Lorsque les claviers sont trop bavards

- Informatique - Hardware -

Date de mise en ligne : mardi 21 octobre 2008

Spyworld Actu

Le rayonnement électromagnétique d'un clavier peut « s'entendre » à plusieurs dizaines de mètres. C'est un fait connu de tous les opérateurs radio modernes, qui utilisent depuis belle lurette des récepteurs à traitement logiciel. C'est également un point technique connu des barbouzes les plus débutantes, car la récupération des données émises par le « scan code » de nos AZERTY est le B.A. BA de l'écoute Tempest, si souvent décrite dans les documents rédigés par la NSA notamment et republiés par le serveur Cryptome.

Mais ce n'est pas parce qu'une technique est ancienne qu'il faut pour autant l'oublier. C'est du moins ce que pensent certains chercheurs de la très sérieuse Ecole Polytechnique de Lausanne (EPFL), qui a légèrement amélioré les procédés connus et s'est lancé dans une étude comparative des claviers plus ou moins bien « blindés ». Démonstration accompagnée d'une double séquence vidéo montrant à quel point il est aisé de récupérer non seulement le couple « login/password » de son voisin, mais également peut-être le code PIN tapoté sur le pavé d'un distributeur de billets ou d'un TPV, terminal de payement mobile.

Peut-on résoudre rapidement cette faille de fabrication ? La réponse est « oui », c'est même à la portée d'un étudiant en première année d'électrotechnique. « A moindre frais ? » la chose est moins évidente. Pour blinder un boîtier en plastique -les claviers métalliques ont disparu de nos bureaux depuis bien longtemps-, il faudrait en recouvrir la surface intérieure d'une peinture conductrice, en fermer la surface supérieure -côté touches- par une mousse également conductrice, blinder et « shocker » à l'aide de câbles écrantés et de perles de ferrite les fils qui en sortent... autant de solutions simples mais qui ont un prix. Ce n'est donc pas un problème technique, car la littérature traitant de ce sujet abonde.

C'est avant tout une histoire de « centimes économisés » et d'économie d'échelle. Les claviers d'« entrée de gamme » ne dépassent pas 5 euros, ce qui laisse bien peu de marge pour des accessoires de sécurisation anti-rayonnement. Les plus perfectionnés, à près de 100 euros, ne sont que des usines à fonctions annexes, pour qui les normes Tempest n'existent pas. Quelques rares fabricants possèdent à leur catalogue des périphériques destinés aux marchés d'Etat et qui respectent strictement les normes en matière de compatibilité électromagnétique. Et dont le prix et l'esthétique n'ont rien à voir avec ce qui se pratique sur le marché grand-public.

Le spectre radiofréquence occupé par un ordinateur est, pour les hackers sérieux, un terrain de jeu inépuisable. Après les hacks WiFi, CPL ou Bluetooth, après l'écoute des « appels de courant » des processeurs dans le domaine du « timing attack », voilà que ressurgissent les écoutes Tempest des claviers. Viendront ensuite les variations de rayonnement des écrans cathodiques ou plats (très différents les uns des autres), les « fuites » par les câbles séries, parallèles et consorts, les échappées des liaisons UWB et « wireless USB », les espionnages du grattement des disques durs... tout s'écoute, tout se mesure. Même deux FPGA enfermés dans des enceintes en béton plombées sont susceptibles de laisser fuir des informations, comme cela a été démontré lors des dernières SSTIC de Rennes. Nihil novi sub sole, rien n'est plus bavard qu'un ordinateur, surtout si celui-ci est situé dans la proximité relative (entre 20 et 200 mètres) d'un récepteur numérique à décodage logiciel digne de ce nom.

Compromising Electromagnetic Emanations of Keyboards
envoyé par pace303

Compromising Electromagnetic Emanations of Keyboards
envoyé par pace303

Post-scriptum :

http://www.communautech.com/actuali...