Sécurité, protection de la vie privée et disponibilité

Yves Deswarte, *David Powell*, Yves Roudier

Journée OFTA Informatique Diffuse

31 mai 2007

Introduction

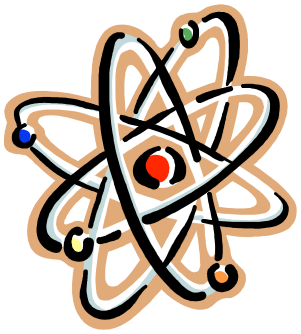
"The goal is to achieve the most effective kind of technology, that which is essentially *invisible* to the user."

Marc Weiser, Ubiquitous Computing, *Communications ACM*, Jul 1993

confiance

- **Sécurité des données et des transactions par rapport aux malveillances**
- **Protection de la vie privée contre les abus des moyens technologiques**
- **Disponibilité des services là et où l'utilisateur en a besoin**

Menaces — fautes accidentelles



Fautes physiques

Environnement physique

- chocs
- humidité
- …

Mobilité & comm. sans fil

- interférences
- portée limitée
- énergie

Fautes de développement

Dynamique

- mobilité
- contexte d'utilisation
- …

Évolutions rapides

- cycle de vie
- hétérogénéité

Fautes d'interaction

Facteurs humains

- public de 7 à 97 ans
- interfaces pauvres et hétérogènes
- dynamique et furtivité

Menaces — malveillances

Fautes physiques

Comm. sans fil

- brouillage

Espaces non protégées

- vandalisme
- sabotage
- vol
- subtilisation et analyse HW

Fautes de développement

Logiciels malveillants

- tentations accrues (infos personnelles critiques)
- subtilisation et re-programmation

Fautes d'interaction

Attaques classiques

- virus
- hameçonnage
- pourriel

Comm. sans fil

- interception (à distance)

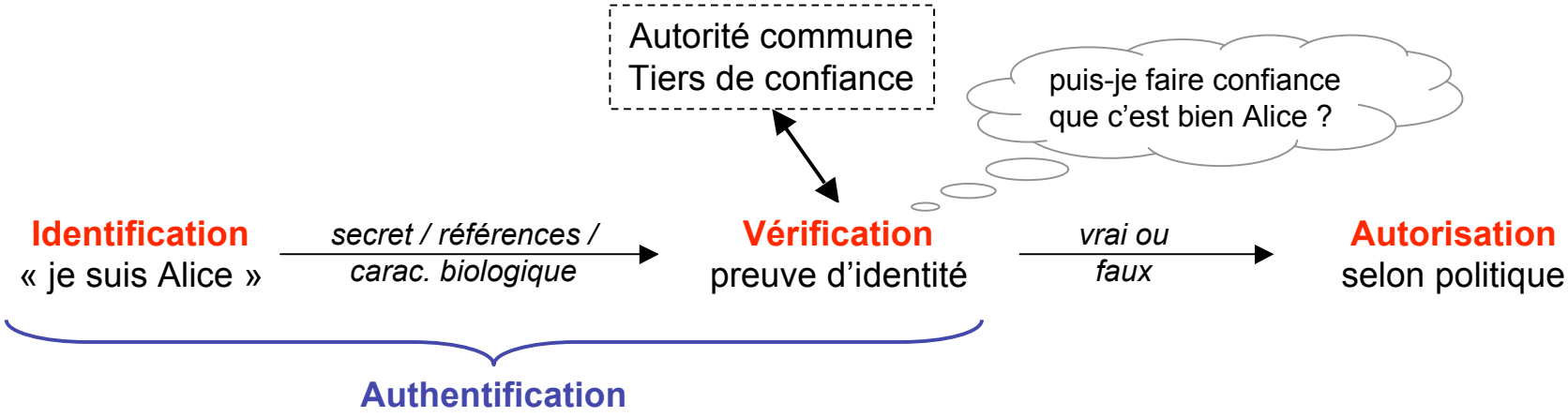
Dispositifs

- identifiables
- localisables

Sécurité

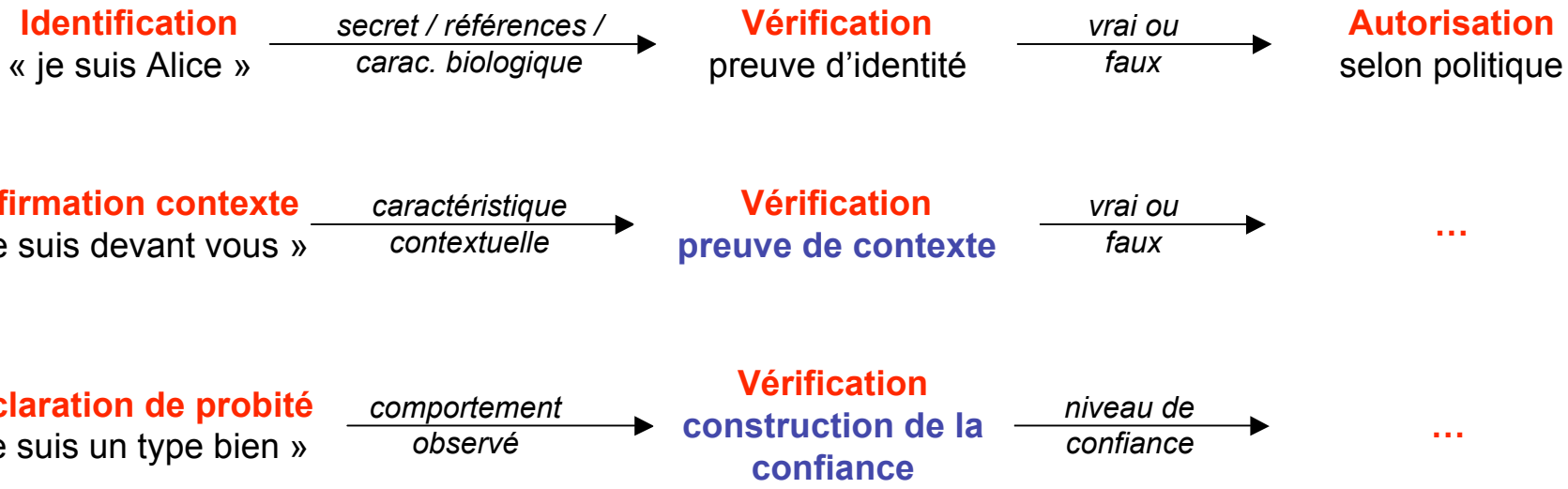
- **Attributs :**
  - *Confidentialité* : absence divulgation non autorisée
  - *Intégrité* : absence de modification non autorisée
  - *Disponibilité* : prêt à l'utilisation autorisée

- **Processus d'autorisation classique**



Sécurité et informatique diffuse

- **Découverte et utilisation de services dans un environnement ouvert et dynamique**
  - importance du contexte physique
  - absence de confiance préalable entre dispositifs
  - fonctionnement sans infrastructure de sécurité globale
  - protection de la vie privée

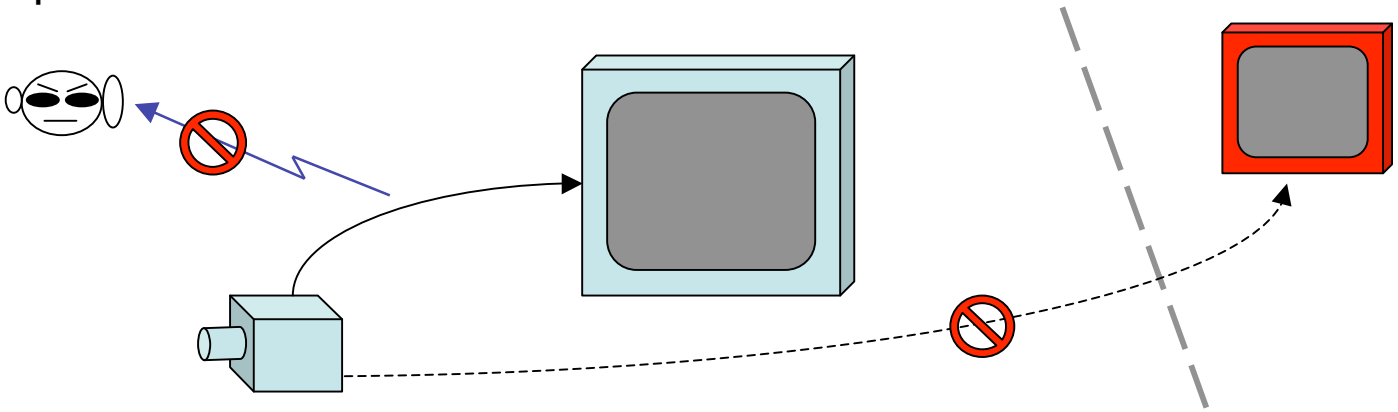


Établissement de la confiance

- **Preuve de contexte**
  - éléments de contexte
    - proximité
    - localité
    - heure
    - identités / rôles dispositifs voisins
  - autorités multiples supplémentaires
    - tickets de contexte
  - contrôle d'accès avec notion de « rôle environnemental »
    - autorisation seulement si conditions de contexte satisfaites
    - ex : selon lieu, heure, et jour de la semaine
- **Construction de la confiance**

Association (appairage) sécurisée

- **But:** établir communication sécurisée entre dispositifs ne partageant au préalable ni contexte ni secret commun



- **Solutions**
  - « imprégnation » par câble pour établir clé commune
  - preuve de proximité par mesure d'un temps « défi-réponse »
  - authentification mutuelle via l'humain (ex. Bluetooth)
  - s'affranchir du clavier :
    - code bar + caméra
    - émetteur son + microphone…
  - dispositifs non-interactifs ? (ex. capteurs en réseau)
    - établissement clé commune par secouage simultané,…

Établissement de la confiance

- **Preuve de contexte**
  - éléments de contexte
    - proximité
    - localité
    - heure
    - identités / rôles dispositifs voisins
  - autorités multiples supplémentaires
    - tickets de contexte
  - contrôle d'accès avec notion de « rôle environnemental »
    - autorisation seulement si conditions de contexte satisfaites
    - ex : selon lieu, heure, et jour de la semaine

- **Construction de la confiance**
  - *évaluation coopération*
    - systèmes coopératifs ou auto-organisés
      - ➔ attaque par égoïsme
    - incitation à la coopération
      - réputation
      - rémunération / amende
        ex : certificats utilisables 1 fois
        [Bussard & Molva 2004]
  - *évaluation comportement*
    - confiance si conformité à un profil standard de comportement
    - ex. déplacements, interactions de l'utilisateur…
    - protection de la vie privée ?

Protection de la vie privée

- **Informatique et libertés (1978) - article 1er**

  « L'informatique doit être au service de chaque citoyen. […] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »

- **Quatre sortes d'exigences (critères communs)**
  - anonymat : secret du nom utilisateur associé à sujet ou opération
  - « pseudonymat » : *idem* sauf utilisateur répond de ses actions
  - non- « chaînabilité » : secret liens entre opérations par un utilisateur
  - non-observabilité : secret opération en cours

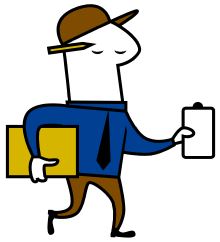
Vie privée et informatique diffuse

- **Nouvelles technologies au service du « big brother » ?**
- **Possibilités accrues de collecte d'infos sensibles**
  - multiplication de dispositifs portables et communicants
  - multiplication de services « contextuels »
    - ➔ besoin technologies garantissant protection de données perso
- **Principes de base**
  1. **principe de souveraineté** sur les données personnelles
     - données perso appartiennent à la personne en question
     - ne devraient être stockées que sur dispositifs sous son contrôle
       - ➔ opportunité pour l'informatique diffuse : dispositif personnel de stockage
  2. **principe de minimisation** des données personnelles
     - divulgation selon besoin d'en connaître (« need to know ») : seules sont fournies les données strictement nécessaires pour la tâche
     - le tiers doit les garder confidentielles (*cf.* souveraineté) et les effacer dès que possible

Exemple : commerce électronique

Client

Marchand



Livreur

Banque du marchand

Banque du client

✔	• objet acheté • validité moyen de paiement	• adresse livraison • identité destinataire • caractéristiques objet acheté	• montant virement • banque du client	• identité client • montant à virer • banque et n° compte du marchand
✖	• identité client • banque client • adresse livraison	• identité client • prix d'achat	• identité client • son numéro de compte • objet acheté • adresse livraison	• objet acheté • adresse livraison

Technologies de protection vie privée

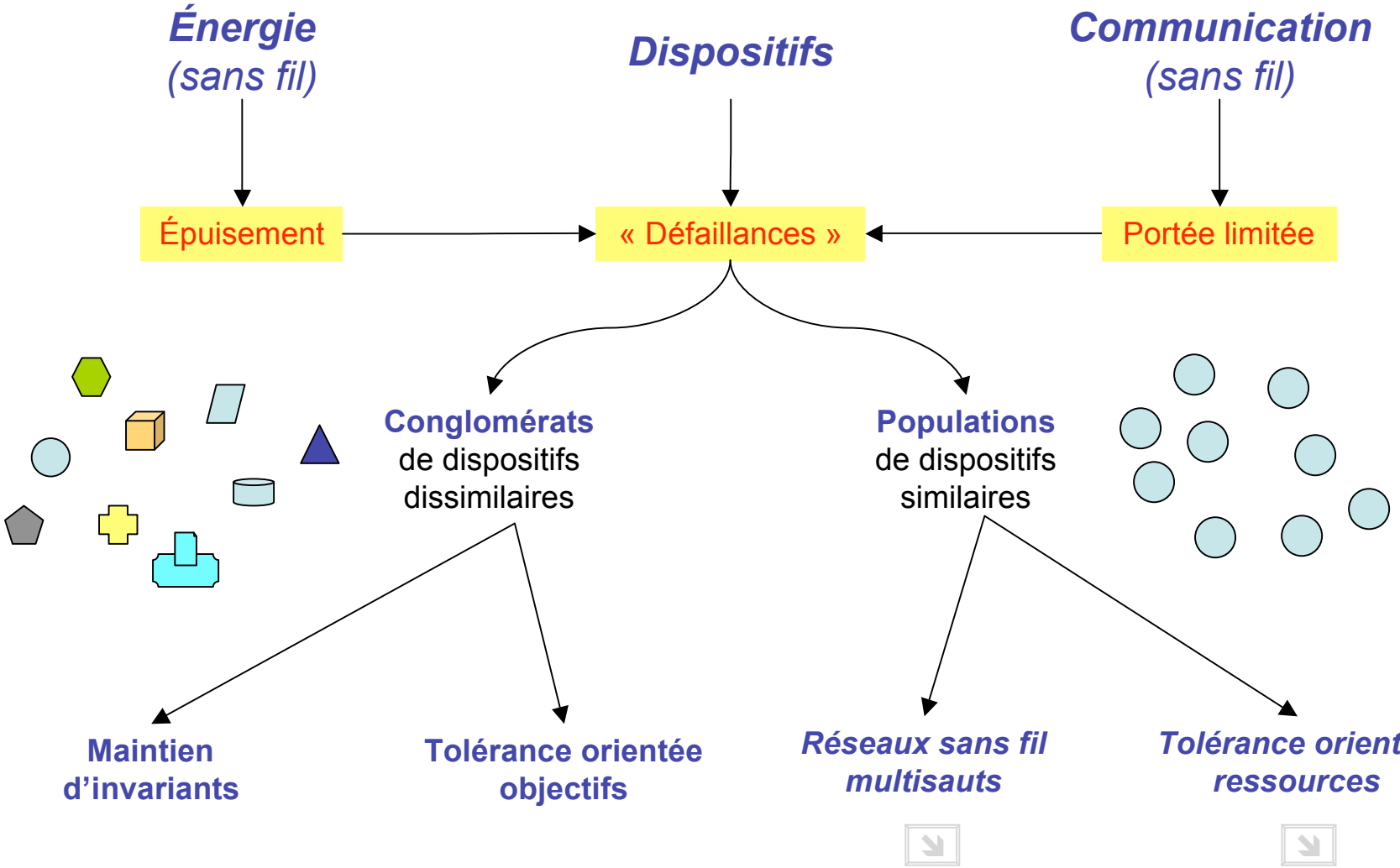
- **Gestion d'identités virtuelles (pseudonymes) multiples**
  - choix selon service, rôle… + définition validité temporelle
  - authentification selon sensibilité du service
    - ➔ opportunité pour l'informatique diffuse : dispositif personnel de gestion de pseudonymes
- **Communication anonyme**
  - @IP est une info sensible
    - ➔ identif. dispositif / lieu / heure
  - tiers d'anonymisation de la communication (MIX)
  - adressage dynamique (DHCP) + tunnel vers mandataire (ex : connexion IP nomade anonyme)
- **Autorisation préservant la vie privée**
  - séparer l'autorisation de l'authentification
  - *garanties anonymes* pour prouver un privilège
  - gestion par des tiers de confiance (hors ligne)
- **Accès anonyme à des services**
  - communication anonyme parfois insuffisante
  - mandataires spécifiques à chaque type d'application
  - ex : service basé sur la localisation

Disponibilité

Services accessibles en tout lieu et à tout instant ?

- **Avec infrastructure fixe**
  - téléphonie
  - informatique nomade…
  - disponibilité ➔ connectivité (à des services disponibles)
- **Sans infrastructure fixe**
  - mode déconnecté
  - situations de crise
  - nouvelles applications : véhicules, robots, micro-dispositifs intelligents…
  - disponibilité ➔ résilience aux fautes et autres menaces casuelles

Disponibilité et informatique diffuse



Conclusion

Informatique diffuse → **Déploiement massif ?**

→ **Applications critiques ?**

Sûreté de fonctionnement : un défi majeur

Sécurité

- sans fil et localisation dispositifs : techniques cryptos particulières de preuve proximité où possession secret
- appairage : choix selon facteur de forme des appareils et acceptation par le public
- construction confiance par évaluation comportement - pb de protection de la vie privée

Protection vie privée

- technologies génériques pour garder le contrôle des infos persos
- technologies spécifiques pour minimiser la divulgation d'infos persos (négociation)
- aspects légaux et techniques de la protection des infos persos ; contrôle de leur transmission aux autorités

Disponibilité

- synonyme de connectivité à l'infrastructure fixe ?
- situations de crise, nouvelles applis - ensembles de dispositifs autonomes…
- populations : tolérance orientée ressources
- conglomérats : tolérance orientée objectifs