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.