A Segurança Informática e o Negócio Electrónico

FICHA TÉCNICA

Título
A SEGURANÇA INFORMÁTICA
E O NEGÓCIO ELECTRÓNICO

Autores
Hugo Magalhães e Alberto Grilo

Editor
© SPI – Sociedade Portuguesa de Inovação
Consultadoria Empresarial e Fomento da Inovação, S.A.
Edifício «Les Palaces», Rua Júlio Dinis, 242,
Piso 2 – 208, 4050 PORTO
Tel.: 226 076 400, Fax: 226 099 164
spiporto@spi.pt; www.spi.pt
Porto • 2006

Produção Editorial
Princípia
Av. Marques Leal, 21
2775-495 S. João do Estoril
Tel.: +351 214 678 710; Fax: +351 214 678 719
encomendas@principia.pt
www.principia.pt

Projecto Gráfico e *Design*
Mónica Dias

Impressão
Rolo e Filhos, Artes Gráficas, Lda.

ISBN 972-8589-68-9

Depósito Legal 249616/06

Projecto apoiado pelo Programa Operacional Plurifundos da Região Autónoma da Madeira (POPRAMIII), co-financiado pelo Estado Português, e pela União Europeia, através do Fundo Social Europeu.

NEGÓCIO ELECTRÓNICO

A Segurança Informática e o Negócio Electrónico

Hugo Magalhães | Alberto Grilo

spi
Sociedade Portuguesa de Inovação

INTRODUÇÃO

A Segurança Informática e o Negócio Electrónico

O advento da globalização económica e das tecnologias da informação e comunicação como a Internet permitiu às empresas reequacionarem as estratégias de actuação no mercado, introduzindo vantagens competitivas em relação ao ambiente de negócios tradicional, nomeadamente o aumento da dimensão dos mercados, a presença permanente (24 horas por dia, sete dias por semana), a redução de custos e a diminuição da cadeia de distribuição. Esta alteração deu origem a uma nova forma de vender e comprar – o negócio electrónico – que se tem convertido num factor fundamental de competitividade e num fortíssimo indutor de desenvolvimento para a generalidade das empresas. A título de exemplo, veja-se o sucesso da Dell Inc., que nos últimos anos apresentou um crescimento acentuado, tornando-se num dos maiores fabricantes e vendedores de computadores a nível mundial.

Contudo, a crescente utilização da Internet como meio para realizar negócios electrónicos e a intensificação das ameaças terroristas trazem consigo um conjunto de preocupações relativas à protecção de dados dos utilizadores e dos sistemas. Além do mais, são infindáveis as histórias dos *hackers* que desafiam os mais sofisticados sistemas de segurança na rede.

Este manual tem como principal objectivo apresentar as ferramentas e as soluções que permitem garantir condições e níveis de confiança elevados em qualquer troca de informação realizada através da Internet. O Capítulo 1 introduz as noções básicas de segurança da informação, designadamente as principais ameaças e as propriedades que a informação deve possuir de modo a evitá-las.

O Capítulo 2 apresenta as principais técnicas de segurança, baseadas em algoritmos criptográficos de chave simétrica, assimétrica e de sumário, que constituem peças fundamentais no conjunto de tecnologias de suporte ao negócio electrónico na Internet. O principal objectivo destes algoritmos é garantir que os intervenientes numa troca de informação tenham garantias de que os requisitos de segurança são satisfeitos.

O Capítulo 3 descreve alguns mecanismos de segurança (*firewalls*, sistemas de detecção de intrusão e antivírus) adicionais para as redes que suportam o fluxo de comunicação no negócio electrónico, que conjugados com as técnicas apresentadas no capítulo anterior fornecem um contributo indispensável para garantir um nível de segurança adequado.

O Capítulo 4 apresenta alguns dos principais modelos de pagamento electrónico, nomeadamente cartões de débito e crédito, na perspectiva da sua utilização na Internet.

Finalmente, o Capítulo 5 descreve a importância de uma política de segurança bem definida e rigorosa num negócio electrónico.

HUGO MAGALHÃES
ALBERTO GRILO

C A P Í T U L O 1

Noções Básicas de Segurança

O B J E C T I V O S

- Identificar as principais ameaças à segurança de uma comunicação feita pela Internet, nomeadamente modificação, repetição, disfarce, negação de serviço, intercepção e repúdio
- Apresentar as garantias de segurança existentes, como confidencialidade, integridade, autenticação, autorização, registo e não-repúdio

Com o advento dos sistemas de informação e da caracterização da sociedade actual como uma sociedade em rede, a generalidade das empresas tornou-se fortemente dependente dos seus sistemas informáticos para gerir as suas actividades comerciais e suportar a tomada de decisão. Não é, por isso, de admirar que os responsáveis pelos sistemas informáticos das empresas se preocupem cada vez mais com os efeitos desastrosos que teria uma ameaça ou um ataque que comprometesse o funcionamento desses sistemas e a informação que possuem.

Este capítulo introduz as principais ameaças à segurança da informação transmitida pela Internet, nomeadamente modificação, repetição, disfarce, negação de serviço, intercepção e repúdio. Para além disso, são também apresentadas as propriedades que a informação deve possuir de modo a evitar essas ameaças.

Ameaças à Segurança

Uma *ameaça* (ataque), no contexto informático, é qualquer acção efectuada com o intuito de comprometer a segurança do fluxo de informação entre duas entidades.

Considere a situação mais simples, em que um emissor envia uma mensagem a um receptor com informação confidencial. Se um terceiro interveniente (atacante) pretender realizar um ataque à comunicação, a acção pode ser levada a cabo sobre:

- a mensagem (Figura 1.1);
- o canal de comunicação;
- a infra-estrutura do emissor ou do receptor.

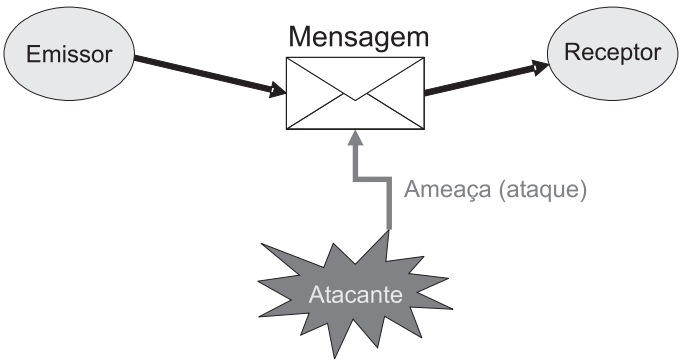


Figura 1.1
Esquema de um ataque a uma mensagem

No entanto, uma vez que, em algumas situações, o atacante é o próprio emissor ou receptor, pode existir uma entidade independente,

em quem ambos confiem (TTP – *trust third party*), para auxiliar a comunicação.

Em termos gerais, os ataques a que os fluxos de informação estão sujeitos podem ser classificados em seis categorias: *modificação*, *repetição*, *intercepção*, *disfarce*, *repúdio* e *negação de serviço (denial of service)*.

MODIFICAÇÃO

Consiste na alteração dos dados da mensagem em trânsito (Figura 1.2). A alteração pode ocorrer de forma acidental ou maliciosa, quando, por exemplo, num negócio, um agente não autorizado altera uma encomenda de dez unidades por parte de uma entidade para 1000 unidades.

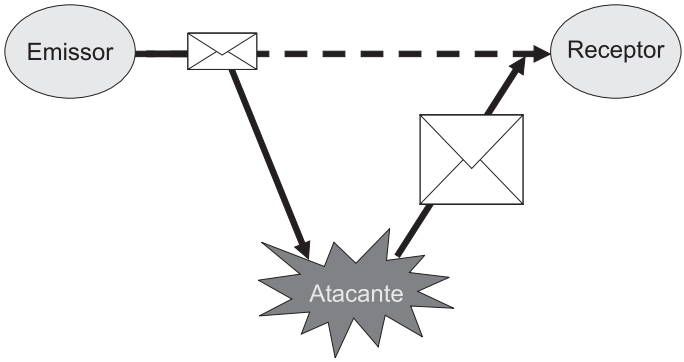


Figura 1.2
Esquema de um ataque de modificação

REPETIÇÃO

Acontece quando uma operação já realizada é repetida, sem autorização, de modo a obter o mesmo resultado (Figura 1.3). Considere, por exemplo, o caso em que um fornecedor utiliza sucessivamente os dados enviados por um comprador para efectuar o pagamento, obtendo de forma ilícita vários pagamentos adicionais.

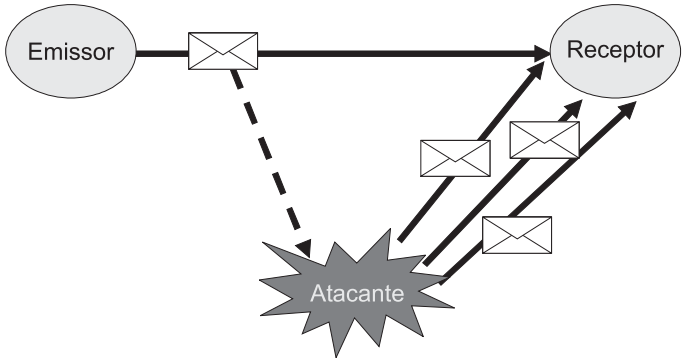


Figura 1.3
Esquema de um ataque de repetição

INTERCEPÇÃO

Ocorre quando se verifica o acesso não autorizado a uma mensagem, que, contudo, não tem a possibilidade de alterar (Figura 1.4). Um exemplo desse ataque é a «escuta» da informação trocada entre duas sucursais de uma empresa por uma empresa concorrente.

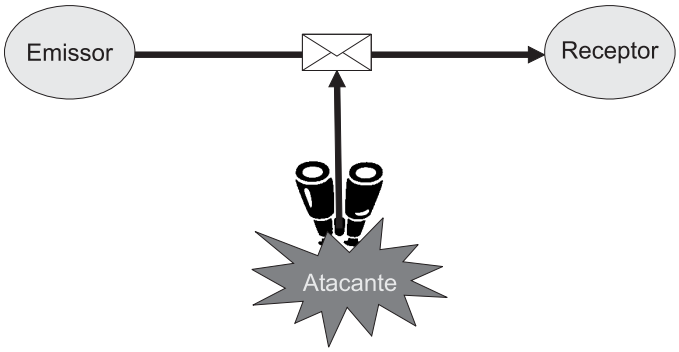


Figura 1.4
Esquema de um ataque de intercepção

DISFARCE

Consiste em apresentar uma identidade falsa perante um determinado interlocutor (Figura 1.5). Isto pode acontecer, por exemplo, quando um agente não autorizado pretende ocultar a sua própria identidade ou quando assume a identidade de outrem com o intuito de prejudicar o detentor daquela identidade.

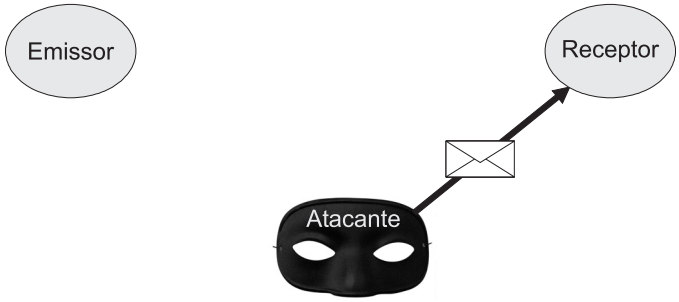


Figura 1.5
Esquema de um ataque de intercepção

REPÚDIO

Consiste na negação de participação numa determinada comunicação ou operação quando de facto se fez parte dela (Figura 1.6). Acontece por exemplo quando um comprador nega a autoria e/ou o envio de uma mensagem com uma ordem de pagamento, ou quando um vendedor nega ter recebido o cancelamento de uma encomenda.

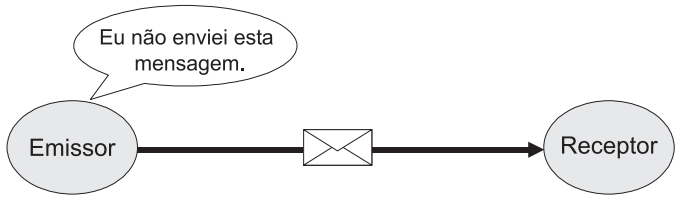


Figura 1.6
Esquema de um ataque de repúdio

NEGAÇÃO DE SERVIÇO

Consiste na realização de um conjunto de acções com o objectivo de dificultar o bom funcionamento de um sistema, por exemplo, saturando uma infra-estrutura de comunicação ou restringindo todas as mensagens para um destino específico (Figura 1.7).

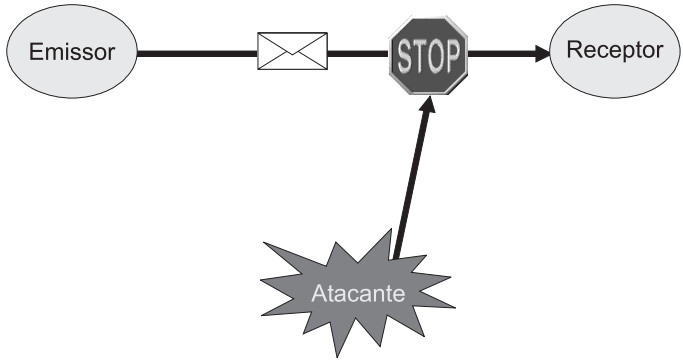


Figura 1.7
Esquema de um ataque de negação de serviço

Estas seis categorias podem ser agrupadas em duas classes de acordo com a metodologia utilizada no ataque: os ataques *activos* e os ataques *passivos* (Figura 1.8).

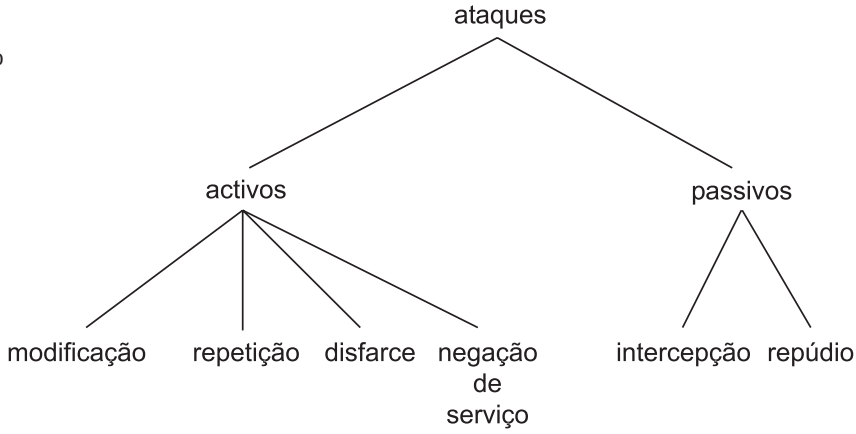


Figura 1.8
Classificação dos ataques de acordo com a metodologia

Garantias de Segurança

As características que a informação deve possuir para garantir a sua segurança podem ser classificadas em *confidencialidade*, *integridade*, *autenticação*, *autorização*, *registo* e *não-repúdio*.

CONFIDENCIALIDADE

É a propriedade que consiste na protecção de informação sensível ou privada contra um ataque de intercepção, ou seja, contra acessos não autorizados. Em geral, essa garantia obtém-se através da codificação dos dados utilizando *algoritmos de cifra* (que serão descritos no Capítulo 2).

INTEGRIDADE

É a característica que consiste na protecção da informação contra um ataque de modificação. Numa comunicação entre dois interlocutores, consegue-se garantir essa segurança ou, pelo menos, detectar que ocorreu uma modificação, utilizando *algoritmos de sumário* (ver Capítulo 2).

AUTENTICAÇÃO

É a propriedade que consiste na protecção contra o disfarce da identidade de um interlocutor de modo a que numa comunicação haja a garantia de os participantes serem quem dizem ser. Isto pode ser conseguido através da utilização de:

1. Segredos entre os participantes, como senhas ou combinações de *username/password*;

2. Dispositivos únicos como *tokens* de segurança, *smartcards* e cartões de «batalha naval»;
   Um *token* de segurança, também por vezes denominado *token* de *hardware*, *token* de autenticação ou *token* criptográfico, é um pequeno dispositivo físico que um utilizador transporta de modo a ter autorização de acesso a um determinado serviço como, por exemplo, uma rede informática (Figura 1.9a). Um *token* pode armazenar uma chave criptográfica, como uma assinatura digital (ver Capítulo 2), dados biométricos como uma

impressão digital ou até incorporar um pequeno teclado para introdução do número de identificação pessoal, mais conhecido por PIN *(personal identification number)*.

Um *smartcard* (Figura 1.9b) é um pequeno cartão de plástico com um microprocessador *(chip)* incorporado de modo a ter capacidade de armazenamento e memória. É cada vez maior o número de cartões de débito e crédito com *smartcards* incorporados. A título ilustrativo, veja-se a seguinte notícia sobre a utilização de *smartcards* para garantir a segurança.

UMA NOVA FORMA DE UTILIZAR OS CARTÕES

«*A tecnologia* chip *traz associada uma maior segurança nas transacções, bem como uma nova forma de relacionamento com o titular do cartão. Os custos operacionais vão diminuir*.

Num futuro próximo, vai ao futebol acompanhado de um simples cartão bancário. Compra o bilhete, que é automaticamente "carregado" no cartão, paga umas bebidas e uns aperitivos encostando-o a um terminal de pagamento, e para entrar no estádio só tem de accionar o torniquete de acesso às bancadas passando o mesmo cartão por um terminal de leitura para validar o bilhete.

A tecnologia *chip* traz consigo desde logo maior segurança das transacções, mas também "uma nova forma de usar o cartão com mais valor para o titular, tal como a inclusão de programas de lealdade dinâmicos em que o titular do cartão parametriza os benefícios de acordo com as suas preferências", explicou Paulo Raposo, director local da MasterCard em Portugal. "O *chip* abre um novo mundo de potencialidades e possibilidades para os bancos, titulares de cartões e negócios que aceitem pagamentos com os mesmos", acrescenta Sérgio Botelho, director-geral da Visa Europe para Portugal.

As duas entidades foram responsáveis pela criação do *standard* global conhecido por EMV, as iniciais de Europay International, hoje MasterCard Europe, MasterCard International e a Visa International. A segurança é elegida como a maior vantagem desta tecnologia. "Trata-se de uma tecnologia mais recente em que no processo de validação de uma transacção existe a troca de mensagens encriptadas entre o terminal de leitura e o cartão obrigando a validações quer no terminal quer no próprio cartão. Os parâmetros de validação numa e noutra partes tornam o processo de quebra de segurança muito mais complicado", comenta Paulo Raposo. De igual modo, Sérgio Botelho reforça o facto de esta nova tecnologia permitir aos portugueses titulares de cartões terem mais segurança nas suas transacções a nível nacional e no estrangeiro, nomeadamente em países onde o risco de fraude é reconhecidamente maior. Além de menores níveis de fraude, os custos administrativos relativos à transacção também serão menores. "Antecipamos a redução de custos operacionais na medida em que a grande maioria das transacções com cartão EMV pode ser efectuada *off-line*, uma vez que o *chip* tem maior capacidade de armazenamento de informa-

ção comparativamente à banda magnética", observa Sérgio Botelho. Quanto aos custos inerentes à nova tecnologia, são variáveis "por que dependem também das economias de escala e da sua aplicação. À medida que mais cartões com *chip* são produzidos e mais terminais *chip* são fabricados, menores são os custos unitários para o sistema", refere Sérgio Botelho, acrescentando: "O custo da produção física de cartões com *chip* EMV pode ser largamente ultrapassado pelos benefícios e vantagens acrescidas que permitem gerar".»

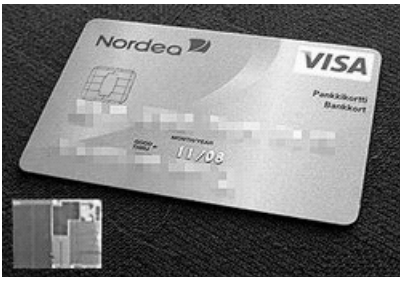
Fonte: *Diário Económico* de 11 de Setembro de 2006 (http://diarioeconomico.sapo.pt/)

Um cartão de «batalha naval» (Figura 1.9c) é um pequeno cartão que contém uma matriz de elementos que permitem a um utilizador a realização de determinadas operações, como, por exemplo, transacções electrónicas bancárias. Suponha que a matriz de elementos é a que se apresenta na Figura 1.9c. Se, para realizar uma determinada transacção, for solicitada a célula A1, então o código de autenticação é «123»;

Figura 1.9
Exemplo de um *token* (a), de um *smartcard* (b) e de um cartão de «batalha naval» (c)

a

b



c

	1	2	3	4	5	6	7	8
A	123	456	789	023	478	552	115	365
B	236	416	589	033	458	142	215	825
C	123	456	789	023	478	552	115	365
D	236	416	589	033	458	142	215	825
E	123	456	789	023	478	552	115	365
F	236	416	589	033	458	142	215	825
G	123	456	789	023	478	552	115	365
H	236	416	589	033	458	142	215	825

Nº de Adesão: 1234567 — 1234 5678 9012

Fonte: http://www.carelink.co.uk, http://en.wikipedia.org/ e http://www.bes.pt

3. Métodos biométricos como impressões digitais, *scan* da íris ou retina e análise da voz. A título ilustrativo, leia-se a seguinte notícia que demonstra a utilização da impressão digital num sistema de pagamento.

PAGUE COM UM DEDO

«*O BioPay é um sistema automático de débito através de impressão digital, único no mundo, desenvolvido para a Galp Energia pela BioGlobal em parceria com a Sagem.*

Parar o carro, encher o depósito e efectuar o pagamento com um simples toque do dedo. É isto que permite fazer o sistema BioPay da Galp Energia que, graças à sua originalidade, foi considerado uma das maiores inovações tecnológicas do ano 2004.

Trata-se da primeira experiência de pagamento biométrico de larga escala, estando já disponível em mais de 70 postos de abastecimento da gasolineira portuguesa, dispersos ao longo de todo o território nacional. E apesar da empresa ainda não ter apostado numa campanha de comunicação junto do público, a adesão a este serviço saldase já num enorme sucesso.

"As pessoas têm manifestado um grande interesse e aderido para além do que eram as nossas expectativas iniciais. As vantagens também são muitas. Basta referir que o cliente poupa 75% no tempo que antes demorava a abastecer o carro", referiu Pedro Nunes, responsável da Galp Energia, à Exame Informática.

E, ao contrário do que se poderia pensar, os automobilistas portugueses não têm mostrado reticências ou preocupação em introduzir as suas impressões digitais no sistema de controlo da gasolineira.

A BioGlobal foi a empresa portuguesa de biometria escolhida pela Galp Energia para proceder à implementação da solução, e o seu administrador Miguel Matos não hesitou em nos garantir que o BioPay respeita na totalidade a inviolabilidade dos dados biométricos que recolhe e gere. "O que acontece quando alguém disponibiliza o seu dedo para registo biométrico é a transformação imediata da imagem do dedo num *template* biométrico que não é mais que um algoritmo encriptado, impossível de duplicar ou de transformar numa imagem real tipo fotografia", refere. Ou seja, por outras palavras, não há o menor risco de apropriação ou uso indevido da impressão digital de ninguém. "Aliás, com a adesão a este sistema, até podemos dizer que a segurança do automobilista aumenta bastante porque deixa de haver necessidade de andar com cartões bancários ou com dinheiro nos bolsos. Basta o dedo", comenta ainda o mesmo responsável.»

Fonte: *Exame Informática* de Fevereiro de 2005 (http://exameinformatica.clix.pt/) (excerto)

AUTORIZAÇÃO

É a característica que assegura a protecção contra acções não autorizadas, garantindo, por exemplo, que apenas um número restrito de participantes pode desempenhar um determinado papel numa operação (como assinar um contrato ou gastar um determinado montante) ou que a entidade que está a realizar determinada tarefa pode efectivamente realizá-la.

REGISTO

É a propriedade que permite o arquivamento de determinadas operações, para análise *a posteriori*, de modo a saber quem fez o quê e quando, especialmente quando se detecta alguma anomalia no funcionamento de um certo serviço ou sistema. Por exemplo, numa época em que o cartão de crédito é cada vez mais utilizado em negócios electrónicos, é importante haver um registo de todas as transacções de forma que se alguém não autorizado fizer uso indevido de um cartão, a acção seja facilmente detectada.

NÃO-REPÚDIO

É a característica que consiste na protecção contra a negação da participação numa determinada operação. O acto de não-repúdio pode ser realizado em três fases distintas, nomeadamente:

1. Na criação, quando o autor de uma mensagem ou de um documento não pode negar a sua autoria e o seu envio, por exemplo, se o documento estiver assinado;
2. Na submissão, quando o autor de uma mensagem ou de um documento obtém uma prova do seu envio como, por exemplo, no correio registado;
3. Na recepção, quando o destinatário de uma mensagem não pode negar que a recebeu como, por exemplo, no correio registado com aviso de recepção.

TESTE OS SEUS CONHECIMENTOS

1. Descreva os principais ataques activos.
2. Diga o que entende por um ataque de repúdio.
3. Explique porque é importante a propriedade de registo de informação.
4. Considera possível garantir confidencialidade sem garantir integridade?
5. Explique quais são os meios para garantir a autenticação de uma identidade.

C A P Í T U L O 2

Suporte Criptográfico – Identificação e Autenticação

O B J E C T I V O S

- Introduzir as noções básicas de criptografia
- Expor os principais algoritmos para codificar/descodificar uma mensagem
- Demonstrar a importância da utilização de assinaturas e certificados digitais
- Apresentar os principais protocolos de segurança para a Internet

A criptografia (do grego kryptós*, que significa escondido, e* gráphein*, que significa escrever) é habitualmente entendida como a ciência que estuda os métodos e os algoritmos pelos quais um texto é transformado da sua forma original para uma forma ilegível a menos que seja conhecido um segredo (chave), que torna o texto fácil de ser lido pelo receptor desejado. No entanto, hoje em dia, a criptografia engloba muito mais do que apenas codificar e descodificar. A utilização da* Internet *e das tecnologias* World Wide Web *como meio para realizar negócios* online *ou vender e comprar produtos e serviços implica que os nossos* e-mails*, pagamentos com cartões de crédito, consultas de páginas ou quaisquer outras operações que queiramos fazer com alguma privacidade passem a estar sujeitos aos olhares e acções daqueles que com os conhecimentos adequados os saibam manusear.*

Este capítulo introduz os principais aspectos da criptografia moderna, nomeadamente algoritmos de codificação/descodificação, assinaturas digitais, certificados digitais, entidades certificadoras e protocolos de segurança que garantem que uma boa parte das acções que realizamos na Internet *são feitas no sossego da nossa privacidade.*

Noções Básicas de Criptografia

O objectivo principal da criptografia é garantir que a troca de informação entre dois intervenientes, um emissor e um receptor, satisfaz os requisitos de segurança, nomeadamente confidencialidade, integridade, autenticação e não-repúdio. Para assegurar confidencialidade na comunicação utilizam-se cifras.

Uma cifra é um algoritmo criptográfico, *i. e.*, uma função matemática injectiva[1] que efectua transformações entre o texto original e o texto codificado (cifrado) e vice-versa.

Habitualmente, não é utilizada uma função, mas uma família de funções indexadas por um parâmetro denominado *chave***.**

Na criptografia clássica, a manutenção em segredo dos detalhes de uma cifra garantia a sua segurança. Actualmente, o algoritmo é conhecido e a qualidade da cifra avalia-se pelo tempo que permanece infringível a ataques de *criptoanálise*.

A criptoanálise é o estudo de métodos para obter a informação contida num texto cifrado sem o conhecimento da chave.

Entre os métodos clássicos de criptoanálise encontram-se o da *força bruta* e o da *análise das frequências*. O primeiro consiste em testar todas as combinações possíveis de caracteres até encontrar a chave que permita a descodificação do texto cifrado. O segundo baseia-se no facto de, em algumas linguagens, certos caracteres (ou combinações deles) ocorrerem mais frequentemente.

ALGORITMOS DE CIFRA

Um algoritmo de cifra é essencialmente um conjunto de procedimentos (matemáticos) em que as técnicas criptográficas se baseiam. A chave de um algoritmo fornece a informação necessária para aplicar esses procedimentos de uma maneira única. Existem três tipos de chaves: *secretas*, *públicas* e *privadas*. No caso de a chave ser secreta, o algoritmo diz-se de *chave simétrica*. Caso contrário, diz-se de *chave assimétrica*.

ALGORITMOS DE CHAVE SIMÉTRICA

Quando se utiliza a mesma chave (secreta) para cifrar e decifrar uma mensagem, o algoritmo denomina-se *chave simétrica* (Figura 2.1).

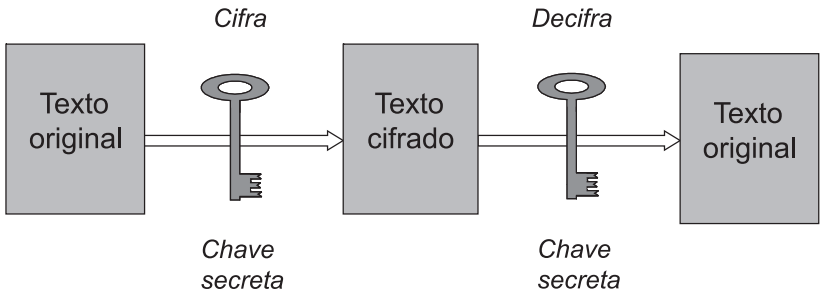


Figura 2.1
Esquema de um algoritmo de chave simétrica

COMO SE PROCESSA A COMUNICAÇÃO?

A comunicação que utiliza estes algoritmos pode ser descrita através dos seguintes passos:

1. O emissor e o receptor escolhem, em segredo, uma cifra e uma chave;
2. O emissor cifra a mensagem e envia-a ao receptor;
3. O receptor decifra a mensagem.

Na criptografia clássica, este tipo de algoritmos era frequentemente utilizado para proteger mensagens de significado militar. Dois dos exemplos mais básicos de técnicas que permitem transformar um texto original em texto codificado designam-se por *substituição* e *transposição*.

EXEMPLO 1 – CIFRA DE SUBSTITUIÇÃO

O algoritmo consiste em substituir cada letra de uma palavra por uma letra diferente de acordo com um esquema predefinido. O exemplo mais conhecido é a cifra de César ou ROTn em que uma letra é deslocada de um passo fixo (n). Consideremos os seguintes alfabetos:

Alfabeto normal:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Alfabeto para a cifragem (ROT3):	d e f g h i j k l m n o p q r s t u v w x y z a b c

Assim, a mensagem *Atacamos para a semana!* é cifrada para *dwdfdprv sdud d vhpdqd!*

EXEMPLO 2 – CIFRA DE TRANSPOSIÇÃO

O algoritmo consiste em «misturar» os conteúdos de uma mensagem utilizando uma chave secreta acordada entre o emissor e o receptor. Consideremos que a chave secreta é *gatos*. Assim, o algoritmo para transformar a mensagem *Atacamos para a semana!* é o seguinte:

1. Escrever a chave secreta e, por baixo, a ordem que apresenta no alfabeto:

g	a	t	o	s
2	1	5	3	4

2. Escrever a mensagem por baixo eliminando os espaços entre as palavras e a pontuação. Se necessário, preencher com letras no final para obter um número já fixado de caracteres na mensagem:

g	a	t	o	s		a	g	o	s	t
2	1	5	3	4		1	2	3	4	5
a	t	a	c	a	→	t	a	c	a	a
m	o	s	p	a		o	m	p	a	s
r	a	a	s	e		a	r	s	e	a
m	a	n	a	u		a	m	a	u	n

3. Ler cada uma das colunas na ordem previamente atribuída em 1. e escrever cada um dos caracteres:

toaa amrm cpsa aaeu asan

Note-se que os métodos da análise de frequências ou de força bruta podem ser facilmente utilizados para atacar estes dois tipos de cifras.

Na era moderna, a comunicação entre emissor e receptor não é feita pelo papel mas pelo computador, no qual a informação é sempre armazenada como uma sequência de dígitos binários. Um exemplo é o código ASCII *(American standard code for information interchange)*, que representa cada caracter (a, b, c, [...], A, B, C, [...], +, -, ?, [...]) através de oito dígitos binários (oito *bits*, que correspondem a um *byte*).

Consoante o seu modo de operação, os algoritmos de chave simétrica podem ser divididos em:

- *cifragem por blocos*;
- *cifragem por* streams.

A cifragem por blocos consiste em agrupar os *bits* de uma mensagem em blocos de tamanho fixo e em processá-los como uma unidade singular. Nos casos em que o tamanho do texto original não é múltiplo do tamanho pré-fixado, o último bloco é preenchido de acordo com uma regra preestabelecida *(padding)* (Figura 2.2).

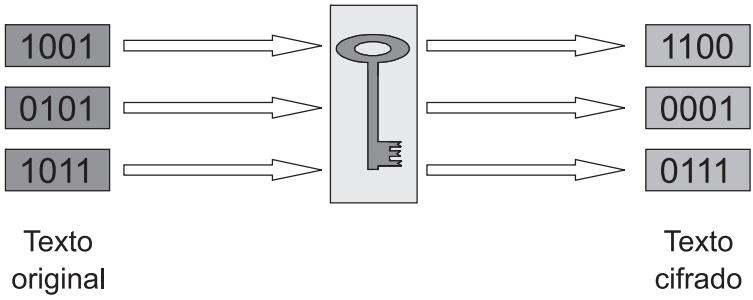


Figura 2.2 Esquema de um algoritmo de cifragem por blocos

A cifragem por *streams* consiste em processar um *bit* ou um *byte* de uma mensagem de cada vez, combinando-o com uma sequência de chaves gerada aleatoriamente (Figura 2.3). A chave da cifra funciona como estado inicial do gerador.

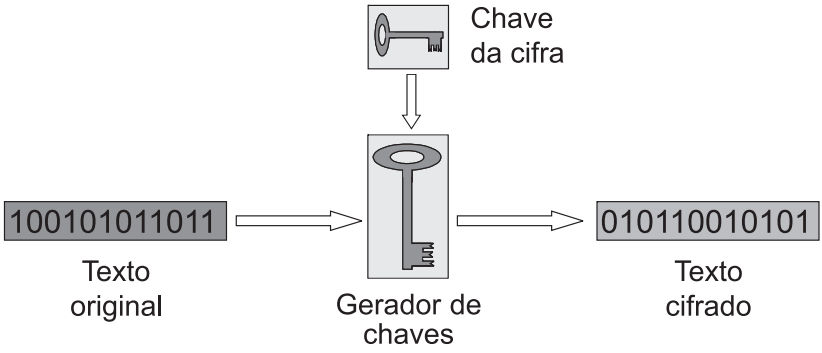


Figura 2.3 Esquema de um algoritmo de cifragem por *streams*

Cifragem por blocos *vs.* cifragem por *streams*

Geralmente, a cifragem por *streams* é executada a uma maior velocidade do que a cifragem por blocos e, além disso, necessita de *hardware* menos complexo. Todavia, ela pode conduzir a graves erros de segurança, em particular quando o estado inicial da chave é repetido em diferentes comunicações. Mesmo assim, a cifragem por *streams* deve ser preferida sempre que não se conheça, à partida, o tamanho do texto. No entanto, a cifragem por blocos também pode ser usada neste caso, mas então devemos escolher entre transmissões eficientes e complexidades acrescidas.

Distribuição de chaves secretas

O maior problema nos algoritmos de chave simétrica é a gestão eficiente das chaves, uma vez que elas têm de permanecer secretas antes, durante e depois de uma comunicação. Uma solução possível consiste em gerar e distribuir previamente as chaves secretas necessárias. No entanto, numa comunicação com N elementos, é necessário gerar, armazenar e proteger N(N-1)/2 chaves, uma para cada par de utilizadores. Uma forma de optimizar os recursos é atribuir a um dos elementos a responsabilidade pelo armazenamento de todas as chaves existentes e pela distribuição aos outros elementos, sempre que necessário. Em alternativa, pode ser utilizada uma *chave de sessão*, gerada em cada comunicação entre emissor e receptor, e imediatamente destruída após o seu fim. Contudo, persiste o problema da distribuição desse tipo de chaves.

O *protocolo de Diffie-Hellman* permite efectuar a troca de chaves secretas (que podem ou não ser de sessão) através de canais públicos e consiste nos passos seguintes:

1. O emissor e o receptor escolhem dois números primos, de grandes dimensões, p e $g<p$ (com algumas restrições que garantem a segurança do protocolo);
2. O emissor gera aleatoriamente um número $k_e<p$ e envia $E=g^{ke} \pmod{p}$ para o receptor;
3. O receptor gera aleatoriamente um número $k_r<p$ e envia $R=g^{kr} \pmod{p}$ para o emissor;
4. Ambos calculam $K=E^{kr} \pmod{p} = R^{ke} \pmod{p}$ que representa a chave.

Note-se que, mesmo sabendo os valores de p, g, E e R, distribuídos através de canais públicos, não é possível determinar K sem o conhecimento de k_e e/ou k_r. Este protocolo abriu o caminho aos algoritmos de chave assimétrica que serão descritos posteriormente.

EXEMPLOS DE ALGORITMOS DE CHAVE SIMÉTRICA

EXEMPLO 1 – DES *(DATA ENCRYPTION STANDARD)*

O DES é um algoritmo *standard* desenvolvido pela IBM na década de 70 e ainda muito utilizado em aplicações bancárias hoje em dia, como por exemplo na protecção do número PIN quando se levanta dinheiro numa caixa Multibanco. Utiliza uma chave de 56 *bits* que é aplicada a blocos de dados com 64 *bits*. Apesar de ser um algoritmo muito rápido, é considerado inseguro em inúmeras aplicações devido ao tamanho da chave ser pequeno. No entanto, existem vários métodos para aumentar a sua segurança, como a cifragem tripla, mais conhecida por 3DES.

EXEMPLO 2 – AES *(ADVANCED ENCRYPTION STANDARD)*

O AES, também conhecido por Rjindael devido à aglutinação dos nomes dos autores, Vincent Rijmen e Joan Daemen, é um algoritmo de cifragem por blocos que foi adoptado como padrão de criptografia pelo Governo dos Estados Unidos da América no final de 2001, após um concurso. Utiliza uma chave de tamanho variável, 128, 192 ou 256 *bits*, que é aplicada a blocos de dados com 128 *bits*. Espera-se que nos próximos anos seja mundialmente utilizado, como foi o caso do seu predecessor (DES).

A tabela seguinte ilustra a aplicação dos algoritmos DES e AES à codificação do texto original «Olá criptografia».

ALGORITMO	CHAVE (formato hexadecimal)	TEXTO CIFRADO (formato hexadecimal)
DES	0123456789abcdef	0be0d1610da4320bd44cc3a92b8c6b50
AES	0123456789abcdef0123456789abcdef	1eca9cd0bf35f0e4d4bd4bb79b77eb9a

Para tornar um texto cifrado, dado um texto original e uma chave arbitrária, utilizando os algoritmos DES e AES, aceda a http://www.cs.eku.edu/faculty/styer/460/Encrypt/JSDES.html e http://www.cs.eku.edu/faculty/styer/460/Encrypt/JS-AES.html, respectivamente.

ALGORITMOS DE CHAVE ASSIMÉTRICA

Quando se utilizam duas chaves complementares, uma pública e outra privada, para cifrar e decifrar uma mensagem, o algoritmo denomina-se *chave assimétrica* ou *chave pública* (Figura 2.4).

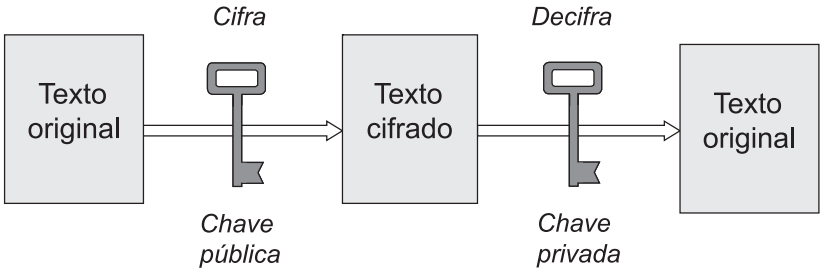


Figura 2.4
Esquema de um algoritmo de chave assimétrica

COMO SE PROCESSA A COMUNICAÇÃO?

A comunicação que utiliza estes algoritmos pode ser descrita através dos seguintes passos:

1. O emissor e o receptor escolhem uma cifra;
2. O receptor envia, em canal aberto, a sua chave pública;
3. O emissor cifra a mensagem com a chave pública do receptor e envia-a;
4. O receptor decifra a mensagem com a sua chave privada.

A criptografia de chave pública baseia-se nas funções *one-way* (de sentido único), *i. e*., funções muito simples de calcular mas praticamente impossíveis de inverter. Assim, utilizando estas funções, qualquer mensagem é muito fácil de cifrar mas difícil de decifrar. No entanto, a decifragem tem de ser possível por parte do receptor. Portanto, utiliza-se habitualmente uma subclasse das funções *one-way*, denominada função *one-way* com *trapdoor*, que permite a inversão desde que se conheça alguma informação adicional (segredo). A aplicação destas funções na criptografia é, então, feita da seguinte maneira: qualquer emissor pode cifrar a mensagem desde que conheça a função; apenas os receptores que possuam o segredo (chave) podem realizar a decifragem.

Algoritmos de chave simétrica *vs.* algoritmos de chave assimétrica

Os algoritmos de chave simétrica assemelham-se a um cofre em que apenas dois elementos possuem a chave. O emissor coloca a mensagem dentro do cofre. Posteriormente, o receptor retira-a. Os algoritmos de chave assimétrica também podem ser comparados a uma caixa do correio. Qualquer pessoa pode enviar uma mensagem para a caixa do correio desde que conheça a morada (chave pública). Só o dono da caixa do correio possui a chave (chave privada) que permite receber as mensagens.

Apesar das suas evidentes vantagens, os algoritmos de chave assimétrica não substituem os algoritmos de chave simétrica uma vez que

são muito mais ineficientes em termos computacionais. Por exemplo, se considerarmos dois algoritmos igualmente seguros, um de chave simétrica e outro de chave assimétrica, o de chave simétrica é pelo menos mil vezes mais rápido do que o de chave assimétrica. Assim, podemos considerar que os algoritmos de chave assimétrica são um complemento aos algoritmos de chave simétrica.

Envelopes digitais

Como foi referido anteriormente, o maior problema dos algoritmos de chave simétrica é a gestão eficiente das chaves secretas. Os algoritmos de chave assimétrica constituem uma alternativa ao protocolo de Diffie-Hellman e fornecem uma segurança adicional na distribuição de chaves secretas (de sessão) através de um sistema híbrido denominado *envelope digital* (Figura 2.5).

COMO SE PROCESSA A COMUNICAÇÃO?

A comunicação que utilize um envelope digital pode ser descrita através dos seguintes passos:

1. O emissor cifra o texto original com uma chave secreta (de sessão);
2. O emissor utiliza a chave pública do receptor, disponível por exemplo num servidor, para cifrar a chave secreta;
3. O receptor decifra a chave secreta utilizando a sua chave privada;
4. O receptor utiliza a chave secreta para obter o texto original.

No entanto, surge o problema de confirmar a autenticidade da chave pública. Esse problema será resolvido mais adiante recorrendo ao conceito de *certificados de chave pública (certificados digitais)*.

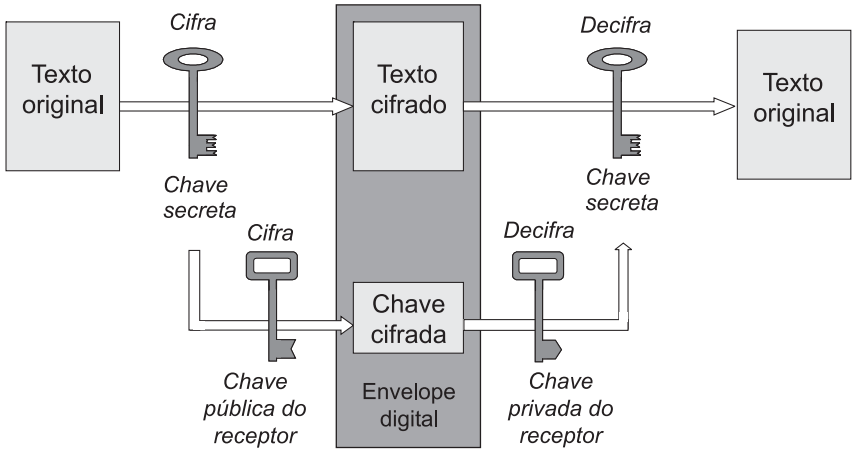


Figura 2.5
Esquema de um envelope digital

EXEMPLOS DE ALGORITMOS DE CHAVE ASSIMÉTRICA – RSA

O RSA é o algoritmo de chave assimétrica mais utilizado a nível mundial, sobretudo em protocolos de negócio electrónico. Foi desenvolvido na década de 70 nos Estados Unidos da América por Ronald Rivest, Adi Shamir e Len Adleman. A sua segurança baseia-se na dificuldade de factorizar computacionalmente um número primo de grandes dimensões. O algoritmo de geração das chaves é muito simples e consiste em:

1. Escolher dois números primos de grandes dimensões, p e q, em que $p \neq q$;
2. Calcular $n=pq$;
3. Escolher aleatoriamente um número que seja primo com $(p-1)(q-1)$;

Após a execução destes passos, as chaves públicas e privadas são constituídas pelos seguintes pares:

Chave pública: (n,e).
Chave privada: (n,d), onde $d=e^{-1}$ (mod $((p-1)(q-1))$.

No que diz respeito à cifragem e decifragem de uma mensagem m, as funções são realizadas pelas seguintes operações:

Cifragem: $c=m^e$ mod (n);
Decifragem: $m=c^d$ mod (n).

Consideremos o seguinte exemplo numérico. Seja

$$p=47,$$
$$q=71,$$
$$n=pq=3337,$$
$$e=79,$$
$$d=1019.$$

A cifragem de $m=688$ (texto original) corresponde a $c=688^{79}$ mod $(3337)=1570$. Facilmente se verifica que utilizando a função inversa, $m=1570^{1019}$ mod (3337), se obtém o texto original. Para um exemplo real aceda a http://en.wikibooks.org/wiki/Transwiki:Generate_a_keypair_using_OpenSSL. Existem outros algoritmos descritos na literatura, como Rabin, ElGamal, McEliece and Knapsacks. Para mais informações, consulte Menezes *et al.* (1996).

Algoritmos de Sumário

Os algoritmos de sumário, habitualmente denominados por *funções de Hash*, assumem um papel fundamental na criptografia moderna, por exemplo na produção de *assinaturas digitais* (ver ponto seguinte). O objectivo das funções de Hash é transformar univocamente a mensagem original (de tamanho variável) num sumário (impressão digital) de tamanho fixo. Uma vez que as funções de Hash não são invertíveis, é computacionalmente impraticável obter o texto original a partir do sumário. Contudo, é probabilisticamente possível que duas mensagens diferentes forneçam o mesmo sumário devido ao facto de as funções não serem injectivas.

É importante referir que, ao contrário dos algoritmos de cifra, cujo principal objectivo é assegurar a confidencialidade da mensagem, os algoritmos de sumário pretendem garantir a integridade.

COMO SE PROCESSA A COMUNICAÇÃO?

A comunicação que utilize estes algoritmos pode ser descrita através dos seguintes passos:

1. O emissor e o receptor escolhem uma função de Hash;
2. O emissor envia a mensagem em conjunto com o sumário;
3. O receptor calcula o seu próprio sumário e compara com o original. No caso de não serem iguais, comprova-se que a mensagem foi modificada em trânsito.

EXEMPLOS DE ALGORITMOS DE SUMÁRIO

EXEMPLO 1 – MD2, MD4 e MD5

O *Message Digest* 2, mais conhecido por MD2, é um algoritmo de sumário que foi desenvolvido por Ronald Rivest (um dos inventores do RSA) em 1989. No entanto, uma série de avanços na criptoanálise levou o autor a melhorá-lo, desenvolvendo em 1990 o MD4 e no ano seguinte o MD5. Em 1996, foi detectada uma debilidade no MD5 e os criptógrafos começaram a recomendar a utilização de outros algoritmos, como o SHA1 e o RIPE-MD. A classe de algoritmos MD produz sumários de 128 *bits* e tem sido amplamente utilizada para garantir a integridade dos ficheiros descarregados através da internet.

EXEMPLO 2 – SHA

A família de algoritmos SHA *(secure hash algoritm)* foi desenvolvida em conjunto pelas agências governamentais americanas NSA (National Security Agency) e NIST (National Institute of Standards and Technology) para incluir no *standard* de assinaturas digitais. O algoritmo mais conhecido, SHA-1, produz um sumário de 128 *bits* e é utilizado actualmente numa grande variedade de aplicações de segurança e protocolos, nomeadamente SSL *(secure sockets layer)*, TLS *(transport layer security)*, PGP *(pretty good privacy)*, etc., que veremos em detalhe mais adiante. Nos últimos dois anos foram divulgados alguns ataques ao SHA-1 que levaram a NIST a publicar quatro algoritmos adicionais, SHA-224, SHA-256, SHA-384 e SHA-512, que produzem sumários de 224, 256, 384 e 512 *bits*, respectivamente. Estes algoritmos são designados colectivamente por SHA-2.

EXEMPLO 3 – RIPE-MD

O RIPE-MD *(RACE integrity primitives evaluation message digest)* é um algoritmo de sumário que foi publicado por Hans Dobbertin, Antoon Bosse-

laers e Bart Preneel em 1996. É baseado no MD4 mas produz sumários de 160 *bits*. Existem outras versões deste algoritmo que produzem sumários de 128, 256 e 320 *bits*, denominadas RIPE-MD-128, RIPE-MD-256 e RIPE-MD-320, respectivamente.

A tabela seguinte ilustra a aplicação dos algoritmos DES e AES à codificação do texto original «Olá criptografia».

ALGORITMO	TEXTO CIFRADO (formato hexadecimal)
MD2	aff29c9af3f42b5318dd12498040bfe3
MD4	dacbeb0df8c255fb64af03f76da11f00
MD5	ccb3ddd9f19bf2026c34e44cc53b8652
SHA-1	4b285781b6934a250bde68d8f1ff73e4a403179e
SHA-224	166befe901626a461844cce286df68e25d8d55405cdb8d3b9934746d
RIPE-MD-128	f7df43a12e457d80f073ce49e96e771a

Para calcular o sumário de um texto arbitrário utilizando os algoritmos acima descritos aceda a http://serversniff.net/hash.php.

Assinatura Digital

A assinatura manuscrita é desde há muito tempo utilizada como prova da autoria ou, pelo menos, de concordância com o conteúdo de um documento. Infelizmente, nos meios tradicionais, assistimos cada vez mais à falsificação de assinaturas e à inserção de documentos não autorizados por entre os documentos originais. Uma assinatura digital é equivalente a uma assinatura manuscrita, mas proporciona geralmente garantias mais fortes, nomeadamente integridade, autenticidade e não-repúdio. Habitualmente, é aplicada a documentos electrónicos, *i. e.*, a qualquer tipo de ficheiros.

Os estados americanos Utah, Massachussets, Califórnia e Florida foram os primeiros a regulamentar, em 1996, a assinatura digital, conferindo-lhe o mesmo valor legal da assinatura manuscrita. Na Europa, Portugal foi um dos primeiros países, conjuntamente com a Alemanha e a Itália, a definir o enquadramento legal pelo Decreto-Lei n.º 290-A/99, de 2 de Agosto (*Diário da República* n.º 178, I série A).

COMO FUNCIONA UMA ASSINATURA DIGITAL?

Uma assinatura digital envolve os seguintes procedimentos (Figura 2.6):

1. O emissor assina o documento, *i. e.*, produz o seu sumário;

2. O emissor cifra o sumário com a sua chave privada e envia o documento conjuntamente com o sumário ao receptor;
3. O receptor decifra o sumário utilizando a chave pública do emissor;
4. O receptor verifica a assinatura calculando o sumário a partir do documento original e comparando-o com o sumário decifrado. No caso de serem iguais, verifica-se que a assinatura não é repudiável, *i. e.*, o emissor não pode negar, *a posteriori*, que enviou o documento porque só ele conhece a sua chave privada.

Mais uma vez convém notar que, para a assinatura digital ser segura, é necessário confirmar a autenticidade da chave pública do emissor, ou seja, é necessário um sistema de certificação das chaves públicas.

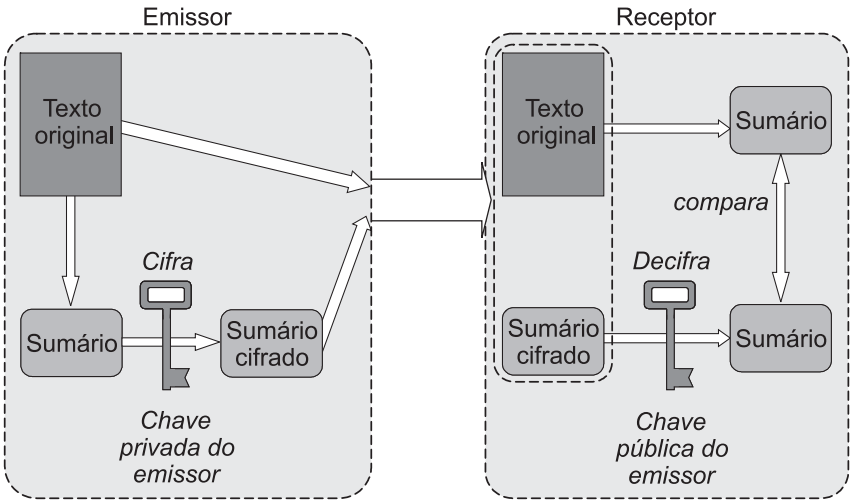


Figura 2.6
Esquema de uma assinatura digital

EXEMPLOS DE ASSINATURAS DIGITAIS

EXEMPLO 1 – RSA

A assinatura RSA é uma adaptação directa do algoritmo de chave assimétrica RSA e utiliza o algoritmo de sumário MD5. Os cálculos matemáticos são exactamente os mesmos, mas neste caso a cifragem é efectuada com a chave privada e a decifragem com a chave pública.

EXEMPLO 2 – DSA

O DSA *(digital signature algorithm)* é o *standard* de assinaturas digitais do Governo dos EUA que foi proposto pela agência americana NIST em 1991 e formalmente adoptado em 1993. A decisão causou imensa polémica, uma vez que

muitas aplicações já tinham sido desenvolvidas com base no RSA. Apesar de ser um algoritmo mais lento do que o RSA, o DSA não tem *royalties*. O DSA é baseado no algoritmo de chave assimétrica ElGamal e utiliza o algoritmo de sumário SHA-1.

Existem outros algoritmos de assinaturas digitais, como Schnorr e ElGamal. Para mais informações, consulte Schneier (1996).

Certificado Digital

Numa comunicação, os intervenientes devem poder ter a certeza de que cada vez que utilizam uma chave pública a entidade com quem pretendem trocar informação possui a chave privada associada. Essa confiança assenta nos certificados digitais.

Um *certificado digital* ou um *certificado de chave pública* é um conjunto de dados que identifica uma entidade, seja ela uma empresa, uma pessoa ou um computador e a respectiva chave pública.

Além da ligação entre a chave pública e o seu titular, o certificado digital fornece também uma ligação indirecta à correspondente chave privada, garantindo assim autenticidade e não-repúdio na comunicação. Para assegurar a veracidade dos dados contidos no certificado ele é assinado digitalmente por uma entidade em quem todos confiam (TTP). O formato mais utilizado para certificados digitais é definido pela norma X.509 da ITU (International Telecommunications Union). Um certificado é constituído por:

1. Versão do certificado – identifica a versão do certificado X.509 (v3 actualmente);
2. Número de série – identificador único do certificado emitido pela TTP;
3. Algoritmo da assinatura – identificação dos algoritmos utilizados pela TTP para a assinatura do certificado, por exemplo, o RSA como algoritmo de cifragem e o MD5 como algoritmo de sumário;
4. Emissor – identificação da TTP que emitiu e assinou o certificado;

5. Período de validade do certificado – intervalo de tempo durante o qual a TTP garante o conteúdo do certificado;
6. Identificação do titular – nome da entidade (empresa ou particular) titular (em casos especiais poderá ser anónimo) cuja chave pública o certificado identifica;
7. Chave pública – chave pública do titular do certificado e correspondente algoritmo utilizado;
8. Extensões – várias extensões ao certificado que permitem, entre outras coisas, restringir as utilizações do par de chaves associado, por exemplo, apenas para verificação de assinaturas digitais.

A Figura 2.7 apresenta um exemplo de um certificado digital.

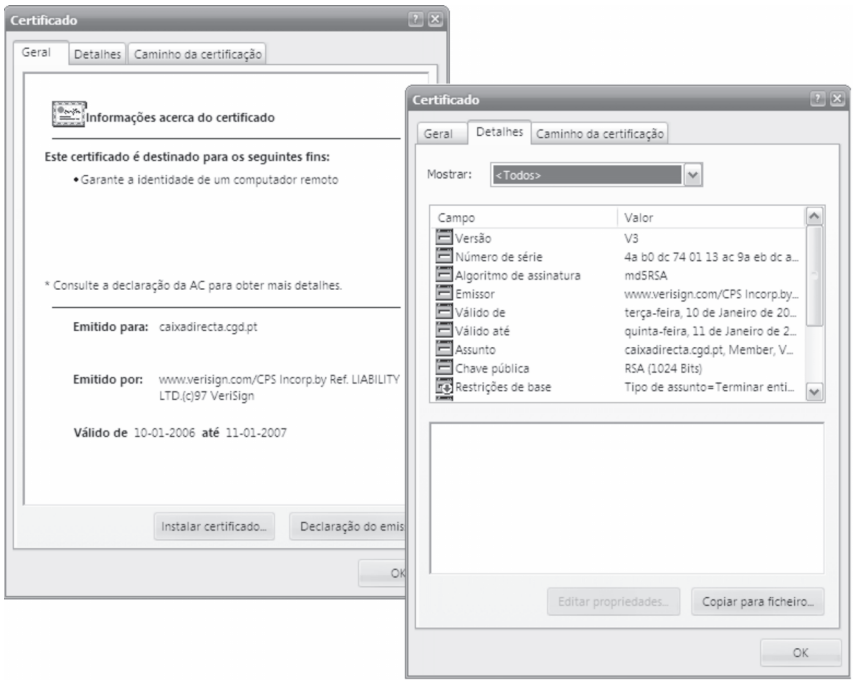


Figura 2.7
Exemplo de um certificado digital (Caixa Geral de Depósitos)

Embora um certificado tenha um período de validade predefinido, poderão surgir situações que obriguem a revogar um certificado, nomeadamente se a chave privada do titular for descoberta ou se algum dos dados identificativos do titular do certificado for alterado. A informação sobre certificados revogados pode ser obtida de duas maneiras: por *certificate revocation lists* (CRL) ou por uma consulta à TTP utilizando o OCSP *(online certificate status protocol)*. As CRL

são normalmente colocadas num local facilmente acessível, do conhecimento geral e disponível ao público denominado repositório. Alguns exemplos de repositório são:

- a directoria X.500;
- os servidores de LDAP *(lightweight directory acess protocol)*.

COMO FUNCIONA A VERIFICAÇÃO DE UMA ASSINATURA DIGITAL?

A verificação de uma assinatura digital envolve os seguintes passos:

1. O receptor do documento obtém o certificado digital do signatário;
2. O receptor do documento obtém o certificado digital da TTP que assinou o certificado do signatário. Em geral, o certificado da TTP está assinado pela própria;
3. O receptor valida a assinatura da TTP no certificado;
4. O receptor obtém a chave pública do signatário a partir do seu certificado;
5. O receptor valida a assinatura digital dos dados.

ENTIDADES CERTIFICADORAS

Uma entidade certificadora é responsável pela emissão e confirmação dos dados presentes num certificado digital. Mais ainda, a confiança que as entidades certificadoras oferecem é a base de um certificado digital. Existem vários factores que podem aumentar a confiança, nomeadamente a existência de:

1. Processos de verificação dos dados do certificado como, por exemplo, verificação presencial, com documento de identificação, *e-mail* ou procuração;
2. Entidades públicas como notários que possuem procedimentos normalizados para efectuar as verificações referidas em 1. Tradicionalmente, estas entidades gozam da confiança do grande público;
3. Empresas privadas que têm de respeitar normas de verificação e de segurança aprovadas pela legislação como a publicação de *Certification Practice Statements* (CPS), nas quais publicitam as suas normas de operação internas.

Em geral, a actividade de uma entidade certificadora é subdividida em duas componentes, uma *certification authority* (CA) e uma *registration authority* (RA).

Uma *certification authority* (CA) é uma entidade que cria ou fornece meios para a criação e verificação de assinaturas digitais, emite e gere o ciclo de vida dos certificados digitais e assegura a respectiva publicidade.

Uma *registration authority* (RA) é uma entidade que presta os serviços relativos à identificação/autenticação do detentor do certificado digital, à celebração de contratos de emissão de certificado digital e à gestão de certificados digitais que não se encontrem atribuídos em exclusivo à CA.

Normalmente, por razões de segurança como, por exemplo, a protecção da chave privada, a CA não está acessível a partir do exterior e só a RA pode comunicar com ela. Em algumas aplicações da Internet, como os *browsers* ou os leitores de *e-mail*, os certificados das CA são obtidos automaticamente. A Figura 2.8 apresenta algumas das CA pré-instaladas no *browser* do Internet Explorer.

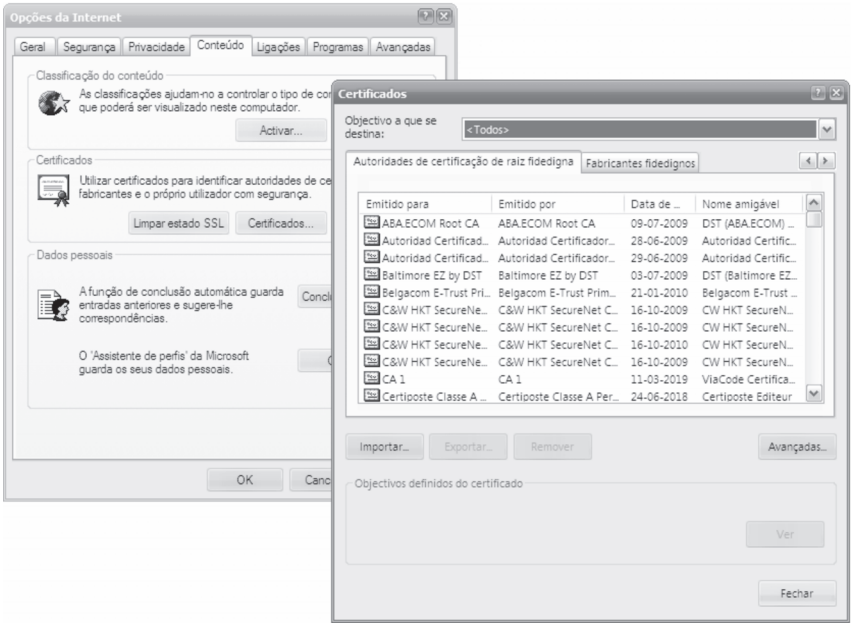


Figura 2.8
CA pré-instaladas no browser do Internet Explorer

Cadeias de certificação

Na utilização de um serviço que exija o conhecimento de uma chave pública, é necessário obter e validar o certificado que a contém. A validação do certificado implica, por sua vez, o conhecimento da chave pública da CA que o emitiu e, consequentemente, a obtenção e autenticação do seu certificado. No entanto, um utilizador pode não

ter hipótese de validar directamente o certificado da CA (por exemplo, se obteve a sua chave pública de forma insegura). Este problema pode ser resolvido se o certificado for assinado por outra CA cujo certificado seja bem conhecido pelo utilizador. Assim, forma-se uma *cadeia de certificação* em que uma CA atesta a veracidade do certificado de outra e assim sucessivamente. No topo encontra-se a *root* (raiz) CA, assim designada por agir como raiz de confiança para todos os elementos que se encontram abaixo dela. A Figura 2.9 ilustra um exemplo de uma *hierarquia* de CA.

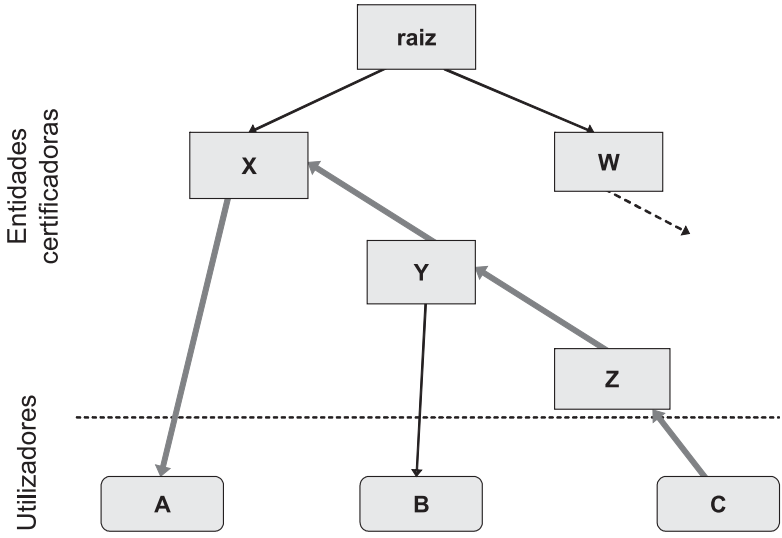


Figura 2.9
Hierarquia de *certification authorities* (CA)

Considerando este exemplo, se o utilizador C pretender verificar o certificado do utilizador A, apenas necessita de seguir a cadeia até encontrar a CA intermediária X, cujo certificado verificará o certificado desse utilizador. A Figura 2.10 apresenta um exemplo real de uma cadeia de certificação (SET – *secure electronic transaction*). O SET é um sistema que foi desenvolvido com o objectivo de solucionar o problema levantado pelos pagamentos com cartões de crédito em redes abertas como a Internet. Como se pode ver na Figura 2.10, no topo da hierarquia encontra-se a raiz CA, em que todos os intervenientes devem confiar. Essa autoridade certifica cada uma das marcas dos cartões de crédito, nomeadamente Visa, American Express e Mastercard, que, por sua vez, certificam CA nas diversas regiões do globo denominadas CA geopolíticas. Estas certificam CA que emitem certificados para os possuidores de cartões de crédito *(cardholders)*, comerciantes *(merchants)* e entidades que autorizam e processam os

pagamentos *(payment gateways)*. No Capítulo 4 serão dados mais detalhes sobre o SET.

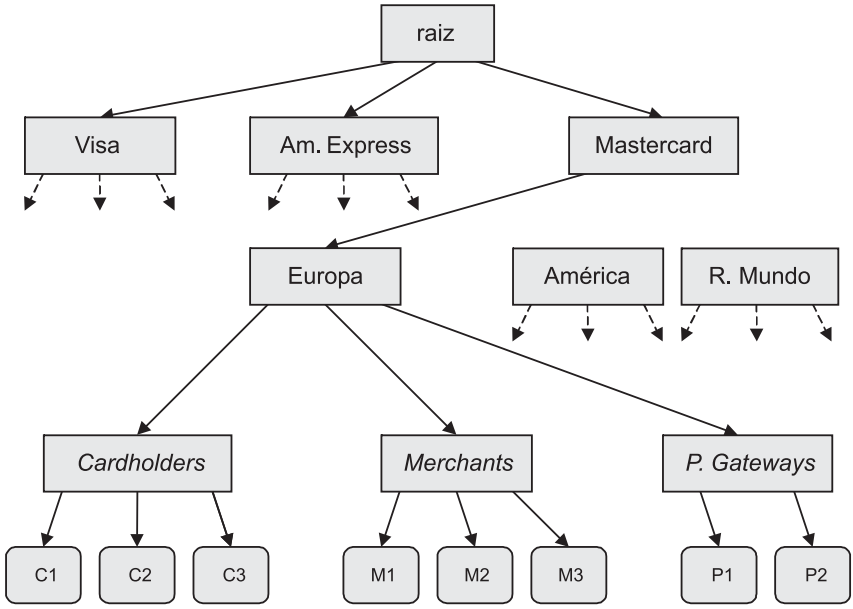


Figura 2.10
Cadeia de certificação do SET *(secure electronic transaction)*

Com o objectivo de desenvolver um ambiente seguro na comunicação em rede aberta, englobando todas as técnicas e todos os conceitos relacionados com a criptografia assimétrica ou de chave pública, foram criadas *infra-estruturas de chave pública* (PKI – *public key infrastructures*). As PKI reúnem um conjunto de *hardware*, *software*, utilizadores, políticas e procedimentos necessários para criar, gerir, armazenar, distribuir e revogar certificados de chave pública, nomeadamente:

- *certification* e *registration authorities*;
- *certification practice statements*;
- cadeias de certificação;
- repositórios de certificados digitais;
- *certificate revocation lists*;
- chaves públicas, privadas e secretas;
- algoritmos de cifra simétrica, assimétrica e de sumário.

A título ilustrativo, veja-se a seguinte notícia sobre a utilização de técnicas criptográficas.

ASSINATURA DIGITAL VAI PROMULGAR LEIS

«*Cavaco Silva, Presidente da República, José Sócrates, primeiro-ministro, e os ministros do seu Executivo vão passar a usar uma assinatura electrónica nos procedimentos legislativos, através de uma "rede segura de informática", adiantou ao CM fonte oficial da Presidência do Conselho de Ministros. O sistema chega mais tarde ao cidadão, por exemplo, através do cartão do cidadão e do passaporte electrónico português. O Governo investiu perto de 200 mil euros na criação do Sistema de Certificação Electrónica do Estado (SCEE), que dentro de duas semanas estará instalado num cofre-forte da Casa da Moeda.*

Segundo o Decreto-lei n.º 116-A/ /2006, publicado em *Diário da República* de 16 de Junho, "o SCEE constitui, assim, uma hierarquia de confiança que garante a segurança electrónica do Estado e a autenticação digital forte das transacções entre os vários serviços e organismos da Administração Pública e entre o Estado e os cidadãos e as empresas". Até agora, Portugal não dispunha de uma tecnologia informática deste tipo.

"O Governo quer dar o exemplo", disse a mesma fonte ministerial. E, por isso, vai começar por aplicar o SCEE a todos os intervenientes no processo legislativo. Ou seja, Cavaco Silva, José Sócrates, ministros e funcionários implicados na aprovação e publicação de leis recebem um cartão pessoal com *chip* e código *pin* (como o sistema dos cartões de telemóvel), que comporta ainda a sua assinatura, igual à manuscrita no bilhete de identidade. Por exemplo, "o Presidente da República poderá assinar um diploma através de uma assinatura certificada", explicou.

Mais tarde, o SCEE vai ser aplicado à Administração Pública, para desburocratizar serviços e permitir a circulação documental por via electrónica, de forma segura.

A partir de 1 Julho, os cidadãos poderão aceder ao *Diário da República* electrónico (em www.dre.pt) de forma gratuita, como um passo no sentido da desmaterialização legislativa.

A independência da Autoridade Nacional de Segurança vai garantir a certificação e fiscalização do sistema, aumentando ainda a confiança dos cidadãos e empresas nesta tecnologia. A Presidência do Conselho de Ministros frisa que o SCEE "não é um serviço de apoio informático" para a resolução de problemas nos computadores.

Cofre-Forte Fecha Sistema

A Casa da Moeda vai terminar em duas semanas a instalação do Sistema de Certificação Electrónica do Estado (SCEE). A sala onde vai ficar tanto o *software* como o *hardware* desta estrutura será uma espécie de cofre-forte, que garante a invulnerabilidade do SCEE. "A ideia é: como isto são chaves públicas e privadas, estão guardadas na Casa da Moeda com um sistema de alta segurança", explicou ao CM fonte da Presidência do Conselho de Ministros.

Por outro lado, o investimento não chegou aos 200 mil euros e nem "vai ter grande impacto na despesa pública", disse a mesma fonte.»

Fonte: *Correio da Manhã*,
18 de Junho de 2006
(http://www.correiomanha.pt)

Redes de confiança

Existe outro modelo de estabelecimento de certificados que não recorre a cadeias de certificação. Esse modelo é designado por *rede de confiança* e baseia-se em relações pessoais entre os vários utilizadores. No entanto, é um modelo pouco seguro porque as relações de confiança são informais e podem ser enganadoras. A Figura 2.11 apresenta um exemplo de estabelecimento de redes de confiança.

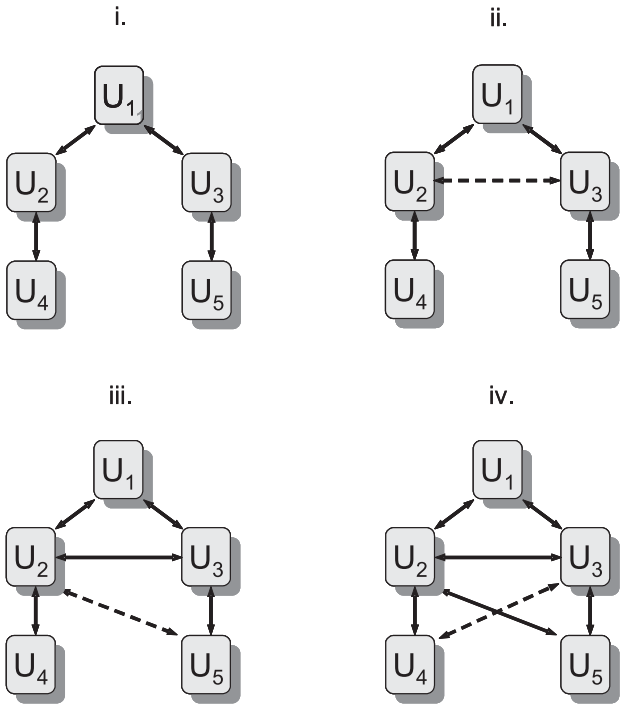


Figura 2.11
Estabelecimento de uma rede de confiança

Considerando este exemplo, suponhamos que os utilizadores U_2 e U_3, que não se conhecem, têm um amigo comum, U_1, em quem confiam. Assume-se por defeito que U_1 confia em U_2 e U_3. Se U_1 apresentar U_2 a U_3, este reconhece U_2, por confiar em U_1. Uma vez que U_3 conhece U_5, de seguida pode apresentar-lhe U_2. Assim, U_2 reconhece U_5 porque confia em U_3. Finalmente, U_3 aceita que U_2 lhe apresente U_4, por agora confiar em U_2.

Aplicando estes conceitos aos certificados digitais, um utilizador U_1 aceita o certificado de um utilizador U_2 se tiver sido assinado por outro utilizador U_3, em que confia. O PGP *(pretty good privacy)*, que veremos na próxima secção, é um exemplo de uma aplicação que recorre a um modelo de redes de confiança.

Aplicações da Criptografia – Segurança na Internet

A Internet e o comércio electrónico oferecem inúmeras possibilidades e oportunidades de negócio às empresas bem como conveniência para os consumidores. Contudo, o aumento das transacções electrónicas nesses canais abertos obriga à existência de ambientes fiáveis para a realização dessas operações de forma segura. Isto é possível com o auxílio da criptografia.

Pretty Good Privacy (PGP)

O PGP é uma aplicação que foi desenvolvida por Phil Zimmermann em 1991 com o objectivo de colocar à disposição do cidadão comum uma infra-estrutura de segurança da informação que garantisse simultaneamente:

1. Privacidade, mediante a utilização de algoritmos de compressão (ZIP) e algoritmos de cifra simétrica (3DES) e assimétrica (RSA e ElGamal) para protecção sobretudo de mensagens de *e-mail*. É de notar que os algoritmos de compressão são aplicados porque permitem poupar espaço e aumentar a segurança, escondendo padrões existentes no texto original;
2. Integridade e autenticação, através da utilização de algoritmos de sumário (MD5 e SHA-1) e assinaturas digitais (RSA e DSA) para a assinatura de mensagens e documentos;
3. Certificação, através de um modelo de redes de confiança para distribuição das chaves públicas.

O PGP teve uma grande aceitação por parte dos utilizadores, sobretudo por ser gratuito. No entanto, o seu autor teve problemas com a justiça americana, alegadamente por ter desrespeitado as leis que restringiam a difusão e utilização generalizada da criptografia. Devido ao modelo de redes de confiança utilizado pelo PGP, a comunidade técnica especializada não aconselha a sua utilização para fins comerciais.

Secure Sockets Layer (SSL)

O SSL é um protocolo de comunicação que foi desenvolvido pela Netscape para garantir integridade e confidencialidade na Internet. É utilizado para proteger ligações do tipo TELNET, FTP e HTTP e o seu

funcionamento baseia-se em sessões estabelecidas entre um cliente e um servidor. O SSL é basicamente constituído por dois subprotocolos:

1. SSL *handshake protocol*;
2. SSL *record protocol*.

O SSL *handshake protocol* é utilizado para definir os mecanismos de autenticação do servidor perante o cliente (e vice-versa, na versão 3.0), transmitir os certificados na norma X.509 e estabelecer as chaves de cifragem dos dados. Alguns dos detalhes do SSL *handshake protocol* estão ilustrados na Figura 2.12.

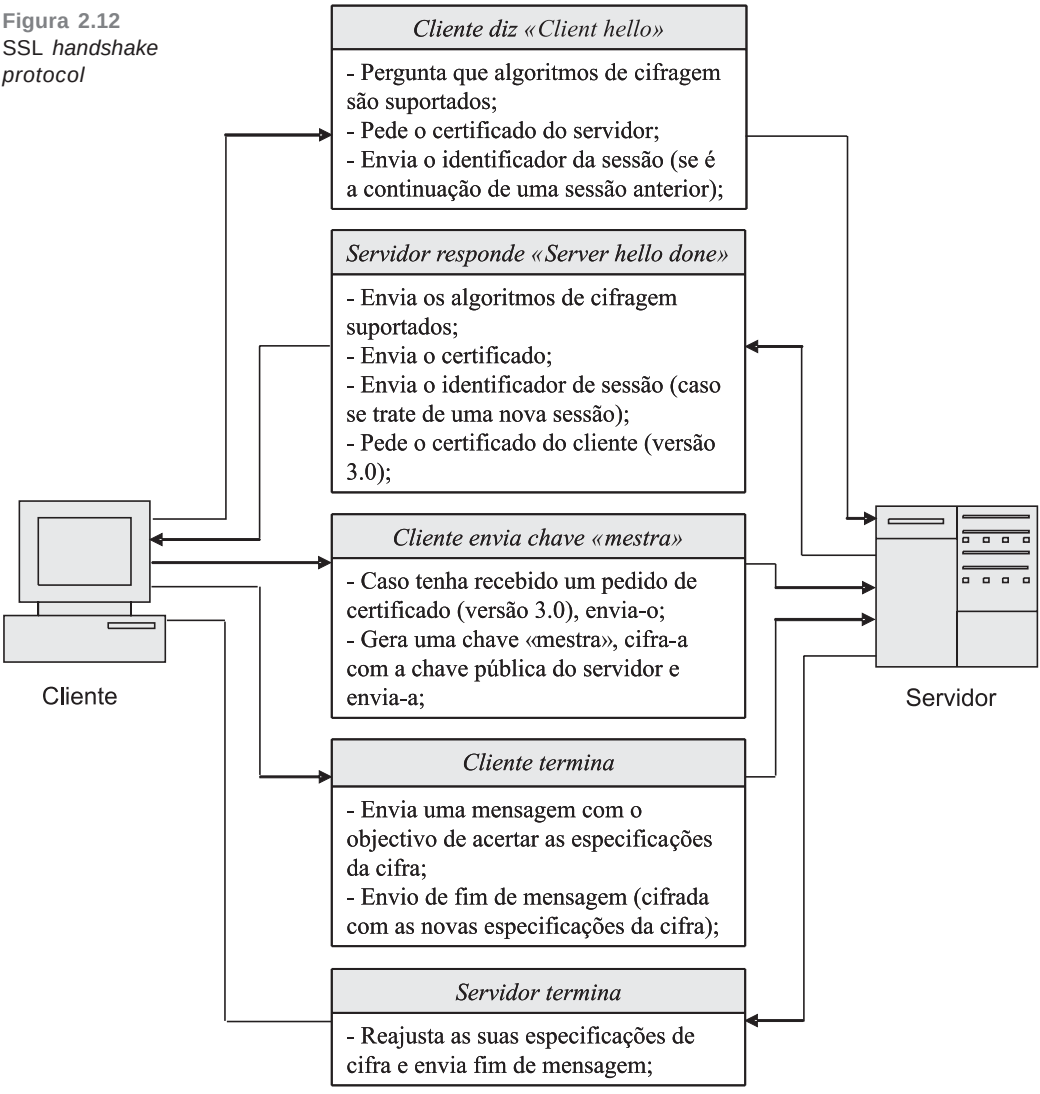


Figura 2.12
SSL *handshake protocol*

O SSL *record protocol* é utilizado durante as sessões de transferência de dados entre o cliente e o servidor. Mais ainda, é aqui que são definidos os formatos dos dados a serem transferidos e fornecidos os mecanismos para compressão, cifragem e verificação da integridade. Actualmente, os algoritmos e as assinaturas digitais que são suportados pelo SSL são:

- algoritmos de cifra simétrica: DES, 3DES, AES, etc.;
- algoritmos de cifra assimétrica: RSA;
- algoritmos de sumário: SHA1 e MD5;
- assinatura digital: RSA e DSA.

O SSL é normalmente identificado pelos *browsers* mais comuns através de um URL do tipo *https://* (Figura 2.13). Note-se que todo este protocolo é feito geralmente de forma automática pelo *browser*, sem o cliente se aperceber.

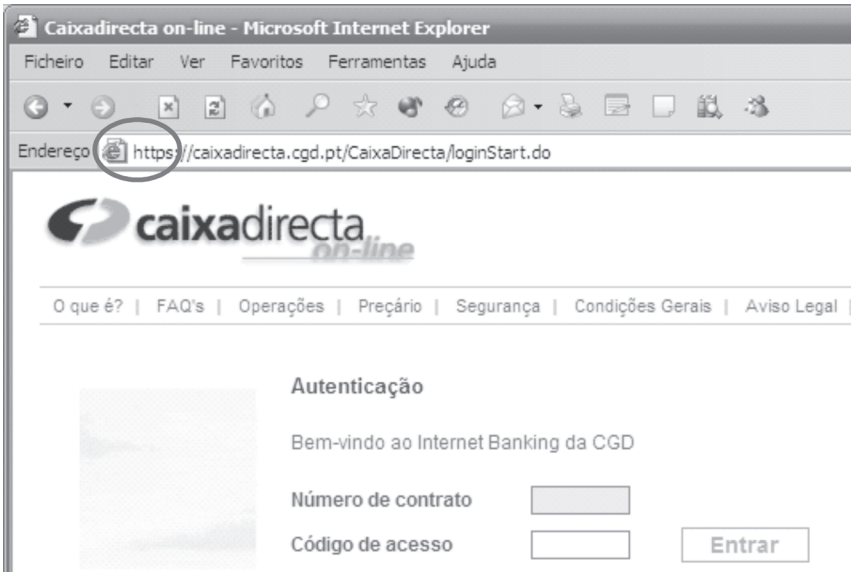


Figura 2.13
Exemplo de uma ligação *https://*

Apesar de o SSL *handshake protocol* incluir todos os mecanismos de segurança necessários para estabelecer uma ligação segura ao servidor, isso pode não ser suficiente. Consideremos o seguinte cenário: um cliente pretende fazer um pagamento referente a uma compra efectuada pela Internet. Para isso, envia o número do seu cartão de crédito através de uma ligação *https://*. Neste caso, a liga-

ção é segura mas o servidor não é necessariamente seguro, *i. e.*, se o número de cartão de crédito do cliente for armazenado sem cuidados adicionais numa base de dados, a informação pode ir parar às mãos daqueles que, com os conhecimentos adequados, os saibam manusear. Assim, devem-se utilizar procedimentos de segurança complementares, como *firewalls* (Capítulo 3).

TRANSPORT LAYER SECURITY (TLS)

O TLS é uma versão actualizada e melhorada do SSL. Do ponto de vista do utilizador não existem diferenças mas internamente foram realizadas melhorias em alguns algoritmos. No entanto foi introduzido um mecanismo de *fall-back* para SSL, em caso de necessidade.

Os algoritmos e as assinaturas digitais suportados pelo TLS são os mesmos do SSL com excepção da assinatura digital DSA que não foi incluída nesta versão. Assim, a grande vantagem do TLS em relação ao SSL reside no facto de o TLS ser completamente livre de patentes.

INTERNET PROTOCOL SECURITY (IPSEC)

O IP é o protocolo de transmissão de mensagens utilizado na Internet *(*versão v4). Este protocolo define uma norma para formatação de um conjunto de elementos (cabeçalho) que são anexados aos dados que se pretendem transmitir, formando pacotes. Dois dos elementos mais importantes do cabeçalho definem os endereços de origem e de destino dos pacotes. Uma das funções do IP é encaminhar os pacotes desde a origem até ao destino. No entanto, existem alguns ataques à segurança na Internet que se baseiam na violação deste princípio de funcionamento. Mais concretamente, certos utilizadores conseguem, por vezes, modificar os cabeçalhos alterando os endereços de origem ou destino. Esta técnica de autenticação de um computador hostil, fazendo-se passar por um computador autorizado, denomina-se por IP *spoofing*. Tendo em vista a resolução deste problema e o controlo de acessos, o grupo de trabalho IPSEC definiu dois mecanismos de segurança para o IP, nomeadamente:

1. *Authentication header*;
2. *Encapsulating security payload*.

O *authentication header*, como o próprio nome indica, providencia mecanismos para a autenticação de origem de pacotes. Para além

disso, inclui serviços de integridade dos seus conteúdos. O *encapsulating security payload* providencia confidencialidade dos pacotes, cifrando o seu conteúdo.

Um conceito-chave que aparece em ambos os mecanismos de autenticação e confidencialidade para o protocolo IP é a *associação de segurança*, que não é mais do que uma relação de sentido único entre um emissor e um receptor que descreve quais os mecanismos de segurança (algoritmos de cifragem) a utilizar para estabelecer uma comunicação segura. Estes algoritmos baseiam-se no *Internet key exchange*, que consiste num protocolo de Diffie-Hellman para troca de chaves secretas conjugado com um certificado de chave pública para autenticação.

Os mecanismos de segurança acima referidos são opcionais na versão IPv4 e obrigatórios na nova versão do IP, o IPv6. Naturalmente, à medida que a utilização do IPv6 se generalizar, estes mecanismos tornar-se-ão também correntes. Uma barreira de ordem não tecnológica ao maior emprego do IPSEC são as restrições à utilização da criptografia impostas pelos Estados Unidos da América e outros países.

REDE PRIVADA VIRTUAL

Uma rede privada virtual, normalmente conhecida por VPN *(virtual private network)*, é uma solução tecnológica que permite que duas ou mais redes privadas comuniquem de forma segura entre si utilizando uma rede pública como a Internet. Basicamente, uma VPN é construída utilizando protocolos de segurança como o IPSEC, que cifra todos os pacotes que são enviados para a Internet. Deste modo, se houver uma intercepção por um agente não autorizado, este não consegue ter acesso ao conteúdo do pacote.

Na actualidade, são inúmeras as empresas que adoptam esta solução com o objectivo de reduzirem os custos das infra-estruturas de comunicação e aumentarem a eficiência dos trabalhadores, permitindo-lhes o acesso remoto à rede da empresa através de uma VPN, com elevados níveis de segurança.

SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME)

O S/MIME foi desenvolvido por um grupo liderado pela RSA Security Inc. (fundada pelos criadores do algoritmo RSA) com o objectivo de adicionar assinaturas digitais ou chaves às mensagens de *e-mail*. A grande diferença em relação a outros sistemas do mesmo

género, como o MOSS (MIME *object security services*), é que as operações de assinatura e cifragem, baseadas em algoritmos e certificados de chave pública (formato X.509) podem ser aplicadas a partes de uma mensagem e não obrigatoriamente à sua totalidade. Hoje em dia, o S/MIME é o sistema mais utilizado comercialmente para protecção do correio electrónico.

TESTE OS SEUS CONHECIMENTOS

1. Sabendo que a chave secreta é «chaves», utilize a cifra de transposição para decifrar a seguinte mensagem: nudren cuccag eefssx oioame gsitax sdienx
2. Se tivesse de escolher entre algoritmos de cifra simétrica e assimétrica, qual escolheria? Justifique.
3. Explique qual o objectivo dos algoritmos de sumário (funções de Hash).
4. Indique as principais diferenças entre o *secure sockets layer* (SSL) e o *transport layer security* (TLS).

NOTAS

Pág. 18

[1] Uma função f: $A \rightarrow B$ diz-se injectiva se, quaisquer que sejam x, y pertencentes ao domínio da função (A), x é diferente de y implica que f(x) é diferente de f(y).

CAPÍTULO 3

Protecção de Dados do Utilizador e dos Sistemas

OBJECTIVOS

- Apresentar os principais sistemas para protecção de dados, nomeadamente *firewalls*, sistemas de detecção de intrusão e antivírus
- Descrever os ataques mais comuns contra sistemas: vírus, *worms* e cavalos de Tróia
- Demonstrar a importância da utilização de serviços de segurança adicionais, como filtragem de conteúdos, *backups* e monitorização remota

A crescente utilização da Internet e das tecnologias da World Wide Web como meio para realizar negócios electrónicos traz, naturalmente, um conjunto de preocupações relativas à protecção de dados dos utilizadores e dos sistemas. Mais ainda, a massificação da utilização da Internet implica o aumento do risco de ataques ao seu funcionamento, por exemplo, tentando sobrecarregar a rede ou usando-a como meio para cometer burlas informáticas. No entanto, os desenvolvimentos científico e tecnológico na área da segurança têm sido grandes, garantindo condições e níveis de confiança elevados em qualquer troca de informação realizada através da Internet.

Este capítulo introduz os principais sistemas para protecção dos dados nomeadamente firewalls*, sistemas de detecção de intrusão e antivírus e descreve algumas das ameaças à segurança mais comuns, como vírus, cavalos de Tróia e* worms.

Firewalls

Uma *firewall* é um sistema ou uma combinação de sistemas (*hardware* ou *software*) que assegura o cumprimento de políticas de controlo de acesso (segurança) entre duas ou mais redes.

Considere o seguinte exemplo, que explica de uma maneira muito simples o que é uma *firewall*: num determinado dia, um escritório de uma empresa recebe a visita de alguns directores de uma empresa concorrente. No entanto, a entrada no escritório só está autorizada a empregados ou clientes da empresa. Os visitantes obtiveram, excepcionalmente, autorizações por parte da administração. Assim, a empresa de segurança pode verificar as credenciais antes de os deixar entrar. Em alguns casos, é também necessário inspeccionar os empregados no sentido de verificar que nenhum transporta objectos que não são permitidos, por exemplo, álcool. Contudo, estas restrições não impedem os empregados de se relacionarem com pessoas fora do escritório. Mais ainda, é permitido aos empregados saírem do escritório, mas nem toda a gente está autorizada a entrar. A empresa de segurança ou qualquer outra entidade responsável por restringir ou controlar o acesso ao escritório da empresa pode portanto ser comparada a uma *firewall.*

Basicamente, no contexto de uma rede informática, uma *firewall* protege uma rede privada de acessos (ataques) vindos do exterior, por exemplo, da Internet, filtrando todo o tráfego que passa entre as duas (Figura 3.1). Para além disso, pode impedir que os computadores des-

sa rede privada comuniquem directamente com o exterior, bloqueando qualquer tentativa de acesso de computadores não autorizados.

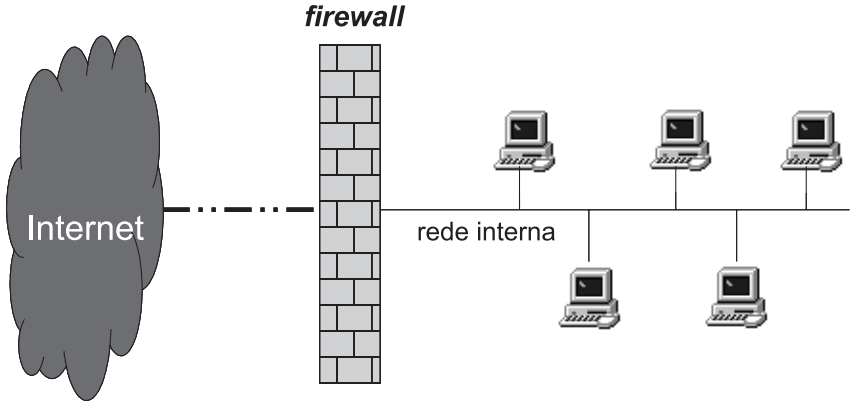


Figura 3.1
Esquema geral de uma *firewall*

Normalmente, uma *firewall* é implementada colocando um *router* (encaminhador) ou um computador (servidor *proxy*) entre a rede interna (privada) e a Internet.

Um *router* é um equipamento informático que tem a capacidade de encaminhar tráfego entre duas ou mais redes de um modo transparente. Actualmente, para além dessa tarefa, um *router* desempenha também funções de filtragem de tráfego entre as redes.

Um servidor *proxy* é um sistema que recebe e processa todos os pedidos relacionados com um determinado protocolo entre duas ou mais redes. Uma vez que todo o tráfego de um certo tipo passa através deste sistema, a sua utilização pode estar enquadrada numa política de controlo de acesso de uma rede privada.

Note que, apesar de uma *firewall* estar normalmente associada a uma ligação com a Internet, é vulgar hoje em dia instalarem-se *firewalls* também em *intranets*. Neste caso, algumas partes da rede interna estão resguardadas de outras componentes da mesma rede.

Geralmente, uma *firewall* faz a filtragem recorrendo ao endereço de origem do pacote IP (ver Capítulo 2). No entanto, uma *firewall* também pode efectuar esta operação com base nos seguintes elementos:

1. Endereço de destino ou combinação origem/destino;
2. Tipo de serviço, por exemplo, permitindo a passagem do tráfego relativo a um certo protocolo (HTTP) de e para um certo servidor.

Para além disso, uma *firewall* pode exercer outras funções como utilizar o IPSEC para:

1. Autenticação da origem dos acessos;
2. Protecção da confidencialidade dos dados, através da cifragem dos pacotes;

Note que este último ponto permite aplicar uma *firewall* à construção de uma rede privada virtual (ver Capítulo 2).

As *firewalls* podem ser classificadas com base nas suas funcionalidades em:

1. *Packet filtering* (filtragem de pacotes);
2. *Proxy application*;

PACKET FILTERING FIREWALLS

Packet filtering é a *firewall* mais básica em termos de segurança que opera na camada de rede do modelo TCP/IP (ver Anexo). Consiste em filtrar os pacotes IP de entrada, permitindo ou negando o acesso àqueles que não verificam as regras que normalmente estão definidas e programadas num *router* específico, denominado *router firewall* (Figura 3.2). Normalmente, o *router firewall* analisa cada pacote e a informação contida no seu cabeçalho, nomeadamente:

- a origem do pacote,
- o destino do pacote,
- o tipo de pacote,

de modo a decidir se o pacote deve ou não passar. Depois de o pacote ter sido analisado, o *router firewall* realiza uma das seguintes tarefas:

- aceita o pacote, o que significa que o deixa passar;
- rejeita o pacote, o que significa que não o deixa passar mas informa a origem do pacote da rejeição;
- nega o pacote, o que significa que o descarta completamente sem informar a origem da rejeição.

Para além destas três acções, o *router firewall* pode também registar a informação acerca dos pacotes e, se necessário, accionar um alarme quando a segurança tiver sido quebrada.

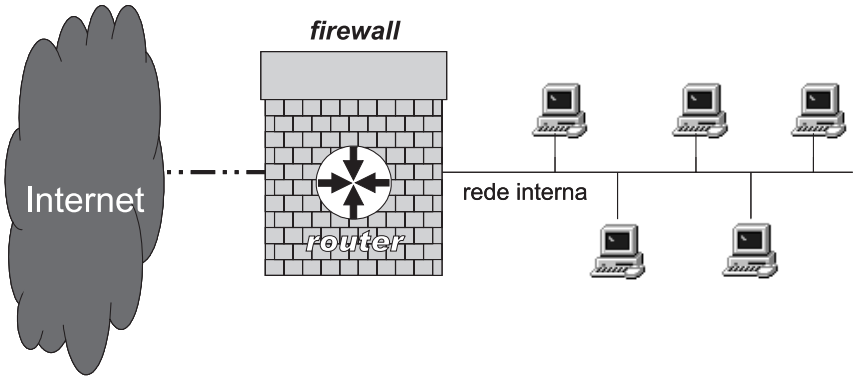


Figura 3.2
Esquema de uma *packet filtering firewall*

O processo de filtragem

Na *packet filtering*, a filtragem pode ser efectuada de três maneiras distintas:

1. *Simple packet filtering,* que bloqueia o acesso dos pacotes IP de todas as origens excepto aquelas que estão definidas na *router firewall*. Em alternativa, pode ser implementada uma estratégia em que todos os pacotes IP são aceites excepto os que provêm de determinadas fontes, por exemplo, de domínios não comerciais. Para além disso, a *router firewall* pode ser configurada de modo a restringir o acesso a determinadas aplicações, permitindo a comunicação apenas por uma determinada porta. Note que algumas das aplicações básicas da Internet, como as ligações HTTP e FTP, utilizam as portas TCP *(transmission control protocol)* 80 e 21, respectivamente;

2. *State tracking*, que permite apenas a entrada de pacotes que chegam em resposta a pacotes que foram enviados. Note que neste caso a operação de filtragem é mais complexa e obriga a uma análise completa de todo o tráfego que atravessa a *firewall*;

3. *Protocol-based filtering systems*, que permitem a entrada de pacotes que utilizam apenas um dos protocolos de transporte, nomeadamente TCP, UDP *(user datagram protocol)*, ICMP *(Internet control message protocol)*.

Vantagens e desvantagens da *packet filtering firewall*

A *packet filtering firewall* tem algumas vantagens, como a protecção da rede contra:

- *port scanning* – técnica que permite descobrir quais os serviços activos dos diversos dispositivos de rede, por exemplo, um servidor;
- *sniffing* – aplicação que escuta e armazena informação trocada na rede;
- *address-spoofing* – ataque que consiste em falsificar o endereço de origem dos pacotes IP, utilizando um endereço interno.

No entanto, a *packet filtering firewall* não consegue impedir ataques de roubos de *password* e de *session-hijacking* (consiste em tomar conta de uma ligação ou sessão existente, passando por cima da autenticação). Para além disso, o facto de não analisar o conteúdo dos pacotes e basear a decisão de aceitação apenas na informação contida nos cabeçalhos possibilita a transmissão para a rede privada de dados maliciosos como vírus e cavalos de Tróia, que analisaremos mais adiante. Assim, a *packet filtering firewall* por si só não representa um sistema de segurança eficaz e é habitualmente combinada com uma *proxy application*.

PROXY APPLICATION FIREWALLS

Uma *proxy application* é uma *firewall* criada a partir de um servidor *proxy* (Figura 3.3). Este servidor controla todo o fluxo de informação entre uma rede interna (privada) e uma rede externa (Internet), operando a nível da camada da aplicação do modelo TCP/IP (ver Anexo). Para além desta característica particular, o servidor *proxy* possui ainda outras características que o tornam apropriado para gerir esse fluxo, entre as quais:

- um servidor *proxy* é totalmente transparente, o que significa que nem as componentes da rede interna nem as da rede externa se apercebem da existência do serviço *proxy*;
- o servidor *proxy* é o único ponto de contacto entre os clientes da rede interna e a rede externa. A grande vantagem é que apenas o servidor *proxy* possui um endereço de IP válido, embora o administrador da rede possa atribuir endereços de IP a outras componentes da rede interna.
- o servidor *proxy* tem a capacidade de realizar a autenticação do cliente, permitindo apenas a alguns elementos da rede interna o acesso à Internet;

- o servidor *proxy* tem a capacidade de armazenar *(caching)* durante um certo período de tempo as páginas da Internet acedidas por um determinado utilizador da rede interna. Deste modo, se uma dessas páginas for solicitada por outro utilizador, o servidor *proxy* fornece a página armazenada, o que evita um novo acesso à Internet e consequentemente diminui o tráfego da rede.

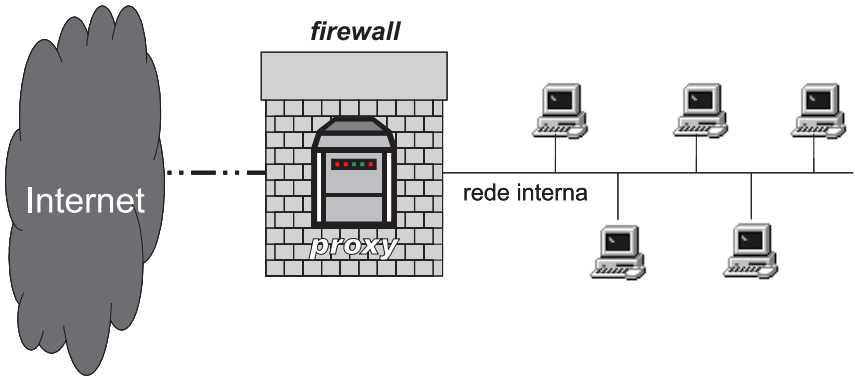


Figura 3.3
Esquema de uma *proxy application firewall*

Consideremos o seguinte exemplo, que ilustra o funcionamento de uma *proxy application firewall* para o protocolo de ligação HTTP: um pedido HTTP de um computador da rede interna é enviado para o servidor *proxy*, que o processa e reenvia para a rede externa, no caso de satisfazer as políticas de controlo de acesso (por exemplo, o bloqueio a certos domínios). Quando a resposta ao pedido é recebida pelo *proxy*, este examina o seu teor e encaminha o resultado para o respectivo computador se não encontrar conteúdo malicioso, como por exemplo certas aplicações Java ou ActiveX, que, se forem executadas, podem permitir a entrada de vírus e cavalos de Tróia.

Vantagens e desvantagens da *proxy application firewall*

Uma *proxy application firewall* tem algumas vantagens já referidas e que representam características do servidor *proxy*, como a capacidade de transparência e de autenticação. Para além disso, uma vez que opera a nível da camada de aplicação do modelo TCP/IP, o servidor *proxy* pode examinar e registar o conteúdo de cada aplicação mais detalhadamente, constituindo uma ajuda na análise do fluxo de informação entre as redes interna e externa. No entanto, cada servidor *proxy* é implementado apenas para uma aplicação da Internet, como, por exemplo, a ligação HTTP, uma vez que necessita de compreender todos os detalhes dessa aplicação para efectivamente poder controlar todo o flu-

xo de informação entre a rede interna e o exterior. Se for necessário outro tipo de ligação como uma FTP, então é preciso instalar outro servidor *proxy*, o que representa uma complexidade adicional.

Detecção de Intrusão

A detecção de intrusão é a arte de descobrir e responder a ataques contra, por exemplo, redes de computadores.

Tradicionalmente, os administradores de rede analisavam manualmente os registos emitidos por diversos sistemas de segurança como *firewalls* de modo a detectarem uma intrusão. Hoje em dia, o processo de análise do tráfego da rede para detecção de entradas não autorizadas é realizado por um *sistema de detecção de intrusão* (IDS – *intrusion detection system*). Como? Primeiro, o IDS examina e regista as actividades dos utilizadores da rede, os acessos aos discos rígidos, a utilização das memórias RAM e dos processadores dos computadores, etc., na procura de padrões de tráfego suspeitos ou anomalias no conteúdo do tráfego. De seguida, compara esses registos com uma base de dados de assinaturas de ataques, *i. e*., um repositório que contém padrões e comportamentos de ataques conhecidos, tal como no caso dos antivírus que veremos na secção seguinte. No caso de os registos coincidirem, o IDS reconhece a intrusão e acciona um alarme para avisar o administrador de rede e/ou tenta detê-la. Assim, o IDS permite detectar ameaças e avaliar os prejuízos numa rede tal como uma câmara de vídeo de segurança numa organização. A Figura 3.4 apresenta um esquema de um IDS.

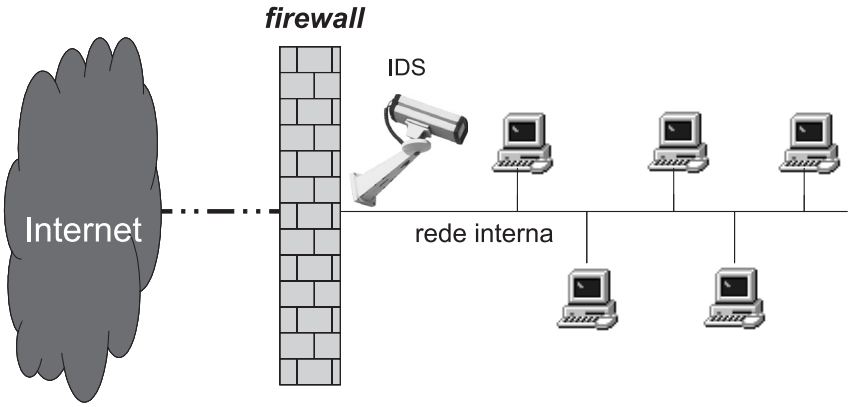


Figura 3.4 Esquema de um sistema de detecção de intrusão (IDS)

Em algumas situações, o IDS pode gerar erros, por exemplo, se não conseguir detectar uma intrusão ou um ataque ou mesmo se considerar uma actividade normal da rede como uma intrusão. Se isto acontecer, um erro como o primeiro é classificado como um falso negativo enquanto um erro como o segundo é classificado como um falso positivo (falso alarme). O objectivo de um IDS é impedir a ocorrência de falsos positivos e minimizar a ocorrência de falsos negativos.

IDS E *FIREWALLS*

As funções de um IDS e de uma *firewall* são habitualmente confundidas e a maioria das pessoas considera que uma *firewall* deve reconhecer um ataque e bloqueá-lo. Contudo, isto não é verdade. Uma *firewall* opera bloqueando todo o tráfego que não satisfaz algumas regras predefinidas pelo administrador de rede. Fazendo uma analogia com o mundo real, uma *firewall* é como uma cerca à volta da rede que tem algumas portas para permitir o acesso restrito. A cerca não tem a capacidade de detectar se alguém está a tentar forçar a entrada, por exemplo, escavando por debaixo dela, ou de verificar se quem está à porta tem autorização para entrar. Uma *firewall* simplesmente restringe o acesso em pontos pré-designados. Em síntese, uma *firewall* não é um sistema dinâmico que pressente a ocorrência de um ataque. Em contraste, um IDS é um sistema muito mais dinâmico, uma vez que tem a capacidade de detectar e reconhecer ataques contra a rede que a *firewall* foi incapaz de perceber. Considere o seguinte exemplo de uma intrusão: um empregado de uma empresa recebe um *e-mail* com um ficheiro (executável) em anexo. O empregado abre o *e-mail*, descarrega o anexo e executa-o, instalando também um cavalo de Tróia. Este abre uma ligação com o computador de um intruso através de um canal normal, por exemplo a porta 80, impedindo assim a sua detecção por parte da *firewall*. Isto deve-se ao facto de a *firewall* estar programada para bloquear o fluxo de informação de outras portas e para considerar natural o tráfego pela porta 80. Se a rede tiver um IDS instalado, qualquer actividade não habitual efectuada pelo cavalo de Tróia será facilmente detectada.

TÉCNICAS IDS

Um IDS baseia-se numa das seguintes técnicas para detectar uma intrusão:

- Detecção de anomalias;
- Detecção de má utilização do sistema;

Técnica de detecção de anomalias

A técnica de detecção de anomalias assenta na hipótese de todas as actividades que não sigam um padrão conhecido serem consideradas actividades anómalas. De modo a diferenciar entre actividades normais e anómalas, o IDS identifica, primeiramente, o perfil do normal funcionamento da rede e cria um valor de referência com base em estatísticas do número de acessos aos discos rígidos, da utilização das memórias RAM e dos processadores dos computadores. Posteriormente, o IDS examina o comportamento da rede e dos seus elementos e compara-o com o valor de referência previamente gerado. Se for observado um ligeiro desvio, o IDS acciona um alarme. Considere o seguinte exemplo, que ilustra esta técnica: a utilização do processador de um determinado computador de uma rede foi de 70% nos últimos 30 dias. No entanto, no dia de hoje, o processador está a ser utilizado a 100%. Para o IDS isto é considerado uma actividade anómala e, portanto, dispara um alarme.

Um IDS baseado nesta técnica tem, contudo, algumas desvantagens, nomeadamente o facto de qualquer pequeno desvio da actividade normal ser tratado como uma intrusão, o que pode aumentar o número de erros falsos positivos. Outra desvantagem desta técnica é o facto de não ter capacidade de identificar o motivo do evento anormal.

Técnica de detecção de má utilização do sistema

A técnica de detecção de má utilização do sistema baseia-se na representação de um ataque na forma de uma assinatura. O IDS mantém uma base de dados com todas as assinaturas de ataques conhecidos e um alarme é gerado quando a assinatura de um ataque coincide com uma assinatura da base de dados. A grande vantagem desta técnica é que a probabilidade de gerar um erro falso positivo é nula. Contudo, um IDS incorporado com esta técnica não consegue detectar ataques novos, ou seja, ataques cuja assinatura não esteja registada na base de dados.

TIPOS DE IDS

Os IDS baseados em técnicas de detecção de anomalias e de má utilização do sistema podem ser classificados, segundo o tipo de dados que analisam, como:

- IDS *network based*;
- IDS *host based*;
- IDS *hybrid*;

IDS *network based*

Um IDS *network based* é constituído por sensores (programas) que analisam os pacotes de dados que atravessam a rede e que são normalmente posicionados em pontos-chave, como por exemplo a seguir às *firewalls*, de modo a detectarem ataques com origem de fora da rede. A principal tarefa dos sensores é procurar padrões de má utilização do sistema, anomalias e, se os houver, enviar um alarme a uma autoridade central que controla toda a IDS, habitualmente designada por estação de comando.

Um IDS *network based* pode ser construído utilizando dois tipos de arquitecturas: tradicional e distribuída. Na arquitectura tradicional, os sensores são instalados em computadores dedicados e colocados em segmentos críticos da rede. Na arquitectura distribuída, cada computador da rede tem instalado um sensor que analisa os pacotes destinados apenas a esse computador, evitando a perda de pacotes especialmente em redes de alta velocidade.

IDS *host based*

Um IDS *host based* analisa os registos do sistema operativo de cada computador *(host)* de modo a detectar ataques com origem de dentro da rede. Esses registos contêm o historial de todas as acções realizadas pelo sistema, como acessos a ficheiros e execução de programas. Quando nota alguma actividade invulgar, o IDS *host based* envia um alarme a uma estação de comando. Um sistema deste tipo é muito eficaz para detectar má utilização da rede porque os dados analisados estão armazenados em cada um dos computadores dos utilizadores autenticados e qualquer comportamento fora do normal será facilmente descoberto.

Um IDS *host based* pode ser construído utilizando dois tipos de arquitecturas: central e distribuída. Na arquitectura central, todos os registos são enviados em tempos predefinidos e por um canal seguro para um computador dedicado que se encarrega de os examinar. Na arquitectura distribuída, cada computador analisa os próprios registos assim que é efectuada uma nova actividade. Assim, a principal vantagem da arquitectura distribuída em relação à arquitectura central é a geração de alarmes em tempo real. No entanto, o desempenho de cada computador da rede é mais afectado na arquitectura distribuída.

IDS *hybrid*

Conforme foi referido anteriormente, um IDS *network based* é eficiente na detecção de ataques com origem no exterior da rede, enquanto um IDS *host based* é forte quando o ataque é interno. Assim, um IDS *hybrid* combina o melhor das duas estratégias num único sistema, gerido apenas por uma estação de comando.

Vírus e Antivírus

VÍRUS

Um vírus informático é um programa que é introduzido num computador sem o conhecimento do utilizador, com a intenção de ser multiplicado e afectar a operação de outros programas ou do próprio computador.

O comportamento de um vírus de computador é semelhante ao de um vírus biológico, nomeadamente durante o processo de contaminação. Enquanto um vírus biológico utiliza as células vivas para se reproduzir, o vírus de computador serve-se de programas executáveis para se multiplicar por outras aplicações. Hoje em dia, no vocabulário comum, o termo vírus de computador é muitas vezes estendido para referir também *worms* (verme), *trojan horses* (cavalos de Tróia) e outros tipos de programas maliciosos que serão descritos mais adiante.

Os primeiros vírus de computador surgiram na década de 80 e, desde então, esse número tem aumentado exponencialmente. A Figura 3.5 ilustra o número de vírus conhecidos no período entre 1990 e 2005.

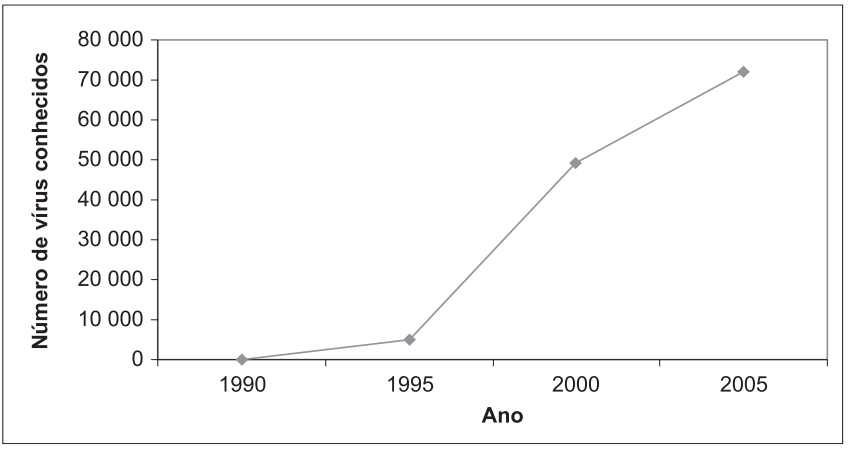


Figura 3.5
Número de vírus conhecidos no período entre 1990 e 2005

Os principais motivos para a criação de um vírus por parte de um *hacker* (pirata informático) são vandalismo, distribuição de mensagens políticas, ataque a produtos de empresas específicas e roubo de *passwords* para proveito financeiro próprio. No passado, os vírus disseminavam-se pelos computadores por meio de dispositivos como disquetes. No entanto, hoje em dia, com a massificação da utilização de redes como a Internet, os vírus propagam-se facilmente através de mensagens de *e-mail* e ficheiros que se descarregam. Os efeitos negativos de um vírus de computador podem variar desde a realização de operações mais ou menos inofensivas, como uma simples exibição no monitor de uma mensagem irritante, até à destruição de ficheiros do sistema ou formatação do disco rígido. A título ilustrativo, veja-se a seguinte notícia sobre os efeitos de um *worm*.

VÍRUS INFORMÁTICO ATACOU *MEDIA* NOS EUA

«*Um vírus informático atacou na noite de terça-feira sistemas que operam com Windows 2000 em órgãos de informação norte-americanos, incluindo as cadeias de televisão CNN e ABC, a agência AP e o jornal* New York Times.

Os problemas na CNN e no jornal nova-iorquino resolveram-se em 90 minutos e a suas operações não foram afectadas, segundo fontes oficiais.

O vírus, do tipo "verme", também desligou computadores no Congresso, actualmente no período de férias parlamentares, e causou problemas na agência noticiosa Associated Press e na fábrica de maquinaria agrícola Caterpillar, no Illinois.

Fonte do FBI disse que os problemas surgidos nos sistemas informáticos dos EUA não pareciam fazer parte de um ataque concertado ou generalizado.

A CNN, segundo a qual a infecção informática se propagou à Alemanha e a alguns países asiáticos, referiu que os seus computadores começaram a falhar tanto em Nova Iorque como em Atlanta a partir das 23:00 TMG (00:00 em Lisboa).

Um perito citado por esta cadeia de televisão por cabo disse que o ataque se deveu a um "verme" informático já em várias versões como "Rbot.ebq", Rbot.cbq, SDBot.bzh e Zotob.d. Ao serem atacados, acrescentou, os computadores ligam-se e desligam-se repetidamente.

A origem do problema, de acordo com fontes de empresas de segurança informática, estará no vírus "zotob", cuja existência foi denunciada segunda-feira, que atacaria principalmente o sistema Windows 2000.

Segundo a empresa norte-americana de software Symantec, autora do antivírus Norton, o vírus em causa tem risco "médio" e aproveita falhas de segurança já detectadas pela Microsoft nos sistemas Windows 95, 98, ME, NT, 2000 e XP.»

Fonte: *Diário Digital*/Lusa,
17 de Agosto de 2005
(http://diariodigital.sapo.pt/)

Meios de propagação

Os meios mais comuns pelos quais os vírus se propagam podem ser divididos em três categorias:

- Disquetes e CD;
- Ficheiros descarregados da Internet;
- Mensagens de *e-mail*.

Disquetes e CD

Tradicionalmente, as disquetes eram o meio de transporte mais comum para os vírus. As situações mais graves ocorriam quando o sector de arranque *(boot)* da disquete estava infectado e esta era utilizada para iniciar o sistema operativo. Neste caso, o sector de arranque do disco rígido ficava também infectado e os ficheiros do sistema operativo eram corrompidos, impedindo o normal funcionamento do computador. Contudo, actualmente, a maioria dos sistemas operativos não permite o arranque do sistema através de uma disquete.

Hoje em dia, CD e outros dispositivos como os *zip* e as *pen drives* podem transmitir vírus se algum dos ficheiros armazenados estiver infectado.

Ficheiros descarregados da Internet

Um vírus também pode ser transferido para o computador através da grande quantidade de *freeware*[1]*, shareware*[2]*, software*, jogos, imagens e ficheiros MP3 disponíveis na Internet. Se um ficheiro corrompido for descarregado, o computador também ficará infectado e, se esse ficheiro for partilhado com outros utilizadores, o vírus poderá rapidamente disseminar-se por toda a rede.

Mensagens de *e-mail*

O *e-mail* é outro meio muito popular de propagar vírus pela Internet. Neste caso, o vírus é enviado através de uma mensagem ou de um ficheiro em anexo. Quando o receptor lê a mensagem ou abre o ficheiro infectado, o vírus é activado e multiplica-se através de várias cópias executáveis. Pode eventualmente enviar, de forma automática, mensagens com essas cópias a todos os contactos da lista de endereços do utilizador, sem que este se aperceba. Os contactos, ao recebe-

rem uma mensagem de alguém conhecido não desconfiam que o anexo está infectado e, desta maneira, o vírus espalha-se rapidamente por toda a rede. Segundo um estudo da International Computer Security Association, cerca de 80% dos vírus entram nos computadores por este meio.

Tipos de vírus

Os vírus podem ser classificados, segundo o ambiente (aplicação ou sistema operativo) requerido para infectar ficheiros no sistema, em:

1. Vírus do sistema de ficheiros;
2. Vírus do sector de arranque;
3. Vírus de *macro*;
4. Vírus de *script*.

Os primeiros propagam-se pelo sistema de ficheiros do sistema operativo e podem ser divididos nas seguintes categorias:

- Vírus que infectam ficheiros executáveis, modificando o seu conteúdo;
- Vírus *companion,* que criam duplicados dos ficheiros infectados, atribuindo o mesmo nome mas com uma extensão diferente, de modo a que o utilizador execute o vírus da próxima vez que aceder ao ficheiro infectado;
- Vírus que criam cópias de si próprios em vários directórios;
- Vírus *link*, que utilizam as características do sistema de ficheiros para alterar a estrutura dos directórios de modo a redireccionar a entrada do directório que contém o ficheiro infectado para a área que contém o código do vírus.

Os vírus do sector de arranque, como o nome indica, infectam a área do disco rígido que é lida quando o sistema operativo está a ser iniciado, substituindo e modificando ficheiros do sistema operativo. Estes vírus eram amplamente propagados através das disquetes, mas, com o declínio da utilização desses dispositivos e com a introdução de processadores com 32 *bits*, quase desapareceram.

As *macros* são pequenos programas (comuns em ficheiros do Office) que são automaticamente executados sempre que é aberto o ficheiro a que estão anexadas. Os vírus *macro* utilizam esses ficheiros

para se propagarem. Em geral, são projectados para inserir caracteres, palavras ou frases nesses documentos, pelo que são consideradas ameaças mínimas. Todavia, propagam-se muito rapidamente pois os utilizadores partilham com frequência ficheiros de dados/texto e não pensam que eles possam ser infectados.

Um *script* é um conjunto de comandos, escritos, por exemplo, em JavaScript ou Visual Basic Script, que podem ser executados sem a participação do utilizador. Podem infectar ficheiros com vários formatos (HTML, por exemplo) e outros *scripts*, como comandos Windows ou Linux. Propagam-se através de aplicações ActiveX quando se descarregam componentes nas páginas da Internet.

Os tipos de vírus enumerados anteriormente podem ainda ser classificados, de acordo com as técnicas que utilizam para infectar os ficheiros, em:

- Vírus de reescrita;
- Vírus parasitas;
- Vírus *companion*;
- Vírus *link*.

No primeiro caso, o vírus substitui o conteúdo do ficheiro infectado pelo seu próprio conteúdo, apagando o original. Desta maneira, os ficheiros tornam-se inúteis e não podem ser recuperados. Os vírus parasitas modificam o conteúdo do ficheiro infectado, em geral um ficheiro executável, acrescentando o próprio conteúdo no início, no fim ou no meio do ficheiro infectado, podendo este ficar parcial ou totalmente danificado.

Todos estes tipos de vírus podem ainda possuir outras características como:

- polimorfismo – o código do vírus altera-se constantemente;
- invisibilidade *(stealth)* – o vírus pode «esconder-se» na memória do computador para não ser detectado;
- encriptação – o código do vírus está codificado.

Outras ameaças

Existem ainda outros programas maliciosos e ameaças que, apesar de não serem vírus, representam também perigo para a segurança do computador:

- *Worm* – programa que se propaga de computador para computador geralmente muito rapidamente, mas que não afecta outros programas. O principal prejuízo causado por um *worm* é a perda de capacidade de processamento do computador;
- *Trojan horse* – programa malicioso que tenta geralmente passar despercebido. O principal objectivo de um *trojan horse* é retirar informação privada de um computador, como, por exemplo, *passwords* de acesso a contas bancárias. Contudo, ao contrário de um vírus, um *trojan horse* não se multiplica;
- *Logic bomb* – programa que é inserido no sistema operativo ou em certas aplicações de modo a «explodir» quando um determinado evento ocorre, por exemplo, um dia da semana ou uma data em particular. Uma vez detonada, a bomba pode alterar ou apagar ficheiros ou até bloquear o computador;
- *Spyware* – programa que permanece escondido no sistema para monitorizar as acções do utilizador e recolher informação confidencial, como *passwords*, registos dos sistemas e outros ficheiros, enviando estes dados para uma entidade externa na Internet;
- *Keylogger* – pequena aplicação que tem como objectivo capturar tudo o que é digitado através do teclado, especialmente números de cartões de crédito e *passwords*;
- *Hijacker* – programa que altera a página inicial do *browser*, impedindo o utilizador de a modificar e de aceder a outras páginas, enquanto é apresentada publicidade;
- *Adware* – programa que exibe publicidade não desejada, frequentemente em janelas novas *(pop-ups)*, e que podem redireccionar a página de pesquisa apenas para endereços comerciais;
- *Phishing* – tipo de fraude electrónica, através de uma mensagem de *e-mail*, que consiste em enganar uma pessoa induzindo-a a revelar informação sensível ou confidencial como *passwords* e números de cartões de crédito. Habitualmente, as mensagens parecem ser de entidades ou pessoas fiáveis, com quem a vítima realiza negócios (bancos e seguradoras). Em geral, é pedido que se faça uma actualização ou validação da respectiva informação numa página que parece ser legítima, mas que

na verdade é uma «cópia» falsificada e cujo propósito é que a vítima divulgue informação pessoal que possa ser utilizada para roubo de identidade ou de dinheiro, para monitorização do computador ou para cometer burlas em nome da vítima. No entanto, é frequente encontrar erros grosseiros ou expressões pouco comuns na redacção destes *e-mails*, que facilmente excluem a hipótese de se estar perante uma comunicação autêntica. A título ilustrativo, veja-se o seguinte exemplo de *phishing* aos utilizadores da Caixa Directa *online*;

«Estimado(a) Cliente,

Com o intuito de melhor o servir, o Caixa Geral de Depositos vem transmitir-lhe que está a proceder á verificação e actualização dos dados do cliente. Com vista a este fim, somos a pedir-lhe que verifique e actualize os seus dados. Para sua maior comodidade poderá fazê-lo através do endereço abaixo mencionado.

https://caixadirecta.cgd.pt/CaixaDirecta/loginStart.do

O cliente dispõe de 5 dias úteis para proceder á actualização de dados. Sendo que não o faça poderá ver o seu acesso restringido. O correcto preenchimento desta informação é fundamental para que as suas operações se façam sem prejuízo, para si.

Caso não seja cliente, ainda, poderá fazê-lo através deste endereço:

https://caixadirecta.cgd.pt/CaixaDirecta/signupStart.do

Gratos pela sua preferência, apresentamos os nossos melhores cumprimentos.

Por favor Não responda A Este Email Porque Você Não receberá Uma Resposta*

Fonte: Caixa Geral de Depósitos

- S*pam* – são mensagens de *e-mail* anónimas, não solicitadas e enviadas maciçamente. Normalmente o *spam* tem fins publicitários, no entanto, o termo também engloba certas mensagens políticas, apelos à caridade, fraudes financeiras *(phishing)* e mensagens que servem para propagar vírus e outros programas maliciosos;
- *Hoax* – mensagem de *e-mail* que avisa as pessoas da falsa existência de perigosos vírus, sugerindo que a mensagem seja distribuída a todos os contactos.

ANTIVÍRUS

Um antivírus é um programa destinado a bloquear a acção dos vírus, analisando os dados que passam pela memória do computador ou o conteúdo dos ficheiros.

O antivírus é uma peça fundamental no combate aos cavalos de Tróia, *worms* e outros programas maliciosos que podem infectar um computador. Normalmente, um antivírus disponibiliza duas técnicas para combater os vírus:

- Protecção em tempo real dos ficheiros, o que significa que o antivírus está permanentemente activo em memória analisando todos os ficheiros que são acedidos, criados ou modificados pelo utilizador ou pelo sistema operativo;
- Análise solicitada ou programada pelo utilizador a determinados ficheiros, pastas ou discos com o objectivo de detectar vírus conhecidos, ou seja, vírus cuja assinatura exista na base de dados (Figura 3.6). A principal desvantagem dessa técnica é o aparecimento diário de novos vírus, o que obriga a manter essa base de dados sempre actualizada. Contudo, a maioria dos antivírus permite a actualização automática da base de dados quando o computador está ligado à Internet.

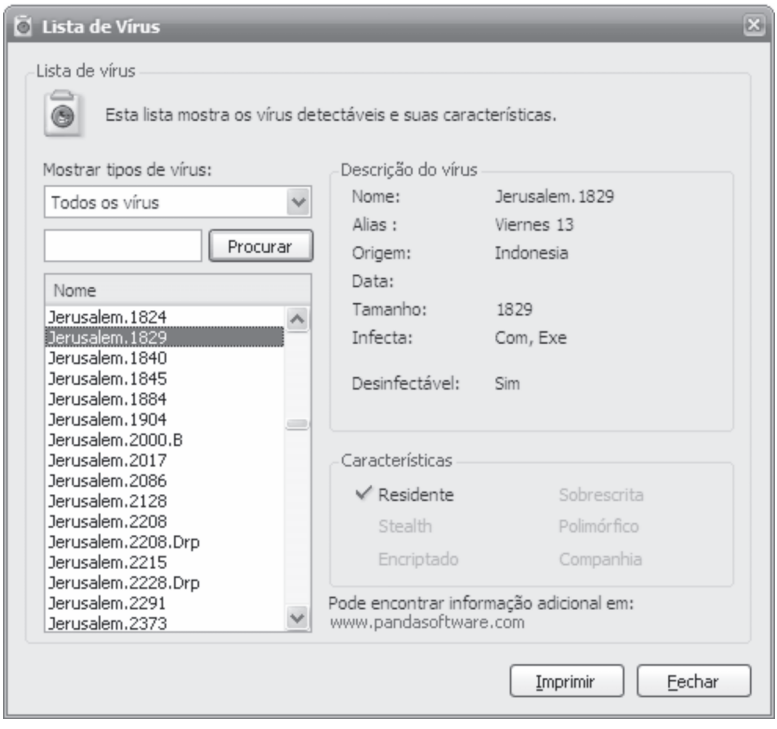


Figura 3.6
Exemplo de uma base de dados de vírus incorporada num antivírus

As empresas que desenvolvem antivírus classificam os vírus, segundo a gravidade dos seus efeitos, a facilidade de infecção e o nível de propagação mundial, em:

- baixo risco – vírus que apenas realiza operações inofensivas como emissão de sinais sonoros. Pode também infectar algumas aplicações que são raramente utilizadas;
- risco médio – vírus com alguma facilidade de propagação e infecção, podendo eliminar ficheiros;
- alto risco – vírus de propagação rápida, normalmente de origem recente («última geração»), que pode causar danos significativos no computador como eliminar todo o conteúdo de um disco rígido.

Medidas de segurança para prevenir ataques de vírus

A melhor forma de evitar que um computador seja infectado por vírus é aplicando as seguintes recomendações:

1. Instalar todas as actualizações *(updates)* disponibilizadas pelo fabricante do sistema operativo que utiliza diariamente. O Windows, por exemplo, fornece a possibilidade de transferir automaticamente as últimas actualizações de segurança da Microsoft pela aplicação *«Automatic Updates»*;
2. Instalar um antivírus e manter a base de dados de vírus sempre actualizada, uma vez que todos os meses são descobertos cerca de 500 vírus novos;
3. Instalar (se possível) um sistema operativo alternativo como o Linux, uma vez que este sistema operativo possui características de segurança adicionais que o tornam praticamente inviolável;
4. Utilizar um *browser* e um programa de *e-mail* alternativo, uma vez que os mais populares *browsers* e programas de *e-mail* da Microsoft – Internet Explorer e Outlook, respectivamente – são frequentemente atacados por *hackers*;
5. Evitar descarregar programas ou ficheiros da Internet de fontes não fiáveis;
6. Evitar abrir uma mensagem de *e-mail* quando o emissor é desconhecido;

7. Evitar (se possível) enviar documentos por *e-mail* em formato Word, uma vez que estes documentos contêm *macros* e, portanto, são mais sujeitos a vírus de *macro*. Uma solução alternativa é enviar no formato RTF *(rich text format)*.
8. Instalar uma *firewall* e um sistema de detecção de intrusão.

SERVIÇOS DE SEGURANÇA

FILTRAGEM DE CONTEÚDOS

A utilização de mecanismos de filtragem de conteúdos, como páginas da Internet ou mensagens de *e-mail*, é cada vez mais comum não só por empresas mas também por particulares, principalmente para bloquear o acesso de crianças e jovens a certo tipo de salas de conversação e grupos de discussão *(newsgroups)*. A filtragem é realizada por *software* que restringe ou elimina o fluxo de tráfego indesejável e que pode estar instalado nos servidores que permitem o acesso à Internet ou em cada computador da rede. A implementação da filtragem de conteúdos em cada organização pode englobar várias vertentes:

- Seleccionar os conteúdos e recursos admissíveis a serem acedidos, enviados e recebidos por cada utilizador, nomeadamente mensagens de *e-mail*, páginas da Internet, mensagens instantâneas, grupos de discussão, etc.;
- Evitar a entrada de vírus e outros programas maliciosos, assim como de publicidade indesejada *(spam)*, e impedir a saída de informação confidencial;
- Limitar o tamanho das mensagens de *e-mail* que podem ser enviadas/recebidas.

Assim, cada organização deverá definir as políticas de acesso e catalogar os conteúdos que podem ser acedidos. Contudo, podem ser levantados alguns problemas legais, pois a filtragem pode ser considerada censura ou violação da liberdade de expressão.

BACKUPS REMOTAS

Uma *backup* (cópia de segurança) consiste na cópia de dados para um determinado dispositivo de armazenamento de modo a que a infor-

mação possa ser facilmente recuperada após uma situação de perda desses dados, devida a um desastre natural (fogo ou inundação), por um vírus ou pelo facto de o utilizador ter apagado acidentalmente informação. Nos últimos tempos, devido à crescente utilização de banda larga, esse processo é realizado através da Internet, guardando-se a informação em locais remotos, *i. e*., geograficamente distintos, e fornecendo às organizações uma maior resistência aos problemas suscitados pelas catástrofes.

Estes serviços são prestados por empresas especializadas independentes que possuem o *software* necessário e servidores com capacidade para armazenar os ficheiros. Contudo, se essas empresas forem vendidas ou abrirem falência, o procedimento de acesso à informação guardada pode ser afectado. Os sistemas de *backup* remotas são constituídos por programas clientes que correm em determinados instantes de tempo (geralmente uma vez por dia) e têm como função comprimir, cifrar e transferir a informação para os servidores remotos, sem qualquer intervenção do utilizador.

Note-se que as *backups* remotas devem fazer parte dos planos de recuperação de desastres e de continuidade do negócio[3] das organizações.

MONITORIZAÇÃO REMOTA

A monitorização de uma rede é um processo que consiste em «vigiar» constantemente os comportamentos de todas as componentes, todos os equipamentos, serviços e aplicações da rede, por exemplo, à procura de falhas de sistema ou sobrecargas que provoquem lentidão. A monitorização é remota quando a vigilância e o controlo são efectuados por empresas especializadas, sendo nesse caso necessário que existam acordos de confidencialidade muito fortes que evitem quebras de segurança.

A monitorização remota permite compreender os perfis de utilização e desempenho dos diversos sistemas da rede e efectuar testes de vulnerabilidade aos diferentes programas e ao próprio sistema operativo de cada computador, que, se não forem descobertos, podem provocar ataques e infecções através de programas maliciosos. Se for descoberta alguma vulnerabilidade , a monitorização deverá possibilitar a realização de actualizações de segurança.

Uma vez que todas as componentes da rede devem ser vigiadas, a monitorização funciona também como um sistema de detenção de intrusão sempre que forem assinaladas tentativas de ataque à *firewall* e ligações não autorizadas.

TESTE OS SEUS CONHECIMENTOS

1. Se tivesse de escolher entre uma *packet filtering firewall* e uma *proxy application firewall*, qual escolheria? Justifique.
2. Indique as principais diferenças entre uma *firewall* e um sistema de detecção de intrusão.
3. Aponte as principais diferenças entre vírus, *worms* e cavalos de Tróia.
4. Indique alguns procedimentos para manter um computador livre de vírus.
5. Qual o principal objectivo da filtragem de conteúdos?

NOTAS

Pág. 58 [1] *Freeware* é um programa de computador, com direitos de autor, disponível na Internet sem custos e por tempo ilimitado.

Pág. 58 [2] *Shareware* é um programa de computador disponível na Internet em que o utilizador deve efectuar o pagamento da licença de utilização se quiser manter o programa após um período de experiência.

Pág. 66 [3] Estes planos referem-se à capacidade que uma empresa deve ter para recuperar de desastres e/ou situações inesperadas, regressando à condição anterior ao evento, de modo a continuar com as operações habituais.

C A P Í T U L O 4

Pagamentos no Âmbito do Negócio Electrónico

O B J E C T I V O S

- Descrever os principais modelos de pagamento electrónico, nomeadamente cartões de crédito e débito, micropagamentos, «moedas» alternativas, *server-side wallets*, PayPal, MBNet e débitos directos
- Explicar os principais protocolos de autenticação (SET, MIA/SET e 3D-Secure) para os pagamentos com cartões de crédito
- Apresentar algumas medidas para protecção de dados nos pagamentos electrónicos

A Internet nasceu em 1969, sob o nome ARPANET, como resultado de um projecto do Departamento de Defesa americano para desenvolver uma rede de computadores militares que continuasse a funcionar mesmo em caso de guerra. Após o abandono do projecto pelos militares, a Internet foi utilizada pela comunidade científica e académica, passando a servir posteriormente interesses comerciais e a sociedade em geral. Diversos serviços foram sendo disponibilizados a nível mundial; entre estes estava a World Wide Web, que possibilitou às empresas a oferta de melhores oportunidades de negócio electrónico, de modo a não serem ultrapassadas num mercado que se foi tornando cada vez mais global. No entanto, o que falta hoje em dia para o negócio electrónico alcançar a adesão total por parte da população são meios para efectuar pagamentos seguros.

Este capítulo introduz os principais modelos de pagamento electrónico, nacionais e internacionais, nomeadamente cartões de crédito e débito, micropagamentos, «moedas» alternativas, server-side wallets*, PayPal, MBNet e débitos directos. Mais ainda, são enunciadas algumas medidas para protecção de dados no pagamento electrónico.*

Pagamentos Electrónicos

Os consumidores estão habituados a utilizar determinados tipos de pagamento nas transacções do comércio tradicional, como moeda, cartão de crédito, cartão de débito e cheque. Contudo, para poderem ser utilizados no negócio electrónico, estes instrumentos têm de ser adaptados de modo a funcionarem em tempo real. Assim, os pagamentos electrónicos referem-se às transferências de fundos, realizadas *online*, entre compradores e vendedores.

Alguns dos entraves ao desenvolvimento e crescimento global do negócio electrónico são a proliferação de sistemas de pagamentos electrónicos incompatíveis (por causa de diversos factores, como o facto de estarem ligados a um único *browser*, por utilizarem métodos criptográficos proibidos em alguns países ou *software* que não é livre) e a falta de um ambiente completamente seguro para a realização das transacções comerciais.

Em relação à segurança do pagamento electrónico existem dois pontos de vista: comprador e vendedor. A principal preocupação do comprador é que os dados relativos ao pagamento (como o número do cartão de crédito) sejam interceptados por terceiros e posteriormente utilizados para cometer fraudes, enquanto a preocupação do vendedor

é saber se realmente receberá o dinheiro da venda efectuada pelo meio de pagamento escolhido pelo comprador.

Entre os modelos de pagamento electrónico mais comuns encontram-se:

- cartões de crédito;
- cartões de débito;
- micropagamentos;
- «moedas» alternativas;
- *server-side wallets*;
- PayPal.

Para além destes, foram desenvolvidos em Portugal dois novos sistemas de pagamento:

- MBnet;
- débitos directos.

A adesão de um comerciante a alguns destes modelos de pagamento traz algumas vantagens, por exemplo, a atracção de um maior número de clientes, e desvantagens, como o aumento de custos/comissões. No entanto, se o comerciante recorrer a um fornecedor especializado de serviços *(payment service provider)*, essas desvantagens podem ser minimizadas.

MODELOS DE PAGAMENTO ELECTRÓNICO

Cartões de crédito

É um sistema utilizado abundantemente no comércio tradicional e que permite efectuar compras em qualquer parte do mundo desde que o vendedor aceite o tipo de pagamento. Contudo, é um sistema passível de sofrer fraudes relacionadas com a utilização de detalhes de cartões (número ou data de validade) falsos ou roubados.

Existem basicamente dois modos de operação com os cartões de crédito: cartão presente e cartão não presente. No primeiro caso, existe um menor risco de fraude porque o comprador se encontra na presença (física) do vendedor, pelo que é possível a sua identificação, por exemplo, pela verificação da assinatura. No caso do cartão não presente, como o nome indica, há uma ausência de contacto

físico entre os intervenientes da transacção, havendo por isso um risco elevado de fraude. Um cartão não presente pode ser utilizado em dois ambientes:

1. *Mail order/telephone order* (MO/TO)

Situações em que o vendedor recebe ordens de compra através de mensagens de *e-mail*, chamadas telefónicas ou fax. Existem modos de autenticar essas transacções:

- CVV2/CVC2 – habitualmente referidos como códigos de segurança do cartão; são os três últimos dígitos do código impresso no verso de todos os cartões;
- AVS *(address verification service)* – sistema que verifica se o endereço fornecido pelo comprador (no momento da compra) coincide com o do dono do cartão de crédito;

2. *Online*

Situações em que o vendedor comercializa os seus produtos/serviços exclusivamente pela Internet, pelo que os dados da transacção são fornecidos por *e-mail* ou directamente na página do vendedor através de formulários *(forms)*.

Os intervenientes habituais num pagamento electrónico feito com um cartão de crédito são:

- *cardholder* ou comprador – proprietário do cartão;
- *issuer* – instituição financeira que emite os cartões e garante o pagamento das operações autorizadas;
- *merchant* ou vendedor;
- *acquirer* – instituição que estabelece um contrato com o vendedor para que este possa aceitar pagamentos com cartão e posteriormente receber o valor;
- *payment gateway* – combinação de *hardware* e *software* operado pelo *acquirer* ou outra entidade por si designada para processamento de mensagens do vendedor relativas a autorizações de pagamentos.

O pagamento electrónico através de um cartão de crédito *online* é efectuado em duas fases: *autorização* e *captura* (Figura 4.1).

- Autorização
  1. Depois de seleccionar (na página da Internet do vendedor) os produtos/serviços que pretende encomendar, o compra-

dor envia os dados (número do cartão, data de validade e quantia total da compra) ao vendedor;

2. O vendedor recebe os dados e reenvia-os ao *payment gateway* de modo a serem processados;
3. A autorização é pedida pelo *payment gateway* ao *acquirer*.
4. O *acquirer* «pergunta» ao banco do comprador ou ao *issuer* se o pagamento pode ser efectuado;
5. O *issuer* envia a mensagem de resposta, com a autorização ou não do pagamento. Em caso afirmativo, o montante correspondente à compra fica «cativo» na conta do comprador, *i. e*., não há transferência imediata de dinheiro;
6. O *acquirer* envia a resposta ao *payment gateway*;
7. Este processa a resposta e envia-a ao vendedor;
8. Se a autorização de pagamento for concedida, o vendedor envia os produtos ao comprador ou presta os serviços solicitados;

- Captura
  9. O vendedor pede ao emissor do cartão que transfira o dinheiro para a sua conta.

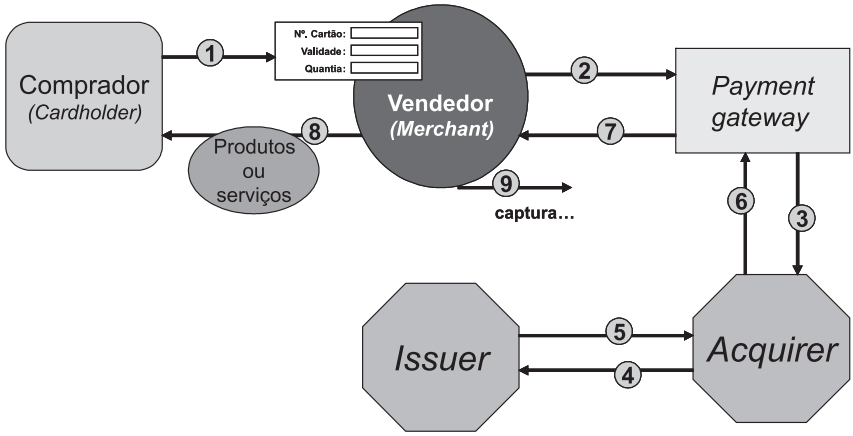


Figura 4.1
Cenário típico do pagamento electrónico através de um cartão de crédito *online*

Os principais problemas de segurança neste processo são a possibilidade de os dados do cartão serem lidos enquanto são transmitidos ou até quando são armazenados pelo vendedor. Além disso, o comprador pode não desejar revelar os dados do cartão ao vendedor ou os dados da compra a outras entidades. Soluções possíveis para estes problemas consistem em utilizar protocolos SSL/TLS (ver Capítulo 2), em impedir que o vendedor armazene os dados do cartão ou em utilizar sistemas do tipo SET *(secure electronic transaction)*.

Secure electronic transaction

Convictas de que muitas vezes esta segurança não existe quando se utiliza um cartão de crédito em pagamentos na Internet e de que os utilizadores sentem necessidade de protecção adicional nos meios electrónicos, algumas empresas iniciaram trabalhos conjuntos para o desenvolvimento de sistemas seguros, normalmente baseados em técnicas criptográficas (ver Capítulo 2). Um dos primeiros sistemas, o SET, foi inicialmente desenvolvido pelas empresas de cartões de crédito Visa e Mastercard, com o apoio de outras empresas como IBM, Microsoft, Netscape, Verisign e RSA, e teve adesão posterior da American-Express e JCB, entre outras.

Os principais objectivos do SET consistiam em garantir:

- confidencialidade da informação financeira, nomeadamente do número de cartão de crédito, uma vez que todas as mensagens trocadas entre o vendedor e o comprador durante a comunicação eram cifradas;
- integridade das mensagens, para que não fossem alteradas durante o fluxo de informação. Isto era conseguido através da utilização de assinaturas digitais;
- privacidade da informação, uma vez que ela só era disponibilizada a quem e onde era necessária (por exemplo, nem o próprio vendedor ficava a conhecer o número de cartão de crédito do comprador);
- autenticação dos participantes nas transacções electrónicas, nomeadamente comprador, vendedor e *payment gateway*, através da utilização de certificados digitais. Assim, o comprador verificava facilmente se o vendedor podia receber pagamentos com cartão de crédito e, por outro lado, sabia de imediato se o cartão era válido;
- interoperabilidade entre as especificações do SET, uma vez que eram aplicáveis a uma grande variedade de plataformas de *software* e *hardware*, de modo que a comunicação entre os intervenientes podia ser sempre realizada.

Assim, com o protocolo SET, quando era emitido um cartão de crédito pelo *issuer*, o comprador recebia um certificado digital que incluía uma chave pública com data de validade. O certificado era assinado digitalmente pelo *issuer* ou pelo *payment gateway* para garantir a sua validade. Um vendedor que aceitasse cartões de crédito

como forma de pagamento recebia um certificado digital, contendo a sua chave pública e a do *issuer*.

A Figura 4.2 apresenta um exemplo do funcionamento do SET:

- O comprador envia ao vendedor, pela página na Internet, a descrição dos produtos/serviços que pretende comprar e a marca do cartão com o qual efectuará o pagamento;
- O vendedor responde, enviando ao comprador uma mensagem, assinada digitalmente, com um código único referente à transacção e o seu certificado digital;
- O comprador verifica a integridade da mensagem e a autenticidade do vendedor. Se tudo estiver correcto, o comprador envia uma mensagem ao vendedor com dois textos, identificados pelo código da transacção:
  - O primeiro texto contém informações necessárias para validar e satisfazer a encomenda (identificação do *issuer* e local da entrega). Esta mensagem é cifrada com a chave pública do vendedor;
  - O segundo texto contém os dados relativos ao cartão (número e data de validade). Estes dados são cifrados num envelope digital com a chave pública do *payment gateway*, pelo que não podem ser lidos pelo vendedor;

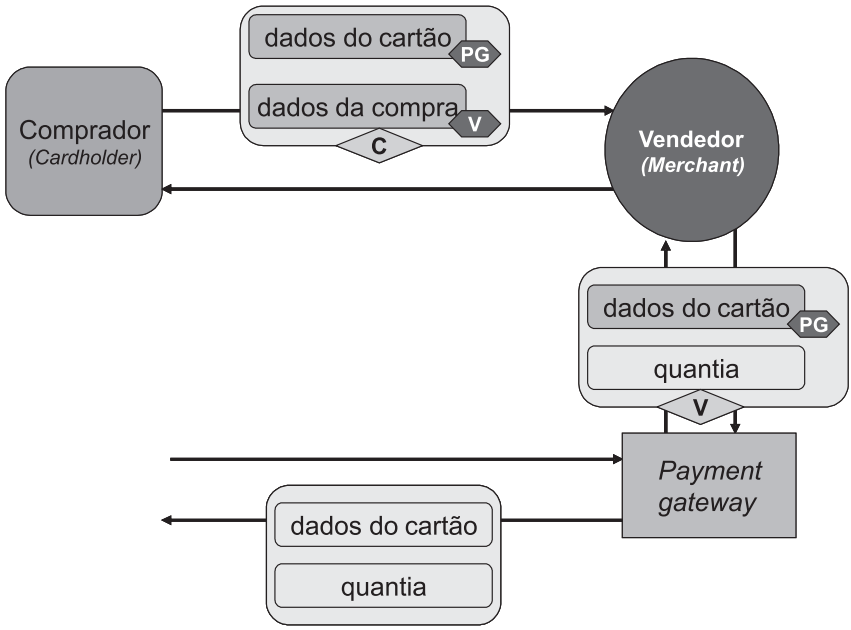


Figura 4.2
Esquema de funcionamento do SET

- O vendedor verifica a integridade e autenticidade da mensagem do comprador, reenviando o envelope digital ao *payment gateway* para processamento do pagamento, juntamente com o seu certificado, tudo cifrado com a chave pública do *payment gateway*;
- Se o pagamento for autorizado, o vendedor envia a encomenda ou presta os serviços.

Contudo, este sistema apresentou grandes dificuldades de adopção, sobretudo pelos compradores, devido à necessidade de instalação de *software* específico e ao elevado custo e complexidade, especialmente quando se compara com a alternativa SSL. Assim, conscientes deste facto, os promotores do SET desenvolveram uma variante: MIA/SET *(merchant initiated authorization)*.

Novos protocolos de autenticação

O MIA/SET aliviou a complexidade mas era insuficiente a nível da segurança, pois eliminava a componente relacionada com o comprador, como por exemplo a funcionalidade de autenticação.

A Visa e a Mastercard procuraram então alternativas, desta vez em separado. A Visa propôs o 3D-Secure, também conhecido por *«verified by Visa»* (VbV), que é um sistema com três domínios (3D):

- *Issuer* ou emissor – constituído por servidores que realizam as operações de activação, validação, verificação e autenticação do cartão do comprador e fornecem respostas ao vendedor assinadas digitalmente;
- *Acquirer* – constituído por um módulo de *software* que fornece a interface entre o 3D-Secure e o *software* do vendedor que processa o pagamento. Também se encarrega de verificar as assinaturas digitais do *issuer* nas respostas de autenticação enviadas ao vendedor;
- Interoperabilidade – constituído pelo Visa Directory, um servidor que encaminha os pedidos de autenticação do comprador solicitados pelo vendedor para o domínio do *issuer*.

Algumas características deste sistema são as seguintes:

- Os vendedores interagem com o *acquirer* e com Visa (através do Visa Directory);

- Os compradores efectuam um registo prévio junto do seu *issuer*, definindo um *username* e uma *password*, introduzindo assim mais um factor de segurança.

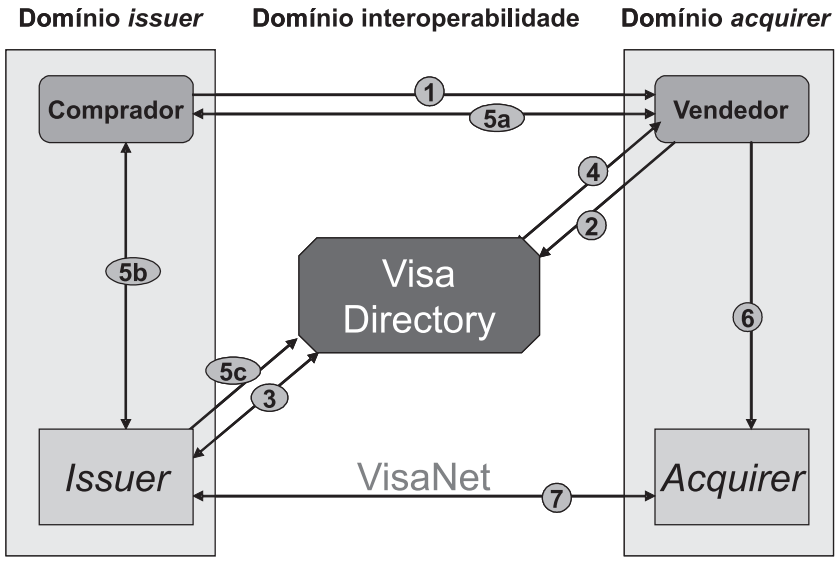


Figura 4.3 Esquema de funcionamento do 3D-Secure

A Figura 4.3 apresenta um esquema do 3D-Secure, que pode ser descrito da seguinte maneira:

1. Após a escolha dos produtos/serviços a encomendar através da página na Internet do vendedor, o comprador clica no botão de «compra», que faz surgir um formulário em que são pedidos os dados do cartão de crédito;
2. O *software* do 3D-Secure do vendedor é activado e envia a informação recebida ao Visa Directory para que este verifique se o comprador já está registado no sistema;
3. Após a autenticação do vendedor, o Visa Directory processa o pedido;
4. O Visa Directory envia a resposta ao vendedor;
5. O *software* do vendedor envia uma mensagem ao *issuer* a pedir a autenticação do comprador. O *issuer* abre uma janela no computador do comprador indicando que o vendedor está a pedir uma autorização de transacção da respectiva quantia. O comprador aprova a operação, por exemplo, introduzindo a *password* do seu registo no sistema. O *issuer* envia então uma mensagem ao vendedor com a resposta da aprovação;

6. O *software* do vendedor processa a resposta e envia um pedido de autorização de pagamento ao *acquirer*;

7. O *acquirer* reenvia o pedido ao *issuer*, através do VisaNet[1]. O *issuer* processa o pedido e responde. Se a transacção for autorizada, o vendedor apresenta ao comprador uma ordem de confirmação com os detalhes sobre a entrega dos produtos ou a prestação de serviços.

O outro protocolo de autenticação, proposto pela Mastercard, é a SPA *(secure payment application)*. Neste sistema, assim como no 3D-Secure, os utilizadores devem efectuar um registo prévio junto do seu *issuer*. No entanto, na SPA só existem dois domínios: o *issuer* e o *acquirer*. Para além disso, neste caso, os vendedores só interagem com *acquirers*.

Embora estes novos protocolos de autenticação forneçam um nível elevado de segurança, devem ser consideradas outras medidas para evitar fraudes nos pagamentos electrónicos. Uma primeira medida pode ser a utilização de listas negras com os dados dos compradores que cometeram fraudes. Nas situações em que o vendedor tiver um ponto de venda (*point of sale* – POS), a lista negra pode também incluir as fraudes cometidas *offline*. Neste caso, podem ainda ser utilizados alguns parâmetros físicos para a detecção de utilização fraudulenta dos cartões *offline*, como por exemplo duas compras quase simultâneas em locais geograficamente afastados. Contudo, esta última medida não pode ser utilizada no contexto *online*, pelo que se podem utilizar heurísticas, como o registo dos históricos das transacções efectuadas pelos cartões ou a consulta de uma lista com os números dos cartões que ainda não foram atribuídos.

Cartões de débito

Um dos mecanismos de pagamento mais utilizados actualmente no comércio tradicional é o cartão de débito. O processo de transacção é semelhante ao dos cartões de crédito, mas no caso dos cartões de débito a quantia é transferida da conta do comprador para a conta do vendedor no momento em que o comprador aprova a compra, através da utilização do código pessoal (PIN – *personal identification number*).

Os cartões de débito podem também ser utilizados para efectuar pagamentos electrónicos desde que:

- exista uma ligação do vendedor à entidade financeira que processa os pagamentos com estes cartões;

- a entidade financeira aceite o modelo de negócio do vendedor.

Entre as formas de pagamento disponíveis para o comprador encontram-se:

- a ATM *(automated teller machine)* ou caixa automático Multibanco – equipamento que permite levantar e depositar dinheiro, consultar saldos e movimentos das contas e efectuar transferências;
- o *homebanking* – página de um banco na Internet;
- o telemóvel.

O funcionamento do cartão de débito para efectuar pagamentos electrónicos (Figura 4.4) pode ser descrito da seguinte maneira: após a encomenda dos produtos/serviços na página da Internet do vendedor, este envia os dados necessários para que o comprador faça o pagamento, nomeadamente, a quantia total e as referências que identificam quer o vendedor quer a compra (passo 1). Posteriormente, o comprador efectua o pagamento, através de uma ATM, do *homebanking* ou do telemóvel, utilizando os dados recebidos do vendedor (passos 2 e 3). Os dados da compra são automaticamente enviados à instituição bancária do comprador (passo 4), que efectua a transferência da quantia indicada para a conta do vendedor, identificada pelas referências enviadas (passo 5).

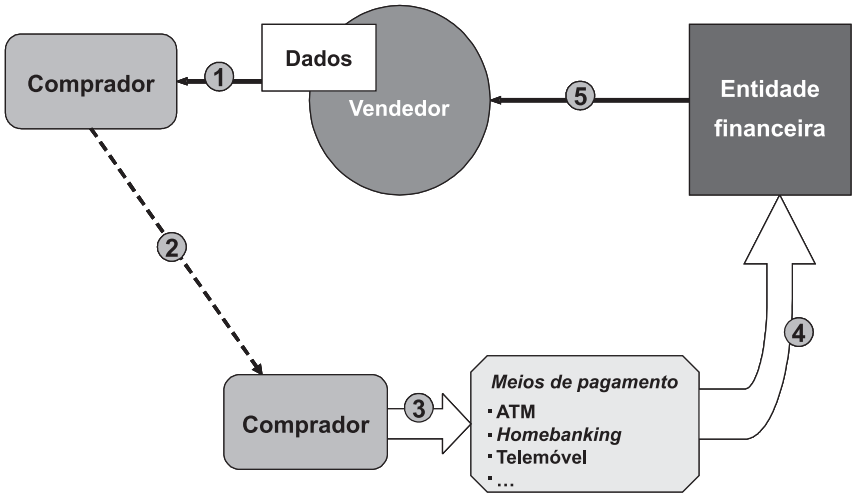


Figura 4.4
Esquema de funcionamento dos cartões de débito

Outra funcionalidade dos cartões de débito, amplamente conhecida e utilizada em Portugal, é a modalidade de «Pagamento de Servi-

ços». Com este sistema, inicialmente suportado pela rede ATM da SIBS[1], em que o débito é feito imediatamente, um utilizador de um cartão de débito pode fazer o pagamento (numa ATM, pelo *homebanking* ou pelo telemóvel) de contas associadas a serviços como água, electricidade, gás, telefone, telemóvel, etc. Devido à grande aceitação pela população, a SIBS e a Unicre[2] desenvolveram um novo modelo, denominado «Pagamento de Compras». Do ponto de vista do utilizador, o sistema é igual ao «Pagamento de Serviços». Do ponto de vista do vendedor, o sistema realiza a transacção em dois tempos, autorização e captura, como já acontecia com os cartões de crédito.

Micropagamentos

A criação de sistemas de pagamentos alternativos aos cartões de débito e crédito em transacções electrónicas de baixo valor, por exemplo, abaixo de um euro, tem sido um dos problemas mais fortemente debatidos no âmbito dos mercados financeiros e tecnológicos. O principal problema na utilização desses meios de pagamento nestas transacções reside no facto de envolverem comissões e, portanto, não fazer muito sentido um determinado vendedor receber 50 cêntimos e pagar 40 cêntimos de comissão. Muitos são os sistemas de micropagamentos que tentam resolver este tipo de problemas, com aplicações diversas como:

- visualização de conteúdos de artigos e documentos;
- *download* de ficheiros de música e imagens;
- subscrição ou assinatura de publicações periódicas ou de outros serviços;
- acumulação de pontos (de fidelização) por cada montante que o cliente gaste na loja que quando atingem um determinado valor se convertem em dinheiro reutilizável em compras/serviços na mesma loja;
- sistemas P2P *(peer to peer)*, em que os utilizadores pagam pelo acesso a determinados recursos partilhados, por exemplo, arquivos de dados;
- sistemas *pay-per-view*, em que os telespectadores pagam pela transmissão televisiva de programas;
- sistemas *pay-per-click*, em que as empresas publicitárias recebem um determinado montante quando um utilizador clica em pequenos anúncios normalmente colocados em motores de busca.

Têm sido propostos vários modelos arquitecturais para sistemas de micropagamentos, alguns bastante complexos tecnicamente, como o Millicent, cuja descrição sai, no entanto, do âmbito deste manual. Todavia, os modelos que parecem ter maior probabilidade de sucesso são os mais simples, baseados em contas correntes, equivalentes a pré-pagos, como é o caso dos telemóveis por carregamento, em que vão sendo descontadas as transacções efectuadas pelos utilizadores.

«Moedas» alternativas

«Moedas» alternativas *(cashback)* consistem basicamente em contas correntes com «pontos» acumulados obtidos após a realização de algumas actividades, como, por exemplo, acesso a determinadas páginas da Internet ou compras *online*. Os pontos podem depois ser utilizados no pagamento de compras em comerciantes aderentes. No entanto, tem de haver uma correspondência entre os pontos e uma moeda com valor legal, uma vez que o utilizador se assim o desejar pode transferir o montante correspondente para a sua conta à ordem. As «moedas» alternativas podem, na verdade, ser consideradas sistemas de micropagamentos com outro tipo de funcionalidades associadas, como, por exemplo, acumulação de pontos extras por cada novo utilizador «recrutado», para as tornar mais aliciantes. Alguns exemplos de «moedas» alternativas são Quidco, Rpoints e CashCash.

Server-side wallets

Server-side wallets são sistemas de controlo de pagamentos baseados em servidores remotos em geral geridos centralmente por comerciantes ou fornecedores de serviços especializados (*payment service providers*, que veremos mais adiante). Em geral, as *wallets* gerem uma conta corrente, com funcionalidades associadas como, por exemplo, o controlo de custos, a definição prévia de produtos ou serviços autorizados ou a utilização de micropagamentos, de modo a tornarem-se mais atractivas. Para além disso, as *server-side wallets* podem também ser usadas como sistemas de autorizações de pagamento em diversos contextos como famílias ou empresas.

PayPal

O PayPal é um sistema de pagamentos baseado em *stored accounts* (contas armazenadas), recarregáveis através de um cartão de

crédito (Visa, American Express ou Mastercard). Basicamente, se um utilizador quiser pagar pelo PayPal, precisa, em primeiro lugar, de abrir uma conta, fornecendo os seus dados pessoais e os do seu cartão de crédito. Contudo, no momento do registo a conta não fica imediatamente activa, ou seja, o utilizador tem de esperar pelo próximo extracto do seu cartão de crédito que contém um débito de um dólar realizado pelo PayPal e na linha associada um conjunto de números, que serão necessários para concluir o processo de abertura da conta. O PayPal obtém assim a garantia de que o utilizador que tenta abrir uma conta é o seu titular.

Após a abertura da conta, para um utilizador efectuar um pagamento, apenas necessita de introduzir o endereço de *e-mail* do receptor e indicar o montante que pretende pagar. Se o receptor não tiver uma conta aberta, terá de abrir uma, tal como o emissor do pagamento, antes de poder receber o dinheiro. Inicialmente, a quantia fica cativa na conta (virtual) do receptor. Se assim o desejar, o receptor pode, posteriormente, transferi-la para uma conta bancária ou utilizá-la para pagar a outro utilizador do PayPal.

Este sistema tem tido um enorme sucesso em todo o mundo com milhões de utilizadores e comerciantes aderentes. Por isso, não foi de estranhar que, no segundo semestre de 2002, a empresa detentora do sistema PayPal fosse adquirida pela ebay (empresa responsável pelo maior mercado de leilões da Internet).

Sistemas de pagamento em Portugal

MBNet

O MBNet é um serviço que foi desenvolvido pela SIBS (arquitectura, tecnologia e operação) e pela Unicre (*marketing* e comercialização), que permite a realização de operações de autorização e de liquidação de compras na Internet, em páginas nacionais ou estrangeiras. O serviço fornece garantias acrescidas de segurança aos compradores em relação, por exemplo, aos pagamentos com cartão de crédito (utilizando MIA-SET), uma vez que estes não necessitam de dar os dados confidenciais dos seus cartões aos comerciantes.

Para um utilizador aderir ao sistema MBNet, deverá possuir um cartão de débito ou crédito emitido por uma instituição bancária participante no sistema e fazer a associação do mesmo cartão ao serviço através dos canais próprios disponibilizados pelo banco ou através da rede Multibanco. No momento da adesão, o sistema fornece au-

tomaticamente uma identificação MBNet *(username)*, devendo depois o utilizador seleccionar o código *(password)* que pretende vir a utilizar. São estes elementos que garantem a confidencialidade e a segurança do sistema.

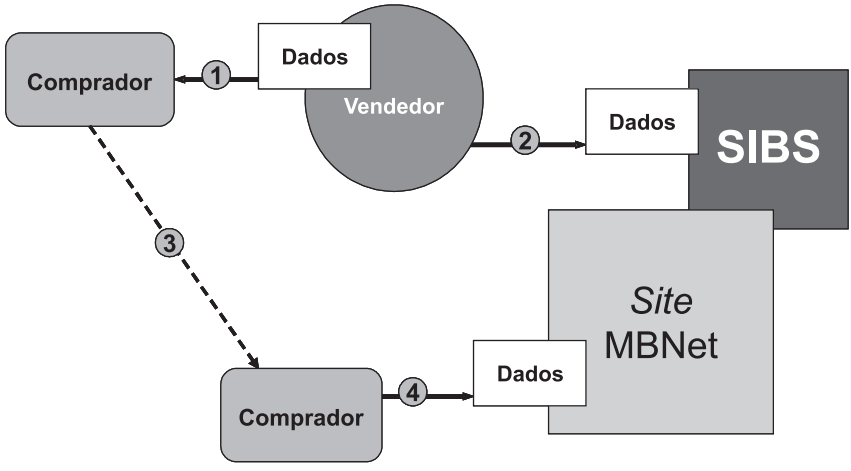
Por questões de segurança e até de controlo pessoal do utilizador, é possível no momento da adesão definir um montante máximo por dia, para cada operação, que poderá ser alterado em qualquer momento pelo próprio utilizador do cartão.

Se um comprador pretender fazer um pagamento a um comerciante aderente ao sistema, tem de receber deste uma referência da transacção. De seguida, deve dirigir-se à página do MBNet ou clicar no ícone (Figura 4.5) que se encontra na barra de ferramentas do seu computador, no caso de ter efectuado previamente a instalação, autenticar-se perante o sistema e introduzir a referência da transacção.

Figura 4.5
Ícone do sistema MBNet

Esta referência é usada pelo MBNet para comunicar com a SIBS e validar a transacção. Após esta etapa, o vendedor recebe a indicação de que o pagamento foi aceite e pode proceder à entrega dos produtos. A Figura 4.6 ilustra os passos do pagamento de uma compra a um comerciante aderente ao sistema MBNet.

Figura 4.6
Esquema de pagamento de uma compra a um comerciante aderente ao sistema MBNet



Para além disso, se o comerciante não for aderente ao sistema MBNet, o utilizador poderá solicitar ao sistema a emissão de um car-

tão de crédito temporário, com um número, uma data de expiração (cartão válido até 30 dias) e um CVV2/CVC2 (ver cartão de crédito) associado, que normalmente serve apenas para um pagamento. Isto significa que é também possível a um utilizador efectuar compras fora da Internet, bastando para isso informar o comerciante dos elementos do cartão temporário acima referidos.

Débitos directos

Um débito directo é um sistema de processamento de cobranças por transferência bancária que permite a um credor emitir uma ordem de pagamento sobre uma conta de um determinado devedor, referente, por exemplo, a contratos de fornecimento de serviços ou bens como água, luz, telefone, televisão por cabo, etc. Para além do devedor e do credor, intervêm ainda neste sistema as seguintes entidades (Figura 4.7):

- Banco do credor – entidade bancária que recebe os pagamentos debitados ao devedor;
- Banco do devedor – entidade bancária que dá a ordem de débito na conta do devedor e transfere os pagamentos para o banco do credor;
- SIBS – entidade que participa como câmara de compensação e notário electrónico, ou seja, que fornece os meios necessários para o funcionamento do sistema;
- Banco de Portugal – entidade reguladora que define o quadro regulamentar de todo o sistema.

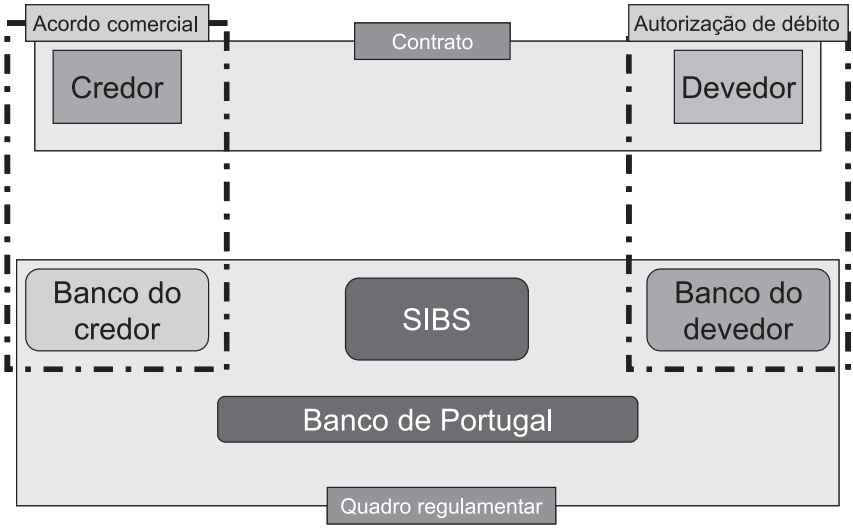


Figura 4.7 Entidades intervenientes no sistema de débitos directos

O sistema de débitos directos pressupõe a realização de um contrato entre o devedor e o credor em que primeiro o devedor concede uma autorização de débito em conta. Essa autorização pode ser realizada através:

- do sistema Multibanco, em que o devedor introduz os elementos que lhe foram antes fornecidos pelo credor, nomeadamente os números de identificação da entidade credora e da autorização de débito (Figura 4.8). Para além disso, o devedor pode definir limites como o montante máximo ou a data até à qual autoriza que lhe seja debitada a conta;
- de uma comunicação com o seu banco, por exemplo, utilizando a página do banco na Internet;
- do credor, por exemplo, no preenchimento de um formulário de adesão à TVCabo.

Figura 4.8
Exemplo de uma autorização de débito directo

Fonte: http://clientes.cabovisao.pt/)

Sempre que o credor pretender realizar um débito, emite e envia a ordem respectiva ao seu banco, indicando o número da autorização. De seguida, o banco envia a ordem ao banco do devedor, que debita o valor respectivo na conta deste e o transfere para o banco do credor. Por fim, este banco credita o dinheiro na conta do credor. No entanto, se, após uma notificação prévia do credor, o devedor verificar que o valor que lhe vai ser cobrado está incorrecto, pode rejeitar essa ordem de débito específica ou até mesmo cancelar a autorização de débito em conta.

PAYMENT SERVICE PROVIDERS

A proliferação de meios de pagamento electrónicos simples e cómodos requer que o vendedor:

- monte uma infra-estrutura própria, com ligação às entidades financeiras;
- faça a administração e manutenção da infra-estrutura;
- tenha *know-how* especializado.

A adesão de um vendedor a um fornecedor especializado de serviços (*payment service provider* – PSP) permite uma considerável redução nesses custos e requisitos. Entre os serviços proporcionados por um PSP encontram-se (Figura 4.9):

- a implementação de *payment gateways* para processamento de autorizações de pagamentos com cartões de crédito e débito;
- a disponibilização de modelos de pagamento como, por exemplo, micropagamentos, subscrições, pontos de fidelização e *server-side wallets*;
- a gestão do risco como, por exemplo, a detecção de fraudes.

Este conjunto de serviços permite garantir:

- a autenticação mútua entre o cliente/vendedor;
- a confidencialidade da informação trocada na Internet;
- a integridade dos dados;
- o não-repúdio da transacção.

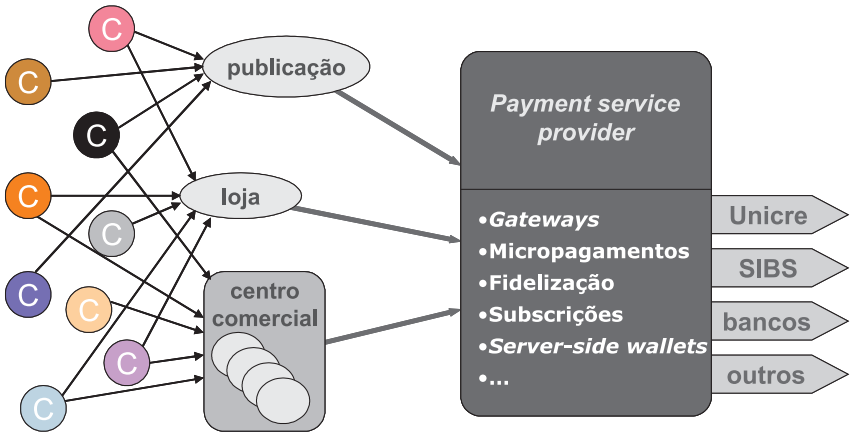


Figura 4.9
Esquema de funcionamento de um *payment service provider*

PROTECÇÃO DE DADOS DE PAGAMENTOS ELECTRÓNICOS

O sistema de pagamentos electrónicos deve ser seguro e proteger a privacidade, para além de dever garantir que nenhum dos participantes é falsamente implicado em transacções fraudulentas. Cada compra efectuada pela Internet, por exemplo utilizando um cartão de crédito, produz um fluxo de informação que é guardado numa base de dados, permitindo criar um perfil do comprador. Assim, todos os detalhes do pagamento de um comprador (dados pessoais, número de cartões de crédito e *passwords*, entre outros) devem ser protegidos, de modo a evitar utilizações não autorizadas e possibilidade de consulta, alteração e eliminação desses dados. O mesmo acontece com a informação dos catálogos do vendedor, nomeadamente produtos, preços ou condições, uma vez que também esses dados podem ser alvo de ataques, por exemplo, de eliminação ou modificação. Para além disso, o sistema deve garantir o não-repúdio por parte quer dos compradores quer dos vendedores, e devem ser asseguradas a entrega e a recepção dos bens ou serviços encomendados.

Do ponto de vista do comprador, algumas medidas de segurança que podem tornar o negócio electrónico mais seguro são:

1. A instalação de um *browser* seguro, que permita a utilização de protocolos *standard* de segurança (como SSL e sistemas do tipo SET) e a apresentação de mensagens de aviso antes do envio de informação sensível para uma página na Internet (indicando se é ou não uma página segura);

2. O envio de informação privada unicamente nos casos em que se sabe quem a vai receber, como vai ser utilizada e onde vai ser guardada;

3. A verificação de quais são as políticas de segurança da empresa, especialmente em relação à confidencialidade;

4. A realização de compras a empresas conhecidas ou, pelo menos, a procura de alguma informação sobre a empresa antes de a compra ser efectuada. Por exemplo, a verificação se é uma empresa certificada, se a morada não é só um apartado ou um endereço de *e-mail*;

5. A leitura, a impressão e o armazenamento das condições do contrato de venda.

Do ponto de vista do vendedor, alguns dos critérios de segurança que podem ser implementados são:

1. A codificação de toda a informação sensível enviada pela Internet;
2. O desenvolvimento e a manutenção de sistemas e aplicações de segurança (antivírus, *firewalls*, sistemas de detenção de intrusão, etc.);
3. A restrição de acesso (físico e por rede) à informação sensível e confidencial (como dados de cartões de crédito ou *passwords*);
4. A atribuição de um código de identificação único a cada pessoa com acesso aos computadores da rede, permitindo assim a monitorização de todos os acessos à informação e aos recursos da rede;
5. A utilização de protocolos de autenticação para pagamentos através de cartões de crédito (3D-Secure ou SPA);
6. A definição de uma boa política de segurança (ver Capítulo 5).

TESTE OS SEUS CONHECIMENTOS

1. Se tivesse de realizar um pagamento electrónico, que modelo escolheria? Justifique.
2. Descreva as principais diferenças entre o SET e o MIA/SET, e entre o SET e o 3D-Secure.
3. Qual é a principal vantagem do sistema MBNet em relação aos cartões de débito e crédito?
4. Quais as vantagens de utilizar um fornecedor especializado de serviços (PSP)?
5. Indique algumas das medidas que um comprador deve seguir para proteger os seus dados quando realiza um pagamento electrónico.

NOTAS

Pág. 78 — [1] Sistema intermediário entre *issuer* e *acquirer* que encaminha os pedidos de autorização de pagamento para o *issuer*, verifica o resultado deste pedido e envia a resposta ao *acquirer*.

Pág. 80 — [2] A SIBS, Sociedade InterBancária de Serviços, S. A. é a maior empresa portuguesa especializada em soluções tecnológicas de pagamentos, responsável entre outros, pelo desenvolvimento da rede Multibanco.

Pág. 80 — [3] A Unicre, Cartão Internacional de Crédito, S. A. é a maior empresa portuguesa especializada na gestão e emissão de cartões de pagamento.

C A P Í T U L O 5

Políticas de Segurança

O B J E C T I V O S

- Descrever os passos de uma análise de riscos
- Apresentar algumas das medidas fundamentais para garantir a segurança do pessoal e dos equipamentos
- Explicar algumas das soluções a adoptar num plano de contingência

Uma política de segurança é um conjunto de regras e procedimentos que visam controlar o acesso a determinados recursos de uma organização, por exemplo, informações confidenciais, aplicações (programas), dispositivos físicos (computadores, impressoras, etc.) ou até mesmo instalações. Uma definição formal e rigorosa dessas regras por parte de uma organização traz benefícios, como, por exemplo, saber que procedimentos adoptar perante determinadas circunstâncias, saber definir os papéis a serem desempenhados por cada interveniente, atribuir responsabilidades em caso de ocorrência de problemas, aplicar sanções aos responsáveis, se for caso disso, e limitar as responsabilidades da organização. No entanto, esses retornos só se conseguem se a política de segurança estiver materializada num documento, se tiver uma divulgação alargada e o envolvimento dos níveis hierárquicos superiores e se for periodicamente reavaliada e actualizada.

Este capítulo apresenta os principais conceitos relacionados com a implementação de uma política de segurança, como a análise de riscos e investimentos, a segurança física, o controlo de acessos e planos de contingência.

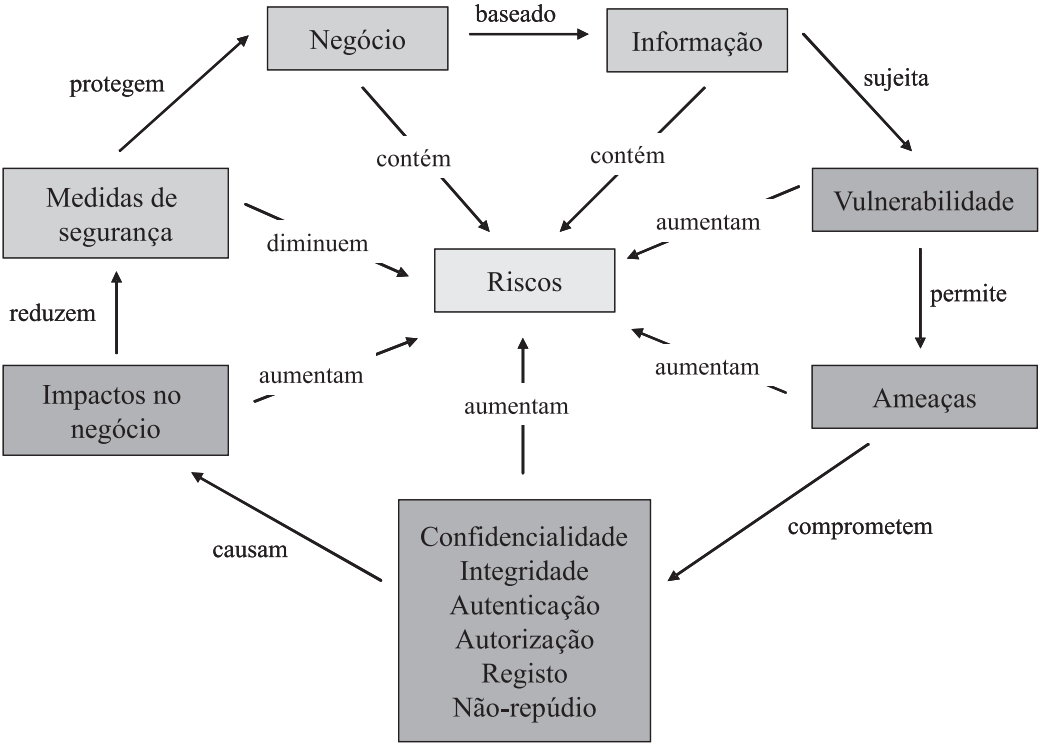
Análise de Riscos

A análise de riscos é o primeiro passo na definição de uma política de segurança de uma empresa. A análise de riscos, como o próprio nome indica, é o estudo dos riscos da realização de uma actividade como, por exemplo, atravessar uma estrada, conduzir um carro, andar de avião ou efectuar um pagamento electrónico na Internet. Alguns riscos fazem simplesmente parte do custo de se fazer um negócio, ou seja, são considerados como parte da operação normal de uma empresa. Existe, por exemplo, o risco do desenvolvimento de uma nova tecnologia que torne os automóveis movidos a gasolina completamente obsoletos. No entanto, o proprietário de uma bomba de gasolina aceita este risco. De modo semelhante, um utilizador de um computador aceita o risco de falha de um dispositivo de armazenamento (disco rígido, CD, etc.) que provoque a perda de toda a informação.

A instalação de novas soluções tecnológicas de segurança pode reduzir drasticamente a gravidade de uma ameaça (sinistro); por exemplo, o utilizador de um computador pode realizar uma cópia de segurança dos seus ficheiros como uma defesa contra uma possível falha do seu disco rígido. Contudo, as grandes empresas envolvidas em inúmeros negócios e, portanto extremamente expostas, não conseguem

determinar facilmente os riscos a que estão sujeitas. Assim, é indispensável a definição rigorosa de uma estratégia para análise de riscos (Figura 5.1). A título ilustrativo, veja-se a seguinte notícia, que demonstra a importância de uma análise de riscos.

Figura 5.1
Ciclo da segurança nos negócios



Fonte: Adaptado de DIAS (2000)

METADE DAS EMPRESAS ESTÁ VULNERÁVEL A ATAQUES INFORMÁTICOS – PROTECÇÃO CUSTA MILHÕES DE EUROS E MUITAS HORAS DE TRABALHO

«Quase metade das empresas não tem a sua infra-estrutura informática protegida a 100% face às vulnerabilidades, conclui a McAfee, líder global em prevenção de intrusão e gestão de riscos de segurança.

O estudo da McAfee, conduzido pela Ipsos Research, inquiriu cerca de 600 executivos de TI europeus pertencentes a empresas com mais de 250 empregados, anunciam em comunicado.

O seu objectivo foi analisar a dinâmica de resposta das empresas perante o anúncio de uma vulnerabilidade no seu sistema.

As conclusões do estudo revelam que, mais de um quarto dos inquiridos (27%) responderam que demoram cerca de 48 horas ou mais a proteger totalmente a sua infra-estrutura, desde que se publica um *patch*[1] até ao momento em que a infra-estrutura informática está totalmente protegida contra essa vulnerabili-

dade. Um em cada cinco (19%) afirmou que demora até uma semana ou mais.

Mais de um terço (36%) das empresas inquiridas na Europa não sabe quantos *patches* foram aplicados nas suas empresas nos últimos 6 meses.

Já 58% dos profissionais de TI inquiridos reconheceram não saber quanto está a custar à sua empresa a aplicação de *patches*. Mas o International Data Corporation[2] prevê que o mercado Europeu de gestão de *patches* venha a alcançar os 88 milhões de dólares em 2010.

Um em cada cinco profissionais de TI declarou investir uma hora ou mais por dia na investigação de vulnerabilidades e *patches*.

E 45% dos inquiridos não estabelecem áreas de negócio prioritárias para receberem patches primeiro.

O estudo da McAfee revela que 20% dos inquiridos dedicam uma hora ou mais por dia na gestão de vulnerabilidades. Na Europa, um em cada dez profissionais informáticos dedica 240 horas por ano a investigar vulnerabilidades, o que equivale a 5 semanas de trabalho dedicadas por inteiro a esta actividade.»

Fonte: Agência financeira, 17 de Abril de 2006
(http://www.agenciafinanceira.iol.pt)

BENEFÍCIOS DE UMA ANÁLISE DE RISCOS

Alguns dos benefícios de uma análise de riscos são:

- o melhoramento do grau de conhecimento – a discussão de questões de segurança pode ajudar a aumentar o nível de interesse e preocupação entre os empregados da empresa;
- o levantamento de recursos e vulnerabilidades – algumas empresas desconhecem por completo alguns dos seus recursos e as vulnerabilidades a eles associadas. Uma análise sistemática pode ajudar na identificação dos factores de exposição;
- o melhoramento dos processos de decisão – algumas soluções de segurança podem reduzir a produtividade mediante um aumento de burocracia para os utilizadores; ou seja, estas soluções não podem ser simplesmente encaradas na perspectiva de protecção que oferecem. De igual modo, algumas ameaças são tão sérias que justificam uma procura contínua de novas soluções tecnológicas;
- a justificação de custos para segurança – algumas soluções de segurança são extremamente dispendiosas sem contudo fornecerem um benefício óbvio. Uma análise de riscos pode ajudar a identificar as componentes de uma solução tecnológica em que vale a pena investir;

PASSOS DE UMA ANÁLISE DE RISCOS

Os passos básicos de uma análise de riscos são:

1. Levantamento e classificação de recursos;
2. Determinação de vulnerabilidades;
3. Estimação da probabilidade de exploração das vulnerabilidades;
4. Cálculo dos prejuízos esperados;
5. Investigação de novas soluções tecnológicas e seus custos.

Levantamento e classificação de recursos

O primeiro passo de uma análise de riscos consiste no levantamento e classificação dos meios humanos e/ou materiais de uma empresa, ou seja, na realização de um inventário. Esses recursos podem ser agrupados em diversas categorias, como:

- aplicações;
- bases de dados;
- arquivos de documentos e comunicações que contenham:
  - relatórios financeiros;
  - especificações de produtos;
  - planos de negócios;
  - listas de clientes e *prospects*;
- computadores e outros dispositivos de *hardware*;
- trabalhadores.

Apesar de em algumas empresas ser procedimento habitual a realização de um inventário anual ao *hardware* por motivos de amortização e obsolência tecnológica, existem, no entanto, outras em que esse inventário pode estar desactualizado. Mais ainda, esse inventário anual raramente inclui recursos intangíveis como dados ou trabalhadores.

Determinação de vulnerabilidades

O levantamento de recursos de uma empresa é uma tarefa simples, porque muitos dos meios humanos e/ou materiais são tangíveis ou facilmente identificáveis. O passo seguinte de uma análise de riscos consiste na determinação das vulnerabilidades desses recursos.

No entanto, é muito difícil identificar até que ponto se é vulnerável a cada ameaça. Mesmo assim, é possível com alguma imaginação prever que ataques podem ocorrer aos recursos e quais as suas fontes.

As garantias requeridas para obter a segurança desejada por uma empresa são confidencialidade, integridade, autenticação, autorização, registo e não-repúdio (ver Capítulo 1). Um ataque é qualquer situação que implique a perda de alguma dessas características. Algumas das questões e dos cenários a considerar incluem:

- Quais são os efeitos provocados por erros não intencionais? Considerar, por exemplo, a divulgação precipitada de planos de negócios ou catálogos de produtos;
- Quais são os efeitos provocados por um acto interno malicioso? Considerar, por exemplo, empregados insatisfeitos ou subornados por empresas concorrentes;
- Quais são os efeitos provocados por um acto externo malicioso? Considerar, por exemplo, o acesso à rede informática por *hackers* ou o acesso às instalações por ladrões;
- Quais são os efeitos provocados por catástrofes físicas e naturais? Considerar, por exemplo, incêndios, tempestades, inundações, quebras de energia ou falhas de equipamento.

Estimação da probabilidade de exploração das vulnerabilidades

O terceiro passo de uma análise de riscos consiste em determinar com que frequência cada vulnerabilidade pode ser explorada. A probabilidade de ocorrência de um ataque está relacionada com o nível de segurança oferecido pelas soluções tecnológicas já existentes e com a probabilidade de algo ou alguém suplantar essa segurança. Apesar de ser praticamente impossível prever a probabilidade de ocorrência de alguns eventos, existem formas de estimar essa probabilidade, como, por exemplo:

- através da observação de dados da população em geral – é impossível determinar quando é que um fogo ou uma catástrofe natural atingirá uma casa. No entanto, as companhias de seguro possuem dados a partir dos quais conseguem prever que num determinado ano, n casas serão afectadas por incêndios, com um prejuízo médio de x. De igual modo, as companhias de seguro possuem dados a partir dos quais se pode inferir a probabili-

dade de suborno por parte de um trabalhador, de assalto a umas instalações, etc.;

- através da observação de dados locais – o sistema operativo de um computador pode efectuar o registo das falhas de *hardware*, número de acessos e tamanho dos ficheiros de dados;
- através do número de casos registados num determinado período de tempo – o analista investiga e faz uma aproximação do número de vezes que um determinado evento ocorreu no último ano. Apesar de o número não ser exacto, porque provavelmente o analista não teve acesso a todas as informações, pode ser considerado uma estimativa razoável;
- através do método de Delphi – é uma técnica em que diversos analistas estimam individualmente a probabilidade de ocorrência de um evento. As estimativas são depois reunidas, reproduzidas e distribuídas a todos os analistas. De seguida, é feita a pergunta aos analistas se desejam modificar algumas das probabilidades estimadas com base nas fornecidas pelos colegas. Após um conjunto de revisões, todas as estimativas são novamente reunidas. Se os valores forem razoavelmente consistentes, a estimativa final é inferida. Se forem inconsistentes, os analistas reúnem-se novamente para discutir a razão da incoerência e seleccionarem uma estimativa final.

Cálculo dos prejuízos esperados

O cálculo do prejuízo financeiro esperado por cada cenário identificado é o passo seguinte de uma análise de riscos. Assim como a probabilidade de ocorrência de um ataque, também este valor é difícil de estimar. Alguns custos, como o custo de substituir uma componente de *hardware*, são fáceis de determinar. Mesmo os custos de substituição de uma aplicação podem ser aproximados com base nos custos de aquisição ou desenvolvimento. No entanto, as consequências para terceiros relacionadas com a perturbação da actividade da empresa, por exemplo, por falha de uma aplicação ou de uma componente de *hardware*, são substancialmente mais difíceis de quantificar.

A divulgação de dados confidenciais de uma empresa a pessoas não autorizadas como dados de um novo produto, resultados de vendas ou informações financeiras pode implicar uma redução da vantagem competitiva e fornecer vantagens a uma empresa concorrente.

Alguns dados financeiros, especialmente dados adversos, podem provocar danos na imagem da empresa e afectar a confiança dos clientes. Assim, neste caso também é difícil determinar os prejuízos directos da divulgação deste tipo de informações.

As seguintes questões podem ajudar na análise das implicações de uma falha de segurança. Apesar de não indicarem custos precisos, as respostas a estas questões podem ajudar a identificar as fontes de custos tangíveis e intangíveis.

- Quais são as implicações futuras em termos de negócios de um acesso não autorizado aos dados confidenciais? Podem esses dados fornecer uma vantagem competitiva às empresas concorrentes? Qual é a diminuição estimada do número de vendas?
- Qual é o efeito psicológico da falha de uma aplicação ou de uma componente de *hardware*? Perda de credibilidade? Perda de negócios? Quantos clientes vão ser afectados? Qual é o seu valor como clientes?
- Quais são os problemas levantados por uma perda de dados? Podem ser recuperados? Podem ser reconstruídos? Com muito trabalho?
- Quanto vale o acesso por terceiros aos dados e aplicações de uma empresa? Quanto é que uma empresa concorrente está disposta a pagar por esse acesso?

Como foi mencionado atrás, não é fácil identificar o custo que cada ameaça coloca para o negócio. No entanto, esse custo deve ser calculado para cada tipo de recursos em presença de cada cenário identificado.

Investigação de novas soluções tecnológicas e seus custos

No caso dos prejuízos financeiros esperados serem inaceitáveis, torna-se indispensável investigar novas soluções tecnológicas de segurança. Se o risco de acesso não autorizado for demasiado elevado, por exemplo, deve ser instalado *hardware* de controlo de acesso como *tokens* de segurança ou leitores biométricos (ver Capítulo 1). No entanto, na instalação de novas soluções tecnológicas, há dois aspectos extremamente importantes a considerar:

- Nível de segurança oferecido;
- Custo.

Em relação ao nível de segurança oferecido, foram apresentadas ao longo deste manual diversas ferramentas como protocolos de segurança do tipo SSL, sistemas de detecção de intrusão, *firewalls*, antivírus e serviços de segurança (*backups*, filtragem de conteúdos) que permitem reduzir ou eliminar o impacto causado por alguns ataques. A selecção de algumas dessas ferramentas por parte de uma empresa está intimamente ligada aos cenários identificados para cada tipo de recursos. Contudo, o custo de aquisição e instalação é também um factor-chave, de tal forma que deve haver um compromisso entre esse custo e a segurança obtida (Figura 5.2). Para além disso, deve ser considerado o retorno do investimento nas novas soluções, ou seja, o custo de aquisição de uma solução para um determinado recurso não deve ser superior ao prejuízo esperado por um ataque a esse mesmo recurso.

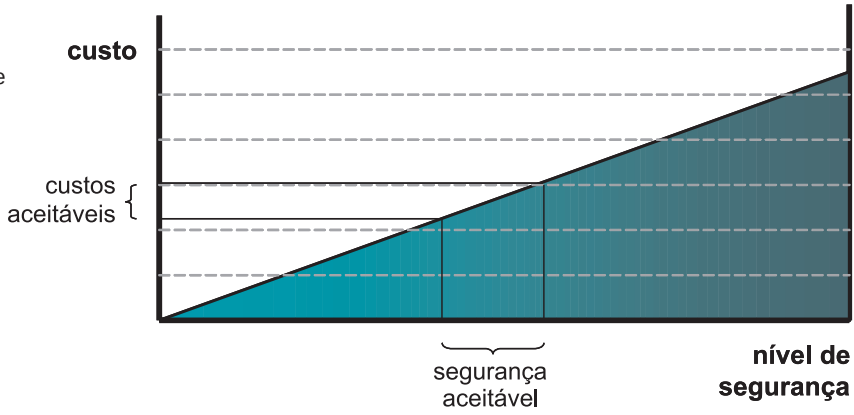


Figura 5.2
Representação do compromisso entre o custo e o nível de segurança oferecido por uma nova solução tecnológica

DOCUMENTAR A POLÍTICA

Após a identificação das vulnerabilidades, a estimação dos prejuízos esperados e a investigação de novas soluções tecnológicas de segurança, é necessário que a empresa apresente uma definição concreta das medidas a serem realizadas de modo a proteger a sua informação privada e a assegurar o pleno funcionamento dos seus negócios. Essas medidas devem estar materializadas num documento de divulgação alargada, que deve ter o envolvimento dos níveis hierárquicos superiores e ser periodicamente reavaliado e actualizado. Assim, o documento a produzir deve conter os seguintes elementos:

- Mensagem da administração, reforçando a importância que a segurança assume;

- Objectivos, indicando:
  - quais os propósitos de segurança da empresa como, por exemplo, a protecção da integridade dos dados ou a protecção contra a «fuga» de informação;
  - qual o compromisso da empresa em relação à segurança, *i. e*., os esforços que a empresa é capaz de realizar para minimizar os prejuízos em caso de incidente;
- Estado actual, indicando alguns dos resultados obtidos através da análise de riscos, nomeadamente a listagem dos recursos existentes, as suas vulnerabilidades e as soluções tecnológicas de segurança já implementadas;
- Recomendações e requisitos, indicando as acções a realizar para implementar a política de segurança, nomeadamente a aquisição e instalação de novas soluções tecnológicas, a definição dos direitos de acesso, das actividades lícitas ou ilícitas e da estratégia de defesa ou contra-ataque;
- Responsabilidades, definindo claramente quem é o responsável e quem tem autoridade para implementar a política de segurança;
- Calendário de execução, definindo o plano de implementação das medidas da política de segurança com a indicação, por exemplo, da ordem de aquisição e instalação das novas soluções tecnológicas;
- Avaliação e revisão, indicando as datas em que se deve fazer um ponto da situação em relação à segurança devido, por exemplo, a factores de obsolência tecnológica ou ao aparecimento de novas vulnerabilidades;
- Glossário, de modo a auxiliar a compreensão por pessoal não técnico.

Segurança Física

A segurança física tem como objectivo a protecção de pessoas, bens e instalações das organizações pela implementação de medidas preventivas e/ou reactivas de modo a assegurar a continuidade do negócio. Inexplicavelmente, muitas organizações não consideram a segurança física importante, gastando quantias avultadas em sistemas

informáticos, nomeadamente sistemas de detecção de intrusão, *firewalls* e antivírus, esquecendo os prejuízos causados, por exemplo, pelo roubo de um portátil com informação sensível pelos empregados de limpeza ou pelo acesso não autorizado a um servidor dentro das próprias instalações. A título ilustrativo, veja-se a seguinte notícia, que demonstra a importância da segurança física.

BANCO AMERICANO SOFRE ROUBO DE DADOS PELA QUARTA VEZ

«*Sistema roubado continha informações como nomes, endereços e números de contas dos clientes do Wells Fargo.*

Pela quarta vez nos últimos 30 meses, o banco americano Well Fargo & Co publicou na sexta-feira (05/05) um comunicado no seu site informando que um computador que pertencia ao seu grupo foi dado como perdido durante o transporte para outra empresa.

A empresa iniciou um processo de notificação dos seus clientes sobre a potencial exposição das suas informações privadas, além de os alertar sobre o que podem fazer para reduzir a exposição da sua identidade roubada. A companhia irá também pagar durante um ano a assinatura de um serviço para monitorização das contas de cada um dos clientes afectados.

O equipamento continha informações como nomes, endereços, números de segurança social e números das contas dos clientes.

"O computador tem duas camadas de segurança, o que dificultará o acesso à informação", afirmou o banco. Até agora, pelo menos, não há nenhuma indicação que a informação armazenada no computador tenha sido usada inadequadamente, disse o porta-voz da empresa, Alejandro Hernandez.

Hernandez não sabe ainda quantos clientes foram afectados pelo incidente. Nem sabe informar quando ocorreu o roubo, mas afirmou que as investigações criminais já estão encaminhadas pelas autoridades. "Até ao momento, as autoridades acreditam que o equipamento foi roubado pelo hardware", e não pelos dados que ele continha, disse Hernandez.

Em Novembro de 2003, dados de milhões de clientes do Wells Fargo foram cedidos quando um ladrão invadiu o escritório. Um ano depois, em Novembro de 2004, a empresa anunciou que três *laptops* e um *desktop* com informações pessoais de milhões de mutuários foram roubados por uma empresa que imprimia mensalmente informativos para o Wells Fargo. O incidente acarretou dois processos contra o banco por negligência e quebra de contrato. O caso foi decidido a favor do banco em Março deste ano.

E, em Fevereiro de 2004, um funcionário da empresa perdeu um *laptop* que continha informações de mais de 35 mil clientes do Wells Fargo.»

Fonte: Adaptado do IDG Now, 9 de Maio de 2006 (http://idgnow.uol.com.br)

A segurança física pode ser dividida em:

- Segurança do pessoal;
- Segurança dos equipamentos.

SEGURANÇA DO PESSOAL

Consiste em reduzir os riscos de falha humana, roubo, fraude ou má utilização dos recursos. Isto exige que todos os funcionários estejam sensibilizados para o cumprimento da política de segurança da empresa. Alguns aspectos fundamentais são os seguintes:

- Formação, de modo a garantir que os funcionários tenham conhecimento das ameaças e preocupações respeitantes à segurança da informação;
- Recrutamento e/ou promoção de funcionários idóneos para os cargos que de alguma maneira permitem o acesso às informações consideradas sensíveis. Para além disso, deve existir uma cláusula de confidencialidade explicitando a importância no sigilo da informação no contrato de cada um dos funcionários, que deve ser válida mesmo após a cessação do contrato;
- Resposta a incidentes, de modo a minimizar os prejuízos causados por falhas de segurança, promovendo a adopção de medidas de correcção adequadas. Além disso, deve ser estabelecido um procedimento de notificação formal da ocorrência de incidentes;
- Medidas disciplinares para os funcionários que tenham violado os procedimentos e as políticas de segurança. Muitas vezes, a existência dessas medidas pode dissuadir funcionários que pretendam cometer fraudes.

SEGURANÇA DOS EQUIPAMENTOS

A segurança dos equipamentos consiste na adopção de medidas de segurança por forma a impedir a perda, o dano ou o prejuízo de equipamentos informáticos ou a interrupção de actividades de negócio. Algumas medidas fundamentais são:

- a instalação de UPS *(uninterruptable power suply)* ou geradores de emergência para protecção dos equipamentos contra falhas de energia;
- a manutenção correcta dos equipamentos de acordo com as especificações do fabricante de modo a garantir as suas integridade e disponibilidade;
- a eliminação ou cifra de informação sensível sempre que for necessária a reparação de equipamentos;

- a eliminação de informação sensível sempre que for entregue equipamento em *leasing*;
- a utilização de cadeados, cabos, etc., para prevenir roubos das estações de trabalho, especialmente computadores portáteis;
- a destruição de suportes removíveis (disquetes, CD, etc.) com informação sensível sempre que estiverem danificados;
- a prevenção contra furtos e observação não autorizada (espionagem) de computadores portáteis fora das instalações da empresa;
- a colocação dos servidores em instalações próprias sob vigilância permanente e com controlo de acessos.

CONTROLO DE ACESSOS

O controlo de acesso é todo e qualquer sistema de segurança construído com o objectivo de proteger instalações, equipamentos ou informações de acessos não autorizados. Normalmente, é implementado um sistema deste tipo com o recurso a meios físicos como guardas, dispositivos mecânicos como chaves e cadeados ou soluções tecnológicas como *tokens* de segurança, *smartcards* e métodos biométricos (ver Capítulo 1).

No contexto de sistemas informáticos, o controlo de acessos permite fazer a identificação, autenticação e autorização dos utilizadores. A identificação e autenticação determinam quem pode aceder ao sistema e em geral baseiam-se num dos seguintes factores:

- Algo que o utilizador conhece como um número de identificação pessoal (PIN) ou uma combinação de *username/password*. No caso de ser utilizada uma *password*, convém que, como medida de prevenção contra ataques de roubo de *passwords* (ver Capítulo 3), ela tenha no mínimo oito caracteres, pelo menos um carácter maiúsculo, um carácter minúsculo e um número e que seja mudada periodicamente;
- Algo que o utilizador tem como *tokens* de segurança ou *smartcards*;
- Alguma característica pessoal do utilizador, como uma impressão digital ou a íris.

A autorização estabelece os privilégios de um utilizador autenticado, indicando o seu tipo de permissão (leitura, escrita e execução).

Todo este processo de identificação, autenticação e autorização implica a existência de «contas» para cada um dos utilizadores que devem ser geridas pelo respectivo administrador do sistema informático. A cada conta, para além das permissões, devem estar associadas as licenças das aplicações *(software)* a que o utilizador pode aceder.

Na perspectiva da segurança das redes, as ferramentas mais utilizadas para efectuar o controlo de acessos são as *firewalls* e os sistemas de detenção de intrusão (ver Capítulo 3), pois permitem bloquear as tentativas não autorizadas à rede. No caso de acessos remotos, através de *modems* ou de redes privadas virtuais (VPN), o controlo de acessos deverá ser efectuado usando um dos meios de identificação e autenticação referidos anteriormente. Finalmente, convém referir que um sistema de controlo de acessos deve ser capaz de registar todos os acessos efectuados, quer sejam ou não autorizados, gravando pelo menos a data, a hora, o local e a identificação do utilizador, de modo a permitir a monitorização da rede.

Planos de Contingência

Um plano de contingência ou plano de recuperação de desastres descreve as medidas que uma empresa deve tomar, incluindo a activação de processos manuais ou o recurso a contratos, para assegurar que os seus negócios vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, em caso de incidente. Algumas destas medidas incluem a adopção de:

- soluções básicas como cópias de segurança dos dados, que devem ser armazenadas *off-site*, *i. e*., em instalações apropriadas, de preferência em locais remotos (ver *backups* remotos – Capítulo 3);
- soluções *cold site*, *warm site* ou *hot site*.

COLD SITE

Dependendo da natureza do negócio de uma empresa, pode ser importante recuperar o mais depressa possível de um desastre. Um

banco, por exemplo, é capaz de tolerar a interrupção dos seus serviços durante um período de quatro horas por causa de um incêndio, mas é incapaz de suportar um período de dez meses para reconstrução das instalações, aquisição e instalação de novos equipamentos. A maior parte dos fabricantes de *hardware* disponibiliza novas máquinas (computadores, servidores) às empresas num período muito rápido em situações de emergência. A questão que se põe é onde colocar este equipamento de modo a retomar as operações habituais.

Na solução *cold site*, uma empresa especializada disponibiliza ao cliente um espaço (centro de recuperação de desastres – CRD), o equipamento e as comunicações contratadas em caso de catástrofe. O cliente é responsável por manter uma cópia de segurança dos dados e por transportar essa cópia para o CRD. Mais ainda, são suas obrigações instalar o equipamento, configurar a rede e restaurar os dados. Nessa solução, o tempo de inactividade pode demorar de 24 horas a alguns dias, dependendo da complexidade dos sistemas, das aplicações e da quantidade de informação a recuperar.

WARM SITE

Na solução *warm site*, o cliente contrata uma infra-estrutura dedicada com suporte de sistemas (processamento e armazenamento) e de comunicações. Assim como na solução *cold site*, o cliente é responsável por manter uma cópia de segurança dos dados, por transportar essa cópia para o CRD e restaurar a informação. A recuperação da actividade demora normalmente entre 12 a 24 horas.

HOT SITE

A solução *hot site* é a mais dispendiosa das três soluções para o cliente, uma vez que é instalada no CRD uma cópia exacta do sistema em operação. Mais ainda, os dados são transferidos assincronamente com várias frequências para o CRD. Assim, quando um desastre ocorre, o sistema alternativo é accionado e a actividade pode ser recuperada em apenas alguns minutos.

Esta solução é especialmente projectada para as organizações que não podem tolerar nenhuma inactividade nos seus serviços, como, por exemplo, instituições financeiras.

TESTE OS SEUS CONHECIMENTOS

1. Indique alguns dos benefícios de uma análise de riscos.
2. Enuncie os passos de uma análise de riscos e explique sucintamente cada um deles.
3. Aponte algumas das medidas fundamentais para garantir a segurança dos equipamentos.
4. Se tivesse de implementar um plano de contingência baseado numa solução *cold site*, *warm site* ou *hot site*, qual escolheria? Justifique.

NOTAS

Pág. 91 **1** *Patches* são actualizações de segurança que os fornecedores de *software* publicam nas suas páginas quando tomam conhecimento de vulnerabilidades nos seus produtos que possam comprometer a segurança do computador e da informação aí residente.

Pág. 92 **2** Reconhecida multinacional de estudos de mercado na área da Internet e das novas tecnologias.

R E F E R Ê N C I A S

BIBLIOGRAFIA

- Banco de Portugal (2002), *Débitos Directos*, Cadernos do Banco de Portugal, n.º 1.
- Banco de Portugal (2004), *Cartões Bancários*, Cadernos do Banco de Portugal, n.º 6.
- BHASIN, S. (2002), *Web Security Basics*, Course Technology.
- DIAS, C. (2000), *Segurança e Auditoria da Tecnologia da Informação*, 1.ª ed., Axcel Books.
- FERREIRA, J. e ALVES, S. (1995), *Segurança dos Sistemas e Tecnologias da Informação*, Instituto de Informática e Autoridade Nacional de Segurança.
- GARFINKEL, S. e SPAFFORD, G. (2002), *Web Security, Privacy & Commerce*, 2.ª ed., O'Reilly.
- KALAKOTA, R. e WHINSTON, A. B. (1997), *Electronic Commerce: A Manager's Guide*, Addison Wesley Longman, Inc.
- MENEZES, A., VAN OORSCHOT, P. e VANSTONE, S. (1996), *Handbook of Applied Cryptography*, CRC Press, Inc.
- MIRA DA SILVA, M., SILVA, A., ROMÃO, A. e CONDE, N. (2003), *Comércio Electrónico na Internet*, 2.ª ed. actualizada, Lidel – Edições Técnicas, Lda.
- PFLEEGER, C. (1997), *Security in Computing*, 2.ª ed., Prentice Hall International, Inc.
- PREETHAM, V. (2002), *Internet Security and Firewalls*, Course Technology.
- RSA DATA SECURITY, Inc. (1996), *Answers to Frequently Asked Questions about Today's Cryptography*, em http://www.rsasecurity.com/rsalabs/
- SCHNEIER, B. (1996), *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 2.ª ed., John Wiley & Sons.
- STALLINGS, W. (2000), *Network Security Essentials: Applications and Standards*, 1.ª ed., Prentice Hall.
- VEIGA, P. (2004), *Tecnologias e Sistemas de Informação, Redes e Segurança,* Porto, Sociedade Portuguesa de Inovação.
- Wikipedia Contributors (2006), *Wikipedia, The Free Encyclopedia*, em http://en.wikipedia.org.

URL

- MBNet http://www.mbnet.pt
- Visa Europe http://www.visaeurope.com

ANEXO A

Modelo TCP/IP

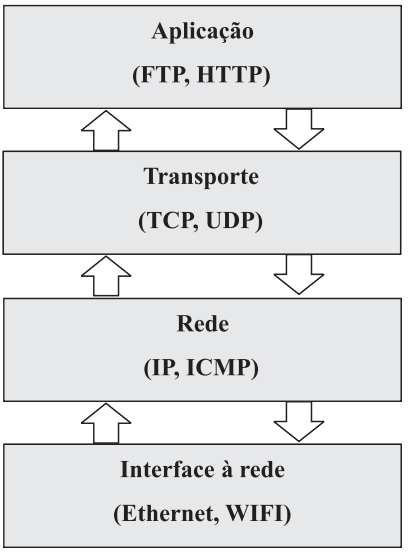
O objectivo inicial do modelo TCP/IP era construir uma rede entre ambientes heterogéneos (com diferentes tipos de computadores e sistemas operativos) que fornecesse um serviço de comunicação universal, denominado Internet. Para que ambientes incompatíveis possam trocar informação (pacotes, *i. e*., os pequenos blocos em que é dividida a informação trocada entre computadores) de maneira coerente e eficiente, é necessário definir um conjunto de normas. Esse conjunto de regras constitui um protocolo. Alguns dos protocolos pertencentes ao modelo TCP/IP são:

- *Internet protocol* (IP) – protocolo que fornece o serviço de rede Internet;
- *transmission control protocol* (TCP) – protocolo de transporte orientado à ligação na Internet;
- *user datagram protocol* (UDP) – protocolo de transporte não orientado à ligação da Internet;
- *Internet control message protocol* (ICMP) – protocolo de envio de relatórios de erro;
- *file transfer protocol* (FTP) – protocolo utilizado para transferência de ficheiros na Internet;
- *hypertext transfer protocol* (HTTP) – protocolo utilizado para transferência de documentos HTML.

O modelo TCP/IP está estruturado em quatro camadas (ver figura na página seguinte):

- Aplicação;
- Transporte;
- Rede;
- Interface à rede.

Figura A.1
Estrutura do modelo TCP/IP



A camada superior – camada de aplicação – é responsável por permitir que as aplicações possam comunicar através de *hardware* e *software* de diferentes sistemas operativos e plataformas. Muitas vezes este processo é chamado de cliente-servidor. A aplicação cliente está em geral num equipamento mais simples e com uma boa interface com o utilizador. A aplicação envia requisições à aplicação servidor, que normalmente está numa plataforma mais robusta e tem capacidade para atender várias requisições diferentes de clientes diferentes. Alguns exemplos de aplicações são o HTTP e o FTP.

A camada seguinte – camada de transporte – tem a função de começar e terminar uma ligação, controlar o fluxo de informação, efectuar processos de correcção e verificação de erros de pacotes e ainda segmentar mensagens e reagrupar pacotes. Os principais protocolos desta camada são o TCP e o UDP.

A camada de rede é responsável por encaminhar os pacotes desde a origem até ao destino, atribuir endereço de rede ao sistema e verificar a validade dos pacotes recebidos. Tem ainda a função de ligação entre as camadas superiores e o *hardware*. O protocolo de rede mais utilizado é o IP.

A primeira camada – camada de interface à rede – fornece os meios físicos que permitem o fluxo de informação entre dois computadores. Os meios de telecomunicação mais utilizados são:

- *Ethernet* – tecnologia de ligação de redes locais (*local area networks* – LAN);
- WIFI – tecnologia de ligação de rede sem fios.

Na Internet, os protocolos utilizados são o TCP na camada de transporte e o IP na camada de rede.

Í N D I C E