Tickets de Métro Electroniques et Vie Privée: un Point de Vue Cryptographique

F.-X. Standaert

UCL Crypto Group, Université catholique de Louvain

Parlement de la Région de Bruxelles-Capitale, 22 Juin 2011

Outline

- Sécurité et vie privée
- Notions de vie privée
  - Identité publique, anonymat, intraçabilité
- MOBIB et le respect de vie privée
- Cryptographie à clé secrète / publique
- MOBIB et la cryptographie
- Améliorations possibles
- Conclusions
- Mon avis

Sécurité ≠ vie privée

- Sécurité : éviter l'accès non autorisé à un lieu (ex : batiment) ou un service (ex : transport public)
  - Habituellement la première préoccupation du gestionnaire de service (motivation financière)
- Vie privée : éviter la fuite d'informations à caractère personnel (nom, adresse, données médicales, . . .)
  - Prioritairement une préoccupation des utilisateurs

- Propriétés "indépendantes" : un système peut être sécurisé sans respecter la vie privée de ses utilisateurs

Outline

- Sécurité et vie privée
- Notions de vie privée
  - Identité publique, anonymat, intraçabilité
- MOBIB et le respect de vie privée
- Cryptographie à clé secrète / publique
- MOBIB et la cryptographie
- Améliorations possibles
- Conclusions
- Mon avis

Identité publique

François-Xavier a pris le bus 22 à Mérode à 11h13. François-Xavier est sorti du bus 22 à Schuman à 11h17. François-Xavier a retiré 20 euros à l'ATM de la rue de la Loi à 11h31. François-Xavier a pris le métro ...

- Les noms sont directement lisibles
  $\Rightarrow$ Pas de protection de la vie privée

Anonymat (faible)

XV27 a pris le bus 22 à Mérode à 11h13. XV27 est sorti du bus 22 à Schuman à 11h17. XV27 a retiré 20 euros à l'ATM de la rue de la Loi à 11h31. XV27 a pris le métro ...

- Utilisation de pseudonymes statiques
- Une seule "rencontre" avec XV27 permet de révéler complètement son identité
- A la longue, le pseudonyme devient une identité

$\Rightarrow$ Faible protection de la vie privée

Intraçabilité

AU31 a pris le bus 22 à Mérode à 11h13. YT66 est sorti du bus 22 à Schuman à 11h17. SV18 a retiré 20 euros à l'ATM de la rue de la Loi à 11h31. DJ34 a pris le métro . . .

- Utilisation de pseudonymes "dynamiques"
- La lecture des différents pseudonymes ne révèle aucune information sur la personnes "contrôlée"

  $\Rightarrow$ Bonne protection de la vie privée

Outline

- Sécurité et vie privée
- Notions de vie privée
  - Identité publique, anonymat, intraçabilité
- MOBIB et le respect de vie privée
- Cryptographie à clé secrète / publique
- MOBIB et la cryptographie
- Améliorations possibles
- Conclusions
- Mon avis

MOBIB et le respect de la vie privée

- Identité publique pour la STIB
- La STIB a la capacité d'utiliser des données à caractère personnel sur les trajets de ses clients, via la constitution d'une base de donnée
- (*ce qui n'implique pas qu'elle le fait !*)

Mais aussi...

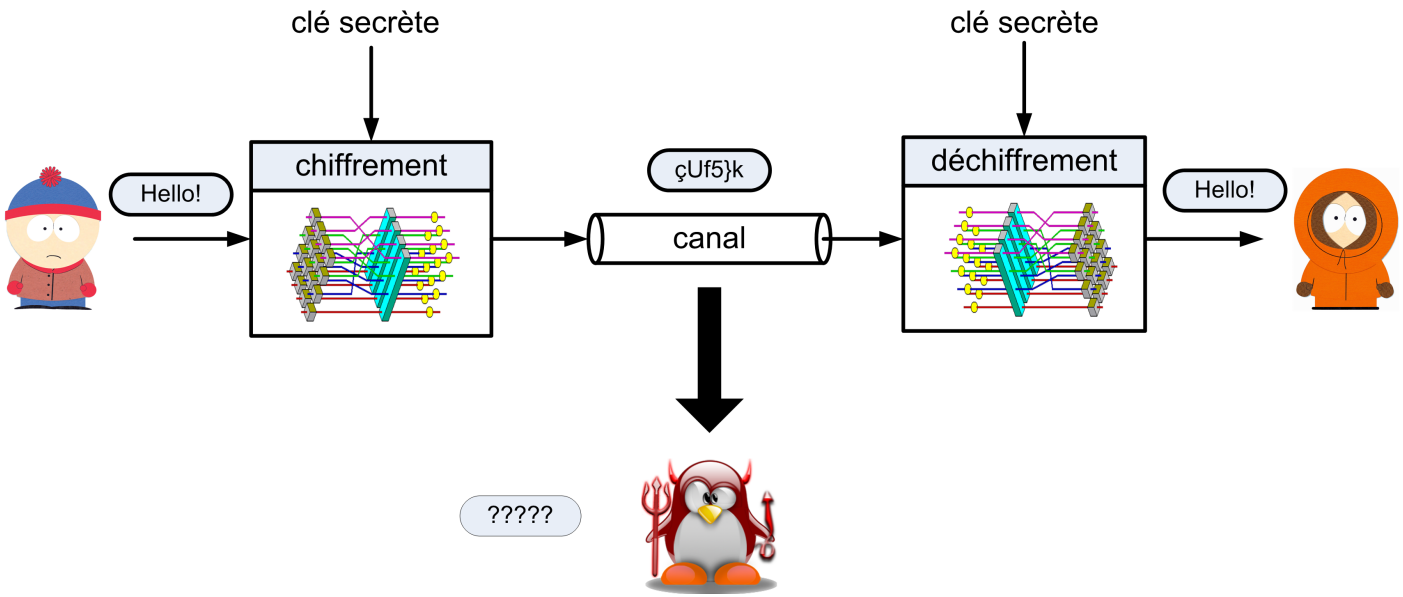
- Identité "publique" pour les usagers tiers *
- Via une lecture sans fil de la carte MOBIB,
  - cfr. Gildas Avoine et al., *MOBIB Extractor*, 2009.
  - "Attaque" à faible coût (nécessite principalement un lecteur RFID d'une vingtaine d'euros)
- (*ce qui ne permet pas de garantir que cette traçabilité n'est jamais exploitée par des tiers malveillants*)

* Plus précisément : il n'existe aucune protection cryptographique de l'identité (et du code postal, et des trois derniers lieux et heures de compostages) des usagers

Outline

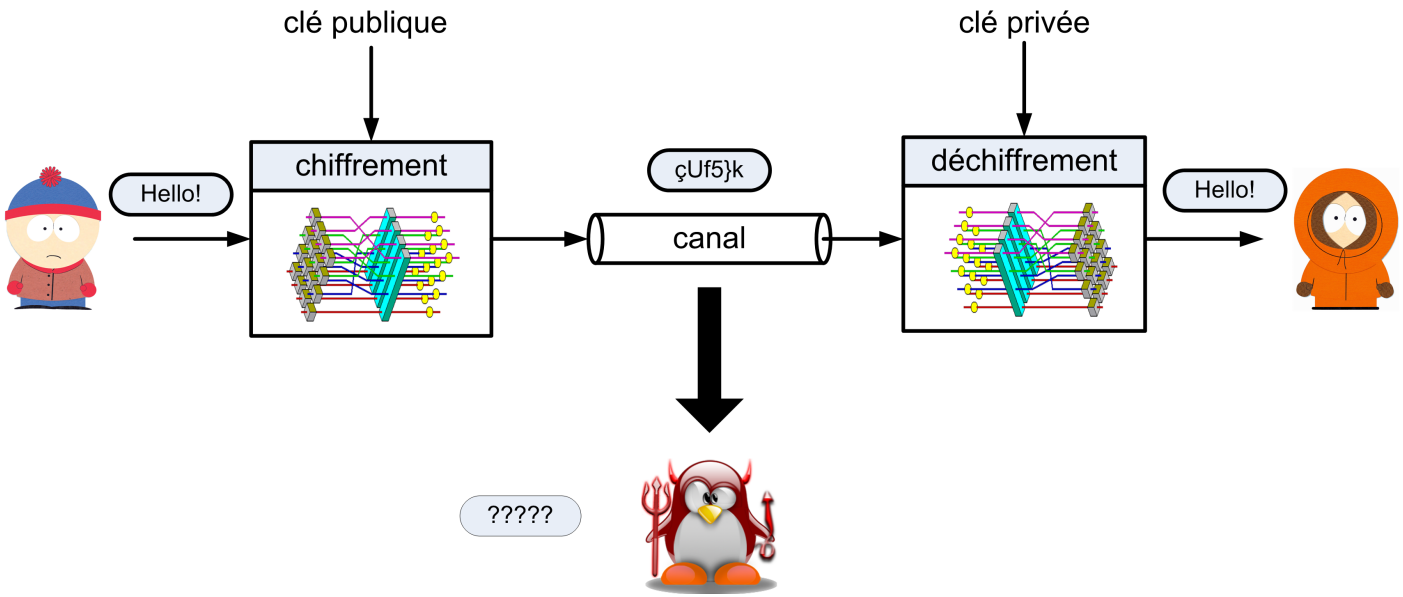
- Sécurité et vie privée
- Notions de vie privée
  - Identité publique, anonymat, intraçabilité
- MOBIB et le respect de vie privée
- Cryptographie à clé secrète / publique
- MOBIB et la cryptographie
- Améliorations possibles
- Conclusions
- Mon avis

Cryptographie à clé secrète



- La même clé est utilisée pour chiffrer et déchiffrer
- L'adversaire peut espionner le canal, mais il n'est pas capable de déchiffrer les messages

Cryptographie à clé publique



- Clé de chiffrement $\neq$ clé de déchiffrement
- "N'importe qui" peut chiffrer un message, mais seul le destinataire peut le déchiffrer

Avantages / inconvénients

- Cryptographie à clé secrète
  - \+ Simple et efficace à mettre en oeuvre
  - \- Nécessité un échange de clé préalable

- Cryptographie à clé publique
  - \+ Permet des fonctionnalités plus complexes (échange de clé, signature électronique, . . .)
  - \- Plus complexe à mettre en oeuvre

- Il s'agit de techniques standardisées dans les 2 cas !
- Par exemple utilisées dans les cartes bancaires

Outline

- Sécurité et vie privée
- Notions de vie privée
  - Identité publique, anonymat, intraçabilité
- MOBIB et le respect de vie privée
- Cryptographie à clé secrète / publique
- MOBIB et la cryptographie
- Améliorations possibles
- Conclusions
- Mon avis

MOBIB et la cryptographie

- MOBIB est basée sur le standard Calypso
- Utilisé dans plusieurs pays (France, Italie)
- Ce standard utilise de la cryptographie à clé secrète (algorithme DES ou 3DES) pour sécuriser le système
  - càd. éviter le clonage de tickets
  - et l'écriture sur la carte (trajets gratuits)

- MOBIB n'utilise pas de cryptographie pour protéger la vie privée des usagers (càd. la lecture de la carte)

Outline

- Sécurité et vie privée
- Notions de vie privée
  - Identité publique, anonymat, intraçabilité
- MOBIB et le respect de vie privée
- Cryptographie à clé secrète / publique
- MOBIB et la cryptographie
- Améliorations possibles
- Conclusions
- Mon avis

Sans changement d'instrastructure

- Protéger la lecture de la carte MOBIB avec de la cryptographie à clé secrète :
  - permettrait de protéger la vie privée des usagers contre des usagers tiers malveillants
  - ne réduirait pas la *capacité* de la STIB à traçer les trajets de ses clients (via une base de donnée)

- L'éventuel respect de la vie privée de cette solution provient de la confiance que les utilisateurs accordent à la STIB, pas d'une garantie mathématique (cryptographique) $\Rightarrow$ difficile à vérifier/quantifier

Avec changement d'instrastructure

- Utiliser des "anonymous credentials" et les techniques de "preuve à divulgation nulle de connaissance" :
  - Permettrait de prouver qu'un ticket de transport est valide et rien de plus $\Rightarrow$ d'offrir une garantie cryptographique du respect de la vie privée !
  - Assurerait l'intraçabilité par défaut des utilisateurs
- La mise en oeuvre de ces techniques nécessite de la cryptographie à clé publique (absente du standard Calypso et de la carte à puce actuellement déployés)

Changement de paradigme

+ Pas de base de données à sécuriser * (ni de confiance en la STIB) car pas de données privées collectées !
  - Problème résolu à sa source (vs. a posteriori)
+ Intraçabilité révocable
  - Si fraude ou problèmes majeurs (attentats, . . .)
+ Cette solution n'empêche pas de constituer des statistiques de fréquentation du réseau

* Tâche difficile : nombreux exemples de pertes d'information !

Outline

- Sécurité et vie privée
- Notions de vie privée
  - Identité publique, anonymat, intraçabilité
- MOBIB et le respect de vie privée
- Cryptographie à clé secrète / publique
- MOBIB et la cryptographie
- Améliorations possibles
- Conclusions
- Mon avis

Conclusions

- MOBIB collecte des données à caractère personnel
- Est-ce grave ? $\Rightarrow$ question politique, juridique
- Est-ce nécessaire ? $\Rightarrow$ Techniquement, non !
- De véritables garanties cryptographiques nécessitent une révision profonde du système mis en place
  - Un pseudonyme statique ne suffit pas !
- Eviter la confusion entre anonymat et intraçabilité

- Note : pas uniquement un problème de vie privée (la sécurité du système, par ex. contre un adversaire qui volerait une borne, mériterait d'être bien analysée)

Outline

- Sécurité et vie privée
- Notions de vie privée
  - Identité publique, anonymat, intraçabilité
- MOBIB et le respect de vie privée
- Cryptographie à clé secrète / publique
- MOBIB et la cryptographie
- Améliorations possibles
- Conclusions
- Mon avis

Mon avis

- MOBIB : un changement de système est souhaitable
- Une solution alternative à base d'anonymous credentials mériterait d'être évaluée et budgétisée
- TEC, SNCB : bien réfléchir avant de poursuivre le déploiement d'un système partiellement obsolète
  - En particulier vu le coût de déploiement de 23 millions d'euros mentionné pour la TEC (RTBF, 6 juin 2011, journal télévisé de 19h30)
- Privilégier un système aux spécifications ouvertes
  - http ://fr.wikipedia.org/wiki/Principe_de_Kerckhoffs