HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC

An toàn hệ điều hành

Trusted Computing – Tính toán tin cậy

Giảng viên: TS. Phạm Hoàng Duy

Điện thoại/E-mail: phamhduy@gmail.com

Bộ môn: An toàn thông tin - Khoa CNTT1

Nội dung

- Khái niệm
- Hạ tầng tính toán tin cậy
- Các tác động

Khái niệm

- Máy tính ngày nay sử dụng kiến trúc mở cho phép người dùng toàn quyền lựa chọn phần mềm cũng như khả năng đọc, xóa hay sửa dữ liệu lưu trữ trên máy tính. Điều này dẫn đến
  - Không an toàn cho người dùng vì kiến trúc mở có nguy cơ bị lây nhiễm vi-rút, sâu hay vô tình cài đặt phần mềm xấu
  - Không an toàn cho mạng mà máy tính kết nối vào do máy tính này có thể chứa phần mềm xấu có thể đe dọa máy tính khác trong mạng
  - Không an toàn cho người sản xuất phần mềm và nội dung do kiến trúc mở cho phép các chương trình, file âm nhạc ... có thể bị sao chép không giới hạn và không bị giảm chất lượng

Khái niệm

- Khái niệm tính toán tin cậy đã được trình bày khá lâu trong lĩnh vực an toàn máy tính và có ảnh hưởng tới việc thiết kế các thế hệ máy tính phổ thông như PC, thiết bị di động
- Tính toán tin cậy đòi hỏi thiết kế lại kiến trúc hệ thống sao cho các thành phần riêng lẻ được định nghĩa một cách tường minh các đặc tính của mình
  - Điều này cho phép người thiết kế có thể xác định hành vi của hệ thống

Khái niệm

- Tính toán tin cậy mô tả các sửa đổi cần thiết về phần cứng và phần mềm để cung cấp nền tảng ổn định để hệ thống máy tính có thể hoạt động trên đó. Hệ thống này có đặc tính
  - Độ đảm bảo cao về trạng thái (cấu hình, tình trạng hoạt động của phần mềm ...) của hệ thống máy tính cục bộ. Do vậy có thể xác định khả năng chấp nhận các tác động không mong muốn
  - Mức độ đảm bảo cao tương đối về trạng thái của hệ thống ở xa. Thể hiện độ tin cậy của việc tương tác trong hệ thống phân tán.

Thách thức

- Các máy tính và phần mềm được cung cấp từ nhiều nhà sản xuất và phân phối khác nhau
  - Làm sao để xác định được máy tính nào là ổn định, phần mềm nào là an toàn?
- Hầu hết hệ điều hành được thiết kế dựa trên ý tưởng có 1 người quản trị hệ thống chuyên nghiệp
  - Người dùng cuối thường thiếu kỹ năng và hiểu biết
- Các vấn đề tương tự cũng gặp phải với các hệ thống mạng

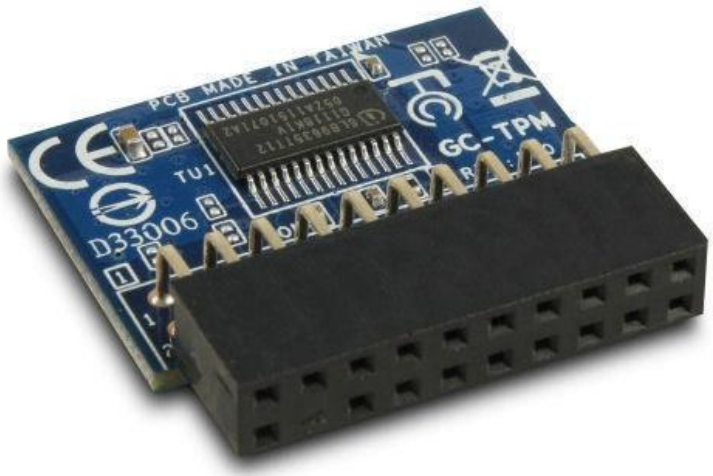
Cơ sở tính toán tin cậy

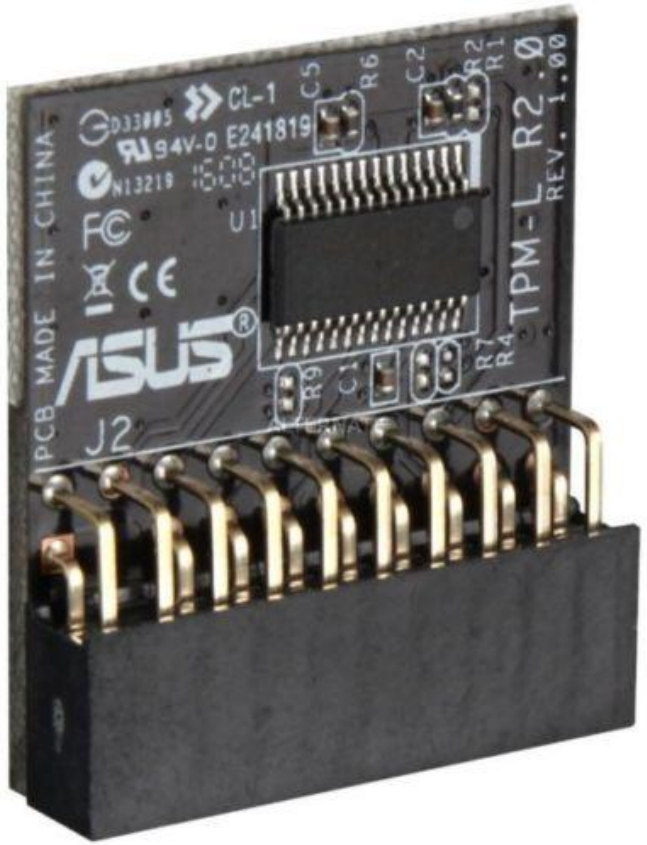
- Về cơ bản cần:
  - Các máy tính được định danh một cách chắc chắn. Sử dụng khóa công khai kèm với khóa bí mật "gắn chặt" liền với hạ tầng tính toán. Cần sử dụng cơ chế phần cứng và chống xâm nhập hay giả mạo.
  - Các máy tính xác định chắc chắn cấu hình và định danh chương trình. Sử dụng mã băm và cơ chế khác. Phần mềm, firmware, BIOS, trình nạp, nhân, chương trình tham gia vào quá trình hoạt động của máy tính cần được kiểm tra thích đáng để đảm bảo mức độ tin cậy và thực thi đúng đắn chính sách an ninh mong muốn.

Cơ sở tính toán tin cậy

- Mô-đun hạ tầng tin cậy (Trusted Platform Module) được định nghĩa là các chức năng phần mềm (lô-gíc) và nhúng vào trong kiến trúc của máy tính bằng cách sử dụng chíp riêng biệt
  - Các chức năng của TPM được xây dựng bằng phần mềm
  - Các chức năng an ninh cần được bảo vệ chặt chẽ được thực hiện thông qua thiết bị phần cứng

Cơ sở tính toán tin cậy





Cơ sở tính toán tin cậy

TPM Mô-đun hạ tầng tin cậy

- TPM đảm bảo các cơ sở tin cậy sau
  - Căn cứ tin cậy cho biện pháp bảo vệ (Root of trust for measurement-RTM
  - Cơ sở tin cậy cho lưu trữ (Root of trust for storage – RTS)
  - Cơ sở tin cậy cho việc báo cáo (Root of trust for reporting – RTR)

TPM Mô-đun hạ tầng tin cậy

- Cơ sở tin cậy biện pháp bảo vệ (RTM)
  - Triển khai một cách tin cậy các thuật toán băm chịu trách nhiệm cho các biện pháp bảo vệ đầu tiên với hạ tầng tính toán.
- Cơ sở lưu trữ tin cậy (RTS)
  - Triển khai tin cậy vị trí được bảo vệ cho việc lưu trữ một hay nhiều khóa bí mật và một khóa lưu trữ gốc (storage root key - SRK);
- Cơ sở tin cậy cho việc báo cáo (RTR)
  - Triển khai tin cậy vị trí được bảo vệ để lưu khóa bí mật đại diện cho định danh duy nhất của hạ tầng, còn gọi là khóa chứng thực (endorsement key - EK).

TPM Mô-đun hạ tầng tin cậy

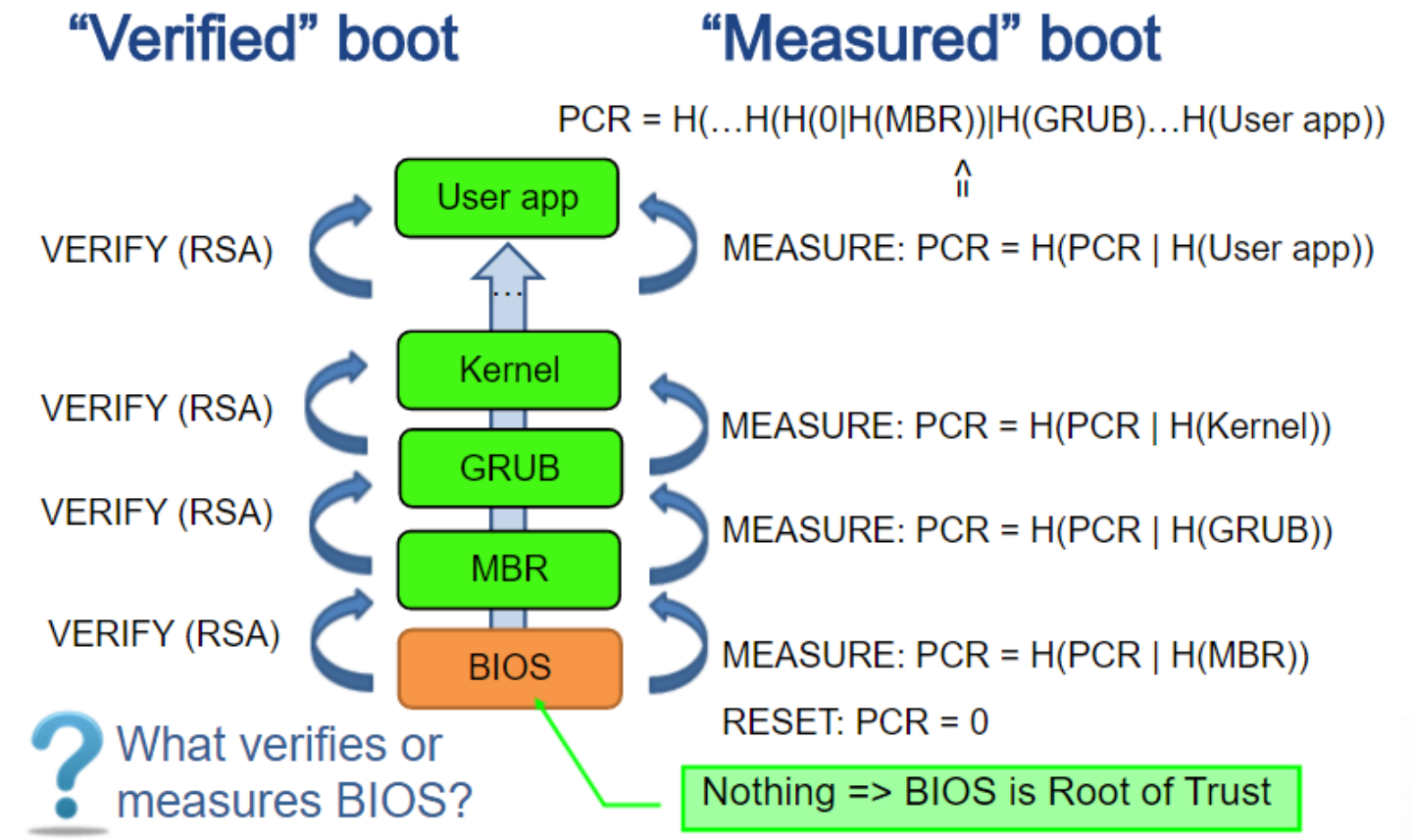
- Các khóa SRK và EK sử dụng cách mã hóa dị bộ (khóa công khai) TPM có nhiệm vụ bảo vệ khóa bí mật trong cặp khóa trên.
  - Phần khóa công khai EK được đăng ký với nơi chứng thực. Khóa EK tồn tại không đổi trong suốt thời gian hoạt động của hạ tầng tính toán
  - SRK được thiết lập khi triển khai cho người dùng và có thể được khởi tạo lại khi thay đổi người dùng.

Khởi động được bảo vệ

- RTM và RTR là các thành phần căn bản để tạo dựng được sự tin cậy thông qua quá trình khởi động được bảo vệ (measured boot) và xác lập khởi động được xác thực (authenticated boot)
- Quá trình khởi động như sau
  1. Khi bật máy, RTM lưu lại chỉ số định danh của hệ thống vào vị trí an toàn. Đây có thể chỉ là biện pháp bảo vệ mã của hạ tầng tính toán hay đơn giản chỉ là định danh
  2. Trước khi khởi tạo các phần tử tiếp theo trong chuỗi khởi động RTM tính toán mã băm của bộ phận đó và lưu lại vào nơi an toàn. Sau đó chuyển quyền điều khiển cho bộ phận đó.
  3. Lặp lại bước 2 cho từng liên kết trong chuỗi

Khởi động được bảo vệ

- Như vậy với bất kỳ chương trình nào và bất cứ khi nào đều có thể nhận được đảm bảo về tính toàn vẹn của bản thân chương trình đó và các chương trình khác tham gia vào hoạt động của nó.
- Do chuỗi chương trình tham gia vào quá trình khởi động rất lớn nên các nhà sản xuất TPM đưa ra giải pháp linh hoạt (dynamic root of trust)
  - Sử dụng đoạn mã cố định từ nguồn tin cậy được phép nạp và chạy chương trình được chọn như vậy làm giảm độ dài của chuỗi khởi động


"Verified" boot
"Measured" boot
PCR = H(…H(H(0|H(MBR))|H(GRUB)…H(User app))
User app
VERIFY (RSA)
MEASURE: PCR = H(PCR | H(User app))
Kernel
VERIFY (RSA)
MEASURE: PCR = H(PCR | H(Kernel))
GRUB
VERIFY (RSA)
MEASURE: PCR = H(PCR | H(GRUB))
MBR
VERIFY (RSA)
MEASURE: PCR = H(PCR | H(MBR))
BIOS
RESET: PCR = 0
What verifies or measures BIOS?
Nothing => BIOS is Root of Trust

TPM- Lưu trữ an toàn

- Lưu trữ an toàn trỏ đến các thanh ghi cấu hình của hạ tầng (Platform Configuration Registers-PCR) bên trong TPM
  - Các ô nhớ này được bảo vệ bằng cách có thể đọc nhưng không thể ghi tùy ý
  - Dữ liệu được ghi vào theo dạng tổ hợp với giá trị băm của dữ liệu hiện thời và giá trị trước đó
- TPM thực hiện việc đóng dấu dữ liệu sử dụng mã khóa công khai với dữ liệu trao đổi.
- TPM cung cấp bản sao có xác nhận trạng thái PCR đảm bảo độ đối tác có thể kiểm tra trạng thái của hạ tầng tính toán. Điều quan trọng là việc xác nhận diễn ra bên trong TPM.

Các tác động của TC

- Các tiếp cận của TC làm thay đổi mạnh mẽ thiết kế của hệ thống máy tính để bàn và ứng dụng phân tán. Điều mới với TC là việc đảm bảo chắc chắn phần mềm chạy cục bộ hay ở xa dựa trên cơ chế mã hóa sử dụng cách thức xác thực đảm bảo.
- TC ngăn chạn các vụ tấn công dựa trên phần mềm nhờ vào các thao tác thiết yều cần có sự chứng thực của phần cứng TPM.

Các tác động của TC

- TC chịu nhiều chỉ trích không chỉ từ cộng đồng mã nguồn mở
  - Tính riêng tư: Không bảo vệ định danh người dùng với một số giao dịch
  - Kiểm soát của bên bán hàng: Bên bán hàng có thể sử dụng TPM khiến cho việc lựa chọn và thay đổi sản phẩm khó khăn hơn với người dùng cuối
  - Chứng thực: Việc chứng thực sử dụng chữ ký khó khăn do số lượng phần mềm lớn vì vậy việc chứng thực cần thực hiện trên cơ sở hành vi của chương trình.
  - Không hỗ trợ mã khóa đối xứng
  - Thực thi luật pháp: việc mã khóa mạnh tác động cả hai bên người dùng hợp lệ và người bẻ khóa. TPM mô tả rõ ràng không có cửa hậu trong thiết bị hợp chuẩn.