2ème année 2005-2006

L'insécurité de la pile IP

Janvier 2006

Objectifs :
- mieux comprendre TCP ;
- comprendre les mécanismes de la pile IP au travers de leurs faiblesses.

▷ **Exercice 1 : Etude simplifiée des performances de TCP**

Le but de cet exercice est d'évaluer simplement les performances du protocole TCP. Nous nous contenterons d'évaluer ces performances lors du fonctionnement nominal (c'est-à-dire après la phase de slow start) de TCP Reno face à des pertes rares et isolées.

Nous ferons plus précisément les hypothèses simplificatrices suivantes :
- *la taille de fenêtre imposée par le contrôle de flux est toujours supérieure à celle imposée par le contrôle de congestion ;*
- *si p est la probabilité de perte d'un paquet, nous supposerons que ces pertes apparaissent périodiquement, c'est-à-dire que $p-1$ segments arrivent sans erreurs, puis le segment suivant est perdu, etc ;*
- *nous supposerons que le temps d'aller-retour rtt est constant ainsi que la taille d'un segment, égal à mss ;*
- *le temps d'émission d'un segment est négligeable devant rtt.*

***1.1** - Soit w la taille de la fenêtre d'émission juste avant la détection de la première perte. Quelle valeur prend $cwnd$ juste après ? Quel mécanisme entre alors en œuvre ?*

***1.2** - Comment évolue alors la valeur de $cwnd$ à partir de cet instant ? Combien de temps faudra-t-il, avec une telle évolution, pour atteindre à nouveau la valeur w ?*

***1.3** - Supposons qu'à cet instant une nouvelle perte soit détectée, et que ce schéma se reproduise périodiquement et "indéfiniment". Représenter graphiquement l'évolution de $cwnd$ au cours du temps. On prendra rtt comme unité de temps.*

***1.4** - Quel est le volume de données, exprimé en octets, émis lors d'une période du schéma périodique précédent ?*

***1.5** - Quelle relation unit la durée de la période et la probabilité de perte p ? En déduire une expression de w en fonction de p.*

***1.6** - Donner alors le débit nominal d'une connexion TCP utilisant des segments de taille mss constante au travers d'un lien caractérisé par un temps d'aller-retour de rtt et une probabilité de perte p.*

■

▷ **Exercice 2 : États de TCP**

Reprendre l'ensemble des chronogrammes d'établissement et de terminaison de connexion TCP en y faisant apparaître les états de la machine TCP ainsi que les événements responsables et/ou conséquents des changements d'état. ■

▷ **Exercice 3 : Problèmes de sécurité de la pile** IP

Le but de cet exercice est d'observer quelques problèmes de sécurité posés par la pile IP[1].

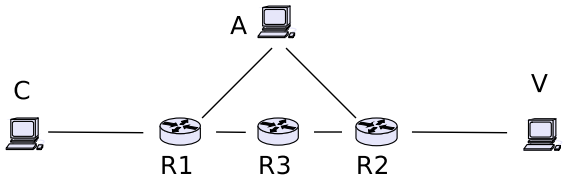

FIG. 1 – Configuration du réseau.

Les exemples que nous allons étudier impliquent les équipements de la figure 1 :

V *est la victime des attaques ;*

A *est l'attaquant ;*

C *est une machine en laquelle V fait confiance ;*

R1, R2 *sont des routeurs s'échangeant des informations par le protocole* RIP.

La troisième affirmation signifie en particulier qu'un utilisateur identifié sur la machine C pourra accéder par le réseau aux ressources de la machine V sans que celle-ci lui demande de s'authentifier à nouveau. Le fait que les paquets proviennent de la machine C lui suffit comme garantie. L'utilisateur peut alors par exemple lancer des commandes, modifier ou effacer des fichiers . . .

Nous supposerons que l'individu perpétrant ces attaques dispose de tous les pouvoirs sur la machine A. Il est en particulier capable de définir à sa guise tous les champs des paquets IP *qu'il émet.*

3.1 - **Le routage par la source.** *Le routage par la source permet à l'émetteur d'un paquet* IP *de choisir la route par laquelle ce paquet cheminera jusqu'à sa destination. Lorsque cette option est utilisée par un client* TCP*, le serveur l'utilise également (avec le chemin inverse, bien sûr).*

Expliquer simplement comment, grâce au routage par la source, A peut simplement accéder aux ressources de V.
Sauf mention contraire, nous supposerons donc maintenant que le routage par la source est désactivé sur les routeurs et V.

3.2 - **Routage par** RIP**.** *Montrer alors comment, grâce à un protocole de routage comme* RIP*, A peut encore accéder aux ressources de V.*

Montrer de plus comment, si le routage par la source est encore activé, A peut également observer tout le trafic échangé entre C et V.

3.3 - **Déni de service.** *Lorsqu'elle reçoit un segment* TCP `syn`*, une machine doit allouer des ressources. A quoi servent ces ressources ?*

Expliquer comment ce mécanisme peut être exploité simplement pour compromettre le fonctionnement d'une machine (la rendant éventuellement inopérante).

3.4 - **L'**ISN **de** TCP**.** *Supposons que A ait rendu la machine C inopérante par une attaque de type "déni de service", et soit capable de prédire les* ISN *utilisés par V.*

Expliquer comment A peut modifier des ressources de V (par exemple effacer un fichier).

■

[1] Les failles étudiées ici sont connues depuis longtemps et des contre-mesures efficaces y ont été apportées.