Rappel sur les vulnérabilités et leur exploitation

Matthieu Herrb

CNRS-LAAS

24 septembre 2007

Plan

Plan

Faute, erreur, défaillance

- **Faute :** défaut du système (vulnérabilité),
  par exemple un fragment de code qui copie de données vers un buffer sans contrôle de la taille.
- **Erreur :** se produit au moment ou la faute est «active».
  Les données d'entrée sont effectivement plus grosses que le buffer
- **Défaillance :** conséquence de l'erreur.
  plantage de ou pire, exécution de code malveillant.

Plan

Mauvaise configuration du système

- Paramétrage par défaut mal adapté
- Mots de passe faibles
- Logicels obsolètes non mis à jour
- Pas de sauvegardes
- Privilèges trop élevés ou droits d'accès trop laxistes
- Approbation de systèmes moins bien sécurisés
- Partage de privilèges par des services sans liens entre eux
- Pas de suivi de l'activité (logs) du systèmes

Fautes logicielles (bugs)

- Injection de code :
  - débordements mémoire (pile, tas)
  - chaînes de format
  - XSS (Cross-Site Sripting) injection de Javascript via une page web vulnérable
  - PHP, SQL, ... (tous les langages interprétés sont potentiellement vulnérables)
- Écrasement de données :
  - race conditions
  - expansion de chemins

Démo

Ingéniérie sociale

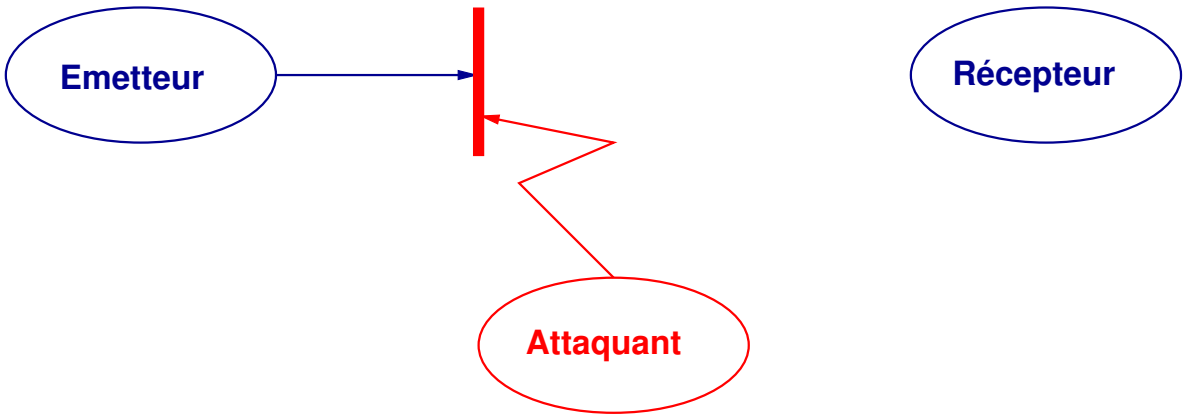
Pas besoin de vulnérabilité logicielle ou matérielle.

- Modèle du cliquodrome : toujours cliquer sur 'Suivant' et 'OK'
- Phishing
- Appât du gain, séduction, désirs...

Prise en défaut de la vigilance de l'utilisateur.

Plan

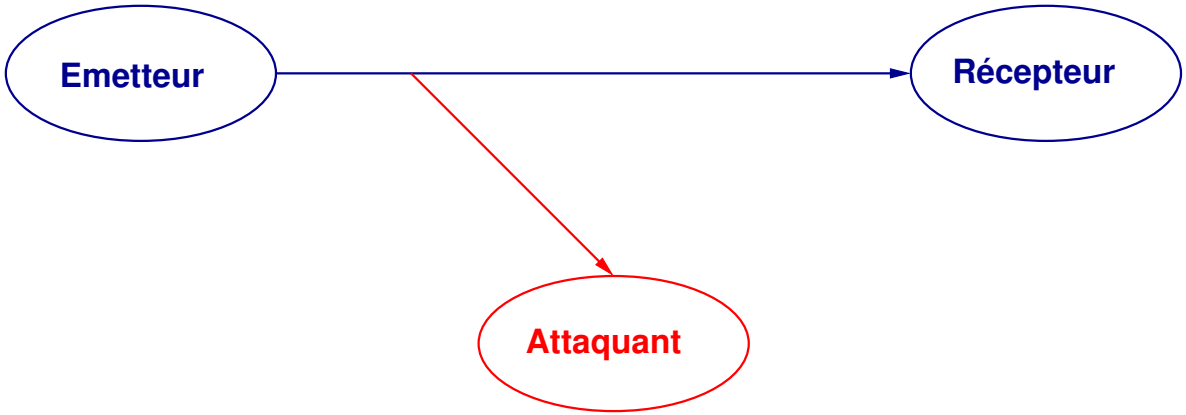
Interruption de service



Atteinte à la disponibilité :

- Destruction physique
- Modifications de configurations
- etc.

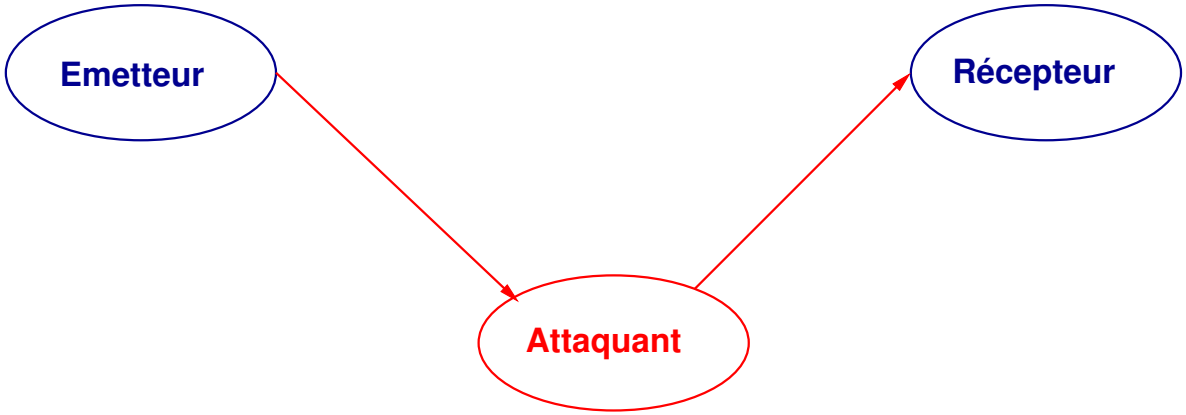
Interception du trafic



Atteinte à la confidentialité :

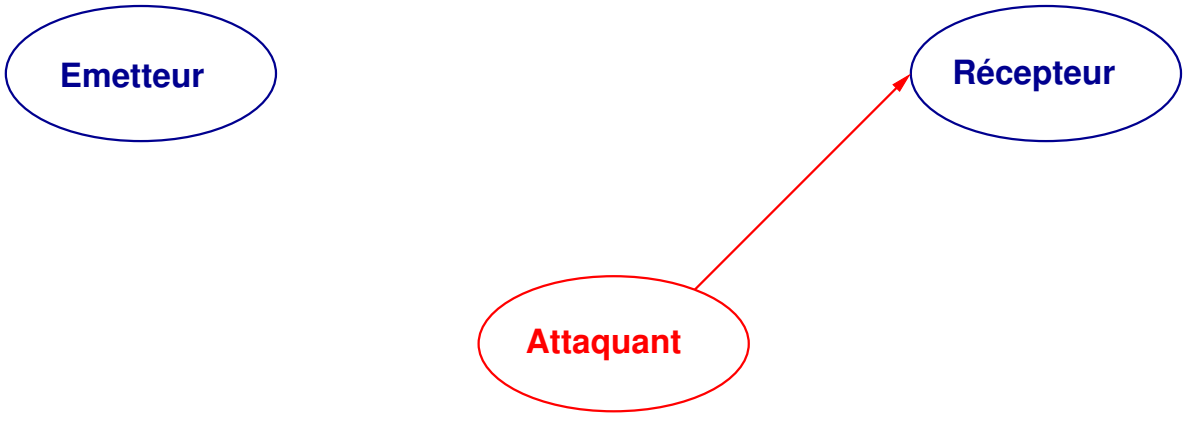
- accès non autorisés aux informations
- copies illicites de données
- Keyloggeurs
- sniffeurs
- etc.

Altération de l'intégrité des données



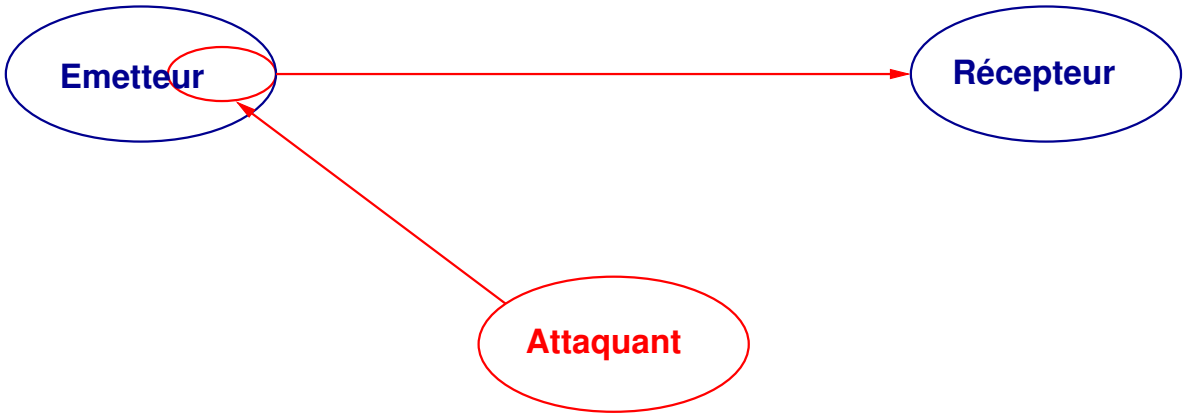
Atteintes à la confidentialité et à l'intégrité

Mascarade



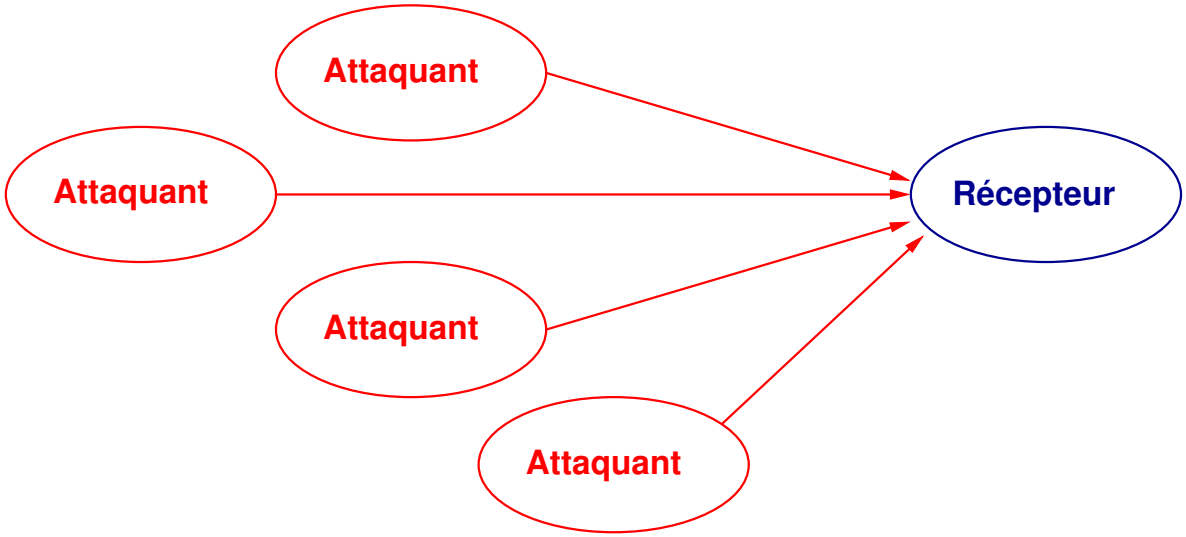
- usurpation d'identité
- diffusion de fausses informations
- phishing (ameçonnage)
- etc.

Infiltration



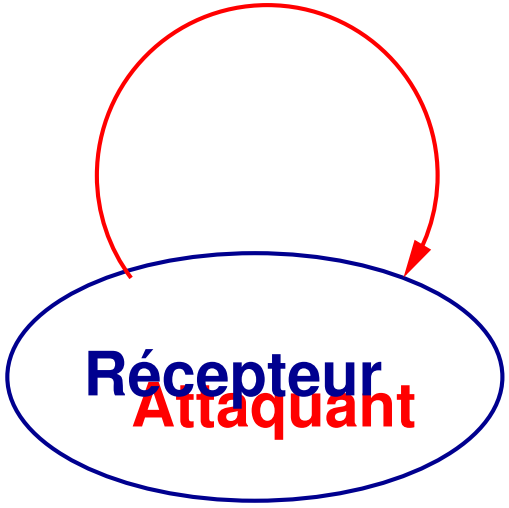
- Chevaux de troie
- Virus
- Botnets

Attaques frontales



- Attaques coordonées
- Refus de service
- Techniques d'amplification (smurf,...)
- etc.

Attaques internes



- Erreurs humaines
- Malveillance
- Ingénérie sociale
- ...

Plan

[1] Reconnaissance du contexte

- Notoriété et intérêt du site, etc.
- Utilisation d'outils ■ anodins ■ : DNS, messagerie, sites Web et FTP, etc.
- Obtention de la visibilité externe et officielle du site

$\longrightarrow$ pas de détection possible

[2] Étude de la cible

- Reconnaissance des services accessibles et des failles potentielles : scans de ports (NMAP), scans des vulnérabilités (Nessus), bannières des services (SMTP, WWW, ...), état des systèmes (SNMP)
- Conservation éventuelle des informations pour un usage ultérieur (grâce aux avis de sécurité !)

$\longrightarrow$ détection possible

[3] Le jour J

- Utilisation d'un «exploit» pour pénétrer un système vulnérable,
- Attaque par force brute des mots de passe,
- Mise en place de backdoors, sniffers, etc.
- ...

$\longrightarrow$ détection possible

[4] Nettoyage des indices

- Destruction des traces,
- Installation d'outils de masquage (remplacement de commandes, modules noyau, ...)

$\longrightarrow$ plus de détection possible si bien fait

[5] Exploitation

- Insertion dans un botnet,
- Serveur pour phishing,
- Diffusion de spam,
- DDoS,
- Vol ou destruction d'informations,
- etc.

$\longrightarrow$ plus ou moins détectable

Plan

Conclusion - pour A3IMP

- Connaître les attaques pour mieux les détecter.
- La machine est *piratée* à partir de l'étape 3 ci-dessus.
- Mais si l'attaque est parfaite : pas détectable après l'étape 4.
- Heureusement, les systèmes sont complexes et les humains faillibles, donc le crime parfait n'existe pas...