



Observatoire  
de la Sécurité  
des Systèmes  
d'Information  
et des Réseaux

[www.ossir.org](http://www.ossir.org)

# Mobilité et sécurité

CIO Perspectives

**Forum mobilités  
DSI restez connectés !  
20 janvier 2005**



**Hervé Schauer**

<Herve.Schauer@hsc.fr>

- Association loi 1901, fondée en 1996
  - 3 groupes de travail aux réunions mensuelles
    - Groupe de travail Sécurité Unix et Réseaux créé en 1987
    - Groupe de travail Sécurité Windows créé en 1996
    - Groupe de travail RESIST à Toulouse créé en 2001
  - Environ 30 adhérents personnes morales et 50 individuels
  - Environ 2800 abonnés aux listes électroniques
- Préoccupations
  - Les **techniques** liées à la sécurité des Systèmes d'Informations
    - Comprendre "comment ça marche"
- Conférence annuelle JSSI : Journée de la Sécurité des SI
  - Mardi 10 mai 2005 : « Protection des nouvelles frontières de l'entreprise »



- Contexte du DSI
- Périmètre du système d'information (SI) d'entreprise
- Outils de la mobilité et périmètre du SI
- Politique de sécurité
- Vol de l'équipement
- Technologies de mobilité et sécurité
  - Bluetooth, WiFi, GSM
- Recommandations
- Conclusion
- Références, remerciements et ressources



- Gérer le quotidien et accroître la productivité interne
- Supporter une foule d'anciennes applications et intégrer des applications nouvelles
- Ouvrir sans arrêt le système d'information sur l'extérieur sans nuire à celui-ci en interne
- Répondre aux exigences des métiers en matière de nouvelles technologies et d'hétérogénéité et développer la cohérence du parc informatique
- Se justifier économiquement
  - Réduire les coûts, calculer des ROI, se transformer en centre de service, ...
- **⇒ La sécurité n'est pas toujours une priorité**
- **⇒ Il faudra y penser avec la mobilité**



- Il y a toujours :
- Un espace dont je suis responsable
  - Le système d'information (SI) de l'entreprise
- Un espace dont je ne suis pas responsable
  - Le reste du monde
- Il existe et existera toujours un **périmètre** entre les deux
- J'applique la **politique de sécurité** de mon entreprise dans le SI et sur ce **périmètre**



- Il semble difficile de se passer de la notion de sécurité périmétrique
  - Même si la notion de périmètre à des limites
    - La maîtrise des canaux de communication
    - L'utilisateur
    - Les équipements nomades et ouverts
  - Même si le périmètre est poreux



- Un commercial s'achète un Palm
- Un ingénieur reçoit en cadeau une clé mémoire USB
- Un financier s'achète un Blackberry
- Un responsable utilise un téléphone portable Nokia
- Une secrétaire écoute de la musique sur un iPod
- Chacun a un ordinateur à la maison
- La majorité d'entre nous ont un ordinateur portable
- Ces équipements sont-ils dans le périmètre ou hors du périmètre du SI ?



- Les données sur ces outils de la mobilité sont les données de l'entreprise
  - La base des clients est dans l'ordinateur portable, dans l'assistant personnel, dans le téléphone portable, dans la clé USB, ...
- L'usage des outils de la mobilité est au moins en partie professionnel
- Ces outils sont à la frontière du SI, mais dans le SI, dans son espace de responsabilité
  - Responsabilité n'est pas entièrement déléguable à l'utilisateur
    - Déléguer entièrement la responsabilité aux utilisateurs → les faire fuir



- Ce qui est dans le périmètre est dans votre gestion de parc
- **Donc j'applique ma politique de sécurité :**
  - Une politique de protection du système d'information de l'entreprise
    - Une organisation, un service de support, des procédures d'alerte, un inventaire temps réel du parc connecté
    - VPN (tunnel chiffré et authentifié)
    - Contrôle d'intégrité et mise en quarantaine avant la reconnexion au réseau d'entreprise
      - Que cela soit à distance ou en local
      - Qu'est-ce que cela change que je me connecte par le tunnel chiffré ou sur le réseau local ?
  - Une politique de protection locale du nomade ou mobile lui-même
    - Firewall + Anti-virus
    - Chiffrement des données
    - Maintien à niveau des moyens de protection lorsque le nomade est à l'extérieur



- Le vol du matériel est très courant
- De plus en plus de voleurs ont compris que les données sur l'équipement peuvent avoir plus de valeur que l'équipement lui même
- La protection des données sensibles en cas du vol de matériel est absolument indispensable



- Nomadisme : connexion au SI par à-coup
- Mobilité : connexion au réseau permanente
- VPN : permet d'établir un certain niveau de confiance pour la connexion du nomade au SI d'entreprise depuis un réseau qui n'est pas de confiance
- État de la sécurité de quelques technologies
  - Messageries universelles
  - Bluetooth
  - WiFi
  - GSM
  - Système d'exploitation



- Beaucoup d'outils utiles à la mobilité sont des systèmes de contournement de la sécurité sur le périmètre :
  - Courrielwebs (*webmails*)
  - Messageries "universelles"
    - Sprint PCS Business Connection : Ré-encapsulation de TCP/IP sur HTTP, serveur central chez Sprint
    - Lotus Notes : Protocole propriétaire sur TCP/IP, serveur central dans l'entreprise
    - Ipracom : Protocole propriétaire en UDP sur IP ré-encapsulé sur HTTP sur TCP/IP, pas de serveur central
    - Enetshare : XMPP, XML et Webdav sur HTTP sur TCP/IP, serveur central dans l'entreprise
    - Blackberry : Protocole propriétaire chiffré traversant systématiquement les serveurs sous le contrôle de Blackberry
  - Messageries instantanées



- Les **lacunes** des implémentations de Bluetooth sont à la portée de tous
  - Pas d'échange de secret partagé (pas de phase de *pairing*) pour de nombreuses fonctions
    - Échange de carte de visite
    - Envoi de messages
  - Et pas de demande de confirmation à l'utilisateur
    - Lecture ou effacement du répertoire ou du calendrier
  - Marche quand le téléphone a Bluetooth activé, et qu'il est en mode visible (ou découvrable)
- Pas de cas d'usage du téléphone (voix ou GPRS) via bluetooth sans secret partagé
  - Sur tous les téléphones que nous avons testés



- HotSpot : point d'accès à l'Internet
  - Tout le monde écoute tout le monde
  - Fausse borne et attaque du VPN
- En entreprise



- Les **lacunes des réseaux GSM** ne constituaient pas des risques significatifs ou généralisés à l'ensemble des utilisateurs
  - Absence de chiffrement entre la borne (BTS) et l'opérateur
  - Attaques sur le chiffrement entre le téléphone portable et la borne
  - Fausses bornes
- Difficile à mettre en oeuvre, coût et compétence élevés
  - Fraudes, surfacturation GPRS, absence d'authentification mutuelle dans l'itinérance, vulnérabilités des équipements, etc
- Concernent les opérateurs eux-mêmes



- Abandon d'une partie de l'infrastructure opérateur aux clients
  - Écoutes et usurpations
  - Fausses bornes
- Attaques accessibles à une large population



- Opportunités de combinaisons d'attaques
- Utilisation des lacunes de Bluetooth ou du WiFi puis du système d'exploitation
  - Intrusion du PC et vol de fichiers lorsque l'on travaille dans le TGV par exemple



- Intégrer la sécurité au départ des projets
- Les compromis demeurent rares : la sécurité n'est pas un frein à la mobilité
- Intégrer la notion de 24h/24h concommittante à la mobilité
- S'organiser pour la sécurité dans la mobilité



- Établir des procédures réalistes
  - Fournir aux employés les moyens de protéger les données sur leurs équipements par leur chiffrement
  - Autoriser et responsabiliser lors des usages mixtes personnels/professionnels
  - Interdire la duplication des données de l'entreprise sur les périphériques non déclarés, et ceux déclarés comme connectés mais strictement à usage non-professionnels
    - iPod
  - Une fois qu'un système souple et performant est opérationnel, mettre en oeuvre des sanctions qui ne permettent pas les passe-droits et la pression
    - Usage d'un ordinateur personnel lorsque son laptop professionnel tombe en panne ou est volé



- Gérer des moyens de connexions hétérogènes
  - Le même PC portable est tantôt connecté au réseau d'entreprise :
    - Dans son bureau sur le réseau filaire
    - Dans la salle de réunion sur le réseau sans fil
    - Via l'accès Internet ADSL de la maison
    - Via une carte GPRS ou UMTS dans le train
    - Via un HotSpot dans un aéroport
  - L'assistant personnel sera connecté en plus
    - Via une liaison Bluetooth ou un cable série USB sur le PC de bureau
  - Idem pour un téléphone portable



- Accepter de gérer et gérer des plates-formes hétérogènes
  - Exemple : fournir de quoi chiffrer ses données pour tous les types d'assistants personnels
    - PalmOS, Symbian, Windows CE, etc
  - Sécurité  $\longrightarrow$  diversité
- Accepter d'intégrer dans le SI de l'entreprise des équipements choisis, achetés et appartenant au collaborateur



- La sécurité n'est pas un frein à la mobilité
- La mobilité est possible car elle se conçoit en toute sécurité
- La mobilité sans la sécurité est une lourde erreur
  - Peut-être à l'avenir une faute

## Questions ?

[Herve.Schauer@hsc.fr](mailto:Herve.Schauer@hsc.fr)

[www.ossir.org](http://www.ossir.org)



- GSM Interception, Lauri Pesonen, Helsinki University, 11/99, <http://www.geocities.com/clubkefia/gsmintercept.htm>
- GPRS from IP security point of view, Stéphane Aubert, HSC, 06/01, <http://www.hsc.fr/ressources/presentations/gprs/>
- Insécurité des environnements JAVA embarqués, Hervé Schauer, HSC, 03/03, <http://www.hsc.fr/ressources/presentations/eurosec03/>
- GSM and 3G Security: on-the-field experiences, Raoul Chiesa & Emmanuel Gadaix, 03/04, Eurosec04
- Présentations sur la sécurité des réseaux sans fil, <http://www.hsc.fr/ressources/themes.html.fr#wireless>
- Qui peut écouter mon téléphone mobile ?, Reinhard Wobst, 03/04, Hakin9 n°1, <http://www.haking.pl/fr/>



## Remerciements

- Franck Davy, Nicolas Jombart, Thomas Seyrat et Alain Thivillon pour leurs contributions
- Denis Ducamp, Guillaume Lehembre, et Jean Olive pour leur relecture et commentaires



- Société de conseil en sécurité informatique depuis 1989
- Prestations intellectuelles en toute indépendance
  - Pas de distribution, ni intégration, ni infogérance, ni régie, ni investisseurs
- Prestations : conseil, études, audits, tests d'intrusion, formations
- Domaines d'expertise
  - Sécurité Windows/Unix/embarqué
  - Sécurité des applications
  - Sécurité des réseaux
    - TCP/IP, PABX, réseaux opérateurs, réseaux avionique, ...
  - Organisation de la sécurité
- Certifications
  - ProCSSI, CISSP, BS7799 Lead Auditor



- Sur **[www.hsc.fr](http://www.hsc.fr)** vous trouverez des présentations sur
  - Infogérance en sécurité
  - Sécurité des réseaux sans-fil
  - Sécurité des SAN
  - Sécurité des bases de données
  - SPAM
  - BS7799
  - etc
- Sur **[www.hsc-news.com](http://www.hsc-news.com)** vous pourrez vous abonner à la **newsletter HSC**

