Sécurité et méthodes formelles

Laboratoire de Sécurité Informatique (LSI)

Mohamed Mejri

Données Massives 2015

29 octobre 2015

Laboratoire LSI

Axes de recherches : Développer des méthodes, techniques et outils permettant d'améliorer

- la sécurité des protocoles cryptographiques,
- la sécurité des applications,
- la lutte contre le piratage informatique,
- la sécurité de téléphones intelligents et la protection de la vie privée,
- la sécurité des applications et des infrastructures infonuagiques, et
- la sécurité de l'Internet des objets

Sécurité de protocoles cryptographiques

- **Protocole :**

$$\begin{array}{lcll} 1. & \text{Alice} & \longrightarrow \text{Bob} & : e_{k_a}(M) \\ 2. & \text{Bob} & \longrightarrow \text{Alice} & : e_{k_b}(e_{k_a}(M)) \\ 3. & \text{Alice} & \longrightarrow \text{Bob} & : e_{k_b}(M) \end{array}$$

- **Hypothèses :**
  - k_a est une clé connue seulement par *Alice*
  - k_b est une clé connue seulement par *Bob*
  - $e_{k_b}(e_{k_a}(M)) = e_{k_a}(e_{k_b}(M))$
- **Propriété de sécurité :** Confidentialité de M
- **Faille :** Une trace du protocole qui montre que l'intrus peut dévoiler M sans connaître k_a ou k_b

$$\begin{array}{lcll} 1. & \text{Alice} & \longrightarrow \text{Devil(B)} & : e_{k_a}(M) \\ 2. & \text{Devil(B)} & \longrightarrow \text{Alice} & : e_{k_a}(M) \\ 3. & \text{Alice} & \longrightarrow \text{Devil(B)} & : M \end{array}$$

Sécurité de protocoles cryptographiques

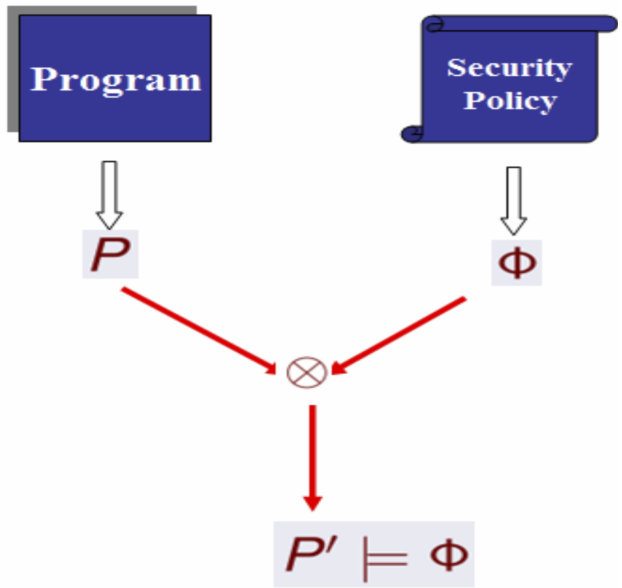
- Trouver des conditions suffisantes et faciles à vérifier permettant de garantir la correction des protocoles qui les respectent par rapport à une propriété donnée.

- Exemple : si C est la condition, P est le protocole et S est la propriété de confidentialité :

$$C(P) \Longrightarrow P \text{ est } S\text{–}Correct$$

Sécurité des applications

Objectifs : Définir un opérateur $\otimes$ permettant d'automatiquement appliquer une politique de sécurité sur un pogramme



Entrées

- Un programme P
- Une politique de sécurité Φ

Sortie $P' = P \otimes \Phi$

- P' respecte Φ : $P' \models \Phi$
- P' « se comporte » comme P excepté quand il est sur le point de violer Φ.
- L'application de la politique est « optimale » : pas de tests ajoutés inutilement

Sécurité du Cloud

Développer des techniques permettant d'effectuer des traitements sur des données dans un Cloud public sans affecter leur confidentialité et leur intégrité.
Étant donné $E_k(a)$ et $E_k(b)$ le chiffrement de a et de b par la clé k, comment, sans décrypter ni a ni b, calculer :

- Trouver $E_k(a + b)$
- Trouver $E_k(a \times b)$
- Etc.

Contrôle de drois d'accès : analyse de conformité

Récupérer automatiquement les politiques de contrôles d'accès implantées dans des réseaux et des applications, et analyser leur conformité par rapport la politique de l'institution en question. Si Φ est la politique implantée dans un système S et Ψ est la politique demandée, alors répondre aux questions suivantes :

- Qui a le droit d'accéder à quoi, quand et comment dans S ?
- $\Phi \approx \Psi$?
- $\Phi \subseteq \Psi$?
- Distance entre Φ et Ψ ?
- Etc.

Sécurité de l'Internet des objets

Développer des techniques permettant d'assurer un bon contrôle d'accès ainsi que le respect de la vie privée dans l'Internet des objets. Ces techniques doivent prendre en considération des contraintes (mémoire, CPU, énergie) liées aux objets.
Étant donné n objets $O_1, \ldots, O_n$ et une politique de sécurité Φ :

- Quel contrôle doit faire chaque objet pour appliquer Φ ?
- Comment trouver la solution optimale en prenant en considération le coût de placer une action sur un objet ?
- Comment prendre l'aspect ad hoc du réseau : certains objets peuvent apparaître et d'autres disparaître à tout moment ?
- Comment prendre en considération que cetrains objets peuvent être « pirates »
- Etc.

Lutte contre le piratge informatique : autres volets

- Développer des techniques et des outils efficaces permettant d'analyser un grand volume de courriels afin de détecter les pourriels et de les classer en campagnes.
- Détection d'intrusions : analyse du trafic et de fichiers de journalisation à la recherche d'intrusions.
- Détection d'attaque web : développer une Proxy qui analyse (éventuellement bloque ou modifie) des échanges entre des clients et des serveurs web pour lutter contre certaines attaques