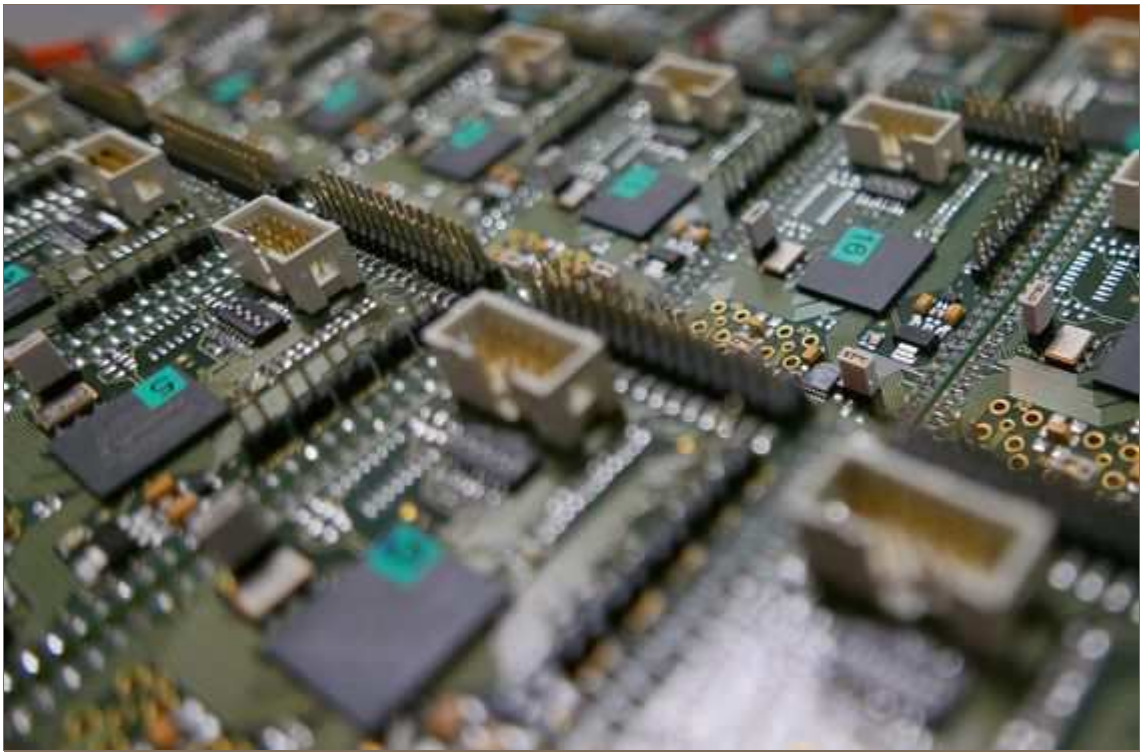
Le Monde
7 décembre 2016

article suivant
Quand le vide cosmique distord la lumière...

Déjouer la contrefaçon de composants électroniques



Des composants électroniques munis de dispositifs anticontrefaçon fabriqués dans le cadre du projet Salware.

Sonia Barcet

InformatiqueLa moitié des fabricants de semi-conducteurs ont été confrontés à des détournements de leurs technologies. Pour éviter les copies illicites, les chercheurs mettent au point des empreintes digitales qui rendent chaque puce unique et traçable

Depuis l'été, il est possible de se procurer la dernière version d'une clé USB qui... détruit les ordinateurs. Cette " tueuse " largue brièvement des charges électriques dans les composants qui ne s'en remettent pas. Récemment, le concept est devenu plus malveillant -encore avec des clés vendues sous des marques connues, pour tromper les acheteurs. Ce n'est que l'un des derniers avatars des méfaits de la contrefaçon des circuits électroniques, mémoire, transistors, processeurs, composants analogiques... qui ne cessent d'augmenter.

Mark Tehranipoor, professeur en cybersécurité à l'université de Floride et spécialiste de ces questions, rappelle dans ses derniers articles que la quantité recensée de contrefaçons a quadruplé depuis 2009. La moitié des fabricants de semi-conducteurs auraient en outre déjà été confrontés à ce problème. *" Deux très importants industriels du domaine aéronautique m'ont parlé de composants électroniques et de circuits intégrés contrefaits dans leurs approvisionnements, notamment de circuits intégrés qui semblaient tout à fait authentiques... mais qui étaient -vides ! "*, rapporte Lilian Bossuet, enseignant-chercheur à l'université de Saint-Etienne.

Le 5 décembre, pour ses travaux de lutte contre les circuits contrefaits, il a reçu le Grand Prix de l'électronique Général Ferrié de la Société française d'électronique, d'électricité et des technologies de l'information et de la communication. Il cite des estimations de l'ordre de 7 % à 10 % de pertes, dues aux contrefaçons, sur plus de 330 milliards de dollars (309 millions d'euros) de chiffre d'affaires pour cette industrie en 2015. Les premiers à avoir tiré la sonnette d'alarme à partir de 2010 sont les militaires américains. Un rapport de 2014 recense des composants défectueux dans les systèmes de vision infrarouge d'hélicoptères, dans le dégivrage d'avions de patrouille, l'affichage des données de vol d'un avion de transport...

" Ce qui est alarmant, c'est qu'un composant coûtant moins de 2 dollars peut compromettre l'intégralité d'un système coûtant plus de 10 millions de dollars, comme le rappellent souvent les responsables des programmes d'armement américains ", souligne Jérome Rampon, directeur d'Algodone, jeune entreprise française qui propose des solutions anticontrefaçon. *" Certes, les secteurs-clés comme la défense, l'énergie, la -finance... sont les plus sensibles, mais le grand -public aussi peut être touché si les systèmes contrefaits contiennent des virus par exemple*, estime Mark Tehranipoor. *On manquait de recherches sur le sujet jusqu'à récemment, mais il y en a de plus en plus et les fabricants ont pris conscience du problème. "* Sur ce marché émergent, plusieurs start-up apportent dessolutions : Intrinsic-ID, Verayo, ICTK, Quantumtrace, Invia...

Mais comment peut-on copier un circuit électronique ? En volant les plans, pour reproduire le composant. Ou bien, plus technique, en l'étudiant par rétro-ingénierie afin d'en percer les secrets. Plus courant est ce qui se passe dans les chaînes de production, qui sont de moins en moins la propriété des entreprises conceptrices. Celles-ci commandent une certaine quantité de circuits à un tiers, qui peut très bien en fabriquer plus pour alimenter un second marché. Enfin, solution la plus économique, le recyclage et le maquillage de composants, tirés des déchetteries, en produits ayant l'apparence du neuf ou des derniers modèles.

Contrôler la chaîne de production

L'industrie a d'abord réagi en développant des contrôles (optique, électrique, par rayons X...) pour vérifier si les composants sont bien authentiques ; ce qui n'est pas toujours simple. Puis elle en est venue à des parades plus directes : mieux contrôler la chaîne de production, ajouter des compteurs de longévité afin de limiter le recyclage illégal, camoufler des circuits sous de fines couches de matière ou ajouter des transistors inutiles.

Plus récemment, d'autres idées sont apparues : doter les circuits de l'équivalent d'empreintes -digitales, uniques et stables dans le temps. Ces techniques exploitent le fait que les procédés de fabrication de la microélectronique ont beau être très précis, il existe en réalité d'infimes différences de comportement entre toutes les pièces. Par exemple, lorsqu'une mémoire vive (RAM) se rallume, ses cellules se mettent aléatoirement dans les états 0 ou 1, mais identiquement à chaque fois. Intrinsic-ID utilise ce principe pour " signer " ces mémoires depuis 2008. D'autres ont proposé d'ajouter des mini-horloges dont la -cadence d'oscillation, aléatoire du fait de la fabrication, serait propre à chaque circuit.

Et comme souvent en matière de sécurité, des chercheurs ont montré qu'il était malgré tout possible de cloner ces parades et donc de leurrer un fabricant. C'est ce qu'a fait Lilian Bossuet en 2013, avant de proposer en 2015 une autre technique utilisant différemment les mini-horloges et qui reste pour l'instant inviolée. Seule une centaine de transistors supplémentaires est ajoutée, ce qui est dérisoire par rapport aux milliards que contiennent les puces désormais.

Au CEA, une autre solution a été étudiée pour gêner la rétro-ingénierie. En " écoutant " un processeur qui calcule, par exemple en surveillant sa consommation électrique, il est possible d'en -déduire les opérations qu'il effectue, voire d'extraire des chiffres secrets utilisés lors d'un chiffrement. La solution Cogito, défendue par -Damien Couroussé du CEA Grenoble, consiste à modifier le programme de calcul aléatoirement... tout en donnant toujours la bonne -réponse. Exemple trivial : au lieu d'effectuer une multiplication par dix, le programme peut faire dix additions. *" Cette génération dynamique de code servait d'abord pour améliorer les performances de calcul mais on a réalisé qu'elle permettait aussi de lutter contre ces attaques visant à percer les secrets des puces "*, indique le chercheur, qui estime être dans une étape préindustrielle.

Son confrère Lilian Bossuet est encore plus proche de la commercialisation grâce à sa collaboration avec Algodone, qui fait suite au projet -Salware, financé notamment par l'Agence nationale de la recherche. *" Nous sommes les premiers à proposer pour le matériel ce qui existe déjà pour les logiciels, à savoir une licence d'exploitation. S'il ne dispose pas d'une clé, l'utilisateur ne peut se servir du circuit ainsi protégé "*, indique Lionel Torres, -cofondateur de cette société et professeur à l'université de Montpellier, qui travaille aussi avec -Intrinsic-ID. L'astuce consiste à ajouter avec parcimonie des portes logiques dans des -endroits-clés du circuit afin d'en bloquer le fonctionnement, et à le débloquer dès lors que la bonne série de chiffres est entrée dans le composant. Une approche parmi d'autres. Mais pour Mark -Tehranipoor, *" plus on avance, plus les contrefacteurs progressent. C'est une course sans fin "*.

David Larousserie

article précédent
Un psychiatre qui inverse les rôles...

article suivant
Quand le vide cosmique distord la lumière...