

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'infailibilité 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 inexistant, 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



Dont Mias

fait, ils en définissent la classe: tous les mammifères présentent au moins quelques poils et la plupart en sont abondamment pourvus. Les poils sont de bons isolants thermiques et protègent le corps contre l'abrasion, l'humidité, les rayons du soleil, les parasites et les microbes pathogènes. Ils servent aussi de camouflage pour tromper les prédateurs, et les motifs de la fourrure permettent aux individus d'une même espèce de se reconnaître.

Les rôles de la fourrure

Qui plus est, les mammifères peuvent utiliser leur fourrure comme un signal social – un mode de communication non verbale – pour indiquer par exemple de l'agressivité ou de l'agitation. Quand un

chien hérisse ses poils, il indique à ceux qui le défient de ne pas s'approcher.

Cependant, même si la fourrure a plusieurs fonctions, quelques lignées de mammifères ont acquis au fil du temps une fourrure si clairsemée et aux poils si fins qu'elle n'a plus aucun rôle. La plupart de ces animaux vivent sous terre ou dans l'eau. Chez les mammifères souterrains, tel le rat-taube, l'apilosité – l'absence de poils – a évolué en réponse à la vie souterraine. Dans ce cas, les poils sont superflus, car les animaux ne se voient pas dans le noir, mais ils se blottissent les uns contre les autres pour se réchauffer.

Chez les mammifères marins qui ne s'aventurent jamais sur terre, telles les baleines, la peau lisse facilite la nage et la plongée, en diminuant les forces de

frottement de l'eau sur la peau. Pour compenser l'absence d'isolation thermique externe, ces animaux ont une couche de graisse sous la peau. En revanche, les animaux semi-aquatiques, par exemple les loutres, ont une fourrure dense étanche, qui emprisonne l'air pour permettre à l'animal de flotter plus facilement. Cette fourrure protège aussi la peau sur le sol.

Les plus grands mammifères terrestres, à savoir les éléphants, les rhinocéros et les hippopotames, ont également une peau nue, si bien qu'ils n'ont pas trop chaud. En effet, plus un animal est grand, plus sa surface corporelle est petite relativement à sa masse, et plus il a des difficultés à évacuer l'excès de chaleur interne. Au Pléistocène – il y a entre deux millions et 10 000 ans –, les mammoths et autres parents des éléphants et des rhinocéros avaient de la fourrure, ce qui leur permettait de vivre dans des environnements froids. Leur isolation externe les aidait à conserver la chaleur du corps et à réduire leurs besoins alimentaires.

Évacuer la chaleur grâce à une transpiration efficace

La peau quasi nue de l'homme n'est pas une adaptation à la vie souterraine ou aquatique, bien que certains pensent à tort que les ancêtres de l'homme soient passés par une phase aquatique au cours de leur évolution (voir l'encadré page 65). Elle n'est pas non plus le résultat d'une grande taille. La peau est devenue presque glabre parce que l'homme a acquis un système de régulation efficace de sa température corporelle. C'est en tout cas ce que suggère l'efficacité de la transpiration humaine.

Garder une température corporelle basse est difficile pour de nombreux mammifères, et pas seulement pour les plus grands d'entre eux, en particulier lorsqu'ils vivent dans des régions chaudes et produisent beaucoup de chaleur en marchant et en courant longtemps. Ces animaux doivent réguler leur température interne, leurs tissus et organes, notamment le cerveau, pouvant être endommagés par un excès de chaleur.

Les mammifères utilisent différentes tactiques pour diminuer leur température interne: les chiens halètent, plusieurs espèces de félins sont plus actives la nuit