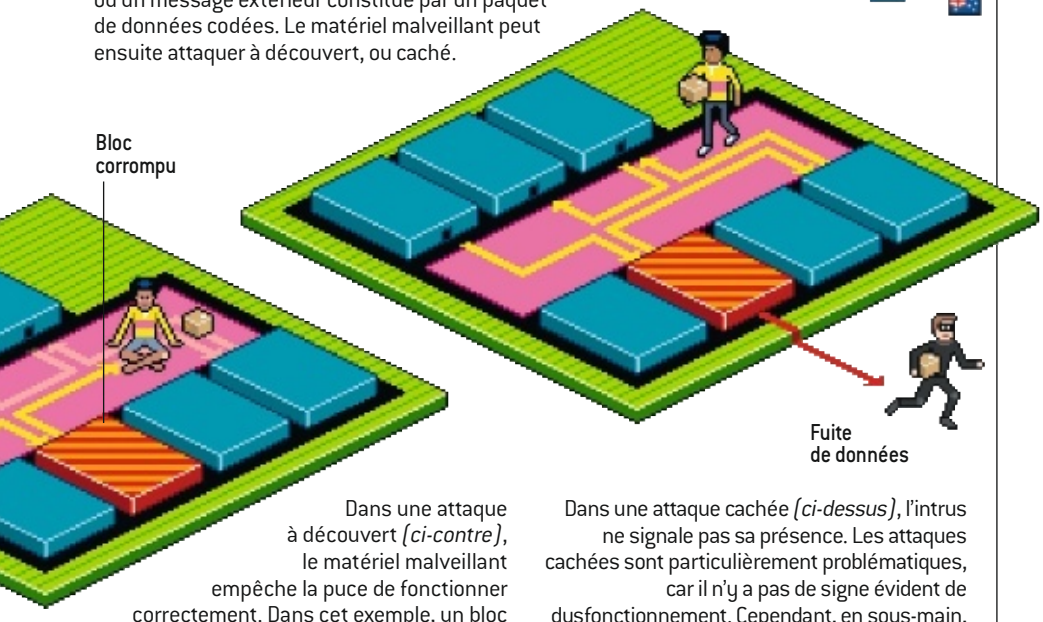
Quand les choses se passent mal

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