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.