Protocoles réseaux : sécurité

30 octobre 2023

1. Politiques de sécurité (ce que/qui je veux empecher de faire quoi)
2. Modèle d'attaque (ce que l'attaquant a le droit de faire)

Propriétés de sécurité qui définissent les politiques de securité :

1. confidentialité
   (a) anonymat/"méta-données"
   (b)
2. authenticité
3. integrité
4. disponibilité, absence de déni. (par ex : un serveur doit être accessible)

Types d'authentifications:

1. chiffrage ad hoc, clé négociée, pas d'auth (pb de man in the middle)
2. TOFU "trust on first use", leap of faith
3. authentification certifiée (mac)

1 SSL/TLS et https

HTTP: pas de mécanisme de sécurité →

- SSL→ auth, chiffrage

HTTPS: HTTP+auth(du serveur)+confidentialité.

2 Pas de couche de convergence

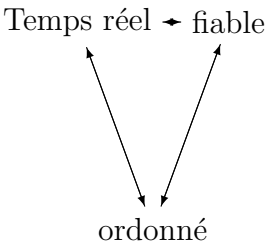
Avant : Seulement IP, en vrai : couche 2/3/4, 802.2/IP/TCP/TLS/HTTP.
Si on choisit http comme couche de convergence :

- Beaucoup d'overhead (headers ?)
- pas de temps reel
- pas de pair à pair

Temps réel $< 50ms$:

- audio $\subseteq$ vidéoconférence
- jeux en ligne
- broadcasting (foot)
- VR

Triangle de Chrobozsceck(massacre):



Remarque 1. *Autres protocoles:*

1. *SCTP*
   (a) $\rightarrow$ *sémantique par messages*
   (b) $\rightarrow$ *partiellement ordonné: flots multiples*
   (c) $\rightarrow$ *fiable/non-fiable*
2. *DCCP*$\rightarrow$ *jamais vu*

Problème :

- *ne traverse pas les NAT*
- *sécurité ?*

Solution:

2.1 Protocoles basés sur UDP

On met UDP entre IP et transport et pour éviter que Le NAT regarde dans les paquets : On chiffre avant la couche transport. On obtient

1. IP→UDP→DTLS(Datagram TLS)→transport.

On peut maintenant utiliser:
→ SCTP over DTLS(pas à la mode).
→ QUICK

- →intégré avec TLS! (le handshake se fait en un seul RTT au lieu de deux)
- →Probleme, c'est a nouveau une sémantique par flots d'octets multiples(y'a aussi par message) (obligé d'avoir un buffer+pb de perte de paquets en plein milieu)(possible de faire plusieurs choses en meme temps)
- par message → non fiable/non ordonné, par flots → fiable, ordonné

Pas possible de faire du pair à pair: TLS! Les téléphones/particuliers ont des NAT, pas de certificats, juste une adresse ip.
→ Solution: UDP brut. Plusieurs pbs:

1. Problème du rendez-vous(général), comment on contacte qqun en UDP?
2. Problème de la traversée du NAT.
3. crypto: auth.

Trop difficile. A la place : **UDP+contrôle**, on ajoute un serveur qui controle

- Les rendez-vous(vie privée)
- Echanges cryptographique (voir tp7)
- Traversée de NAT (voir projet)

BitTorrent: Le fichier telechargé contient un hash qui permet l'authentification au serveur, pb, toutes les ips sont traquées.