



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Insécurité des environnements JAVA embarqués

Eurosec 2003

18 Mars 2003

Hervé Schauer

<Herve.Schauer@hsc.fr>

Plan

- x Situation
- x Situation de la sécurité
- x Sécurité du mobile
- x Absence d'intégrité dans le mobile
- x Exemples d'applets malveillantes
- x Conséquences
- x Autres cas : Java dans la SIM et mobile sans JAVA
- x Solutions
- x Conclusion
- x Références et ressources

Situation

- × Nouveaux téléphones mobiles et assistants personnels
 - × Ordinateur + système d'exploitation
 - × Environnement d'exécution, par exemple JAVA
 - × Lien télécom permanent avec GSM/GPRS
 - × Lien réseau local via le PC
 - × Cable série, sans fil (IEEE 802.15)
- × Usage
 - × Equipements encore peu intégrés dans la gestion de parc des entreprises
 - × Usage professionnel quasi-systématique des équipements acquis de manière personnelle

Situation de la sécurité

- x Entre Internet et entreprise
 - x Firewall avec contrôle de contenu
 - x Cloisonnement, authentification, confidentialité
- x Entre Internet et le mobile
 - x Flux HTTP, FTP, SMTP, POP3, IMAP4, ou VPN privé
 - x Pas de système de contrôle de contenu
 - x La sécurité est déportée sur le mobile
- x Le périmètre du S.I. est décidément bien poreux
 - x Pas ou peu de cloisonnement du S.I.

Sécurité du mobile

- x La sécurité normalisée :
 - x Authentification de l'abonné
 - x Chiffrement de la communication
 - x Signature des applets
- x Pas de sécurité normalisée dans le mobile
 - x Pas de garantie d'intégrité sur le 'bac à sable'
 - x Pas de garantie d'étanchéité et de cloisonnement des applications embarquées
 - x Pas de contrôle de conformité à une politique de sécurité des actions des applets reçues
 - x Exemple : envoi de SMS après validation de l'abonné

Sécurité du mobile

- × Conséquences
 - × Les codes de contrôle du bac à sable ne sont pas protégés
 - × Exemple : possibilité de forcer le code de contrôle de la signature d'une applet téléchargée à répondre toujours OK
 - × Il est parfois possible de sortir du bac à sable
 - × Exemple : vidage de la totalité de la mémoire du mobile
 - × Même si l'applet est signée et syntaxiquement correcte, son accès aux ressources internes du mobile la rend très sensible
 - × Exemple : diffusion de l'annuaire de l'abonné

Sécurité du mobile

- × Pas d'évaluation ni de certification de la sécurité des mobiles
- × Pas d'identification fiable d'un mobile
 - × Seule la carte SIM est identifiée et authentifiée
 - × Impossible à un fournisseur de service de proposer son service sur un nombre limité d'appareils validés
 - × Le type d'appareil est indiqué dans l'en-tête de l'IMEI
 - × L'IMEI peut être falsifiable, voir recopiable sur des mobiles non-sûrs

Absence d'intégrité dans le mobile

- x Application : le déverrouillage frauduleux
- x Déverrouillage de la SIM (*desimlockage*)
 - x Accès direct à la mémoire du téléphone par le port d'extention
 - x Altération des données et/ou du logiciel
- x Déverrouiller = accéder et modifier la mémoire du mobile
 - x Modifier le contenu du mobile
 - x Modifier la machine virtuelle jave et son 'bac à sable'
 - x ...

Exemples d'applets malveillantes

- × Simulation du réamorçage du mobile et vol du code d'accès au mobile
- × Connexion de données à l'insu de l'abonné sur un n° surfacturé
- × Suivi géographique de l'utilisateur par SMS
- × Espionnage des appels (émission SMS avec la date et le destinataire de chaque l'appel)
- × Vol du code d'authentification du service bancaire lors de sa saisie
- × Vol de l'annuaire de l'utilisateur
- × Vol de l'ensemble des informations sur l'assistant personnel comme le répertoire
- × Rediffusion de fichiers à contenu payant
 - × Exemple : renommage d'un fichier MP3 en fichier texte pour permettre son renvoi aux autres

Conséquences

- x Vol d'information
- x Atteinte à la vie privée et à la confidentialité des données internes des entreprises
- x Fraudes
- x Escroquerie financière : détournement de fonds
- x Mise en cause des modèles économiques actuels des fournisseurs de service
 - x Musique/Video
 - x Jeux
- x Mobile nouveau vecteur de diffusion de virus

Sans environnement d'exécution

- x Le problème de fond existe déjà sans environnement ouvert et sans JVM
- x Erreurs dans certains appareils
- x Envoi de SMS payants à l'insu de l'utilisateur par un WAP PUSH mal codé
- x Envoi de SMS qui reconfigurent le mobile
 - x Configuration du mobile par l'opérateur
 - x Configuration des cartes PCMCIA 802.11b + GSM/GPRS

JAVA dans la SIM

- × JVM dans la carte SIM
 - × Mémoire et CPU encore plus limités que dans un mobile
 - × Suppression des contrôles habituels
- × Tous les opérateurs ont accès même les petits
- × Risque de blocage définitif de la SIM en cas d'applet malveillante
- × Sécurité encore sous le contrôle des opérateurs
- × Sera l'unique espoir de '*firewall* embarqué', offrant une certaine confiance, dans les mobiles si la carte SIM n'est pas ouverte aux tiers

Solutions ? (1/2)

- × Organiser la sécurité
 - × Schéma de contrôle et de certification constructeur + opérateur + fournisseur de services ?
 - × Exemple : imposer un contrôle du code des applets avant signature, un suivi des anomalies et une réactivité de correction
- × Construire une norme de sécurité des mobiles et imposer leur évaluation + certification
 - × Schéma de contrôle sur l'ensemble des constructeurs ?
 - × Exemple : imposer un contrôle d'intégrité par la SIM sur le logiciel de base du mobile

Solutions ? (2/2)

- × Intégrer la sécurité dans l'infrastructure de l'opérateur
 - × Contrôle des applets avant téléchargement dans l'infrastructure de l'opérateur ?
 - × Contrôle par des tiers prestataires de sécurité ?
 - × Autorisation du téléchargement d'applets que depuis une plateforme agréée : solution pour l'entreprise
 - × Impose un mobile qui n'est pas déverrouillable...
- × Ajouter sur le mobile un système de sécurité comme sur un PC
 - × Déjà de nombreux éditeurs

Conclusion

- x Les téléphones portables et assistants personnels sont un enjeu majeur de la sécurité pour le futur
- x Les constructeurs de mobiles ne semblent pas toujours intégrer la sécurité dans leur vision
- x Les opérateurs sont en phase de réflexion
- x Les fournisseurs de services doivent prendre en compte les risques actuels dans la construction de leurs applications
- x **Sans doute une ouverture trop rapide de nouveaux services sans intégration de la sécurité dans leur élaboration**

Références et ressources

- x Mobile phone Java risks are 'minimal', The Register, 01/10/02
 - x <http://www.theregister.co.uk/content/55/27360.html>
- x Barrer la route aux virus de téléphones portables, La Recherche n°360, 18/11/02
 - x http://www.hsc.fr/ressources/articles/virus_telephones_portables/