SEGURANÇA e CONFIABILIDADE: na ordem do dia dos sistemas distribuídos

Paulo Jorge Veríssimo
[pjv@di.fc.ul.pt]
FCUL
Faculdade de Ciências de Lisboa - Bloco C5 - Campo Grande - 1700 Lisboa
Tel. 7500103, Fax. 7500084

Sumário

A presente comunicação pretende apresentar conceitos relacionados com os temas de confiabilidade, segurança e sistemas distribuídos, e avançar algumas ideias acerca daquilo que podem ser as vantagens competitivas de produtores e utilizadores de sistemas informáticos que se debrucem seriamente sobre este tipo de tecnologias.A *tolerância a faltas* deixou há muito de ser a etiqueta das centrais nucleares ou dos sistemas aviónicos. A *segurança* deixou igualmente de ser apanágio exclusivo dos sistemas militares e governamentais. A popularização destas técnicas e a crescente dependência dos utilizadores nos sistemas informáticos, tornam-nas de utilização obrigatória, sob pena de insucesso no mercado.Utilizá-las, é conseguir o tipo de vantagem competitiva que pensamos ser adequado às indústrias relacionadas com a informática no nosso País: valor acrescentado a nível sistémico.

Introdução

Quando nos sentamos à frente de um computador, temos a esperança que ele se mantenha em funcionamento o tempo suficiente para fazermos algo de útil. Sabendo que todos os sistemas falham, esperamos então que, pelo menos, esteja bastante menos tempo falhado que a funcionar. Tais propriedades denominam-se genericamente de *confiabilidade.* Fazendo sentido esta intuição, o que é estranho é a inquebrantável fé que parecemos depositar nessa confiabilidade dos sistemas informáticos, sem que tenhamos feito o suficiente--- tecnicamente falando, claro--- para a assegurar. Esta atitude leva amiúde a consequências que se manifestam na forma de meros dissabores ou indisponibilidades--- a maior parte das vezes--- a perdas avultadas de dinheiro--- menos frequentemente--- ou ainda--- raramente--- a perdas de vidas humanas. Infelizmente, a gravidade dos danos é inversamente proporcional à sua frequência, pelo que qualquer dos cenários acima é indesejável. Em Portugal, interessam-nos mais os dois primeiros, uma vez que há uma muito reduzida capacidade de intervenção nos poucos sectores que utilizam sistemas críticos-para-a-vida controlados por computador. Estatísticas em França, por exemplo, situam as perdas anuais (perda de produtividade, perda de negócios, perda catastrófica de informação) relacionadas com a falta de confiabilidade de sistemas informáticos em vários milhares de milhão de francos.

Por outro lado, temos tendência a encarar o conjunto de propriedades geralmente ligado à *segurança* duma forma extremamente branda, e com aquilo que se poderá designar de *ética difusa*. Isto é, como utilizadores, raramente pensamos em salvaguardar a privacidade da nossa informação, ou a dos outros à nossa guarda--- o que é mais grave. Como vendedores ou projectistas, temos tendência a pensar que os nossos produtos são extremamente seguros, com o mesmo tipo de fé inquebrantável que pomos na suposta confiabilidade dos mesmos, e que se propaga nefastamente aos utilizadores. Como terceiros, temos muitas vezes tendência a espiolhar as máquinas e os ficheiros de outrém, numa atitude que vai de mera curiosidade a um desporto, popular hoje em dia, o *hacking* ou pirataria informática, e que assume contornos muito mais obscuros que a maioria pensa. Quando algo de mau

acontece, tendemos a cair no extremo oposto, trancar tudo, o que, em informática, e nos nossos dias de comunicação global, sistemas em rede e cliente-servidor, pode ser ainda mais desastroso. Igualmente aqui, por uma razão ou outra, as consequências económicas, directas ou indirectas (ex. perdas devidas a espionagem industrial), são indesmentíveis.

Há uma terceira faceta do problema, que o vem tornando mais complicado: a explosão imparável da interligação de sistemas em rede, da telemática, dos serviços cliente-servidor, em redes locais ou na Internet. Siglas que identificam de forma popular as múltiplas facetas de uma disciplina com cada vez maior importância nas ciências e engenharias da computação: os *sistemas distribuídos*.

Porquê? Em primeiro lugar, porque em engenharia existe uma lei que define que a confiabilidade de um sistema é inversamente proporcional (quadraticamente) ao número dos seus componentes. Isto é, nas palavras jocosas de Lamport:

> *«um sistema distribuído é aquele em que somos impedidos de trabalhar devido à falha de um computador de que nunca ouvimos falar.»*

Em segundo lugar, porque se um sistema isolado já tem problemas de segurança, muito mais problemático é garantir a segurança de um sistema em rede, sobretudo em rede pública (ex. Internet), onde os acessos têm um grande grau de liberdade e anonimato.

No entanto, por estranho que pareça, os resultados de investigação nestes campos, nos últimos anos, apontam para que as soluções baseadas em sistemas distribuídos atinjam níveis de confiabilidade e de segurança bastante superiores aos dos sistemas centralizados. Esta aparente contradição explica-se por três frases simples:

- o afastamento geográfico introduz independência de falha que permite que um sistema não falhe como um todo, quando falha um ou mais dos seus componentes;
- a fragmentação do estado de um sistema em lugares diferentes permite que um intruso que penetre num só lugar não consiga controlar ou extrair informação útil;
- as técnicas (algumas sofisticadas) que permitem materializar os objectivos acima foram desenvolvidas nos anos recentes.

Existe já tecnologia de ponta nesta área, e ela continua a ser um tema de investigação. Isto é, numa perspectiva de investigação aplicada, trata-se de um excelente tema. Numa perspectiva de industrialização, tem sectores maduros que podem ser incorporados em produtos e serviços, e conseguir o tipo de vantagem competitiva que pensamos ser adequado às indústrias relacionadas com a informática no nosso País: valor acrescentado a nível sistémico.

Assim, a presente comunicação pretende apresentar conceitos relacionados com os temas em discussão: confiabilidade, segurança e sistemas distribuídos, e avançar algumas ideias acerca daquilo que podem ser as vantagens competitivas de produtores e utilizadores de sistemas informáticos que se debrucem seriamente sobre este tipo de tecnologias.

Sistemas Distribuídos

Os sistemas distribuídos são genericamente os sistemas constituídos por diversas máquinas independentes, interligadas por redes frequentemente não fiáveis e com demoras pouco previsíveis. Assim, incluem-se nesta categoria praticamente todos os sistemas e serviços sob denominações como: sistemas em rede, telemáticos, serviços cliente-servidor (bases de dados transaccionais, pesquisa, etc.), em redes locais ou na Internet.

As grandes vantagens dos sistemas distribuídos, em relação a sistemas

centralizados, residem em vários atributos:

- partilha de informação e recursos;
- relação custo/funcionalidade favorável;
- cobertura geográfica;
- fragmentação da informação;
- modularidade, expansibilidade e escalabilidade.

Como mencionámos na introdução, o mero facto de juntar máquinas não benificia em nada a confiabilidade e a segurança:

- um sistema centralizado tem menos componentes, portanto falha menos;
- um sistema centralizado e não interligado é um domínio de segurança bem controlado.

Talvez isto esclareça certos malentendidos e desapontamentos dos projectistas e utilizadores experimentados de sistemas centralizados (o PC individual por um lado, e os sistemas comerciais tipo *mainframe*, por outro), quando se aventuram nos «sistemas em rede», motivados pelas vantagens normalmente propaladas. E certamente motivou a citação de Lamport feita atrás.

Lamport foi um dos maiores impulsionadores do desenvolvimento de técnicas para construir e operar sistemas distribuídos correctamente. E é nessas técnicas que devemos ir beber, para conseguir então as desejadas propriedades que potenciam os sistemas distribuídos como os sistemas do futuro nesta época de comunicação global:

- **fiabilidade e disponibilidade**--- decaimento gradual, pela falha parcial de componentes sem falhar o todo;
- **segurança**--- pela tolerância a intrusões parciais sem o todo ser dominado ou penetrado.

Isto é, à medida que a interligação dos sistemas em rede se torna (cada vez mais) uma hipótese apetecível, os projectistas de sistemas irão invariavelmente seguir um de dois caminhos: «juntar máquinas» através de uma rede; construir um sistema distribuído.

Não é difícil perceber qual será a única com sucesso. Na secção sobre vantagens competitivas, mais à frente, damos alguns exemplos de prováveis insucessos.

Embora Portugal não possua grandes fabricantes informáticos, possui, e pode possuir ainda mais, indústria de sistemas informáticos de valor acrescentado (integração de sistemas, aplicações dedicadas de *software-houses*, sistemas embebidos, etc.), e se é certo que as suas possibilidades de sucesso dependem drasticamente das vantagens competitivas que os seus produtos e serviços possam obter, é-o ainda mais que grande parte dessas vantagens dependerão da tecnologia. Neste caso, da arquitectura e do software.

Dois exemplos servirão para ilustrar o nosso ponto de vista, que defendemos na secção seguinte.

Comecemos pelas aplicações clássicas de acesso remoto. Um sistema transaccional interactivo (OLTP) típico é baseado numa base de dados transaccional situada em *mainframe*, onde estão pendurados quer terminais virtuais que permitem o acesso remoto através de linha dedicada ou rede, ou máquinas de vanguarda (*front-ends*) que dialogam como clientes com o gestor de transacções, numa óptica cliente-servidor.

Na primeira hipótese, trata-se de um sistema absolutamente centralizado, em que apenas deslocámos os terminais umas dezenas ou centenas de quilómetros, e cuja confiabilidade depende da máquina central e da ligação, e cuja segurança depende da metodologia empregue na concretização do acesso remoto. Na segunda hipótese, trata-se de uma computação com controlo e estado partilhado entre o cliente e o servidor, e que por isso, apresenta problemas delicados de coerência em caso de falha (do servidor, do cliente, da rede), e de segurança, uma vez que normalmente estará interligada em rede.

Outro exemplo é um serviço de directório e comércio electrónico baseado em WorldWideWeb, disponibilizado para todo o território Português. Baseado num servidor WWW, a maior parte da lógica que pertence às funções normalmente identificadas com um cliente está na verdade colocada junto do servidor, enquanto que os utilizadores finais, colocados remotamente, são aquilo que hoje em dia se denomina navegadores ou *browsers*, e servem principalmente dois propósitos: enviar comandos que são executados em nome do navegador pelo «cliente» local ao servidor; e retirar informação (*information retrieval*) multimédia do servidor, apresentando-a conveniente-mente ao utilizador final. Estes sistemas, comparados com um cliente-servidor clássico, apresentam muito menos problemas de coerência de estado, mas colocam por outro lado muito maior pressão sobre o servidor, do ponto de vista de confiabilidade, desempenho e segurança.

Confiabilidade

A confiabilidade e a distribuição andam de mãos dadas, porque os melhores sistemas confiáveis são os construídos a partir de técnicas de tolerância a faltas distribuída. Isto é, mesmo que as nossas necessidades não incluam a distribuição, devemos construir o nosso sistema como sendo distribuído, se desejarmos elevada confiabilidade. E assim fazendo, obteremos quase sempre as restantes vantagens dos sistemas distribuídos, nomeadamente: um preço reduzido, escalabilidade e expansibilidade incrementais.

O conjunto de técnicas mais importantes para conseguir confiabilidade enquadra-se no que se denomina *tolerância a faltas*, isto é, a capacidade de um sistema para resistir a falhas dos seus componentes (faltas) sem que o serviço seja afectado. O instrumento mais importante para o conseguir são as técnicas de *replicação* de componentes (hardware e software), e dentre os protocolos e algoritmos mais relevantes avultam aqueles destinados a:

- gerir a replicação;
- assegurar a comunicação fiável entre os participantes do sistema;
- assegurar a coerência do estado distribuído pelos participantes.

Após esta breve introdução, voltamos aos nossos exemplos. Como tornar fiável o sistema OLTP do primeiro exemplo? Podemos utilizar um computador totalmente replicado, com acopulamento forte, que é virtualmente sem paragens (*non-stop*, por ex. Tandem). Podemos utilizar matrizes de discos replicados (RAID) para salvaguardar a informação não volátil, mas não sobrevivemos a falhas da unidade de processamento. Podemos ter duas máquinas iguais (duas *mainframes*, portanto), com o factor custo a tornar-se extremamente elevado para os benefícios: a dupla diversidade (replicação total) é a pior das opções. Podemos, á semelhança de algumas aplicações transaccionais grande-escala que existem em Portugal, ter uma máquina mais pequena em *stand-by*, que serve para manter uma certa disponibilidade de serviço perante a falha da principal, mas normalmente não garante nem uma parte apreciável das funções desempenhadas pela máquina principal, nem uma continuidade de serviço após a comutação (*take-over*), isto é, há estado (ex. transacções) que se podem perder, e têm que ser recuperadas mais tarde, com transacções correctivas e/ou manualmente.

Em alternativa, imagine-se que se fragmenta a base de dados transaccional em diversas partes, e que se replicam partes da mesma base de dados, colocando os fragmentos e as réplicas estrategicamente em diversos sítios, que efectuem uma cobertura razoável do território alvo. O que se conseguiria com esta política?

Fragmentando a base de dados, se existir um factor de localidade dos acessos, estamos a colocar o servidor mais perto do cliente, com as respectivas vantagens em desempenho, custo de comunicação e fiabilidade da mesma. Se não existir, estamos de qualquer forma a estruturar as unidades de replicação. Replicando a base de dados, podemos, caso não exista um factor de localidade bem definido, colocar réplicas de um fragmento estrategicamente perto das várias áreas onde haja uma frequência de acessos à informação contida no fragmento, que o justifique. São semelhantes as vantagens em desempenho, sendo estas réplicas o que vulgarmente se chama de *caches*. Exista ou não um factor de localidade bem definido, podemos replicar

fragmentos criteriosamente para ocorrer a diversos cenários de falha: falha catastrófica do disco; falha momentânea do servidor; falha de comunicações (se existir conectividade para uma réplica alternativa); falha catastrófica do hardware do servidor.

Além disso, adoptando esta arquitectura distribuída: obtivemos os mesmos resultados de confiabilidade a um custo muito menor (o preço do mesmo poder de cálculo de uma *mainframe*, em máquinas modulares de menor porte, é bastante menor); replicação selectiva, não necessitando de ser total para a parte do sistema *on-line*; melhor desempenho médio para acessos remotos; expansibilidade do sistema incomparavelmente maior do que a de uma *mainframe*.

Observemos agora o segundo exemplo. A navegação multimédia, por exemplo através da WorlwideWeb, está a ocupar uma parte cada vez maior do universo das actividades interactivas humanas de hoje em dia: pesquisa de informação; publicação; sistemas de informação empresariais; transacções electrónicas (comércio, banca). Tornou-se vulgar, mesmo em Portugal, uma empresa ou instituição ter uma página WWW, ou mesmo um particular. Grande parte do sucesso desta expansão tem que ver com a expansão da Internet, e com o modelo de computação da WWW, como explicámos, com o centro de gravidade no servidor, o que torna possível a qualquer utilizador iniciado «navegar» sem problemas, e aos servidores modificar e evoluir os seus serviços sem interferir com os utilizadores. No entanto, nem tudo são rosas: tal facto põe uma pressão inusitada sobre o desempenho e a disponibilidade dos servidores WWW, aliada à mesma pressão sobre a largura de banda, latência e conectividade da Internet. Qualquer de nós navegadores habituais já experimentou o desapontamento de não encontrar acessível o servidor que procurou. Se pensarmos que a utilização da WWW e Internet em aplicações «sérias», de grande impacto económico, é hoje já uma realidade, cuja importância só vai aumentar no futuro próximo, existe em definitivo um problema que não pode ser encarado de maneira leviana por quem se queira manter nesse mercado.

Aqui também, embora com *nuances* técnicas que não cabe abordar aqui, as soluções orientadas para a replicação e *caching*, para sistemas de ficheiros distribuídos grande-escala, são a solução para conseguir operar esses sistemas satisfatoriamente.

No entanto, e para terminar, estes sistemas têm de ser projectados e/ou configurados por quem possua algum domínio das tecnologias de sistemas distribuídos e de tolerância a faltas, sob pena de estarmos a *juntar máquinas* em lugar de construir um sistema distribuído: ficou mostrado que será pior a emenda que o soneto. Este suporte sistema para aplicações distribuídas corresponde aquilo que tem sido denominado *middleware*, mas mais que obedecer a um chavão, que tem sido abusado, devemos ter uma noção rigorosa acerca das técnicas que temos de utilizar para obter confiabilidade.

Segurança

Abordemos agora a questão da segurança. A segurança em sistemas informáticos mede-se por conceitos bem definidos:

- **confidencialidade**-- medida em que um serviço/informação está protegido contra o acesso de intrusos;
- **autenticidade**—medida em que um serviço/informação está protegido contra a personificação por intrusos;
- **integridade**-- medida em que um serviço/informação está protegido contra a modificação/deterioração por intrusos;
- **disponibilidade**-- medida em que um serviço/informação está protegido contra a recusa de provisão/acesso provocada por intrusos.

Assim, no âmbito da segurança de sistemas informáticos, é importante: proteger a informação privada e/ou confidencial residente em computadores ou em trânsito através de redes; reconhecer assinaturas electrónicas; evitar e/ou detectar o forjamento, alteração ou destruição dessa mesma informação; evitar acções que visem o bloqueamento de um serviço baseado em computador.

As facetas mais comuns da insegurança dos sistemas informáticos em rede, ou distribuídos, são:

- ataques a máquinas e informação (*hacking*);

- ataques a meios de comunicação (*phreaking*).

Os ataques a máquinas assumem hoje em dia diversas formas, mais ou menos destrutivas, desde vírus, passando por utilização abusiva de recursos, até violação da privacidade ou confidencialidade, com roubo de informação (espionagem industrial, comercial e outras...), terminando na fraude informática. Os ataques a meios de comunicação assumem a forma de escuta não autorizada, e utilização abusiva (grátis) dos mesmos meios. Estes ataques são amiúde combinados, por exemplo, é frequente um pirata apossar-se de uma máquina em território nacional, vindo de uma máquina no estrangeiro através da Internet, para despistar a sua acção. Obviamente, é atraente apossar-se previamente de um meio de telecomunicações, como por exemplo um PPCA com interfaces modem ou um comunicador X.25, para evitar os custos de comunicação para o estrangeiro.

As motivações dos piratas são diversas, e exploram normalmente defeitos (*bugs*) nos sistemas operativos das máquinas vítima, em software aplicacional, ou na configuração das mesmas máquinas. No entanto, a questão da segurança deve ser sempre vista englobando duas facetas: as pessoas e os computadores. Não há tecnologias que resistam a uma política de segurança inexistente, ou que não tenha estes dois factores em conta. E quando se fala do factor humano, fala-se dos piratas, e das pessoas da organização. Estas últimas podem ser uma das ameaças mais graves à segurança. Não tanto por malícia ou falta de ética (sabotagem, espionagem), mas muito principalmente, de acordo com a nossa experiência, por desleixo («não há nada de importante nos nossos computadores»), desconhecimento e ingenuidade. Muita informação de piratagem tem sido conseguida através de engenharia social aplicada aos «ingénuos» das organizações.

Os piratas informáticos são muito menos inofensivos do que se pode pensar. Isto é, a maior são jovens, alguns estudantes, atraídos pela aventura que parece ser o equivalente a forçar a fechadura de um automóvel, ou entrar em casa de alguém que deixou a porta aberta por esquecimento e revistá-la. Queremos com estes exemplos dizer que é necessário um esforço imenso para formar uma «ética da coisa informática», porquanto, na experiência do autor, quando confontados com os exemplos acima, de éticas bem conhecidas como a propriedade privada, a grande maioria dos jovens fica pela primeira vez em confronto com a seriedade de que afinal se reveste entrar no computador de uma pessoa (apesar de ela se ter esquecido de pôr palavra de passe) e abrir as suas «gavetas pessoais», ou de correr um programa caça-palavras-de-passe. Estes jovens, vistos individualmente, estão apenas a tentar uma aventura de que não pensaram bem nas consequências--- sob o novo regime legal em vigor desde o fim de 1992, a maior parte das «brincadeiras» que estudantes mais matreiros fazem nos centros de cálculo e outras máquinas de universidades, são crimes informáticos, alguns deles merecendo prisão. Mas vistos em conjunto, pelo seu número e pela inépcia que por vezes revelam, podem causar danos irreparáveis aos sistemas em que exercitam as suas receitas de aprendiz de feiticeiro.

Por outro lado, há acções de pirataria que se revestem de contornos bastante mais sinistros, e muito mais competentes. A coberto do anonimato de um acesso remoto, é difícil distingui-los dos outros. Por tudo isto, há que encarar a segurança a sério. A nossa experiência mostra que tal não acontece. Nestes dias de comunicação global (ex. Internet, rede telefónica), a insegurança dos nossos sistemas contribui para a dos outros. O número de violações de segurança no nosso país correntemente é enorme. O número de fraudes informáticas é muito mais elevado que se pensa, pelo facto de a maior parte dos casos não serem relatados. Isto cria uma ideia de que «só acontece aos outros», de falsa segurança, que leva muitas instituições e empresas responsáveis a não terem qualquer política de segurança informática, e ainda a terem uma administração de sistemas deficiente ou inexistente. Esta falta de preocupação, por outro lado, gera do lado dos vendedores uma desmotivação para o problema que só o agrava.

A situação que delineámos no início desta comunicação é de que poucas empresas de dimensão se poderão dar ao luxo de não estarem ligadas em rede. Para outras será mesmo uma necessidade vital. Após uma intrusão, sobretudo se provocar danos, há uma tendência para desligar da rede. É

necessário pensar nos custos que isso pode ter. Há um equilíbrio entre os custos de certas *intrusões*, e o de estar *desligado*. Por outro lado, a rede não é o único ponto de ataque. Finalmente, existem hoje tecnologias nos sistemas distribuídos que, não só permitem que operem tão seguramente como os centralizados, mas, tirando partido da descentralização e possibilidade de repartição de informação sensível, podem mesmo exceder esses níveis de segurança.

Antes de qualquer veleidade tecnológica, é necessário a uma empresa ou instituição ter uma atitude em relação à segurança, com ou sem assistência externa:

- definir uma política de segurança;
- efectuar auditorias de segurança;
- ter uma administração de sistemas competente em segurança;
- investir em tecnologia e formação.

Sem política, quaisquer medidas de segurança arriscam-se a ser: ineficazes, descoordenadas, grotescas, insatisfatórias para todos. Para definir a política, a empresa deve começar por efectuar uma auditoria de segurança, preferivelmente externa, que se deverá repetir para aferir os resultados, mais tarde. Um administrador de um sistema distribuído (em rede, telemático, etc.) tem de ter formação sólida em segurança. Uma vez definida a política, há que investir. A segurança tem custos, mas mais vale investir para prevenir, que dispender... a remediar. E obviamente, esses custos são proporcionais à dimensão da empresa, pelo que ninguém deve pensar que não está ao seu alcance. Uma mini-política e infraestrutura de segurança para uma mini-empresa é tão eficaz como uma estrutura mais ambiciosa para uma grande empresa.

A política pode definir domínios (também denominados arcaicamente anéis, conceito que fazia sentido para sistemas centralizados) de segurança. Para cada domínio, a severidade pode ser diferente. Genericamente falando, em sistemas distribuídos existem quatro níveis de severidade quanto à permissividade (os quatro pês) da ligação ao exterior, que devem ser aplicados criteriosamente consoante os casos:

paranóico—completamente desligado da rede;

promíscuo-- ligado à rede sem restrições;

prudente—paranóico com ligações caso-a-caso;

permissivo—promíscuo com cortes caso-a-caso.

Guiadas por uma política efectiva, existem inúmeras tecnologias que permitem atingir os níveis de segurança definidos caso-a-caso:

- anti-vírus
- modems seguros com palavra-de-passe e chamada de volta (*call-back)*;
- anteparas de segurança para redes (*firewalls, bastions*);
- servidores de segurança com controlo de acesso (*Kerberos,Delta-4*);
- cifração de ficheiros e arquivos (*PGP,FRS*);
- comunicação criptográfica (*PGP,PEM, Clipper*);
- palavras-de-passe descartáveis (*S/Key*).

Voltando aos exemplos que demos mais atrás, no sistema OLTP centralizado, utilizado por muitos bancos, cria-se por vezes uma falsa sensação de segurança da comunicação, quando a linha é alugada e, portanto privada. Por outro lado, nas configurações cliente-servidor através de rede pública (Telepac, Internet), as palavras-de-passe e códigos de acesso variados, passeiam pela rede, sem serem cifrados (por norma).

A despeito de se estar sobre linhas privadas, deverá utilizar-se comunicação criptográfica quando a sensibilidade da informação o justifique. Do mesmo modo, sobre rede em cliente-servidor, a entrada em sessão remota deverá ser cifrada, bem como o conteúdo de

certas partes da comunicação que contenham códigos de acesso, ou informação que permita um ataque ao protocolo de modo a forjar uma transacção. Se a base de dados estiver fragmentada em consonância com técnicas de segurança, pode-se tornar extremamente difícil a um pirata que penetre num sítio, obter muita informação útil.

Falando do exemplo WWW, neste momento os navegadores mais conhecidos possuem facilidades de segurança, que permitem a autenticação e confidencialidade necessárias para construir sub-sistemas de comércio electrónico. No entanto, para termos uma ideia da sofisticação dos ataques que podem sofrer estes mecanismos e, portanto, do risco a que estão expostos estes sistemas, mesmo quando concebidos cuidadamente, o protocolo de segurança do navegador mais popular, o Netscape, foi recentemente furado, devido a um defeito do algoritmo de geração de chaves de sessão. Felizmente, este defeito foi descoberto por dois estudantes, que publicaram o feito. A Netscape assim corrigi-lo sem dano de maior aos milhares de utilizadores actuais.

Nenhum sistema é 100% seguro. O método mais robusto de cifração conhecido, a criptografia de chave pública, tem uma probabilidade superior a zero de ser «quebrado». A única coisa que é garantida é que, mercê do comprimento adequado da chave, se pode tornar essa tarefa «computacionalmente inexequível em tempo útil». Mas uma vez que o desempenho é inversamente proporcional a esse comprimento, será de esperar que compromissos sejam feitos, os quais caem

na alçada das políticas de segurança de que já falámos.

Assim, o sistema de uma organização, que vale o que valer o seu elo mais fraco, não pode consistir de uma mera aplicação de receitas, mas ser configurado numa óptica sistémica. Mais uma vez, estes sistemas têm de ser projectados e/ou configurados por quem possua algum domínio das tecnologias de segurança, nomeadamente de sistemas em rede, sob pena de se criar uma situação ainda mais insegura, uma vez que os utilizadores criarão uma sensação de segurança que a realidade não confirma.

Vantagens competitivas

O mercado tem, muito recentemente, mostrado as vantagens competitivas que residem na utilização de tecnologias de sistemas distribuídos. Mas também se encarregará de mostrar que sistemas que não tenham aproximações credíveis de confiabilidade e de segurança falharão:

- porque um sistema transaccional *on-line* está mais vezes off-line que o contrário...
- porque um sistema de pagamento ou transacções electrónicas tem buracos de segurança...
- porque um sistema bancário em rede foi violado por *hackers*...
- porque um sistema WWW dá por demais amiúde a mensagem «...server is down...»
- porque um sistema de base de dados teve uma falha catastrófica onde se perdeu informação vital da companhia...
- porque um sistema de base de dados transaccional «distribuído» fica amiúde incoerente devido a falhas temporárias de comunicação (partições);
- porque uma base de dados de um ministério foi violada por *hacker*s, que divulgaram ou alteraram informação vital sobre cidadãos, projectos em apreciação, dossiers secretos...
- porque um grupo radical de piratas atacou um importante servidor em rede, atafulhando-a com lixo electrónico de modo a bloquear o seu funcionamento...
- porque um sistema de bolsa electrónica em contínuo falhou a meio de uma sessão, e quando recuperou estava totalmente incoerente...
- porque os sistemas de segurança de uma rede GSM foram viciados, permitindo burlas informáticas...
- porque um sistema de porta-moedas electrónico foi quebrado, permitindo enfim o milagre da «árvore-das-patacas»...

A *tolerância a faltas* deixou há muito de ser a etiqueta das centrais nucleares ou dos sistemas aviónicos. É neste momento um conjunto de técnicas utilizáveis e, mais ainda, incorporáveis, com o conhecimento adequado, em qualquer sistema informático.

A *segurança* deixou igualmente de ser apanágio exclusivo dos sistemas militares e governamentais. A popularização das técnicas de cifração informática é tão grande que gerou recentemente reacções alérgicas da parte de governos, que querem controlar severamente as capacidades de cifração civis. Existe correntemente, à semelhança da tolerância a faltas, um conjunto de técnicas de cifração e controlo de acesso que, de igual modo, e com o adequado conhecimento, são incorporáveis em sistemas informáticos.

No entanto, a experiência também tem mostrado, durante o desenvolvimento destas técnicas, que elas valem o que valer o ponto mais fraco (em segurança ou confiabilidade) do sistema. Isto é, o projecto destes sistemas deve ter uma aproximação sistémica, credível e equilibrada nas três vertentes: distribuição, confiabilidade, e segurança. Escusado será dizer que os arquitectos e projectistas dos sistemas as deverão de igual modo dominar.

Por último, as vantagens competitivas que adivinhamos nas tecnologias que foram o tema central desta comunicação estão asseguradas à partida em sede dos utilizadores:

- porque necessitam cada vez mais de sistemas informáticos e redes;
- porque essa dependência os deixa cada dia mais angustiados em relação às implicações na privacidade, autenticidade e integridade da informação;
- porque aprenderam a ser exigentes com a fiabilidade e disponibilidade dos sistemas de que se servem.

Conclusão

Esta comunicação visou tratar a problemática dos modernos sistemas informáticos, sob a óptica da confiabilidade e segurança. A ideia chave que foi apresentada é de que estas técnicas são indissociáveis dos sistemas distribuídos modernos, se se quiser que tenham sucesso num mercado cada vez mais exigente.

No entanto, trata-se de técnicas abordáveis de um ponto de vista sistémico--- de arquitectura e de software--- e, portanto, perfeitamente ao alcance das indústrias relacionadas com a informática no nosso País. Por serem técnicas de ponta, apesar de já apresentarem resultados industriais, constituem ainda um excelente tema de investigação aplicada, adequado à realidade nacional. Nesse sentido, a comunicação abordou ambas as problemáticas do ponto de vista técnico, e avançou algumas ideias acerca daquilo que podem ser as vantagens competitivas de produtores e utilizadores de sistemas informáticos que se debrucem seriamente sobre este tipo de tecnologias.

Para os produtores e utilizadores de sistemas informáticos ficam algumas perguntas e respostas:

--- A confiabilidade e a segurança têm custos? --- sim, mas não há benefícios sem custos.

--- E esses benefícios são reais? --- mais vale investir que dispender, ou «mais vale prevenir que remediar».

Referências:

Sape Mullender, editor. Distributed Systems, 2nd Edition, ACM-Press, Addison-Wesley, 1993.

D. Powell, editor. Delta-4 - A Generic Architecture for Dependable Distributed Computing. ESPRIT Research Reports. Springer Verlag, November 1991.

Kenneth Birman and Robbert van Renesse, editors. Reliable Distributed Computing With the ISIS Toolkit. Number ISBN 0-8186-5342-6. IEEE CS Press, March 1994.

P. Veríssimo, W. Vogels, H. Cartaxeiro, H. Fonseca, INESC, Lisboa; and N. Cook, Newcastle Univ., Newcastle. ``Infrastructure

Support for ESPRIT Basic Research Networks of Excellence''. Report prepared by: December 1994. http://www.inesc.research.ec.org/cabernet/workspace/infra.html

J.Dawson, R.Kay, J.Bryan. Network Security, Byte, April 1994, Vol.20, Nr. 4.

Netscape. Potential Vulnerability in the Netscape Navigator. http://home.netscape.com.

E. Rescorla and A. Schiffman. The Secure Hypertext Transfer protocol. Internet Draft. IETF. December 1994.