lations en trois dimensions montrent la croissance stellaire dans toute sa complexité. L'afflux de matériau n'y est pas uniforme ; les régions denses alternent avec des bulles où la lumière stellaire peut s'échapper. Ainsi, la pression radiative pourrait finalement ne pas faire obstacle à la croissance. Des étoiles compagnons se forment aussi facilement à partir du matériau dense en accrétion, expliquant pourquoi les étoiles massives sont rarement solitaires. Les astronomes cherchent maintenant la confirmation de ces simulations en observant avec le télescope *Spitzer* des régions de formation d'étoiles massives. La vérification sera cependant délicate : la rareté et la brièveté de ces étoiles rendent leur formation difficile à observer.

Heureusement, de nouveaux équipements vont permettre de progresser sur les questions liées à la formation des étoiles. *Herschel* et SOFIA observent depuis peu les longueurs d'onde submillimétriques et de l'infrarouge lointain, domaines où la formation stellaire est la plus facile à voir. Ils ont la résolution spatiale et spectrale nécessaire pour cartographier la répartition des vitesses dans les nuages interstellaires. Aux plus grandes longueurs d'onde, l'interféromètre ALMA, en construction dans les Andes chiliennes, permettra de cartographier les protoétoiles avec un luxe de détails.

Avec ces nouvelles observations, les astronomes espèrent déterminer le cycle de vie complet du milieu interstellaire, des nuages atomiques aux nuages moléculaires, jusqu'aux cœurs préstellaires et aux étoiles, et enfin le retour au gaz diffus. Ils espèrent également observer les disques protostellaires avec une résolution angulaire suffisante pour suivre la chute de matériau issu du nuage, ainsi que comparer les effets de différents environnements sur la naissance des étoiles.

Les réponses auront des répercussions dans d'autres domaines de l'astrophysique. La théorie actuelle de la formation stellaire n'est pas mauvaise, mais ses lacunes nous empêchent d'expliquer certains des aspects les plus importants de l'Univers. La formation stellaire est un processus plus riche que ce que nous avions anticipé. ■

✔ BIBLIOGRAPHIE

M. Krumholz *et al.*, **The formation of massive star systems by accretion**, *Science*, vol. 323, pp. 754-757, 2009. arxiv.org/abs/0901.3157

S. P. Zwart, **Les frères perdus du Soleil**, *Pour la Science* n° 387, janvier 2009. http://bit.ly/pls387-soleil

M. Heydari-Malayeri, **L'énigmatique formation des étoiles massives**, *Pour la Science* n° 359, septembre 2007. http://bit.ly/pls359-etoiles-massives

S. Mohanty et R. Jayawardhana, **La naissance tragique des naines brunes**, *Pour la Science* n° 340, février 2006. http://bit.ly/pls340-naines-brunes

E. Young et *al.*, ***Spitzer* and Magellan observations of NGC 2264 : a remarkable star-forming core near IRS-2**, *Astrophysical Journal*, vol. 642, n° 2, pp. 972-978, 2006. Arxiv.org/abs/astro-ph/0601300

Les attaques de circuits intégrés

John Villasenor

Des microcomposants peuvent être introduits à des fins malveillantes dans les circuits intégrés avant leur sortie d'usine. Tout dispositif électronique est une cible potentielle.

Votre téléphone portable ne répond plus ; le clavier est inactif et vous n'arrivez plus à envoyer ni à recevoir d'appels ou de messages textuels. Après avoir sans succès tenté d'éteindre l'appareil, vous retirez la batterie, la réinsérez, mais le téléphone demeure inerte. Manifestement, la panne est inhabituelle. Quelques heures plus tard, vous apprenez que votre cas est loin d'être isolé : le mobile de millions de personnes s'est figé de façon aussi soudaine qu'inexplicable.

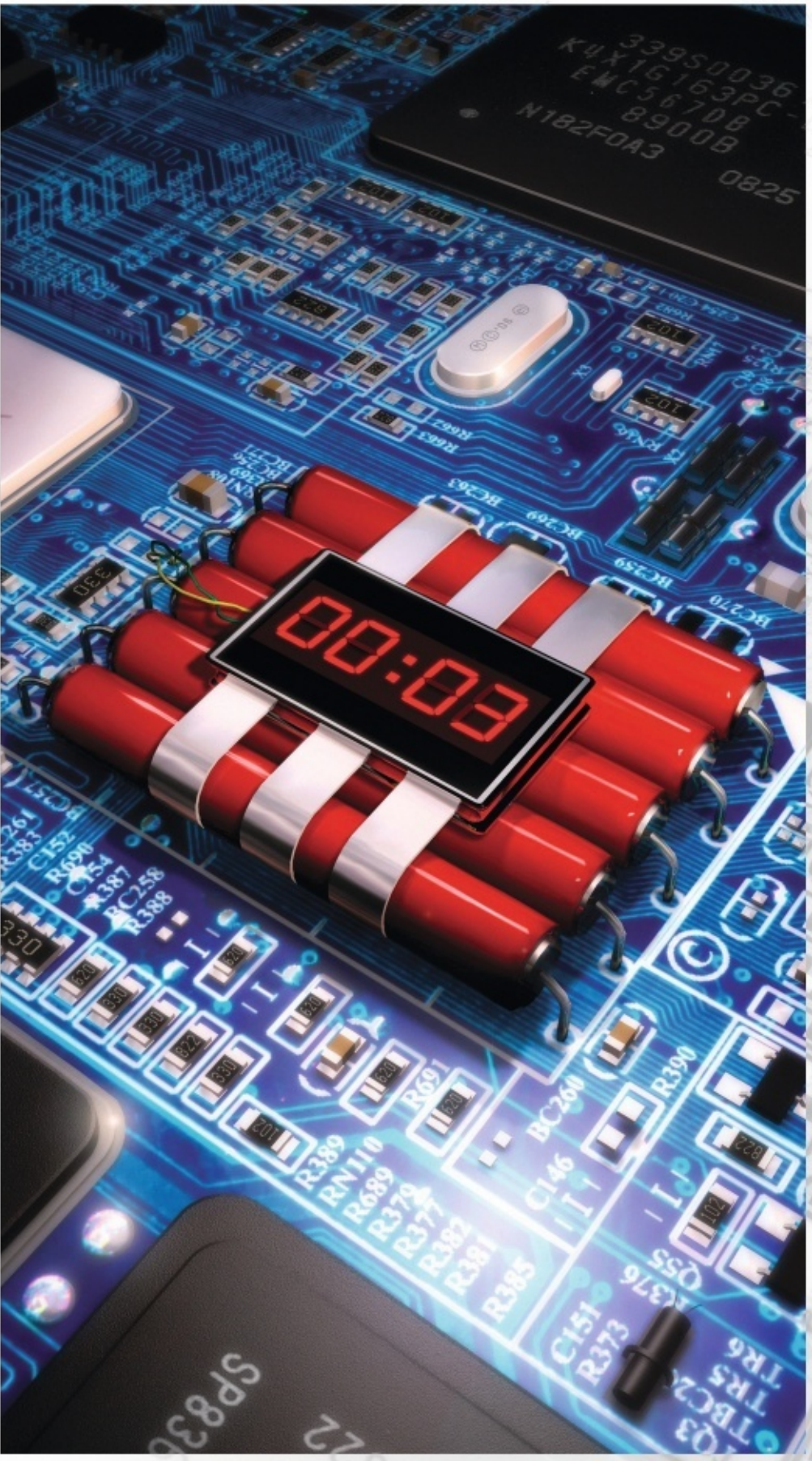
Voilà comment pourrait se manifester une attaque matérielle à grande échelle. Cette menace augmente à mesure que les circuits intégrés qui contrôlent de nombreux équipements de la vie courante se perfectionnent. Chaque circuit, ou puce électronique, est devenu si complexe qu'aucune équipe d'ingénieurs ne connaît tous ses composants ; au contraire, ses différentes parties sont conçues un peu partout dans le monde, puis réunies pour la première fois lorsque la puce est gravée dans du silicium. Le produit final est si complexe que les tests fonctionnels qu'il subit ne peuvent tout vérifier. Aussi, une pièce qui serait insérée dans la puce avec une intention malveillante restera indétectée… jusqu'au moment où elle sera activée par un événement déclencheur. Tel un cheval de Troie, elle ne passera à l'attaque qu'après avoir pénétré dans sa cible.

La nature des attaques matérielles les rend potentiellement bien plus pernicieuses que les vers, virus et autres logiciels malveillants. Même si un virus informatique peut se déplacer de machine en machine, il est en principe possible, à l'aide d'un antivirus, de l'éradiquer du système qu'il a infecté. En revanche, le seul moyen de remédier à une attaque matérielle consiste à changer les circuits infectés. Du moins pour l'instant.

La question tracasse tous les experts de la cybersécurité. En effet, tout ce qui contient un microprocesseur – c'est-à-dire tout ce qui est électronique – est vulnérable. Les circuits intégrés sont au cœur de nos systèmes de communication et de distribution d'électricité. Ils positionnent les volets des ailes des avions de ligne et modulent la puissance du système antiblocage des freins des voitures. Ils contrôlent l'accès aux coffres des banques, aux distributeurs de billets, le fonctionne-

L'ESSENTIEL

- ✔ **De plus en plus complexes et puissants, les circuits intégrés, ou puces électroniques, sont aussi plus vulnérables aux attaques dites matérielles.**
- ✔ **Un « cheval de Troie » matériel peut bloquer le fonctionnement d'une puce des années après sa fabrication.**
- ✔ **Toutefois, la protection des équipements contre ces attaques matérielles ne relève pas de l'utopie.**



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.

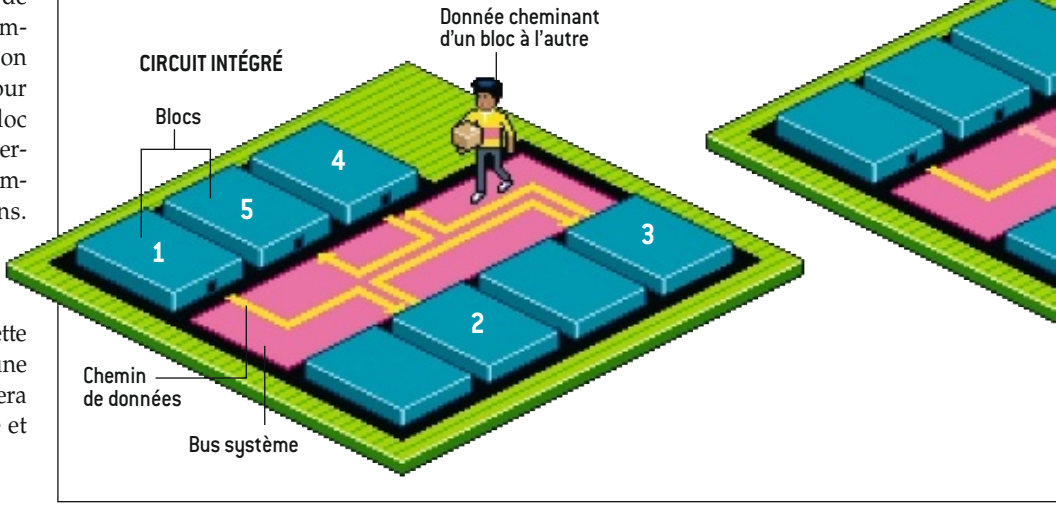
Ces blocs provenant de tiers ne sont pas fournis sous la forme d'un circuit sur silicium, car la conception des puces demande de graver tous les blocs fonctionnels sur la même surface. Au lieu de cela, ils arrivent sous forme d'un fichier de données qui décrit complètement comment le bloc devra être 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

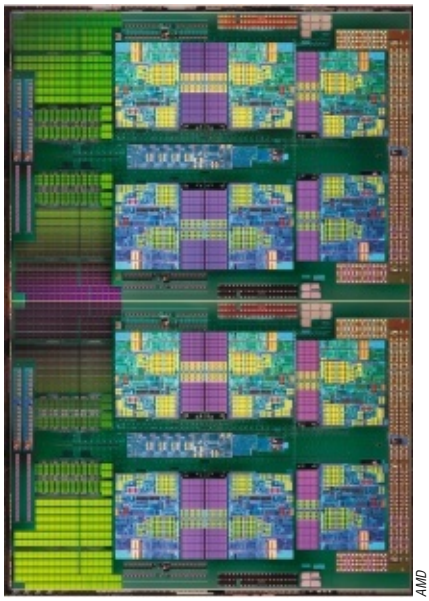
Une puce moderne contient un ensemble de blocs fonctionnels, dédiés chacun à une tâche (ou un ensemble de tâches) particulière. Les données se déplacent de bloc en bloc en passant par le bus système, et la circulation dans le bus est contrôlée par un autre bloc, l'arbitre de bus. Dans une puce de téléphone 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.

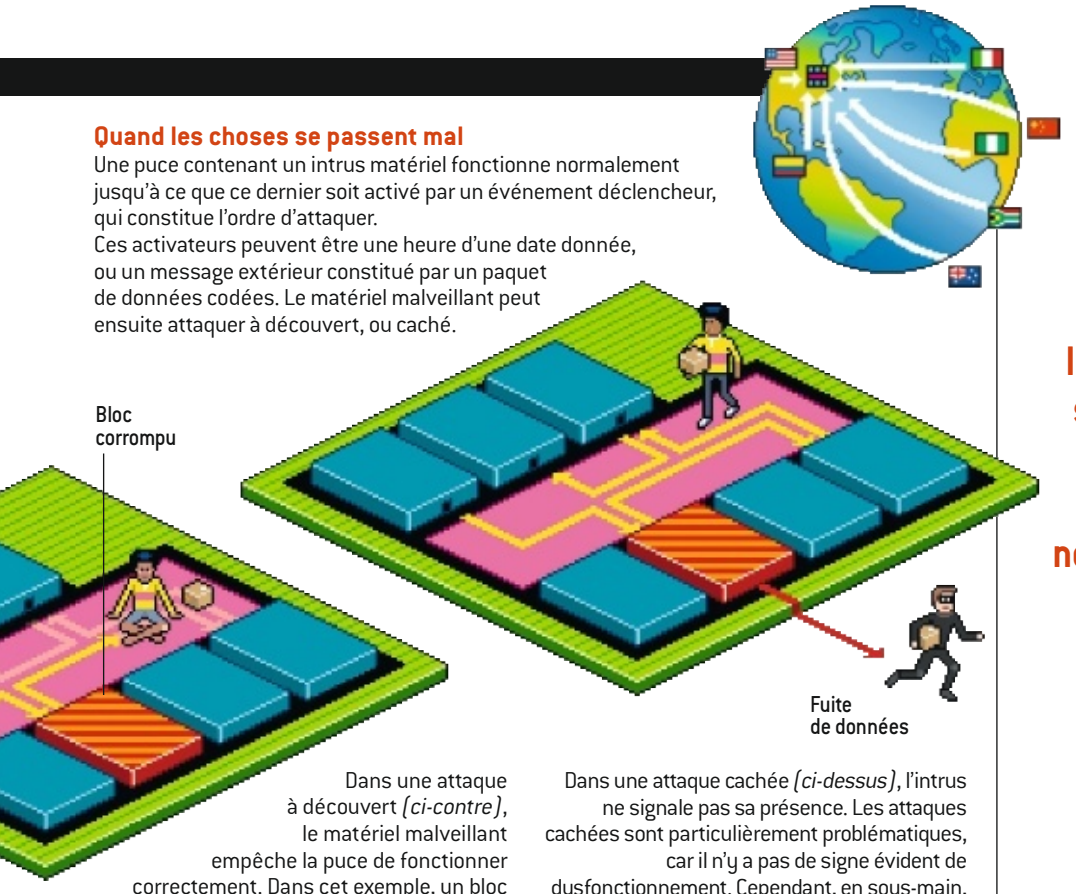

AMD

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.

COMMENT CONTRER LES ATTAQUES MATÉRIELLES

Un circuit intégré sécurisé contient quelques éléments de circuit supplémentaires qui maintiennent l'ordre à l'intérieur de la puce. Quand un comportement hostile est détecté, un ensemble de mesures de sécurité peut être appliqué en quelques microsecondes pour identifier la source de l'attaque et la surmonter. Voici quelques stratégies en cours de développement.

Mesure de sécurité	Ce qu'elle empêche	Comment elle marche
Portier de la mémoire	Toute tentative de la part d'un bloc malveillant de dépasser les limites de sa mémoire propre, ce qui entrave l'espionnage ou la corruption de données.	Un portier assure qu'un bloc n'accède qu'aux parties autorisées de la mémoire, et signale toute tentative d'accès non autorisé.
Bus système sécurisé	Une prise de contrôle malveillante du bus système qui pourrait avoir pour conséquence un arrêt total du circuit ou un ralentissement majeur du fonctionnement.	Le bus analyse des motifs statistiques d'accès au bus par les différents blocs fonctionnels et signale les comportements étranges.
Dispositif de surveillance d'entrée/sortie	L'espionnage à couvert – lorsque la puce essaye de copier des données vers un site hors de la puce.	Le circuit analyse les mouvements de données sur la puce et vers l'extérieur, et compare ce flux avec le motif attendu, signalant toute aberration.
Test de bloc sur place	Une attaque de cheval de Troie matériel qui tente d'endommager un bloc initialement « sain ».	Un vérificateur d'intégrité de puces teste de temps à autre les blocs pour s'assurer qu'ils continuent de fonctionner comme prévu.
Circuits logiques programmables additionnels	Permet au circuit de mettre en quarantaine un bloc contaminé et d'assumer sa fonction.	Les circuits additionnels sont configurés pour remplacer le bloc fonctionnel mis en quarantaine – bien que vraisemblablement à une vitesse plus faible.
Système d'alerte d'attaque	Permet aux autres circuits de se protéger de façon préventive contre des attaques imminentes.	Un circuit attaqué met en place des contre-mesures et envoie un avertissement aux autres dispositifs contenant le même circuit.

Quickhoney

qui pourraient révéler une attaque matérielle. Si une attaque est soupçonnée, le circuit sécurisé identifiera le type d'attaque et prendra les mesures nécessaires pour minimiser les dommages qui en résulteraient.

Dans le cas d'un téléphone mobile paralysé, la panne peut être liée au dysfonctionnement d'un seul bloc d'un circuit intégré. Ce bloc interagit avec tous les autres blocs *via* le bus système. Lequel est lui-même contrôlé par un arbitre de bus, un « agent de la circulation » qui détermine quelles informations peuvent y transiter et à quel moment. Cependant, cette analogie n'est pas parfaite. Alors qu'un agent de la circulation peut ordonner au trafic de démarrer et de s'arrêter, un arbitre de bus n'a pas cette autorité. Il peut donner la permission à un bloc de démarrer, mais le bloc garde ce droit aussi longtemps qu'il veut – héritage de la vieille idée qu'un bloc se comporte toujours correctement. C'est là que réside le problème.

Dans un système habituel, un bloc garde l'accès au bus aussi longtemps qu'il en a besoin, avant de rendre ce droit pour que les autres blocs en profitent. L'arbitre de bus « voit » que le bus système est disponible, et l'assigne à un autre bloc. Mais si un bloc garde le contrôle du bus indéfiniment, de nouvelles données ne pourront plus se déplacer dans le circuit intégré, lequel se bloquera.

Mise en quarantaine

Au contraire, un circuit intégré sécurisé effectue en permanence des vérifications pour s'assurer que les communications entre les différents blocs ne sont pas perturbées. Quand il détecte qu'un bloc monopolise l'accès au bus, il réagit en mettant en quarantaine le bloc menaçant. Il peut ensuite utiliser sa réserve de circuits programmables pour remplacer la fonctionnalité perdue. Ce mécanisme a de fortes chances de ralentir l'équipement, mais il lui permet au moins de continuer à fonctionner.

Cependant, la menace la plus pernicieuse n'est vraisemblablement pas le cas simple où une attaque matérielle met le système hors d'usage. Il peut arriver que l'équipement donne l'impression de fonctionner normalement, alors qu'il agit en réalité à des fins malveillantes. Dans le cas des mobiles, par exemple, le téléphone peut commencer à secrètement

transmettre une copie de tous les messages entrants et sortants à une tierce partie. Un observateur sans méfiance ne remarquerait rien, et l'attaque pourrait continuer indéfiniment.

Dans ce cas particulier, une puce sécurisée surveillerait en permanence la quantité et le type de données entrant et quittant le circuit intégré et comparerait statistiquement le flux d'informations avec celui attendu. Toute anomalie serait signalée comme une fuite potentielle de données, et la puce pourrait alerter l'utilisateur ou commencer à la juguler.

Outre qu'il peut lutter contre les effets des intrus sur son propre fonctionnement, un circuit intégré sécurisé peut signaler aux équipements voisins le type d'attaque et leur permettre ainsi de prendre des mesures préventives pour l'éviter (ou du moins minimiser ses effets). Un tel système de notification n'est pas aussi irréaliste qu'on pourrait le croire, presque tous les systèmes étant plus ou moins connectés. Par exemple, si un circuit sous attaque est en mesure d'identifier le message activateur responsable de la défaillance, il peut alerter les autres circuits pour qu'ils filtrent ce déclencheur.

Les mesures décrites ici ne seront effectives que si les parties du circuit responsables de la gestion de la sécurité sont elles-mêmes sécurisées et dignes de confiance. C'est comme si, pour sécuriser un circuit, il fallait sécuriser sa sécurité. Mais les éléments d'un circuit dédiés à la sécurité ne représentent qu'une petite fraction de la conception globale. Ces éléments peuvent être conçus sur place pour que seuls des intervenants vraiment dignes de confiance y aient accès.

Un compromis entre efficacité et sécurité

Grâce aux efforts des gouvernements, des chercheurs et des entreprises, d'importants progrès ont été réalisés dans la sécurité d'Internet. On ne peut pas en dire autant de l'infaillibilité des circuits intégrés, qui en est à peu près au même stade que la sécurité d'Internet il y a 15 ans : la prise de conscience du problème va croissant, mais les stratégies défensives n'ont pas encore été complètement élaborées, et encore moins mises en pratique.

Une approche de lutte complète contre les attaques matérielles par les chevaux de Troie matériels nécessite des actions à plusieurs niveaux. Les stratégies qui visent à ce qu'aucun matériel compromis ne voie jamais le jour, comme l'initiative de la DARPA, représentent un bon début. Cependant, il est plus important encore de commencer à mettre en œuvre des mesures de conception sécurisée, seules à même d'assurer une défense contre des attaques en cours. Ces mesures demanderont du temps, de l'argent et des efforts. Différents compromis possibles entre efficacité, sécurité et coût permettront d'obtenir un bon niveau de protection pour des coûts acceptables.

Mon équipe, à l'Université de Californie à Los Angeles, a montré qu'il suffit d'augmenter la taille de la puce de quelques centièmes pour y ajouter une circuiterie de défense. La vitesse de fonctionnement baisse un peu, étant donné que les mesures prises pour vérifier le comportement des blocs fonctionnels consomment des ressources du système qui seraient normalement utilisées pour effectuer la tâche en cours.

LA SÉCURISATION DES CIRCUITS INTÉGRÉS devra sans cesse innover pour garder une longueur d'avance sur les dernières attaques matérielles.

Toutefois, les ralentissements sont relativement faibles, voire inexistants, si les mesures de sécurité sont effectuées en utilisant une part des circuits et des unités fonctionnelles inactives.

Inévitablement, la lutte contre les attaques matérielles va devenir une course aux armements comparable à celle que l'on a connue dans l'univers du logiciel. La sécurisation des circuits devra innover continuellement pour garder une longueur d'avance sur les dernières attaques. Pour contrer les failles de sécurité détectées dans les logiciels, il suffit d'aller chercher le remède sur Internet. Il est impossible de télécharger de la même manière du matériel de dépannage. Toutefois, les circuits intégrés modernes peuvent être reconfigurés en partie. Si l'on ajoute des mesures judicieuses au processus de conception, il est envisageable de remplacer automatiquement des parties d'un circuit qui auraient été mises hors d'usage. La flexibilité de la conception est notre meilleure défense. Même si les attaques matérielles sont inévitables, nous ne sommes pas condamnés à les voir réussir. ■

Les puces en chiffres

✔ 1 550
Le nombre estimé d'entreprises dans le monde impliquées dans la conception de circuits intégrés : 700 en Amérique du Nord, 600 en Asie et 250 en Europe, au Moyen-Orient et en Afrique.

✔ 2 500
Le nombre approximatif de nouvelles puces conçues chaque année.

✔ 180
La recette globale des ventes de semi-conducteurs en 2009, en milliards d'euros.

✔ BIBLIOGRAPHIE

L. Kim, J. Villasenor et C. Koc, **A trojan-resistant system-on-chip bus architecture**, *Proceedings of the 2009 IEEE Military Communications Conference*, Boston, octobre 2009.

W. K. Clark et P. L. Levin, **Securing the information highway**, *Foreign Affairs*, novembre-décembre 2009.

D. Agrawal *et al.*, **Trojan detection using IC fingerprinting**, *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, Berkeley, mai 2007.

Pourquoi l'homme n'a plus de fourrure

Nina Jablonski

De récentes découvertes dévoilent pourquoi et quand les hominidés, contrairement aux autres primates, ont perdu leur fourrure. Et l'apparition d'une peau quasi nue aurait favorisé l'émergence d'autres caractéristiques humaines.

L'ESSENTIEL

- La fourrure réchauffe le corps et protège de l'humidité, des rayons du soleil et des microbes.
- Pourtant, l'homme en est dépourvu, mais il est équipé d'un dispositif maintenant sa température corporelle constante, même quand son organisme s'échauffe longtemps.
- En effet, sa transpiration est unique et efficace ; elle évacue bien l'excès de chaleur, notamment parce que sa peau est quasi nue.
- Les scientifiques en ont déduit que les longs trajets entrepris par les premiers hommes auraient favorisé la sélection d'une peau sans fourrure.

L'homme est un primate, mais il est le seul à avoir une peau presque glabre. Tous les autres primates présentent une fourrure dense, par exemple le pelage noir du singe hurleur ou le manteau couleur cuivrée de l'orang-outan. C'est aussi le cas de la plupart des autres mammifères. L'homme a des poils sur la tête et en quelques autres endroits, mais, comparé à ses proches parents, même le plus poilu des hommes ne l'est guère.

Pourquoi l'homme n'a-t-il pas de fourrure ? Cela fait des siècles que les scientifiques réfléchissent à cette question, en vain. Dans l'évolution humaine, la plupart des transitions importantes, telle l'émergence de la bipédie, sont inscrites dans les fossiles des ancêtres. Mais aucun des restes connus n'a conservé de traces de peau humaine.

Toutefois, depuis quelques années, des chercheurs ont remarqué que les fossiles contiennent des preuves indirectes de la transformation de la peau humaine. Grâce à ces indices et aux éléments obtenus depuis dix ans en génétique et en physiologie, nous sommes parvenus à expliquer pourquoi les êtres humains ont perdu leur fourrure, et quand cela s'est produit. En outre, notre scénario suggère que l'apparition d'une peau quasi glabre a participé à l'évolution d'autres traits caractéristiques de l'homme, notamment son cerveau très développé.

Pour comprendre pourquoi les ancêtres de l'homme ont perdu leur fourrure, voyons d'abord pourquoi d'autres espèces en ont une. Les poils sont un revêtement corporel spécifique des mammifères. En