

# Une panorama des architectures sécurisées et de confiance

Guillaume DUC   Ronan KERYELL

Orange Labs (Caen)

Institut TÉLÉCOM, TÉLÉCOM Bretagne, HPCAS (Plouzané)

HPC Project (Meudon)

Computer & Electronics Security Applications Rendez-vous  
C&ESAR — 03/12/2008



# Plan

## Informatique de confiance

Introduction

Trusted Computing Group

Intel Trusted Execution Technology

## Informatique sécurisée

Introduction

Approche co-processeurs

Approche chiffrement de bus

## Relations informatiques de confiance / sécurisée



# Sécurité informatique

- ▶ Virus
- ▶ Spam
- ▶ Vol / corruption de données
- ▶ Protection vie privée
- ▶ Déni de service
- ▶ Vol d'identité
- ▶ Respect de la propriété intellectuelle
- ▶ ...

# Problèmes

- ▶ **Nombreux angles d'attaque**
  - ▶ Matériels (attaque physique contre le CPU, les bus, la mémoire, les supports de stockage, les équipements réseau...)
  - ▶ Protocoles (SMTP...)
  - ▶ Systèmes d'exploitation (failles...)
  - ▶ Applications (erreurs de programmation, rétro-ingénierie...)

# Problèmes

- ▶ Nombreux travaux au niveau logiciel
  - ▶ Algorithmes (chiffrement, intégrité, authentification...)
  - ▶ Protocoles (SSL/TLS, IPsec...)
  - ▶ Systèmes d'exploitation sécurisés
  - ▶ Logiciels de sécurité (antivirus, pare-feu, DRM...)
- ▶ Mais quelle sécurité pour le support d'exécution ?

# Informatique de confiance / sécurisée

- ▶ Deux approches émergent pour résoudre certains problèmes
  - ▶ Informatique de confiance : principalement dans le monde industriel
  - ▶ Informatique sécurisée : principalement dans le monde académique et militaire



# Plan

## Informatique de confiance

Introduction

Trusted Computing Group

Intel Trusted Execution Technology

## Informatique sécurisée

Introduction

Approche co-processeurs

Approche chiffrement de bus

## Relations informatiques de confiance / sécurisée



# Motivations

- ▶ S'assurer qu'un système informatique va se comporter de façon bien définie
- ▶ Résistance à des attaques logiques et quelques attaques physiques (vol notamment)

# Exemples d'utilisation

- ▶ Services distants (e-commerce, e-banking, jeux en ligne, accès VPN...) : vérifier que la plate-forme cliente est digne de confiance (ex. présence des derniers correctifs pour le système d'exploitation, version originale d'un logiciel...)
- ▶ Utilisateur local : protéger ses données (clés de chiffrement, mots de passe...) contre le vol (physique ou logique)

# Trusted Computing Group

- ▶ Groupement d'entreprises
- ▶ Produit des spécifications de composants nécessaires à l'informatique de confiance
- ▶ Groupes de travail dans tous les domaines de l'informatique : PC client, serveur, stockage, réseau, mobile, virtualisation...



# Fonctions de base

- ▶ Fonctions de base pour assurer la confiance (racines de confiance)
  - ▶ Prise de mesures des différents éléments susceptibles d'avoir un impact sur la sécurité de la plate-forme
  - ▶ Stockage sécurisé de ces mesures (et d'autres données)
  - ▶ Attestation à distance de la valeur et de la véracité de ces mesures

# Cas du PC

- ▶ Puce TPM (Trusted Platform Module) normalement soudée sur la carte mère
  - ▶ Mesures incrémentales des éléments intervenant lors du démarrage de l'ordinateur (BIOS, boot loader, noyau de l'OS) et stockage dans des registres du TPM (PCR)
  - ▶ Rapport de ces mesures (signature numérique faite par le TPM) à une entité distante
  - ▶ Stockage sécurisé (par exemple lié à l'état de la plate-forme)
  - ▶ Prise en compte des aspects liés à la vie privée de l'utilisateur (AIK, privacy CA, DAA)

# Autres groupes : exemples

- ▶ Mobile
  - ▶ Spécifications de la version mobile du TPM : le MTM (plusieurs *propriétaires* : fabricant, opérateur, utilisateur)
  - ▶ Secure boot (pour garantir notamment la partie radio)
- ▶ Trusted Network Connect
  - ▶ Spécifications pour permettre/interdire l'accès à un réseau en fonction de la confiance dans la plate-forme cliente

# Critiques

- ▶ Image sulfureuse associée à l'ancien couple TCPA/Palladium et aux DRM
- ▶ Fournisseurs de services pourront décider quels programmes l'utilisateur doit exécuter pour y accéder (comment ces listes seront établies ? ; TPM désactivable mais plus accès au service ?)
- ▶ Compatibilité avec certains modes de distribution des logiciels libres (valeurs de référence / recompilation à partir des sources)
- ▶ Entrave à l'interopérabilité (stockage scellé : document ne pouvant être lu que par un logiciel donné)

# Objectifs

- ▶ Exécution protégée
- ▶ Stockage scellé
- ▶ E/S protégées
- ▶ Affichage protégé
- ▶ Attestation
- ▶ Lancement protégé

# Aspects matériels

- ▶ Utilisation d'un TPM pour les fonctions d'attestation, mesure et stockage sécurisé
- ▶ Chipset : amélioration la protection de la mémoire contre des accès illicites (notamment via DMA)
- ▶ Processeur : mécanisme de partitionnement
- ▶ Périphériques : intégration d'un système de chiffrement

# Plan

## Informatique de confiance

Introduction

Trusted Computing Group

Intel Trusted Execution Technology

## Informatique sécurisée

Introduction

Approche co-processeurs

Approche chiffrement de bus

## Relations informatiques de confiance / sécurisée



# Motivations

- ▶ Confiance dans logiciel (erreurs de programmation, OS trop gros...)
- ▶ Attaques matérielles contre le support d'exécution
  - ▶ Lecture ou modification de la mémoire
  - ▶ Espionnage des bus du processeur (données et adresses)
  - ▶ Attaques directes contre le processeur
    - ▶ Injection de fautes
    - ▶ Mesures de consommation et analyses statistiques
- ▶ Nécessitent des moyens importants mais pas irréalistes (ex. cassage de la X-BOX)
- ▶ **Relativement peu de supports sécurisés d'exécution...**

# Modèle de sécurité

- ▶ Propriétés garanties
  - ▶ *Confidentialité* : un attaquant doit pouvoir obtenir le moins d'information possible sur le code ou les données d'un processus
  - ▶ *Intégrité* : le bon fonctionnement d'un processus ne doit pas pouvoir être altéré par une attaque
- ▶ Attaquant
  - ▶ Contrôle total sur l'extérieur du processeur (bus, mémoire, système d'exploitation, applications...)
  - ▶ Processeur considéré comme inviolable (attaque physique directe, canaux auxiliaires...)
  - ▶ Déni de service exclu
- ▶ Problème : Garder des performances raisonnables



# Application : grilles de calcul, cloud computing

- ▶ Regrouper la puissance de calcul de nombreux ordinateurs pour accélérer certains calculs volumineux
- ▶ Informatique et stockage totalement délocalisés (dans des lieux où il fait frais et avec de l'électricité renouvelable...)
- ▶ Problèmes
  - ▶ Nœuds répartis non administrés physiquement par l'utilisateur
  - ▶ Sécurité (matérielle et logicielle) des nœuds non garantie
- ▶ Le propriétaire d'un des nœuds peut
  - ▶ Perturber l'application  $\rightsquigarrow$  génération de résultats erronés (« médicament non trouvé »...)
  - ▶ Espionner l'application  $\rightsquigarrow$  vol de données, résultats ou algorithmes secrets

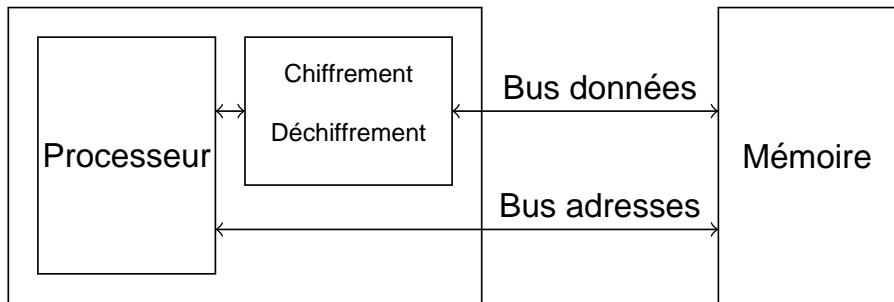


# Coprocesseurs

- ▶ Première solution : environnement d'exécution blindé (processeur, mémoire, bus, etc.) pour les processus sécurisés
  - ▶ Cartes à puce
  - ▶ IBM 4758/4764 (processeur, RAM, mémoire flash)
- ▶ Problèmes
  - ▶ Performances (cartes à puce)
  - ▶ Peu évolutif

# Architectures sécurisées

- ▶ Deuxième solution : exécution de programmes chiffrés
- ▶ Architectures sécurisées avec chiffrement du bus



# Historique

- ▶ Confidentialité
  - ▶ BEST, 1979
  - ▶ DALLAS DS500x, 1995 (commercialisé, cassé par KUHN en 1998)
  - ▶ KUHN (*TrustNo 1*), 1997 : chiffrement asymétrique et support système d'exploitation
  - ▶ GILMONT, LEGAT et QUISQUATER, 1998 : chiffrement hybride
- ▶ Confidentialité et Intégrité
  - ▶ LIE, THEKKATH, MITCHELL, LINCOLN (XOM), 2000
  - ▶ KERYELL (CRYPTOPAGE), 2000
  - ▶ SUH, CLARKE, GASSEND, DIJK et DEVADAS (*Aegis*), 2003 : protection contre les attaques par rejeu
  - ▶ KERYELL, LAURADOUX (CRYPTOPAGE 2), 2003

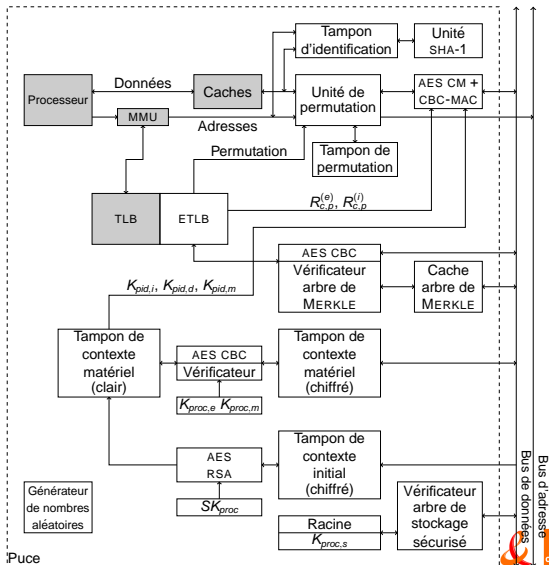


# Exemple : CRYPTOPAGE

- ▶ Garantit confidentialité et intégrité pour les processus sécurisés
- ▶ Mécanisme efficace de chiffrement (mode compteur) et d'intégrité (mélange de MAC et d'arbres de hachage) mémoire
- ▶ Mécanisme de limitation des fuites d'information sur le bus d'adresse (basé sur l'infrastructure HIDE)
- ▶ Prise en charge efficace d'un système d'exploitation non sécurisé (chargement d'un programme, changements de contexte, signaux logiciels, processus légers, etc.)
- ▶ Mécanisme de signature de résultat
- ▶ Mécanisme de stockage sécurisé
- ▶ Mécanisme d'identification de programme



# Exemple : CRYPTOPAGE



# CRYPTOPAGE— Simulations

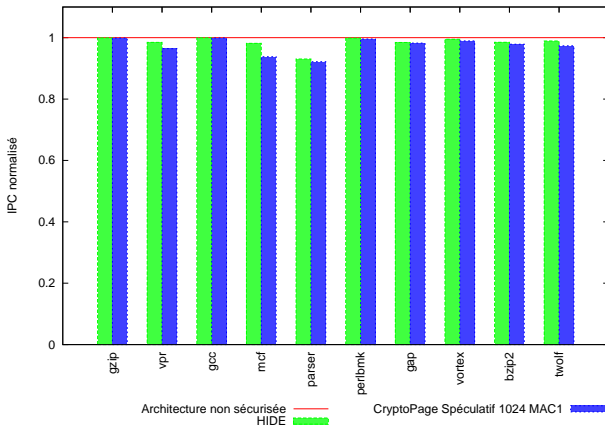
## ▶ Quantitatives

- ▶ Simulateur de micro-architecture SIMPLESCALAR
- ▶  $\rightsquigarrow$  Obtention d'estimations des performances de CRYPTOPAGE

## ▶ Qualitatives

- ▶ Simulateur de PC BOCHS
- ▶ Noyau LINUX adapté
- ▶ Chaîne de compilation adaptée
- ▶  $\rightsquigarrow$  Vérification du bon fonctionnement des mécanismes de CRYPTOPAGE

# CRYPTOPAGE— Performances



- ▶ Performances : pénalité de 3 à 8 % en moyenne par rapport à une architecture classique non sécurisée



# Plan

## Informatique de confiance

Introduction

Trusted Computing Group

Intel Trusted Execution Technology

## Informatique sécurisée

Introduction

Approche co-processeurs

Approche chiffrement de bus

## Relations informatiques de confiance / sécurisée



# Informatique de confiance / sécurisée

- ▶ Informatique de confiance (TCG, Intel TXT) ne remplissent pas les objectifs des architectures sécurisées
- ▶ Certaines attaques physiques non traitées
- ▶ Mémoire non chiffrée  $\rightsquigarrow$  espionnage du bus possible (propriété de confidentialité)
- ▶ Propriété d'intégrité également attaquable via la mémoire ou les bus (malgré mécanisme de vérification régulière)

# Informatique de confiance / sécurisée

- ▶ Architectures sécurisées récentes peuvent répondre aux objectifs de l'informatique de confiance
- ▶ Mécanisme d'attestation pour prouver qu'un résultat a été produit par un processus sécurisé (XOM, AEGIS, CRYPTOPAGE)
- ▶ Mesure de l'état de la plate-forme non nécessaire (l'exécution d'un programme sécurisé n'est possible que sur un processeur sécurisé)
- ▶ Stockage sécurisé prévu par certaines architectures (CRYPTOPAGE)

# Conclusion

- ▶ Sujet d'actualité
- ▶ Nombreuses applications pouvant bénéficier de niveaux de sécurité et de confiance plus élevés (↪ DRM libres... 😊)
- ▶ Architectures de confiance déjà disponibles contrairement aux architectures sécurisées
- ▶ Loi de Moore actuellement : pas d'augmentation de vitesse mais toujours augmentation du nombre de transistors ↪ augmentation du nombre de cœurs et/ou... intégration de la sécurité directement dans le processeur
- ▶ Reste encore beaucoup de travail pour industrialiser processeurs du monde de la recherche

# Problèmes

- ▶ Comme toute technologie, garder une éthique sur les usages...
  - ▶ Acceptabilité de ces technologies ?
  - ▶ Perturbation de l'écosystème informatique ?
  - ▶ Retrait du contrôle des mains de l'utilisateur des applications s'exécutant sur son propre ordinateur ?

# Une panorama des architectures sécurisées et de confiance

Guillaume DUC   Ronan KERYELL

Orange Labs (Caen)

Institut TÉLÉCOM, TÉLÉCOM Bretagne, HPCAS (Plouzané)

HPC Project (Meudon)

Computer & Electronics Security Applications Rendez-vous  
C&ESAR — 03/12/2008

