Universidade Federal do Rio de Janeiro

Escola Politécnica

Departamento de Engenharia Eletrônica e da Computação

DEL - UFRJ

Tema: **TCPA - *Trusted Computing Platform Alliance***

Aluno: *Vitor Ugo Brevilieri*

25/05/2004

Disciplina: Redes I

Prof.: *Otto Carlos Muniz Bandeira Duarte*

Turma EL1 – 2004/1

Índice

Resumo

Este trabalho resume o que é a TCPA, as funções do "chip" Fritz, dá exemplos de suas aplicações e mostra por que estas aplicações são de suma importância para a segurança do lado cliente nas arquiteturas de redes. Também mostrará as críticas que este esquema de segurança vem recebendo de estudiosos e defensores do "software" livre e da privacidade do consumidor.

1. Introdução

Em 1973, Roger Schell, em "Preliminary Notes on the Design of Secure Military Computer Systems", afirmou:

"From a practical standpoint, the security problem will remain as long as manufacturers remain committed to current system architecture, produced without a firm requirement for security.

As long as there is support for ad hoc fixes and security packages for these inadequate designs and as long as the illusory results of penetration teams are accepted as demonstrations of a computer system security, proper security will not be a reality."

Aproximadamente, há 30 anos, Schell previa a situação dos sistemas de computação em que nos encontramos atualmente: sistemas não projetados para as ameaças da Internet moderna, mal implementados e que requerem a contínua instalação de pacotes de segurança. Como conseqüência, milhares de sistemas são comprometidos em taxas crescentes, seja por incompatibilidades, seja por ataques remotos.

Com a missão de, através da colaboração de "hardware", "software", comunicações e vendedores de tecnologia, dirigir e implementar as especificações para uma plataforma de computação melhor e confiável, baseada em "hardware" e sistema operacional, de tal forma que ofereça confiança em plataformas clientes, servidoras, de redes e de comunicações, cinco dentre as maiores empresas de computação do mundo se uniram: Compaq, HP, IBM, Intel e Microsoft, criando assim a "Trusted Computing Platform Alliance" (TCPA), em 1999.

Para tentar solucionar os problemas de segurança, brevemente descritos acima, e inspirados nas sugestões de Schell, o "chip" TCPA (também denominado "chip" "Fritz") foi projetado para prover às máquinas-cliente uma mínima, porém essencial, base de "hardware" para sua segurança. A "Trusted Computing Platform Alliance" produziu especificações abertas para este "chip" de segurança e interfaces de "software" relacionadas. Especificações abertas, amplamente suportadas, acelerarão o projeto, o uso, o gerenciamento e a adoção dos sistemas confiáveis e das soluções que atendem aos desafios do crescente mundo interconectado.

Em 2003, a organização TCPA já contava com mais de duzentos membros e também diversos críticos. Sob a liderança de AMD, HP, IBM, Intel e Microsoft, fundou-se a organização "Trusted Computing Group" (TCG), a qual a TCPA considera como sendo sua sucessora. A TCG incorporou as especificações TCPA como ponto inicial e pretende melhorá-las, além de estendê-las para especificações que abrangem quaisquer dispositivos de computação digital, tais como telefones digitais. Portanto, embora o título do trabalho continue sendo "TCPA - Trusted Computing Platform Alliance", como previamente batizado, qualquer um dos termos já mencionados, ou mesmo "Trusted Computing" (IBM), "Trustworthy Computing", "Palladium" e "NGSCB" (Microsoft) e "Safer Computing" (Intel) seriam adequados como título para o conteúdo que se pretende apresentar.

Muitos críticos afirmam que esta vasta gama de nomes é proposital, pretende confundir consumidores e desviar a atenção daquilo que realmente está por trás disto tudo: Transferir o controle do proprietário do computador para aquele que tenha escrito os "softwares" que o computador esteja executando. Um dos objetivos principais da TCPA seria suportar "Digital Rights Management" (DRM). Por este motivo, a Free Software Foundation prefere referir-se por "Treacherous Computing"! Os críticos tentam mostrar as controvérsias entre as diversas definições de confiança; as máquinas construídas segundo as especificações TCPA serão mais confiáveis do ponto de vista dos vendedores

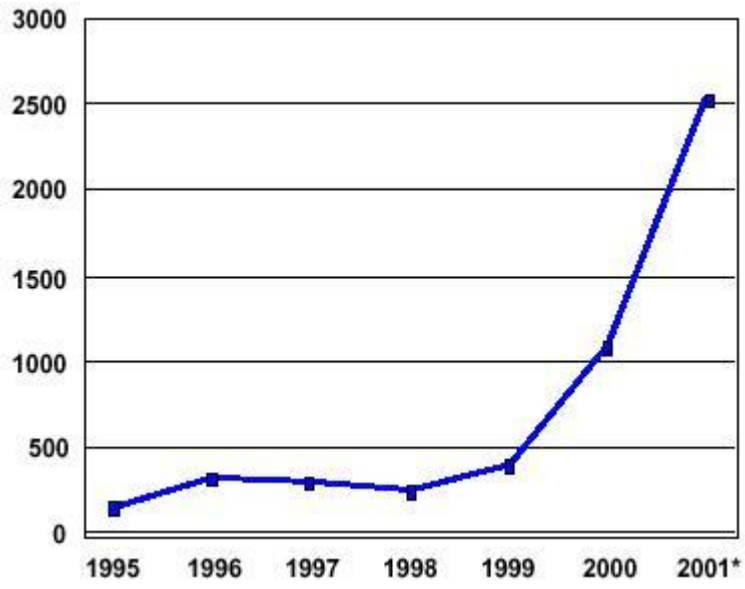
de "software" e da indústria de conteúdo, mas serão menos confiáveis do ponto de vista dos proprietários destas máquinas.

Em contrapartida, membros da TCG defendem a proposta inicial TCPA e suas implementações particulares e afirmam que estas não suportam DRM, mas não garantem que outros membros da TCG vêm fazendo o mesmo trabalho em suas implementações. Isso fica claro em [4], onde David Safford, falando em seu nome e não necessariamente em nome da IBM, tenta levantar as diferenças entre a especificação TCPA e a implementação Palladium da Microsoft, que é um dos maiores alvos dos críticos. A IBM, no entanto, não censura David Safford, ao exibir abertamente suas idéias em seu "site" oficial.

Tentar-se-á exibir o assunto de uma posição neutra, neste trabalho.

2. Vulnerabilidades de e Ataques Remotos a Sistemas de Computação

O gráfico abaixo mostra a evolução da quantidade de diferentes vulnerabilidades de "software" descobertas anualmente. Sendo descobertos em tão elevadas taxas, torna-se quase impossível aplicar todos os pacotes de correção necessários.



(retirado de http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf*)*

Este é um ambiente ideal para os ataques dos "hackers", uma vez que a maioria dos sistemas terá, no mínimo, uma das vulnerabilidades conhecidas. O fato de os sistemas atuais serem extremamente complexos, com cerca de cem milhões de linhas de código num sistema operacional típico, por exemplo, garante que estes erros existirão, uma vez que a taxa média de erros por linha de código é de um erro a cada mil linhas de código. Isto eqüivale a dizer que um sistema operacional típico possui, potencialmente, cem mil erros. Não é surpresa, portanto, que se encontrem cinco mil erros anualmente e que esta taxa esteja crescendo dramaticamente.

Em 2000, Roger Schell e Michael Thompson escreveram um artigo, "Platform Security: What is Lacking?", no qual analisam as ameaças da Internet moderna e mostram como a falta de defesas numa

plataforma impede que aplicações importantes em potencial sejam efetuadas, como comércio eletrônico (esta análise foi resumida em [1]). Serão mostrados, a seguir, as principais categorias de vulnerabilidades que os "hackers" utilizam para atacar um sistema e também as tendências evolutivas dos ataques "hackers" nos últimos anos.

2.1 - Programas Inseguros

Programas inseguros são aqueles cujo projeto é, inerentemente, inseguro no ambiente da Internet. A razão para esta insegurança no projeto é muito simples: estes programas não foram projetados com segurança em mente. Por isso, estes são, inerentemente, explorados por "hackers".

Como exemplo, pode-se citar "telnet" e "ftp", que normalmente enviam nomes e senhas de usuários pela rede sem ao menos encriptá-los. "Hackers" podem, facilmente, gravar estes nomes e senhas enquanto passam pela rede e repetí-los para utilizar o acesso à rede de outros. Outro exemplo é "rlogin", que utiliza o endereço IP do transmissor para autenticação, o que é facilmente forjado.

2.2 - Programas Mal-Configurados

Programas Mal-Configurados são aqueles que possuem facilidades adequadas de segurança em seu projeto e requerem que estas sejam, devidamente, configuradas.

Como exemplo, pode-se citar o NFS ("Network File System"), que pode ser configurado para exportar um sistema de arquivos em modo de leitura apenas, o qual é bem seguro, mas também pode ser configurado para exportar um sistema de arquivos em modo de leitura e escrita para todos os domínios de usuários, o que permite que "hackers" danifiquem este sistema de arquivos facilmente.

2.3 - Programas com Falhas

Programas com Falhas são aqueles com projeto de segurança e configurações apropriadas, mas que possuem falhas de implementação ou codificação que podem ser explorados remotamente. Nestes casos, "hackers" enviam dados maliciosamente preparados para explorar estes erros de implementação.

(retirado de http://www.celepar.gov.br/batebyte/edicoes/2000/bb95/flagrantes.htm)

Uma falha de implementação muito comum são os estouros de "buffer". Um "buffer", que possui tamanho fixo para armazenar dados de entrada, é criado, mas não foi implementada a checagem da quantidade de dados de entrada, que avalia se esta quantidade pode ser devidamente armazenada ou se ocorrerá o estouro do "buffer". O "hacker" pode enviar dados em excesso, de forma que o "buffer" estourará, sobrescrevendo o que segue ao fim do "buffer".

Erros de estouro de "buffer" são, há tempos, conhecidos, e facilmente evitáveis, mas ainda são, freqüentemente, os mais descobertos e explorados.

2.4 - Tendências Evolutivas

Por volta dos anos 80, os "hackers" atacavam amplamente as redes, espionando, passivamente, em busca de senhas, e, ativamente, invadindo sessões. À medida que as aplicações encriptavam, crescentemente, os dados que atravessam a rede, "hackers" se voltaram para atacar diretamente os servidores, principalmente através de configurações mal realizadas e serviços com falhas, como servidores "web", por exemplo. E, à medida que as empresas respondiam com o uso de "firewalls", detecção de intrusos e ferramentas de verificação de segurança, "hackers" começaram a focar os ataques em clientes.

Os interesses nos computadores clientes se justificam por duas razões: primeiro, estes possuem, freqüentemente, nomes e senhas de usuários utilizados em servidores. "Hackers" invadem as máquinas-cliente para tomar suas senhas e entrar em servidores-alvo. Segundo, as máquinas- cliente são uma grande fonte disponível de máquinas de onde se podem lançar ataques DDoS("Distributed Denial of Service").

Enquanto estes ataques oriundos de clientes ocorriam em pequenas taxas, ninguém se importava com a segurança do lado do cliente. No entanto, o aumento destes ataques representa ameaças crescentes, tanto para usuários, quanto para servidores, em negócios eletrônicos. Desta forma, a proteção de dados de autenticação se tornou um fator crítico para o sucesso dos negócios eletrônicos.

3. Funções Principais do "Chip" TCPA

A "Trusted Computing Platform Alliance" foi formada para estabelecer o padrão industrial para subsistemas de computação confiáveis a serem instalados nos PCs. A IBM, uma das empresas fundadoras da TCPA, vem embutindo seu predecessor do "chip" TCPA, chamado de "Embedded Security Subsystem" ("chip" ESS) em seu PC PL300 e em seu "notebook" "T23 Thinkpad Systems", desde 2000. O "chip" ESS é, basicamente, um "chip" "smartcard" que possui uma chave- pública e está diretamente colocado sobre o barramento SMB ("System Management Bus") da placa-mãe. A idéia foi de tornar disponível um "hardware" com uma chave- pública a baixos custos. Para isto, embutiu-se o "chip" ESS na placa-mãe e eliminou- se a necessidade de "smartcards" e leitores especiais no projeto.

Outras empresas procuravam soluções semelhantes e se tornou claro que se deveria chegar a uma solução única e comum a estas empresas, de forma a se estabelecer um padrão. A especificação principal da TCPA define um "chip" que atende aos requisitos de segurança de todas as empresas-membro da TCPA. Adicionalmente, outras especificações TCPA cobrem interfaces específicas de PC e detalhes de "software".

(retirado de http://www.schimak-ottenbach.de/tipps/lexikon/index_t.htm)

O "chip" TCPA, por si só, reúne as três categorias principais de funcionalidades que serão descritas a seguir.

3.1 - Funções de Chave-pública

As funções de chave-pública são muito similares à solução original do “chip”ESS da IBM. Estas proporcionam a geração de pares de chaves no “chip”, usando um “hardware” gerador de números aleatórios, em conjunto com a assinatura da chave-pública, verificação, encriptação e decriptação.

(retirado de http://tigger.uic.edu/depts/accc/newsletter/adn26/figure2.html)

De forma simples, e ilustrado na figura acima, o esquema de chave- pública é um esquema de criptografia de chave assimétrica, onde são usadas duas chaves ligadas matematicamente; se uma é utilizada para criptografar uma mensagem, a outra chave deve ser utilizada para decriptar. Uma das duas é mantida em segredo, a chave- privada. Énecessário que o emissor de mensagens, antes de enviar sua mensagem, utilize a chave-pública do destinatário para encriptar a mensagem. A chave-pública é, a princípio, disponível a qualquer um. Ao receber a mensagem encriptada, o destinatário utiliza a chave-privada para decriptar a mensagem. Ou seja, qualquer pessoa pode enviar uma mensagem confidencial apenas utilizando chave- pública, mas esta mensagem só poderá ser decriptada com a chave- privada do destinatário.

Os sistemas de criptografia assimétrica, geralmente, são mais custosos computacionalmente, em relação aos simétricos; eles normalmente são utilizados para a distribuição da chave simétrica ao destinatário. Após esta passagem, utiliza-se a criptografia simétrica em cima dos dados.

3.2 - Funções de "Boot" Confiável

As funções de "boot" confiável possibilitam a habilidade de armazenar, em registradores de configuração da plataforma (PCR), pedaços ou resumos ("hashes") de informações de configuração ao longo da seqüência de "boot". Uma vez executado o "boot", dados, como chaves simétricas para arquivos encriptados, por exemplo, podem ser lacrados em um PCR, para garantir autenticidade. Os dados lacrados podem ser lidos apenas se o PCR possuir o mesmo valor que possuía no momento da lacração. Então, se uma tentativa é feita de executar o "boot" de um sistema alternativo, ou se um vírus tiver utilizado uma "backdoor" no sistema operacional, o valor do PCR não irá coincidir e a deslacração dos dados irá falhar, desta forma protegendo os dados.

3.3 - Funções de Inicialização e Gerenciamento

As funções de inicialização e gerenciamento permitem ao proprietário do sistema que ele altere as funcionalidades, reinicialize e tome propriedade sobre o sistema. Este grupo de funções é um tanto quanto complexo, de forma a tornar extremamente restritivo o que pode ser realizado na BIOS (tempo de "boot") e o que pode ser realizado durante o tempo normal de execução. Desta forma, operações sensíveis, como ler a chave do registro, não podem ser realizadas por aplicações maliciosas que tentam comprometer a privacidade de algum usuário.

4. Aplicações Importantes do TCPA

4.1 - Proteção de Chaves de Autenticação de Usuários

Devido ao elevado número de vulnerabilidades em sistemas- cliente e à tendência de os "hackers" focarem seus ataques em máquinas-cliente, procurando por nomes e senhas de usuários, é de vital importância prover alguma maneira de proteger informações de autenticação sensível como senhas e chaves-privadas. TCPA provê exatamente esta proteção.

Um usuário pode gerar um par de chaves pública/privada RSA no "chip" TCPA. A chave-privada pode ser configurada para jamais deixar o "chip". Esta chave-privada pode ser utilizada em protocolos seguros, como SSL, para prover forte segurança na autenticação de usuários na Internet. O "chip" TCPA não previne contra os ataques de "hackers" explorando as vulnerabilidades do sistema-cliente, mas certamente protege a chave-privada do usuário. Não importa o que o "hacker" remoto faça, ele não conseguirá obter uma cópia da chave-privada contida no "chip" TCPA.

4.2 - Proteção dos Arquivos e Senhas do Sistema de Arquivos do Usuário

Outra importante aplicação do TCPA é proteger os dados ou arquivos sensíveis do usuário. Utilizando o TCPA, um usuário pode lacrar uma chave de encriptação mestre, para um sistema de arquivos encriptado, em um registrador PCR TCPA. Enquanto o ambiente do sistema operacional se mantiver inalterado, a chave-mestra do sistema de arquivos encriptado pode ser obtida do "chip" TCPA. Se, no entanto, um "hacker" atacar com sucesso um cliente e instalar uma "backdoor" em seu sistema, ou um "software" para a monitoração do teclado, o sistema TCPA perceberá a alteração no sistema operacional e não liberará a chave- mestra do sistema de arquivos encriptado, protegendo, então, os arquivos sensíveis contra o ataque.

5. Críticas ao TCPA e DRM

Nesta seção, será mostrado como a especificação TCPA pode ser utilizada para suportar DRM (“Digital Rights Management”), como, por exemplo, evitar a cópia de dados de música ou vídeo, em favor dos proprietários do conteúdo. Existe, sobretudo, um ataque maior ao projeto conduzido pela Microsoft, enquanto outras empresas da TCG se adiantam em defender seus projetos e juram não compactuar com DRM. Algumas razões favoráveis ao uso do DRM por estas empresas também serão mostradas.

(retirado de http://www.againsttcpa.com/)

5.1 - TCPA suportando DRM

Segundo os críticos, a versão atual do TCPA possui cinco elementos, de forma a suportar o DRM: o "chip" "Fritz", uma facilidade de "memória protegida" pela CPU, um "kernel" de segurança no sistema operacional ("Nexus" na linguagem Microsoft), um "kernel" de segurança em cada aplicativo TCPA ("NCA") e uma infra-estrutura remota de servidores "on-line" de segurança, mantidos por vendedores de "software" e "hardware" para fechar todo o esquema.

A versão inicial do TCPA teria o "Fritz" supervisionando o processo de "boot", de tal maneira que o PC terminasse em um estado previsível, com "hardware" e "software" conhecidos. A versão atual possui o "Fritz" como um componente passivo de monitoração, que armazena o resumo ("hash") do estado da máquina na inicialização. Este "hash" é calculado utilizando-se detalhes de "hardware" (placas de vídeo, de som, etc) e de "software" (sistema operacional, "drivers", etc). Se a máquina termina em um estado aprovado, o "Fritz" disponibilizará para o sistema operacional as chaves criptográficas necessárias para decriptar os aplicativos TCPA e seus dados. Se a máquina termina em um estado ilegal, o "hash" estará diferente e o "Fritz" não liberará as chaves corretas. A máquina ainda estará disponível para executar aplicativos não-TCPA e para acessar dados não-TCPA, mas o material protegido não estará disponível.

O "kernel" de segurança do sistema operacional ("Nexus") interliga o "Fritz" ao "kernel" de segurança em cada aplicativo TCPA ("NCA"). Ele verifica se os componentes de "hardware" são aprovados pela lista da TCG, se os componentes de "software" foram assinados e se nenhum destes possui o número serial revogado. Se mudanças significantes ocorrem na configuração do PC, a máquina deve entrar "on-line" para ser recertificada: o sistema operacional cuida disto. O resultado é o PC, após a execução do "boot", em um estado conhecido, com uma combinação de "hardware" e "software" aprovada (e cujas licenças estão em validade). Finalmente, o "Nexus" trabalha em conjunto com a facilidade de "memória protegida" pela CPU para evitar que qualquer aplicativo TCPA leia ou escreva sobre os dados de outro aplicativo TCPA. Estas capacidades são conhecidas por "Lagrande Technology" (LT) para as CPU’s Intel.

Uma vez que a máquina se encontra em um estado aprovado, com aplicativos TCPA carregados e protegidos contra a interferência de qualquer outro "software", o "Fritz" a certificará para terceiros. Por exemplo, ele irá realizar um protocolo de autenticação com a Disney para provar que esta máquina é um destinatário adequado para sua mídia. Isso significa estar certificando esta máquina como um

usuário de aplicativo autorizado – o "DisneyPlayer", que seja – com seu "NCA" adequadamente carregado e protegido, pela "memória protegida", contra "debuggers" ou outras ferramentas que poderiam ser usadas para acessar, sem a devida autorização, o conteúdo. Em seguida, os servidores da Disney enviam dados encriptados, com a chave que o "Fritz" utilizará para deslacrar o "DisneyPlayer". O "Fritz" disponibiliza as chaves apenas para os aplicativos autorizados e somente enquanto o ambiente permanecer "confiável". Por este propósito, a "confiança" é definida pela política de segurança recebida e controlada pelo servidor do criador da aplicação. Isso significa que a Disney pode insistir, por exemplo, que o aplicativo pegue um dólar toda vez que a mídia seja utilizada. O aplicativo também pode ser alugado. As possibilidades parecem limitadas apenas à imaginação dos vendedores.

5.2 - Interesses Empresariais em TCPA

Além dos interesses destacados na introdução, os críticos tentam mostrar interesses extras para as empresas motivadas no TCPA. É óbvio que empresas criadoras de conteúdo de mídia, como a Disney, apóiam o TCPA na iniciativa de suportar DRM e evitar a pirataria de dados. Empresas de "software" também. Mas quais outros interesses motivariam, por exemplo, a Intel?

Para a Intel, que começou com todo este esquema do TCPA, esta era uma estratégia defensiva. Como a Intel faz a grande parte do seu dinheiro a partir de microprocessadores de PC e possui a maior parte do mercado, ela poderá crescer apenas se aumentar o tamanho do mercado. A Intel está determinada de que o PC será o "hub" da rede caseira do futuro. Se o entretenimento será uma aplicação vital e se DRM será a tecnologia habilitadora crítica, então o PC deve realizar DRM ou se arrisca a sair do mercado caseiro. Uma primeira tentativa veio com o número serial dos processadores Pentium 3, em meados dos anos 90, mas devido à reação adversa do público, a Intel recuou e esperou para realizar um consórcio (TCPA) com a Microsoft e outras empresas. E quais seriam os interesses extras da Microsoft, por exemplo?

"We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains."(Bill Gates)

(retirado de http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html)

Microsoft, que agora está impulsionando a TCG, possui duas razões principais para isso: A primeira, e menos importante, é que ela poderá cortar dramaticamente a pirataria de "software". Com as especificações TCPA, a Microsoft pode amarrar cada PC à sua cópia individual e licenciada do Office e Windows, e eliminar as cópias ilegais de Office e Windows do maravilhoso universo TCPA.

O segundo, e mais importante, benefício para a Microsoft é que o TCPA aumentará, dramaticamente, os custos de mudança de produtos Microsoft (como o "Office") para produtos rivais (como "OpenOffice"). Vale ressaltar que estudos econômicos respeitados concluem que o valor de um negócio relacionado a "software" é, aproximadamente, igual aos custos totais de seus clientes mudando para seu competidor.

Por exemplo, algum tempo atrás, quando compatibilidade significava trabalhar com vários formatos de arquivos, mesmo os concorrentes, existia um conflito real - quando "Word" e "Word Perfect" lutavam pela dominância do mercado, cada um tentava ler os arquivos do outro e fazer com que o outro não pudesse ler seus arquivos. Mas, com a TCPA, o jogo está terminado; sem o acesso às chaves, pode garantir- se que os arquivos não serão lidos pelo concorrente, ou até mesmo, pode garantir-se que arquivos sejam rejeitados pelo aplicativo TCPA se foram criados com cópias de uma

versão anterior deste mesmo "software", mas cujos números seriais foram colocados em listas negras de cópias piratas.

Embora na Europa, a "EU Software Directive" permita que companhias européias façam engenharia reversa nos produtos dos seus competidores no intuito de produzir compatibilidade e produtos mais competitivos, estas leis, na maioria dos casos, apenas garantem o direito de tentar, e não de conseguir realizar isto!

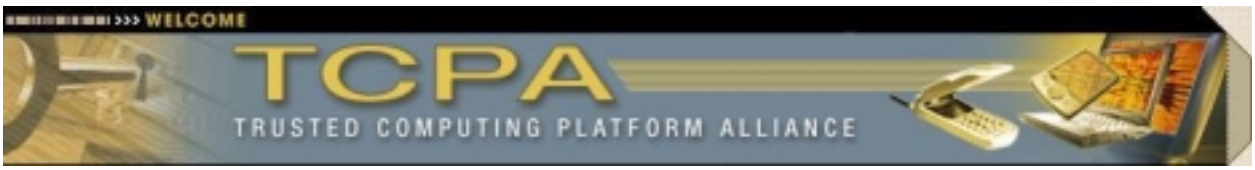
Então, uma firma de advocacia que pretende mudar de "Office" para "OpenOffice" agora, simplesmente precisa instalar o "software", treinar a equipe e converter os arquivos existentes. Em cinco anos, uma vez que esta firma tiver recebido documentos protegidos por TCPA de, talvez, mil clientes diferentes, ela precisará conseguir permissões (na forma de certificados assinados digitalmente) de cada um destes clientes para migrar os seus arquivos para a nova plataforma. A firma, na prática, não estará interessada nisso. Então, estará muito mais amarrada aos produtos da Microsoft, que poderá impor seus preços.

Estas empresas têm interesse também no aumento da prática de comércio e pagamentos eletrônicos. Muitas das funcionalidades dos cartões bancários poderiam ser passados para "software", uma vez que os aplicativos se tornarão seguros com a TCPA. Desta forma, se, no espaço de tempo de dez anos, será inconveniente realizar compras "online" com seu cartão de crédito a menos que você esteja utilizando uma plataforma TCPA, então a situação ficará complicada para os usuários GNU/Linux.

Além disso, se a maioria dos desenvolvedores de "software" habilitarem seus aplicativos para a especificação TCPA e se o "Windows" for o primeiro sistema operacional a suportar a TCPA, então ele adquirirá uma maior vantagem competitiva sobre o GNU/Linux junto à comunidade desenvolvedora.

A questão fundamental é que qualquer um que controle a infraestrutura TCPA estará adquirindo uma enorme quantidade de poder. E existem diversas formas em que este poder pode ser abusivo. Imaginem que o ambiente de computação já fosse totalmente TCPA; e imaginem que o governo norte-americano julgasse a atitude da imprensa como uma atitude não patriótica, no ato da divulgação das fotos das "brincadeiras" dos combatentes norte- americanos, no Iraque. Certamente o poder TCPA seria utilizado rapidamente na forma de censura.

6. Defensores do TCPA



(retirado de http://www.trustedcomputing.org/home)

Algumas das críticas à TCPA a acusam de ser, primordialmente, voltada para atender aos anseios do DRM. Estas críticas argumentam que a TCPA retiraria os direitos dos usuários em suas próprias máquinas, não permitindo “backup” nem deslocamento de tempo ou espaço de conteúdo comprado legalmente.

Os méritos do DRM são um tópico complexo e foram abordados no tópico anterior, mas é fácil, segundo a IBM (como argumentado em [1]), apontar características do “chip” TCPA que o tornam

inadequado para a realização das tarefas em prol do DRM. Além disso, a implementação da IBM para este ”chip”não foi projetada, nem disponibilizada, com a proteção antifalsificação necessária para prover, efetivamente, proteção anticlonagem de dados.

O “chip” TCPA não é, particularmente, adequado para o DRM. Embora ele realmente possua a habilidade de reportar informação assinada do PCR, e o fato de esta informação poder ser utilizada para prevenir a reprodução dos dados, a menos que sistema operacional e aplicativos confiáveis estejam em uso, este tipo de estratégia seria um pesadelo de se gerenciar pelos provedores de conteúdo. A cada qualquer alteração na BIOS, no sistema operacional, ou no aplicativo, ocorreria a alteração dos valores reportados. De que forma os provedores de conteúdo poderiam reconhecer quais valores de PCR seriam válidos, dada a enorme quantidade de plataformas, versões de sistemas operacionais e freqüentes pacotes de reparo de “software”?

Segundo, a versão do “chip” TCPA produzida pela IBM se localiza no barramento LPC, o qual é facilmente monitorável. O “chip” não é defendido contra análises de potência, rádio- freqüência ou temporização. O ponto fraco seria então o fato de que o proprietário físico da máquina poderia, facilmente, recuperar qualquer segredo relativo aos DRM contido no “chip”. A razão para esta aparente “negligência” neste “chip” está no propósito do “chip”, que é de defender os dados do usuário contra ataques remotos, e não contra ataques do próprio usuário.

Além disso, como defendido em [4], condenar TCPA por sua potencialidade em permitir o uso de aplicações em prol do DRM seria um absurdo. Seria o mesmo que apoiar alguns governos em suas tentativas de banir a encriptação de dados, pois a encriptação poderia ser usada por terroristas para esconder suas mensagens.

7. Conclusão

"Hackers" na Internet representam uma ameaça aos clientes e à autenticação utilizada em aplicações de comércio eletrônico. Nossos sistemas operacionais e aplicativos do lado cliente são tão complexos que falhas e vulnerabilidades de segurança em "software" são virtualmente inevitáveis. Torna-se, então, crítica a necessidade de provisão de alguma base de "hardware" de proteção para as chaves de autenticação e encriptação, que as proteja de "hackers" até mesmo na presença de vulnerabilidades de "software". TCPA busca prover esta função crítica de "hardware" de segurança, protegendo a autenticação de um usuário e as chaves de encriptação contra ataques remotos de "software".

TCPA também pode buscar prover a transferência de controle de "software", do proprietário da máquina, para o autor do "software". Como analisado, isto pode trazer conseqüências econômicas globais no século da informação. Portanto, faz-se necessário o debate e divulgação do tema entre a comunidade.

8. Bibliografia

[1] - Safford, David. *The Need for TCPA.* IBM. Outubro, 2002. 7p. Encontrado em: http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf

[2] - Anderson, Ross. *'Trusted Computing' Frequently Asked Questions.* Version 1.1. University of Cambridge, Computer Laboratory. Agosto, 2003. Encontrado em: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

[3] - Arbaugh, William A. *The TCPA; What's wrong; What's right and what to do about.* University of Maryland, Department of Computer Science and UMIACS. 20 de Julho, 2002. Encontrado em: http://www.cs.umd.edu/~waa/TCPA/TCPA-goodnbad.html

[4] - Safford, David. *Clarifying Misinformation on TCPA.* IBM. Outubro, 2002. 7p. Encontrado em: http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf

[5] - Trusted Computing Platform Alliance (TCPA). *Trusted Platform Module Protection Profile.* Version 1.9.7. TCPA Membership. 01 de Julho, 2002. 64p. Encontrado em: http://www.trustedcomputing.org/home

[6] - Trusted Computing Platform Alliance (TCPA). *TCPA PC Specific Implementation Specification.* Version 1.00. TCPA Membership. 09 de Setembro, 2001. 71p. Encontrado em: http://www.trustedcomputing.org/home

9. Questionário

1. Quais são as principais categorias de vulnerabilidades encontradas em sistemas de computação? Descreva, sucintamente, cada uma delas.

R.: A primeira categoria de vulnerabilidades encontradas em sistemas de computação são os Programas Inseguros, cujo projeto é, inerentemente, inseguro no ambiente da Internet, pois, simplesmente, não havia segurança em mente quando estes foram concebidos. A segunda categoria são os Programas Mal-Configurados, que possuem facilidades adequadas de segurança em seu projeto e requerem que estas sejam, devidamente, configuradas, o que nem sempre é realizado por usuários inexperientes. A terceira categoria são os Programas com Falhas, os quais possuem projeto de segurança e configurações apropriadas, mas que possuem falhas de implementação ou codificação que podem ser explorados remotamente.

2. Explique o esquema de criptografia assimétrica e mostre os diferenciais existentes na especificação TCPA.

R.: Qualquer pessoa pode enviar uma mensagem confidencial para outra apenas utilizando chave-pública do destinatário, que é de conhecimento público, à princípio; Não há maiores preocupações em se esconder a chave-pública pois a mensagem só poderá ser decriptada com a chave-privada do destinatário. O diferencial da especificação TCPA é que esta chave- privada se encontra armazenada em "hardware" e pode ser configurada para nunca deixá- lo, ou seja, o "chip" TCPA impede qualquer acesso não-autorizado à chave-privada do usuário.

3. Explique como funciona a aplicação do TCPA na proteção do sistema de arquivos do usuário.

R.: Utilizando o TCPA, um usuário pode lacrar uma chave de encriptação mestre, para um sistema de arquivos encriptado, em um registrador PCR TCPA. Enquanto o ambiente do sistema operacional se mantiver inalterado, a chave-mestra do sistema de arquivos encriptado pode ser obtida do "chip" TCPA. Se, no entanto, um "hacker" atacar com sucesso um cliente e instalar uma "backdoor" em seu sistema, ou um "software" para a monitoração do teclado, o sistema TCPA perceberá a alteração no sistema operacional e não liberará a chave-mestra do sistema de arquivos encriptado, protegendo, então, os arquivos sensíveis contra o ataque.

4. Quais são as principais críticas recebidas e controvérsias apontadas contra o TCPA?

R.: Os críticos afirmam que os principais objetivos do TCPA seriam transferir o controle do proprietário do computador para aquele que tenha escrito os "softwares" que o computador esteja executando e suportar "Digital Rights Management" (DRM). Os críticos apontam as controvérsias entre as diversas definições de confiança; as máquinas, construídas segundo as especificações TCPA, serão mais confiáveis do ponto de vista dos vendedores de "software" e da indústria de conteúdo, mas serão menos confiáveis do ponto de vista dos proprietários destas máquinas.

5. Se a facilidade TCPA pode parecer tão assustadora, por que não é conveniente desabilitá-la?

R.: Primeiro, podem haver casos em que o uso de TCPA é obrigatório, definido pela administração estratégica da sua empresa, por exemplo. Se sua empresa não adotar o uso de aplicativos TCPA, ela corre o risco de ficar isolada se todos as outras empresas usam TCPA. Neste ambiente hostil, todos os aplicativos TCPA podem ser configurados, remotamente por seus autores, para rejeitar os dados de aplicativos que não sejam TCPA, como os seus. Segundo, se a facilidade TCPA for desabilitada, as chaves para decriptar os aplicativos TCPA e seus arquivos não poderão ser acessadas. Terceiro, pela lógica da evolução dos "softwares", os aplicativos TCPA serão capazes de agregar maior valor ao seu trabalho e, por competição, faz-se necessário o uso destes.