Année 2013-2014 — 1ère session

IPB
ENSEIRB MATMECA
BORDEAUX

Sécurité des Systèmes d'Information
IT 218
Paul Dorbec

Filière : Informatique — Année : 2ième — Semestre : S4

Date de l'examen : 19 mai 2014 — Durée de l'examen : 1h30

Documents autorisés ☒ sans document ☐
Calculatrice autorisée ☐ non autorisée ☒

Autre : Le sujet comporte 2 pages. Il est composé de 3 exercices indépendants, qui peuvent être traités dans un ordre quelconque, et dont les questions sont plus ou moins indépendantes. Le barème est donné à titre indicatif.

SUJET

1 Quelques questions d'échauffement

Question 1.1 (2pt)
Pourquoi peut-il être utile d'introduire de la redondance dans un message?

Question 1.2 (2pt)
À quoi peut servir la traduction d'adresses en terme de sécurité?

Question 1.3 (2pt)
Quelle est la différence entre un système de droits de fichiers obligatoire et un système discrétionnaire?

2 The Onion Router

TOR (The onion router) est un réseau d'anonymisation des communications internet.

Question 2.1 (2pt)
Expliquez en quoi Internet n'est pas anonyme par défaut.

Question 2.2 (2pt)
D'une part, les états hésitent à interdire les réseaux anonymes tels que TOR, d'autres part, ce sont des organes étatiques (notamment américains) qui en sont le principal sponsor, et de fréquents utilisateurs. Expliquez.

TOR utilise le protocole suivant (ici simplifié):

1. L'émetteur S utilise une liste de nœuds connus du réseau et choisit un itinéraire: disons $S \to A \to B \to C \to D$, où S et D sont respectivement la source et la destination.
2. S envoie une première demande de connexion au nœud A, contenant la demande et un numéro de connexion N_1, encryptées par la clé publique de A. S et A établissent une connexion identifiée par N_1, et définissent un chiffrement symétrique (K_{SA}) pour la suite de la communication.

3. Puis S demande à A de transmettre une demande de connexion avec B. A transmet donc à B une demande de connexion chiffrée par la clé publique de B, avec en clair un nouveau numéro arbitraire de connexion N_2, qui sera l'identifiant de la connexion. B répond à A les informations nécessaire pour convenir d'un chiffrement symétrique que A transfère à S. Le protocole utilisé (Diffie-Hellman) ne permet pas à A de connaître la clé même s'il voit l'échange de paquet en clair.

4. À partir de ce point, A transfère tous les messages reçus de S avec le numéro N_1 vers B après les avoir déchiffré. Il transmet à S tous les messages reçus avec l'identifiant N_2

5. De la même façon, une clé est choisie entre S et C, puis entre S et D. Les paquets transitent de S vers D chiffré au départ quatre fois, chaque nœud retirant une couche de chiffrement à son tour, d'où le nom du protocole.

Question 2.3 (2pt)
Expliquez pourquoi aucun des nœuds internes du réseau (ici A,B et C) ne sait que S est la source et que D est la destination.

Question 2.4 (2pt)
Expliquez les choix des systèmes de chiffrement (symétrique ou à clé publique) dans le protocole.

Question 2.5 (2pt)
Expliquez pourquoi les numéros de connexions changent ($N_1 \neq N_2$).

Il existe une attaque par canal caché sur le protocole. En effet, sur le site de TOR, il est écrit:

> "Tor does not provide protection against end-to-end timing attacks: If your attacker can watch the traffic coming out of your computer, and also the traffic arriving at your chosen destination, he can use statistical analysis to discover that they are part of the same circuit."

Question 2.6 (2pt)
Expliquez comment, si un utilisateur vous contacte via TOR et si vous avez la possibilité d'écouter le trafic sur une bonne part du réseau dont votre interlocuteur, il est possible d'identifier celui-ci en utilisant le "timing" des communications, en particulier la fréquence de transmission de paquets.

3 Securité et confidentialité

Question 3.1 (2pt)
Google a un outil de retrait automatique d'applications[1] *des téléphones utilisant son système Android. Qu'en pensez vous?*

[1] Après l'examen, vous pouvez jeter un oeil à http://android-developers.blogspot.fr/2010/06/exercising-our-remote-application.html