



Sécurité & mobilité

Chef de Projet : Patrick Ragaru

Assistants : Jean-Paul Humeau, Philippe Perret

18 janvier 2006

- Introduction
- La sécurité des PC portables
- La sécurité des échanges avec les PDA
- Le cas des virus sur PDA
- Conclusion
- Questions / réponses

- Introduction
- La sécurité des PC portables
- La sécurité des échanges avec les PDA
- Le cas des virus sur PDA
- Conclusion
- Questions / réponses

Mobilité : quelques définitions

- La mobilité « *interne* » correspond à des personnes appelées à se déplacer fréquemment sur un même site entre des bureaux et des salles de réunion, ou sur des sites très étendus.
- Le concept de mobilité « *extra entreprise* » correspond à la capacité d'un utilisateur à se connecter aux ressources du SI de l'entreprise en s'affranchissant des contraintes de sa localisation géographique.
- Les technologies sous-jacentes à la mobilité sont communément appelées WLAN (LAN sans fil).

- Deux modes pour la mobilité « extra entreprise » :

- Mode connecté :

un accès permanent (en temps réel ou quasi temps réel) avec le SI

Exemple : application de géo-localisation d'une flotte de transporteurs

- Mode synchronisé ou déconnecté :

le besoin d'accès à distance à l'information ne nécessite pas d'accès permanent au SI. Les informations sont mises à jour à chaque connexion au SI

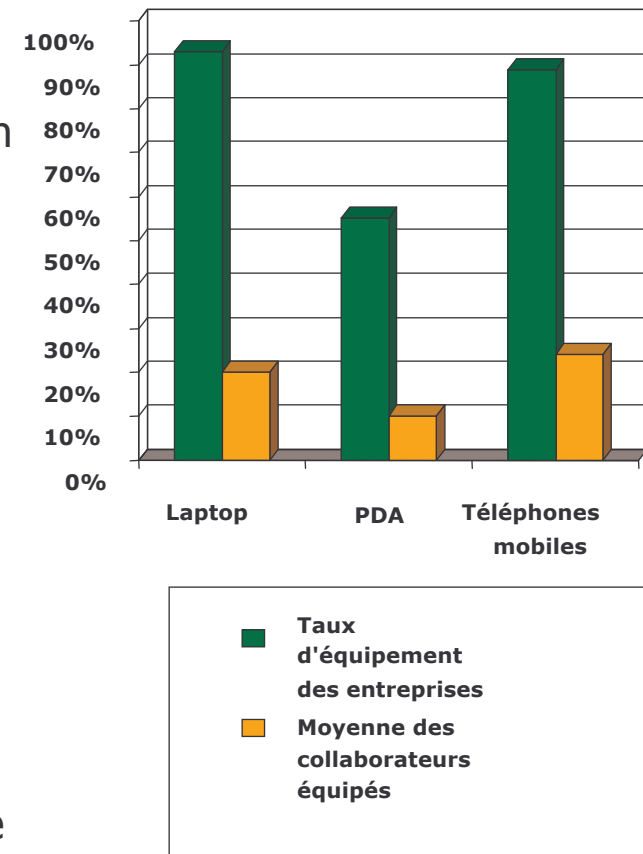
Exemple: une force de vente qui récupère ou met à jour périodiquement des informations commerciales.

- Réaliser des gains de productivité (35%),
- Obtenir une meilleure réactivité des collaborateurs, accompagner la GRC (20%)
- Améliorer le confort de travail « free sitting » & disponibilité « *keep connected anywhere* » (18%).
- La réduction des coûts n'est pas une priorité (2%)

étude CESMO – décembre 2005

Quelques tendances 2005

- Près de 12 millions de salariés itinérants en France fin 2005
- Hausse de 12% du taux d'équipements mobiles en entreprises en 2005 par rapport à 2004 (CESMO).
- Une entreprise sur trois a déjà mis des applications au service de la mobilité et la tendance est à l'augmentation pour 2006
- En 2005 plus d'un accès distant sur cinq est réalisé au travers d'une solution sans fil :
 - 38% des entreprises déclarent avoir l'intention d'investir dans les 2 ans dans une solution de mobilité sans-fil (IDC)
 - 90% des entreprises prévoit de maintenir ses investissements dans le domaine et près de la moitié (44%) compte les augmenter en 2006.
- Le PIM (annuaire, agenda et messagerie) reste le principal besoins.
- Les utilisateurs s'appuient sur le GSM (52%) et le GPRS (60%) mais basculent peu à peu sur le Wifi (51%) dès qu'il est disponible :
 - L'UMTS (15%) et l'EDGE (11%) font une timide entrée



- Pour le RSSI, la mobilité est un enjeu comparable à l'avènement d'Internet :
 - Connectivité accrue au SI de l'entreprise,
 - Nouveaux risques, nouvelles menaces, ...
 - Multiplication des équipements par individus,
 - Moyens de connexions hétérogènes pour un même équipement,
 - Risque d'utilisation de terminaux non homologués, et non déclarés,
- Risques de contournement du périmètre de défense « traditionnel »
- => Nécessité d'adapter la PSSI aux nouveaux enjeux de la mobilité !

- Introduction
- Mobilité : la sécurité des PC portables
- Mobilité : la sécurité des PDA
- Le cas des virus sur PDA
- Conclusion
- Questions / réponses

- Traiter les menaces spécifiques aux PC portables en situation de mobilité
 - => Ne traite pas en détails des menaces « classiques » qui s'appliquent aussi aux postes de travail fixes.
 - => Ne traite en détails pas des menaces liées aux réseaux et aux protocoles de communication (exemple : sécurité Wifi, UMTS)
- Les menaces :
 - Vol / perte des portables
 - Panne, destruction de matériel
 - Virus, vers et autres « malwares »
 - Interception des échanges, intrusions sur le SI

- Risques : perte d'information, atteinte à la confidentialité, intrusions, etc.
- « *La taille des disques durs a enflé, et la masse des informations stratégiques embarquées a suivi la même courbe* »
- Les mesures de protection contre le vol :
 - Verrou « Kensington »
 - Systèmes rendant le portable « inutilisable » ou les données inexploitablees en cas de vol :
 - Contrôle d'accès au boot et au système :
 - Mot de passe BIOS
 - Authentification renforcée – « ce que je sais + ce que j'ai » - (certificat stocké sur carte à puce ou clé USB, etc.)
 - Biométrie (lecteur d'empreinte digitales intégré sur les portables, ...)
 - Chiffrement des données sur le poste :
 - Intégré au systèmes (exemple : EFS)
 - Via des outils spécifiques (Security Box, PGP, Ultimac)
 - Effacement sécurisé des fichiers et du swap
 - Systèmes de contrôle de l'angle de vision
 - Bon sens des utilisateurs nomades (sensibilisation !)



- Le standard TPM (*Trusted Platform Module*) : des puces pour garder les mots de passe en lieu sûr !
 - Puce incluant des capacités de cryptage et de stockage des mots de passe et des clés de cryptage
 - Le TPM est critiqué par des associations de défense de la vie privée qui craignent des dérives :
 - Fonctionnant de manière autonome du système d'exploitation,
 - présence d'un id. matériel unique dans la puce (Pentium III)
 - Supporté par MS Vista et embarqué sur certain portable récents

- PC portable sans disque dur
 - Initiative HITACHI

- Les risques : pertes d'informations, disponibilité
- Les solutions, des PC portables plus fiables et solides :
 - Systèmes « airbag » : détectent les mouvements brusques et arrêtent le disque dur (nombreux modèles récents).
 - Boîtiers plus solides, mousses qui entourent le disque dur ou la mémoire.
 - => Certains constructeurs déclarent assurer une protection contre des chutes jusqu'à 1 mètre de hauteur...
 - Clavier anti-éclaboussure
 - DD en RAID 1
 - Systèmes assurant des sauvegardes automatiques :
 - => accessibles depuis le BIOS, ils permettent de restaurer les données perdues même en cas de corruption du système d'exploitation
 - Sauvegarde à distance des PC portables
- Des caractéristiques à prendre en compte lors du choix d'un matériel ?

Virus, vers, chevaux de Troie et autres malwares, ...

- Les risques : intégrité, confidentialité, ...
- Cette menace *classique* pour les PC fixes est décuplée sur les terminaux mobiles :
 - Infection à l'extérieur du SI (via Wifi, peer-to-peer, etc...) puis infection du SI lors de sa reconnexion au SI de l'entreprise

=> contournement du périmètre de défense de l'entreprise
- Les solutions « traditionnelles » de protection contre les malwares :
 - L'antivirus du poste de travail (à jour !) sur les portables est un minimum
 - Il doit être complété par un pare-feu personnel si le poste est utilisé sur des réseaux externes à l'entreprise (internet, Wifi, etc.)
 - Nombreuses « suites éditeurs » comprenant anti-malware et pare-feu
- Les nouvelles initiatives :
 - Nx-bit / XD-Bit dans les CPU (protéger la mémoire système contre des insertions et des exécutions de code) => non spécifique aux portables
 - Procédure de SAS à la reconnexion interne sur le SI :
 - Sur la base de 802.1X
 - Initiatives CISCO NAC (Network Access Control) et MS NAP (Network Access Protection)

- Menaces : confidentialité, intégrité, intrusions, ...
- La fin des connexions filaires (RTC/RNIS,...) :
 - Internet
 - HotSpots Wifi
 - 2/2.5/3G; Wifi : abonnement data des opérateurs
- Quid de la sécurité sur le réseau de transports (UMTS, Wifi) ?
- Et reste la problématique de sécurité des accès au SI !
- Les solutions :
 - Les pare-feu personnels
 - Les solutions VPN :
 - SSL vs. IPSEC
 - OWA, ...
 - Authentification forte des PC portables lors de l'accès au SI
 - token,
 - Carte à puce & certificat (TPM !)



L'utilisateur nomade, ..., le maillon faible ?

- 55% des utilisateurs de portables précisent que leur entreprise dispose d'une politique de gestion d'usage d'Internet sur ordinateurs portables,
- 30% des entreprises se contentent d'une adhésion écrite à la PSSI, mais :
 - la moitié des employés reconnaissent avoir laissé des tiers N'APPARTENANT PAS à l'entreprise utiliser leur pc portable.
 - 20% d'entre eux avouent ne pas savoir précisément qui a pu se servir de leur portable.
 - 86% reconnaissent télécharger des softs n'ayant absolument aucun rapport avec leur activité professionnelle (et ce généralement en dehors du bureau)
 - 42 % des utilisateurs ont déjà utilisé ces portables sur des réseaux peer-to-peer,
 - 74% des « téléchargeurs » ne regardent pas les conditions d'utilisation des logiciels
 - ⇒ 15% des utilisateurs découvrent des softs sur leur portable
- L'utilisation de terminaux mobiles rend plus que jamais nécessaire la sensibilisation des utilisateurs à la SSI

- Introduction
- Mobilité : la sécurité des PC portables
- Mobilité : la sécurité des PDA
- Le cas des virus sur PDA
- Conclusion
- Questions / réponses

-
- Historique
 - Présentation des PDA communicants
 - Synchronisation distante
 - Terminal mobile

- Les téléphones portables (qui permettaient de téléphoner)
 - Ecran une ligne (pas de couleur)
 - Petit répertoire
 - SMS

- Les PDA (qui offraient des fonctions d'agenda, de répertoire, de taches, de calculatrice...)
 - Pas de communications réelles
 - Connexion filaire (série puis USB) avec un PC avec des logiciels et protocoles propriétaires

- Fonctions essentielles des PDA (calculatrice, agenda répertoire...)
- Téléchargement de sonneries
- Appareil photo
- Connexion avec des PC (utilisation comme modem)
- « Haut débit »

- Communications :
 - Infra-rouge
 - Bluetooth
 - GPRS
 - UMTS
- GPS
- Téléphone
- Intégration de fonctions PC (client de messagerie, traitement de texte, tableur, applications spécifiques...)
- Internet

- On arrive donc à :
 - Des téléphones avec des fonctions PDA
 - Des PDA avec des fonctions de téléphone
- Il y a donc convergence
- Création des :
 - SmartPhone
 - PDA communicants
- Techniquement très similaires mais présentation différente

- Un **Smartphone** est un [téléphone mobile](#) couplé à un [PDA](#). Il permet une meilleure gestion du temps grâce à des fonctionnalités agenda/calendrier mais également de la navigation [web](#), de la consultation de courriel, une connectivité à un client de messagerie instantanée, la navigation [GPS](#), etc.
- Un smartphone permet d'installer des applications additionnelles sur l'appareil. Les applications peuvent être développées par le fabricant, par l'opérateur ou par n'importe quel autre éditeur de [logiciel](#). La forte valeur ajoutée d'un smartphone est donc sa logithèque car un logiciel créé, par exemple, pour un Smartphone Windows Mobile ne sera compatible QUE avec les appareils fonctionnant sous ce système d'exploitation.
- **En 2005, seuls 2% des téléphones mobiles sont des smartphones** mais les analystes prévoient d'arriver à 25% d'ici à 2009. C'est pour cette raison que le smartphone est devenu une des grandes orientations stratégiques de [Microsoft](#).

(Wikipedia)

- Téléphonie (utilisation de la sécurité GSM native)
- PDA (Agenda, répertoire, tâches, messagerie...)
- Applications locales
- Terminal mobile

- Plusieurs sources incompatibles (plus ou moins selon les fonctions) entre elles :
 - Symbian (Psion, Motorola, Nokia...)
 - PalmOS
 - Windows Mobile
 - BlackBerry

- Tout en un (téléphone, PDA et « PC »)
- Possibilité de recevoir des emails en tant réel (moins encombrant qu'un portable) :
 - Utilisable en réunion
 - Utilisable au restaurant...
- Le but n'est pas d'échanger des romans : c'est un peu le SMS du riche
- Effet de mode au départ : un VIP sans BlackBerry était « has been »

- Fonctions PDA :
 - Messagerie interconnectée à celle de l'entreprise
 - Agenda interconnecté à celui de l'entreprise
 - Taches interconnectées à celles de l'entreprise

- Applications mobiles
 - Messagerie distincte de celle de l'entreprise
 - Navigation Internet
 - Accès à des applications d'entreprise

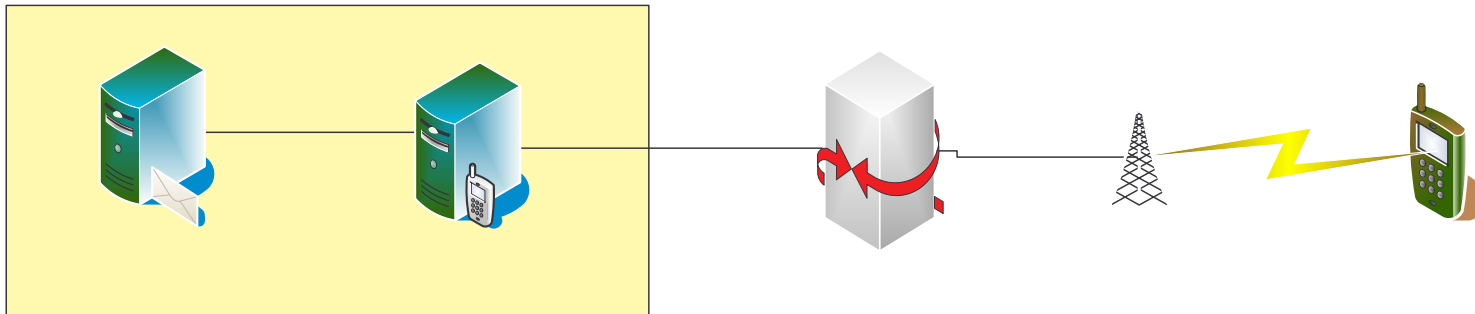
- Principe constant :
 - Synchronisation avec un véritable environnement utilisateur (Notes, Exchange...).

- Push e-mail :
 - Fortement mis en avant par BlackBerry
 - Présent dans les autres environnements

- Assez propriétaire

- Problème des pièces jointes (genre une doc de 300 pages)

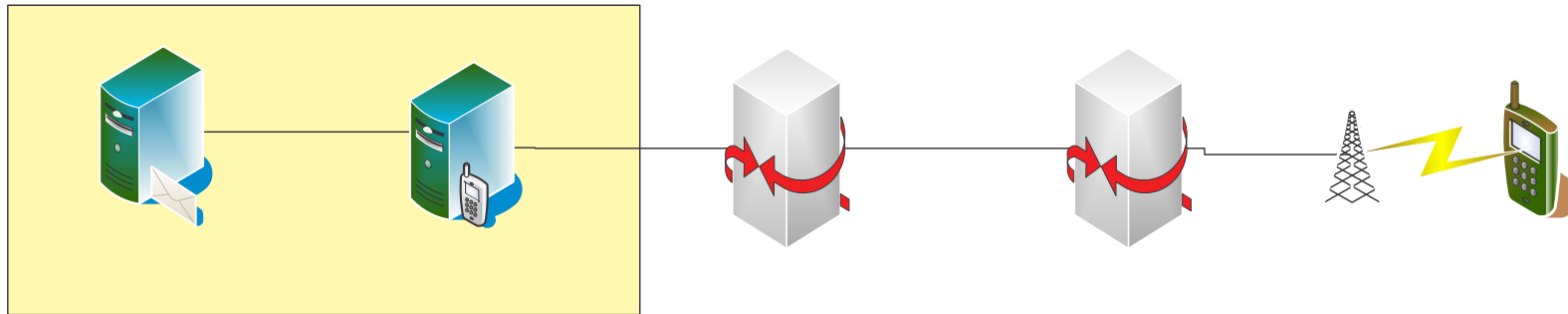
- Interception des échanges PDA-entreprise
- Non-connaissance de l'émetteur de la sortie des informations de l'entreprise :
 - L'émetteur envoie vers un destinataire local (information normalement confinée)
 - Le serveur de messagerie transfert vers le mobile (l'information est sortie)



- Tentative de standardisation (Open Mobile Alliance)
- Nécessité d'une passerelle en entreprise (peut être à l'extérieur pour des petites structures)
- Lien direct avec la passerelle opérateur

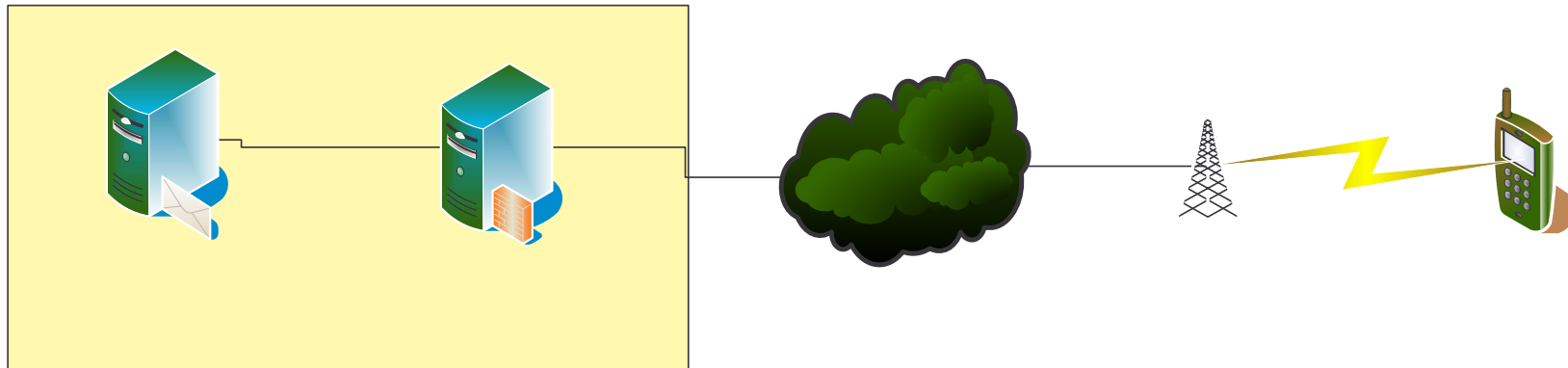
Entreprise

- Chiffrement de bout en bout (256 bits)
 - 256 bits efficaces distribués sans contrôle, il ne faut pas rêver
- Risques d'interception liés à l'opérateur et au roaming (déplacements)



- Schéma propriétaire
- Nécessité d'une passerelle en entreprise (peut être à l'extérieur pour des petites structures)
- Passage par une passerelle intermédiaire (Angleterre, Canada, Singapour)
- Nokia offre également ce mode de diffusion
Entreprise

- Chiffrement de bout en bout (256 bits)
 - 256 bits efficaces distribués sans contrôle, il ne faut pas rêver
- Passage par des passerelles sur lesquelles des interrogations sont fréquemment formulées.
- Analyse sécuritaire par EADS
 - RIM communique beaucoup dessus
 - Aucune conclusion n'a été officiellement publiée par EADS



- Microsoft → simple (ce n'est pas de la pub)
- Ne marche vraiment qu'avec du Microsoft
 - Exchange 2003
 - ISA Serveur (non obligatoire)
 - Windows Mobile

- Echange en SSL pour les synchronisations
- Possibilité d'IPSec
- Pas de passerelle intermédiaire autres que de l'internet
- Effacement à distance du PDA
- Lien donnant des informations générales :

http://download.microsoft.com/download/1/a/5/1a572c42-10b5-469d-9acb-cedd2e634985/WM_Devices_Lifecycle.doc

- Problématique identique à celle des PC (ou autres) portables
- Possibilité d'utiliser du HTTPS et du S/MIME
- Le cas de la messagerie externe est peu réaliste dans le monde de l'entreprise.
- Le PDA est alors un terminal comme un autre

■ Deux possibilités :

- Utilisation d'un accès à des services accessibles depuis Internet (y compris via IPSec ou SSL).
 - Cas standard non spécifique à des PDA et pouvant se confondre à la sécurité d'accès à partir de PC
- Utilisation d'accès mettant en œuvre les passerelles d'entreprise (BES, NBC...)

- Concerne les plates-formes « propriétaires »
- Microsoft utilisant l'internet n'entre pas dans ce cas.
- Applications réalisées en Java (spécification Java Mobile)
- Les fonctions de sécurité sont identiques à l'utilisation en mode PDA

- Arrivée de PDA communicants dans les entreprises
- Problème de la maîtrise de la sécurité par les RSSI (dur d'imposer des choses à des VIP)
- Il convient de faire très attention à ces outils surtout pour les fonctions de messagerie (la sortie d'information n'est plus une action délibérée)

- Introduction
- Mobilité : la sécurité des PC portables
- Mobilité : la sécurité des PDA
- Le cas des virus sur PDA
- Conclusion
- Questions / réponses

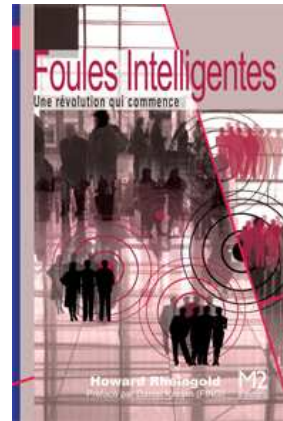
- La croissance inéluctable des PDA's
 - Les « Smart mobs » d'Howard Reingold
 - L'intelligence ambiante de Rafi Haladjian
- Connecté partout et tout le temps (à haut débit)
- Et les virus dans tout ça ?
- L'état de l'art de la défense

La croissance inéluctable des « PDA's »

- Les foules intelligentes
Howard Reingold

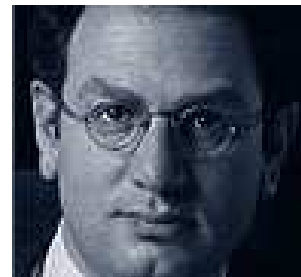
Préfacé par Daniel Kaplan
(FING)

Titre original : SmartMobs



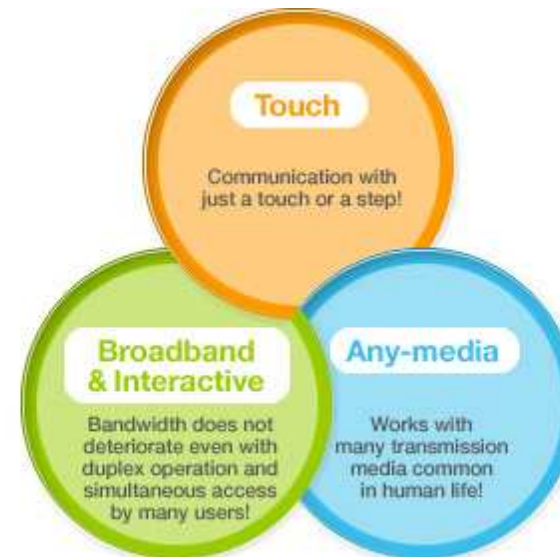
- L'intelligence ambiante
Rafi Haladjian

Du Minitel au Wifi en passant par Ozone, Violet et Nabaztag



■ Trois temps

- L'homme et ses périphériques
- Les objets au service de l'homme
- L'homme modifié →→→→

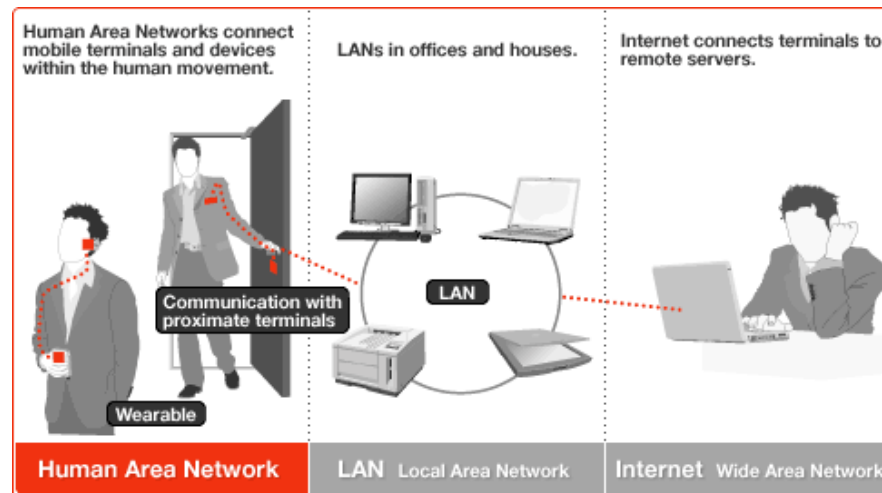
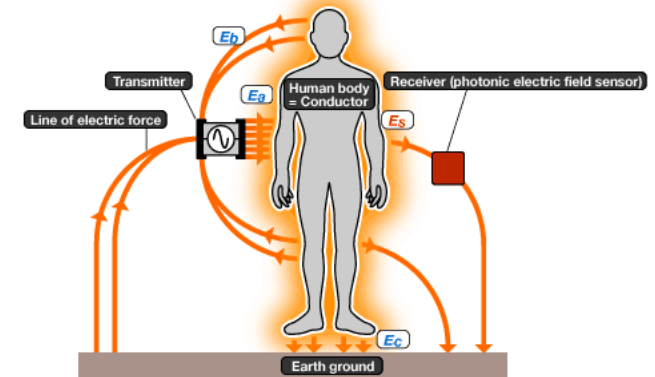
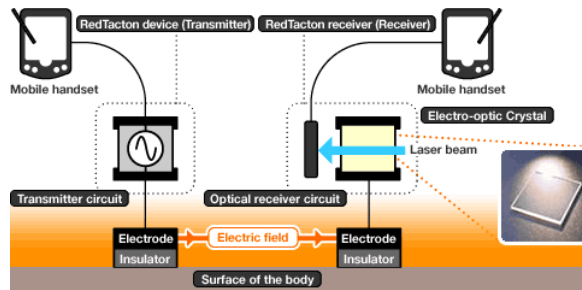
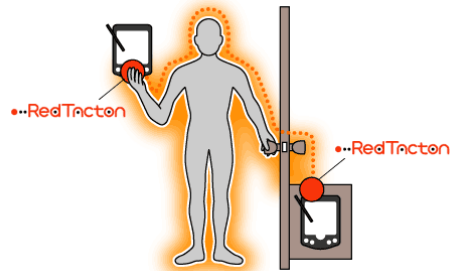


Red Tacton

<http://www.redtacton.com>

Les « Human Area Networks »

- Ils sont déjà là !



<http://www.redtacton.com/en/info>

Could future computer viruses infect humans?

Question posée à Kevin Warwick Professeur de cybernétique
à l'université de Reading

[http://networks.silicon.com/webwatch/0,39024667,39125887,00
.htm](http://networks.silicon.com/webwatch/0,39024667,39125887,00.htm)

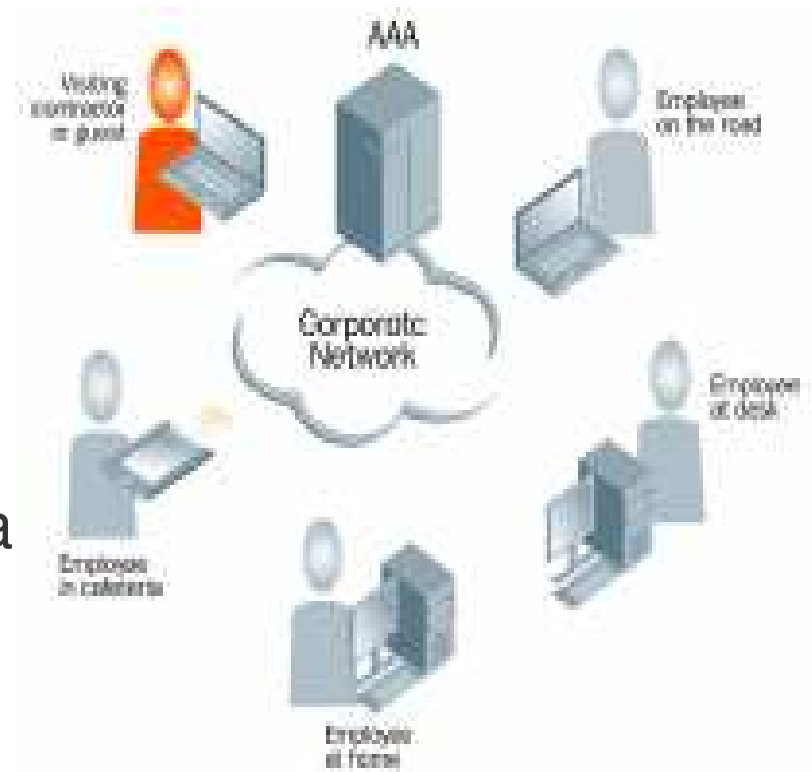
En attendant la réponse...

- Les vecteurs de contamination :
 - Email infecté : PDA en connexion internet (filaire ou Wifi)
 - Synchronisation avec un PC infecté
 - Transfert de fichier infecté via port IR depuis ou vers un autre PDA
 - Téléchargement de fichiers infectés sur Internet

- La connexion Internet (GPRS, Wi-Fi...)
 - Virus, vers et programmes troyens guettent → incidence sur le SI
- PDA et Smartphones servent plutôt de vecteurs de transmission aux virus que de cibles finales.
- PDA cheval de Troie :
 - Une fois le PDA connecté au réseau de l'entreprise (WLAN, Bluetooth, etc.), le code malicieux agit en toute quiétude.
 - Il peut, par exemple, collecter des données sur l'entreprise, les stocker temporairement sur le PDA, et les émettre de nouveau une fois le PDA connecté à internet...

Le réseau d'entreprise reçoit :

- Les collaborateurs sur la route,
- Les collaborateurs à leur bureau
- Les collaborateurs à la maison
- et, même, les collaborateurs qui jouent avec leur PDA à la Cafétéria



■ Antivirus, évidemment !

Indispensable : Protéger le PDA par un antivirus mais :

- Le choix d'un antivirus est plus difficile pour un PDA que pour un ordinateur standard : plate-formes multiples.
 - Le mode de MàJ proposé par l'éditeur doit être compatible avec le mode d'utilisation du PDA :
 - . copie des signatures par l'utilisateur,
 - . console d'administration antivirus d'entreprise
 - . mise à jour via internet.
- Les éditeurs ont leur solution PDA : Trend Micro, Secuser, Symantec, Kaspersky Labs, etc

■ Chiffrement

- Efficace mais complexe : PDA, smartphones, ordinateurs portables.

■ Applets Java et contrôles Active X

- Java intégré à plus de 94 millions de téléphones cellulaires dans le monde à ce jour.

Nom	Type	Origine	Plate-forme	Niveau de risque
Cabir	Virus	49 A	Symbian	Pas destructeur, dans la nature
Duts	Virus	49 A	Pocket PC, Windows CE	Pas destructeur, Prototype
Phage	Virus	Inconnue	Palm OS	Destructeur, rare
Brador	Cheval de Troie	Auteur inconnu, Russie	Pocket PC, Windows CE	Vol d'informations
Mosquito	Cheval de Troie	Sodom Bin Loader, pseudo inconnu à ce jour	Symbian	Dialer, SMS surtaxés
Skulls	Cheval de Troie	Inconnue	Symbian	Toutes le fonctions sont désactivés sauf les appels vocaux

D'après Mikko Hypponen directeur de la recherche F-Secure et Vincent Gullotto VP recherche Mac Afee – ZDNet France

- Chrys Rouland responsable technique chez ISS :
 - La VoIP devient un nouveau champ d'investigation pour les Cyber pirates avec le Spam over IP (SPIP)
 - Windows CE et Symbian (60% des PDA's) constitueront les cibles privilégiées des vers.
- Pour ISS, les mesures prises pour protéger les données confidentielles des abonnés. L'arrivée du WiMax mobile devrait attirer les cyber pirates de tout poil.
- Les fichiers JPG,PDF,DOC, XLS mal protégés par les opérateurs constituent des cibles privilégiées.

Source Christophe Lagane VNUnet.fr - janvier 2006

- Tiré de : Six Strategies for Defense-in-Depth
 - S1 : Authentifier et autoriser tous les utilisateurs du réseau
 - S2 : Utiliser les VLANs pour séparer les trafics et assurer une sécurité au niveau le plus fin,
 - S3 : Utiliser le système des firewalls pour assurer la granularité de sécurité visé
 - S4 : Mettre en place le cryptage pour assurer la sécurité du réseau
 - S5 : Identifier les menaces contre l'intégrité du réseau et apporter les corrections nécessaires
 - S6 : Inclure les points terminaux dans la charte de sécurité

■ Contrôler et auditer souvent

- Auditer l'espace radio de la société
- Vérifier et valider le niveau de sécurité des systèmes mobiles existants, mis en place par les utilisateurs eux-mêmes ou par l'entreprise.
- Assurer le suivi des solutions de mobilité existantes pour garantir qu'elles répondent aux objectifs de l'entreprise, en termes de performances et de sécurité..

■ Un problème de comportement des Hommes

- À l'origine, les PDA ont été introduits au sein de l'entreprise par les utilisateurs. Sans le savoir, ils ont également introduit les risques associés à leur utilisation.
- Il est nécessaire d'opérer et de répéter la sensibilisation aux risques.

- Introduction
- Mobilité : la sécurité des PC portables
- Mobilité : la sécurité des PDA
- Le cas des virus sur PDA
- Conclusion
- Questions / réponses

- **Spécificités d'un projet de mobilité:**
 - La diversité des intervenants : utilisateurs, ingénieurs télécoms/réseaux/système, propriétaires des ressources du SI, opérateur, RSSI, plus que dans autres projets un dysfonctionnement de l'un ou de l'autre de ces spécialités impacte la perception de la QoS.
 - Le contexte technique est atypique : devices hors contrôle de la DSI, utilisateurs en mouvement, réseaux publics
 - Risque fort d'inadéquation de la PSI au projets de mobilité

- Adapter la PSI à la mobilité:
 - Par exemple définir le comportement type avec des Pocket PC ou des smart phones
 - Adapter les profils utilisateurs à la mobilité
 - Durcir les dispositifs : SAS de décontamination, forçage des mises à jour en mode déconnecté du SI, etc.).
 - Embarquer systématiquement la sécurité dans les terminaux mobiles
 - Proposer des solutions sécurisées de mobilité uniquement quand cela est nécessaire
 - Prévoir les comportements à risques : remise de messagerie sur des serveur externes n'appartenant à la société

- Les réseaux sont de plus en plus interconnectés et moins maîtrisés en terme de sécurité
- La mobilité est une réalité incontournable, elle correspond à un besoin et son succès est déjà assurée :
 - convergence des attentes des DSI et des utilisateurs
 - disponibilité des technologies de transport et de sécurité
 - => la sécurité n'est plus un frein à la mobilité
- Les risques en terme de sécurité sont liés au manque d'encadrement des projets qui sont souvent initiés en dehors des méthodes internes
- Le besoin essentiel est encore la messagerie mais ce n'est qu'une étape vers un accès total vers le SI

- Questions / réponses

- Patrick RAGARU

XS pôle sécurité - Associé

pragaru@xs-polesecurite.fr

www.xs-polesecurite.fr

- Philippe PERRET

Security Box - Directeur Technique

philippe.perret@msi-sa.fr

www.securitybox.net

- Jean-Paul HUMEAU

JPH Consult

jphumeau@jphconsult.net

www.jphconsult.net