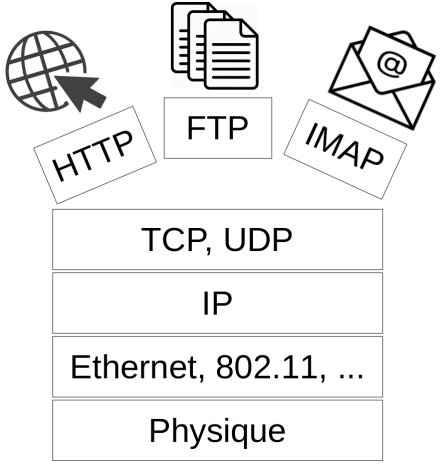
Sécurisation des protocoles

Introduction

Anaïs Gantet, Benoît Camredon
TLS-SEC 2018/2019

Pile protocolaire IP "classique"

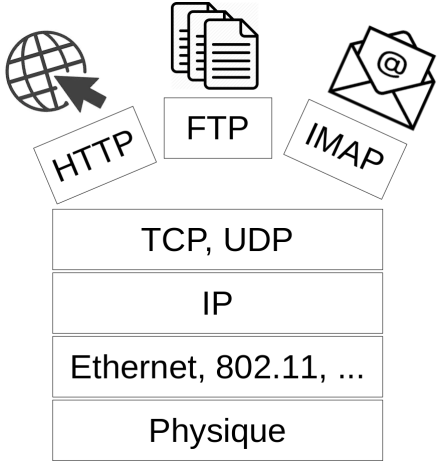
- Des protocoles de niveau 2
- Un protocole de résolution d'adresse (ARP)
- Un protocole réseau : IP
- Des protocoles transports : TCP, UDP
- Des protocoles applicatifs : HTTP, SMTP, FTP, IMAP, etc.



Pourquoi vouloir sécuriser les protocoles de communication ?

Pile protocolaire IP "classique"

- Des protocoles de niveau 2
- Un protocole de résolution d'adresse (ARP)
- Un protocole réseau : IP
- Des protocoles transports : TCP, UDP
- Des protocoles applicatifs : HTTP, SMTP, FTP, IMAP, etc.



Risques ?

- Ecoute de données en clair
- Usurpation d'identités
- Possibilité de modification de trafic (rejeu, modification du flux, etc.)
- etc.

Eléments de définition d'un protocole sécurisé

Ce que l'on souhaite assurer

- Confidentialité
- Authentification
- Intégrité
- Anti-rejeu
- Confidentialité persistente

La mauvaise solution de la "sécurité par l'obscurité"

- Quoi ? Sécurité fondée sur l'aspect propriétaire/secret du fonctionnement du protocole
- Problème : Risque de la rétro-ingénierie
- Conclusion : A éviter en pratique

Eléments de définition d'un protocole sécurisé

La mauvaise solution de la "sécurité par l'obscurité"

- Quoi ? Sécurité fondée sur l'aspect propriétaire/secret du fonctionnement du protocole
- Problème : Risque de la rétro-ingénierie
- Conclusion : A éviter en pratique

Outils cryptographiques à notre disposition

- Chiffrement symétrique
- Chiffrement asymétrique
- Fonctions de hachage
- Dérivation de clés

Protocoles sécurisés existants

Quelques exemples

- PGP, S/MIME, HTTPS, KERBEROS, SSH, SSL, TLS, EAP, IPSec, etc.

Plus en détails dans la suite de ce cours

- SSL/TLS (Transport layer security)
  - Chiffrement des données
  - Authentification par certificats
  - Intégrité des messages
  - Possibilité de confidentialité persistente
- SSH (Secure SHell)
  - Chiffrement des données
  - Authentification forte
  - Encapsulation d'autres flux
  - (Administration distante de machines)
- EAP (extended authentication protocol): Framework d'authentification
  - Utilisé pour contrôler l'accès à un médium
  - Authentification par mot de passe
  - Authentification par clé