleatório $desafio_A$;
    - Utiliza *K* para cifrar $desafio_A$ e $desafio_B$: $E_K(desafio_A, desafio_B)$;
- *A* transmite para *B*: $E_K(desafio_A, desafio_B)$;
- *B* executa algumas tarefas:
    - Decifra $E_K(desafio_A, desafio_B)$: $D_K(E_K(desafio_A, desafio_B))$;
    - Se $desafio_B$ recebido é igual ao gerado, *B* envia para *A*: $E_K(desafio_A)$;
- *A* decifra $D_K(E_K(desafio_A))$ e verifica se $desafio_A$ recebido é igual ao gerado.

A e *B* autenticaram-se mutuamente utilizando uma senha *S* e um desafio criado por cada um. Ao final do processo, a chave de autenticação *K* passa a ser utilizada como chave de sessão durante a comunicação.

3.3.5.2 *Simple password exponential key exchange* (SPEKE)

O protocolo SPEKE é similar ao protocolo EKE. Ao invés de utilizar um valor *g* fixo (em g^x mod *p*) e cifrar o resultado com a senha *P*, utiliza-se a própria senha *P* por meio de uma funçao *f*(*P*) para gerar o valor *g* (JABLON, 1996). O protocolo passa a utilizar ($f(P)^x$ mod *p*). Este valor é transmitido sem estar cifrado pela senha *P*. Este modo requer menor processamento que o protocolo EKE.

Originalmente os protocolos EKE e SPEKE foram concebidos com a senha sendo armazenada em claro no servidor de autenticação. Posteriormente, estes protocolos foram modificados e passaram a utilizar uma função *one-way hash* para armazenar a senha. No entanto, existe um problema em ambos os protocolos: a escolha dos números primos. Eles devem ser grandes o suficiente para evitar a quebra da criptografia.

3.4 Conclusão

Neste capítulo foram apresentados os principais protocolos baseados em senha, ou seja, aqueles baseados em algo que o usuário conhece: a senha. Também foram mostradas as formas para avaliar a qualidade das senhas.

Este capítulo também se propôs a esclarecer o conceito de assinatura eletrônica, termo utilizado de forma incorreta pelos *sites* de *Internetbanking* dos bancos brasileiros.

Os sistemas de autenticação baseados em senha são usados nos *sites* de *Internetbanking* dos bancos brasileiros para identificar e autenticar as pessoas. São fáceis de implementar, de baixo custo e de fácil utilização pelo usuário.

4 AUTENTICAÇÃO BASEADA EM "PROVA POR POSSE"

Até recentemente a maioria dos procedimentos de autenticação e controle de acesso eram baseados na relação entre um nome de usuário e uma senha. No entanto, ao invés de memorizar siglas e senhas, os usuários podem proteger sua identidade utilizando um artefato. O artefato pode ser algo lógico como um arquivo ou um dispositivo físico como um *token*[9].

O processo de validação do artefato (e conseqüente identificação do usuário) também proporciona a autenticação de usuário. Os sistemas de autenticação baseados em "prova por posse" também podem ser utilizados no *Internetbanking*.

Neste trabalho são considerados artefatos lógicos os arquivos em computador que armazenam a chave privada, das chaves assimétricas e da certificação digital. Serão vistos, nas próximas seções, conceitos a respeito de chaves assimétricas e certificação digital.

Os artefatos físicos, os *tokens*, possuem vários formatos e tamanhos. Segundo Smith (2002, p. 256), os *tokens* possuem as seguintes propriedades fundamentais:

- O *token* deve ser algo físico e está sob a posse de um usuário;
- O *token* deve ser difícil de duplicar;
- A perda do *token* implica na perda de acesso ao ambiente;
- O roubo do *token* pode ser detectado pelo usuário do *token*.

Os *tokens* podem ter uma camada adicional de segurança, pelo emprego de PINs. Os *tokens* avançados contêm um microprocessador e memória semicondutora. Estes *tokens* aceitam protocolos sofisticados de autenticação, como a utilização de chaves assimétricas, proporcionando um alto nível de segurança. São conhecidos como *smart cards*.

Segundo Smith (2002, p. 256), os *tokens* podem ser divididos em categorias:

- Ativo: gerando diferentes saídas para autenticação, conforme a circunstância;
- Passivo: o *token* é meramente um dispositivo para armazenar o segredo.

Paine e Burnett (2002, p. 231) dividem os *tokens* pela necessidade de contato com um dispositivo de leitura.

A publicação NIST-800-12 (1985, p. 184) divide os *tokens* em duas categorias:

- *Tokens* de memória, que armazenam e não processam dados;
- *Smart tokens*, que incorporam também circuitos integrados.

Este trabalho utilizará esta abordagem, dividindo-os em:

---

[9] *Tokens*, PINs e *smart cards* são descritos neste capítulo.

- *Tokens*: dispositivos utilizados em sistemas OTP e para armazenagem de dados;
- *Smart cards* ICP e *tokens* ICP: contendo circuitos integrados que são utilizados para armazenar a chave privada.

4.1 Chaves assimétricas

As chaves assimétricas são utilizadas nos algoritmos de criptografia assimétrica. Estes algoritmos pressupõem a existência de duas chaves (denominadas chaves assimétricas), uma delas geralmente mantida pública e a outra mantida privada, chamadas respectivamente chave pública e chave privada. Estão ligadas entre si por meio de equações matemáticas complexas. Embora baseadas em conceitos matemáticos altamente sofisticados, as chaves assimétricas podem ser utilizadas facilmente.

A segurança das chaves assimétricas é baseada na dificuldade em resolver problemas matemáticos que demandam muito tempo para efetuar os cálculos. O tamanho da chave também influencia a segurança: quanto maior seu tamanho, maior sua entropia. Deste modo, o número de combinações a serem testadas torna-se muito grande, exigindo muito tempo para descobrir as chaves mediante o uso de força bruta.

O precursor dos algoritmos de criptografia assimétrica foi o protocolo Diffie-Hellman. Este protocolo permite a troca de segredos em um canal de comunicação inseguro. Um exemplo da utilização deste protocolo pode ser visto na seção 3.3.5.

O algoritmo criptográfico assimétrico mais utilizado é o RSA. Este algoritmo apresenta similaridades de funções matemáticas com Diffie-Hellman e pode ser utilizado para cifrar mensagens. Segundo Souza (2004), o RSA tem base na facilidade de computar o produto de dois números primos grandes e na dificuldade de fatorar esse produto. Este produto é conhecido como chave RSA.

Outros algoritmos criptográficos também utilizados são:

- Criptografia Curvas Elípticas (ECC): algoritmo baseado na teoria dos números[10], que proporciona alto nível de segurança mesmo com chaves de tamanho pequeno;
- El Gamal: algoritmo baseado no cálculo de logaritmos discretos.

A criptografia empregando chaves assimétricas pode ser utilizada para implementar os seguintes serviços de segurança:

- Confidencialidade;

[10] A teoria dos números trata de problemas computacionalmente difíceis de resolver (Souza, 2004).

- Autenticação da mensagem;
- Autenticação do usuário;
- Autenticação do parceiro.

Qualquer uma das duas chaves, pública ou privada, pode cifrar um documento ou uma mensagem. A utilização da chave pública do destinatário para cifrar uma mensagem permite a confidencialidade, pois somente o detentor da chave privada correspondente é que irá conseguir decifrar a mensagem. A Figura 6 mostra a utilização das chaves assimétricas.

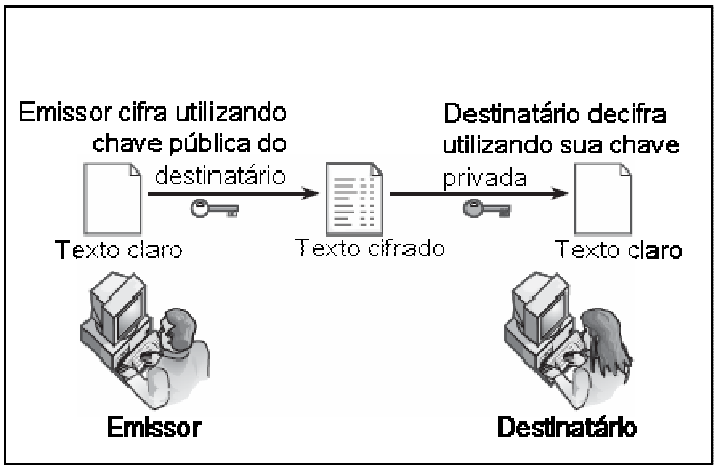


Figura 6: Utilização das chaves assimétricas para confidencialidade

A autenticação da mensagem é feita utilizando a chave privada do emissor. Este processo é conhecido como assinatura digital. Uma mensagem que tenha sido assinada digitalmente com a chave privada poderá ser validada utilizando a chave pública correspondente. Qualquer usuário que tenha a chave pública do emissor poderá validar a mensagem.

A assinatura digital é um tipo de assinatura eletrônica. É o resultado do processo de *hashing*, calculado a partir da mensagem, que produz um valor conhecido como digesto. O digesto é cifrado, utilizando a chave privada do emissor e anexada à mensagem. O recebedor verifica a autenticidade do seguinte modo: calcula o digesto da mensagem original e compara com o digesto recebido, após ter sido decifrado utilizando a chave pública do emissor.

A seqüência a seguir apresenta um dos métodos de autenticação de usuário ou entidade parceira, baseado no desafio:

a) O usuário requisita acesso ao servidor;
b) O servidor gera um número aleatório e transmite para o usuário;
c) O usuário cifra este número utilizando sua chave privada e envia para o servidor;

d) O servidor utiliza a chave pública do usuário para verificar se o valor retornado somente pode ter sido cifrado, utilizando a chave privada dele.

A Figura 7 ilustra esta forma de autenticação.

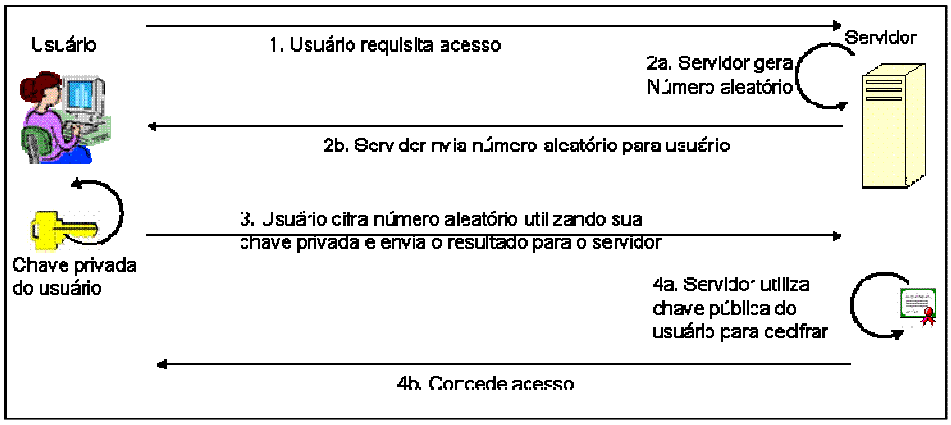


Figura 7: Exemplo de autenticação utilizando certificação digital

Uma das vantagens em utilizar chaves assimétricas é que a chave pública de um usuário poderá estar disponível para qualquer entidade em um repositório público.

4.2 Certificação digital

A autenticação por meio de certificados digitais também é baseada na utilização de chaves assimétricas.

O certificado digital é uma forma segura de disponibilizar a chave pública de uma determinada entidade. O certificado digital permite acreditar na chave pública de uma entidade, pois ele é assinado por uma entidade confiável. Esta entidade, que emite e assina os certificados digitais, é conhecida como Autoridade Certificadora (*AC*).

Além da chave pública, existem outros dados que também constam em um certificado digital. Estes dados podem variar de acordo com o padrão utilizado. O padrão mais utilizado é o X.509, versão 3 do ITU (*International Telecommunications Union*). A Tabela 3 apresenta os principais dados que constam em um certificado digital, segundo o padrão X.509.

O período de validade que consta no certificado digital refere-se à validade do próprio certificado digital. As chaves assimétricas não possuem validade.

O padrão X.509 prevê extensões de acordo com a finalidade do certificado digital. Por exemplo, o padrão SET (*Secure Electronic Transaction*) define um conjunto de extensões direcionado para aplicações que executam transações eletrônicas entre entidades.

Tabela 3: Principais dados em um certificado digital

Campo	Descrição
Versão	Versão do padrão X.509 utilizado
Número serial	Um número inteiro definido pela *AC*. O nome da *AC* e o número serial definem um único certificado
Algoritmo de assinatura do certificado	Identifica o algoritmo utilizado pela *AC* para assinar o certificado emitido (por exemplo: RSA com SHA-1)
Nome do emissor	O nome da entidade que emite e assina o certificado. Este nome é conhecido com DN (*Distinguished Name*)
Período de validade	Datas de início e fim da validade do certificado
Nome da entidade ou pessoa certificada	Identificação da entidade ou pessoa associada à chave pública armazenada neste certificado
Informações da chave pública	Valor da chave pública e indicação do algoritmo no qual ela deve ser usada
Extensões	Outros atributos do certificado digital
Assinatura digital	Assinatura digital do certificado efetuado pela autoridade certificadora

A emissão e a utilização de certificados digitais no Brasil estão regulamentadas pela medida provisória 2.200-2 que instituiu a ICP-Brasil e outras instruções normativas, como a resolução 7 (ICP-Brasil, 2004). Esta resolução trata dos requisitos mínimos para políticas de certificação na ICP-Brasil.

4.2.1 Processo de verificação do certificado digital

O certificado digital é verificado do seguinte modo:

a) Verificação da assinatura da *AC*

O objetivo de verificar a assinatura da *AC* é assegurar que a chave pública que consta no certificado digital não está corrompida e que os outros dados no certificado estão como a *AC* os definiu. A verificação da assinatura digital da *AC* no certificado digital é realizada do seguinte modo:

- Gera-se um digesto, por meio de uma função *hashing*, a partir dos dados do certificado digital;
- O bloco de assinatura digital, contido no certificado digital, é decifrado utilizando a chave pública da *AC* emissora do certificado;
- Os valores são comparados, devendo ser iguais.

O certificado digital que contém a chave pública da *AC* pode ser verificado do mesmo modo, desde que uma *AC* superior a tenha assinado. Estas *ACs* são denominadas *ACs* intermediárias. Este processo repete-se até que todos os certificados das *AC*s intermediárias sejam validados pela última *AC*, denominada *AC* raiz.

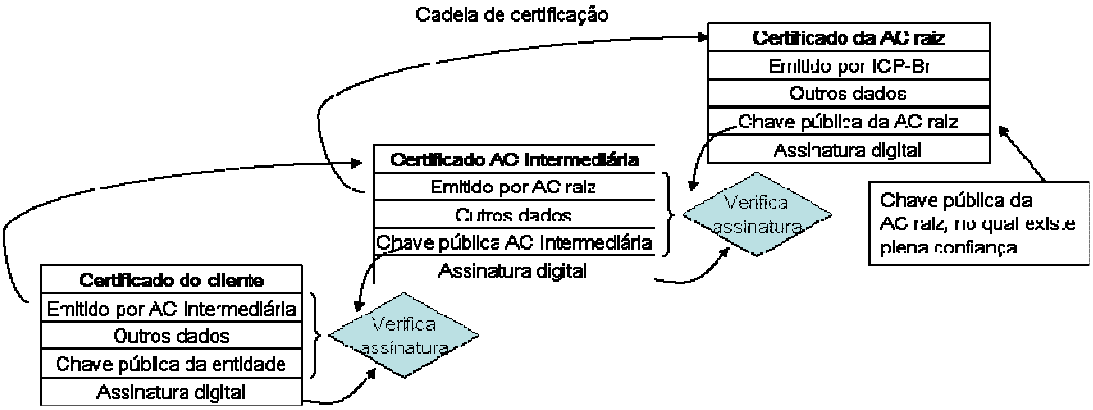


Figura 8: Verificação da assinatura digital na cadeia de certificação

O certificado digital da *AC* raiz é validado de outro modo. Como deve existir plena confiança na *AC* raiz, este certificado digital é auto-assinado. Um certificado digital auto-assinado é aquele em que a chave privada utilizada para assinar digitalmente o certificado digital é a chave privada correspondente à chave pública que consta no próprio certificado digital. A decodificação do bloco de assinatura para comparação dos *hashs* é realizada utilizando a chave pública do próprio certificado digital.

Todo o processo de validação dos certificados digitais é conhecido como validação da cadeia de certificação. A Figura 8 mostra este processo.

b) Verificação das restrições básicas

O padrão X.509 define vários campos opcionais que podem ser incluídos num certificado digital. Um destes campos indica as restrições básicas do certificado digital:

- O comprimento máximo permitido da cadeia de certificação do certificado digital e;
- Se o certificado é de autoridade de certificação ou de entidade final;

c) Período de validade

As chaves assimétricas devem ser utilizadas dentro do período de validade do respectivo certificado digital. Portanto, seu uso deve ser posterior à data de início da validade do certificado digital e anterior às datas de expiração do certificado digital e dos certificados digitais das *AC*s dentro da cadeia de certificação;

d) Lista de certificados revogados

A lista de certificados revogados (LCR) é regularmente publicada e assinada pela *AC*. Contém os números seriais dos certificados digitais emitidos por ela que foram revogados e a data da revogação. Um certificado digital pode ser revogado, por exemplo, porque o usuário requisitou seu cancelamento, seja por perda ou por outro motivo;

e) Verificação *on-line*

A validade do certificado digital pode ser conferida diretamente na *AC*. Neste caso, a verificação é feita por meio do protocolo *Online Certificate Status Protocol* (OCSP). Este protocolo permite receber informações da validade de um ou mais certificados digitais de modo seguro e digitalmente assinado (Myers, 1999). O protocolo HTTP geralmente é utilizado para a comunicação.

f) *Key Usage* e *Extended Key Usage*

O par de chaves assimétricas associadas a um certificado digital pode ter várias finalidades. Para determinar sua utilidade podem-se utilizar os campos *Key Usage* e *Extended Key Usage*. Estes campos restringem as operações que podem ser efetuadas com o certificado digital, como assinatura digital e cifragem dos dados. Estes campos são utilizados, por exemplo, na ICP-Brasil para determinar o tipo de certificado digital: sigilo e assinatura digital;

4.2.2 Armazenamento da chave privada

Segundo Smith (2002), a forma mais comum de armazenamento da chave privada é em arquivos. A chave privada também pode estar armazenada em dispositivos especializados, como *smart cards* e *tokens* ICP, ou em mídias removíveis, na forma de arquivos.

Os padrões mais utilizados quando armazenadas em arquivos são PKCS#8 e PKCS#12, definidos pela empresa RSA. O formato PKCS#8 descreve a sintaxe de armazenamento da chave privada e de seus atributos. Estes dados podem estar protegidos mediante o uso de um algoritmo de criptografia cuja chave é derivada de uma senha (PKCS#5). O formato PKCS#12 define o formato do arquivo utilizado para armazenar as chaves assimétricas, acompanhada da cadeia de certificação, protegido por um segredo (senha ou PIN). Este formato é flexível, contendo várias instâncias de armazenamento. Tal flexibilidade pode causar incompatibilidade entre sistemas baseados em PKCS#12.

O armazenamento da chave privada dentro do *smart card* ou do *token* ICP pode ser feito de vários modos. Segundo Smith (2002), os processos de geração e armazenamento que melhor oferecem segurança são:

a) Importação do par de chaves

Um *software*, que está instalado em um computador, é utilizado para a geração do par de chaves e, em seguida, a chave privada é armazenada no *smart card* ou no *token* ICP;

b) Geração do par de chaves internamente

Um *software* gerador do par de chaves encontra-se dentro do *smart card* ou do *token* ICP. Este processo exige alto poder de processamento e o tempo para a geração do par de chaves é demorado em relação ao primeiro processo. No entanto, tem a vantagem de a chave privada não sair do *smart card* ou do *token* ICP.

4.2.3 ICP-Brasil

A infra-estrutura de chaves públicas ICP-Brasil (2004) é um conjunto de técnicas, práticas e procedimentos, que é implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública.

A medida provisória 2.200-2 dá validade jurídica a documentos gerados em forma eletrônica e assinados utilizando certificados digitais emitidos no âmbito da ICP-Brasil.

A autoridade certificadora raiz, dentro da ICP-Brasil, é mantida pelo ITI (Instituto de Tecnologia da Informação), uma autarquia federal ligada à presidência da república.

Existem 8 tipos de certificados na ICP-Brasil, 4 relacionados com assinatura digital e 4 relacionados com sigilo. Estes certificados definem escalas de requisitos de segurança nos quais os tipos variam entre os requisitos menos rigorosos e os requisitos mais rigorosos. A Tabela 4 relaciona estes certificados e seus requisitos mínimos.

Tabela 4: Comparativo de requisitos mínimos por tipo de certificado

<table>
<tr><th rowspan="2">Tipo de certificado</th><th colspan="3">Chave criptográfica</th><th rowspan="2">Validade máxima do certificado (anos)</th><th rowspan="2">Freqüência de emissão de LCR (horas)</th><th rowspan="2">Tempo limite para revogação (horas)</th></tr>
<tr><th>Tamanho (bits)</th><th>Processo de geração</th><th>Mídia armazenadora</th></tr>
<tr><td>A1 e S1</td><td rowspan="3">1024</td><td>Software</td><td rowspan="2">Smart card ou token, sem capacidade de geração de chave e protegidos por senha</td><td>1</td><td>48</td><td>72</td></tr>
<tr><td>A2 e S2</td><td rowspan="2">Hardware</td><td>2</td><td>36</td><td>54</td></tr>
<tr><td>A3 e S3</td><td rowspan="2">Smart card ou token, ambos com capacidade de geração de chave e protegidos por senha ou por hardware criptográfico</td><td rowspan="2">3</td><td>24</td><td>36</td></tr>
<tr><td>A4 e S4</td><td>2048</td><td>12</td><td>18</td></tr>
</table>

Fonte: ICP-Brasil, 2005

Conforme Resolução 36 de 21/10/2004 (ICP-Brasil, 2004), os sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil passam por um processo de homologação que

é executado pelo LEA (Laboratório de Ensaios e Auditoria). O objetivo da homologação é proporcionar maior segurança à infra-estrutura de chaves públicas brasileira e garantir a interoperabilidade dos sistemas mediante o cumprimento de requisitos técnicos mínimos.

4.3 *Smart card*

O *Smart card*[11] é um cartão plástico, aproximadamente do tamanho de um cartão de crédito. Ele pode ser utilizado de várias maneiras: para identificar e autenticar um usuário; como cartão de crédito ou cartão de débito bancário; em transações *off-line*; para armazenar dados pessoais e também para armazenar a chave privada do usuário.

A utilização do *smart card* exige uma leitora ou um terminal, nos quais os contatos elétricos localizados no *smart card* entram em contato físico com os contatos do dispositivo, para fornecer alimentação elétrica, aterramento e sinal de dados. De acordo com Paine e Burnett (2002), o arranjo físico e a definição funcional desses contatos têm impacto na interoperabilidade do *smart card* e da leitora, pois esses dispositivos não podem se comunicar a menos que os contatos sejam definidos da mesma maneira.

Segundo Paine e Burnett (2002), uma "leitora" é a unidade que tem uma interface com um computador que executa a maior parte do processamento. Um terminal é um dispositivo auto contido de processamento.

As propriedades físicas e as características de comunicação do chip embutido são padronizadas internacionalmente por meio da norma ISO 7816 (1998). Este padrão descreve desde as propriedades elétricas até as dimensões do *smart card* :

- **ISO 7816-1**: define as dimensões físicas dos *smart cards* de contato e o posicionamento de chips, fitas magnéticas e qualquer alto relevo dos cartões. Também descreve a resistência requerida para eletricidade estática;
- **ISO 7816-2**: define a dimensão, a localização, o propósito e as características elétricas dos contatos do *smart card*;
- **ISO 7816-3**: descreve os sinais elétricos e os protocolos de transmissão, definindo os requisitos de voltagem e de corrente para os contatos elétricos definidos na ISO 7816-2;

[11] Este trabalho utilizará o termo " *smart card*" ao invés de "cartão inteligente", visto que este termo é utilizado de forma generalizada em periódicos, pesquisas científicas e em outras publicações.

- **ISO 7816-4**: define um conjunto de comandos para fornecer acesso, segurança e transmissão de dados do cartão, isto é, o cartão lê grava em sua memória;
- **ISO 7816-5**: define os identificadores de aplicativo AIDs (*Application Identifiers*) que são utilizados para identificar um aplicativo específico;
- **ISO 7816-6**: descreve as regras de codificação dos dados necessários para vários aplicativos;
- **ISO 7816**-7: define os comandos da linguagem estruturada SCQL (*Structured Car Query Language*);
- **ISO 7816-8**: estabelece os comandos para operações de segurança;
- **ISO 7816-9**: define os comandos para administração dos cartões;
- **ISO 7816-10**: descreve os sinais eletrônicos e resposta para reinicializar cartões síncronos;
- **ISO 7816-11**: define os procedimentos para verificação pessoal através de biometria;
- **ISO 7816-15**: estabelece a aplicação de informações criptográficas. Foi baseado no padrão PKCS#15, criado pela RSA.

A empresa RSA criou outros padrões que também são aceitos e utilizados internacionalmente (Paine; Burnett, 2002), (ISO, 1998), (Kaliski, 2000):

- **PKCS #11**: define a interface de programação (API) para acesso às funções fornecidas pelo *smart card* às aplicações;
- **PKCS #15**: define padrão que permite utilizar *tokens* criptográficos em aplicações. Cobre dois grupos de equipamentos: *hardware* (*tokens* e *smart cards*) e *soft-tokens* (implementados por *software*).

4.3.1 *Smart card* de memória

O *smart card* de memória não possui poder sofisticado de processamento e não pode gerenciar arquivos dinamicamente. Comunica-se com a leitora utilizando protocolo síncrono. De acordo com Paine e Burnett (2002), existem três tipos principais de *smart cards* de memória:

a) Cartões de memória padrão

Utilizados unicamente para armazenagem de dados e não têm nenhuma capacidade de

processamento. Esses cartões são considerados como disquetes de tamanhos variados sem mecanismo de bloqueio;

b) Cartões de memória protegida/segmentada

Esses cartões têm uma lógica pré-definida para controlar acesso à memória. Esses dispositivos podem ser configurados com proteção contra gravação de parte ou de toda a memória. Alguns desses cartões podem ser configurados para restringir os acessos de leitura e gravação mediante a utilização de senha ou PIN. Ainda podem ter a memória dividida em seções, proporcionando multifuncionalidade;

c) Cartões de memória de valor armazenado

Esses cartões são projetados para armazenar valores, podendo ser descartáveis ou recarregáveis.

4.3.2 *Smart card* ICP

O *smart card* ICP contém um chip de circuito integrado embutido e é utilizado para armazenar certificados digitais. Fornece capacidade computacional embutida no próprio cartão e capacidade de memória. Podem conter várias funções criptográficas por meio do chip de circuito integrado. Alguns cartões podem até mesmo abrigar múltiplos pares de chaves e respectivas cadeias de certificação.

O *smart card* ICP é uma solução de segurança para tarefas como autenticação e assinatura digital. Provê proteção mecânica contra adulteração e fraudes no armazenamento de chaves privadas e outras informações pessoais, além de proporcionar portabilidade e segurança dos dados armazenados entre computadores no trabalho, em casa ou em outro local.

Por possuir capacidade computacional e memória, o *smart card* pode estar programado com todas as funções de acesso e informações necessárias no próprio cartão. Deste modo, não necessita acessar recursos externos potencialmente vulneráveis toda vez que é utilizado para executar uma transação, tornando-o resistente a ataques. Devido a essa característica, o *smart card* ICP é utilizado em aplicativos que necessitam de proteção forte de autenticação e segurança.

Segundo Paine e Burnett (2002), no *smart card* ICP a memória é alocada em seções independentes, atribuídas para funções ou aplicativos específicos. Um microprocessador embutido gerencia essa alocação de memória e o acesso a arquivo. Ele gerencia os dados organizados em estruturas de arquivos via um sistema operacional de cartão (*Card Operating System*). Este *software* controla acesso à memória do cartão. Como resultado, várias funções e

aplicativos podem residir no cartão. Isso significa que transações de negócios podem utilizar esses cartões para distribuir e manter uma variedade de produtos.

4.3.3 *Smart card* EMV

Em 1996, Europay, Mastercard e Visa definiram em conjunto um novo padrão de especificações para assegurar interoperabilidade entre os chips dos *smart cards* e os terminais, independente do fabricante, instituição financeira ou de onde ele possa ser utilizado. Este padrão, identificado como EMV, foi baseado nas especificações da ISO 7816, que tratam de padrões sobre circuitos integrados de cartões com contatos. EMV incorporou novos tipos de dados e regras de codificação especialmente para a indústria financeira(EMV, 2000).

Para estar em conformidade com o padrão EMV, os *smart cards* devem atender a 2 níveis de certificação:

- Nível 1: certifica as características eletromagnéticas, as interfaces lógicas e o protocolo de transmissão;
- Nível 2: certifica a aplicação que estará no *smart card*.

As leitoras de *smart card* devem estar certificadas no nível 1. Dispositivos que efetuem leitura e executem processamento devem estar certificados nos dois níveis.

Estes *smart cards* são utilizados como cartões de créditos.

4.4 PIN

Os termos “senha” e “PIN” (*Personal Identification Number*) geram confusão, dando a impressão que o PIN é utilizado para autenticar usuários (como a senha é utilizada).

O PIN é uma forma de identificação de acesso utilizado em dispositivos para identificar o usuário perante o próprio dispositivo. Segundo Smith (2002, p.278), um dos objetivos do PIN é reduzir o risco de personificação no caso de roubo do dispositivo. O PIN também pode ser utilizado no processo gerador de senha válida para um único acesso.

O PIN pode ser composto por números ou por números e letras, normalmente com tamanho entre 4 e 8 caracteres.

4.5 *Tokens*

Os *tokens* são dispositivos utilizados para identificar e autenticar usuários em sistemas

de autenticação. Os *tokens* podem ser utilizados para fornecer senhas válidas para um único acesso ou como dispositivos para armazenamento de dados, utilizados na autenticação.

Esta seção divide os *tokens* nas seguintes categorias: *tokens* de memória, *tokens* OTP e *tokens* ICP.

4.5.1 *Token* de memória

O *token* de memória somente possui capacidade para armazenar dados. O processamento (leitura e gravação) destes dados é feito por outro dispositivo.

O exemplo mais comum utilizado no ambiente bancário é o cartão magnético, que contém dados em sua fita magnética. Os dados são lidos quando o cartão magnético é passado na unidade de leitura do cartão no caixa automático.

Dispositivos como disquetes, CD-ROM, CD-RW e *Pen Drivers* também são utilizados para este fim.

4.5.2 *Token* OTP

O *token* OTP tem como característica gerar senha dinamicamente, que é utilizada para o usuário se autenticar nos sistemas. A senha é gerada por uma função matemática e é válida para um único acesso ou válida por um determinado período de tempo.

O sistema de autenticação por *token* OTP é composto por dois componentes (servidor e *token*) que funcionam de modo sincronizado (Paine; Burnett, 2002). O servidor de autenticação abriga um registro de semente do usuário. Esta semente é utilizada pelo servidor de autenticação para verificar se a senha informada pelo usuário, gerada pelo *token*, é válida. O *token* também possui a semente e a utiliza para gerar a senha.

Segundo Smith (2002, p. 264), os PINs podem ser utilizados como proteção adicional a estes processos de autenticação. Os PINs podem atuar como:

- Parte da senha, onde o PIN é anexado à senha gerada;
- Senha para desbloquear o processo de geração da senha OTP ou;
- Parte da semente que é utilizado para a geração da senha.

Os *tokens* OTP podem ser divididos em três categorias:

a) Seqüência de código válido por um período (temporal)

Os *tokens* baseados em tempo utilizam o relógio interno juntamente com a semente para

produzir uma senha. Esta senha é válida por um período de tempo determinado (entre 40 e 180 segundos). Existe uma "janela de tempo" utilizada pelo servidor em que a senha é válida mesmo se o tempo tenha acabado, porque a geração do tempo (*clock*) pode variar entre equipamentos, mesmo que seja do mesmo fabricante. A sincronização é feita pelo servidor, comparando a senha atual com uma nova senha requisitada. A Figura 9 ilustra a geração de senhas OTP temporal;

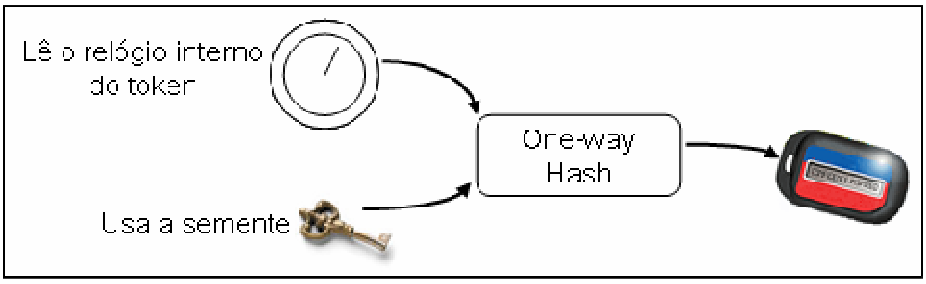


Figura 9: Gerando senha OTP temporal
Fonte: Smith, 2002, p. 269

b) Seqüência de código por contador

Os *tokens* baseados em contador incorporam um contador interno e o utilizam para gerar uma nova senha, sempre que necessário. Normalmente o usuário deve pressionar um botão no *token* que inicia o processo incrementando o contador. A princípio pode haver perda de sincronismo com o servidor. No entanto, isto é contornado pelo servidor, que requisita ao usuário que o mesmo se autentique novamente. Deste modo, o servidor compara a semente e o contador da senha anterior com o da nova senha informada, verificando se as senhas informadas foram geradas pelo mesmo *token*. A Figura 10 ilustra o processo de geração de senhas OTP por contador.

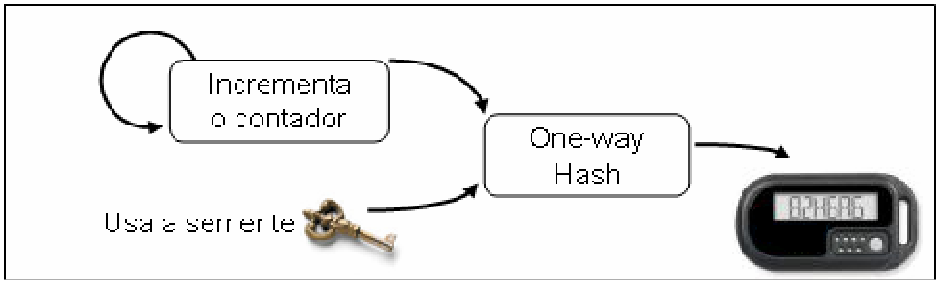


Figura 10: Gerando senha OTP por contador
Fonte: Smith, 2002, p. 267

Existem fabricantes de *tokens* que utilizam ambos os tipos de *tokens*, os baseados em tempo e os baseados em contador, para gerar a senha. Também existem *softwares* geradores de senhas que substituem os *tokens*. São conhecidos como *soft tokens*. Podem ser utilizados em computadores, Palms, PDAs e aparelhos celulares;

c) Calculadora desafio-resposta

Funciona com uma premissa semelhante à dos geradores de senha de uma única vez (OTP), mas com intervenção do usuário. Uma semente é sincronizada, tanto no servidor de autenticação, quanto no equipamento (computador, Palm, PDA ou aparelho celular).

À medida que o usuário se conecta, o servidor de autenticação envia um desafio, gerado aleatoriamente. O usuário deve inserir este desafio recebido na calculadora, que por sua vez realiza uma operação matemática baseado neste desafio, exibindo a resposta. A Figura 11 ilustra o processo de geração de senhas por desafio-resposta.

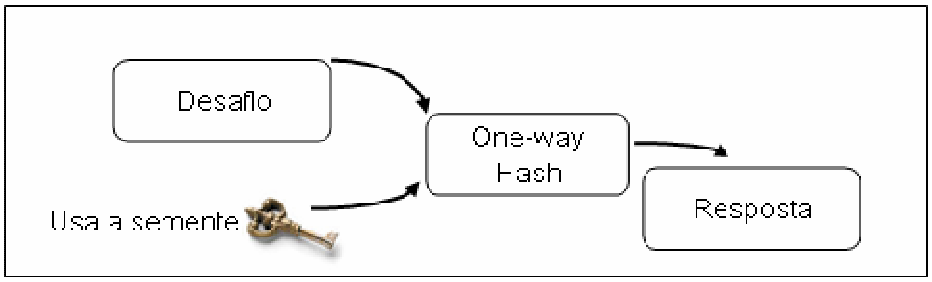


Figura 11: Calculadora desafio-resposta
Fonte: Smith, 2002, p. 288

4.5.3 *Token* ICP

Os *tokens* ICP possuem as mesmas funções e características dos *smart cards* ICP, apesar de possuírem o formato diferente do padrão ISO 7816 e se comunicarem através de portas USB, dispensando as leitoras. Utiliza-se um programa instalado no computador para a comunicação.

4.6 Aparelho Celular com chip

O desenvolvimento da tecnologia dos aparelhos celulares agregou capacidade de armazenamento e processamento de dados. Isto permitiu utilizar o aparelho celular como um dispositivo para autenticação.

Com o advento da tecnologia GSM (*Global System for Mobile Communications*), que usa *smart cards*, a certificação digital pode ser utilizada no aparelho celular como forma de autenticação. O GSM foi desenvolvido pela indústria de telecomunicações européia, baseado na especificação ISO 7816. O aparelho celular utiliza um chip conhecido como SIM (*Subscriber Identify Module*). O chip SIM é um tipo de *smart card* e pode armazenar chaves privadas.

A comunicação segura entre o aparelho celular e o sistema *Internetbanking* pode ser feita utilizando o protocolo WTLS (*Wireless Transport Layer Security*), que atua de maneira similar ao protocolo SSL. O protocolo WTLS é um componente adicional do protocolo WAP (*Wireless Application Protocol*).

Por exemplo, suponha que um sistema *Internetbanking* disponibilize um serviço que, para determinadas transações, envia uma mensagem para o aparelho celular do usuário. A autorização da transação pode ser feita com o envio de uma resposta, assinada digitalmente, com sua chave privada que está armazenada no chip.

O aparelho celular também pode ser utilizado como um cartão *token*, do mesmo modo que os cartões geradores de senha de uma única vez. O programa gerador de senha deve estar instalado no aparelho celular.

4.7 Conclusão

Neste capítulo foram apresentados mecanismos de autenticação baseados “no que se possui”, que são pouco utilizados ou podem ser utilizados no *Internetbanking* para autenticar o usuário. Foram apresentados os termos “artefato lógico”, que é algo que o usuário possui armazenado em arquivo e “artefato físico”, que é algo físico que o usuário possui.

Este capítulo também se tratou dos conceitos de chaves assimétricas, certificação digital, PIN, *smart cards* e *tokens*. Também introduziu a utilização de certificação digital em aparelhos celulares com tecnologia GSM e chip SIM.

5 ANÁLISE DAS VULNERABILIDADES E CONTROLES

Este capítulo descreve as vulnerabilidades dos sistemas de autenticação e os controles empregados para minimizar o problema.

Como mencionado na seção 1.2, considera-se "sistema de autenticação" os programas, infra-estruturas de rede, equipamentos e processos necessários para que a autenticação do usuário ocorra.

5.1 Vulnerabilidades

As vulnerabilidades são fragilidades ou erros que podem causar danos e prejuízos para a atividade ao serem exploradas intencionalmente ou acidentalmente. Nas seções a seguir estão descritas as principais vulnerabilidades relacionadas aos sistemas de autenticação analisados.

5.1.1 *Man-in-the-middle* na comunicação

O acesso pela Internet ao *Internetbanking* é feito pelo navegador utilizando o protocolo HTTPS. O protocolo HTTPS é a utilização do protocolo HTTP sobre o protocolo SSL.

O protocolo SSL foi originalmente desenvolvido pela Netscape e serviu de inspiração para o IETF criar o protocolo TLS (*Transport Layer Security*) (Chapman, Zwicky; 1995). Segundo Garfinkel e Spafford (1997), o protocolo situa-se entre a camada de aplicação e a pilha de protocolos TCP/IP, situada na camada de transporte. Provê serviços de segurança para os protocolos da camada de aplicação como:

a) Privacidade, utilizando cifragem dos dados;
b) Autenticação dos parceiros de comunicação, por meio da certificação digital;
c) Integridade da mensagem, utilizando *Message Authentication Code*.

A Figura 12 localiza o protocolo SSL na pilha TCP/IP.

HTTP
SSL
TCP
IP

Figura 12: SSL na pilha TCP/IP

O protocolo SSL é ativado após a conexão TCP estar estabelecida. O cliente envia uma mensagem de boas vindas (*client hello message*) para o servidor que responde com outra

mensagem de boas vindas (*server hello message*). Esta troca de mensagens serve para estabelecer os atributos da conexão que incluem a versão do protocolo, a identificação da sessão, o método criptográfico utilizado, o protocolo de compressão de dados e a criação de uma chave de sessão.

Em seguida, o servidor envia seu certificado junto com a cadeia de certificação. O navegador do usuário verifica se o certificado combina com o nome do *host* qualificado (FQDN). A validade do certificado e a cadeia de certificação também são verificadas. Opcionalmente, o servidor pode requerer o certificado do cliente para concluir a conexão.

O navegador do usuário e o servidor negociam uma chave de sessão, que será utilizada no restante da comunicação. A partir deste ponto, os dados irão trafegar em um canal seguro. A Figura 13 ilustra o processo de geração da chave de sessão, no protocolo SSL/TLS.

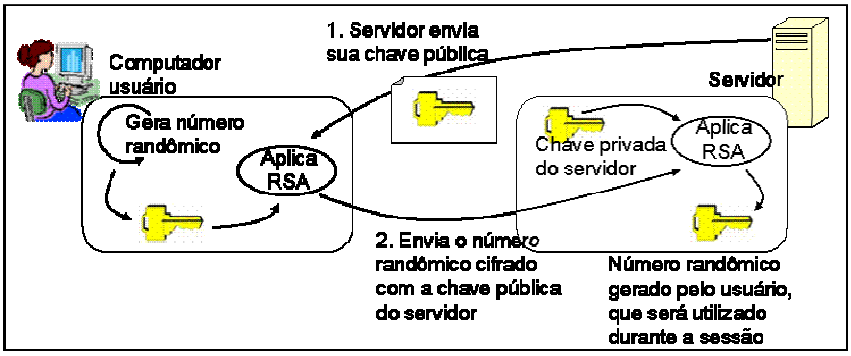


Figura 13: Geração da chave de sessão no protocolo SSL/TLS
Fonte: Smith, 2002, p. 267

O acesso ao *Internetbanking* pela Internet pode ser alvo de ataque conhecido como *man-in-the-middle*. Este ataque é sofisticado e pode ser executado utilizando um *site* impostor que se situa entre o usuário e o servidor, atuando como *proxy*, com certificado digital contendo dados idênticos e assinado por uma autoridade certificadora não confiável, por exemplo. A Figura 14 ilustra este tipo de ataque. Suponha que exista um *site* parecido com o verdadeiro. O usuário é induzido ou direcionado a utilizar este *site* por meio de:

- Engenharia social;
- Vulnerabilidades no servidor DNS, resultando no envenenamento da tabela de resolução de nomes;
- Comprometimento da tabela de roteamento TCP/IP;
- Modificação da tabela HOSTS do computador do usuário;
- Outras situações.

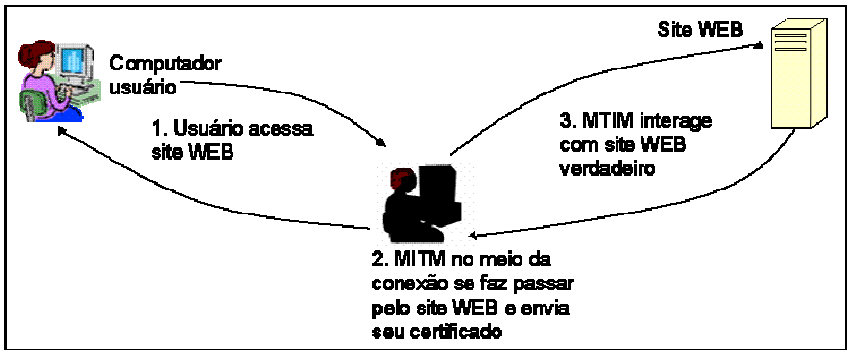


Figura 14: Ataque *man-in-the-middle*
Fonte: Smith, 2002, p. 402

Existem duas técnicas principais de ataques *man-in-the-middle*. Em ambas as situações, o usuário não percebe o servidor impostor e todos os dados transmitidos entre o cliente e o servidor, como senhas, dados da conta corrente, etc., são passíveis de observação:

a) Servidor impostor com certificado SSL não confiável

O navegador verificará que o certificado digital não é confiável e emitirá uma mensagem de alerta. O usuário geralmente não entende o alerta ou simplesmente o descarta, continuando o processo, ou seja, fechando a conexão com o servidor impostor;

b) Servidor impostor sem certificado SSL

Nesta situação, o servidor impostor não possui certificado digital. A identificação de que a conexão HTTP está em SSL é muito sutil, sendo sinalizada por meio de um símbolo no formato de cadeado, no canto inferior do navegador.

O usuário poderá não perceber ou desconhecer a identificação e continuar conectado ao servidor impostor.

5.1.2 Fornecimento de dados sensíveis para um servidor impostor

Outra vulnerabilidade, ligada à autenticação do usuário, é induzi-lo a fornecer os dados de autenticação para um servidor impostor utilizando técnicas como as descritas na seção 5.1.1, fazendo-o acreditar que está no servidor verdadeiro. A diferença em relação à situação anterior é que o servidor impostor serve como repositório dos dados, não atuando como *proxy*.

O usuário é induzido a informar os dados bancários e os dados de autenticação como:

- A senha, em sistemas de autenticação que utilizam senha. Os dados obtidos podem ser utilizados posteriormente;

- A senha OTP, em sistemas de autenticação que utilizam *tokens* OTP. Os dados obtidos devem ser utilizados imediatamente, em vista da curta validade da senha OTP;
- Uma ou mais respostas, em sistemas que utilizam desafio-resposta. Os dados obtidos podem ser utilizados posteriormente.

5.1.3 Vulnerabilidades na infra-estrutura de acesso

Infra-estrutura de acesso é o conjunto de serviços como DNS, roteadores, canal de comunicação, provedor de acesso, que o usuário utiliza para acessar o sistema *Internetbanking*.

Esta infra-estrutura pode apresentar vulnerabilidades, transparente para quem as utiliza, mas de grande impacto, podendo ser utilizadas como forma para a obtenção da senha. Por exemplo, o provedor de acesso pode estar com problemas na configuração do servidor DNS, resolvendo o nome para um local falso. Os pacotes TCP/IP podem ser observados ou sofrerem modificações durante o trajeto.

As vulnerabilidades por falhas não intencionais na administração da infra-estrutura devem ser consideradas. A configuração inadequada de um equipamento ou serviço de rede pode possibilitar a alteração de rotas, por exemplo.

5.1.4 Armazenamento das senhas no servidor de autenticação

Dependendo do modo como as senhas estão armazenadas no servidor de autenticação, elas podem estar vulneráveis à captura. Por exemplo, as senhas podem estar armazenadas em uma tabela dentro de um banco de dados. Pode-se efetuar uma cópia não autorizada desta tabela. A seguir, caso as senhas estejam armazenadas de modo cifrado, elas podem ser descobertas utilizando ataques por força bruta e por dicionário de dados.

5.1.5 Observação de dados sensíveis quando digitados

Para provar a identidade, que normalmente é o número da conta corrente, o usuário utiliza sua senha. Existe a necessidade de digitar a senha no computador antes de enviar para o sistema de autenticação validá-la. Neste momento ela pode ser observada através de programas maliciosos introduzidos no computador do usuário.

Os *mouse-loggers*, por exemplo, capturam a área da tela ao redor do clique do mouse, apanhando o que é digitado em teclados virtuais.

A senha também pode ser capturada através da simples observação de sua digitação. Esta técnica também é conhecida como *shoulder surfing*.

5.1.6 Escrita de senhas

Sendo a senha algo que precisa ser memorizado, ela é passível de esquecimento. Se a senha for muito complexa e difícil de memorizar, o usuário pode acabar anotando-a em papel. Deste modo, a senha também pode ser capturada através das informações deixadas pelo usuário no papel sobre a mesa ou no lixo.

5.1.7 Observação das senhas na memória do navegador

Os navegadores e seus componentes podem apresentar vulnerabilidades que possibilitam a obtenção de dados confidenciais, como a senha. Por exemplo, uma vulnerabilidade no JavaScript utilizado pelos navegadores Firefox permite a captura de blocos da memória alocada para o navegador, mostrando-os no próprio navegador. Um código malicioso pode capturar e armazenar estes dados. Os dados digitados para acessar o sistema *Internetbanking* podem estar dentro do bloco de memória capturado (Mozilla, 2005).

5.1.8 Escolha de senha trivial pelo usuário

O processo de autenticação utilizando senha ainda é o processo mais utilizado no sistema *Internetbanking*. Os bancos brasileiros possibilitam ao usuário escolher sua própria senha. Normalmente esta senha tem tamanho entre 4 e 6 caracteres e deve ser numérica.

O usuário tenderá a escolher uma senha que seja fácil de lembrar. Com 4 dígitos, podem-se escolher datas no formato “ddmm”. Deste modo, o primeiro dígito fica limitado a 0, 1, 2 e 3. O segundo e o quarto dígitos, de 0 a 9. O terceiro somente pode ser 0 ou 1. Logo, tem-se em torno de 366 possíveis combinações e a entropia ficaria em torno de 9 *bits* ($\log_2$ 366*).* Isto é 27 vezes menor do que se utilizassem todas as combinações possíveis: a entropia ficaria em torno de 14 *bits* ($\log_2 10000$).

A senha é válida por tempo indeterminado, sem que o sistema de autenticação requisite ao usuário sua alteração periodicamente.

5.1.9 Tentativa de descoberta da senha por ataques por força bruta ou por dicionário de dados

Existe a possibilidade de utilizar força bruta para tentar o acesso à conta corrente. A utilização de mecanismos para bloquear o acesso do usuário após um determinado número de tentativas é uma prática que pode ser contornada utilizando-se uma variação da tentativa de acesso por força bruta. Pode-se tentar quebrar a senha de um usuário até seu direito de acesso ser bloqueado. Parte-se, então, para outro usuário, seguindo o mesmo processo até descobrir um usuário e senhas válidas, obtendo o acesso.

O mesmo princípio pode ser utilizado para ataques por dicionário de dados.

5.1.10 Inexistência da irretratabilidade da ação de autenticação

Irretratabilidade é uma propriedade que exige evidências para que as partes envolvidas não possam afirmar que não participaram da transação. Estas evidências devem ser dadas pelos sistemas de autenticação.

Os processos de autenticação baseados em senhas e em *tokens* OTP não oferecem garantias contra repúdio. Estes processos de autenticação não provêem mecanismos para assegurar que somente o usuário poderia ter se autenticado, pois existe a necessidade de compartilhar o segredo com o sistema de autenticação, possibilitando a observação ou alteração por outrem.

5.1.11 Cópia não autorizada da matriz impressa ou da lista de senhas

Os materiais nos quais são impressas a lista de senhas e a matriz impressa podem não ser resistentes a cópias por processos xerográficos, possibilitando a cópia dos dados. A cópia também pode ocorrer durante o processo de fabricação da matriz impressa e da lista de senhas.

5.1.12 Roubo da sessão de usuário autenticado

Em aplicações WEB, a camada de aplicação é a responsável pelo controle da sessão (Meier; *et al*, 2003). Este controle é necessário porque o protocolo HTTP é *stateless*, ou seja, não são mantidos estados no lado cliente nem no lado servidor. Toda vez que uma mensagem HTTP é enviada não é possível relacioná-la à mensagem anterior. Para implementar controle

da sessão de uso sobre o protocolo HTTP, é necessário utilizar artifícios adicionais, como os descritos a seguir:

a) Utilização de *cookies*

Segundo Garfinkel e Spafford (1997), um *cookie* é um bloco de dados que o servidor WEB pode encaminhar para o navegador. O *cookie* é mantido na memória do navegador e também pode ser armazenado em disco se o tipo for persistente. O tipo persistente permite guardar dados para posterior reuso por um *site* WEB. Uma vez recebido, o *cookie* é enviado ao servidor WEB para cada nova requisição HTTP. O *cookie* permite à aplicação identificar que o usuário já está autenticado.

A aplicação WEB pode apresentar falha no controle da sessão do usuário, possibilitando o roubo da sessão de usuário autenticado. O roubo da sessão ocorre quando o *cookie* é capturado e utilizado em um acesso não autorizado, contornando o sistema de autenticação. Outra falha pode permitir que o usuário esteja em mais de uma conexão ao mesmo tempo.

b) Utilização de URL para armazenar o controle da sessão

O protocolo HTTP permite a passagem de parâmetros pela URL. Deste modo, pode-se utilizar um parâmetro para identificar a sessão do usuário. Por exemplo, suponha a seguinte URL:

https://www.banco.com/P?CONT=.nH8k8iYoWXRmvULRB4N6FoVyUUnCkQeDoQAApkh14pouvndh%2fX%3d1142820519%2fE

Neste exemplo, a variável CONT armazena o valor do controle da sessão e o envio dos dados é feito pela URL (comando “GET” do protocolo HTTP).

A passagem de parâmetros por este modo é insegura, visto que os navegadores tem como padrão armazenar o histórico das URLs acessadas em arquivo.

Da mesma forma que no controle da sessão por meio de *cookie*, a aplicação WEB pode apresentar falha no controle da sessão do usuário, possibilitando o contorno do sistema de autenticação, utilizando a URL capturada.

c) Utilização de variável no código HTTP para armazenar o controle da sessão

O protocolo HTTP permite criar variáveis para armazenarem dados dentro de uma página HTTP.

Uma variável pode ser utilizada para armazenar um valor que identifique a sessão do usuário. Este valor é gerado pelo servidor de autenticação e encaminhado ao navegador dentro de uma página HTTP. O envio dos dados seria executado pelo comando “POST”.

Entretanto, ainda é possível capturar a variável por meio de programas maliciosos instalados no computador do usuário e contornar o sistema de autenticação, caso a aplicação WEB apresente falhas.

5.1.13 Insegurança no armazenamento da chave privada

Atualmente é comum o emprego de autenticação mediante o uso de certificados digitais no *Internetbanking*, apesar de esta tecnologia existir há pelo menos 20 anos. Alguns bancos utilizam tecnologia proprietária, enquanto outros utilizam certificados digitais no âmbito da ICP-Brasil.

Algumas formas de armazenamento da chave privada são inseguras, tornando-as vulneráveis a ataques. A princípio não existem restrições quanto ao local onde a chave privada do usuário deve ser armazenada. Ela pode estar armazenada dentro do navegador, em arquivo dentro do computador ou em mídia removível. Estas formas de armazenamento da chave privada propiciam a cópia durante sua utilização. A Tabela 5 exibe as características de segurança dos principais dispositivos de armazenamento.

Tabela 5: Armazenamento das chaves assimétricas

Mídia	Característica
Armazenamento de dados (HDs, disquetes, CDs e memória externas)	Flexível
	Pouca segurança
	Custo baixo
*Smart card*s	Maior segurança
	Outras utilidades

As chaves privadas armazenadas em *tokens* USB e cartões de memória podem ser copiadas. Este processo também pode ser executado em outras mídias nas quais as chaves privadas podem ficar armazenadas, como discos rígidos, disquetes e CDs.

5.1.14 Personificação dos servidores utilizando certificado digital indevido

Outra vulnerabilidade é a geração de certificados digitais em nome de outra entidade ou utilizar um certificado digital que tenha o *key usage* incorreto para gerar um terceiro certificado digital. Deste modo, pode-se passar a utilizar este certificado como se fosse a entidade verdadeira. Esta vulnerabilidade depende do ritual utilizado pela Autoridade Certificadora “de confiança do usuário” para emitir o certificado e das provas de autenticidade

da requisição, como a comprovação de documentos. Desta forma, um certificado válido pode ser utilizado para implementar uma conexão SSL em um falso *site*. Também é possível criar um certificado digital utilizando uma Autoridade Certificadora falsa e induzir o usuário a aceitá-lo.

5.1.15 Atualização e manipulação da lista de certificados revogados

Conforme descrito na seção 4.2.1, a lista de certificados revogados (LCR) é um arquivo contendo os números seriais dos certificados digitais emitidos pela autoridade certificadora (*AC*) que não podem ser mais utilizados. Também consta na LCR, seu *timeframe*[12], sendo atualizada periodicamente.

Um certificado digital que foi revogado, mas não consta na LCR utilizada pelo sistema de autenticação, poderá ser considerado como válido no processo de verificação do certificado digital.

5.1.16 Escolha de segredo trivial para proteger a chave privada

A chave privada é protegida por um segredo (senha ou PIN) quando está armazenada em arquivo (geralmente no formato PKCS#12), em *smart card* ICP ou *token* ICP. Logo, a escolha do segredo influencia a segurança do armazenamento da chave privada. Este segredo tem as mesmas propriedades e vulnerabilidades que uma senha comum, como a escolha de uma senha trivial.

Um segredo escolhido trivialmente pode ser alvo de ataques de dicionário de dados.

5.1.17 Ataque de força bruta ao segredo utilizado para proteger a chave privada

Ao obter o arquivo que contém a chave privada pode-se executar ataque de força bruta até descobrir o segredo pois o arquivo não possui mecanismos que limitem esta tentativa.

5.1.18 Vulnerabilidade dos *tokens*

Algumas das vulnerabilidades dos *tokens* são causadas pelo usuário, como a perda do

---

[12] *Timeframe* significa, em uma tradução livre, “janela de tempo”.

token ou a criação de *tokens* extras como cópia de segurança.

Segundo Smith (2002), existem vulnerabilidades cujos processos de exploração são bastante sofisticados e que afetam os *tokens* OTP:

- Durante o processo de autenticação a senha OTP pode ser capturada e utilizada ao mesmo tempo em que a conexão legítima é bloqueada;
- Em *tokens* OTP que utilizam PIN:
    - O *software* utilizado para gerar a senha OTP pode ser capturado e analisado para descobrir o PIN, utilizando ataque por força bruta. No entanto, depende do roubo do *token*;
    - Observação de uma seqüência de senhas OTP de uma vítima. De posse do *software* gerador da senha, descobre-se o PIN mediante a verificação do resultado com as senhas capturadas.

5.1.19 Vulnerabilidade dos *smart cards* ICP

De acordo com Paine e Burnett (2002), existem muitas evidências na indústria da computação de que os *smart cards* melhoram significativamente a segurança de qualquer transação: fornecem um armazenamento à prova de adulteração para a identidade e conta do usuário e protegem contra várias ameaças de segurança, como um armazenamento negligente da chave privada. Entretanto, os *smart cards*, como outros sistemas de autenticação, apresentam vulnerabilidades.

Os *smart cards* estão sujeitos à corrupção dos dados ou a recepção de dados incorretos, pela adulteração da leitora ou do terminal. Abbot (2002) lista outras vulnerabilidades potenciais:

a) Análise diferencial da energia

Utiliza análise estatística da energia utilizada pelo *smart card* durante a função de criptografia para determinar a chave privada armazenada;

b) Ataque de sincronismo

Descobre o tempo das operações com as chaves privadas pelo *smart card* e analisa este dado para determinar a informação criptográfica;

c) Engenharia reversa dos chips

Descobre como o chip do *smart card* funciona, examinando e desmontando-o. É um processo destrutivo e freqüentemente é necessário executar o mesmo procedimento em mais de um chip;

d) Falhas de projeto ou implementação

É a vulnerabilidade mais séria nos *smart cards*. Este tipo de vulnerabilidade tende a ser mais fácil de explorar e replicar;

e) Aplicações com várias funções

Um *smart card* pode conter múltiplas aplicações. Como é a interação das organizações que contém aplicações no cartão? Quem seria o emissor do cartão? O que aconteceria se a aplicação do emissor fosse cancelada ou não mais necessária? Todos os dados no cartão poderiam ser compartilhados legalmente ou ilegalmente pelas aplicações? O que aconteceria se acabasse a parceria das empresas na utilização dos cartões? Uma aplicação poderia atacar a outra? E a negação de serviço?

Outra vulnerabilidade que pode ser explorada, apesar de não estar relacionada com a autenticação, é a indução do usuário a assinar um documento cujo conteúdo ele não tenha conhecimento.

5.2 Controles

Os controles são mecanismos, elementos ou processos que visam reduzir, eliminar ou transferir o risco das ameaças causadas pelas vulnerabilidades, mantendo-as em conformidade com os padrões estabelecidos. Alguns destes controles estão relacionados nas seções abaixo.

5.2.1 Sigilo, integridade da comunicação e autenticação de parceiro

Um dos métodos mais utilizados para prover sigilo da comunicação e autenticação do parceiro é o protocolo SSL/TLS.

O protocolo SSL/TLS provê o serviço de segurança confidencialidade mediante a cifragem dos dados e autenticação do parceiro (servidor), quando o cliente acessa o sistema *Internetbanking*.

O protocolo SSL/TLS também pode ser utilizado para prover outros serviços de segurança como integridade e autenticação de usuário. A utilização de certificados digitais pelo usuário permite sua autenticação por meio do protocolo SSL/TLS.

5.2.2 Cadastramento do computador do usuário

Uma forma de restringir a personificação seria cadastrar o computador de onde se inicia

o processo de autenticação e utilização do serviço *Internetbanking*.

A verificação do computador é feita mediante a assinatura gerada por um software a partir dos dados do computador, como número serial do disco rígido, do sistema operacional, endereço MAC da placa de rede, entre outros.

No entanto, o acesso ficaria limitado aos computadores cadastrados e, em caso de mudança do computador ou de um de seus componentes, uma nova assinatura deve ser gerada e cadastrada.

5.2.3 Armazenamento seguro das senhas no servidor de autenticação

As senhas somente devem ser conhecidas pelo usuário. Logo, deve-se armazenar o *hash* da senha utilizando-se algum processo *one-way hash*.

5.2.4 Utilização de HSM para armazenar dados sensíveis

O HSM (*Hardware Module Security*) é um equipamento desenvolvido para armazenar e proteger dados sensíveis, como senhas e chaves privadas. Todo o processamento que envolva a utilização dos dados sensíveis, é executado dentro do HSM. Ele é menos suscetível a falhas e vulnerabilidades de sistema e resistente à adulteração.

O HSM também pode ser utilizado para gerar o par de chaves pública e privada. Esta geração é feita dentro do HSM, evitando a manipulação externa da chave privada.

A obtenção de acesso não autorizado ao servidor de autenticação não implica na obtenção das senhas ou chaves privadas.

O HSM pode ser conectado diretamente ao servidor de autenticação por meio de porta RS-232 ou placa PCI, por exemplo. Também pode estar conectado à rede local. Neste modo, deve existir uma criptografia na comunicação entre o servidor de autenticação e o HSM.

5.2.5 Utilização de teclados virtuais para digitação das senhas

Os teclados virtuais foram criados para evitar a captura das senhas quando são digitadas no teclado convencional. A Figura 15 mostra um exemplo de teclado virtual.

Para evitar a captura da senha, alguns teclados virtuais modificam as posições das teclas a cada acesso. A própria localização do teclado virtual pode ser alterada a cada digitação. Em outros teclados virtuais, o caractere é modificado ou encoberto quando o mouse está sobre ele.

Existem teclados virtuais que piscam quando o botão do mouse é pressionado e outros que atuam como se fossem imãs, quando o mouse fica sobre uma tecla virtual.

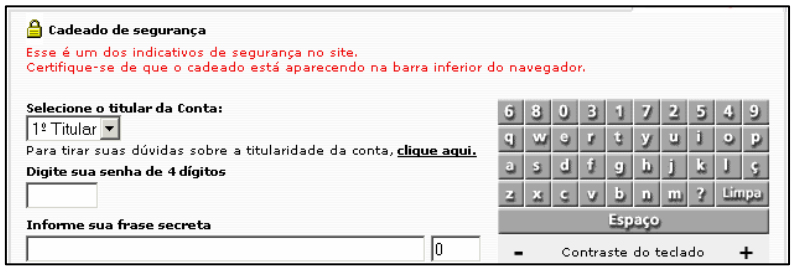


Figura 15: Exemplo de teclado virtual

5.2.6 Utilização de teclados dinâmicos para digitação das senhas

O teclado dinâmico é uma variação do teclado virtual cujo principal objetivo é diminuir a probabilidade de acerto. Sua principal característica é a representação de dois ou mais caracteres em um único símbolo. Por exemplo, suponha que a senha seja ABC e o teclado dinâmico como representado pela Figura 16:

1			2			3		
X	K	C	R	T	A	B	E	G

Figura 16: Exemplo de teclado dinâmico

O resultado será 231. O valor observado não possibilita a conversão direta para a senha correta. Neste exemplo, a chance de acerto é de 1/27 (existem 27 combinações possíveis).

5.2.7 *Plugins* de segurança

O *plugin* de segurança é um programa, instalado no computador do usuário, que é ativado quando se acessa o s*ite* de *Internetbanking*.

A função do *plugin* de segurança é evitar que um programa malicioso consiga capturar as informações de autenticação. Isto é feito monitorando e bloqueando requisições arbitrárias entre o navegador e o sistema operacional.

5.2.8 Autenticação positiva

A autenticação positiva é o nome dado para uma segunda autenticação na qual a senha é a resposta a uma pergunta pessoal, como a data de nascimento, por exemplo. Esta autenticação ocorre após a autenticação inicial do usuário.

5.2.9 Validação das senhas e tentativas de acesso

As senhas que se referenciam a datas de aniversário do titular da conta corrente não devem ser aceitas no processo de cadastramento, assim como senhas com os mesmos dígitos ou seqüências, como 123456.

O número de tentativas de acesso dentro de um espaço de tempo deve ser limitado, devendo bloquear o direito de acesso.

5.2.10 Cifragem da senha antes da transmissão

Apesar de os sistemas de autenticação baseados em WEB normalmente utilizarem-se do protocolo SSL para prover sigilo da comunicação, a cifragem da senha antes de ser transmitida para o sistema de autenticação fornece uma garantia adicional contra sua observação no canal de comunicação.

5.3 Conclusão

Este capítulo apresentou as principais vulnerabilidades dos sistemas de autenticação, decorrentes de falhas de projeto, implementação, humanas, obsolescência tecnológica, dentre outros.

Também foram apresentados controles que são utilizados para minimizar eventuais riscos decorrentes da utilização de sistemas de autenticação que apresentam vulnerabilidades.

6 ANÁLISE COMPARATIVA

Cada sistema de autenticação possui vantagens e desvantagens. Por exemplo, senhas podem ser observadas, adivinhadas, entregues ou esquecidas. *Tokens* podem ser perdidos ou roubados.

Um bom sistema de autenticação é aquele em que o custo do ataque[13] é maior que o ganho em potencial resultante de um ataque bem sucedido. O aumento do custo do ataque pode ser obtido em decorrência da utilização de tecnologias que dificultem a obtenção não autorizada das credenciais de acesso ao sistema *Internetbanking*.

Para analisar os sistemas de autenticação de usuário, foram feitos levantamentos dos serviços de segurança que podem estar presentes no processo de autenticação de usuário; do mecanismo baseado em senha e dos outros mecanismos de autenticação que podem ser utilizados. Em seguida, foram apresentadas as principais vulnerabilidades e controles de segurança existentes nos sistemas de autenticação.

Após o levantamento dos sistemas de autenticação, análise das vulnerabilidades e descrição dos possíveis controles pôde-se selecionar alguns parâmetros representativos para possibilitar uma análise comparativa, levando em consideração características de segurança, conveniência e economia (menor custo), que serão apresentados neste capítulo. Ao final do capítulo, será apresentada uma tabela resumo com todos os sistemas de autenticação e suas avaliações, com a intenção de facilitar a visualização da comparação.

6.1 Parâmetros de comparação

Os parâmetros de comparação escolhidos pretendem propiciar a identificação de vantagens e desvantagens dos sistemas de autenticação analisados, de forma que seja possível compará-los utilizando o mesmo parâmetro de comparação.

Os parâmetros de comparação podem utilizar métricas quantitativas e qualitativas. A métrica quantitativa analisa valores mensuráveis. A métrica qualitativa analisa fatores que satisfazem a determinados requisitos dependentes da percepção humana, que não podem ser ou não são comumente mensurados. Embora diferentes, as métricas quantitativas e qualitativas podem ser combinadas a fim de se obterem avaliações consistentes sobre o objeto

[13] Inclui tempo e dinheiro gastos para identificar vulnerabilidades, bem como a possibilidade descoberta e prisão.

da análise. Para se obter um padrão de análise e facilitar a visualização, os parâmetros quantitativos serão convertidos para qualitativos.

Neste trabalho serão utilizados os seguintes valores qualitativos: muito baixo, baixo, médio, alto e muito alto.

6.1.1 Definições

Neste capítulo, o termo "objeto de autenticação" expressa os dados de autenticação como senhas, PINs, *tokens* OTP e artefatos como lista de senhas, matriz impressa, arquivo contendo a chave privada, todos utilizados pelo usuário para se autenticar.

O termo "DCS" (dados críticos de segurança) representa as informações sensíveis, como os objetos de autenticação, cuja divulgação ou modificação podem comprometer a segurança. Por exemplo: as senhas dos usuários; o *login*; o número da conta-corrente; as sementes dos sistemas OTP.

O termo "objeto de autenticação derivado" significa o objeto de autenticação utilizado no processo de autenticação do usuário, criado a partir do objeto de autenticação original. A Tabela 6 correlaciona o objeto de autenticação e o objeto de autenticação derivado em relação ao sistema de autenticação.

Tabela 6: Correlação entre objeto de autenticação, objeto de autenticação derivado e o sistema de autenticação

Sistema de autenticação baseado em	**Objeto de autenticação**	**Objeto de autenticação derivado**
Senha	Senha	Senha
Senha + ZKP[i]	Senha	Chave de autenticação
Desafio-resposta	Matriz impressa	Resposta ao desafio
Lista de senhas	Cartela contendo a lista de senhas	Senha
Chaves assimétricas	Chave privada	Desafio[ii] / chave simétrica de sessão[iii]
Tokens OTP	Semente + algoritmo	Senha OTP

[i] *Zero knowledge protocol*
[ii] No caso de autenticação por desafio
[iii] No caso de canais tipo SSL/TLS

A Figura 17 situa a localização do DCS, do objeto de autenticação e do objeto de autenticação derivado.

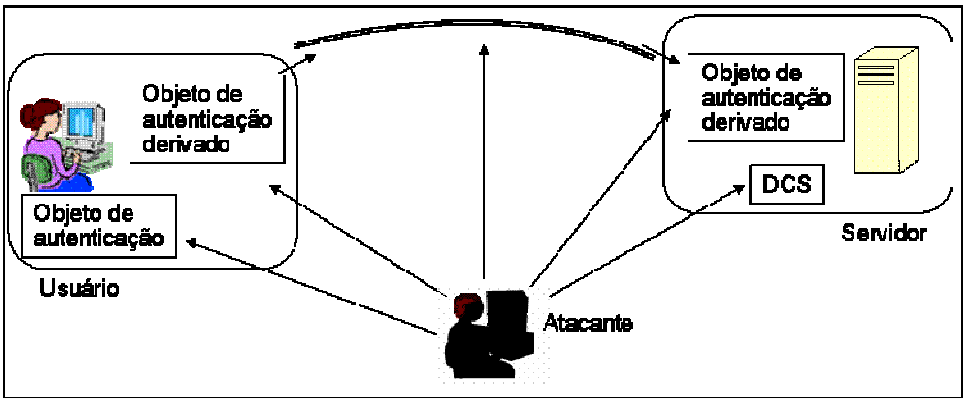


Figura 17: Localização de alguns dos objetos relacionados à segurança

Existem parâmetros, chamados parâmetros derivados, que são resultados da combinação de outros parâmetros, denominados primitivos. Nestes casos, os valores assumidos pelos parâmetros derivados são determinados conforme a Tabela 7. Um parâmetro avaliado negativamente tende a qualificar o resultado de forma desfavorável.

Tabela 7: Valores de parâmetros combinados derivados de dois parâmetros primitivos

	Muito alto	**Alto**	**Médio**	**Baixo**	**Muito baixo**
Muito alto	Muito alto	Alto	Alto	Médio	Muito baixo
Alto	Alto	Alto	Médio	Baixo	Muito baixo
Médio	Alto	Médio	Médio	Baixo	Muito baixo
Baixo	Médio	Baixo	Baixo	Muito baixo	Muito baixo
Muito baixo	Muito baixo	Muito baixo	Muito baixo	Muito baixo	Muito baixo

6.1.2 Classes de parâmetros

A análise dos sistemas de autenticação deve ser estudada sob a ótica da segurança, conveniência e economia. Assim, os parâmetros selecionados foram agrupados nas seguintes classes:

- Parâmetros relacionados à segurança;
- Parâmetros relacionados à conveniência;
- Parâmetro relacionado à economia.

A seguir, será detalhada cada uma destas classes.

6.1.3 Classe de parâmetros relacionados à segurança

Sob o ponto de vista de segurança existem diversos parâmetros que podem ser utilizados para realizar uma análise comparativa dos sistemas de autenticação. Neste trabalho foram selecionados os seguintes parâmetros:

- Espaço médio de ataque;
- Nível de segurança da proteção utilizada para armazenar DCS no servidor de autenticação;
- Dificuldade do roubo, cópia ou observação do objeto de autenticação;
- Freqüência da troca do objeto de autenticação;
- Dificuldade da personificação quando do roubo do objeto de autenticação;
- Dificuldade da observação do objeto de autenticação derivado em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor;
- Freqüência ou possibilidade de alteração do objeto de autenticação derivado;
- Dificuldade da personificação quando do roubo do objeto de autenticação derivado;
- Irretratabilidade da autenticação;
- Suporte à autenticação do cliente em sessão SSL/TLS.

Estes parâmetros são detalhados nas seções a seguir.

6.1.3.1 Espaço médio de ataque

O "espaço médio de ataque" é um parâmetro quantitativo, apresentado na seção 3.2.1. Possibilita avaliar diferentes sistemas de autenticação, pela estimativa de sua resistência contra as tentativas de ataque por força bruta ou por dicionário de dados.

Existem outros parâmetros relacionados a este como *keyspace* e entropia. A utilização do parâmetro *keyspace* para avaliar os sistemas de autenticação apresentados neste trabalho poderia causar confusão, dando a impressão de que a segurança de alguns sistemas de autenticação seria equivalente. A entropia é utilizada na composição do parâmetro espaço médio de ataque.

Por exemplo, uma senha numérica com tamanho de 6 dígitos, teoricamente teria o mesmo *keyspace* de um *token* OTP com 6 dígitos. No entanto, a senha pode ser afetada pela tendência do usuário em escolher senhas triviais, o que não ocorre com *tokens* OTP. A influência do usuário é captada pelo parâmetro espaço médio de ataque.

O espaço médio de ataque proporciona uma comparação mais eficiente, visto que padroniza valores que possuem diferentes pesos para cada sistema de autenticação. Para possibilitar um melhor entendimento, este parâmetro será apresentado como parâmetro qualitativo, utilizando a regra de conversão descrita na Tabela 8.

Este parâmetro está relacionado com as seguintes vulnerabilidades:

- "Escolha de senha trivial pelo usuário", descrita na seção 5.1.8;

- "Tentativa de descoberta da senha por ataques por força bruta ou por dicionário de dados", descrita na seção 5.1.9;
- "Escolha de segredo trivial para proteger a chave privada", descrita na seção 5.1.16.

Tabela 8: Regra de conversão do espaço médio de ataque

Valor	**Significado**
Muito alto	Espaço médio de ataque acima de 2^{100}
Alto	Espaço médio de ataque entre 2^{80} e 2^{99}
Médio	Espaço médio de ataque entre 2^{64} e 2^{79}
Baixo	Espaço médio de ataque entre 2^{56} e 2^{63}
Muito baixo	Espaço médio de ataque abaixo de 2^{50}

6.1.3.2 Nível de segurança da proteção utilizada para armazenar DCS no servidor de autenticação

Este parâmetro indica a qualidade da proteção do DCS, quando da necessidade de armazenamento no servidor de autenticação. Está relacionado com as vulnerabilidades:

- "Armazenamento das senhas no servidor de autenticação", descrita na seção 5.1.4;
- "Atualização e manipulação da lista de certificados revogados", descrita na seção 5.1.15.

É mais seguro que o processo de autenticação não exija a necessidade de armazenar DCS no servidor de autenticação. A Tabela 9 descreve o significado dos valores que este parâmetro pode assumir. Considera-se que o nível mínimo aceitável seja "Médio".

Tabela 9: Significado dos valores para análise do nível de proteção do DCS

Valor	**Significado**
Muito alto	Não é necessário armazenar DCS
Alto	DCS armazenado e manipulado em equipamento específico conectado ao servidor de autenticação
Médio	DCS armazenado com cifragem irreversível
Baixo	DCS armazenado com cifragem reversível
Muito baixo	DCS exposto podendo ser observado facilmente

6.1.3.3 Dificuldade do roubo, cópia ou observação do objeto de autenticação

Este parâmetro indica se o objeto da autenticação pode ser obtido, por meios não autorizados, no computador utilizado pelo cliente. Está relacionado com as vulnerabilidades:

- "Observação de dados sensíveis quando digitados", descrita na seção 5.1.5;
- "Escrita de senhas", descrita na seção 5.1.6;
- "Observação das senhas na memória do navegador", descrita na seção 5.1.7;

- "Cópia não autorizada da matriz impressa ou da lista de senhas", descrita na seção 5.1.11;
- "Insegurança no armazenamento da chave privada", descrita na seção 5.1.13.

A Tabela 10 descreve o significado dos valores que este parâmetro pode assumir.

Tabela 10: Significado dos valores para análise da dificuldade do roubo, cópia ou observação do objeto de autenticação

Valor	**Significado**
Muito alto	Objeto físico que não permite cópia e exige PIN
Alto	Objeto físico que não permite cópia
Médio	Objeto físico passível de cópia
Baixo	Objeto lógico passível de cópia e exige PIN
Muito baixo	Objeto lógico passível de cópia

6.1.3.4 Freqüência da troca do objeto de autenticação

Este parâmetro indica a validade do objeto de autenticação para o sistema de autenticação. Quanto menor a validade, menor o risco de sucesso de personificação do usuário utilizando o objeto de autenticação roubado. A Tabela 11 descreve o significado dos valores que este parâmetro pode assumir.

Tabela 11: Significado dos valores para análise da validade do objeto de autenticação

Valor	**Significado**
Muito alto	Realiza troca em intervalos de 1 dia
Alto	Realiza troca em intervalos inferiores a 1 ano
Médio	Realiza troca em intervalos superiores a 1 ano inclusive
Baixo	Momento de troca a critério do usuário
Muito baixo	A troca nunca é realizada

6.1.3.5 Dificuldade da personificação quando do roubo do objeto de autenticação

Este parâmetro é derivado dos parâmetros descritos nas seções 6.1.3.3 e 6.1.3.4. Indica se o roubo do objeto de autenticação permite a personificação do usuário perante o sistema de autenticação. Seu valor é determinado pela Tabela 7, descrita na seção 6.1.1.

6.1.3.6 Dificuldade da observação do objeto de autenticação derivado em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor

Este parâmetro indica se o objeto de autenticação derivado, descrito na seção 6.1.1, pode ser observado na comunicação, por meio de ataque *man-in-the-middle* em conexões

SSL/TLS, ou da sua observação, em caso de divulgação em site impostor. Este parâmetro está relacionado com as vulnerabilidades:

- "*Man-in-the-middle* na comunicação", descrita na seção 5.1.1.
- "Fornecimento de dados sensíveis para um servidor impostor", descrita na seção 5.1.2;
- "Personificação dos servidores utilizando certificado digital indevido", descrita na seção 5.1.14.

A Tabela 12 descreve o significado dos valores que este parâmetro pode assumir.

Tabela 12: Significado dos valores para análise da dificuldade de observação do objeto de autenticação derivado

Valor	**Significado**
Muito alto	Dados não são suficientes para personificação do usuário
Alto	Dados são suficientes para personificação do usuário desde que utilizados imediatamente
Médio	Dados são suficientes para personificação do usuário na e-nésima tentativa
Baixo	Dados são suficientes para personificação do usuário na próxima tentativa de autenticação
Muito baixo	Dados são suficientes para personificação do usuário em qualquer tentativa de autenticação

6.1.3.7 Freqüência ou possibilidade de alteração do objeto de autenticação derivado

Este parâmetro indica a validade e a previsibilidade do objeto de autenticação derivado gerado a partir do objeto de autenticação. O objeto de autenticação derivado é previsível quando se conhece o próximo valor a ser utilizado. Por exemplo, as respostas da tabela desafio-resposta; as senhas da lista de senhas. Desta forma, ao ser observado e utilizado imediatamente, possa-se personificar o usuário. O objeto de autenticação derivado não é previsível quando é gerado de modo aleatório pelo objeto de autenticação. Por exemplo, a uma senha gerada por um *token* OTP.

A Tabela 13 descreve o significado dos valores que este parâmetro pode assumir. Uma avaliação razoável seria "Baixo".

Tabela 13: Significado dos valores para análise da freqüência de alteração do objeto de autenticação derivado

Valor	**Significado**
Muito alto	Alterado a cada autenticação e não previsível
Alto	Alterado periodicamente - período na ordem de minutos
Médio	Alterado a cada autenticação e previsível
Baixo	Alterado periodicamente – período superior a minutos
Muito baixo	Alterado quando o objeto de autenticação é alterado

6.1.3.8 Dificuldade da personificação quando do roubo do objeto de autenticação derivado

Este parâmetro é derivado dos parâmetros descritos anteriormente nas seções 6.1.3.6 e 6.1.3.7. Indica se a posse do objeto de autenticação derivado permite a personificação do usuário perante o sistema de autenticação. Seu valor é determinado pela Tabela 7, descrita na seção 6.1.1.

6.1.3.9 Irretratabilidade da autenticação

Este parâmetro indica se o sistema de autenticação provê irretratabilidade. A Tabela 14 descreve o significado dos valores que este parâmetro pode assumir.

Tabela 14: Significado dos valores para análise da irretratabilidade da autenticação

Valor	Significado
Alto	Suporta irretratabilidade
Baixo	Não suporta irretratabilidade

6.1.3.10 Suporte a autenticação do cliente em sessão SSL/TLS

Este parâmetro indica se o sistema de autenticação permite a autenticação do lado cliente de uma sessão de comunicação SSL/TLS, com o uso de autenticação por certificados digitais. A Tabela 15 descreve o significado dos valores que este parâmetro pode assumir.

Tabela 15: Significado dos valores para análise do suporte à autenticação SSL/TLS

Valor	Significado
Alto	Suporta autenticação de cliente SSL/TLS
Baixo	Não suporta autenticação de cliente SSL/TLS

6.1.4 Classe de parâmetros relacionados à conveniência

Os parâmetros relacionados à conveniência estão associados ao conforto e comodidade do usuário. As seções a seguir relacionam os parâmetros selecionados para avaliar os sistemas de autenticação.

6.1.4.1 Facilidade de uso

Este parâmetro indica o grau de facilidade para o usuário em utilizar o sistema de autenticação. A

Tabela 16 descreve o significado dos valores que o parâmetro pode assumir.

Tabela 16: Significado dos valores para análise da facilidade de uso

Valor	**Significado**
Muito alto	Utilização extremamente simples
Alto	Fácil utilização
Médio	Requer atenção para utilizar
Baixo	Necessita atenção e conhecimento para utilizar
Muito baixo	Muita atenção e muito conhecimento para utilizar

6.1.4.2 Mobilidade

Este parâmetro indica a possibilidade de utilizar o sistema de autenticação a partir de diferentes equipamentos. A Tabela 17 descreve o significado dos valores que este parâmetro pode assumir.

Tabela 17: Significado dos valores para análise da mobilidade

Valor	**Significado**
Muito alta	O usuário não precisa transportar objeto de autenticação
Alta	O usuário necessita transportar objeto de autenticação
Média	O usuário necessita transportar objeto de autenticação e conectá-lo ao computador
Baixa	O usuário necessita transportar objeto de autenticação, conectá-lo a dispositivo específico e instalar módulos de *software* do dispositivo
Muito baixa	Acesso do usuário a partir de um só local e objeto de autenticação pode precisa estar conectado ao dispositivo

6.1.4.3 Independência da arquitetura

O parâmetro "independência da arquitetura" indica quanto o sistema de autenticação é independente do tipo de hardware, componentes de hardware (como interface USB, leitora de *smart card*), sistema operacional e navegador que o usuário esteja utilizando.

Tabela 18: Significado dos valores para análise da independência da arquitetura

Valor	**Significado**
Muito alto	Independente de sistema operacional e *hardware*
Alto	Dependente de sistema operacional ou *hardware*, ambos muito utilizados
Médio	Dependente de sistema operacional e *hardware*, ambos muito utilizados
Baixo	Dependente de sistema operacional ou *hardware*, ambos pouco utilizados
Muito baixo	Dependente de sistema operacional e *hardware*, ambos pouco utilizados

A avaliação dos sistemas de autenticação por este parâmetro de comparação somente é possível após a identificação da tecnologia utilizada para desenvolver o portal WEB. Segue, a título de ilustração, a Tabela 18 que descreve o significado dos valores que este parâmetro pode assumir, esclarecendo sua dependência com a tecnologia utilizada.

6.1.4.4 Aproveitamento para outras finalidades

Este parâmetro indica se o objeto de autenticação pode ser usado para outras utilidades. Por exemplo: assinatura digital; armazenamento de informações pessoais. A Tabela 19 descreve o significado dos valores que este parâmetro pode assumir.

Tabela 19: Significado dos valores para análise do aproveitamento para outras finalidades

Valor	**Significado**
Alto	Pode ser utilizado para outras finalidades
Baixo	Não pode ser aproveitado

6.1.5 Classe de parâmetros relacionados à economia

A economia está relacionada diretamente com os gastos, porém em ordem inversa, sendo uma métrica quantitativa. Quanto maior o gasto, menor a economia. Inclui as despesas utilizadas para manter o sistema de autenticação, servidores, aquisição de dispositivos, suporte ao usuário, distribuição e logística. Este grupo de despesas será denominado de "gastos com infra-estrutura".

As despesas para o usuário utilizar o sistema de autenticação, quando existirem, serão denominadas de "gastos para o usuário". Nestas despesas incluem-se, por exemplo, o custo de aquisição de dispositivos de leitura; de aquisição de certificados digitais ICP-Brasil; de manutenção dos certificados digitais; de reposição de *tokens* OTP e tarifas bancárias, cobradas dos usuários.

As despesas relacionadas com necessidades emergenciais de alteração do sistema de autenticação para se adaptar, por exemplo, à mudança das normas legais ou para contornar problemas de segurança causado pela descoberta de novas vulnerabilidades ou obsolescência da tecnologia utilizada serão denominadas "gastos emergenciais de manutenção". Pode ocorrer que estes gastos sejam superiores à migração para um sistema de autenticação que apresente melhores características de segurança.

Em vista da dificuldade em mensurar estes valores, o parâmetro custo será avaliado pela métrica qualitativa.

6.1.5.1 Economia nos gastos

Para seguir o padrão de avaliação dos outros parâmetros, nos quais quanto mais alto o valor, melhor é o sistema de autenticação, este parâmetro avaliará a "economia nos gastos". A Tabela 20 descreve o significado dos valores associados a este parâmetro. Esta tabela pressupõe que o sistema de autenticação é utilizado por muitos usuários.

Tabela 20: Significado dos valores para análise da economia nos gastos

Valor	**Significado**
Muito alta	Nenhum gasto para o usuário e baixo com infra-estrutura
Alta	Gastos baixo para o usuário e baixo com infra-estrutura
Média	Gastos alto para o usuário e baixo com infra-estrutura
Baixa	Gastos baixo para o usuário e alto com infra-estrutura
Muito baixa	Gastos alto para o usuário e alto com infra-estrutura

6.2 Avaliação dos sistemas de autenticação

Os sistemas de autenticação avaliados pelos parâmetros de comparação descritos na seção 6.1, são:

- Sistemas de autenticação baseados em senhas utilizando requisição-resposta;
- Sistemas de autenticação baseados em senhas utilizando desafio-resposta;
- Sistemas de autenticação baseados em senhas utilizando lista de senhas;
- Sistemas de autenticação baseados em senhas utilizando o protocolo *zero knowledge password*;
- Sistemas de autenticação baseados em senhas utilizando S/Key;
- Sistemas de autenticação baseados em chaves assimétricas;
- Sistemas de autenticação baseados em chaves assimétricas com certificados digitais;
- Sistemas de autenticação baseados em *tokens* OTP.

6.2.1 Sistemas de autenticação baseados em senhas utilizando requisição-resposta

Os sistemas de autenticação baseados em senhas foram abordadas na seção 3.2. A utilização de senhas para autenticar o usuário proporciona algumas vantagens:

a) O processo de verificação e validação das senhas não requer sistemas complexos, tampouco alta capacidade de processamento e equipamentos robustos ou sofisticados;
b) As senhas são fáceis de armazenar e manipular.

No entanto, as senhas possuem várias vulnerabilidades: elas podem ser capturadas ou descobertas, apresentadas nas seções 5.1.1 a 5.1.10; seu armazenamento no servidor de autenticação apresenta vulnerabilidade descrita na seção 5.1.4 – "Armazenamento das senhas no servidor de autenticação". Este trabalho pressupõe que a senha está armazenada no servidor de autenticação por meio de algoritmo que produza cifragem irreversível (*one way hash*). Entretanto, para ressaltar os problemas de armazenamento das senhas, a Tabela 21 mostra o nível de proteção da senha armazenada em claro e com cifragem reversível. Uma solução para armazenar senhas é a utilização de HSM, conforme descrito na seção 5.2.4 – "Utilização de HSM para armazenar dados sensíveis".

Tabela 21: Avaliação dos sistemas de autenticação baseados em senha utilizando requisição-resposta

Segurança			
	Espaço médio de ataque		Muito baixo
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação		
		Senha em claro	Muito baixo
		Senha com cifragem reversível	Baixo
		Senha com cifragem irreversível	Médio
		Senha armazenada no HSM	Muito Alto
	Dificuldade da personificação quando do roubo do objeto de autenticação		Muito baixo
		Dificuldade do roubo, cópia ou observação	Muito baixo
		Freqüência da troca	Baixo
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado		Muito baixo
		Dificuldade de observação em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor	Muito baixo
		Freqüência de alteração	Baixo
	Irretratabilidade da autenticação		Baixo
	Suporte à autenticação do cliente em conexões SSL/TLS		Baixo
Conveniência			
	Facilidade de uso		Muito alto
	Mobilidade		Muito alta
	Independência da arquitetura		---
	Aproveitamento para outras funcionalidades		Baixo
Economia			
Economia nos gastos			Muito alta

A tendência dos usuários em escolher senhas fáceis, destacada na seção 5.1.8 – "Escolha de senha trivial pelo usuário", influencia o espaço médio de ataque. Uma senha com tamanho de 6 dígitos, criada de forma aleatória, tem espaço médio de ataque em torno de 2^{18}

(500.000 tentativas). Segundo Smith (2002), este valor significa um tempo aproximado de 524 segundos para descobrir a senha, em um ataque direto. Já uma senha com tamanho menor ou escolhida com base em datas, o espaço médio de ataque e o tempo para descobri-la é menor ainda.

Procuram-se reduzir as vulnerabilidades das senhas por meio de controles como os relacionados nas seções 5.2.1 a 5.2.10. As senhas não apresentam características de irretratabilidade e não possuem recursos para dificultar a personificação. Um controle que pode ser utilizado para reduzir a possibilidade de personificação é o cadastramento de computador (descrito na seção 5.2.2).

A Tabela 21 apresenta a avaliação dos sistemas de autenticação baseados em senhas, utilizando os parâmetros de comparação selecionados.

6.2.2 Sistemas de autenticação baseados em senhas utilizando desafio-resposta

Na autenticação em sistemas baseados em desafio-resposta, apresentado na seção 3.3.1, o usuário precisa responder corretamente ao desafio para se autenticar.

Tabela 22: Avaliação dos sistemas de autenticação baseados em senha utilizando desafio-resposta

Segurança			
	Espaço médio de ataque		Muito baixo
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação		
		Senha em claro	Muito baixo
		Senha com cifragem reversível	Baixo
		Senha com cifragem irreversível	Médio
		Senha armazenada no HSM	Muito Alto
	Dificuldade da personificação quando do roubo do objeto de autenticação		Baixo
		Dificuldade do roubo, cópia ou observação	Médio
		Freqüência da troca	Baixo
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado		Médio
		Dificuldade de observação em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor	Médio
		Freqüência de alteração	Médio
	Irretratabilidade da autenticação		Baixo
	Suporte à autenticação do cliente em conexões SSL/TLS		Baixo
Conveniência			
	Facilidade de uso		Médio
	Mobilidade		Alta
	Independência da arquitetura		---
	Aproveitamento para outras funcionalidades		Baixo
Economia			
Economia nos gastos			Alta

Este protocolo apresenta desvantagens como:

a) A tabela de respostas necessita estar armazenada no servidor de autenticação, que está sujeito às vulnerabilidades descritas nas seções 5.1.4 e 5.1.9;
b) Usuário necessita carregar a matriz impressa contendo as respostas;
c) Necessidade de renovar a tabela de desafio e respostas.

A Tabela 22 exibe a avaliação deste sistema de autenticação, utilizando os parâmetros de comparação selecionados.

No caso de roubo de uma das respostas (o objeto de autenticação derivado) para tentar executar a personificação, existe a possibilidade de a resposta do próximo desafio ser a resposta roubada. A autenticação por meio de desafio-resposta também não apresenta características de irretratabilidade. O cadastramento de computador, descrito na seção 5.2.2, pode ser utilizado para minimizar estes riscos.

Em uma matriz impressa não consta todas as combinações possíveis. Por exemplo, supondo que o protocolo desafio-resposta utiliza senhas formadas por números com tamanho de 4 dígitos, têm-se um total de 10.000 combinações. Mas, a tabela de respostas em poder do usuário apresenta apenas 0,7% das combinações possíveis (70 respostas). No entanto, o espaço médio não sofreria a influência de qual grupo de respostas foi selecionado. Em um eventual ataque, todas as combinações são válidas. Neste exemplo, o espaço médio de ataque estaria em torno de 2^{12}.

6.2.3 Sistemas de autenticação baseados em senhas utilizando lista de senhas

Os sistemas de autenticação que utilizam lista de senhas, abordada na seção 3.3.3, possuem a vantagem que para cada acesso é necessário utilizar uma nova senha da relação. Caso esta senha seja observada, poderá não ter nenhuma utilidade naquele momento. A lista de senhas apresenta as seguintes desvantagens:

a) A lista de senhas necessita estar armazenada no servidor de autenticação, que está sujeito às vulnerabilidades descritas nas seções 5.1.4 e 5.1.9;
b) Usuário necessita carregar um “cartão de papel” contendo a lista de senhas;
c) Deve existir um controle e sincronismo das senhas já utilizadas pelo usuário e pelo sistema de autenticação;
d) Necessidade de renovar a lista de senhas.

O espaço médio de ataque pode variar, por exemplo, em função do tamanho da senha e dos caracteres utilizados para gerar as senhas. Suponha que um algoritmo gera senhas com tamanho de 8 caracteres e utiliza números e letras do alfabeto diferenciando maiúsculas de minúsculas: o espaço médio de ataque estaria em torno de 2^{46}.

No caso da divulgação dos DCS e da última senha utilizada da lista de senhas (o objeto de autenticação derivado) em *site* impostor, é possível personificar o usuário na próxima tentativa de autenticação. Esta senha capturada é a que o sistema de autenticação está aguardando para a próxima autenticação. Se considerarmos que sempre é utilizada a mesma lista de senhas, a senha capturada também será válida para uma autenticação futura.

A autenticação por meio de lista de senhas não apresenta irretratabilidade, visto que as senhas também necessitam estar armazenadas no servidor de autenticação.

Um controle que pode ser utilizado para minimizar os problemas descritos acima é o cadastramento de computador (descrito na seção 5.2.2).

A Tabela 23 exibe a avaliação deste sistema de autenticação utilizando os parâmetros de comparação selecionados.

Tabela 23: Avaliação dos sistemas de autenticação baseados em lista de senhas

Segurança			
	Espaço médio de ataque		Muito baixo
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação		
		Senha em claro	Muito baixo
		Senha com cifragem reversível	Baixo
		Senha com cifragem irreversível	Médio
		Senha armazenada no HSM	Muito Alto
	Dificuldade da personificação quando do roubo do objeto de autenticação		Baixo
		Dificuldade do roubo, cópia ou observação	Médio
		Freqüência da troca	Baixo
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado		Baixo
		Dificuldade de observação em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor	Baixo
		Freqüência de alteração	Médio
	Irretratabilidade da autenticação		Baixo
	Suporte à autenticação do cliente em conexões SSL/TLS		Baixo
Conveniência			
	Facilidade de uso		Médio
	Mobilidade		Alta
	Independência da arquitetura		---
	Aproveitamento para outras funcionalidades		Baixo
Economia			
Economia nos gastos			Alta

6.2.4 Sistemas de autenticação baseados em senhas utilizando *zero knowledge password*

A descrição do protocolo *zero knowledge password* e suas características foram abordadas na seção 3.3.5. A utilização deste protocolo agrega níveis adicionais de segurança a autenticação por meio de senhas:

a) Não é possível observar a senha do usuário no canal de comunicação. Somente a chave de autenticação (objeto de autenticação derivado) pode ser observada;
b) Utilização de uma chave de autenticação, que é usada como chave de sessão, válida para um único acesso.

Entretanto, apesar da eficácia do protocolo em proteger a senha na comunicação (que não é transmitida), ela ainda pode ser observada no ambiente do usuário. Também não apresenta características de irretratabilidade e recursos para dificultar a personificação. Um controle utilizado para reduzir a personificação é o cadastramento de computador (descrito na seção 5.2.2). Aplica-se ao espaço médio de ataque, a mesma avaliação das senhas discutida na seção anterior. A Tabela 24 exibe a avaliação deste sistema de autenticação, utilizando os parâmetros de comparação selecionados.

Tabela 24: Avaliação dos sistemas de autenticação baseados em senhas utilizando *zero knowledge password*

Segurança			
	Espaço médio de ataque		Muito baixo
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação		
		Senha em claro	Muito baixo
		Senha com cifragem reversível	Baixo
		Senha com cifragem irreversível	Médio
		Senha armazenada no HSM	Muito Alto
	Dificuldade da personificação quando do roubo do objeto de autenticação		Muito baixo
		Dificuldade do roubo, cópia ou observação	Muito baixo
		Freqüência da troca	Baixo
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado		Alto
		Dificuldade de observação em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor	Alto
		Freqüência de alteração	Muito alto
	Irretratabilidade da autenticação		Baixo
	Suporte à autenticação do cliente em conexões SSL/TLS		Baixo
Conveniência			
	Facilidade de uso		Muito alto
	Mobilidade		Muito alta
	Independência da arquitetura		---
	Aproveitamento para outras funcionalidades		Baixo
Economia			
Economia nos gastos			Muito alta

6.2.5 Sistemas de autenticação baseados em senha utilizando S/Key

A utilização de sistemas de autenticação baseados em senha utilizando o protocolo S/Key, abordados na seção 3.3.4, possui algumas vantagens:

a) Os DCS armazenados no servidor de autenticação não são suficientes para personificar o usuário. A senha armazenada (cifrada por função *one-way hash*) é utilizada pelo sistema de autenticação para validar a próxima autenticação do usuário. Quando o protocolo S/Key é implementado como desafio-resposta, o número da senha a ser informada pelo usuário e parte da semente também estão armazenadas no servidor de autenticação. Ainda assim, estes dados não são suficientes para personificar o usuário;
b) A necessidade de informar a quantidade de acessos obriga a geração de um novo objeto de autenticação periodicamente. A senha (objeto de autenticação derivado) é válida para um único acesso.

O espaço médio de ataque não é afetado, mesmo que o usuário escolha sua parte da semente de modo trivial. Quando o protocolo S/Key é utilizado no modelo "desafio-resposta" o usuário necessita utilizar um *software* para gerar a senha. Isto pode limitar sua mobilidade.

Tabela 25: Avaliação dos sistemas de autenticação baseados em senhas utilizando S/Key

Segurança		
	Espaço médio de ataque	Muito baixo
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação	Médio
	Dificuldade da personificação quando do roubo do objeto de autenticação	Médio
	Dificuldade do roubo, cópia ou observação	Médio
	Freqüência da troca	Médio
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado	Médio
	Dificuldade de observação em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor	Baixo
	Freqüência de alteração	Muito alto
	Irretratabilidade da autenticação	Baixo
	Suporte à autenticação do cliente em conexões SSL/TLS	Baixo
Conveniência		
	Facilidade de uso	Médio
	Mobilidade	Alta
	Independência da arquitetura	---
	Aproveitamento para outras funcionalidades	Baixo
Economia		
Economia nos gastos		Alta

No caso da divulgação dos DCS e da senha (o objeto de autenticação derivado) em *site* impostor, é possível personificar o usuário na próxima tentativa de autenticação quando o S/Key é utilizado como lista de senhas, o que não ocorre no modo desafio-resposta: a senha informada pelo usuário é gerada a partir dos dados informados pelo servidor de autenticação.

A autenticação utilizando o protocolo S/Key não apresenta irretratabilidade, visto que no modelo "lista de senhas", as senhas são impressas e podem ser copiadas; no modelo "desafio-resposta", o *software* utilizado para gerar a próxima senha e o segredo do usuário podem ser copiados. É possível personificar o usuário em um ataque *man-in-the-middle*.

A Tabela 25 apresenta a avaliação dos sistemas de autenticação baseados em senha e utilizando o protocolo S/Key.

6.2.6 Sistemas de autenticação baseados em chaves assimétricas

A utilização de sistemas de autenticação baseados em chaves assimétricas, abordados na seção 4.1, possibilita a irretratabilidade, pois a chave privada precisa ficar somente em poder do usuário. Entretanto, a chave privada, além do problema do armazenamento discutido na seção 5.1.13 – "Insegurança no armazenamento da chave privada", também pode estar vulnerável dependendo do segredo escolhido para protegê-la (vulnerabilidade descrita na seção 5.1.8 – "Escolha de segredo trivial para proteger a chave privada").

Outras questões devem ser observadas na utilização das chaves assimétricas:

a) Onde é gerada a chave assimétrica do usuário;
b) Qual o algoritmo é utilizado para gerar as chaves (público ou secreto);
c) Tamanho dos números primos utilizados pelo algoritmo (tamanho da chave);
d) Qual é a relação de confiança entre o usuário, o sistema de autenticação e o sistema gerador das chaves assimétricas;
e) Como a chave pública é disponibilizada para o sistema de autenticação;
f) Como o usuário toma posse da chave privada.

Este trabalho considera que a chave privada está armazenada no computador do usuário. Entretanto, podem-se aplicar as mesmas avaliações do armazenamento da chave privada, quando da utilização de certificados digitais, descritas nas seções a seguir.

O algoritmo RSA está presente em vários navegadores e é o mais utilizado para gerar chaves assimétricas. A segurança deste algoritmo é supostamente baseada na dificuldade de encontrar os dois números primos cujo produto é a chave RSA.

Uma das formas para deduzir as chaves assimétricas geradas pelo algoritmo RSA é descobrir estes números primos utilizando técnicas de fatoração. Como existem regras para a geração da chave RSA, pode-se eliminar os valores irrelevantes, reduzindo, desta forma, o tempo de pesquisa. De acordo com Smith (2002), estas técnicas de fatoração fazem com que o espaço médio de ataque seja a metade do tamanho da chave RSA. Outras técnicas foram desenvolvidas para eliminar valores irrelevantes, como *quadratic sieve* (crivo quadrático) e *number field sieve* (crivo de corpo numérico) Smith (2002).

Segundo Smith (2002), estas técnicas não são eficientes para chaves RSA superiores a 429 bits. Para chaves RSA maiores, normalmente utiliza-se a heurística para estimar o número de passos computacionais necessários para fatorar os valores. De acordo com Smith (2002), este mesmo valor deve ser utilizado para estimar o espaço médio de ataque para chaves RSA. De acordo com Smith (2002), o espaço médio de ataque para chave com tamanho de 1024 *bits* é de 2^{86} e para chaves com 2048 bits é de 2^{116}.

Para efeito de análise, este trabalho irá considerar chaves com 1024 *bits*, visto que se identificou que os *Internetbanking* utilizam chaves com este tamanho.

A Tabela 26 exibe a avaliação deste sistema de autenticação, utilizando os parâmetros de comparação selecionados.

Tabela 26: Avaliação dos sistemas de autenticação baseados em chaves assimétricas

Segurança			
	Espaço médio de ataque		Alto
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação		Muito alto
	Dificuldade da personificação quando do roubo do objeto de autenticação		Baixo
		Dificuldade do roubo, cópia ou observação	Baixo
		Freqüência da troca	Médio
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado		Muito alto
		Dificuldade de observação em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor	Muito alto
		Freqüência de alteração	Muito alto
	Irretratabilidade da autenticação		Alto
	Suporte à autenticação do cliente em conexões SSL/TLS		Alto
Conveniência			
	Facilidade de uso		Médio
	Mobilidade		Muito baixa
	Independência da arquitetura		---
	Aproveitamento para outras funcionalidades		Baixo
Economia			
Economia nos gastos			Baixa

6.2.7 Sistemas de autenticação baseados em chaves assimétricas com certificados digitais

Uma das vantagens dos sistemas de autenticação baseados em chaves assimétricas com certificados digitais é que existe uma terceira entidade que valida a chave pública do usuário por meio do certificado digital.

Os certificados digitais podem ser utilizados para diversas finalidades, tais como:

a) Assinatura digital: no conceito das chaves assimétricas, a chave privada pode ser utilizada para assinar um documento digitalmente. Existe a garantia do emissor e da autenticidade do documento;
b) Confidencialidade e privacidade: utiliza-se o certificado digital do destinatário da mensagem para o documento. Apenas este poderá decifrar o documento utilizando sua chave privada;
c) Autenticação mútua em conexões SSL: o servidor WEB pode estar autenticado pelo seu certificado digital, assim como o usuário. Um procedimento de autenticação está descrito na seção 4.1.

A segurança do processo de autenticação por meio de chaves assimétricas com certificados digitais está relacionada à confiança na autoridade certificadora e ao controle e guarda da chave privada utilizada pelo usuário e pela autoridade certificadora. O controle e armazenamento da chave privada pelo usuário serão analisados nas seções a seguir.

Existe um risco em confiar na autoridade certificadora, que pode assinar um falso certificado (discutido na seção 5.1.14). Também existe o risco de se utilizar um certificado digital que esteja revogado (discutido na seção 5.1.15).

Outro fator importante é o PIN utilizado para abrir o repositório que armazena a chave privada. Este PIN apresenta as mesmas características da senha. Por exemplo, um PIN com tamanho de 6 caracteres composto somente por caracteres numéricos, tem espaço médio de ataque de 2^{19}. Porém, utilizando todos os caracteres alfanuméricos do teclado, o espaço médio de ataque passa a ser de 2^{34}.

A irretratabilidade de uma assinatura digital efetuada com a utilização de certificados digitais não pode ser contestada, pois somente a utilização da chave privada relacionada à chave pública contida no certificado digital pode ter executado a ação.

A necessidade de renovar o certificado digital, no âmbito da ICP-Brasil, varia de 1 a 3 anos. Esta renovação influencia o tempo de vida do objeto de autenticação.

6.2.7.1 Chave privada armazenada em arquivo

A chave privada armazenada em arquivo (formato PKCS#12) possui algumas vantagens:

a) Manipulação mais flexível;

b) Possibilidade de existir cópia de segurança.

A cópia não autorizada deste arquivo pode gerar vulnerabilidades, conforme as descritas nas seções 5.1.16 – "Escolha de segredo trivial para proteger a chave privada" e 5.1.17 – "Ataque de força bruta ao segredo utilizado para proteger a chave privada". A chave privada também pode ser capturada durante sua utilização, pois o processamento criptográfico é realizado no computador e a chave privada fica exposta na memória.

No âmbito da ICP-Brasil, a opção de armazenar a chave privada em arquivo não é permitida. No entanto, para efeito de comparação será considerada a validade do certificado digital de 1 ano.

A Tabela 27 exibe a avaliação deste sistema de autenticação, utilizando os parâmetros de comparação selecionados.

Tabela 27: Avaliação dos sistemas de autenticação baseados em chaves assimétricas com a chave privada armazenada em arquivo

Segurança		
	Espaço médio de ataque	Alto
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação	Muito alto
	Dificuldade da personificação quando do roubo do objeto de autenticação	Baixo
	Dificuldade do roubo, cópia ou observação	Baixo
	Freqüência da troca	Médio
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado	Muito alto
	Dificuldade de observação em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor	Muito alto
	Freqüência de alteração	Muito alto
	Irretratabilidade da autenticação	Alto
	Suporte à autenticação do cliente em conexões SSL/TLS	Alto
Conveniência		
	Facilidade de uso	Médio
	Mobilidade	Muito baixa
	Independência da arquitetura	---
	Aproveitamento para outras funcionalidades	Alto
Economia		
Economia nos gastos		Baixa

6.2.7.2 Chave privada armazenada em *smart cards* e *tokens* ICP

Como a utilização da chave privada é realizada internamente no *smart card* ou no *token* ICP, isto torna praticamente impossível sua captura.

O *smart card* ICP ou o *token* ICP possui a vantagem de poder armazenar outros dados, como informações pessoais. O *smart card* ICP apresenta algumas desvantagens:

a) O usuário deve possuir conhecimentos básicos sobre *smart cards* ICP, como o tipo de leitora com a qual o *smart card* ICP pode interagir;
b) Necessidade da utilização da leitora e do *driver* da leitora no computador. O *token* ICP também exige a instalação de um *driver*;
c) Pode apresentar problemas de compatibilidade. Ou seja, cada fabricante desenvolve seu próprio *smart card* ICP que somente pode ser utilizado em determinada leitora.

Eventualmente, o *smart card* ICP pode apresentar vulnerabilidades, conforme as descritas na seção 5.1.19.

No âmbito da ICP-Brasil, a validade do certificado digital com a chave privada armazenada em *smart card* ou em *token* ICP, sem capacidade de geração, é de 1 ano. Para *smart card* ou *token* ICP com capacidade de geração, a validade é de 3 anos. Este trabalho considera, para efeito de comparação, esta última opção. A Tabela 28 exibe a avaliação deste sistema de autenticação, utilizando os parâmetros de comparação selecionados.

Tabela 28: Avaliação dos sistemas de autenticação baseados em chaves assimétricas com a chave privada armazenada em *smart cards* e *tokens* ICP

Segurança		
	Espaço médio de ataque	Alto
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação	Muito alto
	Dificuldade da personificação quando do roubo do objeto de autenticação	Médio
	Dificuldade do roubo, cópia ou observação	Muito alto
	Freqüência da troca	Médio
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado	Muito alto
	Dificuldade de observação em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor	Muito alto
	Freqüência de alteração	Muito alto
	Irretratabilidade da autenticação	Alto
	Suporte à autenticação do cliente em conexões SSL/TLS	Alto
Conveniência		
	Facilidade de uso	Baixo
	Mobilidade	Baixa
	Independência da arquitetura	---
	Aproveitamento para outras funcionalidades	Alto
Economia		
Economia nos gastos		Muito baixa

6.2.7.3 Chave privada armazenada em mídias removíveis

Os *tokens* de memória, chamados aqui de mídias removíveis para melhor compreensão, foram descritas na seção 4.5.1. A Tabela 29 exibe a avaliação deste sistema de autenticação.

As mídias removíveis apresentam um custo financeiro baixo. No entanto, a segurança da chave privada pode ficar comprometida, pois sua utilização é feita no computador. Desta forma, ela pode ser capturada na memória ou quando é transferida do dispositivo de armazenamento para o computador.

No âmbito da ICP-Brasil, a validade do certificado digital com a chave privada armazenada mídias removíveis é de 1 ano.

Tabela 29: Avaliação dos sistemas de autenticação baseados em chaves assimétricas com a chave privada armazenada em mídias removíveis

Segurança			
	Espaço médio de ataque		Alto
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação		Muito alto
	Dificuldade da personificação quando do roubo do objeto de autenticação		Médio
		Dificuldade do roubo, cópia ou observação	Médio
		Freqüência da troca	Médio
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado		Muito alto
		Dificuldade de observação em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor	Muito alto
		Freqüência de alteração	Muito alto
	Irretratabilidade da autenticação		Alto
	Suporte à autenticação do cliente em conexões SSL/TLS		Alto
Conveniência			
	Facilidade de uso		Médio
	Mobilidade		Média
	Independência da arquitetura		---
	Aproveitamento para outras funcionalidades		Alto
Economia			
Economia nos gastos			Baixa

6.2.7.4 Chave privada armazenada em chip SIM, utilizado em aparelho celular

A utilização de aparelhos celulares para autenticar o usuário é similar à autenticação utilizando *smart cards* ICP, sendo a leitora o próprio aparelho celular.

O cartão SIM também permite outras utilizações como, por exemplo, o armazenamento de agenda telefônica e configuração da linha.

A Tabela 30 exibe a avaliação deste sistema de autenticação.

Tabela 30 Avaliação dos sistemas de autenticação baseados em chaves assimétricas com a chave privada em chip SIM

Segurança			
	Espaço médio de ataque		Alto
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação		Muito alto
	Dificuldade da personificação quando do roubo do objeto de autenticação		Médio
		Dificuldade do roubo, cópia ou observação	Muito alto
		Freqüência da troca	Médio
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado		Muito alto
		Dificuldade de observação em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor	Muito alto
		Freqüência de alteração	Muito alto
	Irretratabilidade da autenticação		Alto
	Suporte à autenticação do cliente em conexões SSL/TLS		Alto
Conveniência			
	Facilidade de uso		Médio
	Mobilidade		Alta
	Independência da arquitetura		---
	Aproveitamento para outras funcionalidades		Alto
Economia			
Economia nos gastos			Baixa

6.2.8 *Tokens* OTP

Os *tokens* OTP foram abordados na seção 4.5.2. Uma das vantagens em utilizar *token* OTP nos sistemas de autenticação é a curta validade do objeto de autenticação derivado, que neste caso é a senha OTP.

A personificação pode ser facilitada se o *token* OTP não precisar de PIN no processo de geração da senha OTP. A utilização do PIN em conjunto com *token* OTP provê uma camada adicional de segurança. Entretanto, somente *token* OTP sem PIN será avaliado, visto que se observou que este é o tipo mais utilizado em ambientes WEB. Outras vulnerabilidades dos *tokens* OTP estão descritas na seção 5.1.16.

Segundo Smith (2002, p. 268-270), a senha gerada pelos *tokens* OTP é o resultado de uma função matemática. Para ataques *offline* deve-se tentar quebrar a função. Por exemplo, sistemas que utilizam o algoritmo DES com chave de 56 *bits* possuem um espaço médio de ataque de 2^{55}. Para ataques interativos, considerando que o tamanho da senha OTP seja de seis dígitos, o espaço médio de ataque seria de 2^{19}. Neste trabalho, será considerada esta situação, pois representa maior risco.

A Tabela 31 exibe a avaliação deste sistema de autenticação, utilizando os parâmetros de comparação selecionados.

Tabela 31: Avaliação dos sistemas de autenticação baseados em *tokens* OTP

Segurança		
	Espaço médio de ataque	Muito baixo
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação	Médio
	Dificuldade da personificação quando do roubo do objeto de autenticação	Médio
	Dificuldade do roubo, cópia ou observação	Alto
	Freqüência da troca	Médio
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado	Alto
	Dificuldade de observação em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor	Alto
	Freqüência de alteração	Alto
	Irretratabilidade da autenticação	Baixo
	Suporte à autenticação do cliente em conexões SSL/TLS	Baixo
Conveniência		
	Facilidade de uso	Médio
	Mobilidade	Alta
	Independência da arquitetura	---
	Aproveitamento para outras funcionalidades	Baixo
Economia		
Economia nos gastos		Baixa

6.3 Resultado da análise

Os sistemas de autenticação que podem ser utilizados para autenticar usuários no *Internetbanking* foram analisados utilizando os parâmetros descritos na seção 6.1. Estes parâmetros estão associados às características desejadas nos sistemas de autenticação, como segurança, conveniência para o usuário e economia (menores custos). A Tabela 32 apresenta a avaliação de todos os sistemas de autenticação analisados. Esta tabela fornece um ponto de partida para o profissional, que necessita efetuar avaliações, escolher parâmetros relevantes que o auxiliem na escolha de sistemas adequados aos seus negócios.

Os protocolos *zero knowledge* apresentam peculiaridades que impedem a observação da senha na comunicação durante o processo de autenticação, além de efetuar autenticação mútua. Mas não impedem sua captura ao digitá-la.

Os sistemas de autenticação de usuários baseados “em posse” apresentam maiores dificuldades para a personificação. Podem-se combinar sistemas de autenticação para dificultar a personificação. Por exemplo, um sistema *Internetbanking* utiliza sistema de autenticação baseado em senha, pode utilizar um *token* OTP para concluir a autenticação. A avaliação destes sistemas poderia ser efetuada combinando as avaliações individuais de cada sistema de autenticação, por exemplo.

Nos sistemas de autenticação que utilizam senha, pelo menos duas entidades necessitam compartilhar o segredo (a senha) para que a autenticação possa ocorrer. A mesma situação ocorre com sistemas que utilizam *tokens* OTP: a semente e o algoritmo precisam ser conhecidos por pelo menos duas entidades. Já nos sistemas de autenticação que utilizam chaves assimétricas, somente uma entidade conhece o segredo (a chave privada). Esta característica torna a autenticação nestes sistemas irretratáveis: não é possível alegar que outra entidade também conhece o segredo. A autenticação é efetuada utilizando este segredo, sem a necessidade de apresentá-lo ao sistema de autenticação.

Os sistemas de autenticação baseados em *smart cards* e *tokens* ICP com certificados digitais fornecem irretratabilidade e podem ser utilizados para outras finalidades, como por exemplo, a substituição dos cartões magnéticos. A utilização dos certificados digitais também está relacionada à confiança na Autoridade Certificadora. Esta confiança pode ser adquirida com o passar do tempo e a utilização por vários usuários ou por força de lei, como na ICP-Brasil.

A questão da autenticação está relacionada em oferecer um ambiente propício para que cada um responda pelos seus atos. Sob esta visão, a segurança deve ser responsabilidade de todas as entidades participantes do processo: usuário, meio de acesso e empresa.

Chega-se a conclusão que quanto maior o nível de segurança, mais complexa é a utilização do sistema de autenticação pelo usuário e mais gastos são necessários.

Tabela 32: Comparativo da análise dos sistemas de autenticação

	Senhas utilizando					*Tokens* OTP	Chaves Assimé-tricas	Chaves assimétricas com certificado digital e chave privada armazenada em			
	Requisição Resposta	Desafio Resposta	Lista de senhas	ZKP	S/Key			Arquivo	Mídia removível	*Smart card* ICP	Chip SIM
Segurança											
Espaço médio de ataque	Muito baixo	Muito baixo	Muito baixo	Muito baixo	Muito baixo	Muito baixo[§]	Alto	Alto	Alto	Alto	Alto
Nível de segurança da proteção utilizada para armazenar DCS no servidor autenticação	Médio[†]	Médio[†]	Médio[†]	Médio[†]	Médio	Médio	Muito alto	Muito alto	Muito alto	Muito alto	Muito alto
Dificuldade da personificação quando do roubo do objeto de autenticação[i]	Muito baixo	Baixo	Baixo	Muito baixo	Médio	Médio	Baixo	Baixo	Médio	Médio	Médio
Dificuldade da personificação quando do roubo do objeto de autenticação derivado[ii]	Muito baixo	Médio	Baixo	Alto	Médio	Alto	Muito alto	Muito alto	Muito alto	Muito alto	Muito alto
Irretratabilidade da autenticação	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo	Alto	Alto	Alto	Alto	Alto
Suporte à autenticação do cliente em conexões SSL/TLS	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo	Alto	Alto	Alto	Alto	Alto
Conveniência											
Facilidade de uso	Muito alto	Médio	Médio	Muito alto	Médio	Médio	Médio	Médio	Médio	Baixo	Médio
Mobilidade	Muito alta	Alta	Alta	Muito alta	Alta	Alta	Muito baixa	Muito baixa	Média	Baixa	Alta
Independência da arquitetura	---	---	---	---	---	---	---	---	---	---	---
Outras funcionalidades	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo	Alto[1,2,3]	Alto[1,2,3]	Alto[1,2,3]	Alto[1,2,3,4]
Economia											
Economia nos gastos	Muito alta	Alta	Alta	Muito alta	Alta	Baixa	Baixa	Baixa	Baixa	Muito baixa	Baixa

[i] Parâmetro derivado dos parâmetros "Dificuldade do roubo, cópia ou observação do objeto de autenticação" e "Freqüência da troca do objeto de autenticação".
[ii] Parâmetro derivado dos parâmetros "Dificuldade de observação do objeto de autenticação derivado em ataque *man-in-the-middle* ou divulgação em site impostor" e "Freqüência da troca do objeto de autenticação derivado".
[1] Assinatura digital
[2] Confidencialidade e privacidade
[3] Autenticação mútua
[†] Supondo armazenado utilizando cifragem irreversível
[§] Considerada a situação que representa maior risco (ataque interativo)

7 ESTUDO DE CASO

Este capítulo apresenta estudos de caso mostrando exemplos de utilização da Tabela 32.

7.1 Caso 1: *Token* OTP ou *smart card* ICP

Neste caso, deseja-se identificar o ganho adicional se migrar o sistema de autenticação baseado em *token* OTP para o sistema de autenticação baseado em certificação digital, utilizando *smart card ICP*. O ganho poderá ser observado por meio da Tabela 33.

Tabela 33: Verificação do ganho adicional do *token* ICP para *smart card* ICP

		***Token* OTP**	***Smart card* ICP**	**Ganho/ Perda[14]**
Segurança				
	Espaço médio de ataque	Muito baixo	Alto	▲
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação	Médio	Muito alto	▲
	Dificuldade da personificação quando do roubo do objeto de autenticação	Médio	Médio	=
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado	Alto	Muito alto	▲
	Irretratabilidade da autenticação	Baixo	Alto	▲
	Suporte à autenticação do cliente em conexões SSL/TLS	Baixo	Alto	▲
Conveniência				
	Facilidade de uso	Médio	Médio	=
	Mobilidade	Alta	Média	▼
	Independência da arquitetura	---	---	---
	Aproveitamento para outras funcionalidades	Baixo	Alto	▲
Economia				
Economia nos gastos		Baixa	Muito baixa	▼

Os maiores ganhos na migração do sistema de autenticação estão na Segurança. O usuário, a princípio, poderá ter sua mobilidade prejudicada. Entretanto, ele poderá utilizar o *smart card* ICP para outras finalidades.

7.2 Caso 2: requisição-resposta e desafio-resposta ou *token* OTP

Neste caso, um *site Internetbankin*g utilizando sistema de autenticação baseado em

[14] Legenda:
▲Ganho
▼Perda
= Permanece inalterado

senha, está disponível. Deseja-se agregar mais segurança, adicionando outra camada de autenticação, como desafio-resposta ou *token* OTP.

Se adicionar desafio-resposta, a avaliação poderá ser efetuada conforme a Tabela 34:

Tabela 34: Avaliação do sistema de autenticação utilizando requisição-resposta e desafio-resposta

	Requisição Resposta	**Desafio Resposta**	**Avaliação 1**
Segurança			
Espaço médio de ataque	Muito baixo	Muito baixo	Muito baixo
Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação	Médio	Médio	Médio
Dificuldade da personificação quando do roubo do objeto de autenticação	Muito baixo	Baixo	Baixo
Dificuldade da personificação quando do roubo do objeto de autenticação derivado	Muito baixo	Médio	Médio
Irretratabilidade da autenticação	Baixo	Baixo	Baixo
Suporte à autenticação do cliente em conexões SSL/TLS	Baixo	Baixo	Baixo
Conveniência			
Facilidade de uso	Muito alto	Médio	Médio
Mobilidade	Muito alta	Alta	Alta
Independência da arquitetura	---	---	---
Aproveitamento para outras funcionalidades	Baixo	Baixo	Baixo
Economia			
Economia nos gastos	Muito alta	Alta	Alta

Se adicionar *token OTP*, a avaliação poderá ser efetuada conforme a Tabela 35:

Tabela 35: Avaliação do sistema de autenticação utilizando requisição-resposta e *token* OTP

	Requisição Resposta	***Token* OTP**	**Avaliação 2**
Segurança			
Espaço médio de ataque	Muito baixo	Muito baixo	Muito baixo
Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação	Médio	Médio	Médio
Dificuldade da personificação quando do roubo do objeto de autenticação	Muito baixo	Médio	Médio
Dificuldade da personificação quando do roubo do objeto de autenticação derivado	Muito baixo	Alto	Alto
Irretratabilidade da autenticação	Baixo	Baixo	Baixo
Suporte à autenticação do cliente em conexões SSL/TLS	Baixo	Baixo	Baixo
Conveniência			
Facilidade de uso	Muito alto	Médio	Médio
Mobilidade	Muito alta	Alta	Alta
Independência da arquitetura	---	---	---
Aproveitamento para outras funcionalidades	Baixo	Baixo	Baixo
Economia			
Economia nos gastos	Muito alta	Baixa	Baixa

Nesta situação, adicionar o sistema de autenticação baseado em *tokens* OTP (avaliação 2) agregará maior segurança, em relação ao desafio-resposta (avaliação 1), como poderá ser observado na Tabela 36.

Tabela 36: Comparação das avaliações

		Avaliação 1	**Avaliação 2**	**Ganho/ Perda**[15]
Segurança				
	Espaço médio de ataque	Muito baixo	Muito baixo	=
	Nível de segurança da proteção utilizada no armazenamento dos DCS no servidor autenticação	Médio	Médio	=
	Dificuldade da personificação quando do roubo do objeto de autenticação	Baixo	Médio	=
	Dificuldade da personificação quando do roubo do objeto de autenticação derivado	Médio	Alto	▲
	Irretratabilidade da autenticação	Baixo	Baixo	=
	Suporte à autenticação do cliente em conexões SSL/TLS	Baixo	Baixo	=
Conveniência				
	Facilidade de uso	Médio	Médio	=
	Mobilidade	Alta	Alta	=
	Independência da arquitetura	---	---	---
	Aproveitamento para outras funcionalidades	Baixo	Baixo	=
Economia				
Economia nos gastos		Alta	Baixa	▼

7.3 Conclusão

Estes estudos de caso serviram para mostrar a utilização da Tabela 32 em situações distintas. Também serviram para apontar como interpretar os resultados encontrados.

[15] Legenda:
▲Ganho
▼Perda
= Permanece inalterado

8 CONCLUSÕES

Este trabalho surgiu da constatação de que o grande volume de transações financeiras efetuadas pela Internet atrai, cada vez mais, quadrilhas de fraudadores e que os usuários das instituições financeiras ainda são ingênuos, em relação à segurança, ao utilizar os serviços disponíveis na Internet.

Um dos fatores que mais contribui para as fraudes é a autenticação de usuário ser realizada por meio de senhas. Muito utilizada até hoje, a autenticação por meio de senhas não permite validar eficazmente o usuário, não tendo como evitar a personificação.

O estudo das características dos sistemas de autenticação e a comparação entre estes sistemas procuram contribuir para minimizar o problema. As fraudes vêm gerando perdas financeiras e desconfiança dos usuários dos serviços financeiros oferecidos em ambientes WEB.

8.1 Conclusão

Este trabalho realizou uma análise comparativa dos sistemas de autenticação remota de usuário no acesso a sistemas WEB, mais especificamente para sistemas de *Internetbanking*, por meio da comparação de diversos parâmetros, agrupados em três áreas: segurança, conveniência e economia (menor custo).

Alguns destes parâmetros de comparação foram selecionados da literatura. Contudo, verificou-se que estes parâmetros eram insuficientes para caracterizar de forma mais abrangente os sistemas de autenticação de usuário para ambientes WEB. Por este motivo, tornou-se necessário escolher parâmetros adicionais para serem analisados.

O principal resultado do trabalho está resumido na Tabela 32, que apresenta o comparativo da análise dos sistemas de autenticação utilizando os parâmetros de comparação.

O resultado da análise serve como uma bússola para o profissional da área, fornecendo subsídios para a seleção dos sistemas de autenticação mais apropriados às necessidades do negócio, em função das restrições existentes relacionadas à segurança, conveniência e custos.

Este trabalho complementa o trabalho de O'Gorman (2003), acrescentando novos parâmetros de comparação e descrevendo controles para reduzir os riscos associados às vulnerabilidades. Com relação aos de trabalhos de Pinkas e Sander (2002), Santos, *et al.* (2004), Lagares e Souza (2005) e Carnut e Hora (2005), apresenta meios para comparar os

novos protocolos de autenticação baseados em senhas com outros sistemas de autenticação. Este trabalho complementa o trabalho de Nilsson, Adams e Herd.(2005), avaliando a conveniência de uso dos sistemas de autenticação para o usuário.

Este trabalho não teve como objetivo indicar a melhor alternativa, já que cada ambiente possui características específicas, as quais podem restringir as opções de escolha.

8.2 Dificuldades encontradas

Durante o desenvolvimento deste trabalho não foi possível efetuar uma estimativa dos custos de implantação e manutenção dos sistemas de autenticação.

O levantamento dos sistemas de autenticação foi feito pela observação dos *sites* de *Internetbanking*, já que os detalhes da autenticação é uma questão estratégica dos bancos.

8.3 Contribuições

Este trabalho gerou contribuições como a descrição das vulnerabilidades relacionadas aos sistemas de autenticação em ambientes WEB e os controles que podem ser utilizados para minimizá-las.

Outra contribuição deste trabalho foi relacionar e comparar outros sistemas de autenticação baseados em senha como:

- Desafio-resposta;
- Lista de senhas;
- S/Key;
- *Zero Knowledge Password*.

Também relacionou e comparou sistemas de autenticação utilizando certificação digital em aparelhos celulares com chip SIM.

Outra contribuição deste trabalho foi identificar os parâmetros de comparação que podem ser utilizados para analisar sistemas de autenticação com características diferentes. A literatura apresenta alguns parâmetros de comparação que podem ser utilizados para comparar diferentes sistemas de autenticação. Os seguintes parâmetros foram selecionados da literatura:

- Espaço médio de ataque (Smith, 2002);
- Dificuldade do roubo, cópia ou observação do objeto de autenticação (O'GORMAN, 2003);
- Irretratabilidade da autenticação (O'GORMAN, 2003);

- Facilidade de uso (O'GORMAN, 2003);
- Custo (O'GORMAN, 2003).

Contudo, os parâmetros selecionados eram insuficientes para analisar os sistemas de autenticação de usuário. Para caracterizar os sistemas de autenticação de usuário de forma mais abrangente, novos parâmetros de comparação foram definidos:

- Nível de segurança da proteção utilizada para armazenar DCS no servidor de autenticação;
- Freqüência da troca do objeto de autenticação;
- Dificuldade da personificação quando do roubo do objeto de autenticação;
- Dificuldade da observação do objeto de autenticação derivado em ataque *man-in-the-middle* ou da sua divulgação em *site* impostor;
- Freqüência ou possibilidade de alteração do objeto de autenticação derivado;
- Dificuldade da personificação quando do roubo do objeto de autenticação derivado;
- Suporte à autenticação do cliente em sessão SSL/TLS;
- Mobilidade;
- Independência da arquitetura;
- Aproveitamento para outras finalidades.

A utilização destes parâmetros de comparação, que são descritos na seção 6.1, permite identificar as principais características de um sistema de autenticação. Tais parâmetros foram agrupados em 3 áreas: segurança, conveniência e custo.

Outra contribuição é a Tabela 32. O formato de tabela permite avaliar as características de um sistema de autenticação quando se utiliza mais de um fator de autenticação. Este formato aceita que se agreguem novos sistemas de autenticação que possam ser utilizados para identificar e autenticar o usuário em ambientes WEB e compará-los com os atuais.

8.4 Trabalhos futuros

No desenvolver do trabalho foram identificados pontos que podem ser estudados em trabalhos futuros. Um dos pontos identificados é o estudo dos sistemas de autenticação pelo parâmetro espaço médio de ataque, quantificando valores para o objeto de autenticação (como senhas, *tokens*) e o objeto de autenticação derivado (como a senha OTP).

Outro ponto importante é a tecnologia escolhida para desenvolver os sistemas WEB. A utilização de tecnologias proprietárias ou que somente possam ser executadas em plataforma

específica, mesmo que bastante utilizada, pode impor limitações para o usuário, restringindo seu direito, por exemplo, de escolher o navegador e sistema operacional que melhor lhe convém. Um trabalho futuro poderia avaliar este ponto, complementando este trabalho no parâmetro independência da arquitetura.

REFERÊNCIAS

ABBOT, J. Smart Cards: How Secure Are They?. **SANS Reading Room**. Março. 2002. Disponível em <http://www.sans.org/rr>. Acesso em: 25 abr. 2005.

ARONSSON, A. H. Zero knowledge Protocolos and Small Systems. **Network Security**. Department of Computer Sciense. Helsinki University of Technology. [1995]. Disponível em <http://www.tml.tkk.fi/Opinnot/Tik-110.501/1995/zeroknowledge.html>. Acesso em: 9 set. 2005.

Banco Central do Brasil. **Estatísticas**. BCB. 2005. Disponível em <http://www.bcb.gov.br /htms/Deorf/d200503/quadro7.asp >. Acesso em: 13 abr. 2005.

BELLOVIN, S.; MERRIT, M. Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionay Attacks. In: Proceedings of the IEEE Symposium on Research in Security and Privacy. **Proceedings…** Oakland, CA, EUA. Maio. 1992. p. 72-84.

CARNUT, M. C.; HORA, E. C. Improving the Diceware Memorable Passphrase Generation System. In: VII Simpósio Segurança em Informática (SSI˙2005), São José dos Campos, SP, Brasil. **Anais...** Novembro. 2005.

CERTISIGN. **Central de FAQS**. [2005]. Disponível em http://www.certisign.com.br/suporte /central_faqs/icpbrasil/icp.jsp>. Acesso em: 02 fev. 2005.

CHAPMAN, D. B.; ZWICKY, E. D. **Building Internet Firewalls**. O´Reilly, Novembro. 1995. 517 p. ISBN 1-56592-124-0.

EMV. **Frequent Asked Questions**. [2000]. Disponível em <http://www.emvco.com>. Acesso em: 19 maio 2005.

Federação Brasileira dos Bancos. **Resultados**: Números de contas, cartões de débito e clientes com *InternetBanking*. FEBRABAN. Disponível em <http://www.febraban.org.br>. Acesso em: 15 fev. 2006.

GARFINKEL, S.; SPAFFORD, E.H. **Web Seurity & Commerce**. O´Reilly, Junho. 1997. 500 p. ISBN 1-56592-269-7.

HALLER, N. M. The S/Key One Time Password System. Proceedings of the Symposium on Network and Distributed Systems Security. Internet Society. Fevereiro. 1994. **Electronic Proceedings...** Disponível em <www.alw.nih.gov/Security/FIRST/papers/password/skey.ps>. Acesso em: 18 nov. 2005.

Infra-estrutura de Chaves Públicas-Brasil. **O que é ICP-Brasil**. ICP-Brasil [2004]. Disponível em <http://www.icpbrasil.gov.br>. Acesso em: 03 dez. 2004.

Infra-estrutura de Chaves Públicas-Brasil. **Resolução 41**. ICP-Brasil [2005]. Disponível em <http://www.icpbrasil.gov.br>. Acesso em: 30 mai. 2005.

International Organization for Standardization. Information technology **-** Security Techniques **-** Non**-**repudiation - Part 1: **General**. ISO/IEC 13888-1:2004. 15 p. Junho. 2004.

_____. Identification cards - Integrated circuit(s) cards with contacts - Part 1: **Physical characteristics**. ISO/IEC 7816-1:1998. 03 p. Novembro. 1998.

_____. Identification cards - Integrated circuit cards - Part 2: **Cards with contacts - Dimensions and location of the contacts**. ISO/IEC 7816-2:1999. 05 p. Janeiro. 2005.

_____. Identification cards - Integrated circuit(s) cards with contacts - Part 3: **Electronic signals and transmission protocols**. ISO/IEC 7816-3:1997. 27 p. Abril. 2003.

_____. Identification cards - Integrated circuit cards - Part 4: **Organization, security and commands for interchange**. ISO/IEC 7816-4:2005. 83 p. Janeiro. 2005.

_____. Identification cards - Integrated circuit cards - Part 5: **Registration of application providers**. ISO/IEC 7816-5:2004. 2 p. Dezembro. 2004.

_____. Identification cards - Integrated circuit cards - Part 6: **Interindustry data elements for interchange**. ISO/IEC 7816-6:2004. 19 p. Maio. 2004.

_____. Identification cards - Integrated circuit(s) cards with contacts - Part 7: **Interindustry commands for Structured Card Query Language**. ISO/IEC 7816-7:1999. 36 p. Janeiro. 2005.

_____. Identification cards - Integrated circuit cards - Part 8: **Commands for security operations**. ISO/IEC 7816-8:2004. 19 p. Junho. 2004.

_____. Identification cards - Integrated circuit cards - Part 9: **Commands for card management**. ISO/IEC 7816-9:2004. 12 p. Junho. 2004.

_____. Identification cards - Integrated circuit(s) cards with contacts - Part 10: **Electronic signals and answer to reset for synchronous cards**. ISO/IEC 7816-10:1999. 7 p. Janeiro. 2005.

_____. Identification cards - Integrated circuit cards - Part 11: **Personal verification through biometric method**s. ISO/IEC 7816-11:2004. 33 p. Março. 2004.

_____. Identification cards - Integrated circuit cards - Part 15: **Cryptographic information**. ISO/IEC 7816-15:2004. 70 p. Janeiro. 2004.

JABLON, D. Strong Password-Only Authenticated Key Exchange. **ACM SIGCOMM Computer Communication Review**. ACM Press. Vol. 26, no. 5, p. 5-26. Outubro. 1996.

KALISKI, B. Further improvements in PKCS #11 and PKCS #15. **RSA Security**. [2000] Disponível em <http://www.rsasecurity.com/rsalabs/staff/bios/bkaliski/publications/other/kaliski-pkcs-11-and-15-ctst-2000.ppt>. Acesso em: 02 fev. 2005.

LAGARES, K. A. P.; SOUZA, J. N. Apresentação de Senhas em Máquinas Hostis. In: VII Simpósio Segurança em Informática (SSI`2005), São José dos Campos, SP, Brasil. **Anais...** Novembro. 2005.

LAMPORT, L. Password Authentication with Insecure Communication. **Communications of the ACM**. ACM Press. Vol. 24, no. 11, p. 770-772. Novembro. 1981.

MENEZES, A.; van OORSCHOT, P.; VANSTONE, S. Identification and Entity Authentication. In: :_____ **Handbook of Applied Cryptograph**. CRC Press, 1996. Cap. 10. p. 385-424

MEIER, J. D., *et al*. **Improving Web Application Security: Threats and Countermeasures**. Microsoft Press. 2003.

MYERS, M., *et al*. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. RFC 2560. **IETF**. Junho. 1999. Disponível em <http://www.ietf.org/rfc/rfc2560.txt>. Acesso em: 16 ago. 2005.

MOZILLA. **Mozilla Foundation Security Advisory 2005-33**. [2005]. Disponível em <http://www.mozilla.org/security/announce/mfsa2005-33.html>. Acesso em: 01 jul. 2005.

NILSSON, M.; Adams, M.; Herd, S. Building Security and Trust in online banking In: Conference on Human Factors in Computing System*s* CHI'05 extended abstracts on Human factors in computing systems. Portland. OR. USA. **Proceedings...** 2005. p. 1701-1704

National Institute of Standards & Technology. An Introduction to Computer Security: The NIST Handbook. FIPS 800-12. **NIST**. Outubro. 1995.

_____. Underlying Technical Model for Information Technology Security. SP 800-33. **NIST**. Dezembro. 2001.

O'GORMAN, L. Comparing Passwords, Tokens and Biometrics for User Authentication. **Proceedings of the IEEE**, Vol. 91, No. 12, p. 2019-2040, Dezembro. 2003.

PAINE, S.; BURNETT, S. **Criptografia e Segurança: O Guia Oficial RSA**. Tradução de Edson Furman Lciewicz. Editora Campus 2002. 367 p.

PERLMAN, R.; KAUFMAN C. Secure Password-Based Protocol for Downloading a Private Key In: The 1999 Network and Distributed System Security Symposium. Internet Society Conference. 1999. **Proceedings...** Disponível em <www.isoc.org /isoc/conferences/ndss/99/ proceedings/papers/perlman.pdf >. Acesso em 9 set. 2005.

PINKAS, B; SANDER, T. Securing Passwords Against Dictionary Attacks In: The 9th ACM Conference on Computer and Communications Security. Washington, DC, USA. 2002. **Proceedings...** p. 161-170

RSA Security Inc. What are Message Authentication Codes? **RSA** .[2005]. Disponível em <www.rsasecurity.com/rsalabs/node.asp?id=2177#>. Acesso em 3 dez 2005.

SANTOS, F. G., *et al*. **Autenticação utilizando senhas descartáveis baseadas em caos**. [2004]. Disponível em <http://inf.ufsc.br>. Acesso em: 17 maio 2005.

SCHNEIER, B. Customers, Passwords, and Websites In: **IEEE Security & Privacy Columns**. Julho/Agosto. 2004.

SMITH, Richard E. **Authentication: From Passwords to Public Keys**. Addison Wesley, 2002. 550 pp. ISBN 0-201-61599-1

SOUZA, B. A. **Teoria dos números e o RSA**. Dissertação (Mestrado em Matemática Aplicada) – UNICAMP, Campinas, 2004.

GLOSSÁRIO

Ameaça – evento ou atividade executada de maneira deliberada ou intencional, podendo causar danos em sistemas, através da exploração de vulnerabilidade.

Dados críticos de segurança (DCS) - representam informações sensíveis e relacionadas à segurança, tais como, chaves criptográficas privadas, chaves simétricas de caráter secreto, chaves de sessão e dados de autenticação (senhas e PIN, por exemplo), cuja divulgação ou modificação podem comprometer a segurança de um módulo criptográfico.

Digesto – ver *hash*.

Engenharia social – técnica para obter informações sensíveis sem autorização, enganando ou induzindo o detentor das informações a fornecê-las.

Função *one-way hash* (função de espalhamento) – algoritmo que gera um valor com tamanho fixo a partir de uma mensagem, utilizado para identificar se a mensagem foi alterada. Não é possível derivar a mensagem original a partir deste valor.

GSM – sistema de comunicação utilizado em aparelhos celulares, que permite a utilização de 8 linhas simultâneas na mesma freqüência.

Hash – valor com tamanho fixo produzido por uma função *hashing*, cujas características são não ser possível recompor o valor original a partir do *hash* e que a alteração de pelo menos um *bit* da mensagem original altera o *hash*.

Impresonation – representar ser outro indivíduo de tal modo que uma terceira parte distinta acredite que é o verdadeiro parceiro, aceitando a identidade: personificação.

Keylogger – tipo de programa espião que captura as teclas pressionadas.

Keyspace – conjunto de valores diferentes e possíveis para uma chave.

Matriz impressa – Termo utilizado para designar o cartão de papel nos quais as respostas estão impressas no formato de matriz ou tabela.

Man-in-the-middle – tipo de ataque em que a mensagem original é interceptada antes de chegar ao destino, podendo ser manipulada.

Mouse-logger – tipo de programa espião que captura eventos do mouse, como o clique.

NTLM – protocolo de autenticação que utiliza o conceito de desafio-resposta. É baseado no protocolo de autenticação LAN Manager (LM) desenvolvido pela IBM.

Sistemas de autenticação - são os programas, equipamentos, infra-estruturas de rede e processos necessários para que a autenticação do usuário ocorra.

Spyware – programas espiões instalados no computador sem o conhecimento do usuário, ou instalados através de controles ActiveX ou Java, que podem estar armazenados em páginas de *sites* da Internet.

Trojan – programa que se instala no computador do usuário, tendo como objetivo o roubo de dados específicos. Após colher os dados, como número de contas e senhas bancárias, enviam estes dados e pode auto destruir-se, eliminando qualquer vestígio de sua existência.

Vulnerabilidade – falha ou fragilidade de um sistema ou programa, que pode possibilitar brechas para a ocorrência de danos no sistema ou programa.