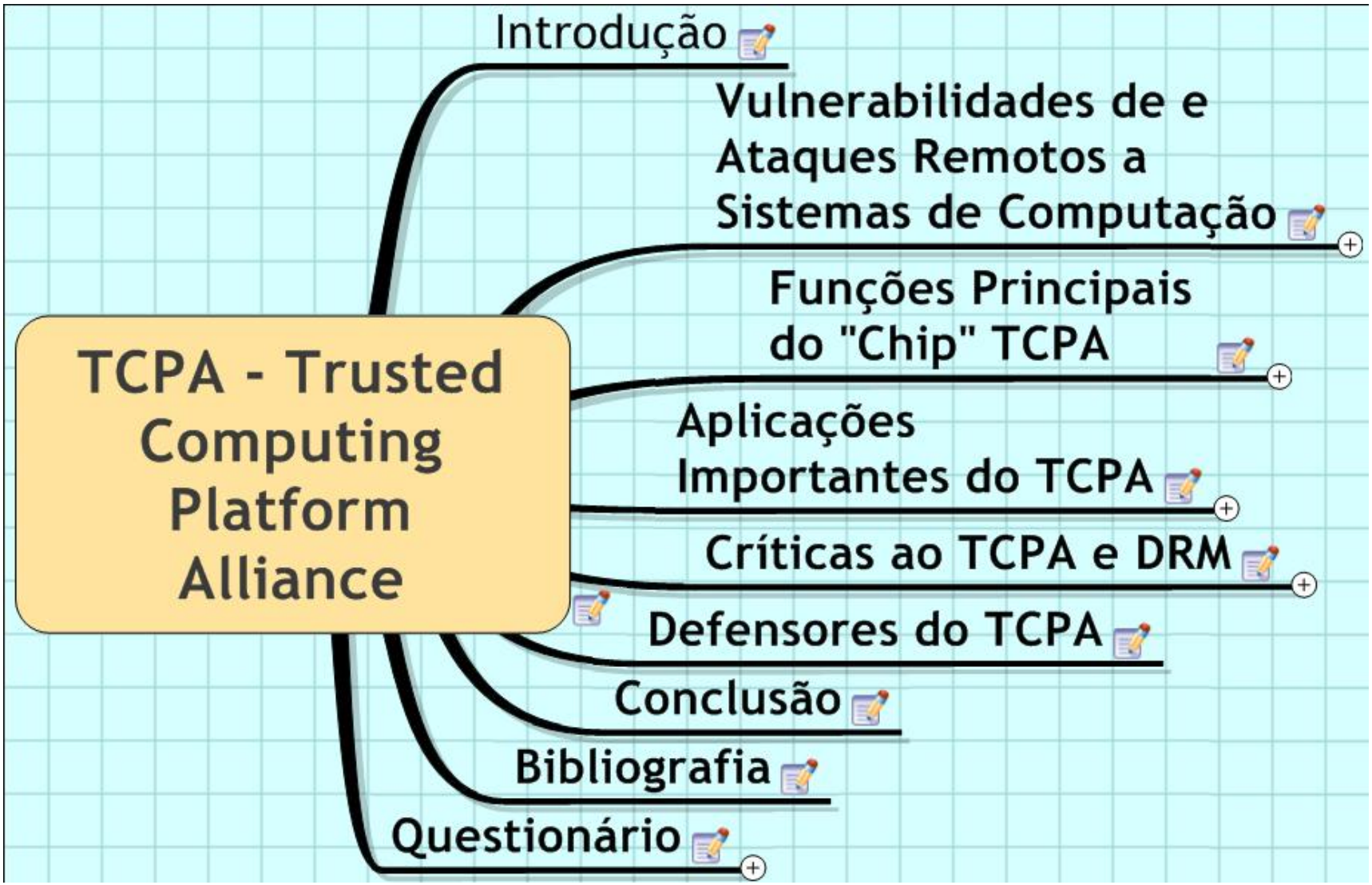
TCPA – Trusted Computing Platform Alliance

Autor: *Vitor Ugo Brevilieri*

27 de Maio de 2004

Universidade Federal do Rio de Janeiro
Departamento de Engenharia Eletrônica e da Computação
Disciplina: Redes I Turma: 2004/1
Prof.: *Otto Carlos Muniz Bandeira Duarte*

Índice


TCPA - Trusted Computing Platform Alliance
Introdução
Vulnerabilidades de e Ataques Remotos a Sistemas de Computação
Funções Principais do "Chip" TCPA
Aplicações Importantes do TCPA
Críticas ao TCPA e DRM
Defensores do TCPA
Conclusão
Bibliografia
Questionário

Introdução

Roger Schell, em “Preliminary Notes on the Design of Secure Military Computer Systems”(1973), 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.”

Introdução

Previsão dos Sistemas de Computação atuais, feitas por Roger Schell:

- Não projetados para as ameaças da internet moderna;
- Mal implementados;
- Requerem a contínua instalação de pacotes de segurança.

Conseqüência:
Incompatibilidades e ataques remotos comprometem milhares de sistemas, em taxas crescentes.

Introdução

Compaq, HP, IBM, Intel e Microsoft fundam a TCPA, em 1999. Missão da TCPA:

“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”

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

Introdução

TCPA produz especificações abertas para a base de "hardware" necessária às máquinas-cliente, isto é, o "chip" TCPA, e para as interfaces de "software" relacionadas.

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

Especificações abertas, amplamente suportadas, acelerarão o projeto, o uso, o gerenciamento e a adoção dos sistemas confiáveis.

Introdução

"Status" da organização em 2003:

- ± 200 membros;
- Milhares de Críticos na Europa e Estados Unidos

Em 8 de Abril de 2003, ocorre a criação da TCG, Trusted Computing Group, por AMD, HP(Compaq), IBM, Intel e Microsoft. Todos os membros da TCPA são convidados.

Introdução

- A TCPA reconhece a TCG como sua sucessora;
- A TCG incorpora as especificações TCPA como sendo seu ponto inicial, pretendendo:
  - Aperfeiçoá-las;
  - Estendê-las para diversos dispositivos de computação digital (PDA’s, telefones, etc.);

Introdução

Termos relacionados:

- “Trusted Computing” (IBM);
- “Trustworthy Computing”, “Palladium” e “NGSCB” (Microsoft);
- “Safer Computing” (Intel);

- “Treacherous Computing” (Free Software Foundation).

Introdução

Críticas:

• Vasta gama de nomes é propositadamente, pretende confundir consumidores e desviar a atenção daquilo que realmente está por trás disto tudo;

• Transferir o controle do proprietário do computador para o autor do “software” que o computador esteja executando.

• Um dos objetivos principais da TCPA seria suportar “Digital Rights Management” (DRM).

Introdução

Críticas: O que é “confiável”?

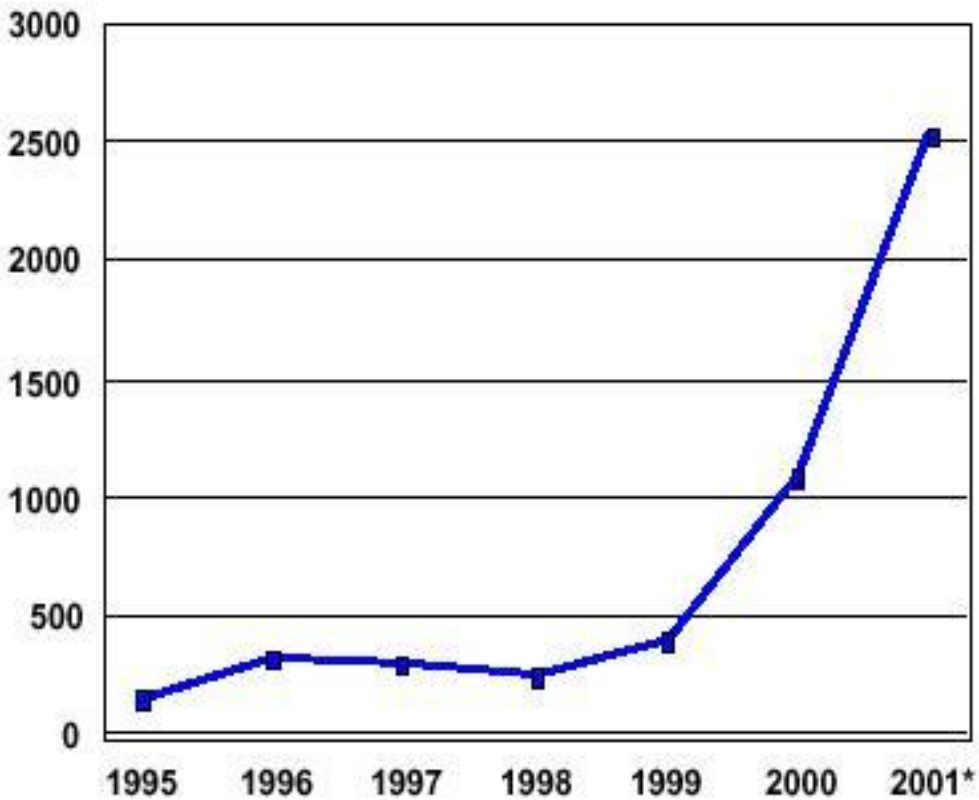
• As máquinas construídas segundo as especificações TCPA serão mais confiáveis do ponto de vista dos vendedores de “software” e da indústria de conteúdo;

• Mas serão menos confiáveis do ponto de vista dos proprietários destas máquinas.

Alvo Preferencial: Microsoft.

Vulnerabilidades de e Ataques Remotos a Sistemas de Computação

Erros de “software”: quantidade anual descoberta



Sistemas Complexos:

$(1x10^8)$linhas

x (1erro/1000 linhas)

100000 erros

Como corrigí-los?!

Paraíso dos “Hackers”

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

Vulnerabilidades de e Ataques Remotos a Sistemas de Computação

Tipos de Vulnerabilidades freqüentes:

• Programas inseguros: "telnet" e "ftp", que, normalmente, enviam nomes e senhas de usuários pela rede sem ao menos encriptá-los.

• Programas Mal-Configurados: NFS (“Network File System"), que pode ser configurado para exportar um sistema de arquivos em modo de leitura apenas, ou em modo de leitura e escrita para todos os domínios de usuários.

Vulnerabilidades de e Ataques Remotos a Sistemas de Computação

Tipos de Vulnerabilidades freqüentes:

- Programas com Falhas: estouros de "buffer". Com tamanho fixo de armazenagem, deve-se realizar a verificação da quantidade de dados de entrada. São erros, há tempos, conhecidos e freqüentes.

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

Vulnerabilidades de e Ataques Remotos a Sistemas de Computação

Tendências Evolutivas dos Ataques “Hackers”:

- Anos 80, atacavam as redes, espionando, em busca de senhas, e invadindo sessões → Aplicativos encriptam os dados que atravessam a rede;
- Voltaram-se para atacar diretamente os servidores, principalmente através de configurações mal realizadas e serviços com falhas, como servidores “web” → Empresas usam “firewalls”, detecção de intrusos e ferramentas de verificação de segurança
- Começaram a focar os ataques em clientes.

Vulnerabilidades de e Ataques Remotos a Sistemas de Computação

Interesses nos computadores-cliente:

- Computadores-cliente possuem nomes e senhas de usuários utilizados em servidores que poderão ser atacados.
- Computadores-cliente são uma grande fonte disponível de máquinas de onde se podem lançar ataques DDoS("Distributed Denial of Service").

O aumento destes ataques representa ameaças crescentes, para usuários e servidores, em negócios eletrônicos. A autenticação torna-se um fator crítico.

Funções Principais do “Chip” TCPA

IBM (2000) - “Embedded Security Subsystem” (“chip” ESS) em PC PL300 e “notebook” “T23 Thinkpad Systems”;

O “chip” ESS é, basicamente, um “chip” “smartcard” sobre a placa-mãe e possui uma chave-pública. Redução de custos no projeto do sistema.

Outras empresas querem soluções semelhantes e surge a necessidade de padronização da questão, que seria atingida com a criação da TCPA.

Funções Principais do “Chip” TCPA

Funções de Chave-pública (criptografia assimétrica):

Funções Principais do “Chip” TCPA

Funções de Chave-pública:

Funções Principais do “Chip” TCPA

Funções de Chave-pública:

Funções Principais do “Chip” TCPA

Funções de Chave-pública:

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

Funções Principais do “Chip” TCPA

Funções de Chave-pública:

• 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.

• Geralmente, a criptografia assimétrica é utilizada para a distribuição da chave simétrica ao destinatário. Após esta passagem, utiliza-se a criptografia simétrica em cima dos dados.

Funções Principais do “Chip” TCPA

Funções de “Boot” Confiável:

- Armazenar, em PCRs, “hashes” de informações de configuração, ao longo da seqüência de “boot”.
- Após o “boot”, dados, como chaves simétricas para arquivos encriptados, podem ser lacrados em um PCR, para garantir autenticidade. Os dados lacrados só poderão ser lidos se o PCR possuir o mesmo valor que possuía no momento da lacração.
- Se uma tentativa é feita de executar o “boot” de um sistema alternativo, ou se um vírus tiver utilizado uma “backdoor” no SO, o valor do PCR não irá coincidir e a deslacração dos dados irá falhar.

Funções Principais do “Chip” TCPA

Funções de Inicialização e Gerenciamento:

- Permitem ao proprietário do sistema que ele altere as funcionalidades, reinicialize e tome propriedade sobre o sistema.
- Funções complexas, de forma a tornar 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.

Aplicações Importantes do TCPA

Proteção das Chaves de Autenticação dos Usuários:

- É importante prover uma maneira de proteger informações de autenticação sensíveis, como senhas e chaves-privadas, mesmo que os ataques “hackers” tenham sucesso. Lembre das tendências evolutivas.
- Pode-se gerar um par de chaves-pública/privada RSA no “chip” TCPA. A chave-privada pode ser configurada para jamais deixar o “chip”. O “chip” TCPA não previne contra os ataques de “hackers” remotos, mas certamente protege a chave-privada do usuário, que está contida no “chip” TCPA.

Aplicações Importantes do TCPA

Proteção dos Arquivos e Senhas do Sistema de Arquivos dos Usuários:

• Com o TCPA, um usuário pode lacrar uma chave de encriptação mestre, para um sistema de arquivos, em um registrador PCR-TCPA. Enquanto o ambiente do SO se mantiver inalterado, a chave-mestra do sistema de arquivos encriptado pode ser obtida do "chip" TCPA. Se, no entanto, um "hacker" atacar um cliente e instalar uma "backdoor", o sistema TCPA perceberá a alteração no SO e não liberará a chave-mestra do sistema de arquivos encriptado, protegendo, então, os arquivos contra o ataque.

Críticas ao TCPA e DRM

Mecanismo TCPA suportando DRM:

Os cinco elementos do TCPA suportando o DRM:

- o “chip” “Fritz”(pejorativo para o “chip” TCPA);
- 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”);
- uma infra-estrutura remota de servidores “on-line” de segurança, mantidos por vendedores de “software” e “hardware” para fechar todo o esquema.

Críticas ao TCPA e DRM

Mecanismo TCPA suportando DRM:

• O “Fritz” é um componente de monitoração, que armazena o “hash” do estado da máquina na inicialização. Este “hash” é calculado utilizando-se detalhes de “hardware” e de “software”(SO, “drivers”, etc). Se a máquina entra em um estado aprovado, o “Fritz” disponibilizará para o SO as cripto-chaves necessárias para decriptar os aplicativos TCPA e seus dados. Caso contrário, o “hash” estará diferente e o “Fritz” não liberará essas chaves. A máquina ainda estará disponível para executar aplicativos não-TCPA e para acessar dados não-TCPA, mas o material protegido não estará disponível.

Críticas ao TCPA e DRM

Mecanismo TCPA suportando DRM:

• O “Nexus” interliga o “Fritz” aos “NCAs”. Ele verifica se o “hardware” é aprovado 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).

Críticas ao TCPA e DRM

Mecanismo TCPA suportando DRM:

- 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.

Críticas ao TCPA e DRM

Mecanismo TCPA suportando DRM:

Por exemplo, ele irá realizar um protocolo de autenticação com a Disney para provar que esta máquina é um destinatário adequado para sua mídia, ou seja, nela está instalado o “DisneyPlayer”,com seu “NCA” carregado e protegido pela “memória protegida” contra “debuggers”.
Em seguida, os servidores da Disney enviam dados encriptados, com a chave que o “Fritz” utilizará para deslacrar o “DisneyPlayer”.

Críticas ao TCPA e DRM

Mecanismo TCPA suportando DRM:

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 do e controlada pelo servidor do autor da aplicação. Isto é, 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 exploração comercial parece limitada só à imaginação dos vendedores.

Críticas ao TCPA e DRM

Interesses Empresariais em TCPA:

Além dos interesses louváveis descritos na introdução, e da anti-pirataria possível com o DRM para a Disney e empresas de “software”, quais seriam os interesses extras das empresas-membro do TCPA?

Críticas ao TCPA e DRM

Interesses Empresariais em TCPA:

Intel – microprocessadores de PC - Líder do TCPA:

• É uma estratégia defensiva. Como possui a maior parte do mercado, só poderá crescer 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.

Críticas ao TCPA e DRM

Interesses Empresariais em TCPA:

Microsoft – “softwares” de PC - Líder do TCG:

- Anti-pirataria;

“Bill Gates has dreamed of finding a way to make the Chinese pay for Software” (Ross Anderson)

- Aumentar os custos de mudança de produtos Microsoft (como o “Office”) para produtos rivais (como “OpenOffice”);

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

Críticas ao TCPA e DRM

Interesses Empresariais em TCPA:

• 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, cujos aplicativos raramente entrarão na lista de aprovados TCG.

Críticas ao TCPA e DRM

Interesses Empresariais em TCPA:

• 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.

Críticas ao TCPA e DRM

Interesses Empresariais em TCPA:

• 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.

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

Defensores do TCPA

É fácil, segundo a IBM, 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 proteção anticlonagem de dados. A IBM não defende (diferente de “repudia”) o projeto Microsoft.

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

Defensores do TCPA

- 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.

Defensores do TCPA

• 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”?

• 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.

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.

Conclusão

• 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”.

Conclusão

• 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.

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

Bibliografia

[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

Questionário

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

Questionário

R1.: Programas Inseguros - seu projeto é inseguro no ambiente da Internet, pois não havia segurança em mente quando estes foram concebidos.

Programas Mal-Configurados - possuem facilidades adequadas de segurança e requerem que estas sejam, devidamente, configuradas, o que é raro.

Programas com Falhas - possuem projeto de segurança e configurações apropriadas, mas possuem falhas de implementação ou codificação que podem ser explorados remotamente.

Questionário

2. Explique o esquema de criptografia assimétrica e mostre o diferencial existente na especificação TCPA.

Questionário

R2.: Qualquer pessoa pode enviar uma mensagem confidencial para outra utilizando, apenas, a 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.

Questionário

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

Questionário

R3.: Com o TCPA, um usuário pode lacrar uma chave de encriptação mestre, para um sistema de arquivos, em um registrador PCR-TCPA. Enquanto o ambiente do SO se mantiver inalterado, a chave-mestra do sistema de arquivos encriptado pode ser obtida do “chip” TCPA. Se, no entanto, um “hacker” atacar um cliente e instalar uma “backdoor”, ou um “software” para a monitoração do teclado, o sistema TCPA perceberá a alteração no SO e não liberará a chave-mestra do sistema de arquivos encriptado, protegendo, então, os arquivos contra o ataque.

Questionário

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

Questionário

R4.: Os críticos afirmam que os principais objetivos do TCPA seriam: transferir o controle do proprietário do computador para o autor dos “softwares” que o computador esteja executando e suportar “Digital Rights Management” (DRM).

Os críticos apontam as seguintes controvérsias nas 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 das máquinas.

Questionário

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

Questionário

R5.: Podem haver casos em que usar TCPA seja obrigatório, definido pela administração de uma empresa. Se a empresa não adotar o TCPA, ela arrisca ficar isolada, se todos as outras empresas usam TCPA. Neste ambiente, todos os aplicativos TCPA podem ser configurados, remotamente por seus autores, para rejeitar os dados de aplicativos não-TCPA. Segundo, as chaves para decriptar os aplicativos TCPA e seus arquivos não poderão ser acessadas. Terceiro, os aplicativos TCPA serão capazes de agregar maior valor ao seu trabalho e, por competição, faz-se necessário o uso destes.