Du matériel aux applications, introduction à la sécurité informatique

Etienne Helluy-Lafont

February 20, 2018

Université Lille 1

Présentation

- DUT Informatique à l'IUT A:
- Master TIIR: Infrastructure et réseau
- Thèse en cours sur la détection dans l'internet des objets
- Membre de l'association SecurInLille

Plan

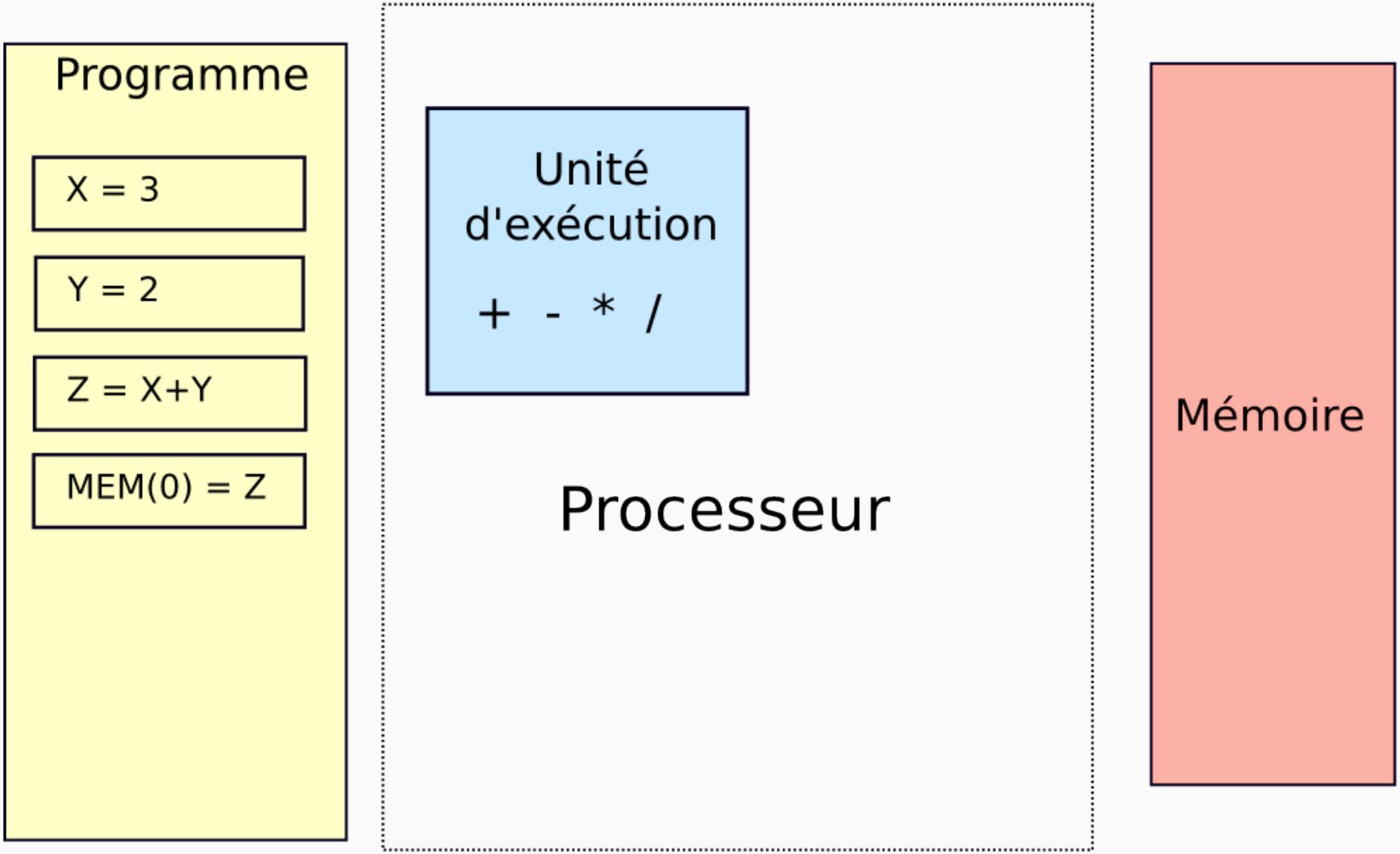
- Spectre & Meltdown
- Vulnérabilités
- Modèle de sécurité
- Contremesures

Spectre & Meltdown

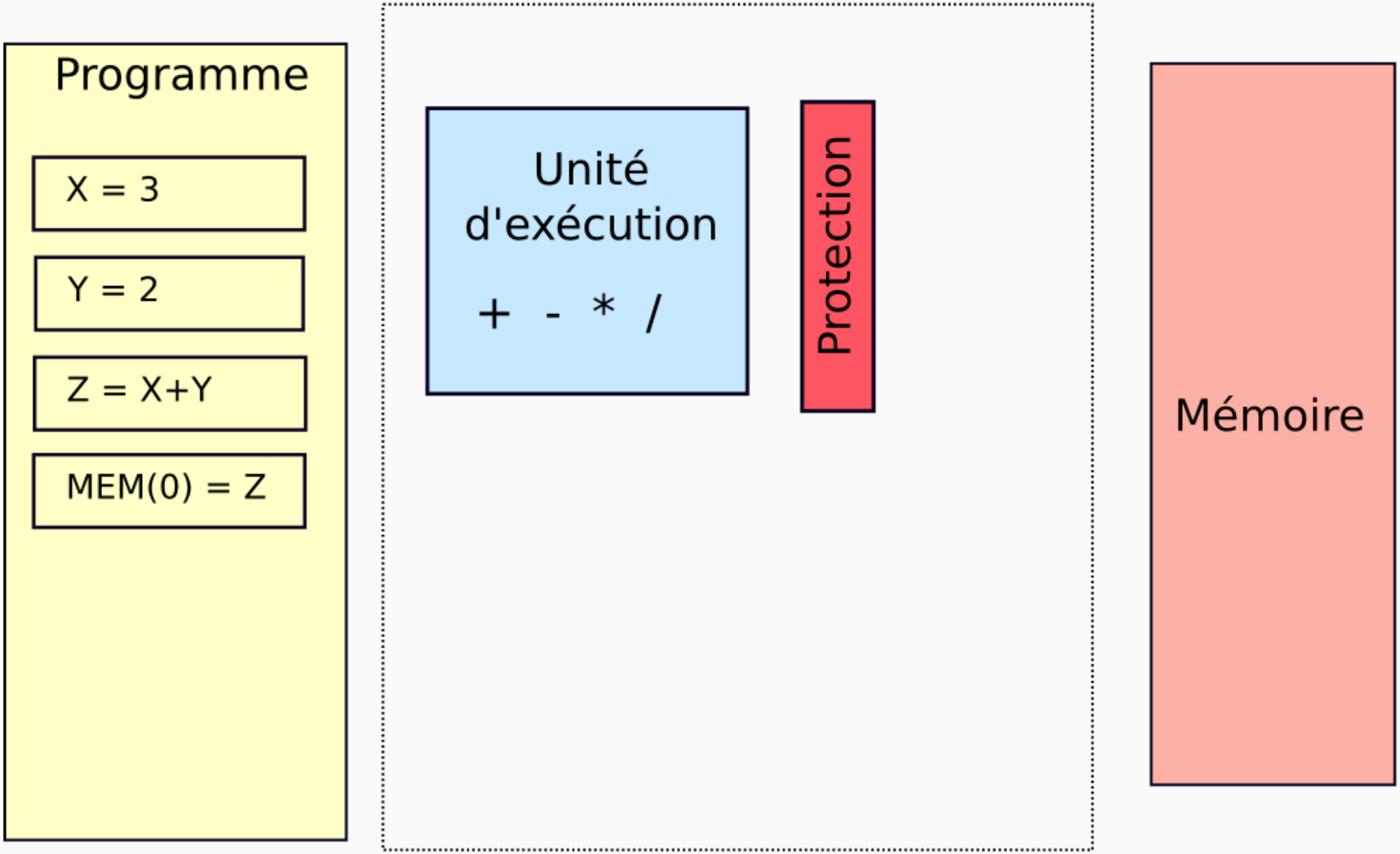
Spectre & Meltdown

- Meltdown et Spectre: Une faille dans les processeurs
- Deux noms différents pour un seul problème
- Faille au niveau *micro-architectural*: Fonctionnement interne du processeur

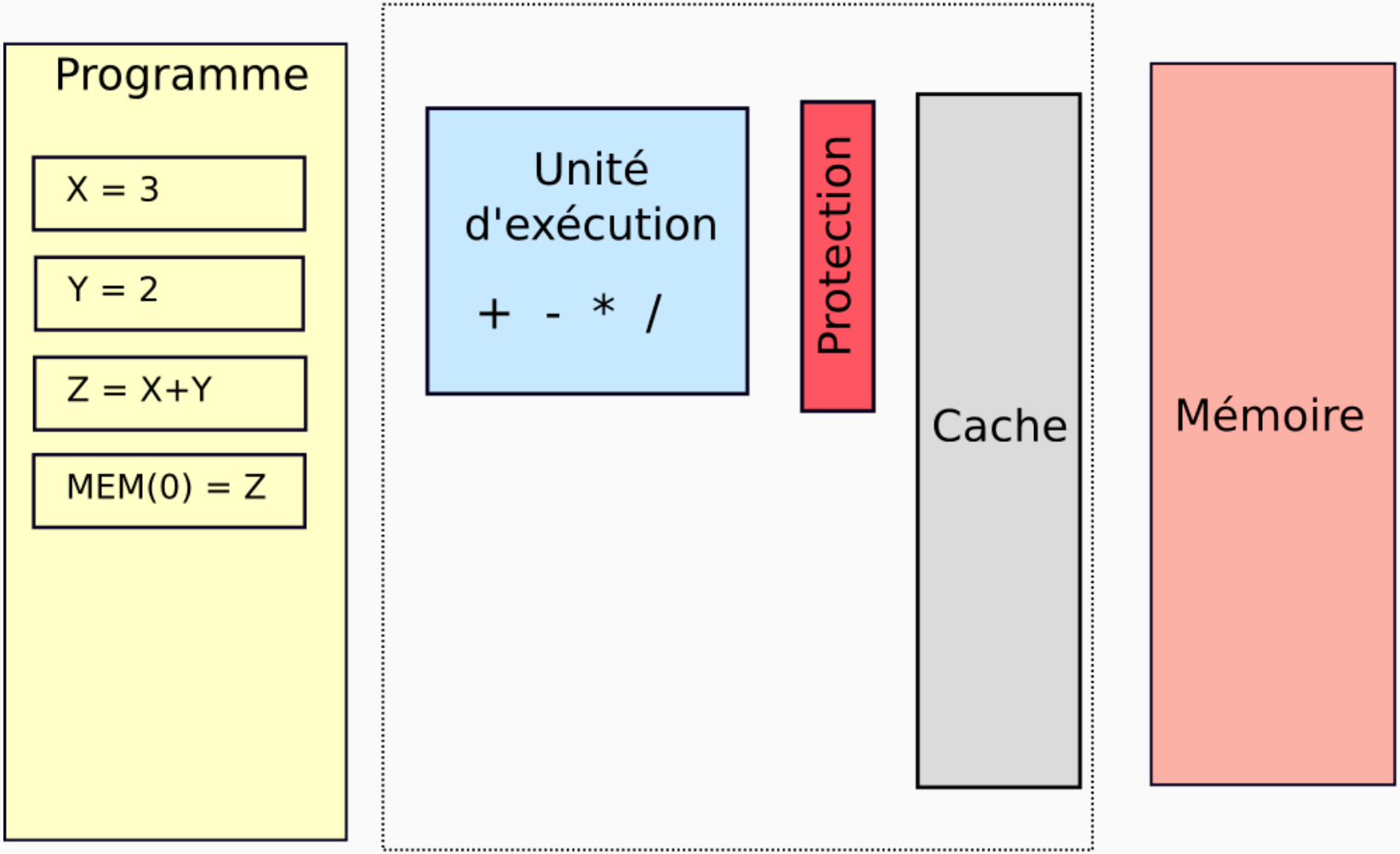
Meltdown


Programme
X = 3
Y = 2
Z = X+Y
MEM(0) = Z
Unité d'exécution
+ - * /
Processeur
Mémoire

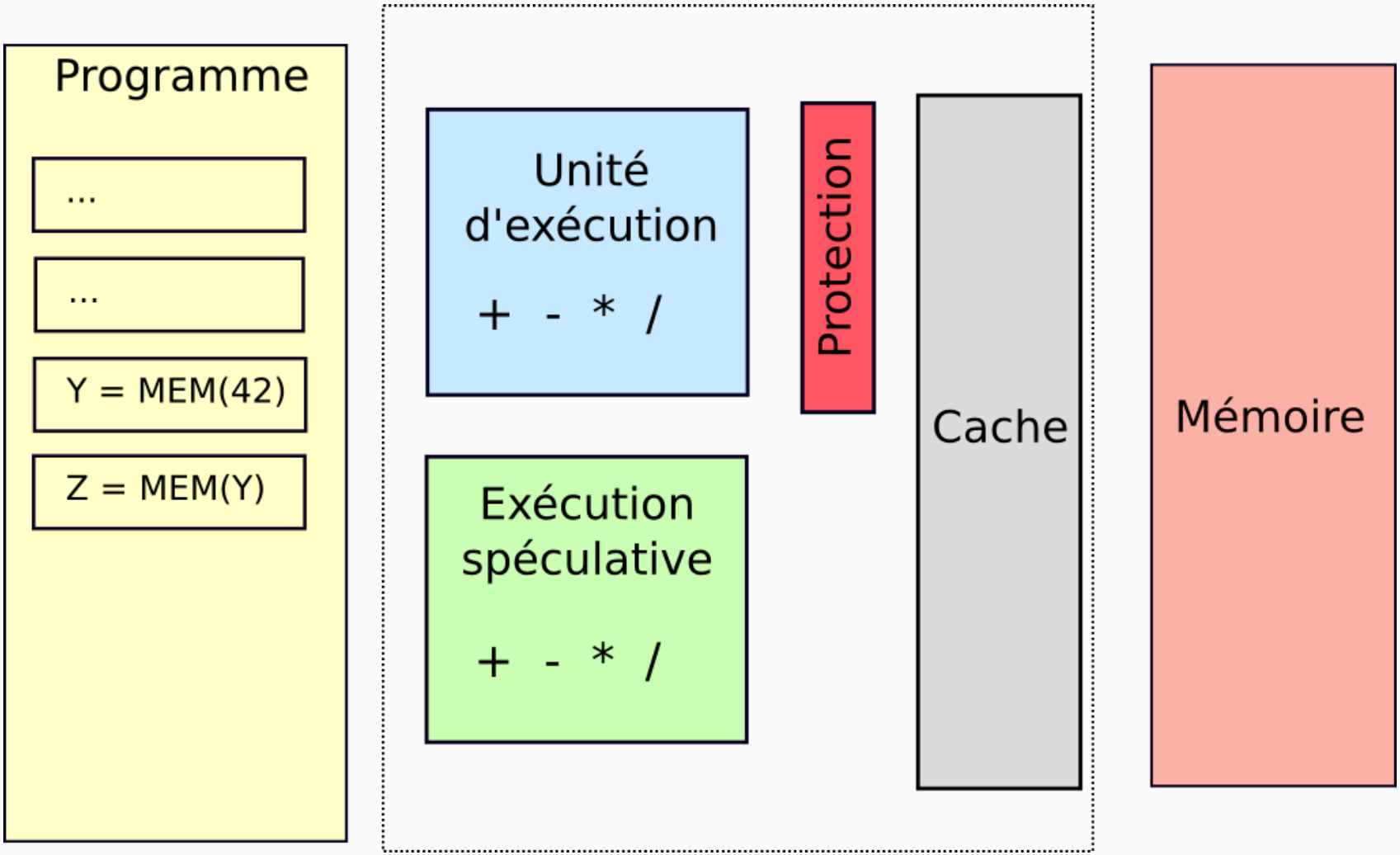
Meltdown


Programme
X = 3
Y = 2
Z = X+Y
MEM(0) = Z
Unité d'exécution
+ - * /
Protection
Mémoire

Meltdown


Programme
X = 3
Y = 2
Z = X+Y
MEM(0) = Z
Unité d'exécution
+ - * /
Protection
Cache
Mémoire

Meltdown


Programme
...
...
Y = MEM(42)
Z = MEM(Y)
Unité d'exécution
+ - * /
Exécution spéculative
+ - * /
Protection
Cache
Mémoire

Anneaux de protection dans un processeur Intel

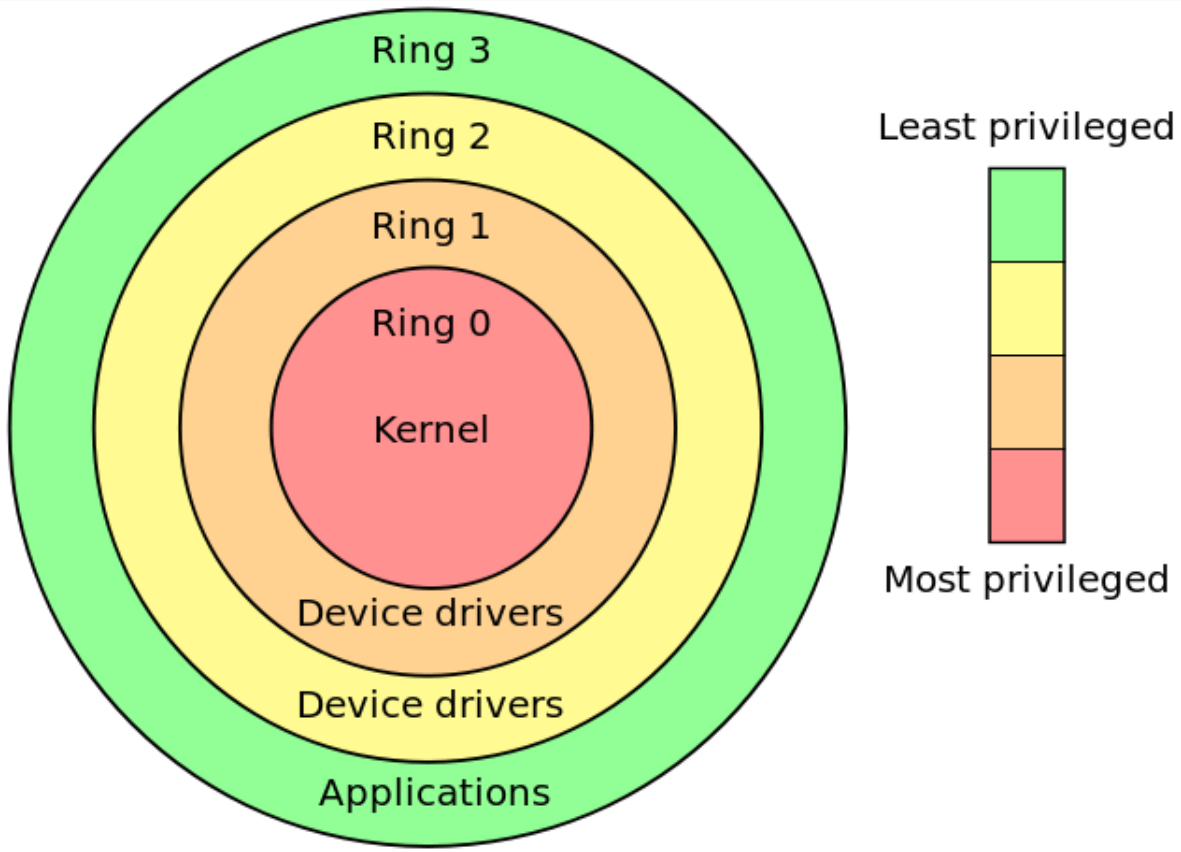


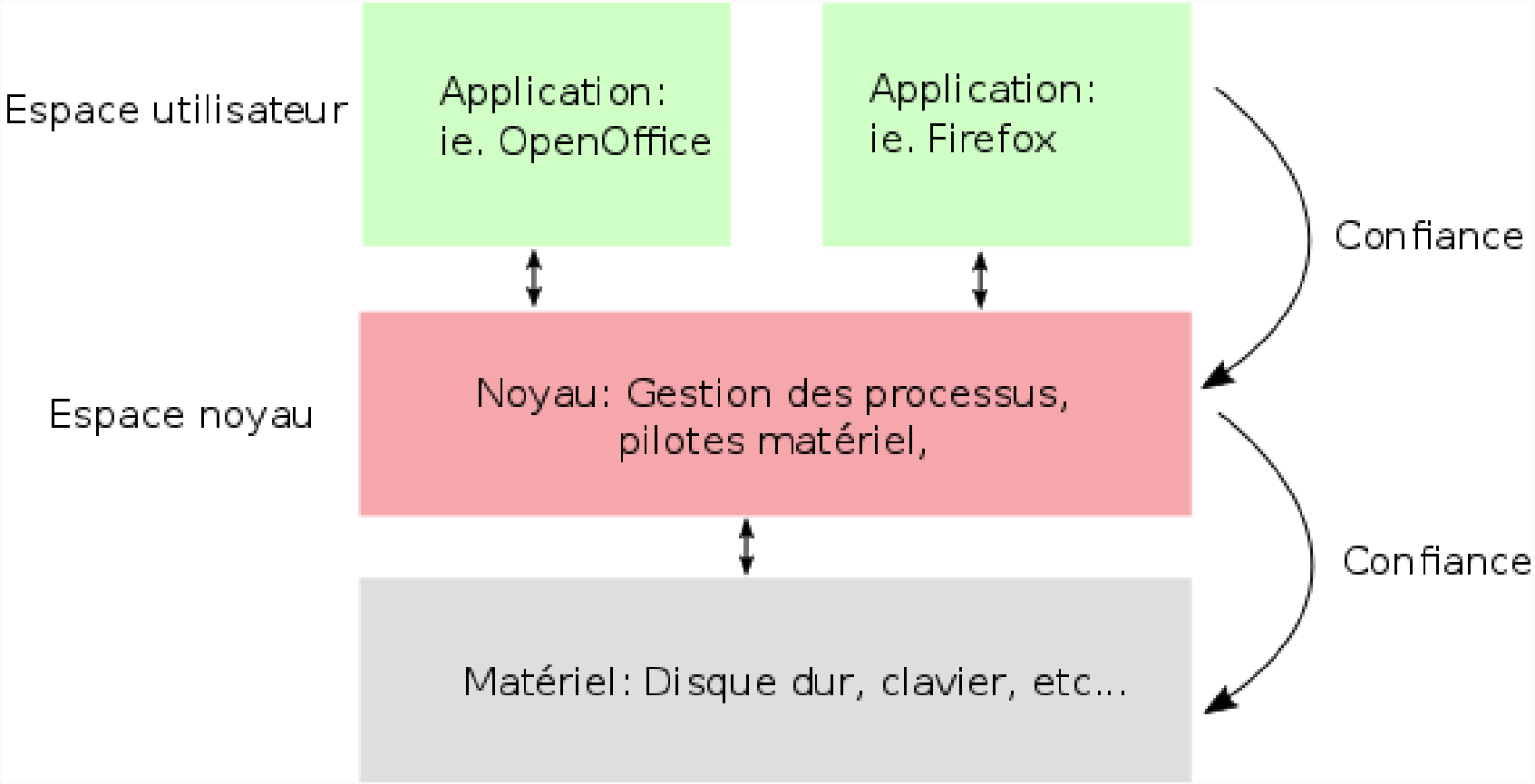
Figure 1: Annaux de protection dans un processeur Intel. (Hertzsprung, Wikipedia anglais, CC BY-SA 3.0)

Anneaux de protection dans un processeur Intel

- Plusieurs *modes d'exécution*
- Linux / Windows: Deux modes, *Superviseur* et *Utilisateur*
- Utilisateur: Applications
  - Accès restreint à la mémoire, aux fichiers, etc.
- Superviseur: Noyau, pilotes matériels
  - Accès total

Base de confiance

Une chaine qui repose sur le matériel



Vulnérabilités

- Humaines: Manipulation des opérateurs
- Dans la conception: Failles "logiques", effets imprévus d'une fonctionnalité, d'un protocole.
- Dans l'implémentation: Erreurs de programmation
- Dans le déploiement: Liée à l'environnement, à la configuration, au matériel

Vulnérabilités: Conception

- Cas de Meltdown & Spectre:
  - Séparation des privilèges entre les modes d'exécution
  - Structures matérielles partagées entre les modes d'exécution
  - Resultat: Effets *micro-architecturaux* observables par tous
- Plus difficiles à détecter et à corriger
- Peuvent exister dans plusieurs produits différents
- Peut exister dans des spécifications

Vulnérabilités: Implémentation

Exemple répandu: Injection

- Mauvais traitement d'entrée utilisateur
- Exemple: Injection SQL dans un formulaire web
  - "SELECT id WHERE name='$login' and pass='$password' "
  - L'utilisateur entre: login="toto", password="' or '1'='1"
  - "SELECT id WHERE name='toto' and pass='' or '1'='1' "
- *"Never trust user input"*

Vulnérabilités: Implémentation

Exemple répandu: Dépassement de tampon

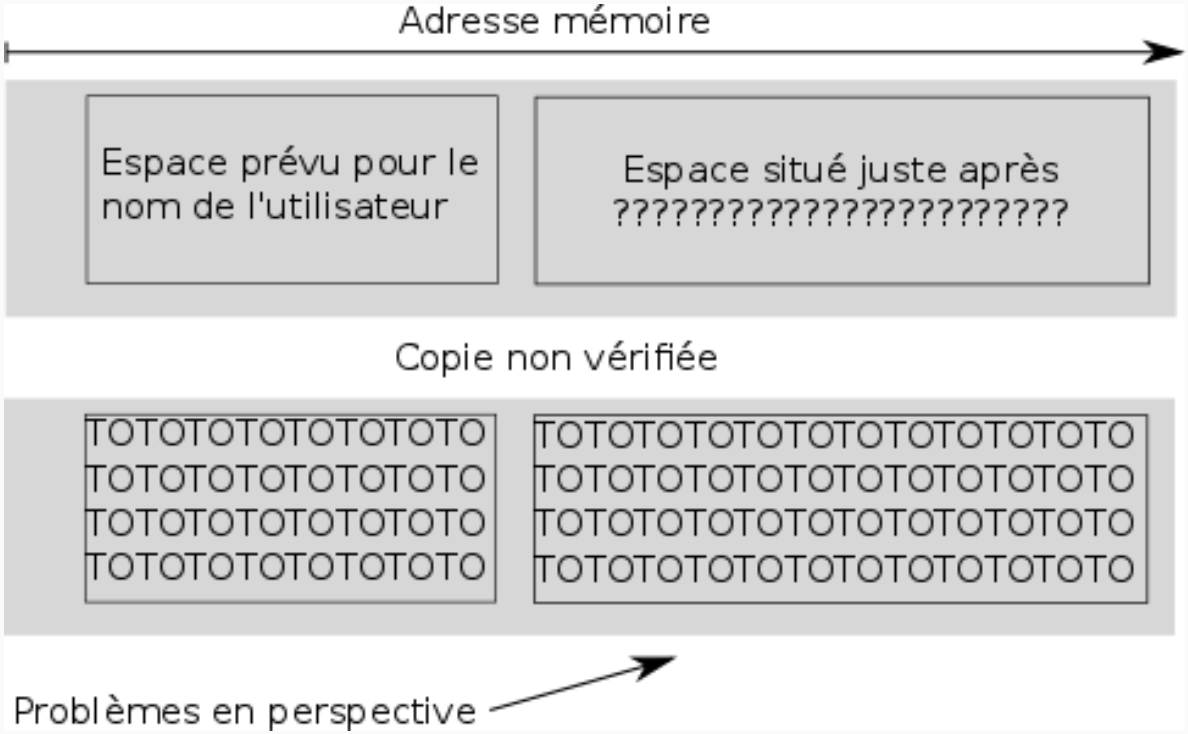


Figure 2: Corruption mémoire

- *"Never trust user input"*

Modèle de sécurité: Propriétés

- Confidentialité
- Disponibilité
- Intégrité

Modèle de sécurité: Identification et analyse des risques

- Identifier les actifs: Que doit-on protéger ?
- Identifier les menaces: Quels risques ? Quels adversaires ?
- Identifier les rôles: Qui a accès à quoi?
- Analyser les risques: Hiérarchiser les menaces par impact/vraisemblance

Contremesures: Développement

- Respect de bonnes pratiques de développement, de normes de sécurité
  - ANSSI: Agence Nationale pour la Sécurité des systèmes d'Information
  - NIST: National Institute of Standards and Technology
- Utiliser des composants éprouvés: Ne pas réinventer la roue
- Audits, vérification de code
- Service après vente: Veille, distribution de mises à jour

Contremesures: Déploiement

- Détection/Prévention d'intrusion
  - Sur le réseau: Interconnections, accès sans-fil, etc.
  - Sur les hôtes: Antivirus, etc.
- Isolation
  - Segmentation du réseau
  - Sur une même machine: Hyperviseurs, sandbox
  - Défense en profondeur: Multiples lignes de défenses autonomes
- Formation des utilisateurs

Contremesures: Organisation

- Normes: Par exemple ISO/CEI 27001.
  - Plan/Do/Check/Act: Processus d'amélioration continue
- Parfois obligatoires: Données de santé, bancaires, etc.
- Règlement Général sur la Protection des Données
  - Protection de la vie privée dès la conception et par défaut
  - Démontré au moyen de certifications

Merci

Questions?

Lectures

https://www.ssi.gouv.fr/administration/bonnes-pratiques/