



## EDITORIAL

### EDITORIAL

p1

### AGENDA

p1

### ACTUALITES

p2

### ZOOM

➤ L'audit de conformité

p3

### L'ESSENTIEL

➤ Un point sur la sécurité Bluetooth

p5

Les entreprises ne sont pas épargnées par les attaques informatiques. Même dans un passé récent, certains gouvernements ont été des cibles. Ainsi l'Estonie a subi en avril 2007 une attaque d'envergure visant les réseaux du gouvernement, des banques et des médias. Cette attaque est intervenue directement après que les Estoniens aient décidé de retirer du centre de Tallinn un monument à la gloire de l'Armée Rouge. Cette affaire a, semble-t-il, eu deux conséquences : premièrement, la création d'un "Centre d'excellence de l'Otan pour la défense cybernétique" à Tallinn par l'OTAN, deuxièmement, le déclenchement en France d'une volonté de se doter de moyens renforcés.

Ainsi, dans l'actualité du mois de juin, après l'arrivée du soleil, on remarquera, en France, la sortie du Livre Blanc sur la Défense et la Sécurité Nationale. La sécurité des Systèmes d'Information est prise en compte, notamment par la création d'une agence dédiée. Preuve que la sécurité logique fait partie intégrante des objectifs de défense de la nation, pour les quinze prochaines années (seulement ?). Comme dans les autres domaines militaires, une stratégie de défense des Systèmes d'Information sera à élaborer de manière exhaustive. Le secteur civil et le domaine militaire se rejoignent de plus en plus dans cette activité sécuritaire.

Pour l'heure et pour mieux comprendre la problématique du contrat et du respect de son contenu, nous vous proposons un premier article sur l'audit de conformité, qui permet de contrôler si les engagements ont bien été tenus.

Le second article s'intéresse aux ondes, pas toujours bien sécurisées, surtout celles utilisées dans le transport de l'information sur des petites distances. Il sera ici fait état de l'analyse des vulnérabilités du protocole Bluetooth.

Bonne lecture à tous...

## AGENDA

### Eurosec' 2008 - Paris le 18 septembre 2008

Le Forum EUROSEC est la Conférence Européenne de référence sur la sécurité des Systèmes d'Information.

Pour la 19<sup>ème</sup> année consécutive, vous êtes invité à venir confronter vos expériences et vos attentes en matière de sécurité du SI, sur chacun des volets managérial, fonctionnel, humain, technique et scientifique.

➤ Plus d'infos : <http://www.forum-eurosec.com/>

### HACK.lu 2008 - Luxembourg du 22 au 24 octobre 2008

Cette convention internationale sur trois jours a pour objectif de réunir différents acteurs de la sécurité du SI. Les thèmes abordés seront :

- la sécurité liée au Système d'Information ;
- le respect de la vie privée ;
- les technologies de l'information dans ses implications culturelles et techniques au sein de la société.

➤ Plus d'infos : <http://www.hack.lu>



## ACTUALITÉS

### **S**elon une récente enquête du CLUSIF, les entreprises Françaises « délaissent » la sécurité de leur système d'information

Une étude récemment publiée par le Club de la Sécurité des Systèmes d'Information Français (CLUSIF) nous dresse un constat très *sombre* concernant les préoccupations des sociétés Françaises vis-à-vis de la sécurité de leur Système d'Information. En effet, en cas d'incident sur le Système d'Information, une grande majorité d'entre elles n'a pas de *plan B*, ou est incapable d'en évaluer réellement les dégâts.

De plus, bien qu'elles soient pour la plupart couvertes, une grande majorité

de ces entreprises n'exploitent pas leur assurance lorsqu'elles ont été victimes d'incident.

Cette enquête 2008 sur les « Menaces Informatiques et Pratiques de Sécurité en France » a été menée auprès de six cents Responsables de la Sécurité des Systèmes d'Information (RSSI) d'entreprises de plus de deux cents employés.

Cette enquête établit entre autre :

- l'absence d'évaluation des impacts financiers,
- la similitude avec les incidents détectés durant l'année précédente,
- mais aussi, les énormes progrès faits dans le cadre de la réalisation ou de la mise en œuvre des logiciels et procédures.

**Pour en savoir plus :**

<http://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2008.pdf>



### **L**a justice américaine met Microsoft Windows 7 et Internet Explorer 8 sous surveillance

Le Département de la justice américaine (DOJ) va continuer de surveiller les agissements de Microsoft concernant deux futurs produits majeurs : Windows 7 et Internet Explorer 8. C'est ce que rapporte le site américain Networkworld.com, sur la base d'un document juridique publié par le Département de la justice américaine.

En effet, suite au compromis signé par Microsoft en 2002 avec les autorités *antitrusts*, la justice Américaine veut vérifier si ces deux produits, respectent

bien les engagements pris, et si l'éditeur n'enfreint pas la législation locale sur la concurrence.

Cette surveillance sera assurée par un comité technique auquel l'éditeur s'engage à communiquer les informations sur les développements des deux logiciels. Ce comité portera une attention particulière à l'intégration du navigateur (IE : Internet Explorer pour ne pas le citer) dans le système d'exploitation. Il va également vérifier l'exhaustivité des informations communiquées par

Microsoft aux autres éditeurs concernant les protocoles de communication de Windows 7, afin qu'ils puissent développer des logiciels interopérables avec le prochain système.

**Pour en savoir plus :**

<http://www.networkworld.com/news/2008/062008-ms-antitrust.html>



### **T**éléchargement illégal : la riposte graduée validée ?

Le projet de loi Hadopi, ou de « Création et Internet » ou encore « loi Olivennes » (du nom du PDG de la FNAC qui l'a inspirée), est un projet de loi concernant principalement les droits d'auteur sur Internet, élaboré par la ministre de la culture Christine Albanel en 2008.

Ce projet de loi a été examiné par le conseil des Ministres le 18 juin dernier.

Le texte répond, assure Christine Albanel, à une urgence née du « pillage grandissant des œuvres sur les réseaux numériques ».

Sans surprise, une grande majorité des ayants droit du cinéma et de la musique a soutenu en bloc cette démarche et l'a fait savoir par communiqué de presse commun.

Ce texte clairement inspiré par les industries culturelles propose une surveillance des adresses IP sur l'Internet Français et une « réponse graduée » contre le téléchargement numérique illégal.

Toutefois, au titre de la riposte graduée, les internautes sanctionnés pourront voir la durée de suspension de leur abonnement réduite s'ils acceptent une transaction avec la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet (« l'Hadopi »)

La riposte graduée au cœur de cette disposition marque donc ici le retour du judiciaire.

Début juin, Christine Albanel se réjouissait de la validation par le Conseil d'Etat de l'ensemble des options

proposées par le Gouvernement. Cependant, le journal « Les Echos » en date du 17 juin 2008, révèle que le juge administratif aurait en réalité *retoqué* certaines dispositions. Ces éléments vont-ils dans le sens du déluge de critiques, qui a accompagné la présentation du projet de loi ?

Le projet de loi Dadvsi relatif « au droit d'auteur et la copie privée » adopté en mars 2006, et maintenant l'Hadopi relatif « à la riposte graduée » montrent bien la difficulté de légiférer sur des éléments et comportements relatifs aux nouvelles technologies où l'environnement et les modes de vie sont en perpétuelle évolution.

**Pour en savoir plus :**

[http://fr.wikipedia.org/wiki/Loi\\_Hadopi](http://fr.wikipedia.org/wiki/Loi_Hadopi)



## ZOOM

### La démarche de l'audit de conformité contractuelle en matière de sécurité des Systèmes d'Information

L'audit de conformité est une opération de contrôle ; il s'agit d'un rapprochement entre des éléments de provenances différentes afin d'en vérifier à la fois la compatibilité, et éventuellement la couverture des risques résiduels à l'issue de cette analyse. Dans le domaine de la sécurité des S.I., il s'agit bien souvent de prendre comme référence la Politique de Sécurité des Systèmes d'Information (PSSI), qui est elle-même la déclinaison de normes et de lois particulières pour les besoins sécuritaires de l'entreprise. Face à cette référence sécuritaire constituée, il convient de prendre en compte d'autres documents comme les contrats de prestation (de service ou de fourniture), l'organisation et/ou organigramme établi, ainsi que leurs processus et leurs procédures opérationnels. De même, il convient d'examiner la bonne application de ces documents conformément à la politique de sécurité en vigueur.

L'audit de conformité contractuelle peut être de différentes natures. Dans la sécurité logique, l'audit peut porter sur :

- L'analyse comparative des contrats avec les prestataires et les éléments qui leurs sont nécessaires pour se conformer au contrat (comme les procédures applicables dans le cadre du contrat, ...).
- La compatibilité du contrat avec la politique de sécurité de l'entreprise et la vérification d'éventuelles brèches sécuritaires contenues dans le contrat concerné (en raison d'un contrat qui n'est pas conforme aux préconisations établies).
- La conformité du livrable, objet du contrat, avec la politique de sécurité de l'entreprise.
- Etc.

En d'autres termes, il s'agit de vérifier qu'il ne demeure pas d'écart substantiel entre d'une part le contrat et d'autre part les éléments comparatifs (politique de sécurité de l'entreprise, prestations du fournisseur, engagement du prestataire, bonne exécution du contrat sur l'aspect sécurité des Systèmes d'Information, ...).

#### L'objectif

L'intérêt d'un tel audit est d'identifier d'éventuelles différences et de définir les risques liés aux écarts constatés. Ces derniers doivent être listés, puis hiérarchisés selon leur criticité et leur impact pour le demandeur de l'audit. A partir de cette énumération, un plan d'action est à mener pour réduire l'occurrence des principales menaces.

Généralement, les références de sécurité (normes, PSSI, ...) existent à la fois dans l'entreprise et chez le prestataire. Leur concordance d'application n'est pas régulièrement vérifiée.

En l'absence d'une telle concordance, avant la signature du contrat, la phase de négociations entre l'entreprise et son fournisseur permet d'assurer la couverture des risques.

En l'absence d'une telle concordance, après la signature du contrat, les responsabilités de chacun sont proportionnelles aux engagements signés. Elles peuvent être préjudiciables tant pour le fournisseur que pour l'entreprise en matière de répercussions (en terme d'image, de qualité

de service, ...). Les pénalités financières prévues peuvent atteindre des montants très importants, mais en cas de sinistre, l'atteinte à l'image de marque de l'entreprise ne pourra pas être réparée totalement. Aussi, l'entreprise comme le fournisseur ont intérêt à se prémunir contre une telle probabilité d'occurrence. Cependant, dans la pratique, les demandes d'un audit de conformité sont à l'initiative de l'entreprise, en raison du principe de précaution, et permettent d'obtenir une expertise certifiée sur l'objet de l'audit de conformité.

De part son appellation, l'audit de conformité fait partie intégrante des audits de sécurité, puisque tous les aspects (organisationnels, fonctionnels et techniques) sont pris en considération dans cette démarche (par exemple, la norme ISO 27002 qui dans son chapitre 15 prévoit les modalités de mise en conformité).

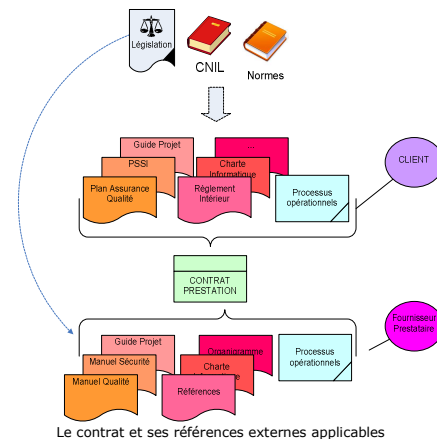
#### La démarche de l'audit de conformité

Le contrat qui lie le fournisseur à l'entreprise est la clé de voûte de la sécurité du système, objet dudit contrat. Car il définit les moyens (et parfois le résultat) pour cette prestation.

C'est également la première étape de l'audit de conformité : l'objet du contrat définit l'étendue des règles de sécurité à respecter (c'est le périmètre de la prestation), et également, les responsabilités des cocontractants pour toute la durée de cette collaboration.

**Attention :** tout traitement inadéquat des éléments de sécurité équivaut, sur le plan contractuel, à une brèche qui peut-être synonyme de risque pour l'entreprise ou le fournisseur.

A fortiori, qu'en est-il en l'absence de tout contrat ?



Plusieurs points peuvent être mentionnés ici (de manière plus ou moins explicite) : la responsabilité commerciale et civile, la protection des données, les assurances, ... ainsi que les clauses de sécurité (confidentialité, ...). L'ensemble de ces clauses représente un niveau global de sécurité. Cependant, les renvois à des documents externes au contrat sont nécessaires (comme les règles de sécurité : PSSI, note d'utilisation de charte informatique, contrôle d'accès pour le personnel extérieur, ...). Aussi, nous nous attacherons à présenter, dans la suite de l'article, les clauses de sécurité habituellement rencontrées.

Les aspects de sécurité correspondent notamment :

- à l'engagement de confidentialité ;
- au traitement et à la conservation des données par le prestataire ;
- aux risques liés aux opérations sensibles pour les besoins de l'activité ;
- aux obligations générales du prestataire de prudence et de vigilance dans le déroulement des actions faisant l'objet du contrat.

S'ils ne sont pas explicitement développés, des renvois à d'autres documents techniques référencés dans le contrat (comme la politique de sécurité, la charte informatique ou bien encore les règles de l'établissement, ...) sont nécessaires pour assurer un niveau suffisant en matière de sécurité.

Toutefois, la difficulté intervient souvent dans cette situation de frontière entre ce qui est référencé et ce qui ne l'est pas : l'entreprise doit mettre à la disposition du prestataire les documents référencés. Il est d'ailleurs préférable de transmettre une



copie (paraphée conjointement) pour valider la prise de connaissance des différents intervenants au contrat. Tous les intervenants au contrat doivent avoir le même niveau de connaissance de l'information, et la formalisation demeure le seul témoin temporel dans cette démarche.

Ainsi, le contrat sert de fondement dans la définition du périmètre de sécurité ; par conséquent, ce qu'il ne traite pas représente la zone de risque tant pour l'entrepreneur que pour le fournisseur. En d'autres termes, **ce que le contrat ne couvre pas ne doit pas être une zone de risque.**

NB : dans les grandes sociétés ou les groupes industriels, le contrat-type (ou convention type) est celui de l'entreprise auquel se conforme le fournisseur ou le prestataire. Des négociations peuvent avoir lieu pour modifier certains paragraphes, rarement l'ensemble du contrat.

La prise de connaissance du contrat par les intervenants directs peut contribuer à « cadrer » les actions à entreprendre, et donc, limiter les risques de dérives comme le débordement de l'entreprise sur les tâches à accomplir par le prestataire ou l'attribution de tâches non planifiées initialement dans le contrat. Il s'agit ici de risques dits « projets » qui ont une répercussion sur la sécurité même du projet, comme la prise de connaissance d'information confidentielle, n'étant initialement pas dans le périmètre du projet et sur lequel le prestataire n'est pas engagé... la limite est franchie.

Cette prestation a posteriori, peut parfois même basculer en amont de la signature en raison de l'urgence de la situation. Dans ce cas, l'entreprise s'adresse à un prestataire de confiance qui accepte, souvent aux motifs des bonnes relations. Bien évidemment, la théorie et la pratique sont parfois différentes en raison de l'urgence de la situation, et surtout, de la relation de confiance.

### La conformité fonctionnelle

Un des premiers aspects fonctionnels (ou administratif) à vérifier porte sur les obligations légales. Les déclarations à effectuer auprès de la CNIL pour tout traitement de fichiers contenant des données à caractère personnel comme : la base de données des clients, le fichier du personnel de l'entreprise, les fichiers prospects, ... selon qu'il y ait enregistrement vidéo ou non. Pour favoriser ces démarches administratives, la CNIL a mis en œuvre des formulaires simplifiés (voir le site Internet de la CNIL). L'auditeur également vérifiera les licences d'exploitation (logiciel et

progiciel, sur les outils de chiffrement, ...), les contrats de maintenance en sécurité (anti-virus, pare-feux, ...), la propriété industrielle (gestion des brevets) et enfin, les certifications obtenues (si elles sont nécessaires ou justificatives dans le cadre du contrat).

L'auditeur demandera que son correspondant lui présente les justificatifs officiels et actualisés. A défaut, une copie ou un extrait ne sont pas suffisants pour attester la régularité des pièces présentées.

Un autre aspect important à prendre en considération dans la démarche d'audit de conformité est la qualité des interlocuteurs face à l'auditeur. Ces personnes doivent avoir une bonne connaissance du périmètre concerné tant d'un point de vue technique que dans les relations avec le prestataire. De la même manière, le représentant du fournisseur-prestataire doit connaître l'ensemble des éléments qui sont engagés dans le contrat. A ce titre, le signataire n'est pas le bon interlocuteur (mis à part dans les petites structures) pour présenter les processus, les documents applicables au contrat, ou encore les aspects techniques. De plus, la connaissance de l'historique des relations client et fournisseur constitue une valeur ajoutée pour l'amélioration des points critiques soulevés lors de l'audit de conformité, et ainsi, favoriser la résolution des risques encourus.

### La conformité technique

La prestation d'audit de conformité technique prend en compte l'existant qui correspond au livrable du prestataire. L'origine de ce livrable se trouve dans l'expression des besoins de l'entreprise qui est formalisée dans l'objet du contrat. Les livrables réalisés sont examinés soit en phase de recette, soit en phase production. Pour le mode projet, l'intervention idéale pour un audit de conformité est au moment de la recette puisqu'il permet à l'entreprise de valider ou non la réception du/des lots. A contrario, l'audit de conformité en phase de production intervient a posteriori de la réception, et donc, avec des impacts plus importants en cas d'écarts importants.

L'analyse technique va à la fois considérer la conformité par rapport aux documents (non seulement le contrat, mais également des pièces techniques telles que cahier des charges, architecture, cartographie réseau, règles d'administration, ...) et effectuer une investigation approfondie sur le système lui-même. L'auditeur est un expert technique qui examine les développements opérés, l'architecture du S.I., la configuration des serveurs et des applications et la supervision (fréquence des

mises à jour, suivi des alertes, efficacité du système de détection, délai d'intervention, durée de maintenance, récurrence des sauvegardes, mode d'archivage, durée et mode de rétention des données, ...).

Par exemple, concernant les données à caractère personnel (comme les bases clients), l'auditeur constatera que ces dernières sont chiffrées, qu'elles ne sont pas accessibles sans un *login/mot de passe* et que l'attribution des droits d'accès est bien appliquée (techniquement) conformément à la politique de sécurité en vigueur.

Tout ou partie de ces précédents points font l'objet d'un compte-rendu d'audit qui évalue le niveau de sécurité constaté et est suivi d'un plan d'action pour chacun des écarts. En conclusion du rapport d'audit est mentionné le niveau global atteint, et s'il est conforme à l'objet du contrat.

### La conformité organisationnelle

En matière d'infogérance par exemple, un des aspects particulièrement sensible, est l'organisation mise en œuvre pour la supervision, la maintenance et/ou l'archivage des données.

Ces aspects peuvent faire l'objet d'un long développement tellement l'ampleur de ces activités nécessite des moyens importants. Succinctement, l'entreprise qui sous-traite tout ou partie de son Système d'Information fait un transfert de responsabilité vis-à-vis d'une société spécialisée.

Lors d'audit de conformité dans ce domaine d'activité, il s'avère indispensable de contrôler l'attribution des droits et des fonctions de chaque intervenant. Par exemple, éviter soit qu'une personne puisse avoir accès à trop de domaines avec des droits administrateur sur chaque base de données, soit qu'un mot de passe générique soit utilisé et empêche toute traçabilité sur l'imputation des actions.

Dans ce cadre, le contrat qui renvoie à l'application des mesures de sécurité consignées dans un document de l'infogéreur (bonnes pratiques) doit être également examiné et contrôlé dans la pratique.

De même, le système de validation (documentaire, technique, ...) doit lui aussi faire l'objet d'une traçabilité, et doit être auditable par l'entreprise.

Comme nous l'avons montré l'audit de conformité n'est donc pas uniquement un contrôle documentaire ou administratif. Comme tout audit, son champ d'application dépend de l'étendue à investiguer. Ce périmètre qui est défini dans l'objet du contrat d'audit peut tout aussi bien être fonctionnel, organisationnel ou technique ; n'est-ce pas le corollaire de la place prépondérante du contrat dans toute relation commerciale ? Cet article n'a ni pour but ni pour objet de délivrer de quelconque conseil de nature juridique ; il importe donc à chaque entreprise d'associer à toutes les étapes de sa démarche, un professionnel du droit intervenant sur les nouvelles technologies...



## ZOOM

### Un point sur la sécurité Bluetooth

Annoncé à l'origine comme le système qui allait supprimer tous les câbles, Bluetooth a tardé à s'imposer à cause d'un prix plus élevé que prévu. La sécurité du protocole était a priori raisonnable, puisqu'offrant chiffrement et authentification à bas niveau en natif. Pourtant, lorsqu'il a commencé à vraiment se répandre sur les téléphones sans fil, de nombreuses failles ont été publiées et sa réputation a souffert alors que seules les applications étaient fautives.

Plus récemment, la première attaque contre le protocole proprement dit a été publiée, et la technique nécessaire pour transformer une clé USB en « air sniffer » a été divulguée...

#### Introduction et rappels

##### Architecture physique

Bluetooth est un système de réseau radio à courte portée, dont le but affiché est de s'affranchir des câbles.

Les périphériques de classe 1 sont censés porter à une centaine de mètres, ceux de classe 2 à une dizaine de mètres, et ceux de classe 3 à moins d'un mètre – la classe 3 est conçue pour des badges sans contact, par exemple.

Il ne faut pas confondre la portée utile dans un cas nominal avec celle qui peut être atteinte avec des équipements spéciaux (antennes directionnelles, amplificateurs...) qui ont permis d'établir des communications sur plusieurs kilomètres. Il ne faut pas compter sur la portée « limitée » des connexions Bluetooth pour protéger la confidentialité des données.

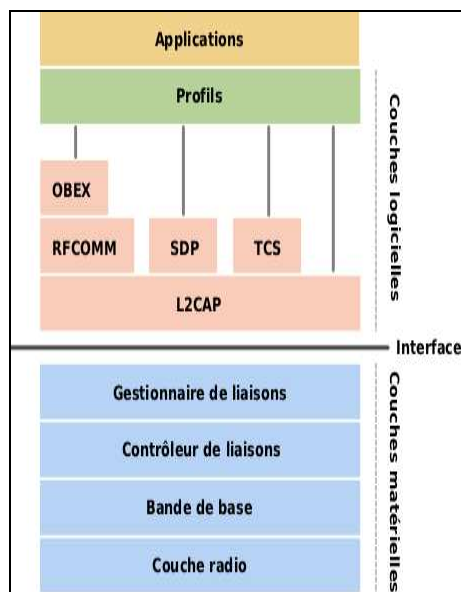
Le réseau de base est le *piconet*, composé d'un maître qui fournit une horloge de référence et d'au plus 7 esclaves. Le maître et un esclave peuvent décider d'échanger leurs rôles. Un périphérique peut faire partie de plusieurs piconets mais ne peut être maître que sur un seul à la fois; l'ensemble constitue un *scatternet*.

Bluetooth prévoit du chiffrement de lien et l'authentification<sup>1</sup> du nœud distant, mais ces fonctions ne sont pas obligatoirement actives, ou pas pour tous les services.

Au niveau physique, Bluetooth utilise un système de saut de fréquences<sup>2</sup> (*frequency hopping*) pour limiter les brouillages. La séquence pseudo-aléatoire des canaux est calculée à partir de l'horloge du périphérique maître. Ce n'est pas une fonction de sécurité à proprement parler mais ceci peut ralentir certaines attaques.

Voici un schéma de la pile Bluetooth, provenant de

<http://fr.wikipedia.org/wiki/Bluetooth/> :



Certains flux (audio par exemple) sont envoyés par les couches les plus basses. Mais la plupart des applications est construite sur la couche RFCOMM qui s'appuie sur L2CAP (*Logical Link Control and Adaptation Protocol*). L2CAP est en charge de la fragmentation et du ré-assemblage des paquets (jusqu'à 64 Ko). RFCOMM offre, entre autres, une émulation RS232 et des communications fiables type TCP ; 30 canaux sont disponibles (au lieu des 65535 ports TCP).

Bluetooth offre des services de découverte :

- des dispositifs à proximité, par envoi de paquets *inquiry* (INQ) ;
- des services tournant sur un dispositif, grâce au *Service Discovery Protocol* ; les applications peuvent s'enregistrer auprès de SDP.

Parmi les couches applicatives, on peut mentionner OBEX pour le transfert<sup>3</sup> de fichiers, HID pour les souris et clavier, et PAN pour l'établissement de connexion IP<sup>4</sup>...

<sup>3</sup> OBEX a été développé initialement pour les communications infrarouge (IRDA). Cf <http://en.wikipedia.org/wiki/OBEX>

<sup>4</sup> On peut aussi faire du PPP sur un canal RFCOMM.

##### Sécurité Bluetooth : chiffrement et authentification

Dès le début, Bluetooth a offert du chiffrement du lien et l'authentification des points distants, soit au niveau lien (mode 3), soit au niveau applicatif (mode 2).

En mode 1, aucune communication n'est chiffrée ou authentifiée. En mode 2, la sécurité est demandée par service (authentification et éventuellement chiffrement). En mode 3, toutes les communications sont authentifiées et éventuellement chiffrées. La spécification Bluetooth compare le mode 1 (pas de sécurité) à un mode 2 dans lequel aucun service ne demanderait d'authentification / chiffrement.

On peut établir :

- en mode 1 ou 2, des connexions en clair, sans authentification ;
- en mode 2 ou 3, des connexions en clair mais avec authentification ;
- en mode 2 ou 3, des connexions chiffrées et avec authentification.

Il n'est pas possible de chiffrer sans authentifier, c'est-à-dire que Bluetooth ne supporte pas de fonction de type « chiffrement opportuniste ».

L'authentification passe par un processus de *pairing*, lors duquel une *link key* est générée. Le *pairing* nécessite d'entrer un même code PIN sur les deux équipements. Le terme est trompeur, il n'est pas comparable au code PIN d'une carte à puce (bancaire ou SIM) :

- le PIN est quelconque, de longueur inférieure ou égale à 16 octets une fois codé en UTF-8, donc de 8 à 16 caractères. En tout cas, la spécification ne le limite pas à 4 chiffres ;
- sauf exceptions<sup>5</sup>, le PIN n'est pas fixe, c'est un code jetable choisi par l'utilisateur lors du *pairing*. Il n'a pas à être identique au code PIN de la carte SIM du téléphone, par exemple.

Pour plus d'information, lire le white paper « Bluetooth security architecture ».

<sup>1</sup> Ces deux fonctions de sécurité sont basées sur de la cryptographie symétrique.

<sup>2</sup> La bande des 2,4 GHz est découpée en 79 canaux de 1 MHz de large. Les équipements Bluetooth calculent à partir de l'horloge du maître une séquence pseudo-aléatoire. Tous les quanta de temps, les équipements sautent au canal suivant dans la séquence. Ainsi, si une bande de fréquence est brouillée, elle n'est utilisée qu'une faible partie du temps et peu de paquets sont perdus. Le quantum par défaut vaut 625 µs, soit 1600 sauts par seconde.

<sup>5</sup> Sur des périphériques sans clavier (comme les oreillettes), le PIN est fixé à la fabrication. Sur les téléphones, le PIN est souvent limité à 4 chiffres.



## Autres éléments de sécurité

Même si les communications sont en clair, elles ne peuvent pas être interceptées par un équipement standard, les cartes ne remontant que les paquets qui leurs sont destinés. Un *air sniffer*, comparable à une carte Ethernet en mode *promiscuous*, est assez onéreux<sup>6</sup>.

Il est *a priori* impossible de transformer un matériel standard en *air sniffer* : les équipements qui offrent l'upload de firmware n'acceptent en général que du code signé, il est douteux<sup>7</sup> qu'on puisse y installer un firmware spécifique. En mars 2007, Max Moser<sup>8</sup> annonce dans un message sur les listes Bugtraq et Full-Disclosure avoir réussi à uploader un firmware spécial sur une clé Bluetooth bas de gamme basée sur un chip CSR (*Cambridge Silicon Radio*) ; sa description était très vague, mais il n'y avait aucune impossibilité technique à ce qu'il avançait.

Il a été confirmé par la suite que cette opération est tout à fait réalisable, et que des firmwares FrontLine pirates circulent. Un *air sniffer* est donc réalisable pour moins de 30 €.

Un dispositif peut ne pas répondre aux paquets INQ. Ce mode « invisible » offre une protection basique :

- le périphérique peut encore être détecté par un *air sniffer* dès qu'il émet, mais il peut rester silencieux s'il est passé dans un des modes *basse consommation* ;
- ou bien on peut tenter de balayer toute la plage des BD\_ADDR. La taille de l'espace d'adressage est a priori dissuasive (48 bits), mais les 3 premiers octets (l'OUI) identifient le constructeur et n'ont que peu de valeurs différentes<sup>9</sup>. Il ne reste donc que 3 octets à brute-forcer, soit  $2^{24} = 16\,777\,216$  adresses. Les outils RedFang ou Bluesniff savent faire cela. Le processus est lent car si le périphérique est en sommeil, le temps de synchronisation n'est pas négligeable à cause du saut de fréquence mentionné ci-dessus mais la recherche peut être accélérée avec plusieurs périphériques Bluetooth<sup>10</sup> en parallèle.

## Attaques historiques contre les téléphones

De nombreuses failles ont été signalées sur les téléphones. Elles étaient toutes liées à

une mauvaise utilisation de la pile Bluetooth ou à de grossières erreurs de codage.

Les fonctions *licites* offertes via Bluetooth sont :

- envoi ou réception de vCards ;
- envoi ou réception d'autres fichiers, en particulier multimédia (sonneries en MP3...);
- sauvegarde ou restauration de l'annuaire complet ;
- connexion IP ;
- et éventuellement, pilotage du téléphone, accès à toutes les fonctions : envoi ou lecture de SMS, ouverture d'appels, ...

Toutes ces fonctions devraient demander une authentification, sauf la réception de vCards qui est effectivement permise sur certains mobiles. Le « Bluejacking » consiste à envoyer un fichier à un téléphone, mais les conséquences de cette prétendue attaque ne sont pas dramatiques.

Les attaques « historiques » sont toutes liées à ces fonctions :

- Initialement, certains mobiles ne demandaient ni authentification (mode 1) ni confirmation pour quelque fonction que ce soit. Il est évident que dans ce cas, tout est accessible :
  - lecture du répertoire par GET OBEX ou API propriétaire ;
  - numérotation par envoi de commandes AT11 sur un canal RFCOMM ;
  - envoi de SMS, lecture des SMS en mémoire...
- Outre ce point, la *sécurité par l'obscurité* a été très répandue. Certains constructeurs pensaient que du moment qu'un service n'était pas documenté ou ne s'enregistrait pas auprès du service SPF, il était protégé.
  - L'attaque « Bluebug » est basée sur ce principe : elle permettait de *siphonner* l'agenda ou même de passer des communications.
- L'attaque « Bluesnarf » consiste à exploiter le fait que la réception par OBEX est ouverte sur certains mobiles alors que l'envoi est soumis à autorisation. Bluesnarf envoie une requête GET au service PUSH (non protégé) ; sur les mobiles vulnérables, l'agent traite la requête sans vérifier son type.
- Certains téléphones portables ont une ergonomie douteuse ou une interface utilisateur buguée.
  - L'attaque « backdoor » consiste à établir un *pairing*, puis supprimer l'entrée de la liste des périphériques de confiance alors que la relation de confiance reste établie. Ainsi, on peut se reconnecter sans que le

propriétaire du périphérique vulnérable en ait conscience.

L'intérêt de cette attaque est très limité, il est improbable que les propriétaires de téléphones vérifient régulièrement la liste des *link keys*.

Actuellement, la plupart de ces failles est corrigée dans les équipements modernes et leur comportement est beaucoup plus prudent. Par exemple, le Nokia 9300 nécessite un *pairing* avant d'établir une communication, puis demande confirmation à chaque connexion, même si l'équipement distant est connu.

## Attaques plus récentes

### Attaque de Shaked & Wood

Le protocole Bluetooth était considéré comme totalement sûr jusqu'à l'attaque sérieuse développée contre le processus de *pairing*. Elle conduit à casser le PIN par force brute. Toutefois :

- elle nécessite un *air sniffer* puisque les cartes standard ne remontent que les données qui leur sont destinées ;
- elle a lieu pendant le *pairing* qui n'est fait en théorie qu'une fois. Les auteurs s'appuient sur une seconde attaque qui fait croire au *maître* que l'*esclave* a perdu sa clé et relance une négociation ;  
NB : Ceci ne marche pas en face d'un Linux avec Bluez qui refuse d'oublier la *link key* précédente.
- la force brute ne trouvera pas un PIN complexe et long, certes difficile à entrer sur un téléphone, mais envisageable avec des PC ou PDA.

### Bluetooth Stack Smasher

D'après Pierre Betouin, auteur du fuzzer BSS et du papier « (In)sécurité du Bluetooth - De nouvelles menaces »<sup>12</sup>, de nombreuses piles Bluetooth seraient encore vulnérables à des dénis de service au minimum. Il est possible que certaines failles soient exploitables pour exécuter du code arbitraire. Il est difficile d'en avoir le cœur net car les moyens de debugging manquent sur les téléphones<sup>13</sup>.

### Car whisperer

Cet outil<sup>14</sup> se connecte à une oreillette Bluetooth, et reçoit son flux audio et peut aussi en envoyer. Il est bien distribué et se compile sans difficulté sur Linux. Un script Perl fourni permet d'intercepter toutes les oreillettes qui passent à portée. Les seules opérations manuelles sont de changer des chemins d'accès dans le script, et remplacer

<sup>6</sup> Par exemple, le sniffer FrontLine est distribué en Europe à plus de 10 000 €

<sup>7</sup> Avant même l'annonce de Max Moser, CSR n'a jamais répondu à nos demandes d'information.

<sup>8</sup> Cf [http://www.remote-exploit.org/research/busting\\_bluetooth\\_myth.pdf](http://www.remote-exploit.org/research/busting_bluetooth_myth.pdf)

<sup>9</sup> Cf <http://standards.ieee.org/regauth/oui/>

<sup>10</sup> Cf l'article de Pierre Betouin mentionné plus bas

<sup>11</sup> Cf

[http://fr.wikipedia.org/wiki/Commandes\\_AT](http://fr.wikipedia.org/wiki/Commandes_AT)

ou

[http://en.wikipedia.org/wiki/Hayes\\_command\\_set](http://en.wikipedia.org/wiki/Hayes_command_set)

<sup>12</sup> Cf <http://securitech.homeunix.org/blue>

<sup>13</sup> Certains ont un port JTAG, ce qui ouvre des perspectives intéressantes.

<sup>14</sup> Voir

<http://trifinite.org/Downloads/carwhisperer-0.2.tar.gz>



le `pin_helper` dans `/etc/bluetooth/hcid.conf` - le `helper` est le programme qui donne le PIN, éventuellement après l'avoir demandé à l'utilisateur (celui qui est fourni connaît les PIN des divers constructeurs).

Carwhisperer marche car la plupart des oreillettes supporte de se ré-attacher à un autre téléphone (*multi pairing*) et ont un code PIN en dur invariable, très souvent à 0000 d'ailleurs. Quelques rares constructeurs tirent un PIN au hasard à la construction de l'oreillette.

*NB : comme le nom l'indique, cet outil marche contre les « voitures Bluetooth » - le système n'est rien de plus qu'une oreillette.*

## Autres périphériques :

### Souris et clavier

Le comportement est variable selon le fabricant.

D'après <http://klausler.com/msbtkb-linux.html>, Apple fabriquerait des claviers sur lesquels on effectue un vrai processus de *pairing* avec PIN, et où le canal Bluetooth est chiffré et authentifié.

Nous avons réalisé quelques essais avec un clavier et une souris Bluetooth d'une autre marque. Ils sont invisibles et ne répondent aux INQ que lorsqu'on appuie sur un bouton « connexion » accessible dessous ; dès qu'un PC se connecte au périphérique, il redevient invisible et ne répond plus aux autres demandes de connexion. Il n'est donc pas possible d'intercepter le flux de données par un processus de *multipairing*, comme dans le cas des oreillettes Bluetooth. Toutefois, en l'absence de véritable *pairing*, cette sécurité est fragile : la communication est en clair. Un *air sniffer* constituerait une *key logger* redoutable.

### PC

Le comportement des divers systèmes d'exploitation testés dépend du logiciel installé.

Linux<sup>15</sup> et BSD ne démarrent que le strict minimum par défaut : HCI (le service de base), SDP (énumération des services) et très souvent HID (gestion des claviers et souris).

Le cas de Microsoft Windows est un peu moins simple car plusieurs logiciels existent. Parmi les cas testés, *Bluesoleil*<sup>16</sup> démarre de nombreux services, dont OBEX, mais n'accepte ni la lecture de répertoire, ni l'envoi de fichiers.

HID permettrait de brancher un clavier et une souris à distance sur une machine, mais

il n'existe guère de scénario réaliste. Pour que cette attaque ait un intérêt, il faudrait que le PC ne soit pas accessible physiquement mais qu'il soit à portée de la radio, et idéalement que l'écran soit visible ; par exemple s'il est derrière une vitre, dans un bureau fermé à clé. Et encore faudrait-il que la station ne soit pas verrouillée, et que le système accepte que le clavier soit branché sans confirmation. Quelques essais sous Linux ou Windows ont systématiquement conduit à une intervention de l'utilisateur pour brancher le clavier ou la souris. Sur MacOS X, Bluetooth n'est pas actif par défaut et le système n'accepte pas de connexion de clavier ou de souris sans intervention de l'utilisateur.

Une fois Bluetooth activé sur MacOS X, SDP montre un port série « Bluetooth-PDA-Sync » et un service « OBEX Object Push ». Il a été possible d'envoyer des fichiers. MacOS est bugué : les fichiers sont reçus sans confirmation de l'utilisateur, contrairement à ce qu'annonce la GUI, et ils arrivent dans le répertoire « Public » au lieu du « Documents » spécifié. Mais le système renomme les fichiers quand il y a un conflit, et refuse les changements de répertoire : il n'est pas possible d'exploiter ce bug pour écraser des fichiers, il n'a donc pas d'impact en terme de sécurité.

### Profils divers

La spécification Bluetooth est disponible gratuitement - il suffit de s'inscrire sur <http://www.bluetooth.org/>. Au document « core specification », qui fait 1200 pages, s'ajoutent des « profils » supposés assurer la compatibilité entre équipements d'un même type. Quelques *white papers* ont été édités par des groupes de travail.

La lecture des profils pourrait ouvrir des pistes d'attaques.

Les profils sont interdépendants : un profil peut réutiliser ou faire référence à des parties d'un profil plus général. Les profils de plus haut niveau sont plus permissifs. A priori, rien n'oblige un constructeur à utiliser le profil le plus contraignant.

Generic Access profile	
Service Discovery Application Profile	TCS-BINbased profiles
	Cordless telephony profile
	Intercom profile
Serial port profile	
Dial-up Networking Profile	Generic Object Exchange profile
Fax profile	File transfer profile
Headset profile	Object push profile
LAN access profile	Synchronization profile

La plupart des profils indique que le chiffrement et l'authentification sont optionnels, mais doivent être supportés au cas où le périphérique distant les demanderait. La formule qui revient souvent est : *"Link level authentication and encryption are mandatory to support and optional to use. Bonding is mandatory to support and optional to use"*.

Quelques profils imposent le chiffrement et l'authentification, comme le DIAL-UP NETWORKING PROFILE qui précise : *"For security purposes, authentication is used,*

*and all user data is encrypted. For this, the baseband/LMP mechanisms are used"*.

De même, CORDLESS TELEPHONY PROFILE impose l'authentification et le chiffrement.

**Rappel** : *le support de l'authentification et du chiffrement ne suffit pas à protéger la communication dans le cas des oreillettes, à cause du PIN en dur et du multi-pairing.*

Un profil exclut ces fonctions de sécurité, ce qui ouvre des perspectives : VIDEO DISTRIBUTION PROFILE (*"Content Protection is provided at the application level and is not a function of the Bluetooth link level security protocol"*).

Quelques profils sont « hasardeux » :

- OBJECT PUSH PROFILE : *"Link level authentication and encryption are mandatory to support and optional to use. Bonding is mandatory to support and optional to use. OBEX authentication is not used"*.
- A contrario, le FILE TRANSFER PROFILE demande d'être capable de supporter la sécurité applicative : *"Support for link level authentication and encryption is required but their use is optional. Support for OBEX authentication is required but its use is optional"*.

Et le SYNCHRONIZATION PROFILE l'impose : *"The profile fundamentals are the same as defined in Section 2.4 in GOEP [2], with the addition of the requirements that bonding, link level authentication, and encryption (Fundamentals 1 and 3 in GOEP) must always be used for this profile"*.

- PERSONAL AREA NETWORKING<sup>17</sup> PROFILE n'impose pas le chiffrement ou l'authentification.
- HANDS-FREE PROFILE laisse le chiffrement ou l'authentification en option, et pour supporter les appels multiples, autorise le *multipairing* (mais le terme n'apparaît nulle part).
- BASIC PRINTING PROFILE (BPP) : *"Link-level authentication and encryption are mandatory to support and optional to use. If the Printer initiates authentication it may do so by using a fixed PIN. The PIN may be changed using a proprietary method in the Printer. The use of a fixed PIN is explained in Section 14.2.1 of [1]. How the fixed PIN is communicated to the user of the Sender is not specified"*.

Ceci signifie qu'il doit être possible de se connecter sur une imprimante, mais l'intérêt est assez limité.

En conclusion, il n'y a guère que les caméras Bluetooth qui présenteraient une faiblesse potentielle, si le chiffrement applicatif n'est pas en place.

<sup>15</sup> Sur Linux, on peut dénombrer quatre piles Bluetooth, mais la plus répandue est Bluez. Cf <http://www.bluez.org>

Les configurations sont plus cohérentes sur BSD ou MacOS X.

<sup>16</sup> Cf <http://www.bluesoleil.com>

<sup>17</sup> Rappel : PAN est l'un des moyens pour se connecter à IP via Bluetooth



Suite aux écrits publiés durant des années sur le sujet, les constructeurs semblent avoir pris la sécurité un peu plus au sérieux (Bluetooth inactif par défaut, pairing avec demande de PIN, confirmation systématique sur une connexion RFCOMM...). Les téléphones se défendent beaucoup mieux qu'il y a quelques années, les failles applicatives mentionnées ne concernent probablement plus que des vieux matériels. On ne peut exclure que certains modèles comportent encore des failles (services cachés...) et il est difficile d'estimer le nombre de vieux téléphones vulnérables encore en circulation.

Les fragilités face aux attaques de bas niveau (Bluetooth Stack Smasher) sont plus difficiles à exploiter que les vieilles failles mais la correction semble encore négligée par les fabricants.

Les seuls équipements signalés comme facilement vulnérables actuellement sont les oreillettes ; la mise en place d'un PIN aléatoire suffirait à mettre carwhisperer en défaut.

Pour les autres classes de périphériques, la lecture des « profils » n'a pas montré de voie d'attaque claire sauf pour les caméras. Ces spécifications sont de trop haut niveau pour conclure sur la sécurité des équipements concernés, seuls des tests permettraient d'avoir une certaine assurance.

Certains périphériques ne chiffrent pas la connexion et sont donc vulnérables à un air sniffer. Ceci est intéressant pour les claviers (keylogger), ou les connexions TCP/IP (PAN ou PPP) ; les autres applications de Bluetooth (synchronisation de PDA ou de téléphone) sont de trop courte durée pour être vraiment intéressantes, vu la sensibilité somme toute réduite des informations transférées. Sauf à supposer que l'utilisateur stocke des données confidentielles en clair sur un équipement facile à voler, ce qui est certainement une plus mauvaise pratique !

## 📁 Références

### Spécification Bluetooth :

<http://www.bluetooth.org/>  
<https://www.bluetooth.org/spec/>  
<http://en.wikipedia.org/wiki/Bluetooth/>  
<http://fr.wikipedia.org/wiki/Bluetooth/>  
<http://www.palowireless.com/infotooth/tutorial.asp/>

<http://www.xgarreau.org/aide/divers/bluetooth/theorie.php/>  
[http://www.freebsd.org/doc/en\\_US.ISO8859-1/books/handbook/network-bluetooth.html](http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-bluetooth.html)  
<http://www.thewirelessdirectory.com/Bluetooth-Overview/Bluetooth-Specification.htm>  
Bluetooth Security Architecture (white paper disponible sur bluetooth.org)

### Attaques :

<http://www.secuobs.com/news/05022006-bluetooth7.shtml>  
[http://trifinite.org/trifinite\\_stuff\\_bluebug.html](http://trifinite.org/trifinite_stuff_bluebug.html)  
<http://www.wirelessve.org/entries/show/WVE-2005-0002>  
[http://trifinite.org/trifinite\\_stuff\\_carwhisperer.html](http://trifinite.org/trifinite_stuff_carwhisperer.html)  
<http://www.secuobs.com/news/05022006-bluetooth1.shtml>  
<http://secuobs.com/news/05022006-bluetooth2.shtml>  
<http://secdev.zoller.lu/>  
<http://www.thebunker.net/resources/bluetooth>

[http://www.networkchemistry.com/bluescanner/BluetoothSecurityThreat\\_WhitePaper.pdf](http://www.networkchemistry.com/bluescanner/BluetoothSecurityThreat_WhitePaper.pdf)  
<http://securitech.homeunix.org/blue/>  
[http://securitech.homeunix.org/blue/ArticleFR\\_bluetooth\\_pbetouin.pdf](http://securitech.homeunix.org/blue/ArticleFR_bluetooth_pbetouin.pdf)  
<http://bluesniff.shmoo.com/>  
<http://www.securiteam.com/tools/5JP0I1FAAE.html>

[http://www.schneier.com/blog/archives/2005/06/attack\\_on\\_the\\_b\\_1.html](http://www.schneier.com/blog/archives/2005/06/attack_on_the_b_1.html)  
<http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/>

### Logiciels :

<http://www.holtmann.org/linux/bluetooth/>  
<http://www.bluez.org/>  
<http://fr.wikipedia.org/wiki/Bluez>  
<http://people.csail.mit.edu/albert/bluez-intro/>  
<http://affix.sourceforge.net/affix-tech-doc/1.1/index.html>  
<http://affix.sourceforge.net/>  
<http://www.research.ibm.com/BlueDrekar/>

<http://developer.axis.com/software/bluetooth/>  
<http://search.cpan.org/~iguthrie/Net-Bluetooth-0.37/Bluetooth.pm>  
<http://openobex.triq.net/>  
<http://www.betaversion.net/btdsd/>  
<http://www.secuobs.com/bss-0.8.tar.gz>  
<http://bluesniff.shmoo.com/>  
<http://www.pentest.co.uk/src/btscanner-2.1.tar.bz2>

**Divers :** <http://openobex.triq.net/obexftp/services>



Inscription à la Newsletter : [newsletter-subscribe@esec.fr.sogeti.com](mailto:newsletter-subscribe@esec.fr.sogeti.com)

Désinscription : [newsletter-unsubscribe@esec.fr.sogeti.com](mailto:newsletter-unsubscribe@esec.fr.sogeti.com)

### Agence ESEC

**Sogeti Infrastructures Services**  
6-8 rue Duret 75016 Paris - France  
Tél. : +33 (0)1 58 44 26 79  
Site : <http://esec.fr.sogeti.com>  
Mail : [esec@esec.fr.sogeti.com](mailto:esec@esec.fr.sogeti.com)

Société par Actions Simplifiées au capital de 15 999 790 € - RCS Paris 479 942 583  
Conformément à la loi « Informatique et libertés » du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.  
Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au directeur de l'agence ESEC.

Sogeti ne peut être tenue pour responsable en cas avéré de détournement des liens, communiqués à titre d'illustration dans ses propos.

Cette newsletter a été réalisée par des consultants sécurité de l'agence **ESEC**.

Responsable de la publication :

- Edouard **JEANSON**

Auteurs :

- Michel **ARBOI**
- Marc **BOUVIER**

Rédacteur en chef :

- Marc **BOUVIER**
- Daniel **ROUMI**

Relecteurs :

- Alexandre **GAZET**
- François-René **HAMELIN**
- Jérémy **RENARD**
- Nicolas **VIRY**

