La sécurité dans les transaction informatiques, quels enjeux?

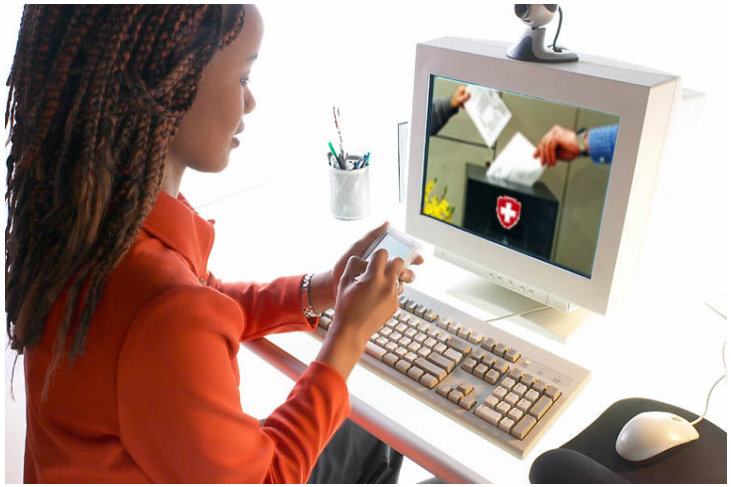
Dr. Philippe Oechslin
chargé de cours

fondateur
OBJECTIF SÉCURITÉ
Architecte de la sécurité informatique

philippe.oechslin@objectif-securite.ch

Les transactions informatiques

- Commerce
  - Billets d'avion
  - Livres, CDs
  - Achats ménagers
- Source d'information neutre
  - Horaires
  - Informations techniques
  - Informations médicales
  - Actualités (news.google.com)
- Banques
  - Télébanking
  - Bourse électronique
- Et bientôt:
  - le vote électronique:



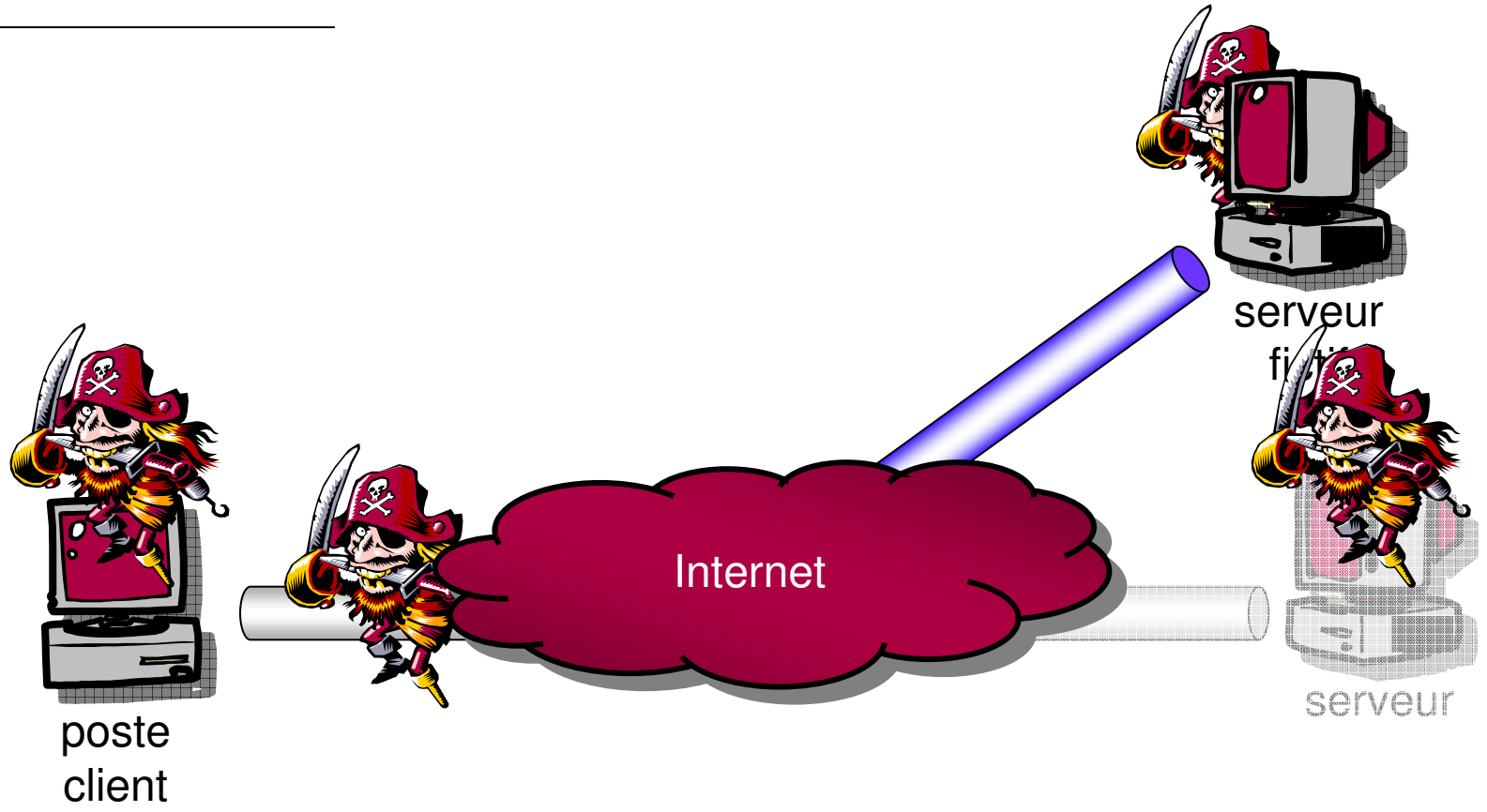
Les transactions sont elles sûres?

- Les questions que peut se poser l'internaute:
  - Qui est-ce qui va voir mon numéro de carte de crédit?
  - Qui stocke quelle information à mon sujet?
  - Qui peut accéder à mon compte?
  - Le système est-il disponible quand j'en ai besoin?

Les enjeux techniques

- Il faut protéger
  - La confidentialité,
  - L'intégrité,
  - La disponibilité
  - L'authenticité,
  - La sphère privée,
  - L'anonymat

Sources d'attaques



Exemple de Serveurs piratés

- Vol de la base de données client du WEF à Genève en 2001
  - 27'000 noms, adresses, e-mail et téléphones
  - 1'400 cartes de crédit
- Les clients d'une banque peuvent consulter les comptes de tous les autres clients! (Cahoot, UK, la semaine passée)
- Cross-Site scripting:
  - Exemple Adobe,
  - Banque Cantonale

 démo

Exemple de sites fictifs

- En 2001 un virus informatique redirigeait les requêtes vers une banque suisse sur un site qui lui ressemblait
- Phishing: depuis deux ans, on ne compte plus les sites fictifs créés pour récolter des mots de passes

Exemple de clients manipulés

- Une enquête aux USA, le mois passé, PC privés:
  - 20% infectés par un virus
  - 80% par un spyware
- Le PC privé du client échappe au contrôle de la société qui offre la transaction
  - Même si le serveur et la communication sont sécurisés, on ne sait pas ce qui se passe sur le PC du client.
- En février de cette année, le virus WebMoney modifiait IE pour voler les mots de passe à la volée

Que faut-il en penser?

- Faut-il être parano?
  - Le risque zéro n'existe pas!
- L'enjeu principal est de gagner la confiance de l'utilisateur
- On peut limiter les risque en mettant en place une sécurité systématique

Comment sécuriser les transactions

- Sécurité technique
  - Utiliser les bons outils cryptographiques
  - Concevoir une architecture de sécurité
  - Auditer la sécurité
- Sécurité Organisationnelle
  - Formaliser la gestion de la sécurité
  - Préparer les mesures en cas d'incident
    - Endiguement, reprise
    - Recherche de preuves
    - Communication
  - Régler la responsabilité dans les contrats

Questions?