Olivier Savry
Thomas Hiscock
Mustapha El Majihi

SÉCURITÉ MATÉRIELLE DES SYSTÈMES

Vulnérabilités des processeurs et techniques d'exploitation

DUNOD

Illustration de couverture : matejmo/istockphoto.com

Cet ouvrage a été réalisé avec le soutien d'Investir l'avenir et de Nanoelec

© Dunod, 2019
11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-079529-1

Table des matières

Introduction

Les cyber-attaques en tout genre ont envahi les actualités quotidiennes. La dépendance accrue de nos sociétés aux solutions automatisées, aux algorithmes et au numérique en général ouvre la voie à des menaces de plus en plus prégnantes. Des données récentes laissent à penser que la croissance des cyber-attaques n'est plus linéaire, mais qu'elle a pris une trajectoire exponentielle. Un phénomène poussé par l'ingéniosité toujours renouvellée des attaquants. Ces derniers évoluent dans un monde de plus en plus complexe, et donc de plus en plus vulnérable où l'accès à l'information et à la connaissance est facilité par nos modes de communications ultra-rapides.

L'intrication et l'interopérabilité de tous les systèmes qui nous entourent – transports (trains, avions, voitures…), énergie, gestion des ressources, habitat (domotique), gestion de la ville (*smart cities*), outils de production (usines) – où le maillon le plus faible est susceptible de présenter des failles, ouvrant la porte à des risques toujours plus probables de black-out total. Si on remonte l'arbre de causes de ces attaques, le cœur du problème se révèle : les processeurs. Ils sont la partie active de ces CPS (*cyber physical systems*) et de l'IoT (*internet of things*) relié par l'Internet. Nous nous appuyons tous les jours sur ces solutions pour nous simplifier la vie, au prix d'un risque d'aliénation que l'on ne mesure pas toujours quand leur sécurité n'est pas assurée.

Une étude du cycle de développement de ces systèmes à base de processeurs montre que les failles ont trois raisons essentielles :

1. La sécurité des processeurs et des logiciels embarqués n'est pas pensée en amont du développement du système. Bien souvent, on réalise après coup (souvent à la suite d'une attaque) que des vulnérabilités structurelles sont présentes. La réaction est alors de « patcher », avec le risque de déplacer le problème et de dégrader les performances.
2. L'implémentation de fonctions de sécurité est un travail difficile nécessitant l'avis d'experts. Malheureusement, il y aura toujours plus de développeurs et de concepteurs que de spécialistes de la sécurité (qui sont rares et coûteux).
3. Les ingénieurs, les développeurs et même les experts n'ont pas toujours les outils pour répondre au défi de la sécurité de systèmes toujours plus complexes.

> Outre le fait que, souvent, on ne peut adapter l'implémentation de la sécurité qu'à un certain niveau défini de risques, il est à regretter qu'on n'ait pas sur le marché de solutions accessibles à tous pour développer des produits sûrs.

C'est dans ce contexte que cet ouvrage prend tout son sens. Nous espérons qu'il apportera aux développeurs, aux étudiants en informatique et aux électroniciens numériques des moyens d'appréhender les vulnérabilités des processeurs, de prendre conscience des nombreuses attaques qu'elles rendent possibles et de leur exploitation. Nous avons voulu concevoir un ouvrage d'accès facile et qui se suffit à lui-même, tout en permettant au lecteur d'approfondir les sujets abordés avec de nombreuses références vers des articles scientifiques plus pointus, rédigés par des experts du domaine. Toute cette bibliographie est aisément accessible en ligne. Ainsi, ce livre pourra servir avantageusement de guide à des concepteurs de processeurs voire de systèmes complexes qui se soucient un tant soit peu de leur sécurité.

Lors de la rédaction, il n'a pas été simple de définir un cadre de travail sans laisser échapper de vulnérabilité capitale. Nous avons pris le parti de regarder le synoptique d'une architecture moderne de processeur avec tous ses composants et de déterminer les menaces qui pesaient sur chacun d'eux. La Figure I.1 est une architecture générique fusionnant des concepts venant à la fois d'Intel, d'AMD et d'ARM qui a constitué le plan de ce document.

Une grande partie du schéma est couverte par les différents éléments de la hiérarchie mémoire : registres, caches, DRAM, flash ou disque dur, qui sont les principales portes d'entrée des attaques. Le premier chapitre est entièrement dédié à l'étude de ces menaces. Nous plongerons ensuite au plus profond de l'architecture. Nous voyons sur la figure les multiples cœurs incontournables des puces actuelles, avec de l'exécution parallèle et désordonnée d'instructions et de la prédiction de branchements. Ces éléments nécessaires à l'augmentation des performances sont, depuis les attaques récentes et très médiatisées Spectre et Meltdown, des accès aisés pour les hackers. Le seond chapitre dressera un état des lieux des vulnérabilités qui apparaissent à ce niveau de conception (la microarchitecture) et abordera en détails les attaques *Spectre* et *Meltdown*. Nous ferons ensuite une incursion vers les vulnérabilités des programmes comme le fameux *buffer overflow* qui exploite les structures des processus en mémoire. Nous y verrons également d'autres possibilités pour détourner le flot de contrôle des programmes. Toutefois, on se limitera à l'étude des failles qui sont la conséquence de vulnérabilités du matériel. Ainsi, une injection SQL ou une attaque XSS ne seront pas abordées car ce sont des attaques purement software qui laisse l'attaquant confiné aux logiciels attaqués comme la base de données ou le serveur

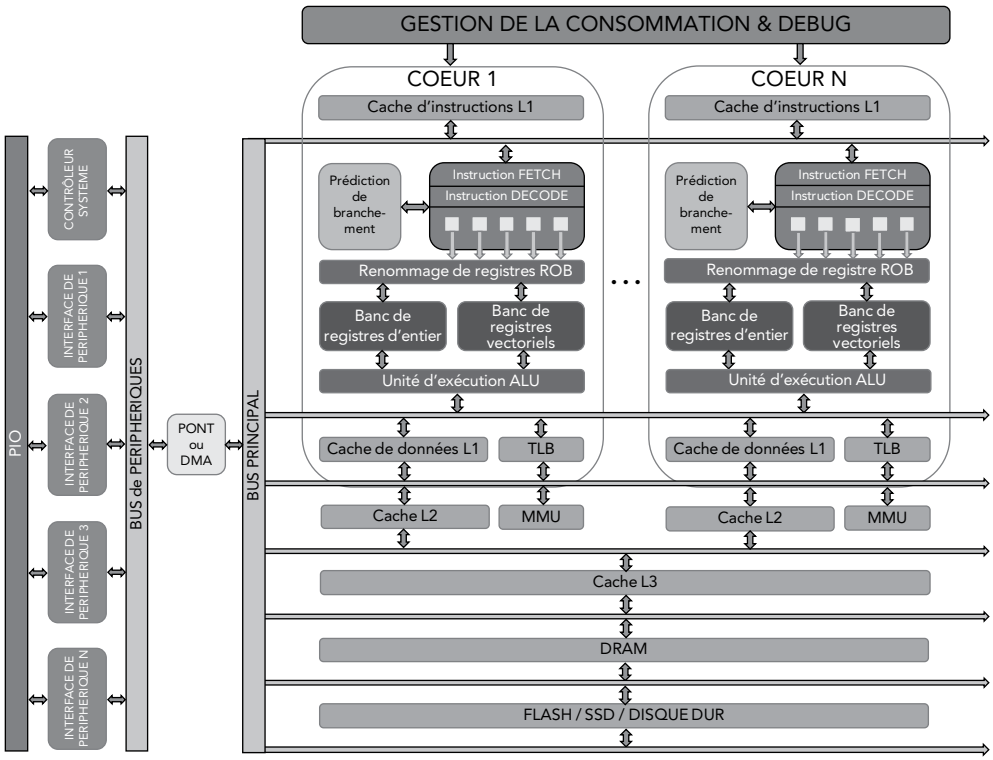

Figure I.1 Synoptique d'un processeur moderne

web PHP, contrairement à un *buffer overflow* qui mettra en défaut l'intégrité de la mémoire du processeur. Le chapitre suivant sera consacrée aux *secure boot* dont la conception très contrainte est une source de failles. En suivant notre synoptique de la Figure I.1, le cinquième chapitre étudiera les bus, les interfaces de debug et d'administration à distance (Intel ME), les périphériques, le DMA (*direct memory access*) et la gestion de l'énergie qui apportent leur lot de menaces. Enfin, l'ouvrage s'achèvera sur deux chapitres importants : les attaques par canaux cachés comme la SPA (*simple power analysis*) et la DPA (*differential power analysis*) et les attaques en faute avec entre autres l'exemple de la DFA (*differential fault analysis*).

Pour chaque attaque ou vulnérabilité étudiée, nous nous efforcerons de spécifier son cadre précis, ses causes, ses conséquences, les composants du processeur affectés, les biens mis en danger et son opportunité, c'est-à-dire la probabilité qu'elle apparaisse. Nous nous focaliserons bien sûr sur les principes de fonctionnement de ces vulnérabilités, ce qui donnera au lecteur l'occasion de revisiter ou de découvrir l'architecture des processeurs.

Nous conclurons en dérivant de toutes ces attaques des objectifs de sécurité à même de faire prendre conscience à chacun des exigences d'un processeur sécurisé et du chemin qui reste à faire pour y parvenir.

Une dernière remarque avant d'entamer cette plongée dans l'architecture des processeurs : nous avons pris le parti de garder les termes anglo-saxons pour un certain nombre de désignations d'attaques afin de préparer les novices à la lecture d'ouvrage majoritairement en anglais, mais aussi pour faciliter la compréhension des lecteurs déjà compétents dans le domaine.

Enfin, nous tenons à remercier l'IRT NanoElec et tous ses membres pour avoir rendu possible cet ouvrage.

1 Vulnérabilités des mémoires

Dans ce chapitre, nous allons introduire dans un premier temps des notions préliminaires sur la hiérarchie mémoire en l'occurrence, la mémoire cache, la mémoire virtuelle, la mémoire SRAM, la mémoire DRAM et la mémoire Flash. Dans un deuxième temps, nous présenterons les vulnérabilités potentielles de ces composants matériels à travers l'explication et l'analyse des principales attaques qui profitent de ces failles de sécurité.

1.1 Préliminaires

1.1.1 Hiérarchie mémoire

La hiérarchie mémoire d'un système numérique est constituée de différents types de mémoires. Ces dernières se distinguent par leurs vitesses d'accès, leurs débits, leurs capacités et leurs coûts. La rapidité de la mémoire est dépendante de sa technologie de fabrication et par conséquent de son prix. Depuis la fin des années 1980, les performances des processeurs se sont améliorées bien plus rapidement que celles des mémoires DRAMs. Il y a ainsi aujourd'hui une différence très importante entre la vitesse d'exécution d'un processeur et la latence d'un accès en mémoire DRAM (phénomène du « *memory wall* », Figure 1.1).

Pour combler cette différence, la mémoire est structurée en une hiérarchie de mémoires de différentes latences, tailles, débits et coûts. La conception d'une hiérarchie mémoire est un sujet de recherche complexe et très actif. La Figure 1.2 illustre de manière simplifiée la hiérarchie mémoire d'un serveur et celle d'un téléphone mobile.