Contrôle continu écrit numéro 1 de sécurité informatique

M1 d'informatique

25 mars 2011 – durée : 2 heures

Les notes de cours sur papier sont autorisées. Les machines sont interdites.

Cryptographie à clés secrètes (5 points)

1. (1 point) Le chiffre de Vigenère est-il une substitution mono-alphabétique, une substitution poly-alphabétique ou une transposition ? Dites pourquoi.
2. (2 points) Quel est le seul exemple de chiffrement par substitution de polygrammes que nous avons étudié dans ce cours ? Donnez la suite m de lettres obtenue en cryptant le nom de ce chiffrement au moyen de la technique de César avec un décalage de 4.
3. (2 points) Déchiffrez le message suivant, sachant qu'il a été calculé au moyen du chiffre de Vigenère avec la clé m de la question précédente : smrzpd.

Cryptographie à clés publiques (5 points)

1. (2 points) On considère le chiffrement RSA. On choisit $p = 7$ et $q = 13$. Combien vaut n ? Combien vaut z ? On choisit $e = 5$: est-ce correct et pourquoi ? Donnez une valeur correcte pour d. Cryptez le message $M = 2$.
2. (3 points) Expliquer comment la cryptographie à clés publiques permet de réaliser les objectifs suivants lors de l'échange d'un message : confidentialité, intégrité, authentification de l'expéditeur et du destinataire, non-répudiation de l'expéditeur.

Pirates et techniques d'attaque (5 points)

Quelles sont les catégories de pirate, de hacker et de technique d'attaque que vous reconnaissez dans le scénario suivant ?

Monsieur X est un écologiste convaincu qui milite activement au sein d'un groupe tentaculaire de passionnés. C'est également un hacker de premier ordre. Son groupe lui confie la mission de collecter des informations importantes enregistrées sur un serveur hautement sécurisé, propriété d'une grosse entreprise. Monsieur X commence par se renseigner sur le service informatique de l'entreprise en se glissant discrètement dans les poubelles stockant toute la paperasse jetée par les employés. Il récolte ainsi le nom de plusieurs personnes clés. Pendant un week-end, il se rend au service informatique de l'entreprise en se faisant passer pour un employé d'une boîte de maintenance s'occupant habituellement des machines. Il prétend être envoyé par un responsable dont il a trouvé le nom dans la poubelle et parvient à accéder physiquement au serveur. Grâce à des logiciels pointus qu'il a programmés lui-même, monsieur X parvient à récupérer les informations nécessaires à son groupe. Monsieur Y fait également partie du groupe de monsieur X ; consultant en sécurité informatique auprès de plusieurs grosses entreprises, monsieur Y s'adonne parfois à des pratiques plus douteuses : il lui arrive d'utiliser des informations confidentielles que lui fournit son activité professionnelle pour fabriquer des logiciels d'intrusion qu'il vend sur Internet à des personnes comme monsieur Z, ignare en informatique, qui cherche des programmes automatiques (dont il ne comprend rien au fonctionnement) pour attaquer diverses cibles.

Malwares (5 points)

1. (0.5 point) Donnez le nom de deux malwares sévissant actuellement, ou ayant sévi dans le passé. Donnez le type (virus, ...) de chacun de ces malwares.
2. À quel type de malware (virus, ...) a t-on affaire dans chacun des scénarios suivants ?
   (a) (1.5 point) Monsieur X reçoit un courrier électronique comportant une pièce jointe dont le nom se termine par `.txt`. Il ouvre la pièce jointe pour tenter de lire ce qu'il croit être du texte. Il s'agit en fait d'un fichier exécutable dont le code explore la liste des contacts de monsieur X et envoie à tous ces contacts un courrier électronique contenant la pièce jointe malicieuse, assurant ainsi sa reproduction.
   (b) (1.5 point) Monsieur X télécharge un programme qu'il a trouvé sur Internet et l'exécute sur son ordinateur. Tout semble se dérouler correctement, mais monsieur X est loin de se douter qu'en lançant ce programme, il a activé un petit bout de code, qui en a profité pour introduire une porte dérobée dans son ordinateur. Quelques jours plus tard, un pirate informatique se connecte à distance à l'ordinateur de monsieur X en utilisant la porte dérobée. En fouillant dans le disque dur de la machine, le pirate retrouve des informations sur la carte de crédit de monsieur X et s'en sert pour effectuer des achats sur Internet.
   (c) (1.5 point) Monsieur X télécharge un programme qu'il a trouvé sur Internet et l'exécute sur son ordinateur. Tout semble se dérouler correctement, mais monsieur X est loin de se douter qu'en lançant ce programme, il a activé un petit bout de code, qui en a profité pour se dupliquer dans tous les fichiers exécutables qui tournent au même moment. Les jours suivants, monsieur X lance quelques-uns des exécutables modifiés de cette façon ; à chaque fois, le bout de code supplémentaire va se dupliquer dans les exécutables qui tournent au même moment. Monsieur X ne se rend compte de rien, jusqu'au 26 avril (date anniversaire de la catastrophe de Tchernobyl) où tous les exécutables modifiés qui tournent alors écrasent avec des données aléatoires le premier mégaoctet de chaque disque dur (le MBR) connecté à sa machine.