Segurança em Redes de Comunicação

Fernando António D. F. Cozinheiro, Nelson Pacheco da Rocha

***Resumo* – O presente artigo tem como objectivo principal a identificação dos riscos potenciais associados à utilização distribuída de meios informáticos e ao acesso a sistemas de informação, e as possíveis soluções que minimizem os riscos de segurança. Na parte final são apresentados alguns aspectos particulares dos sistemas de segurança adoptados pela Universidade de Aveiro (UA).**

***Abstract* – This paper aims to present the risks associated with the use of distributed computing environments and with the access to information systems, identifying the solutions currently available that could minimise them. At the end, some cases of study are presented, using real security implementations adopted by Universidade de Aveiro (UA).**

I. INTRODUÇÃO

O problema da segurança informática deve ser colocado a vários níveis, desde os vírus informáticos, à ocupação de áreas de trabalho alheias, passando pela adulteração da identidade de utilizadores, pela "escuta" de comunicações ou mesmo pela segurança física do pessoal, instalações e suportes lógicos. A adopção de medidas de segurança não pode ser feita de uma forma parcelar, pois na realidade a ruptura de uma das vertentes da segurança de um sistema poderá comprometer a segurança do sistema na sua totalidade. A época actual pode ser caracterizada por uma dependência crescente face às tecnologias de comunicação, motivando a busca contínua das soluções que proporcionem maior facilidade de utilização dos serviços e, simultaneamente, permitam os melhores fluxos de informação. Interessa também automatizar ao máximo todos os processos e minimizar os recursos necessários à manutenção do bom funcionamento dos serviços. É ainda necessária a existência de um compromisso entre a facilidade de acesso aos diversos serviços de comunicação e a segurança dos sistemas instalados em redes privadas, por forma a evitar a sua exposição a ataques oriundos de utilizadores externos ou desencadeados internamente.

O perigo para as instituições agudiza-se ainda mais pelo facto dos problemas de segurança introduzidos por um qualquer utilizador local poderem comprometer a segurança dos recursos da instituição na sua totalidade. Não se pense, no entanto, que os problemas de segurança se colocam apenas ao nível das ligações remotas, pois esse tipo de problemas pode também ocorrer em ligações locais. Na realidade, a utilização partilhada de sistemas, serviços ou meios de comunicação apresenta invariavelmente um grau de insegurança associado.

Tem vindo a assistir-se ao aparecimento de muitas empresas e produtos vocacionados para a manutenção de níveis satisfatórios de segurança, capazes de proporcionarem barreiras de segurança nos pontos de interligação com o exterior. Têm também sido disponibilizados diversos protocolos, suportados por uma diversidade de produtos, alguns de distribuição gratuita, capazes de garantirem o sigilo nas ligações entre sistemas, recorrendo à utilização de chaves de criptografia. Por outro lado, algumas aplicações existentes, tais como o WWW (World Wide Web), deixaram de considerar a segurança como segunda prioridade.

II. SEGURANÇA / INSEGURANÇA EM REDES DE COMUNICAÇÃO

O número de ataques, bem como a sua gravidade, tem vindo a aumentar significativamente, mercê da facilidade com que qualquer utilizador pode aceder a documentos de referência, contendo a definição e pormenores da implementação dos diversos protocolos de comunicação, bem como às listas de vulnerabilidades (*bugs*) detectadas nos vários sistemas e serviços. A disponibilização em domínio público de aplicações de apoio à "escuta" das comunicações (*sniffers*) tem também contribuído francamente para o aumento de utilizadores com actividades reprováveis, tendo por alvo a obtenção de informações que podem colocar em risco a segurança de alguns sistemas informáticos. A realização deste tipo de operações requer a utilização de sistemas de vigia com um estatuto especial de funcionamento (modo promíscuo). Se bem que em sistemas UNIX a reconfiguração de sistemas requeira poderes de administrador, ao nível dos computadores pessoais cada utilizador é livre de fazer o que a sua consciência lhe ditar.

Apesar de existirem outros perigos, as operações de *sniffing* são as mais preocupantes na maioria dos ambientes, pois possibilitam a gravação de conversações que recorram à infra-estrutura de comunicações. Desta forma, a insegurança no acesso a um sistema a partir de computadores pessoais, para ler ou enviar mensagens de correio, poderá manifestar-se pela possibilidade de captura do *login* e *password* de acesso, bem como pela gravação de todas as mensagens que circulam na rede. Apesar de terem sido desenvolvidos sistemas mais elaborados de

passwords, por forma a evitar a sua travessia através da rede de comunicações (Kerberos, por exemplo), ou forçar a utilização de *passwords* descartáveis (S/Key), garantindo a inofensividade da sua captura por caçadores furtivos, verifica-se que a necessidade de segurança nas comunicações ultrapassa largamente a simples defesa de *passwords*, exigindo-se assim a adopção de métodos de defesa mais eficientes.

Apesar do seu enorme potencial económico, a Internet, tal como a conhecemos hoje não possui quaisquer mecanismos intrínsecos de protecção da informação transmitida. Apesar de poderem ser utilizados *firewalls* e outros mecanismos de controlo de acessos, é extremamente simples proceder à recolha da informação que circule nos canais de comunicação ou à intercepção de chamadas (*hijacking*), sem que qualquer dos interlocutores possa detectar a intrusão. A utilização de algoritmos de criptografia nas comunicações entre sistemas, extremo-a-extremo, constitui provavelmente a forma mais segura de comunicar, permitindo a constituição de VPNs (Virtual Private Networks).

A segurança nas comunicações em redes locais apresenta geralmente formas distintas das apresentadas pelas comunicações em redes públicas, nomeadamente as seguintes:

- Os ataques internos poderão ser mais diversificados, podendo comprometer sistemas integrados em rede por diversas arquitecturas protocolares (TCP/IP, IPX, AppleTalk, NetBEUI e outras), ao passo que as ligações ao exterior, incluindo a Internet, são feitas tipicamente via TCP/IP, estando bloqueada a passagem de tráfego de quaisquer outros tipos, salvo o que é encapsulado no TCP/IP;
- Os ataques desencadeados localmente usufruem de alguma flexibilidade nas metodologias de ataque escolhidas, pois as comunicações locais são feitas normalmente sem quaisquer tipo de restrições, pelo que podem ser utilizados quaisquer portos de comunicação, excepto se os administradores desses sistemas tiverem desactivado explicitamente os portos de comunicação desnecessários;
- A existência de áreas pessoais em sistemas UNIX representa uma probabilidade considerável de sucesso nos ataques ao sistema em causa, por poderem ser utilizados nos ataques programas com vulnerabilidades, gozando de estatuto privilegiado durante o tempo de execução. Em sistemas não dotados de mecanismos de “Shadow Passwords” ou TCB (Trusted Computing Base), é ainda possível a confrontação de *passwords* criptografadas, sem quaisquer restrições, com *passwords* constantes em dicionários disponíveis publicamente ou criados pelos utilizadores, sendo designada por *cracking* esse tipo de operações.

Em termos de prevenção e combate a ataques de segurança gerados em redes locais, existem, no entanto, formas ímpares, nomeadamente pelo facto da determinação das identidades dos autores de ataques poder apresentar níveis de certeza superiores, e simultaneamente por ser substancialmente mais rápida a adopção de sanções. A reacção ou aplicação de sanções contra utilizadores externos, mesmo quando confirmadas as proveniências dos ataques desencadeados, apresenta significativos níveis de dificuldade na concretização e são geralmente exageradamente morosos.

I. REQUISITOS DE SEGURANÇA

A adopção de medidas, visando o aumento da segurança na comunicação entre sistemas, deve ser norteada pela necessidade de satisfazer os requisitos a seguir descritos [1]:

- Autenticação: Diz respeito à prova da identidade, sendo esta realizada tipicamente recorrendo a um *login* e a uma *password*, ou mesmo a um dispositivo de *hardware*. Constata-se que uma grande parte dos serviços actualmente disponibilizados nas redes públicas de comunicações não recorrem a mecanismos de autenticação, e mesmo os que o fazem utilizam processos bastante simples, frequentemente ultrapassados por utilizadores menos escrupulosos;
- Controlo de acessos: Tem a ver com a permissão ou negação de acesso de utilizadores a sistemas, periféricos ou a objectos lógicos (directório ou serviços num sistema remoto, por exemplo). Ao nível das comunicações via TCP/IP, não existe qualquer norma universal, variando de acordo com a implementação do serviço. O controlo de acessos baseado na identidade dos utilizadores depende dos mecanismos de autenticação existentes;
- Integridade: Relaciona-se com a necessidade de assegurar que as informações acedidas viajam sem alterações desde o servidor até ao utilizador final, ou que as mensagens trocadas entre quaisquer utilizadores se mantêm inalteradas durante todo o trajecto. A violação da integridade pode verificar-se a vários níveis, desde a alteração de mensagens de correio trocadas entre utilizadores, ou até processos mais sofisticados de intercepção de pacotes trocados entre sistemas aquando do estabelecimento de ligações, resultando na apropriação de ligações alheias [2];
- Confidencialidade: Diz respeito com o estabelecimento de garantias de inviolabilidade, em termos de consulta ou leitura da informação trocada entre utilizadores ou sistemas. O risco de falta de confidencialidade é bem patente no serviço de correio electrónico, por exemplo, pois as mensagens passam por vários sistemas sob a forma de envelopes abertos, estando sujeitas a eventuais interferências de administradores de sistemas com níveis de ética duvidosos. O perigo existe também na troca de mensagens dentro de um sistema, pois as mensagens passam por filas de espera (*spool*) e

são depositadas em caixas de correio (*mailboxes*). Os riscos de quebra de confidencialidade são também altamente prováveis em quaisquer outros serviços (FTP / File Transfer Protocol, WWW, TELNET, ou outros), bastando recorrer a um dos muitos programas em domínio público com capacidade de "escuta" (*sniffing*). Se bem que nem todas as informações trocadas entre utilizadores ou sistemas careçam do mesmo nível de confidencialidade, algumas há que requerem confidencialidade absoluta, tais como o fornecimento de números de cartões de crédito ou a introdução de *passwords* de acesso a sistemas ou serviços.

I. MECANISMOS DE AUTENTICAÇÃO

De uma forma geral, a autenticação é vista na perspectiva da utilização de *passwords*. Embora estas sejam de facto utilizadas na maioria das situações, existem actualmente variadíssimas técnicas de autenticação.

A. Kerberos

O sistema Kerberos foi desenvolvido pelo projecto Athena, conduzido pelo MIT. Os seus objectivos principais foram a disponibilização de mecanismos de autenticação e criptografia, recorrendo a alterações em programas de comunicações, clientes e servidores. A autenticação é feita de forma distribuída, recorrendo a mecanismos bastante robustos. Outros requisitos a realçar, impostos aquando do seu desenvolvimento, foram os seguintes [2]: permitir a autenticação em um ou em ambos os sentidos; possibilitar a autenticação sem a necessidade de troca de *passwords* nos canais de comunicação; dispensar a existência de *passwords* sobre a forma não codificada em quaisquer dos ficheiros intervenientes; exigir um mínimo de esforço na conversão de qualquer programa de comunicações.
Apesar de todos estes ambiciosos objectivos, o Kerberos teve algumas dificuldades de aceitação, numa primeira fase, essencialmente pelos seguintes motivos:

- Exige programas-cliente e servidor adaptados, pelo que limita a gama de escolha de aplicações pelos administradores de comunicações e utilizadores;
- A configuração e manutenção do sistema distribuído Kerberos é árdua. A complexidade aumentará ainda mais se o sistema operativo não suportar de origem o Kerberos, ou se não existir qualquer solução comercial disponível, pois exigirá um volume de trabalho bastante superior ao exigido por outras soluções;
- O sistema Kerberos não é facilmente escalável, pois requer a utilização de chaves independentes por cada par de sistemas sujeitos a interligação. Assim, o número de chaves a atribuir está sujeita a um crescimento geométrico.

A adopção da versão 5 do Kerberos no DCE (Distributed Computer Environment), pela Open Software Foundation, constitui uma das etapas mais significativas da sua existência, podendo ser a causa da sua adopção generalizada. A disponibilização recente do Kerberos em domínio público pode ser o impulso determinação nesse sentido [4].

A. Smart Cards

A autenticação de utilizadores com base em *passwords* proporciona níveis de segurança bastante reduzidos, existindo inúmeras situações passíveis de serem exploradas por utilizadores menos bem intencionados. Basta pensar, por exemplo, na existência de programas em execução num computador pessoal, com capacidade de memorização de todas as entradas por teclado ou dos caracteres exibidos no écran.
A introdução de um nível de segurança adicional poderá ser conseguida através da utilização de sistemas baseados em *Smart Cards*. Embora bastante limitadas, começam já a existir disponíveis algumas soluções comerciais e a sua utilização de cartões irá certamente ter uma evolução bastante significativa nos tempos vindouros, pois o governo americano impôs recentemente como obrigatório o uso do Fortezza [5] para os utilizadores Internet do governo federal. Este oferece a codificação de dados em volume, por forma a permitir a privacidade nas comunicações, utilizando chaves de codificação robustas, e ao mesmo tempo permite a autenticação dos utilizadores recorrendo à associação de dois elementos identificativos: palavra-chave, ou PIN, e cartão magnético.

B. TACACS / RADIUS

O TACACS, definido no documento [6], é um protocolo de autenticação de utilizadores perante equipamentos de comunicações (encaminhadores ou servidores de terminais, por exemplo), podendo ser feito o registo das actividades de autenticação. O XTACACS (Extended TACACS) representa uma evolução do seu antecessor. Em qualquer dos casos, o método de autenticação consiste na utilização de um *login* e de uma *password*, os quais são fornecidos pelo utilizador imediatamente após o estabelecimento do canal de comunicação, sendo este par de informações enviado de imediato a um servidor de autenticação, o qual tem o respectivo *daemon* em permanente execução.
Tendo em vista obter informações mais detalhadas sobre as actividades realizadas por utilizadores em ligações remotas, por forma a poder efectuar-se a afectação de custos, a Livingston Enterprises Inc. desenvolveu o RADIUS (Remote Access Dialup User Service), um sistema com funcionalidades idênticas às apresentadas pelo TACACS e XTACACS, se bem que em número acrescido.

C. PAP / CHAP

A autenticação de ligações realizadas por PPP (Point-to-Point Protocol), recorrendo a *modems* sobre linhas assíncronas ou por RDIS (Rede Digital com

Integração de Serviços), é possível recorrendo a dois protocolos: PAP (Password Authentication Protocol) e CHAP (Challenge-Handshake Authentication Protocol) [7]. Nos casos em que a negociação do protocolo de autenticação é possível, deve ser feita a tentativa de utilização do CHAP prioritariamente, por apresentar atributos mais robustos de autenticação.

O PAP disponibiliza um mecanismo simples de identificação entre sistemas, baseado numa operação em dois passos, sendo utilizado imediatamente após o estabelecimento do canal de comunicação (*Link Establishment*). O sistema cliente envia sucessivamente pares de informação do tipo *login* / *password* até que o servidor seja capaz de autenticar o sistema cliente ou até que a ligação seja desactivada por esgotamento do período de tempo previsto para a fase de autenticação. Uma das principais limitações do PAP consiste no facto das *passwords* viajarem entre os sistemas cliente e servidor sem qualquer tipo de criptografia, podendo ser capturadas em operações de *sniffing*. Esta limitação pode ser ultrapassada no caso de ser suportada a utilização de *passwords* descartáveis (*one-time passwords*).

O CHAP é utilizado para verificar periodicamente a identidade dos sistemas clientes, utilizando um mecanismo em três passos: Depois de estabelecido o canal de comunicação, o sistema servidor envia uma chave (*challenge*) para o sistema cliente (*peer*); utilizando uma função "one-way hash", o sistema cliente responde ao servidor; finalmente, este confronta a resposta devolvida pelo sistema cliente com o resultado dos seus próprios cálculos.

I. CONTROLO DE ACESSOS

O controlo de acessos pode verificar-se a vários níveis, quer ao nível dos sistemas informáticos, quer ao nível dos equipamentos de comunicações.

A. Controlo de Acessos a Sistemas UNIX

O controlo de acessos a sistemas UNIX, em termos dos serviços requeridos ou dos sistemas clientes, pode ter como resultado a introdução de um nível de segurança adicional. A maioria das implementações dos programas-servidores (*daemons*) não possui mecanismos intrínsecos para o controlo de acessos. A solução consiste em utilizar um programa especial, suficientemente genérico, capaz de proceder ao atendimento de ligações aos serviços controlados e de as passar aos verdadeiros programas-servidores, depois de verificadas as permissões de acesso.

O programa **inetd** é utilizado tipicamente como activador dos programas-servidores à medida que surgem os pedidos de acesso aos respectivos serviços. Este modo de funcionamento permite a realização de algumas actividades de apoio à manutenção da segurança: registo da origem e data das ligações; controlo de acessos a serviços com base na identificação do sistema de origem.

O programa **tcp-wrapper** tem funções idênticas às do programa **inetd**, mas possui características adicionais interessantes, tais como a possibilidade de execução do programa **finger** em sentido inverso (isto é, na direcção do sistema cliente). Dessa forma, permite a obtenção de informações sobre a identidade dos utilizadores presentes no sistema cliente, aquando do estabelecimento ou tentativa de estabelecimento de ligações. Permite ainda proceder ao envio de mensagens de aviso, sempre que se verifiquem tentativas de acesso não autorizadas [8].

B. Firewalls

Com o objectivo de reduzir ao mínimo o número de sistemas acessíveis a partir do exterior, é vulgar a existência de duas zonas de rede, com mecanismos de protecção bem distintos: uma zona pública, exposta a possíveis tentativas de ataque a partir de redes externas, onde se encontram instalados tipicamente servidores de informação e uma zona protegida por sistemas do tipo *firewall*, por forma a minimizar acessos estranhos a partir do exterior (ver Fig. 1).

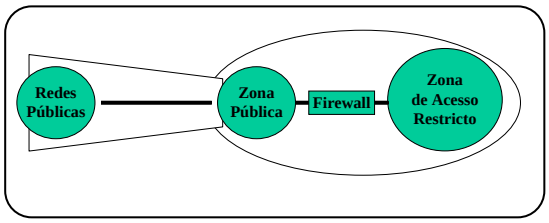

Fig. 1 – Zonas de segurança

O objectivo de um *firewall* é o de possibilitar níveis de isolamento das redes locais em relação a redes externas, por forma a inibir o acesso aos serviços ou recursos privados. Atendendo ao facto da Internet ter o TCP/IP como base, a maioria dos sistemas de *firewall* existentes destinam-se ou estão configurados para desempenhar as funções de controlo de acessos apenas para esta arquitectura protocolar. A ausência de quaisquer *firewalls*, expõe todos os sistemas de uma rede interna a ataques provenientes do exterior.

Os sistemas do tipo *firewalls* em uso podem ser classificados em três tipos [9], por interagirem a níveis distintos da arquitectura protocolar e por apresentarem formas de funcionamento distintos, sendo que, na maioria dos casos, as instituições optam pela adopção de uma solução baseada na conjugação dos vários tipos de *firewalls*:

- Packet Filter Gateways: Trata-se de um sistema que transmite pacotes de informação entre duas ou mais interfaces. As capacidades de filtragem são possíveis graças à existência de um nível adicional de código no seu *kernel*, que lhe permite realizar uma série de confrontações com uma lista de regras, por forma a decidir-se pelo encaminhamento ou pelo simples bloqueamento de pacotes;
- Application-Level Gateways: Este tipo de sistemas requer programas-servidores (*daemons*) especiais,

por cada uma das aplicações a suportar, em substituição dos tradicionais (**telnetd** ou **ftpd**, por exemplo). Embora podendo parecer menos funcional, este tipo de *firewalls* proporciona níveis superiores de segurança. Além disso, em alguns ambientes, permite o registo de actividade. Por último, introduz facilidades acrescidas de controlo das comunicações a partir do exterior ou para o exterior, recorrendo a protocolos de autenticação, podendo ser estabelecidos mecanismos de permissão por utilizadores;

- Circuit-Level Gateways: O recurso a este tipo de *firewalls* não requer a utilização de diversos portos de comunicação, de acordo com a aplicação a utilizar, conforme acontecia no caso anterior, bastando a ligação a um único porto de comunicação, bem definido. Uma vez ultrapassados os formalismos de autenticação, o tráfego da informação processa-se transparentemente entre os sistemas de origem e destinatários da comunicação. Poder-se-á dizer que a utilização deste tipo de *firewalls* é bastante mais simples. Esta simplificação exige no entanto que as aplicações utilizadas sejam desenvolvidas de acordo com determinadas especificações.

A. Servidores de Proxies

Os servidores de *proxies* podem operar a vários níveis, permitindo maior ou menor liberdade na escolha dos programas de comunicação utilizados [10], sendo considerados ao nível dos "Application-Level Gateways" ou "Circuit-Level Gateways". O modo de funcionamento pode diferir entre servidores, apesar do objectivo ser a disponibilização de canais de comunicação entre os sistemas locais a uma organização e os sistemas externos, por forma a minizar os riscos de ataque. Poderão também ser utilizados com tarefas complementares, tais como: armazenamento (*caching*) da informação transferida, filtragem da informação entrada ou saída, registo de ligações.

Ao nível do controlo de acessos, as soluções mais conhecidas baseiam-se na utilização das implementações do protocolo SOCKS (versões 4 ou 5) ou do FWTK (Firewall Toolkit da Trusted Information Systems). A primeira destas soluções proporciona um nível de transparência praticamente total, pois a identificação do sistema e/ou do utilizador é efectuada automaticamente. A solução baseada no FWTK implica uma identificação mais convencional, tendo no entanto a vantagem de poder ser utilizado qualquer programa-cliente. Existe ainda um número bastante significativo de implementações comerciais.

B. Listas de Acessos

O funcionamento dos encaminhadores com listas de acesso activas pode ser considerado como ao nível dos "Packet Filter Gateways", podendo o seu comportamento ser controlado com base nos endereços de origem e destino, nos portos de comunicação (aplicações) utilizados pelos sistemas servidores e clientes, podendo utilizar-se nas comunicações baseadas em diferentes arquitecturas protocolares: TCP/IP, Novell IPX, AppleTalk, e outros.

No caso de sistemas com funções de filtragem em ambientes TCP/IP, utilizados tipicamente na interligações de instituições à Internet, o bloqueamento de pacotes é realizado com base nos endereços IP ou nos números dos portos de comunicação associados (para os protocolos que suportam a noção de portos) [11], de origem ou de destino. A decisão pode ainda ser tomada com base no tipo de pacote: UDP, TCP, ICMP (Internet Control Message Protocol), etc. De uma forma geral, as regras são aplicadas fora de qualquer contexto, sendo as decisões tomadas com base no conteúdo de cada um dos pacotes em circulação. Dependendo do tipo de encaminhadores em utilização, é ainda possível proceder à filtragem com base no sentido da comunicação, isto é, utilizando os sentidos de entrada ou saída dos pacotes.

As listas de acesso consistem numa enumeração de condições, com as quais são confrontados cada um dos pacotes que cruzam a interface nas quais se encontram activas, sendo a análise feita sequencialmente, até que uma das condições especificadas seja aplicável ao pacote cuja permissão de passagem se encontre em circulação. As condições especificam claramente qual o tráfego permitido ou proibido.

As listas de acesso podem ser elaboradas com duas perspectivas diferentes:

- Proibir as ligações com origem ou destinos específicos, por apresentarem riscos inerentes bem conhecidos, permitindo todas as ligações restantes;
- Permitir apenas as ligações consideradas aceitáveis, tanto em termos de origem, como em termos de destino, proibindo todas as restantes.

I. CONFIDENCIALIDADE E INTEGRIDADE

Uma percentagem significativa de ataques a sistemas informáticos recorre a informações capturadas. Importa, pois, garantir a confidencialidade das informações que circulem nas redes de comunicações ou armazenadas em sistemas, adoptando as soluções convenientes.

A solução para a criptografia nas comunicações pode ser efectuada de duas formas: ao nível de uma das camadas protocolares intermédias ou ao nível da aplicação. Embora sendo a menos satisfatória, a solução mais frequente é baseada na criptografia ao nível da aplicação, pois não requer modificações significativas nos sistemas operativos, quase sempre dependentes dos fabricantes. Essa facilidade será incluída intrinsecamente na próxima geração do protocolo IP (IPv6, também designada por IP Next Generation), sob a designação IPsec, podendo mesmo afirmar-se que a utilização da criptografia será feita automaticamente, sem que o utilizador tenha que a activar. Até lá, a solução consiste na utilização de aplicações com facilidades de criptografia, recorrendo ou não a técnicas convencionais, baseadas na existência de

um par de aplicações complementares: cliente e servidor. Daí resulta a inexistência de soluções globais, utilizáveis nas mais diversas plataformas informáticas. No entanto, existem já algumas iniciativas que visam disponibilizar as facilidades do IPsec na versão actual do IP.

A. Acesso a Sistemas de Informação

As evoluções mais recentes, poderão vir a fazer da Internet a plataforma por excelência para a realização de negócios, incluindo operações bancárias, sendo para tal necessário garantir níveis de segurança e privacidade adequados. Eis as soluções disponíveis para o WWW:

- SSL é um protocolo de criptografia que opera a baixo nível, podendo por isso ser utilizado na criptografia de comunicações realizadas por protocolos de alto nível, tais como o HTTP (HyperText Transfer Protocol), o NNTP (NetNews Transfer Protocol) ou o FTP. Possui mecanismos de autenticação do servidor, criptografia da informação circulada e autenticação de sistemas clientes. A utilização das facilidades de autenticação requer a obtenção de certificados, junto de organismos reconhecidos (Certifying Authorities) [12].
- protocolo S-HTTP (Secure HTTP) está disponível na implementação derivada do servidor da NCSA (National Center for Supercomputer Applications). Trata-se de um protocolo de alto nível, utilizável apenas com o HTTP. Apesar de possuir um conjunto de características mais rico do que o apresentado pelo SSL, tem tido pouca aderência, provavelmente pelo facto da Netscape Communications Corporation ser uma das empresas líderes no mercado dos *browsers* de WWW [13].
- SET (Secure Electronic Transactions), constitui a solução mais evoluída de criptografia ao nível do WWW, sendo utilizado na Internet como suporte à realização de transacções económicas.

A. Sessões de Trabalho Remoto

Nas sessões de trabalho remoto é aconselhável o recurso a facilidades de criptografia, por forma a minimizar a probabilidade de apropriação por terceiros dos elementos (*login* / *password*) utilizados no controlo de acessos.

O conjunto **F-Secure SSH**, constitui uma das soluções mais abrangentes, permitindo o estabelecimento de ligações remotas seguras sobre redes de comunicações públicas / partilhadas, podendo considerar-se como uma evolução do protocolo TELNET. Pode também ser utilizado para a criação de servidores de *proxies* locais, por forma a garantir a segurança nas comunicações baseadas em outros protocolos: POP (Post Office Protocol), SMTP (Send Mail Transfer Protocol), HTTP, e outros. Neste caso, os servidores aguardam por ligações nos portos de comunicação apropriados, reenviando o pedido de interligação ao sistema remoto, garantindo que a troca de dados da comunicação propriamente dita se efectua através de um canal seguro [14].

Existem ainda outras alternativas, se bem que bastante mais limitadas em termos de funcionalidades: SSL-telnet e SSL-ftp, NetCrypto e outros. Qualquer uma das soluções requer a utilização de programas-servidores específicos e respectivos programas-cliente.

B. Correio Electrónico

A troca de mensagens entre utilizadores por correio electrónico pode ser feita com segurança, utilizando um dos protocolos existentes: PEM ou PGP [15]:

- De uma forma sucinta, as características principais do PEM (Private Enhanced Mail) são as seguintes: a confidencialidade, recorrendo à utilização de chaves públicas e privadas; a manutenção da integridade de mensagens; a autenticação do remetente a terceiros, recorrendo a assinaturas digitais das mensagens [2];
- Numa primeira análise, poder-se-á dizer que o PGP (Pretty Good Privacy) [16] e o PEM disponibilizam funcionalidades idênticas: autenticação, integridade, criptografia e autenticação do remetente a terceiros. A grande diferença entre ambos reside no facto do PEM recorrer a uma hierarquia bem definida de registo de chaves, feita junto de entidades oficiais, enquanto o PGP deixa a recolha de assinaturas e o seu registo numa base pessoal (*keyrings*) ao encargo do utilizador [2, 13]. Esta flexibilidade foi o ponto forte na adopção generalizada do PGP, para troca de mensagens pessoais.

A utilização das facilidades disponibilizadas por ambas as soluções não requer quaisquer modificações nos programas-servidores de correio electrónico, pois isso fica ao encargo dos programas utilizados na leitura e expedição de mensagens ou por aplicações externas.

I. CASOS DE ESTUDO: SEGURANÇA NA UA

A UA tem vindo a implantar uma infra-estrutura de comunicações diversificada e a reforçar a sua capacidade de interligação ao exterior, visando servir toda a Comunidade, incluindo as áreas administrativas, educacionais e de investigação. Em termos de evolução, tem recorrido sucessivamente à utilização das tecnologias Ethernet, FDDI e SMDS, encontrando-se em vias de migrar total ou parcialmente para Fast Ethernet e ATM. A existência destas tecnologias tem permitido a constituição e o acesso a diversos serviços e a introdução de tecnologias de suporte à difusão de audio ou vídeo.

A disponibilização de mecanismos de segurança na UA tem sido norteada pelos seguintes objectivos:

- Disponibilização de mecanismos de criptografia, para comunicações entre sistemas;

- Constituição de servidores intermediários (*proxies*), para suporte às comunicações entre sistemas internos e sistemas externos;
- Criação de servidores para autenticação de utilizadores;
- Activação de mecanismos de sistemas de rastreio e registo de actividades suspeitas, por forma a recolher informações de apoio à identificação de ataques, e respectiva resolução.

A. Interligação da UA com o Exterior

Na UA, o XTACACS (Extended TACACS) é utilizado no controlo de acessos por SLIP (Serial Line Internet Protocol) / CSLIP (Compressed Serial Line Internet Protocol) / PPP (Point-to-Point Protocol) através de linhas telefónicas comutadas e no controlo de acessos aos encaminhadores instalados em diversos pontos da rede do Campus Universitário. Os protocolos PAP (Password Authentication Protocol) e CHAP (Challenge-Handshake Authentication Protocol) são utilizados na autenticação de sistemas em ligações do tipo RDIS.

A ligação da UA à RCCN e através desta à Internet, é feita através do CICUA, recorrendo a um conjunto de equipamentos especiais. O canal de interligação é suportado por uma ligação SMDS (Switched Multimegabit Data Service), operando a 2 Mbps, prevendo-se que em breve venha a ser reforçada esta capacidade. A Fig. 2 apresenta uma diagrama esquemático da interligação da UA com o exterior.

De uma forma sucinta, o esquema de interligação da UA com o exterior pode ser assim caracterizado:

- A interligação entre as redes Ethernet de *backbone*, FDDI e ATM é feita no encaminhador GTUA, instalado no CICUA. Este encaminhador recebe ainda o troço de rede onde se encontram instalados os equipamentos receptores de ligações SLIP/PPP e RDIS, exercendo ainda as funções de gestor de controlo de acessos (GTACL);
- O acesso ao exterior é feito de uma forma controlada, por questões de racionalização dos limitados recursos de interconexão com o exterior e por forma a garantir um nível de segurança aceitável para os sistemas informáticos instalados no Campus, utilizando os encaminhadores GTACL e GTEXT;
- De uma forma geral, o acesso ao exterior apenas é possível através dos servidores de *proxies* e de *caching* instalados, suportados pelos sistemas com as designações PROXY1 e PROXY2, estando o acesso a estes condicionados por limitações geridas pelo encaminhador GTACL ou ao nível dos próprios servidores de *proxies*;
- O encaminhador GTEXT, por defeito, limita-se a bloquear a passagem do tráfego directo para o exterior de todos os sistemas, a menos do tráfego trocado com o exterior (nos sentidos de entrada ou saída) por alguns sistemas de informação ou por sistemas com funções especiais;
- Os sistemas com acesso à UA (por SLIP / CSLIP / PPP, RDIS, ou mesmo TCP/IP sobre X.25) estão sujeitos ao mesmo tipo de restrições impostas aos sistemas instalados nas diversas redes locais, pois os encaminhadores que acolhem esse tipo de chamadas estão colocados a montante do sistema com funções de controlo de acessos (GTACL).

Por forma a garantir níveis mais adequados de segurança para os sistemas instalados na UA, as ligações entre a UA e o exterior têm vindo a ser suportadas por diversos

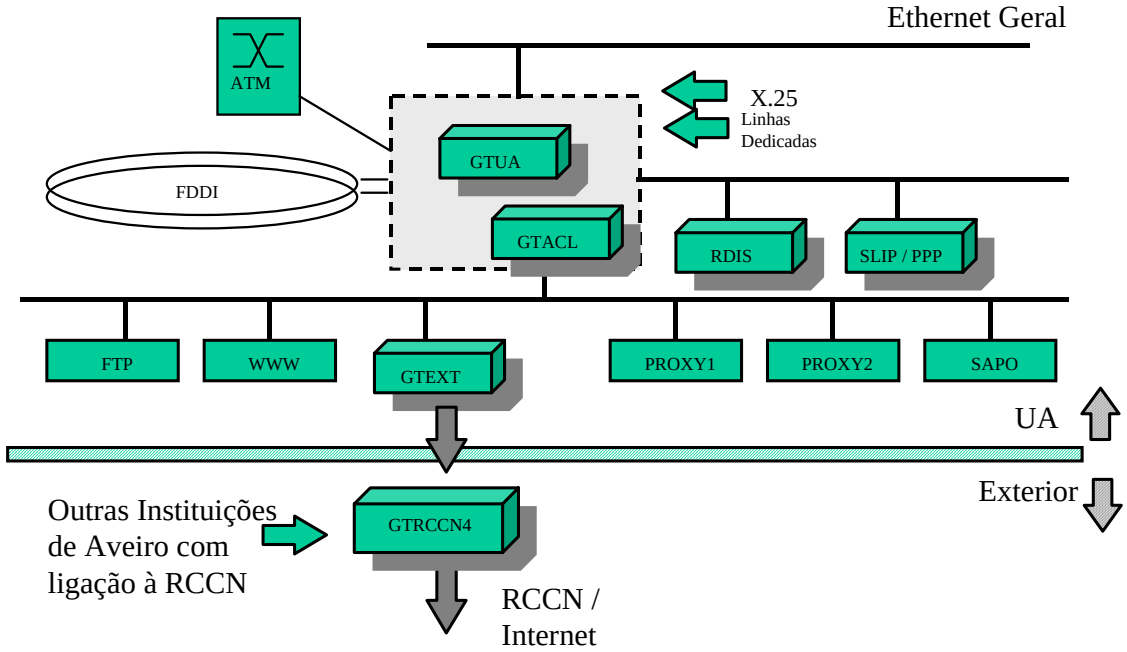

Fig. 2 – Diagrama da interligação com exterior

servidores intermediários (*proxies*). Complementarmente, e dependendo da solução em uso, poderá ainda ser efectuado o armazenamento de informações públicas (*caching*), acedidas tipicamente por *browsers* de WWW, tendo por objectivo a sua disponibilização para outros utilizadores que as requeiram, dispensando-se a necessidade de transferir as mesmas informações tantas vezes quantas as solicitadas.

A. Acesso aos Serviços Administrativos

O acesso a aplicações / sistemas instaladas nos Serviços Administrativos da UA, a partir de sistemas instalados em locais bem concretos (tipicamente secretarias) dos diversos Departamentos, Secções Autónomas, Serviços visou criar condições de utilização distribuída, minimizando a necessidade de deslocação de pessoas. A solução actual consiste na utilização de diversas aplicações e equipamentos [17].

O SSH permite o estabelecimento de ligações remotas seguras sobre redes de comunicações públicas, comportando-se como um substituto do protocolo TELNET, sendo dotado de mecanismos de segurança ao nível da criptografia e autenticação.

A capacidade de recepção de listagens por impressoras instaladas nas diversas secretarias, geradas ao nível do servidor, fazendo uso das facilidades de impressão remota disponibilizadas genericamente por sistemas UNIX, é possível pela utilização de uma aplicação informática específica, a instalar nos computadores clientes (RPM / Remote Print Manager).

Por último, e por forma a garantir índices de imunidade satisfatórios dos sistemas clientes, tendo em vista impossibilitar a instalação de *sniffers* de teclado do tipo TSR, sugere-se a adopção do Microsoft Windows NT 4.0 (versão *workstation*). A utilização deste sistema operativo ao nível dos sistemas clientes, garantirá facilidades de administração acrescidas, por impossibilitar desconfigurações do conjunto.

A solução adoptada apresenta, pois, múltiplos níveis de segurança:

- Acesso a computadores pessoais controlado, recorrendo às facilidades disponibilizadas pelo Microsoft Windows NT 4.0 Workstation, baseadas na utilização de *login* / *password* individuais;
- Controlo de acessos por endereços IP ao nível do encaminhador instalado no ponto de interligação entre a rede local dos Serviços Administrativos e a rede geral do Campus universitário;
- Confrontação de endereços IP com endereços físicos (MAC *addresses*) de placas de rede, ao nível do encaminhador referido no ponto anterior;
- Autenticação de sistemas clientes e servidores (protocolos RSA);
- Autenticação de utilizadores por *login* / *password* ou por processos alternativos (protocolos RSA);
- Criptografia extremo-a-extremo (protocolos IDEA, DES, 3DES);
- Acesso ao sistema informático central por *login* / *password*, individuais ou departamentais;
- Acesso às aplicações informáticas *login* / *password;*
- Criptografia extremo-a-extremo (protocolos IDEA, DES, 3DES).

A. Gestão Descentralizada de Sistemas de Informação

O servidor de WWW da UA pretende servir os Departamentos / Secções / Serviços com interesse em disponibilizar informação por HTTP, e tem o FreeBSD (uma variante do UNIX) como sistema operativo de base. Com a proliferação de editores de HTML para computadores pessoais, torna-se evidente que há todo o interesse em que a manipulação das informações se faça directamente em ambientes baseados nas diversas variantes do MS Windows.

Uma das soluções seria proceder à exportação das diversas áreas de informação, utilizando o protocolo NFS (Network File System). Esta solução apresentaria alguns problemas de segurança, além de alguma falta de flexibilidade em termos do controlo das hierarquias de directórios exportadas.

Apesar da estrutura de informação não ser a mais adequada para uma gestão descentralizada, já é possível parcialmente, tendo por base o servidor SAMBA e de alguns programas complementares, incluídos no conjunto. Desta forma, em vez de serem os PCs a ter que suportar os protocolos elaborados (NFS, por exemplo), o SAMBA permite exactamente o inverso, fazendo com que as hierarquias exportadas por este sejam vistas como um *drive* nos PCs. Em termos de segurança, o SAMBA permite níveis de segurança superiores aos proporcionados por outros mecanismos de partilha de recursos, nomeadamente através do recurso a *passwords* (criptografadas ou não), autenticação ou a execução de operações nos *file systems* com o UserID do utilizador.

B. Registos de Actividade

Nos casos em que os ataques à segurança de sistemas sejam desencadeados a partir de outros sistemas, a análise dos processos utilizados poderá ser facilitada se existirem mecanismos de sincronismo dos relógios em uso por todos os sistemas. Essa facilidade é disponibilizada pelo SNTP (Simple Network Time Protocol) [18]. A utilização de servidores deste tipo, além de proporcionar um sincronismo horário entre os sistemas, permite ainda um nível de rigor considerável em termos de funcionamento dos próprios relógios internos dos sistemas, sendo o erro da ordem de milésimos de segundo relativamente a servidores mundiais de referência.

Os actuais sistemas UNIX ou mesmo encaminhadores possuem mecanismos de *logging*, normalmente suportados pelo programa-servidor **syslogd**, podendo as informações de registo de actividades ser passadas a servidores centrais, por forma a garantir o armazenamento

de informações de apoio ao diagnóstico dos ataques. É típica a remoção dos rastos dos passos utilizados em ataques bem sucedidos, por forma a dificultar as operações com vista à identificação da origem dos ataques, dos *logins* utilizados ou das vulnerabilidades exploradas. A utilização de sistemas de registo centrais dificulta claramente a remoção de quaisquer rastos pelos atacantes, pois os registos são feitos à medida que ocorrem os acontecimentos dignos de registo, e a remoção desses registos requer a permissão de acesso com estatuto privilegiado ao servidor de registo central.

I. ALGUMAS CONSIDERAÇÕES FINAIS SOBRE SEGURANÇA

Conforme referido anteriormente, a actual versão do IP (IPv4) em uso na Internet enferma de alguns problemas de segurança sérios por não dispor de mecanismos de autenticação e criptografia abaixo do nível da aplicação. A resolução dos problemas nas comunicações será reduzido significativamente pela inclusão no IPv6 de dois mecanismos integrados, capazes de garantir níveis mínimos de segurança, sendo designados respectivamente por "IP Authentication Header" e "IPng Encapsulation Security Header" [19]. Enquanto o primeiro mecanismo proporciona autenticação e integridade (sem confidencialidade), o segundo oferece a integridade e a confidencialidade aos datagramas IPv6.

Apesar de ser notório o aparecimento de variadas soluções, há que reconhecer que, por muitas melhorias que se introduzam na área da segurança dos sistemas, serviços e meios de comunicação, restará sempre uma boa parcela de segurança que dependerá do utilizador. Veja-se por exemplo a seguinte citação, incluída em [20]: *"A segurança é uma atitude mental, uma prática e uma disciplina. A sua implementação e observância é essencialmente um problema das pessoas."*

REFERÊNCIAS

[1] "Internet Firewalls and Network Security" - Karanjit Siyan, Chris Hare - News Riders Publishing, ISBN 1-56205-437-6, 1995

[2] "Actually Useful Internet Security Techniques" - Larry J. Hughes, Jr. - News Riders Publishing, ISBN 1-56205-508-9, 1995

[3] "Building Internet Firewalls" - D. Brent Chapman & Elizabeth D. Zwicky - O'Reilly & Associates, ISBN 1-56592-124-0, 1995

[4] "Implementing Internet Security" - Frederic J. Cooper, Chris Goggans, John K. Halvey, Larry Hughes, Lisa Morgan, Karanjit Siyan, William Stallings, Peter Stephenson - New Riders Publishing, ISBN 1-56205-471-6, 1995

[5] "Basic Certification Requirements for FORTEZZA Applications" - http://www.armadillo.huntsville.al.us/Fortezza_docs/draft.html - Version 1.0, 1996

[6] "An Access Control Protocol, Sometimes Called TACACS" - C. Finseth - RFC 1492, University of Minnesota, Julho/1993

[7] "PPP Challenge Handshake Authentication Protocols (CHAP)" – W. Simpson - RFC 1994, Agosto/1996

[8] "TCP Wrapper: Network monitoring, access control, and booby traps" - Wietse Venema, Eindhoven University of Technology – ftp://cert.org/pub/tools/tcp_wrappers/

[9] "Firewalls and Internet Security: Repelling the Wily Hacker" - William R. Cheswick, Steven M. Bellovin - Addison Wesley, ISBN 0-201-63357-4

[10] "Classical versus Transparent IP Proxies" - M. Chatel - RFC 1919, Março/1996

[11] "Assigned Numbers" - J. Reynolds, J. Postel - RFC 1700, Outubro/1994

[12] "The SSL Protocol" – Netscape Communications, Inc. - http://home.netscape.com/newsref/std/SSL.html

[13] "The Secure HyperText Transfer Protocol" - E. Rescorla, A. Schiffman - http://www.commerce.net/information/standards/drafts/shttp.txt

[14] "Overview of the F-Secure SSH Client Products" - White Paper - http://www.Europe.DataFellows.com/f-secure/fclinttp.htm - May 1996

[15] "E-Mail Security: How to Keep your Electronic Messages Private" - Bruce Schneier - John Wiley & Sons, Inc., ISBN 0-471-05318-X, 1995

[16] "PGP Message Exchange Formats" – D. Atkins, W. Stallings, P. Zimmermann - RFC 1991, Agosto/1996

[17] "Acesso das secretarias da U.A. à Administração: Plano de Implementação" – Fernando Cozinheiro – Centro de Informática e Comunicações / UA, 1997

[18] "Simple Network Time Protocol" – D. Mills - RFC 2030, Outubro/1996

[19] "IP Authentication Header" - R. Atkinson - RFC 1826, Agosto/1995

[20] "Segurança dos Sistemas e Tecnologias da Informação - Manual Técnico" - Jorge Ferreira, em colaboração com Sebastião Alves e Autoridade Nacional de Segurança - Instituto de Informática, ISBN: 972-96816-0-0 e 972-96837-0-0, 1995