CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Sécuriser des applications mobiles, il y a un OWASP Top10 pour ça

Paris 13 Avril 2016

http://www.google.fr/#q=sebastien gioria

Application Security Expert and Coach

OWASP France Leader, Founder & Evangelist

OWASP ISO Project & OWASP SonarQube Project & OWASP CSRF Guard Leader

Legal and Forensics expert for Cour of Appeal of Poitiers

Proud father of youngs kids trying to hack my digital life

Twitter : @Spoint/@OWASP_France

Agenda

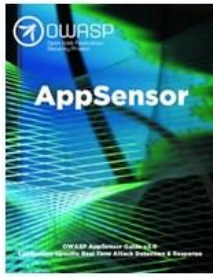
- OWASP ?
- OWASP Top10 Mobile
- Q/A

OWASP Best-sellers

Learn

Contract

Design



Code

Testing

Maturity

OWASP Top10 Mobile 2016

- M1: Improper Platform Usage
- M2: Insecure Data
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality Issues
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

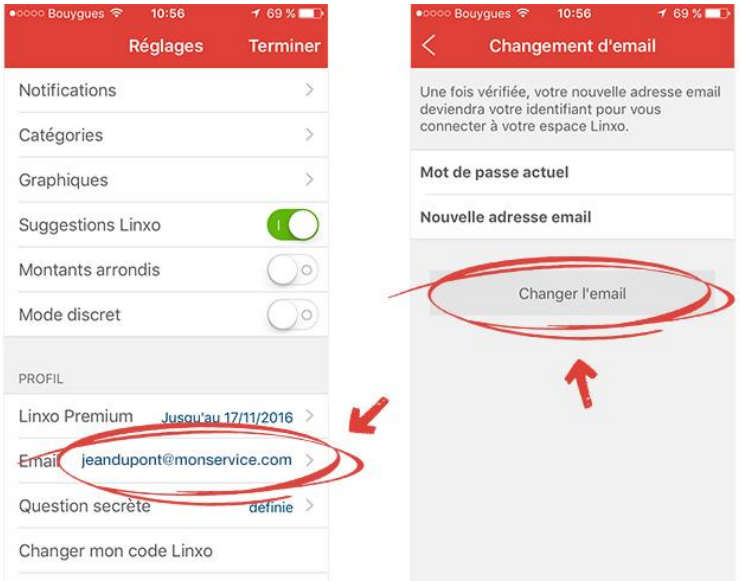
RELEASE CANDIDATE

M1 : Improper Platform Usage

- Risque :
  - Vol de données, fraude au paiement, …
- Solution :
  - Analyse de l'application, respect des guidelines
- Complexité de mise en œuvre
  - Moyenne
- Coût
  - Moyen

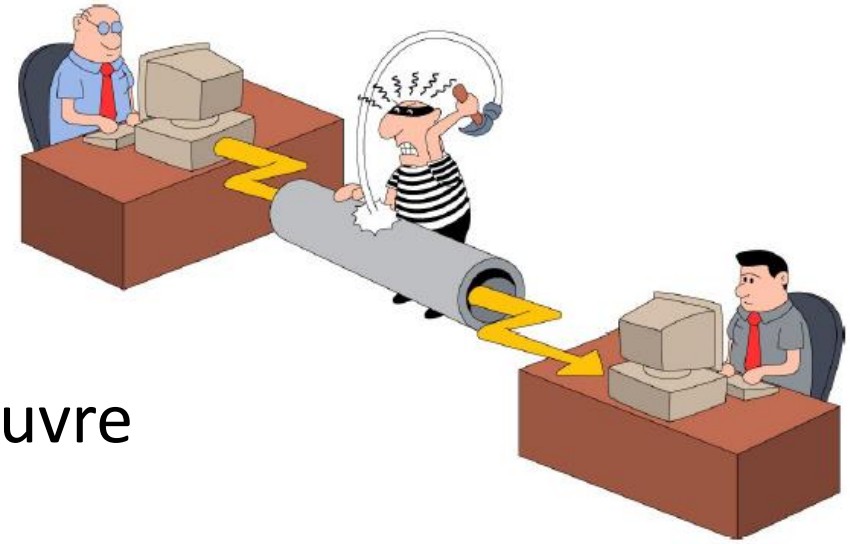
M2 : Insecure Data

- Risque :
  - Vol de données sur le terminal, ou dans le cloud
- Solution :
  - utilisation des « coffres forts de plateforme »
- Complexité de mise en œuvre
  - Simple
- Coût
  - Nul (ou presque)



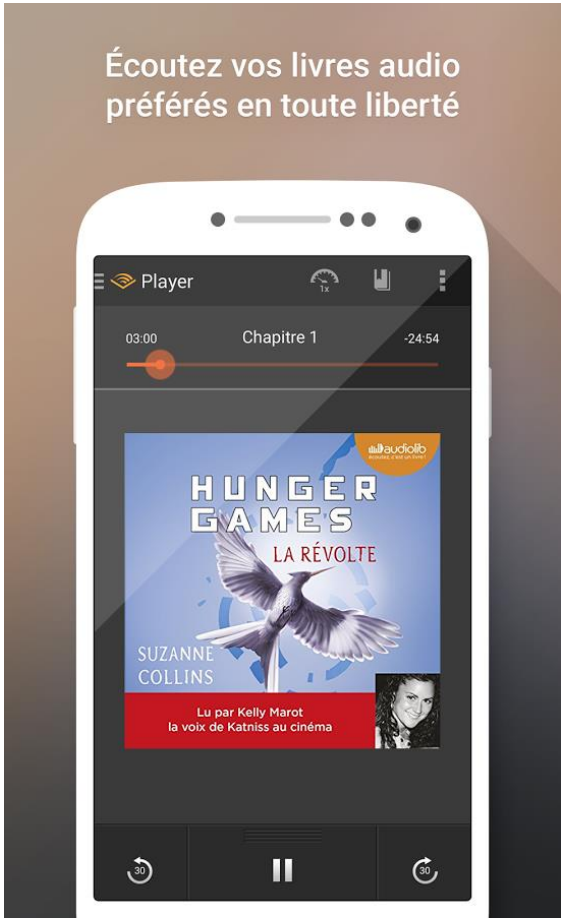
M3 : Insecure Communication

- Risque :
  - Vol de données sensibles
- Solution :
  - Mise en place de TLS
- Complexité de mise en œuvre
  - Simple
- Coût
  - Faible



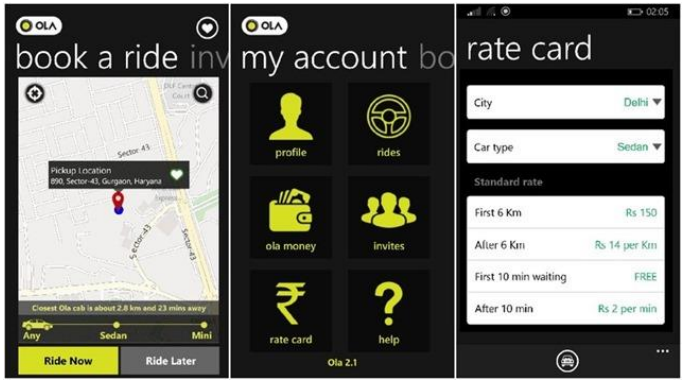
M4 : Insecure Authentication

- Risque :
  - Exposition de données a un utilisateur non autorisé
- Solution :
  - Authentification multi-facteur
  - Système de déconnexion
  - Gestion correcte des sessions
- Complexité de mise en œuvre
  - Simple à Complexe
- Coût
  - Faible à élevé



M5 : Insufficient Cryptography

- Risque :
  - Vol de données, Exposition de données sensibles
- Solution :
  - Utiliser un bon système de chiffrement, avec des clefs non prédictibles
- Complexité de mise en œuvre
  - Faible
- Coût
  - Faible



M6 : Insecure Authorization

- Risque :
  - Accès a des opérations de type CRUD sans autorisation
- Solution :
  - Mettre en place de l'habilitation et pas juste de l'authentification
- Complexité de mise en œuvre
  - Moyen
- Coût
  - Moyen

M7 : Client Code Quality Issues

- Risque :
  - Prise de contrôle sur le terminal
- Solution :
  - SecureCoding, revue de code
- Complexité de mise en œuvre
  - Moyenne à complexe
- Coût
  - Moyen à élevé.

M8 : Code Tampering

- Risque :
  - Prise de contrôle
- Solution :
  - Anti-virus ?
  - Mécanismes de signatures
- Complexité de mise en œuvre
  - Complexe
- Coût
  - Elevé

M9 : Reverse Engineering

- Risque :
  - Décompilation et analyse de l'application
- Solution :
  - Obfuscation
- Complexité de mise en œuvre
  - Simple à complexe
- Coût
  - Moyen

"This was fine for your nephew's fifth, Sire, but I fear it is set for a sterner test."

M10 : Extraneous Functionality

- Risque :
  - Vol de données, d'accès, …
- Solution :
  - Analyse du code avant mise en production

- Complexité de mise en œuvre
  - Moyenne
- Coût
  - Moyen

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Merci