Facultat d'Informàtica de Barcelona
UNIVERSITAT POLITÈCNICA DE CATALUNYA

CONCEPTES AVANÇATS DE SISTEMES OPERATIUS
Departament d'Arquitectura de Computadors

# Arquitectures amb TCPA i SO Palladium

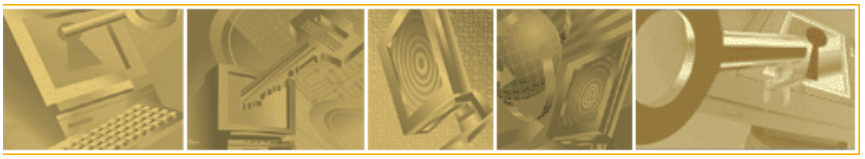
(Seminaris de CASO)

Autors
**Xavier Vilademunt Gómez**
**David Carrascal Rierola**

Facultat d'Informàtica de Barcelona
UNIVERSITAT POLITÈCNICA DE CATALUNYA

CONCEPTES AVANÇATS DE SISTEMES OPERATIUS
Departament d'Arquitectura de Computadors

# TCPA



## Què és TCPA?

- Trusted Computing Platform Aliance.
- Unió de la majoria de les empreses més importants en el món del hardware i el software:
  - Compaq, HP, Intel, IBM i Microsoft com a fundadores
  - Adobe, American Express, American Megatrends, AMD, Motorola, National Semiconductors, Dell, Novell, Philips, Samsung, Fujitsu, Siemens, etc.

  amb l'objectiu de crear unes especificacions públiques destinades a millorar la seguretat dels sistemes informàtics.
- Comporta un canvi a nivell de l'arquitectura del PC instal·lant dos components passius, és a dir que no tindran control sobre les accions de l'ordinador en el seu us normal sinó que el proveiran de diverses funcionalitats noves.



## Què es pretén?

- Amb TCPA es busca incrementar el nivell de seguretat existent avui en dia als PC convencionals.
- Als últims anys el problema dels atacs remots s'ha incrementat gairebé exponencialment. Bàsicament tres tipus d'atacs:
  - Programes insegurs: telnet, ftp... Trames no encriptades
  - Programes mal configurats: Permeten seguretat però l'usuari no ho fa servir
  - Programes amb bugs: Errors de programació, els més perillosos actualment
    - Buffer Overflows i Parsing Errors

## Com funciona?

- Fins ara, segons la nomenclatura que utilitza TCPA, un PC es podia dividir en diferents nivells:

| | |
|---|---|
| Sistema | Perifèrics, drivers i aplicacions |
| Plataforma | Unitats de disc, targetes, font alimentació |
| Placa Base | CPU, memòria, bussos d'interconnexió |
| Microprocessador | |



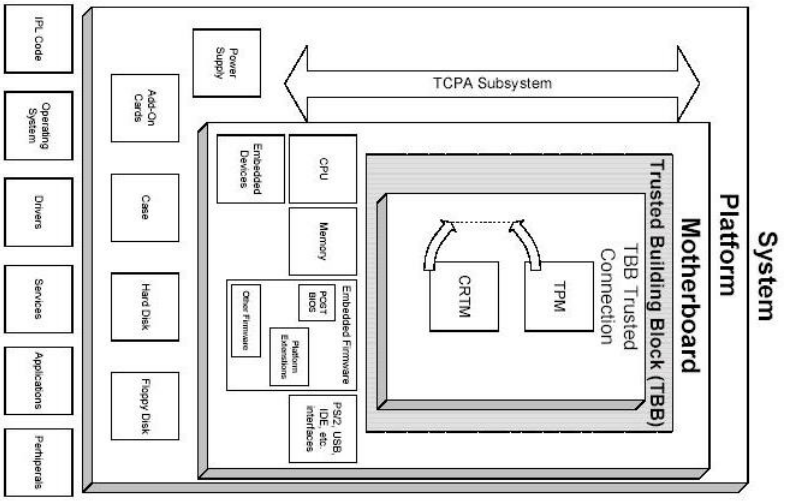
## Com funciona?

- El nou model que TCPA proposa, introdueix algun canvi en aquesta concepció:

| | |
|---|---|
| Sistema | Sense cap canvi |
| Plataforma | El subsistema TCPA està en aquest nivell |
| Placa Base | CPU, memòria, bussos d'interconnexió |
| Microprocessador | |
| TBB | Format per dos components: TPM i CRTM |

- El subsistema TCPA és el conjunt de tots els components hardware que s'usen en TCPA: TBB, CPU, memòria, etc.

# Com funciona?






# CRTM (Core Root of Trust Module)

- És el mòdul des d'on es comença l'execució quan el sistema arranca (també després d'un reset).
- Es considera indispensable que romangui inalterable i que la seva integritat estigui sempre assegurada.
- És equivalent a les BIOS actuals. Es pot actualitzar, encara que només ho podrà fer el fabricant.
- Quan s'arranca el PC, el CRTM comprova:
  - La seva pròpia integritat
  - Els components del sistema
  - Les ROM dels perifèrics
  - El codi d'arrancada del que s'executarà a continuació: IPL

## TPM (Trusted Platform Module)

- És el component més important. Ha d'estar unit a la placa base (físicament o mitjançant una SmartCard).
- Conté:
  - 8 registres de 32 bits: PCR[0], PCR[1], ..., PCR[7]. Cada PCR fa referència a l'estat de parts del sistema en conjunt.
  - Varis algoritmes criptogràfics microprogramats: SHA-1, RSA, RNG, 3DES (la versió 2.0 de TCPA incorporarà AES).
  - Operacions que es faran servir per comprovar la integritat del sistema.
- Amb aquestes característiques, el TPM ens ajudarà a saber si ha canviat l'estat del sistema: canvi en l'arquitectura o en el software. Però és un element que no pren decisions.



## Funcionament del TBB

- Així és com actua el sistema en una seqüència d'arrancada:

1. El CRTM comprova la seva integritat.
2. El CRTM, usant les funcions que li ofereix el TPM, omple els 8 registres amb l'estat actual del sistema.
3. Es passa el control a l'IPL (carregador del SO) que anirà estenent la cadena de confiança.

- La cadena de confiança és la seguretat que ens dóna TCPA de que el nostre sistema és segur fins aquell moment.

## Reacció del SO

- Quan s'ha carregat el SO, aquest farà les comprovacions que cregui pertinents (si es que vol fer-les) del canvis que han succeït al sistema. Això es fa comprovant els valors dels PCR i comparant-los amb una Taula de Logs carregades en espai de sistema.
- Aquestes comprovacions no són obligatòries: només les fan els SO que vulguin utilitzar les capacitats que TCPA els ofereix de comprovar canvis. Els programadors decideixen.
- Opcions:
  - No acceptar els canvis inesperats
  - Ignorar la informació



## Altres aportacions de TCPA

- Emmagatzematge protegit: Mitjançant firmes digitals, es poden protegir dades.
  - Es guarda una taula amb:
    - Les claus que s'empren per signar un hash de les dades a més de les que s'usen per comprovar la signatura.
    - Les claus que s'empren per xifrar/desxifrar les dades amb el hash concatenat.
  - Aquestes claus estan xifrades amb una clau (que actua com a clau mestra) generada a la TPM i protegida per hardware.

  Les dades i les claus encriptades es poden compartir amb altres sistemes.

## Altres aportacions de TCPA

- Identitats: es donen els mecanismes per obtenir un certificat d'una Autoritat Certificadora (AC) de forma anònima.
- L'objectiu que es busca és l'anonimat:
  - Mitjançant un sistema de firmes s'aconsegueix expedir un certificat a una TPM que li demani.
  - Quan es faci servir aquesta nova identitat, tothom tindrà la certesa que el certificat pertany a una TPM però ningú sabrà a quina TPM pertany.
- A la pràctica, aquest anonimat pot no existir:
  - Una AC pot guardar-se la ip del sistema que li ha fet la requesta. Es podrà saber quin sistema fa servir aquell certificat.
  - No es deixa clar si per demanar el certificat el TPM ha d'enviar un identificador únic. Si fos així, diferents AC podrien fer un matching dels certificats d'un TPM.



## Conclusions TCPA

- És un estàndard obert, no està dissenyat per un SO en particular: hi ha drivers tant per Linux com per Windows.
- Basa gran part del seu treball en la confiança sobre AC, amb el problema que aquestes poden identificar qui ha fet la petició i després relacionar l'usuari amb les seves accions comprometent l'anonimat de l'usuari.
- Es podrà desactivar sempre que es vulgui.
- Ja hi ha sistemes (els ThinkPad de IBM) que incorporen versions light de TCPA (anomenades ESS).
- Començarà a implantar-se en un futur no molt llunyà.

# Palladium

## Què és Palladium?

- Forma part de NGSCB: Next-generation secure computing base:
  - Una nova implementació de TCPA anomenada SSC.
  - Un nou model de Sistema Operatiu anomenat Palladium.
- Proposta de Microsoft per crear un entorn més segur a l'usuari.
- Es busca:
  - Protecció extrema de zones de memòria.
  - Potenciar els DRM (Digital Rights Management).
  - Entrades / sortides segures.
  - Protecció d'arxius.

## SSC (Security Support Component)

- Extensió de les característiques de TCPA, diferències:
  - Proporciona protecció hardware per cada procés de la seva zona de memòria.
  - Proporciona mecanismes per protegir l'entrada / sortida d'un usuari.
  - Autenticació de l'arrancada de la part del kernel que s'encarrega de guardar les dades protegides en memòria ( TOR o nexus).



## Com funciona Palladium?

- Els canvis fonamentals es centren a nivell kernel. Dos nous components:
  - TOR (Trusted Operating Root) més conegut com Nexus.
  - TA (Trusted Agents).
- Nexus:
  - Controla les crides al sistema.
  - Emmagatzematge de dades crítiques
  - Protegeix la zona de memòria on resideix el kernel i les dades encriptades que s'hi guardin dels processos d'usuari.

## Com funciona Palladium?

- TA:
  - Programes que s'executen en mode usuari en una zona de memòria especial anomenada "trusted space".
  - Usen funcions del Nexus per encriptar dades i guardarles a l'espai del kernel. Aquestes dades només les podrà consultar el TA que les ha guardat.
  - Aquests programes tindran més prioritat alhora de ser atesos quan facin una crida de sistema.



## Com funciona Palladium?

- Protecció de memòria:
  - Es pretén que el Nexus impedeixi l'accés a les pàgines de memòria principal d'altres aplicacions.
  - Així es busca que les aplicacions siguin segures i evitar que siguin observades ni per altres aplicacions ni pel SO.
  - Amb això es pretén estendre la protecció entre processos fins al punt que ni tan sols el superuser pugui controlar el que passa al sistema.
  - Tot això permetrà que el propietari d'un ordinador no pugui capturar vídeo, àudio o dades que estigui reproduint.

## Com funciona Palladium?

- TOR externs:
  - S'intenta crear un sistema que comprovi la seguretat del nostre SO de forma distribuïda.
  - Entitats externes al PC que autenticaran parts del SO per assegurar que no han estat modificades.
  - S'envien dades del SO al TOR extern i aquest ens torna una resposta sobre la seva integritat.
  - No es podrà saber quines dades del nostre SO demana el TOR.
  - Tot i així la seva finalitat no és tant la de donar més seguretat al sistema sinó la d'ajudar a millorar les aplicacions que usin DRM.



## Com funciona Palladium?

- DMR (Digital Rights Management):
  - És un sistema que proveeix als creadors de continguts (des de música i pel·lícules fins a documents de word) d'una sèrie d'eines per controlar els seus copyrights.
  - Limita l'accés als usuaris que han adquirit una llicència per reproduir aquest contingut.
  - Permet la distribució segura, la promoció i la venta de contingut digital a través d'internet.
  - Amb Palladium aquests sistemes es podrien reforçar. Al expedir llicències és podrà actuar com un TOR extern.

## Com funciona Palladium?

- Exemple de funcionament:
  - Un usuari vol reproduir una pel·lícula en un SO amb palladium
  - Envia de forma encriptada la clau pública que esta emmagatzemada en el seu TPM junt amb una sol·licitud de reproducció de la pel·lícula.
  - Un TOR rep aquesta petició i es guarda informació de la petició.
  - El TOR manegarà els drets d'autor corresponent.
  - Abans de reproduir la pel·lícula, el TA te dues opcions:
    - buscar la llicencia que el TOR ha guardat en la memòria del kernel del SO i comprovar si l'hi és permès de reproduir.
    - Enviar a un TOR extern la sol·licitud de reproducció i aquest li envia, després de comprovar la llicència, una clau per desencriptar el vídeo.



## Conclusions Palladium

- Palladium aporta certa seguretat a l'usuari, però amb greus contrapartides:
  - Poder identificar a cada usuari de forma unívoca pel creador del SO.
  - Possible pèrdua del control i la llibertat d'execució del PC per qualsevol tipus de contingut, principalment interessats en el DRM.
  - Tot i que millora la seguretat, no serà capaç d'evitar coses com els virus, un dels objectius que reclamen.

## Bibliografía

- FAQs:
  - http://www.trustedcomputing.org/docs/TPM_QA_071802.pdf
  - http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/NGSCB.asp
  - http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html
- Articles interessants:
  - http://wintermute.homelinux.org/miscelanea/Seguridad%20en%20TCPA.txt
  - http://www.research.ibm.com/gsal/tcpa/
  - http://www.cs.umd.edu/~waa/TCPA/TCPA-goodnbad.html



## Bibliografía

- Especificacions:
  - http://www.trustedcomputing.org/docs/TCPA_PCSpecificSpecification_v100.pdf
  - http://www.trustedcomputing.org/docs/main%20v1_1b.pdf
- Demos de DRM:
  - http://www.microsoft.com/windows/windowsmedia/drm/demos.aspx