Réseaux Avancés
L3 Informatique

Cours 1: Introduction

Osman SALEM
Maître de conférences
osman.salem@parisdescartes.fr

UNIVERSITÉ PARIS DESCARTES
UFR DE MATHÉMATIQUES ET INFORMATIQUE

Objectif de l'ECUE

- Renforcer vos connaissances en réseaux:
  - Réseaux Avancés: réseaux du semestre 5 + techniques avancées
  - Approfondir et compléter vos connaissances en réseaux:
    - Protocoles et services
    - Pas de retours sur ce que vous avez vu en réseaux (ARP, IP, adressage et subnetting)
    - Continuité et initiation à la configuration des équipements CISCO
  - Sécurité des réseaux
    - Vulnérabilités et attaques
    - Outils et systèmes cryptographiques: chiffrement symétrique
    - Protocoles de sécurité: SSL
  - Théorie de la file d'attente (Initiation)
    - M/M/1, M/M/1/K, M/M/C, M/M/C/K, M/M/∞

Organisation de l'enseignement

- Responsable: M. Osman SALEM
- 12 semaines avec :
  - 1h30 de cours (Jeudi de 10h15-11h45) : Amphi Fourier
  - 2h de TD/TP
    - 3 groupes
      - 1 groupe le Mercredi de 14h15 à 16h15 et 2 groupes le Vendredi matin
- Quelques site utiles…
  - Moodle de l'UFR Math-Info
    - http://moodle.univ-paris5.fr/
    - Inscrivez-vous pour recevoir des emails d'information
    - Support du cours/TD/information diverses

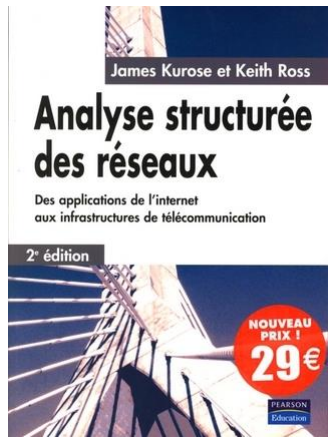
Planning 2018

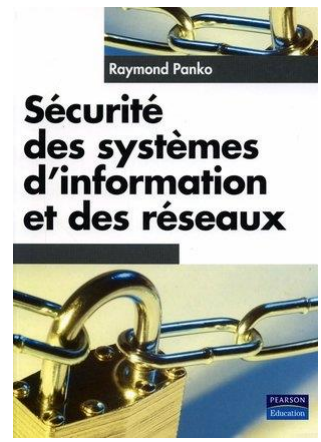
Semaine	Semaine	Cours	TD	commentaires
S1	25/01	1	1	
S2	01/02	2	2	
S3	08/02	3	3	
S4	15/02	4	4	
S5	22/02	5	5	
S6	08/03	6	6	
S7	15/03	***Partiel 1***	7	
S8	22/03	7	8	
S9	29/03	8	9	
S10	05/04	9	10	
S11	12/04	10	11	
S12	19/04	11	12	
S13	26/04		?	***Partiel 2 ?***

Evaluation

- Modalité de calcul de la note finale de l'U.E.
  - Contrôle Continu
    - Partiel 1
    - Partiel 2

Bibliographie





Plan

- 3 Parties
  - Sécurité
    - Chiffrement symétrique
  - Réseaux
    - Prise en main des outils de configuration
  - Performance
    - Théorie de la file d'attente

Plan

- Cours 1: Introduction à la sécurité
- Cours 2: Chiffrement symétrique: Scytale, Substitution, Transposition
- Cours 3: César, Vignère, Auto-Chiffrement, Playfair, Rail Fence
- Cours 4: Enigma, Stéganographie, Kerberos
- Cours 5: Initiation à la configuration des équipements CISCO
- Cours 6 : Configuration de Switch CISCO
- Cours 7: Configuration des Routeurs CISCO
- Cours 8: Configuration des protocoles de routage
- Cours 9: Théorie de la file d'attente : notation de Kendall
- Cours 10: Théorie de la file d'attente : M/M/1, M/M/1/K

Travaux dirigés et pratiques

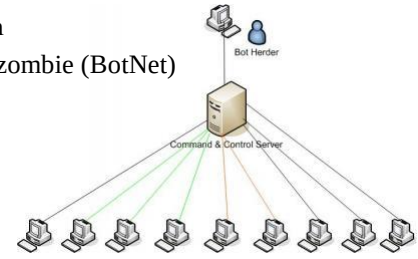
- TDs et TPs
  - Exercices et problèmes illustrant les concepts présentés en cours
    - Questions et rappel de cours
    - Tous les exercices proposés ne seront pas traités en TD
- Outils
  - Mot de passe en claire avec Telnet et FTP
  - Wireshark
  - Secure Shell: SSH, SCP et SFTP
  - CISCO Packettracer

Partie I: la sécurité des réseaux

Introduction

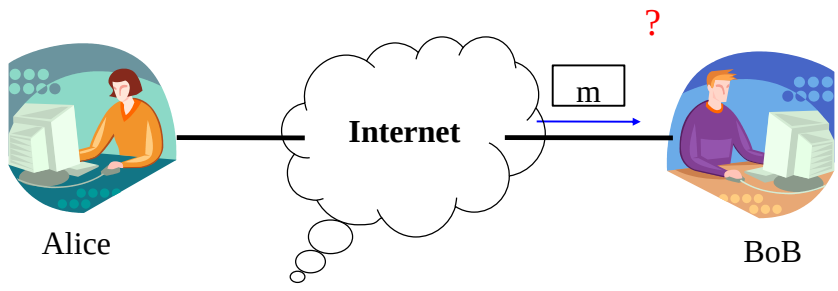
Logiciel malveillant

- Logiciel malveillant
  - Objectif: nuire au système
  - Virus, Vers, cheval de Troie
    - Virus: besoin d'une intervention humaine pour se propager
    - Vers: se reproduit en s'envoyant à travers un réseau
    - Cheval de Troie: installation d'une porte dérobée
  - Suppression des fichiers
  - Installation d'un logiciel espion
  - Transformer notre machine en zombie (BotNet)



Ce qui peut mal se passer…

- …quand l'ordinateur de BoB reçoit ou s'attend à recevoir un message ***m*** ?

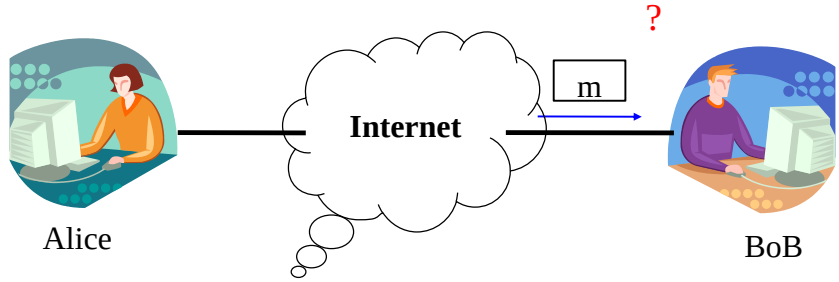


Qui sont Bob et Alice?

- … dans la vie réelle, qui sont Alice et Bob ?
- Navigateur/serveur web pour le commerce électronique (achat on-line)
- Banque on-line client/server
- Serveurs DNS
- Routeurs qui transmettent leurs tables de routage

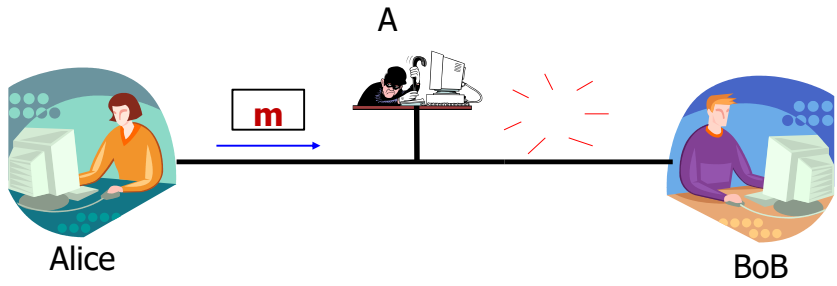
Ce qui peut mal se passer…

- …quand l'ordinateur de BoB reçoit ou s'attend à recevoir un message ***m*** ?



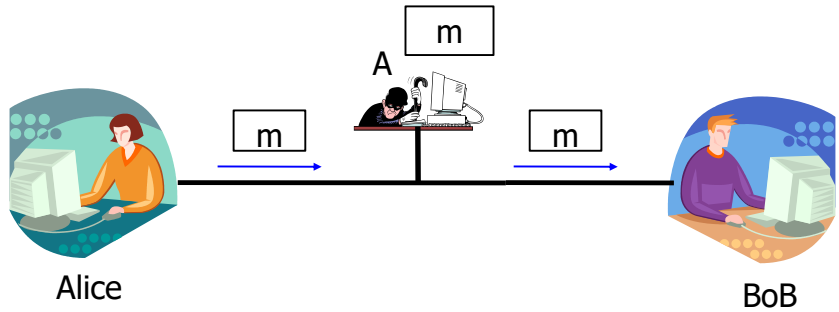
Une perte de message

- Un adversaire A a fait disparaître le message ***m*** au cours de la transmission



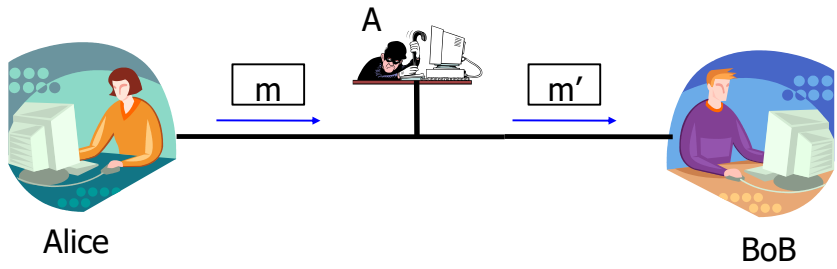
Une interception de message

- Un adversaire A a constitué une copie de ***m*** quand il est passé



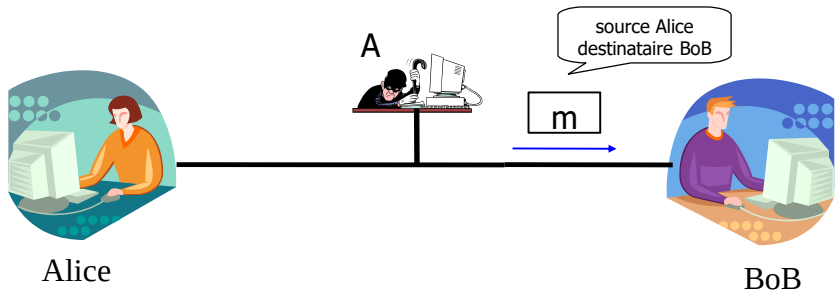
Une modification de message

- Un adversaire A a modifié le contenu du message ***m*** qui est devenu m'



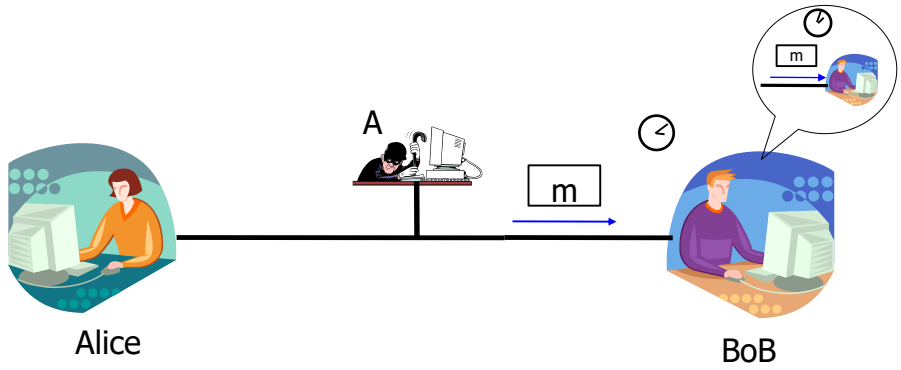
Une insertion de message

- Un adversaire A a fabriqué un message ***m***, en prétendant que c'est Alice qui en est l'émetteur (**usurpation d'identité**)



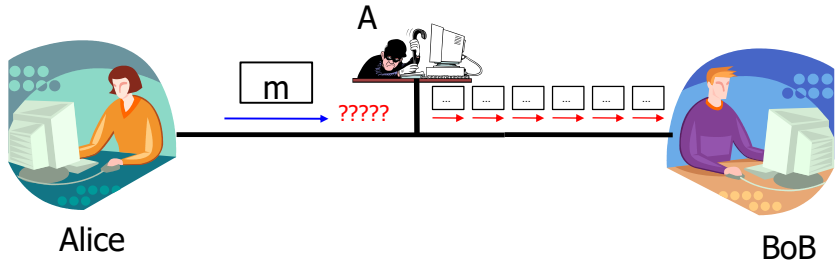
Une duplication de message

- Un adversaire A a envoyé de nouveau un message **m** qui avait été envoyé auparavant par Alice et reçu par BoB (“**rejeu**”)

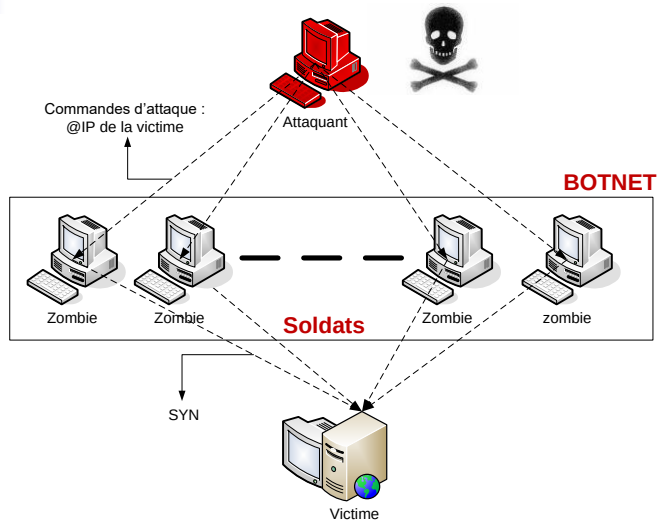


Un déni de service

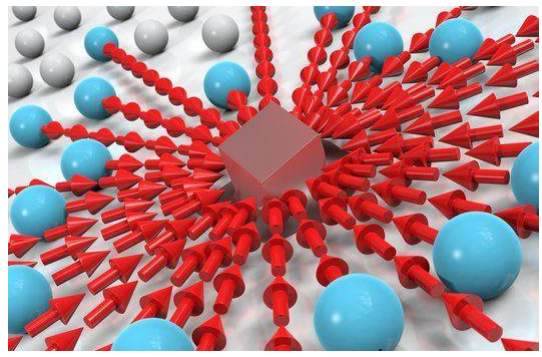
- Un adversaire A peut bloquer le message **m** en submergeant BoB de messages

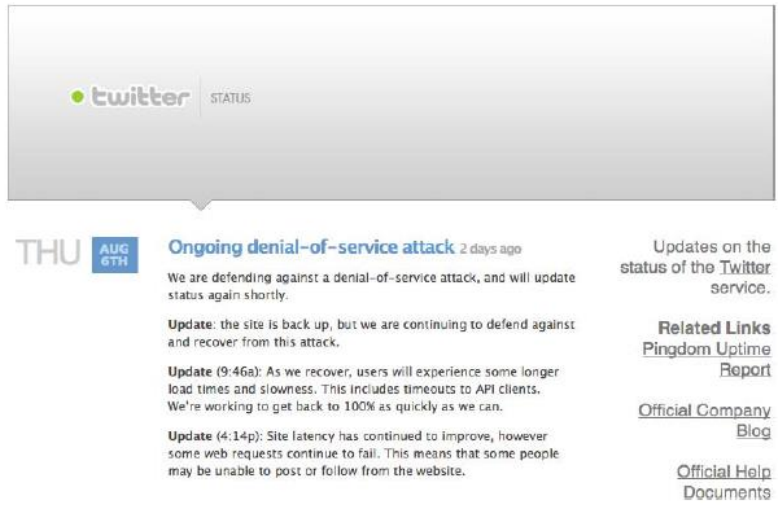


Les menaces de déni de service



Les menaces de déni de service





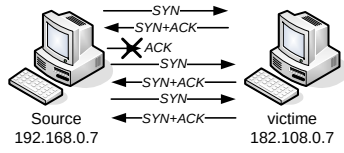
DDoS

- Distributed Denial of Service
  - Recently many servers were victims of DDoS

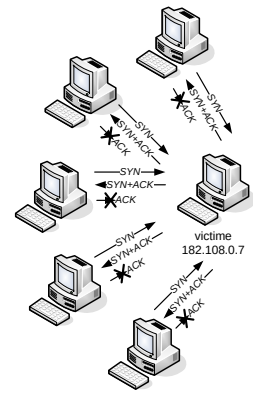
24

DoS, DDoS: SYN Flooding

- SYN FLOOD: inondation SYN
  - Un attaquant harcèle le serveur avec TCP SYN (demande d'ouverture d'une connexion)
  - Mais il ne répond pas au message final
  - TCP instaure une connexion semi-ouverte pour quelques minutes (~75s)
  - Les messages SYN peuvent engorger le module TCP



DoS



DDoS

Mnémonique

- Qu'est ce qu'un hacker ? Cracker ?
  - Un hacker est une personne qui veut comprendre les choses …
  - … Jusqu'à les moindre détails
  - Comment devenir un Hacker ?
  - Crackers: exploitation des connaissances avec des mauvaises intentions
- Qu'est ce qu'un script kiddie ?
  - Outils d'exploitation de vulnérabilités facile à utiliser
- Pourquoi les autres essaient d'accéder d'une façon illégale à notre système ?
  - Curiosité, revanche, extorsion de fond, terrorisme, vol de ressources, vandalisme, etc.

Les différents types d'attaques

- **Attaques passives**
  - Analyse de trafic
  - Interception de message
- **Attaques actives**
  - Perte de message
  - Modification de message
  - Insertion de message
  - rejeu
  - déni de service

Méthodes d'attaques

- Ecoute passives
  - Obtenir une copie de l'information sans autorisation
  - Login et Mot de Passe
- Usurpation d'identité
  - Transmission de messages avec autres identité
- Modification
  - Changement du contenu

Méthodes d'attaques

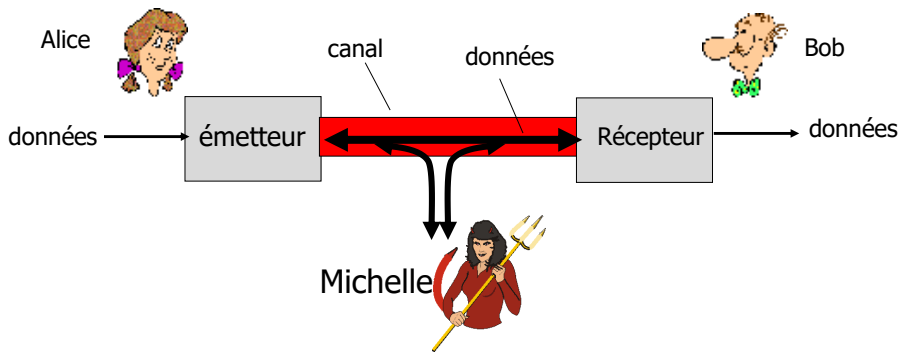
- Rejeu
  - Enregistrement du trafic et re-injection
  - Ex: retransmission du message de paiement
- Exploitation
  - Utilisation d'une vulnerabilité d'un logiciel pour obtenir un accès
- MITM: Man In The Middle
  - Interception de communications entre diffèrent partenaires

Les services de sécurité

- Confidentialité
- Intégrité
- Authentification
- Anti-rejeu
- Disponibilité
- Contrôle d'accès
- Non-répudiation
- Anonymat

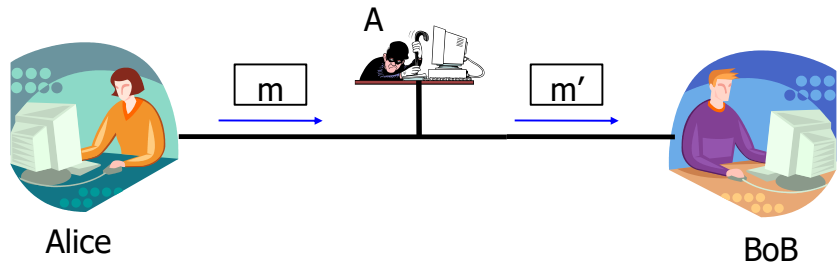
Confidentialité

- Seul le récepteur patenté du message peut lire le message, celui-ci reste secret (ou inexploitable) pour tous les autres utilisateurs
  - **Empêcher les utilisateurs malicieux de lire une information confidentielle**



Intégrité

- Quand le récepteur reçoit le message ***m***, il peut vérifier que celui-ci est intact, c'est-à-dire égal au message que l'émetteur a envoyé
  - **L'information n'est pas été altérée durant son transfert**
  - Objective: empêcher un modification par des utilisateurs malicieux



Authentification

- Quand le récepteur reçoit le message ***m***, il peut vérifier que c'est bien l'émetteur **Alice** qui l'a envoyé

  - La preuve s'appuie sur un *secret* que connaît l'utilisateur
    - Mot de passe
  - La preuve s'appuie sur un *objet* unique que possède l'utilisateur
  - La preuve s'appuie sur une caractéristique *physique* de l'utilisateur
    - Techniques biométriques
      - Empreintes digitale, rétine de l'œil, vocale
      - Forme du visage
      - Etc.
    - Pas très précis



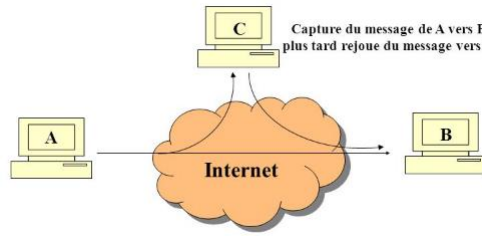







Anti-rejeu

- Quand le récepteur reçoit le message **m**, il peut vérifier si celui-ci est bien un nouveau message (le message **m** n'a pas déjà été émis et reçu...)



Disponibilité

- Propriété d'un système à être accessible et utilisable par tout utilisateur autorisé
  - Accessible lorsqu'un utilisateur autorisé en a besoin

Contrôle d'accès

- Mécanisme destiné à gérer les droits d'accès aux ressources et aux données
- Les utilisateurs ne peuvent accéder qu'aux ressources et données pour lesquels ils disposent spécifiquement des droits
- Les utilisateurs ne peuvent pas accéder aux ressources et données pour lesquels ils ne disposent pas des droits

Non-répudiation

- Quand le récepteur reçoit le message **m**, il peut être certain que l'émetteur du message a effectivement envoyé un message
- Le récepteur peut montrer la preuve à une tierce partie, preuve que l'émetteur ne peut pas nier
- Quand le récepteur reçoit le message **m**, l'émetteur du message peut être certain que m a été effectivement reçu
- L'émetteur peut montrer la preuve à une tierce partie, preuve que le récepteur ne peut pas nier

Anonymat

- L'identité de l'émetteur est cachée au récepteur
- Quand le récepteur reçoit le message **m**, il n'a aucune indication quant à l'émetteur du message
- Ex: Proxify.com