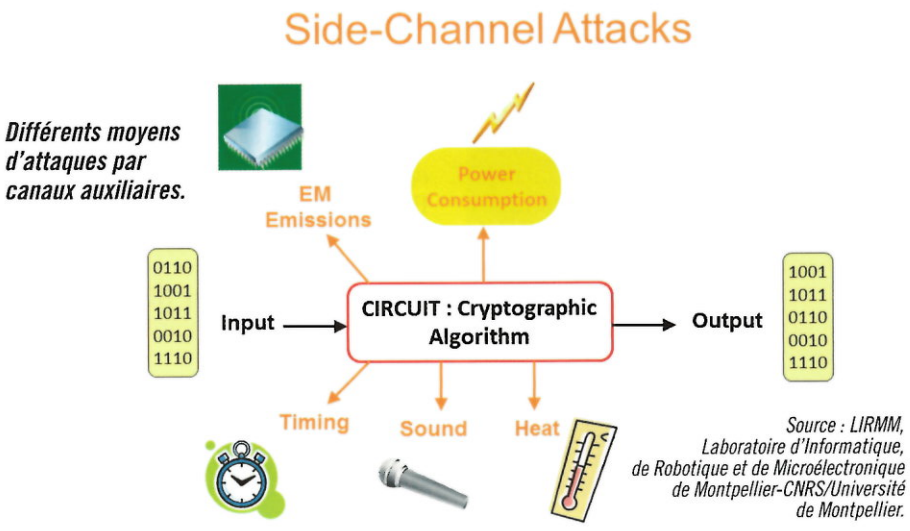
Les attaques par canaux auxiliaires : un danger encore méconnu

Les attaques par canaux auxiliaires (ou « side channel attacks » en anglais) sont des attaques très particulières, qui utilisent les propriétés physiques d'un composant ou d'un microprocesseur pendant le processus de chiffrement pour attaquer les clés servant à sécuriser la transmission de l'information… et s'en emparer. Encore peu connues, sauf dans le monde des cartes à puces, elles peuvent faire des ravages.

Commençons par le début, et par la définition d'une attaque par canaux auxiliaires, ou « side channel » en anglais. Ces attaques ont été tout d'abord connues dans le monde des composants et microprocesseurs embarqués. En effet, comme le définit Guillaume Duc, enseignant-chercheur à Télécom ParisTech, *« dans le domaine de la cryptographie, un algorithme s'exécute sur un support physique, un microprocesseur, la puce d'une carte de paiement, par exemple. Or, le composant qui effectue les calculs de chiffrement introduit des canaux d'entrée/sortie supplémentaires, les fameux canaux auxiliaires, liés à ses caractéristiques physiques »*, notamment lors de l'opération de chiffrement/déchiffrement de l'algorithme. Il est alors possible, selon Guillaume Duc, *« d'utiliser les propriétés physiques du composant pour dérober des informations sensibles »*. Expliquons-nous : lorsqu'un composant effectue des calculs, sa température, sa consommation électrique, le rayonnement électro-magnétique qu'il émet, le bruit qu'il produit etc... vont varier en fonction des données qu'il transmet ». Sans rentrer dans le détail d'équations trop compliquées, *« chaque variation sur ces canaux auxiliaires peut constituer une indication sur les informations qu'il manipule »*, précise Guillaume Duc. *« L'attaque par canal auxiliaire va constituer, via différents moyens, à* « espionner » ces canaux pour dérober de l'information sensible ». *« L'attaquant prend en compte des phénomènes physiques très simples liés aux propriétés du composant. En utilisant le fait que ces paramètres physiques dépendent de ce que le composant est en train de calculer, il est possible de retrouver la clé de chiffrement, et, ainsi, de dérober des informations précieuses »*, renchérit Louis Goubin, cryptologue de renom, professeur à l'université de Versailles-Saint-Quentin en Yvelines. Dans certains cas, l'attaquant se contente d'observer les propriétés physiques du composant, et de les capter. On parle alors d'attaques « passives ». Dans d'autres cas, l'attaquant utilise du matériel (rayon laser, sonde, introduction volontaire d'erreurs pour provoquer certains comportements révélateurs du composant), pour s'emparer de l'information lors du calcul. On parle alors d'attaques «actives».

> "Utiliser les propriétés physiques du composant pour dérober des informations sensibles."
>
> **Guillaume Duc,** *enseignant-chercheur à Télécom ParisTech.*



Différents moyens d'attaques par canaux auxiliaires.

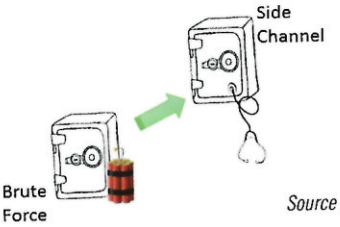
Source : LIRMM, Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier-CNRS/Université de Montpellier.

Des attaques connues dès le milieu des années 1990

Ces attaques, qui sont longtemps restées confinées dans les laboratoires

Side-Channel Attacks

- Basées sur l'information récupérée sur l'implantation physique du crypto-système
  - Information temporelle
  - Consommation électrique
  - Emanation électromagnétique
  - Son
  - Lumière
  - ...



Source : LIRMM.

Différence entre une attaque de force brute et une attaque par canaux auxiliaires.

de recherche, ont été connues dès le milieu des années 1990. Le chercheur Paul Kocher en a parlé dans un article novateur dès 1996. Dans la même veine, le cryptologue français Serge Vaudenay a mené une attaque via le temps de réponse sur le protocole SSL/TLS (SSL/TLS est un protocole ayant pour but de créer un canal de communication authentifié, protégé en confidentialité et en intégrité),ce qui a conduit les concepteurs du standard à faire une mise à jour critique.

Une autre attaque temporelle a été menée dans le cadre d'une implémentation AES (AES pour Advanced Encryption Standard -soit *« standard de chiffrement avancé »* en français), variante de Rijndael, algorithme de chiffrement symétrique le plus utilisé actuellement, sur le cache d'un processeur.

Enfin, le mathématicien et cryptologue israëlien Adi Shamir a montré l'efficacité de la cryptanalyse acoustique du bruit d'un processeur lorsqu'il calcule. En effet, les condensateurs d'un composant qui chargent et se déchargent émettent un « claquement » aisément mesurable.

La carte à puce très attaquée

« En ce qui concerne les supports, précise Louis Goubin, *le circuit le plus attaqué reste encore celui de la carte à puce »*. Aucune statistique ne fuite sur ce domaine sensible, mais on peut aisément comprendre les proportions d'une telle attaque dans un secteur aussi stratégique que la fabrication de cartes à puces. En pratique, les cartes bancaires, les cartes SIM des opérateurs télécom, les cartes d'abonnement pour les chaînes de télévision cryptées font partie des supports visés par ce type d'attaques. Notamment les cartes d'abonnement des télévisions cryptées pour lesquelles le trafic s'avèrerait particulièrement lucratif.

Parmi les types d'attaques citées, la plus utilisée, selon Louis Goubin *« est celle qui utilise la consommation électrique, même si elle reste difficile à effectuer, surtout pour les gros circuits, car, quand on mesure la consommation du circuit, la consommation de toute la puce est mesurée. « Toutes les parties du circuit ne manipulant pas l'information sensible visée vont donc introduire du bruit parasite dans les mesures »*, souligne de son côté Guillaume Duc. A l'en croire, l'attaque par le temps de calcul *« n'est pas, en général, très utilisée ». « L'attaque par la mesure de la variation du rayonnement électromagnétique est plus intéressante, car plus précise »* poursuit Guillaume Duc. *« Elle nécessite une antenne adéquate, qui cible précisément la zone du circuit qui manipule le secret »*. En laboratoire, les techniques d'attaques les plus fréquemment utilisées sont l'attaque via le temps de calcul, et celle sur les variations du rayonnement électromagnétique.

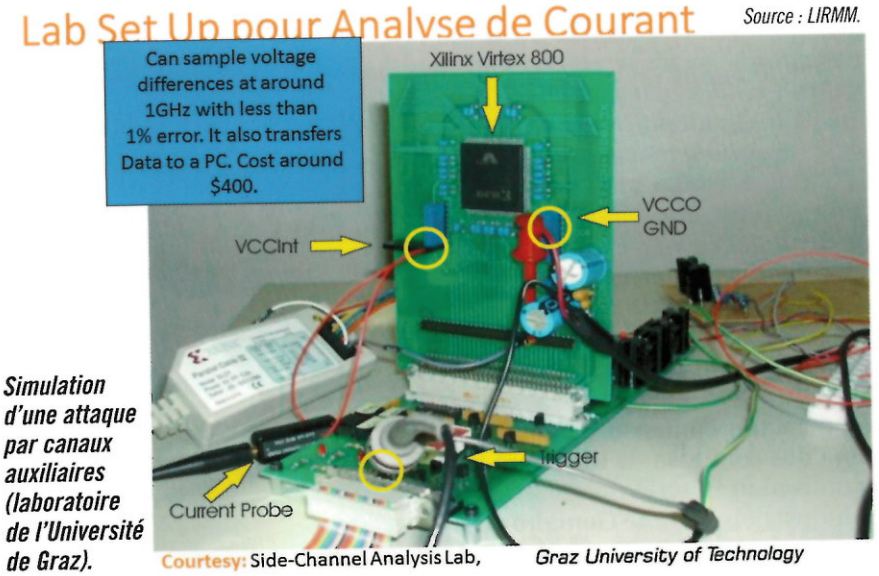
Quelques semaines pour arriver à des résultats probants

Parlons laboratoires, justement : ce type d'attaques ne s'improvise pas. Comme le précise Louis Goubin, *« ces attaques sont tout de même assez complexes à mettre en œuvre : il faut d'abord du matériel un peu sophistiqué ; mesurer la variation du courant électrique nécessite déjà de posséder un oscilloscope perfectionné, qui coûte plusieurs milliers d'euros. Ensuite, ce type d'attaques prend du temps, il faut quelques semaines pour arriver à des résultats probants »*.

Savoir mener ce type d'attaques n'est pas non plus à la portée du premier « script kiddie » venu, comme le confirme Guillaume Duc. *« Les attaquants doivent trouver les bonnes compétences en traitement du signal, par exemple. Ce sont plutôt des profils de Bac + 3/Bac + 5, qui possèdent du matériel sophistiqué. Ce n'est pas à la portée de tout le monde ». « Tout ceci me fait penser que ces attaques sont plutôt l'œuvre de pirates organisés et de bandes mafieuses »*, conclut Louis Goubin. Elles ont le temps, le matériel, et l'argent pour recruter les compétences.

Les parades existent

Face à cela, bien évidemment, les parades existent, développées, et nous



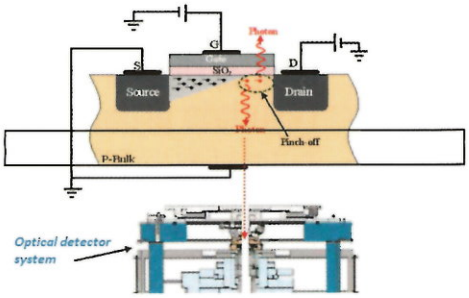
Source : LIRMM.

Simulation d'une attaque par canaux auxiliaires (laboratoire de l'Université de Graz).

Courtesy: Side-Channel Analysis Lab, *Graz University of Technology*

Attaques en Emission de lumière

Source : LIRMM.



allons le voir, dans les laboratoires des universités et des industriels de la carte à puce, comme Gemalto ou Oberthur Technologies. *« Face à ces attaques par canaux auxiliaires, la première technique consiste à s'assurer que le composant ne fait plus fuir d'informations du tout »* explique Guillaume Duc. *« Les parades physiques sont les plus évidentes à mettre en œuvre. Par exemple, on peut développer des solutions qui permettent au composant d'avoir toujours le même temps de calcul, ou bien de générer toujours la même consommation de courant quand il fonctionne. Mais cette dernière parade est compliquée à mettre en œuvre. De plus, il est très difficile d'équilibrer le rayonnement électromagnétique du composant ».*

« On peut aussi utiliser une deuxième technique qui consiste à « découper » *le secret en deux ou plusieurs éléments, de manière mathématique. Il sera ainsi plus difficile à obtenir car l'adversaire devra récupérer les différents morceaux du secret qui sont manipulés à des instants ou à des endroits du circuit différents. C'est ce que l'on appelle le masquage. »*

On peut enfin, et ce sont les dernières techniques utilisées, rendre l'attaque plus difficile, soit en rajoutant du « bruit » parasite, soit en enfermant le composant dans une sorte de cage de Faraday qui emprisonne l'émission de rayonnement électromagnétique. Cette dernière parade est efficace, mais très coûteuse, et rendrait le coût des composants impropre à son utilisation en série.

Les industriels comme Gemalto ou bien encore Oberthur Technologies travaillent depuis bien longtemps dans leurs laboratoires très protégés sur ces attaques identifiées et sur les contremesures qui permettent de les contrer, même s'ils sont peu enclins, et on les comprend, à livrer leurs secrets sur ce sujet éminemment sensible. Christophe Giraud, responsable du groupe Cryptographie & Sécurité chez Oberthur Technologies, précise juste que *« les attaques par canaux auxiliaires ont bien évidemment été identifiées depuis très longtemps. Nous avons nos propres laboratoires et nous travaillons aussi avec des laboratoires indépendants agréés par l'Anssi. Pas un produit ne sort de chez nous sans qu'il ait été protégé, audité et analysé pour être certain qu'il soit robuste face à ce type d'attaques ».*

> “Ces attaques sont plutôt l'œuvre de pirates organisés ou de bandes mafieuses.”
>
> **Louis Goubin**, *cryptologue de renom, professeur à l'université de Versailles-Saint-Quentin*

Les machines virtuelles peuvent aussi être attaquées

Mais, face au développement de cloud computing, d'autres types d'attaques par canaux auxiliaires peuvent apparaître sur les serveurs eux-mêmes, notamment dans les cas de transactions sécurisées (protocole HTTPS, standard de communication SSL/TLS). *« Le temps de réponse du serveur peut donner une information sur la clé utilisée par le serveur, précise Guillaume Duc. Par ailleurs récemment, on a pu mener des attaques par canaux auxiliaires sur des machines virtuelles utilisées dans le cloud computing : une application malicieuse s'exécutant sur une première machine virtuelle pouvant voler, en ciblant les variations de temps de calcul introduit par les caches des processeurs, des données manipulées par une seconde machine virtuelle tournant sur une même machine physique ».* La solution consiste alors à isoler la machine, et à ne pas exposer le système à des tiers. Dans le cas d'un cloud service provider, il faut qu'il propose une offre de machines dédiées à une certaine activité.

En conclusion, nous pouvons dire que les attaques par canaux auxiliaires, encore trop souvent ignorées, sauf dans le monde de la carte à puce, peuvent faire des ravages. C'est donc une erreur pour les industriels et les CSP de ne pas s'en préoccuper. ■

Sylvaine Luckx