Examen “Sécurité et vie Privée dans les réseaux” CERI 14 mars 2014

Question 1 - P2P (10 minutes)

Démontrez l’intérêt d’utiliser un système P2P pour faire de la réplication de contenu à très grande échelle. Pour cela, pensez à expliquer la relation entre le temps et la capacité de service des réseaux P2P. De plus indiquez au bout de combien de temps *n* clients auront pu downloader le contenu. Comparez ces résultats avec le modèle classique client-serveur pour *k* serveurs et *n* clients.

Question 2 - Vie privée (15 minutes)

Vous devez transporter un message ultra secret et voulez être certain que personne ne pourra l’intercepter. Pour cela, vous allez impliquer 6 personnes dans le transport de l’information. Vous savez que ces personnes ne seront jamais plus de 3 dans la même pièce. Encodez votre secret de sorte que ces personnes ne puissent jamais retrouver le message lorsqu’elles se rencontrent. Pour vous aidez à réaliser cela, utilisez un schéma de Shamir (*k*, *n*). Choisissez *k* et *n* de manière intelligente (c’est-à-dire que les individus n’arriveront jamais à décoder le message et que vous minimisez le nombre de calculs que vous devez faire).

Le message est *D = 2014*, construisez *n* encodages pour le *n* que vous avez choisi. Ensuite montrez que vous ne savez pas retrouver *D* en utilisant *k-1* valeurs encodées puis montrez que vous obtenez *D* dès lors que vous avez au moins *k* encodages.

Question 3 - Réseaux (15 minutes)

Lors du TP, vous avez réalisé une attaque de type “cache poisoning ARP”. Expliquez le principe de cette attaque et les types de “security threats” que vous pouvez réaliser avec cette attaque. Comment pouvez-vous protéger votre réseau de telles attaques *1)* sans changer le protocole ARP *2)* en changeant le protocole ARP.

Question 4 - Imagination (20 minutes)

L’objectif du protocole LISP (*Locator/Identifier Separation Protocol*) est de séparer la notion de localisation topologique et d’identité. Pour ce faire, les routeurs se basent sur le principe d’association et d’encapsulation: lorsqu’un router reçoit un paquet, le routeur détermine où le paquet doit être envoyé (=localisateur) sur base de la destination du paquet (=identifiant). Il encapsule alors le paquet et l’envoie au routeur de destination qui, à son tour, décapsulera le paquet et le délivrera à sa destination finale.

Les routeurs apprennent les associations identifiant/localisateurs en utilisant un protocole similaire à DNS: pour connaitre les localisateurs d’un identifiant, le routeur envoie un Map-Request et reçoit en réponse un Map-Reply avec la liste des localisateur pour cette identifiant, le liens entre le Map-Request et le Map-Reply se faisant uniquement par le biais d’un nonce. En se basant sur ce protocole, construisez une attaque de type *déni de service*, une attaque de type *espionnage* (eavesdropping) et une attaque de type *intrusion*.