Comment aborder la sécurité dans un projet mobile

En 2013, selon le cabinet Gartner, 2,4 milliards de portables, tablettes et PC ont été vendus dans le monde. La sécurité mobile est devenue un enjeu majeur, notamment à travers le Bring Your Own Device. À cette fin, la stratégie à adopter doit être définie en amont du projet! Florian Aeschlimann

Dans «Les nouveaux modes de travail à l'ère du digital», Orange Business Services indique que 62% des sociétés européennes ont fourni un accès mobile sécurisé à leurs salariés en 2013. Une tendance aujourd'hui à la hausse: selon l'analyste Benedict Evans, 4 milliards de smartphones et tablettes circuleront en 2017. CompTIA affirme également que «85% des PME, en 2011, utilisent des appareils technologiques personnels à des fins professionnelles». Si les problématiques liées à la mobilité diffèrent peu de celles des projets informatiques classiques, la sécurité mobile se pose essentiellement en termes techniques mais aussi fonctionnels.

Quel niveau de sécurité pour les applications mobiles?

Toujours selon l'étude d'Orange Business Services, pour 65% des entreprises européennes, la sécurité entraînera des changements dans les modes de travail dans les trois prochaines années.

Comment assurer le succès d'un tel projet? En définissant les impératifs de sécurisation en amont du projet. De ces prérequis découlent des choix techniques adaptés, par exemple: cibler une plateforme spécifique, développer une application web ou native… Ces choix de sécurité imposent aussi certaines contraintes fonctionnelles qui peuvent poser des problèmes d'ergonomie. Ainsi, les nouveaux smartphones proposent des alternatives à l'image de la biométrie – le Touch ID d'Apple ou le finger print scanner de Samsung.

Si les web apps offrent un niveau de sécurité acceptable pour un grand nombre d'applications, elles se révèlent en revanche insuffisantes lorsqu'un niveau de sécurité élevé est souhaité. Les applications natives présentent alors un niveau de gestion sécurisée supérieur. Toutefois, elles demeurent dépendantes des spécificités du système d'exploitation – Android, iOS – et par conséquent de ses failles. En effet, les ingénieurs de Codenomicon affirment que 50% des applications Android contiennent des failles de sécurité. Récemment, l'une d'elles a touché 80% des utilisateurs: des programmes malveillants, identifiés en tant qu'applications authentiques, ont pu accéder aux données de l'utilisateur.

Comment gérer les modes online/offline?

Selon le mode utilisé, le support mobile se trouve plus ou moins exposé aux risques de sécurité. En offline, il s'avère impossible d'envoyer un ordre de suppression des données, d'identifier les éventuelles tentatives d'intrusion ou de les bloquer. C'est pourquoi, il est nécessaire d'envisager des mesures de sécurité différentiées, adaptées aux exigences induites par le mode online et «renforcées» en mode offline pour pallier les risques induits par ce statut déconnecté.

Toutefois, des solutions existent, notamment en cryptographie, pour proposer un niveau de sécurité adapté à la puissance de calcul, inévitablement réduite sur un support mobile: temps d'expiration de session plus long en mode online, destruction des données en offline…

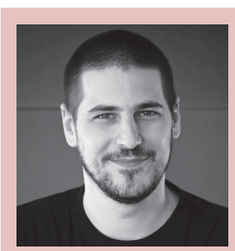
Gérer la cryptographie sur mobile

Si les algorithmes de chiffrage dépendent du support matériel, la cryptographie est un savant compromis entre le temps d'attente et la puissance de calcul. Deux possibilités s'ouvrent aux DSI:

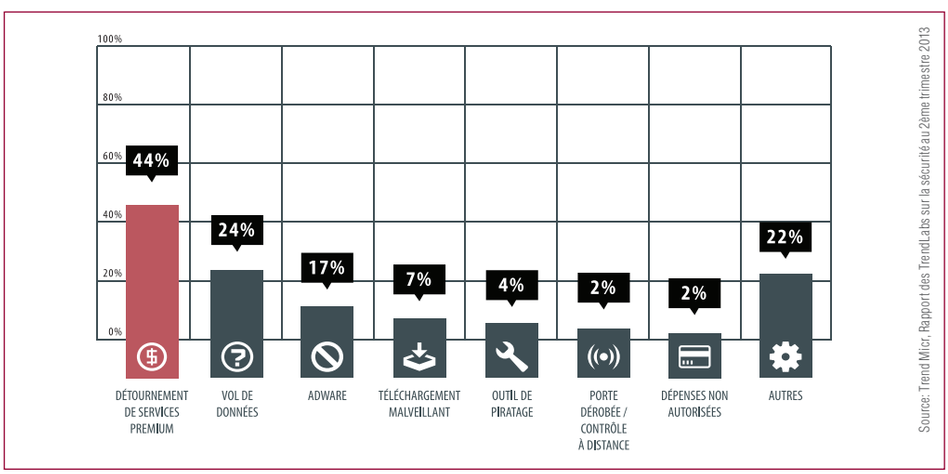
- Utiliser l'API native: se reposer sur les algorithmes de la plateforme et bénéficier d'optimisations, gages de performances.
- Coder directement un algorithme spécifique dans l'application lorsque ceux offerts par la plateforme ne répondent pas aux exigences.

Sur un mobile, les capacités de calculs sont moindres par rapport à celles d'un PC. La vérification d'un mot de passe peut s'avérer plus longue, diminuant l'expérience utilisateur. L'enjeu est de déterminer le temps minimum nécessaire pour obtenir un niveau de sécurité suffisant tout en offrant une réactivité satisfaisante à l'utilisateur. Ce compromis doit être déterminé lorsque que l'on utilise un algorithme de hachage, tel que celui offert par la librairie b-crypt, qui, malgré sa complexité, sera plus difficile à «casser» si le nombre d'itérations de calcul est élevé.

Malgré leurs failles, les solutions de sécurité mobile se développent. Pour le DSI, l'important reste de trouver le juste milieu entre les possibilités techniques de la plateforme, ses besoins en sécurité et l'expérience utilisateur.



Florian Aeschlimann
Expert technique, Cross Agency



Explosion des menaces mobiles: les failles de dispositifs font apparaître de nouveaux risques.