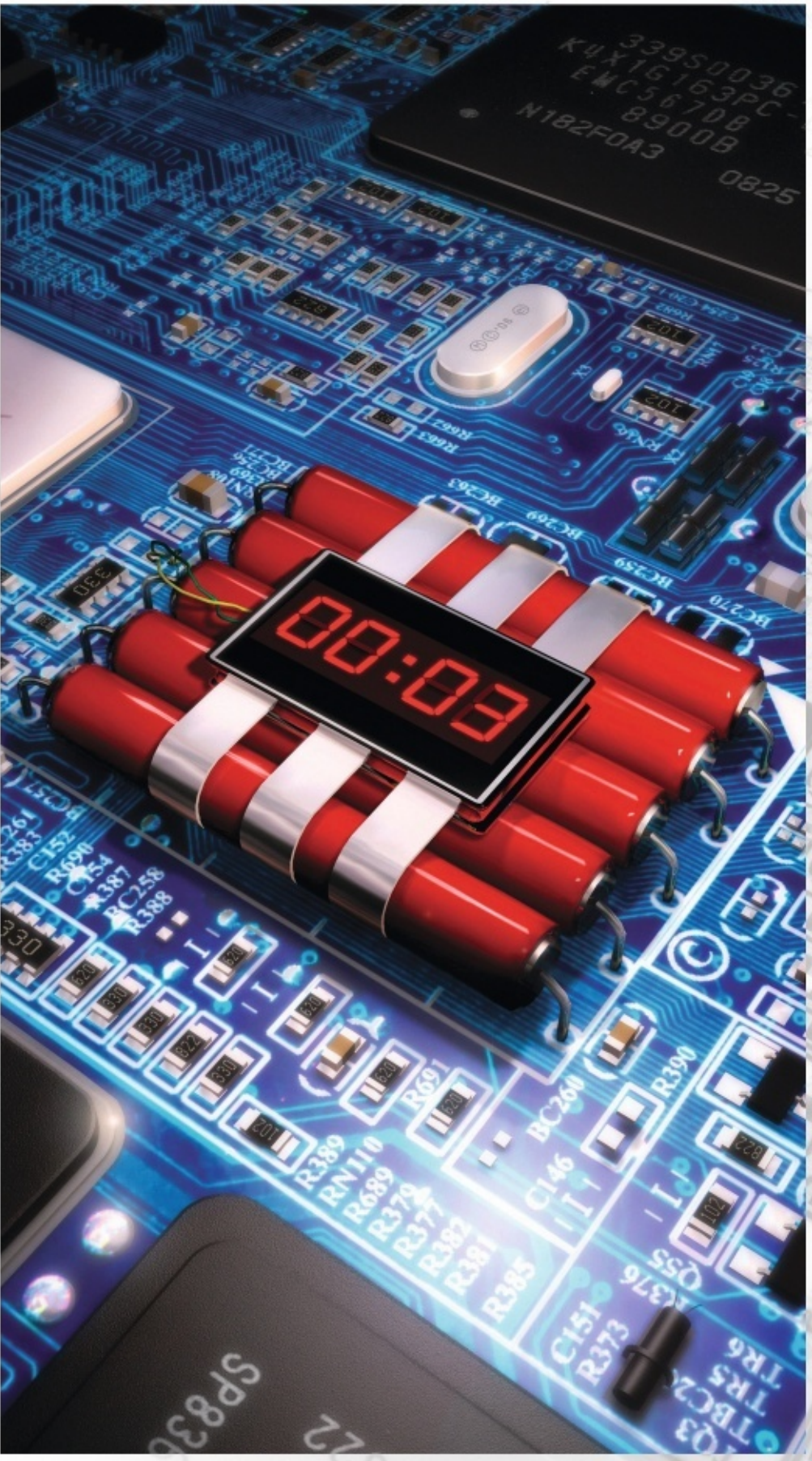


Kenn Brown Monolithic Studios

ment des marchés financiers, et presque tous les systèmes sensibles utilisés par les forces armées. Ainsi, une attaque matérielle bien conçue pourrait interrompre les transactions commerciales ou immobiliser divers secteurs stratégiques.

Les chevaux de Troie matériels peuvent rester indécelables pendant des années. Ils ne s'activent que lorsqu'ils sont déclenchés par un événement, telles une date et une heure particulières. À cause de cette faille, il est possible que de tels composants aient déjà été dissimulés dans des équipements électroniques. Aucune attaque matérielle de grande ampleur n'a été confirmée officiellement jusqu'à présent, mais la lutte contre les virus logiciels nous l'a appris : il suffit d'un petit nombre de gens mal intentionnés dotés de connaissances techniques pour faire des dégâts.

Dès maintenant, il faut se poser les questions suivantes : quelles formes ces attaques pourront-elles prendre ? Qu'en résulterait-il ? Et, plus important encore : que peut-on faire pour les détecter et les arrêter, ou du moins minimiser leurs conséquences ?

Des blocs intrusifs

Un circuit intégré, ou puce électronique, est un ensemble d'éléments électroniques miniaturisés et interconnectés (transistors, diodes, etc.), gravé sur un socle de matériau semi-conducteur, le plus souvent du silicium. Les circuits intégrés modernes sont assez petits – quelques centimètres carrés –, mais peuvent contenir plusieurs milliards de transistors. C'est la taille et la complexité des puces modernes qui rendent possibles ces attaques.

Les puces sont divisées en sous-unités, les blocs, qui effectuent des tâches différentes. Par exemple, dans un téléphone portable, un premier bloc sert à stocker les images d'une vidéo ; un deuxième compresse cette vidéo en un fichier MPEG, et un troisième convertit le fichier dans un format qui peut être transmis par une antenne. Les données se déplacent de bloc en bloc à travers le bus système, qui agit comme une autoroute connectant les différentes parties de la puce.

Quand une entreprise se lance dans la conception d'un nouveau circuit intégré, elle détermine d'abord les blocs fonctionnels dont elle va avoir besoin. Elle conçoit certains de ces blocs sur place,

soit *de novo*, soit en modifiant un modèle de bloc utilisé pour une de ses précédentes puces. D'autres blocs sont achetés auprès d'entreprises tierces spécialisées dans les circuits accomplissant tel ou tel type de fonctionnalités – recevoir des données à partir d'une antenne, par exemple.

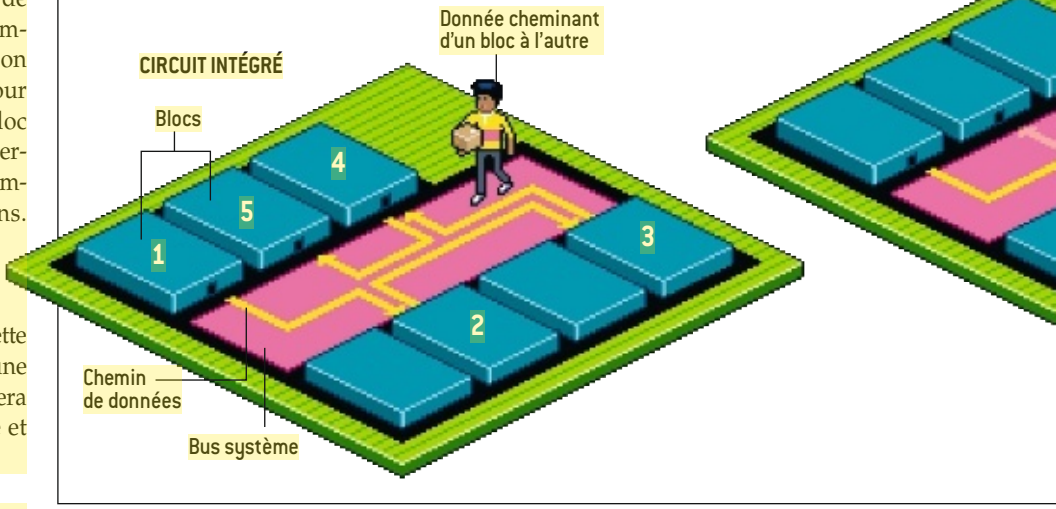
Ces blocs provenant de tiers ne sont pas fournis sous la forme d'un circuit sur silicium, car la conception des puces demande de graver tous les blocs fonctionnels sur la même surface. Au lieu de cela, ils arrivent sous forme d'un fichier de données qui décrit complètement comment le bloc devra être gravé dans le silicium. Ce fichier peut faire des milliers de lignes, ce qui rend sa lecture et la compréhension de toutes les parties de son fonctionnement quasi impossibles pour un être humain. Le concepteur du bloc fournit généralement aussi un logiciel permettant à l'acheteur de modéliser son comportement dans différentes situations. Avant que les circuits soient imprimés, l'entreprise simule comment les modèles des différents blocs de la puce fonctionnent ensemble pour s'assurer que cette dernière jouera le rôle espéré. Après une batterie de tests, l'entreprise commencera alors la fabrication physique, longue et coûteuse, du circuit intégré.

LE PROBLÈME GLOBAL DE SÉCURITÉ

Une puce comporte des circuits conçus sur plusieurs continents, par des centaines de personnes travaillant pour diverses entreprises. Grâce à cette globalisation, il est plus rapide et moins cher de développer de nouveaux produits. Mais cela multiplie également les risques, parce qu'il est presque impossible de détecter un intrus matériel caché parmi les centaines de millions de transistors de la puce durant sa fabrication.

À l'intérieur d'un circuit intégré

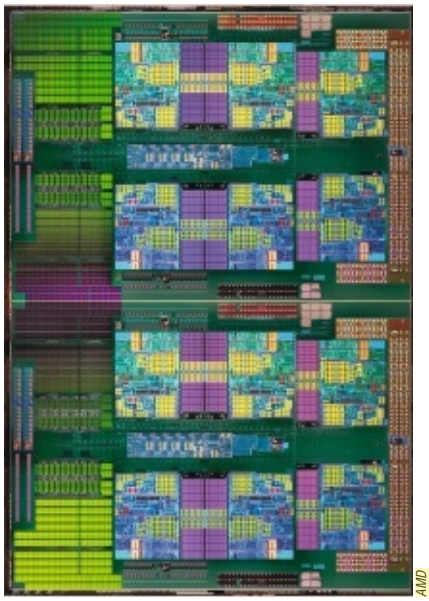
Une puce moderne contient un ensemble de blocs fonctionnels, dédiés chacun à une tâche (ou un ensemble de tâches) particulière. Les données se déplacent de bloc en bloc en passant par le bus système, et la circulation dans le bus est contrôlée par un autre bloc, l'arbitre de bus. Dans une puce de téléphone mobile, par exemple, les données passent d'un bloc mémoire (1) à un bloc qui effectue des calculs (2), puis à un autre qui code et décode de l'information (3) et à des blocs (4 et 5) qui échangent des données avec des sites extérieurs.



Un problème de confiance

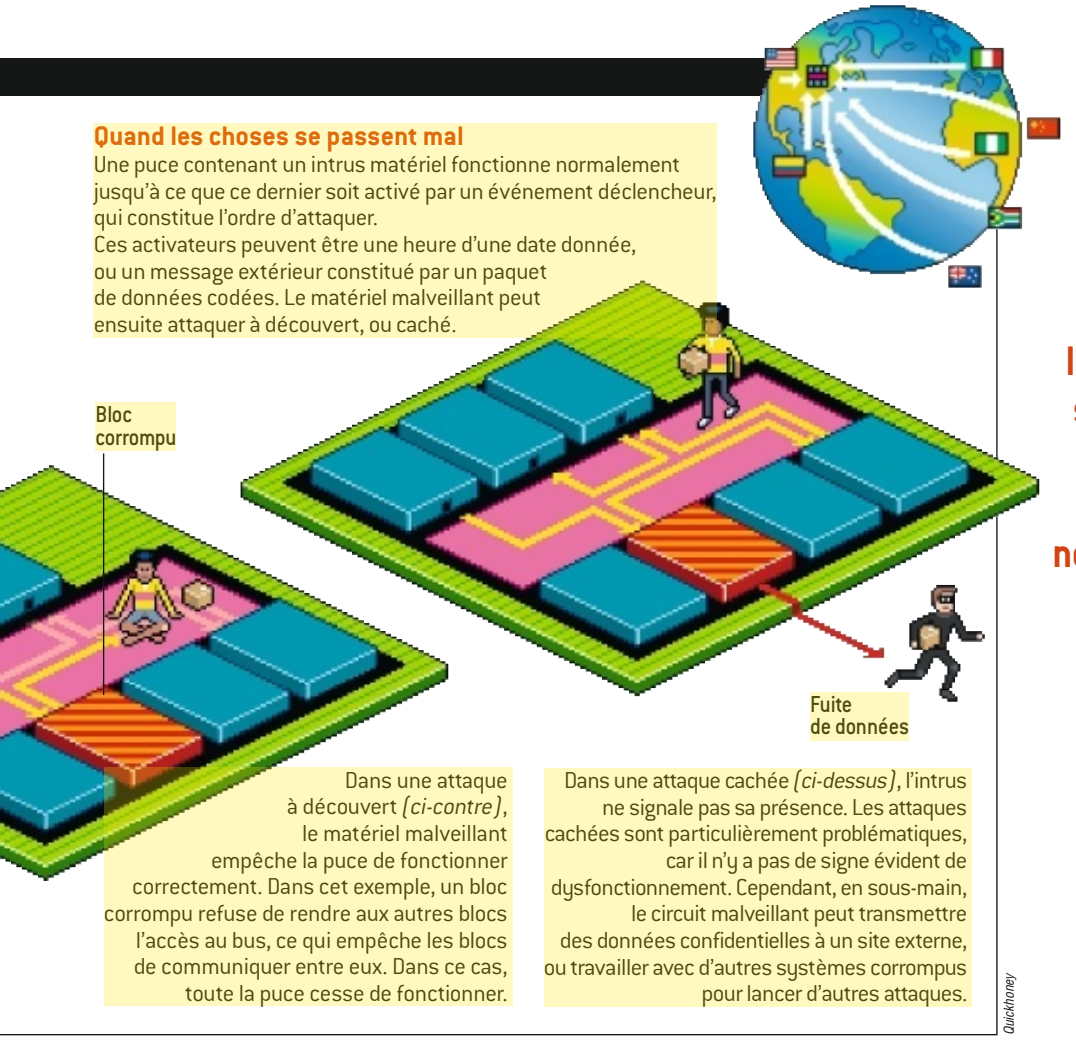
C'est ici que se trouve le talon d'Achille : puisqu'un éventuel intrus s'active sous l'effet d'un événement déclencheur, les fabricants de puces devraient en théorie tester leurs modèles de blocs contre toutes les activations imaginables. C'est mission impossible, tant le nombre de déclencheurs potentiels est grand. Outre son activation interne par une date et une heure, un matériel dissimulé peut être déclenché par exemple par la réception d'un message ou d'un courriel contenant une séquence spécifique de caractères. Les entreprises auront beau tester leurs puces, cela n'éliminera qu'une petite fraction des déclencheurs possibles.

À l'époque des débuts des circuits intégrés, personne ne se souciait des pirates. Les premières puces étaient entièrement conçues sur le même site par de petites équipes travaillant ensemble. Cette organisation garantissant la sécurité, on savait que chaque composant de la puce ferait ce que l'on en attendait, et les concepteurs ont pu établir des protocoles « ouverts », c'est-à-dire accessibles et modifiables par d'autres concepteurs autorisés. Cette histoire est à rapprocher des choix faits aux débuts du réseau Internet, quand une petite communauté d'universitaires décida de construire une plateforme ouverte qui supposait que tout le monde se comporterait honnêtement. Cette hypothèse n'a pas résisté à la croissance d'Internet.


AMD

LE PROCESSEUR OPTERON 6100 D'AMD, ici sur une vue légèrement agrandie, réunit deux circuits intégrés qui contiennent au total plus de 1,8 milliard de transistors. Les couleurs correspondent aux différents blocs fonctionnels.

Aujourd'hui, la conception d'un seul circuit intégré peut mettre à contribution des milliers de personnes travaillant sur des sites répartis sur plusieurs continents. Un fabricant des États-Unis peut combiner des blocs issus de plusieurs de ses filiales avec d'autres provenant de fournisseurs américains, européens ou indiens, puis faire fabriquer la puce dans une usine chinoise. Ces réseaux mondiaux se sont imposés ces dernières années et ont permis de réduire les coûts et d'améliorer la productivité. En revanche, assurer la sécurité dans ces conditions est bien plus compliqué qu'à



Quand les choses se passent mal

Une puce contenant un intrus matériel fonctionne normalement jusqu'à ce que ce dernier soit activé par un événement déclencheur, qui constitue l'ordre d'attaquer.
Ces activateurs peuvent être une heure d'une date donnée, ou un message extérieur constitué par un paquet de données codées. Le matériel malveillant peut ensuite attaquer à découvert, ou caché.

Dans une attaque à découvert *(ci-contre)*, le matériel malveillant empêche la puce de fonctionner correctement. Dans cet exemple, un bloc corrompu refuse de rendre aux autres blocs l'accès au bus, ce qui empêche les blocs de communiquer entre eux. Dans ce cas, toute la puce cesse de fonctionner.

Dans une attaque cachée *(ci-dessus)*, l'intrus ne signale pas sa présence. Les attaques cachées sont particulièrement problématiques, car il n'y a pas de signe évident de dysfonctionnement. Cependant, en sous-main, le circuit malveillant peut transmettre des données confidentielles à un site externe, ou travailler avec d'autres systèmes corrompus pour lancer d'autres attaques.

Quickhoney

Dans la réalité, les mesures prises pour sécuriser la conception et la fabrication des circuits intégrés ne sont jamais parfaites.

l'époque où tout était fait sur un seul site. Il n'est pas improbable qu'un tiers non autorisé accède à la conception en cours et la corrompe sans que cela soit détecté. Il y a aussi un risque faible, mais non négligeable, que l'élaboration de la puce soit dénaturée par une personne légitimement inscrite dans le processus.

Sécuriser les circuits

Idéalement, les pirates ne devraient jamais avoir l'occasion d'accéder au circuit intégré durant sa conception et sa fabrication. Si toutes les étapes de la chaîne étaient effectuées par des entreprises et des personnes dignes de confiance, dans un environnement sécurisé, et si les puces étaient testées de façon exhaustive, alors – du moins en théorie – le risque qu'un agent malveillant s'en prenne à un élément du circuit serait quasi nul. C'est cette stratégie que l'Agence du Pentagone pour les projets de recherche avancée de défense, la DARPA *(Defense Advanced Research Projets Agency)*, a mise en avant avec son programme *Trust in Integrated Circuits* (Confiance dans les circuits intégrés). Cependant, dans la réalité, les mesures prises pour sécuriser la conception des circuits ne sont jamais parfaites.

En plus des mesures de protection en amont, les concepteurs de matériel doivent construire des circuits qui identifient les attaques et y répondent au moment où elles ont lieu. On peut voir cela comme une sorte de force de police urbaine : si une ville se doit de prendre toutes les mesures raisonnables visant à prévenir les délits, ces efforts ne seront jamais efficaces à 100 pour cent ; elle doit aussi disposer d'une police capable de réagir vite et de façon pertinente quand des délits sont effectivement commis.

Une puce capable de détecter des attaques et d'y répondre est nommée circuit sécurisé. Elle peut intégrer une circuiterie supplémentaire conçue spécialement pour surveiller son fonctionnement et rechercher des comportements

L'AUTEUR

John VILLASENOR est chercheur au Département de génie électrique de l'Université de Californie à Los Angeles.