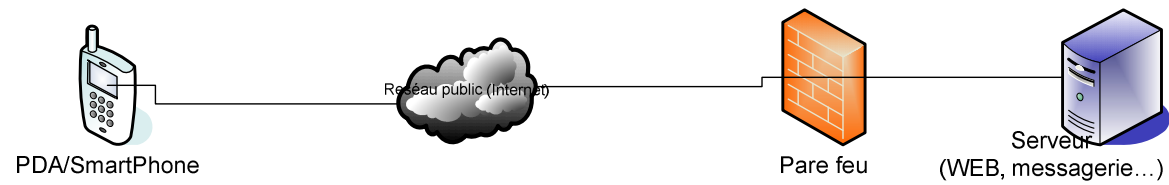




Sécurisation des PDA communicants

Mercredi 15 novembre 2006

- Architecture générale
- Menaces
- Mesures de protection
- Acteurs du marché



- Le terminal (PDA/SmartPhone)
- Le réseau d'accès
- Le réseau d'entreprise

- Accès non autorisé au terminal
- Accès aux données du terminal :
 - Agenda
 - Contacts
 - Taches
 - Mails
 - Fichiers
- Altération du terminal
 - Virus
 - Chevaux de troie

- Grands classiques :
 - Disponibilité
 - Confidentialité
 - Intégrité
 - Authenticité

- Accès non autorisés :
 - Vol d'informations
 - Altération d'informations
 - Utilisation frauduleuse

- Introduction de virus/chevaux de Troie

- Les PDA créent des portes ouvertes sur le SI
- La sécurisation des accès au réseau d'entreprise est généralement primordiale par rapport à celle du terminal.

- Cette sécurisation implique la mise en place d'une authentification sur les accès
- Cela implique la transmission de cette authentification de façon sécurisée entre le terminal et le SI
- Il faut mettre en place une authentification réelle sur les terminaux (généralement des mots de passe triviaux lorsqu'ils existent).

- Utilisation de certificats/mot de passe sur les accès. Problématique de la sécurisation de l'accès aux certificats (et clés associées)
- Sécurisation du transport : VPN IPSEC, VPN SSL, Tunnels SSL
- Authentification forte sur le PDA : biométrie, carte à puce, mot de passe long (pas très viable)

- Penser à mettre un firewall
 - Entrant (évident) : filtrage des flux, détection des attaques connues...
 - Sortant : pour limiter les effets d'un cheval de Troie
- Mettre un anti virus (après l'éventuel chiffrement)

- Mise en place de la sécurisation des flux
- Moyens techniques : VPN IPSEC, VPN SSL, Tunnels SSL.
- Technologies souvent lourdes pour des terminaux mobiles
- Les VPN IPSec existants sont généralement fonctionnellement limités
- Tunnels SSL = SSL sur le protocole applicatif de base (POP3->POP3S...)
- Permet généralement d'assurer également la fonction d'authentification pour le SI

- Chiffrement des données sensibles (de préférence de façon transparente)
- Anti-virus (tant pour le terminal que pour les postes/serveurs auquel il se connecte)
- Effacement sécurisé des données sensibles (attention aux mémoires)

- Encore plus contraignant que sur PC
- Souvent aucune authentification configurée
- Mot de passe (réel) :
 - dur à saisir (pas toujours de vrai clavier),
 - long pour voir juste un RDV
- Biométrie : lié au terminal, qualité/sécurité très variable
- Carte à puce : Problème du lecteur (il existe des lecteurs bluetooth [voir la sécurité])
- Carte SIM : Simple, permet un SSO téléphone/terminal, détournement d'une fonction.

- ControlBreak (SafeBoot)
- Crédent (assez lié à HP)
- MSI/ARKOON
- PointSec
- Utimaco

- Société de service et éditeur de logiciels spécialisé dans la sécurité logique et les réseaux
- Produits : Gamme Security BOX®
- Actionnaire : ARKOON (100%)

- Adresse : 3 place Renaudel
69003 LYON
Tél : 04 78 14 04 10 Fax : 04 78 14 04 11
Web : <http://www.securitybox.net>

- Philippe PERRET
Directeur technique
philippe.perret@msi-sa.fr