Semaine du hack : et ils dégainent leur code encore fumant...

- Informatique - Sécurité Informatique -

Date de mise en ligne : dimanche 22 fÃ©vrier 2009

Spyworld Actu

Février, c'est le premier mois des « hacking conferences ». Avec la BlackHat de Washington, avec les comptes-rendus de la Schmoocon...un feu d'artifice de communications, d'exploits, de hacks, tous plus médiatisés les uns que les autres. Et çà commence très fort, avec cet exposé de Chris Paget lors de la Schmoocon, qui nous reparle du clonage des RFID... ceux des passeports, bien entendu. Mais cette fois-ci, il s'agit des passeports américains délivrés aux frontaliers qui, chaque jour, traversent l'une des frontières des Etats-Unis pour affaires : Canada, Iles Caraïbes et Bermudes ainsi que le Mexique.

Ce document de voyage un peu particulier se présente sous la forme d'une carte de crédit, et intègre un RFID fonctionnant sur 900 MHz. Une technologie probablement fort utile pour compter du bétail dans un champ, mais considérablement trop indiscrète pour être employée dans une chaine d'identification des personnes. Détectables et lisibles à plus d'un kilomètre de distance, pouvant être aisément perturbés et très probablement piratés lors de l'échange des données entre la carte elle-même et le système d'interrogation légitime, ces RFID ont, malgré de nombreux avis défavorables, été manifestement adoptés par les instances gouvernementales américaines. Au grand bonheur de Paget.

Côté Black Hat, les codes les plus protégés explosent de toutes parts. Joanna Rutkowska et Rafal Wojtczuk signalent l'existence de plusieurs bugs dans le Software Manager Management Mode des processeurs Intel, rééditant l'exploit de l'an passé. Car déjà, un problème du SMM avait permis à ce couple de chercheurs de compromettre un hyperviseur Xen, démonstration faite précisément lors d'une Black Hat. Cette fois, c'est la TXT, Trusted Execution Technology d'Intel qui est mise à mal par cette petite erreur de conception. Selon les chercheurs, il serait possible d'utiliser plus d'une quarantaine de moyens pour exploiter ce défaut capable de compromettre le processus de boot « sécurisé » de la machine. Or, TXT exécute le lancement d'un noyau ou d'un hyperviseur en partant du principe qu'il peut compter sur l'intégrité de ce fameux SMM... Security News précise que, tant que le constructeur n'aura pas corrigé les erreurs en question, l'équipe d'Invisible things ne divulguera aucun détail technique concret.

Toujours de la Black Hat, le contournement de SSL par Moxie Marlinspike. Le Reg étale les exploits de ce hacker sur deux pages, qui s'achèvent avec un témoignage d'admiration de la part de Dan Kaminsky, qui lui aussi mis à mal SSL (ou plus exactement une édition particulière de SSL). Dans les grandes lignes, il semblerait que ce hack consiste, à l'aide d'un utilitaire baptisé SSLstrip, à détourner l'internaute victime dès qu'il a reçu la page Web précédant celle qui devrait logiquement activer la liaison sécurisée. Ce n'est pas SSL qui est compromis, mais sa mise en oeuvre. Bien sûr, la page injectée par le pirate ayant effectué le détournement devra présenter les mêmes aspects que celle à laquelle s'attend l'internaute, quitte même à afficher une url au format HTTPS à l'aide d'un certificat bidon qui, de toute manière, n'est vérifié par personne. Mise en confiance par les pages Web précédentes, la victime n'aura alors aucun doute quant à l'authenticité des écrans suivants, et fournira sans la moindre hésitation tous les mots de passe possible. Relatant ce même hack, nos confrères de Security News rapportent cette remarque de Marlinspike « Si vous obtenez le mot de passe d'un site, vous avez de fortes chance que ce même mot de passe soit utilisé également sur dix autres sites ». Un tel piège tendu sur un vague blog sans grand intérêt peut devenir une source d'alimentation d'identités et de crédences également utilisables sur des sites bancaires ou de payement en ligne.

Achevons ce rapide tour de la BH Washington en mentionnant cet article d'Information Week sur le hack des systèmes de reconnaissance faciale intégré dans certains ordinateurs Lenovo, Asus ou Toshiba. L'affaire n'est pas nouvelle et avait déjà fait l'objet d'une communication et de plusieurs vidéos de démonstration de la part de l'équipe de Nguyen Minh Duc du BKIS (Bach Khoa Internetwork Security Center) d'Hanoi. Cnis avait publié un article à ce sujet en décembre dernier.

Post-scriptum :

http://www.cnis-mag.com/fr/semaine-...