

News Letter n° 3
Juillet Août 2007



Edito

Avant de nous quitter pour quelques semaines ensoleillées... nous vous proposons notre dernière News Letter avant la rentrée. Nous espérons qu'elle vous donnera à réfléchir pour tout l'été !

Nous lançons à cette occasion notre série du thème « expliqué à ceux qui n'y connaissent rien » et souhaitons vivement que par cette nouvelle rubrique, nous puissions répondre à certaines de vos questions.

Nous sommes toujours heureux de recueillir vos témoignages et vos suggestions de contenus pour nos lettres. N'hésitez à nous faire part de vos articles ou livres blancs que vous souhaiteriez publier sur notre site.

Forum ATENA vous souhaite d'excellentes vacances et vous retrouvera à la rentrée pour des activités nombreuses et enrichissantes pour chacun d'entre vous !

Pauline Duffour
Administrateur Forum ATENA
redaction@forumatena.org

A la une

Adhérez à l'association !

Vous y rencontrerez, à travers nos ateliers, d'autres adhérents très intéressants, dans un climat propice pour nouer des relations de travail fructueuses.

Le mois de juin s'est terminé en apothéose avec l'événement tenu à l'EPITA sur le thème hautement passionnel de la sécurité des Smartphones /PDA. Si vous n'étiez pas encore convaincus de nous rejoindre, lisez plutôt le commentaire de Joël Courtois, Directeur Général de l'EPITA :

« Ouverture, communication, formation, échange, recherche, partenariats autant de mots-clés communs aux ambitions du Forum ATENA et à l'esprit d'une école d'ingénieurs. C'est donc avec conviction que nous soutenons de telles actions dans les TIC, qui rapprochent enseignement, recherche et industrie.

Nous avons eu le plaisir d'accueillir la conférence sur la sécurité des SMARTPHONE/PDA et d'apprécier une manifestation de très grande qualité. Le Forum ATENA sera donc toujours le bienvenu à l'EPITA. »

NEWS

Les documents d'identité

Obligations légales – Sécurités – Fraude et Contre-mesures

Assez curieusement, il n'existe pas en France de textes précisant spécifiquement quels sont les documents administratifs valant justificatifs d'identité. Il s'ensuit que c'est au chef de l'établissement public ou privé dans lequel un contrôle d'accès est organisé de définir lui-même quels documents il entend se faire produire en fonction de la rigueur plus ou moins grande de la politique de sécurité qu'il entend mener.

Quels documents exiger ?

- la carte nationale d'identité : pour notre pays, elle a été créée par un décret du 22 octobre 1955. Elle est strictement personnelle mais reste propriété de l'Etat. Elle permet de justifier de son identité et de valoir aussi acte de naissance et certificat de nationalité française.
- Le passeport : c'est le document international de voyage répondant aux normes de l'Organisation Civile Internationale. Ce document reste aussi propriété de l'Etat.

Le permis de conduire, comme son nom l'indique, est un titre autorisant son titulaire à conduire un véhicule terrestre à moteur. Il a une durée de vie illimitée. Nous ne prôtons pas l'utilisation de ce document comme pièce d'identité acceptable lors d'un contrôle d'accès en raison à la fois :

- de la multitude de faux qui existent dans notre pays. Selon les estimations parues dans la presse, il y aurait 2,7 millions de faux permis (sur les 42 millions en circulation),
- de l'absence de sécurités documentaires sur les anciens modèles.

Les autres documents qui peuvent valoir justificatifs d'identité (permis de chasser, carte d'identité de fonctionnaire...) ne peuvent être retenus que si le contrôleur documentaire connaît préalablement le document présenté et peut en contrôler son authenticité.

Quels sont les risques ?

Aux côtés des risques inhérents à la présentation d'un faux document¹ tels que l'obtention induite d'un

avantage social, l'usurpation d'identité, le vol ou l'escroquerie, on ignore généralement qu'il existe, dans certains cadres professionnels, des obligations de présentation et de contrôle des titres d'identité assorties de pénalités lourdes en cas de non-respect. Ainsi :

- l'article L 625-1 et suivants du CESEDA applicable pour tous les transporteurs internationaux routiers et aériens de voyageurs,
- l'article L 341-6 du Code du Travail applicable lors de l'embauche aux employeurs et aux entreprises de travail temporaire confirmé par l'arrêt BRACA de la Chambre Criminelle de la Cour de Cassation le 29 mars 1994,
- le décret 2006-212 du 23 février 2006 pour l'accès aux secteurs d'activités d'importance vitale,
- l'article L 563-1 du Code Monétaire et Financier qui dans le cadre de la lutte contre le blanchiment de l'argent oblige les banques à s'assurer de l'identité de leurs clients.

Qu'appelle-t-on Sécurités des documents ?

Un document d'identité répond à une norme de fabrication et contient divers éléments permettant de certifier son authenticité. La publicité de ces sécurités varie suivant les pays. La Belgique par exemple décrit publiquement les sécurités de son passeport. La France a plus une tradition de secret.

Le contrôle d'un document d'identité s'exerce sur 3 niveaux :

- le niveau 1 : contrôle visuel que toute personne peut exercer à partir de l'examen du document,
- le niveau 2 : contrôle assisté par un équipement de préférence informatique pour effectuer certains contrôles et lire la puce ou le code à barres du document quand il y en a,
- le niveau 3 : réservé aux autorités publiques : recours à la consultation des fichiers.

Contre Mesures de niveau 1

Par exemple, s'agissant du **niveau 1** et de la carte d'identité française :

- elle utilise le format rectangulaire ID7 (ou A7 = 74 x 105 mm) conforme à la norme ISO 7810,
- le plastique est solidaire de la carte elle-même,
- la forme des coins est arrondie,
- des stries existent sur le pourtour de la carte,
- le gaufrage RF est présent sur chaque côté,

¹ Par ailleurs, il existe aujourd'hui au niveau des Préfectures des comités composés de fonctionnaires et de personnes du secteur

privé qui se penchent sur la question de la fraude à l'identité. Le sujet est réellement d'actualité.

- le luminophore est présent au verso (point large blanc au verso à droite de la CNI),
- la marque en creux de la pince se distingue nettement au verso,

L'examen visuel peut se prolonger par :

- la vision en transparence du filigrane,
- la vision des 3 micro-perforations (vrais trous dans la carte)
- et par le contrôle de présence des signes RF sous OVI (Optical Variability Ink) : ces mentions sont soit marrons soit vertes en fonction de l'inclinaison du document.

Si l'on s'attache au recto de la carte d'identité :

- la photo contient les initiales de son détenteur,
- la guilloche (lignes courbes de fond d'impression) est continue entre le fond d'impression et la photo,
- la police de caractères des éléments variables (nom, prénoms...) est spécifique et ne trouve pas dans le commerce, de même que la police de la piste lisible par la machine (MRZ . 2 lignes du bas).

La vérification d'un document d'identité n'écarte pas le bon sens. Ainsi sur un passeport, le mot Ambassade écrit avec un seul S est forcément suspect, la mention REPUBLIQUE DE BELGIQUE est très innovante.

Contre Mesures de niveau 2

D'autres vérifications de **niveau 2** sont possibles. Elles demandent de recourir :

- à des équipements simples de grossissement de l'image pour rechercher notamment ce qu'on appelle des micro-impressions comme le nom du graphiste DURAND MEGRET ou la ligne horizontale REPUBLIQUE FRANCAISE,
- à un scanner informatique de type CCD pour notamment :
 - o apprécier le degré de bleuissement de la carte sous rayons UltraViolet : le papier fiduciaire utilisé est élaboré avec du coton et ne contient pas d'agents « blanchissants » (azurants optiques),
 - o calculer l'exactitude des deux lignes de la piste MRZ (Machine Readable Zone),
 - o contrôler la cohérence entre ces données et celles qui figurent au verso,

- o vérifier la présence d'autres signes de sécurités n'apparaissant que sous UV (pastilles colorées...),
- o vérifier le procédé d'impression (laser, jet d'encre...),
- o accéder à des annuaires électroniques publics pour s'assurer de l'existence d'une adresse postale,
- o accéder à une base de données des documents de référence,
- o accéder à une base de données mise en place spécialement pour le contrôle d'accès dans un lieu précis : liste des personnes interdites de casinos par exemple,
- o lire la puce des nouveaux documents biométriques.

Ce type d'équipement informatique est autorisé par la CNIL, qui le considère comme un « œil intelligent ». Cependant, tous traitements opérés à partir des données personnelles recueillies lors de la numérisation tombent sous le coup de la loi Informatique et Libertés.

L'équipement, associé aux logiciels et bases de données ad hoc, doit aussi s'accompagner d'un environnement comprenant :

- une formation des contrôleurs documentaires qui peut s'entreprendre avec l'aide des services de l'Etat,
- une procédure de remontée des alertes à un niveau de décision,
- un strict respect des règles de la CNIL.

Conclusion

La seule question que nous devons nous poser lors de la mise en place d'un contrôle d'accès physique aux portes de nos entreprises (ou de l'embauche d'un salarié) est celle de savoir si nous nous bornons à relever l'identité qu'on nous déclare ou si nous estimons devoir la vérifier un peu plus sérieusement en fonction des risques existants et préalablement définis dans la politique de sécurité de l'entreprise.

De la réponse, découle la mise en place ou non des moyens appropriés.

Raphaël Rocher, SECALLIANCE

La sécurité des Smartphones, et des PDA

Quelle attitude adopter ?

Ce sujet brûlant fait encore l'actualité dans la presse nationale et internationale. Beaucoup d'informations circulent, et fort du succès de l'évènement organisé par l'atelier Sécurité, un point s'imposait sur ce sujet.

La démocratisation des Smartphones et des PDA dans les entreprises soulève beaucoup de questions en termes de sécurité. Stations mobiles synchronisées en permanence avec le réseau interne de l'entreprise, elles font aussi partie intégrante de son système d'information. C'est la mobilité qui rend la gestion de ces périphériques très sensible.

Smartphones, PDA : quelle politique ?

Un PDA, assistant personnel, est un ordinateur de poche dont les principales fonctionnalités sont un agenda, un répertoire téléphonique, un bloc-notes auxquelles se sont désormais greffées de nombreuses fonctions multimédias (lecteurs mp3/vidéos, dictaphones...). Les différentes extensions ont rendu les PDA communiquant via WiFi, Bluetooth jusqu'à les rendre concurrents en termes de fonctionnalités, avec les Smartphones. Aujourd'hui la principale différence se situe sur la taille de l'écran (plus grande pour les PDA) et leur capacité d'écriture (plus grande pour les Smartphones).

Les Smartphones réunissent les fonctionnalités d'un PDA et d'un téléphone mobile, une sorte de solution deux en un. On y trouve également, un navigateur Web, la possibilité de consulter ses e-mails avec parfois une messagerie instantanée, la navigation GPS... En outre, il est possible de développer ou d'installer des applications tierces comme des progiciels ou des clients légers.

Les utilisateurs de ces terminaux mobiles recherchent un accès rapide et direct aux informations de leur entreprise, partout dans le monde, à n'importe quel moment, comme s'ils étaient dans leur bureau. Leur objectif étant d'optimiser leur temps de travail, tout en gardant une facilité d'utilisation.

L'entreprise souhaite satisfaire l'attente de ses employés tout en préservant la sécurité de son système d'information. Elle doit donc mettre en place une politique de sécurité correspondant aux besoins de l'utilisateur : protection du terminal, protection des données stockées et transmises, protection du système d'information, définitions des règles d'utilisation.

Cette solution doit pouvoir s'adapter, suivant les évolutions des besoins, de manière aisée.

Les Smartphones étant majoritairement utilisés dans le monde des affaires, il faut donc pouvoir assurer quatre points majeurs de sécurité : l'authentification de l'utilisateur, la confidentialité et l'intégrité des données, ainsi que la disponibilité du terminal mobile.

L'authentification permet à l'utilisateur d'être identifié de manière unique, il est le seul à pouvoir utiliser son Smartphone, au contraire des ordinateurs de bureau ou plusieurs personnes peuvent y avoir accès.

La confidentialité des informations assure que seul l'utilisateur autorisé est en mesure de consulter ses données, l'intégrité assure que les données n'ont pas été modifiées.

Enfin l'utilisateur doit pouvoir utiliser tous les services fournis par son Smartphone et ceci à tout moment.

Devenus micro ordinateurs de poche et ultra communicants (WiFi, bluetooth...), leur déploiement doit être traité avec les mêmes procédures et le même soin qu'un ordinateur portable. La définition des besoins des utilisateurs, des risques associés à son utilisation, du niveau de criticité des accès au Système d'Information (SI) et des données stockées, sont des étapes primordiales à tout choix de solutions et au déploiement de celles-ci. La définition d'une politique de sécurité est aussi une phase importante qui doit être abordée afin d'avoir une parfaite maîtrise des procédures d'utilisation et d'administration de ces produits.

Il est important de considérer ces outils de communication non pas comme des jouets mais comme des extensions du système d'information. Analyser les données qui seront échangées entre le réseau d'entreprise et ces stations mobiles permet de définir au mieux la politique de sécurité à mettre en place autour de ces stations. Une politique de sécurité entraîne toujours un lot de contraintes pour l'utilisateur. Il faut trouver un équilibre entre la sécurité de l'information et ce que cela impose à l'utilisateur. Une politique trop contraignante amène souvent l'utilisateur à la contourner. Une sensibilisation est donc aussi nécessaire afin de « faire comprendre » à l'utilisateur les raisons de cette politique et le bien fondé de ces contraintes.

Architectures et spécificités

Les Smartphones et les PDA utilisent une infrastructure similaire. A l'extérieur de l'entreprise, ils se synchronisent en passant par un opérateur GSM/GPRS. Grâce aux stations de base (BTS), ils accèdent au réseau de l'entreprise. En interne, il est possible de les mettre à jour via du WiFi, sans sortir de l'Intranet. La synchronisation depuis l'extérieur se fait donc via un opérateur et via l'Internet.

Fabriqué par Research In Motion (RIM), la solution Blackberry au cœur de la polémique actuelle propose une architecture légèrement différente permettant le « push-mail » : système de messagerie permettant à l'utilisateur de recevoir quasi instantanément le courriel dans sa boîte électronique sans avoir besoin d'aller la consulter.

Pour cela, au sein de l'entreprise, est mis en place un serveur (BES), qui est connecté en permanence aux serveurs de l'entreprise (de type Web, applications, messagerie) et aux serveurs situés au sein de RIM (au Canada ou en Angleterre).

Le « push-mail » est réalisé de la façon suivante : le BES chiffre les courriers électroniques reçus et les transmet aux serveurs RIM qui eux-mêmes les envoient directement sur les Blackberry des utilisateurs. Le terminal se charge de déchiffrer le message à la réception. Cela permet de recevoir les e-mails avec un délai très court sans faire de multiples requêtes à intervalles réguliers. De même, deux avantages techniques en découlent : désengorger les serveurs car moins de requêtes, augmenter l'autonomie du terminal mobile.

Les serveurs RIM à l'étranger (Canada et Angleterre) sont au centre des discussions, car ils acheminent tous les messages électroniques. Tous les courriers envoyés à des BlackBerry se situant en Europe vont donc passer par le serveur situé en Angleterre, afin que celui-ci puisse réaliser le « Push ». Une personne malintentionnée pourrait donc attaquer ce serveur afin de récupérer des informations confidentielles.

Néanmoins RIM assure que son infrastructure ne fait que transmettre le message et que celui-ci reste chiffré de « bout en bout » (du serveur BES situé dans l'entreprise au terminal BlackBerry destinataire), donc même si une personne malveillante récupérerait un courrier électronique, il faudrait qu'elle puisse le décrypter en cassant l'AES 256 bits utilisé par RIM pour chiffrer les messages. Ceci est actuellement impossible si l'algorithme a été correctement implémenté et les clés correctement générées.

De plus les solutions proposées par les autres fabricants de Smartphones passent par des opérateurs pouvant également avoir des serveurs à l'étranger. Lors de déplacements internationaux, la continuité des services est assurée par des accords entre l'opérateur du pays d'origine et un ou plusieurs opérateurs locaux. Il n'est donc pas possible de contrôler le cheminement des informations de l'entreprise jusqu'aux terminaux mobiles. La politique de sécurité doit donc bien s'appuyer sur des éléments maîtrisables de « bout en bout ».

Les données sont à l'extérieur...

Un PDA se synchronise régulièrement sur le réseau de l'entreprise. La synchronisation peut s'effectuer via plusieurs modes possibles. Ici, nous nous intéresserons essentiellement à la synchronisation sans fil, via une carte WiFi, ou un opérateur fournissant la 3G par exemple.

Les e-mails transitent donc à l'extérieur de l'entreprise. Deux points importants sont à analyser. L'envoi des informations passe par un opérateur et donc par des serveurs inconnus. Il est alors nécessaire de faire confiance en cet opérateur, ou de connaître son mode de fonctionnement avec certitude et précision. Les communications sont-elles chiffrées et comment ?

Le deuxième point est le stockage des données sur le Smartphone. Lorsque le message électronique est arrivé à destination (sur la station mobile), il y est disponible. En cas de perte ou de vol, sans aucune protection, n'importe qui aura accès à ses informations. Pour résoudre ce problème, il existe des logiciels permettant de chiffrer tout ou partie des données contenues dans un PDA. Le déchiffrement des données ne s'y exécute qu'après authentification forte. Les solutions chiffrant l'intégralité des données s'exécutent généralement, lorsque l'on éteint le PDA (chiffrement), et lorsqu'on le rallume (déchiffrement). Cela peut poser problème si le PDA est perdu ou volé alors qu'il est allumé.

Il est donc important de bien identifier les besoins réels et mixer les méthodes de protection de données. On peut imaginer chiffrer les données les plus importantes dès leur réception. Une évolution serait aussi de mettre en place un système de verrouillage du Smartphone dès que son propriétaire s'en éloigne. Cela nécessite de porter sur soi une puce de type RFID (Radio Frequency Identification) dont la portée serait limitée à quelques centimètres. Ainsi en cas de perte ou de vol, les données seraient préservées puisque le Smartphone perdu ou volé serait verrouillé.

Attaques possibles

Beaucoup de monde s'accorde à dire que l'augmentation de PDA favorisera l'apparition de virus et autre malwares. Surtout, s'ils restent considérés comme le maillon faible du système d'information, ils seront ciblés dans le but d'attaquer le réseau de l'entreprise tout entier.

Au même titre que les ordinateurs, ces périphériques, parfois considérés à tort comme des jouets, sont en proie aux mêmes menaces, virus, chevaux de Troie, déni de service, messages indésirables (SPAM). Toutes les menaces, qui sont connues dans le monde des PC, sont aujourd'hui transférées sur les mobiles. De plus la taille des appareils favorise le vol ou tout simplement l'oubli dans les lieux publics.

Pour pallier le problème de la perte ou du vol, certains opérateurs permettent d'effacer l'intégralité des données contenues dans un Smartphone à distance via le réseau. Ainsi une personne malveillante ne pourra pas exploiter les données du Smartphone, cependant cela peut poser de graves problèmes si ce pirate prend la main sur l'infrastructure pouvant ainsi effacer en masse le contenu des dits terminaux. A ce niveau, les failles sont critiques.

De plus le chiffrement de bout en bout résiste-t-il bien aux interceptions ? Quels sont les « bouts » ? Si un utilisateur lit ses données confidentielles dans un train, une personne pourrait lire par-dessus son épaule.

Généralement le chiffrement est réalisé entre le Smartphone et le réseau de l'entreprise. Que deviennent les informations ensuite ?

Par ailleurs, le pirate ne vise jamais les points forts d'une architecture. Par exemple, au lieu d'attaquer le chiffrement, il pourrait plutôt concentrer ces efforts sur une faille applicative, qui peut être la lecture d'une pièce jointe, ou une faille du navigateur Web. Les applications mobiles sont souvent moins robustes que sur un PC, du fait des contraintes d'un système embarqué. En effet,

La qualité de service expliquée à ceux qui n'y connaissent rien

La qualité de service, couramment nommée « QoS » - *Quality of Service* – s'intéresse aux facteurs qui influent sur la satisfaction de l'utilisateur final. Les services comme les contraintes qui y sont liées sont particulièrement variés. Ainsi, les services interactifs (jeux, téléphonie ...) nécessitent un faible temps de réponse, les services synchrones (vidéo, téléphonie ...) demandent un rythme du signal en sortie du réseau identique à ce qu'il est en entrée, les réseaux de stockage s'appuient sur un temps de réponse court et une perte d'information faible ...

Le sujet est vaste, limitons-nous ici à quelques-uns des mécanismes qui altèrent le transport de la voix.

Le temps, cet ennemi ...

Exemple de phénomène indésirable : l'écho. Si l'écho améliore le confort des échanges téléphoniques lorsqu'il est quasi simultané, il rend les conversations impossibles dès qu'il est décalé.

L'écho est généré par le bouclage entre émission et réception, le temps pris pour retourner le signal à la source créant le délai d'apparition de l'écho. Le phénomène apparaît dès 10 millisecondes, mais

malgré l'augmentation des fonctionnalités, il ne faut pas perdre de vue que la puissance de calcul reste inférieure à celle d'un ordinateur.

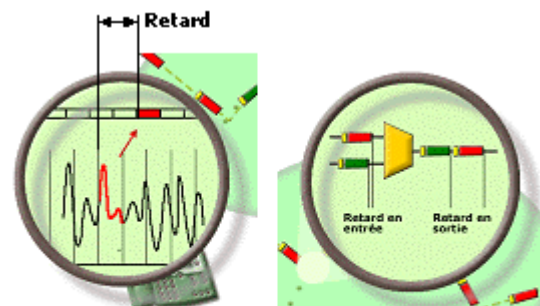
Les moyens de protections ne se sont pas fait attendre, des antivirus ou des systèmes de chiffrement de données sont disponibles sur le marché. Des systèmes d'administration, de déploiement de mises à jour ou d'effacement à distance ont également été mis au point.

Conclusion

Des efforts doivent être faits sur l'information et l'éducation des utilisateurs (qui restent le maillon faible de la chaîne de sécurité) ainsi que sur la sécurisation des réseaux par les opérateurs.

Aujourd'hui, ces terminaux mobiles restent au cœur des questions de sécurité. Ils véhiculent les informations à l'extérieur de l'entreprise, milieu difficile à maîtriser. Il est donc primordial de bien élaborer la politique de sécurité et le périmètre d'utilisation.

Ecrit par un groupe de stagiaires de EADS Secure Networks - Céline THULLET, Thomas GALLIANO, Jonathan PIMENTA FERNANDES, Charles DELATTRE.



Le retard lié à la mise en Les variations de retard dans les routeurs
paquets

reste supportable jusqu'à 150 millisecondes grâce à des mécanismes d'annulation. Au-delà, les interlocuteurs doivent eux-mêmes se policer pour éviter que les propos ne se chevauchent.

Autre phénomène, la variation de ce délai donne à la voix un aspect métallique ; en cas de variation trop importante la voix est hachée. Cette variation est nommée gigue ou jitter en anglais.

La téléphonie classique, avec un « tuyau » réservé en permanence permet de maîtriser le délai : il est constant et uniquement fonction de la distance.

Et la voix devient IP

Avec la technologie IP les différents services transportés par le réseau partagent le même média : fibre, cuivre, faisceaux hertziens Les paquets de voix cohabitent avec les paquets de données

Globalement les phases de codage/mise en paquets, traversée du réseau et décodage « coûtent » chacune 50 ms.

La situation se complique dès qu'il y a plusieurs réseaux à emprunter. Les opérations de transcodage sont alors coûteuses tant sur le plan du délai - quelques dizaines de millisecondes - que distorsion.



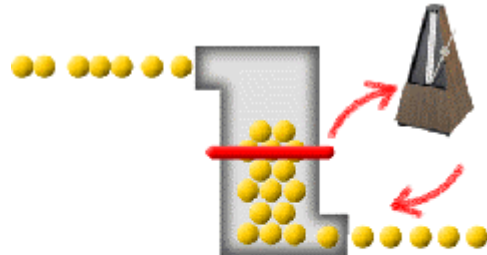
Dès lors les questions et les choix à effectuer affluent : est-il préférable de faire des paquets courts avec peu d'information pour optimiser le temps de mise en paquets au détriment du rendement - les en-têtes des paquets sont toujours là ? La compression du signal ne va-t-elle pas dégrader le remplissage des paquets ? N'est-il pas préférable de compresser les en-têtes ?

Les variations de délai sont générées essentiellement dans les routeurs qui doivent gérer l'arrivée quasi-simultanée de différents flots de paquets de tailles et de cadences aléatoires. Des pertes de paquets peuvent arriver lorsque le trafic est tel que le routeur atteint l'engorgement. Les mécanismes de régulation permettent de freiner l'engorgement en limitant les accès à l'entrée du réseau. Ces mécanismes concernent les trafics qui ne sont pas « temps réel ».

Ces fluctuations, très variables, sont liées au taux d'occupation du réseau. On relève couramment une fluctuation de quelques 10 millisecondes avec des pics de plusieurs centaines de millisecondes.

Des outils pour maîtriser du temps

Pour absorber les variations, le signal est lissé en sortie par des mémoires tampon.



Un exemple de mémoire tampon : les paquets remplissent à une cadence quelconque une mémoire dont la cadence de sortie est asservie au seuil de remplissage..

Le signal est restitué avec un débit constant. Le retard introduit est une des origines du retard de 50 millisecondes évoqué précédemment.

Lorsque les variations de retard sont telles que la mémoire tampon ne peut les absorber, des paquets sont perdus et le signal est haché.

Les mécanismes de qualité de service proposés aujourd'hui permettent de réduire à la fois le temps de traversée du réseau et ses variations en donnant la priorité aux flux sensibles, en réservant la bande passante ou en imposant une route dans le réseau qui affine la répartition du trafic grâce à de l'ingénierie de trafic. La gestion des réseaux s'appuie sur des logiciels grâce auxquels le comportement est simulé.

Les phénomènes qui ont une incidence sur la qualité de service sont connus et un certain nombre de mécanismes permettent de les pallier. Les modes de fonctionnement tels que la réservation de bande passante ou le ratio « overhead » sur charge utile soulignent que l'avantage du passage en IP est au niveau de la « mutualisation » des ressources de transport et plus qu'au niveau d'un gain en bande passante.

Jacques BAUDRON, iXTEL
Secrétaire Général Forum ATENA
jacques.baudron@ixtel.fr

La signature électronique expliquée à ceux qui n'y connaissent rien en cryptologie

Prenons l'incontournable couple de la littérature en cryptologie : Alice et Bob.

Quand Alice reçoit un document papier de Bob, elle vérifie que le document est bien signé par celui-ci, ce qui établit que Bob l'a au moins lu avant de l'envoyer. Elle vérifie aussi que l'enveloppe, dans laquelle Bob l'a mis, n'a pas été altérée, ce qui établit que le document n'a pas été modifié par une autre personne, après que Bob l'a signé et avant sa réception.

Dans un échange de document numérique, la **signature électronique** atteste de l'**authenticité** du document (il vient bien de Bob) et de son **intégrité** (il n'a pas été altéré).

Comment prouver ses deux notions ? Permettez-moi d'expliquer d'abord, le plus simplement possible, à vous béotiens de la cryptologie, deux petites technologies : le **chiffrement asymétrique** et le **chiffrement à sens unique**.

Le chiffrement asymétrique

Ce chiffrement dit aussi chiffrement à clé publique met en jeu un couple de clés. **Une clé privée** et **une clé publique**, qui sont bien sûr liées par plusieurs propriétés. Un exemple est le chiffrement **RSA**.

- La clé privée, comme son nom l'indique doit rester la propriété de son propriétaire (ici Bob) et ne doit en aucun cas être divulguée par lui. La clé publique qui lui correspond est, toujours comme son nom le laisse supposer, une information à diffuser largement au contraire.
- Connaissant une clé publique, il est mathématiquement, disons « quasi-impossible », de retrouver en un temps raisonnable la clé privée qui lui correspond. Ceci repose sur des problèmes mathématiques particulièrement ardues à résoudre comme la factorisation d'un grand nombre en deux nombres premiers, ou le problème du logarithme discret, mais ne nous égarons pas, restons simples et basiques.
- Ce que Bob chiffre avec sa clé privée ne peut être déchiffré que par ceux qui détiennent sa clé publique correspondante. Ce que Alice a chiffré avec la clé publique de Bob ne peut être déchiffré que par Bob qui est le seul à connaître sa clé privée.

Vous êtes toujours avec moi ?

Chiffrement à sens unique

Il ne s'agit pas ici de chiffrer un document pour le déchiffrer ensuite mais juste de calculer une empreinte qui va caractériser ce document (on dit un condensat en français quand on est puriste et un hash quand on abuse d'anglicismes).

Cet article ou la totalité de cette newsletter, passés par un algorithme de chiffrement à sens unique (mettons le **SHA1**) produit une suite de 160 bits. Tous les volumes numérisés de la Comédie Humaine de Honoré de Balzac vont de même, passés par l'algorithme de chiffrement à sens unique, produire une suite de 160 bits.

Si on change ne serait-ce qu'un accent ou une virgule, dans un document, l'empreinte produite à partir du document modifié est complètement différente. Ainsi l'empreinte d'un document calculée par ce chiffrement à sens unique caractérise bien ce document.

Le mécanisme de la signature électronique

Bob veut envoyer un document signé électroniquement à Alice. Il passe, automatiquement via son outil de signature bien entendu, par les étapes suivantes :

- Il calcule l'empreinte du document grâce à une fonction de chiffrement à sens unique ;
- Il chiffre cette empreinte avec sa clé privée, que seul lui possède ;
- Il joint l'empreinte chiffrée au fichier et envoie le tout à Alice.

Alice reçoit l'ensemble, document et empreinte chiffrée. Elle possède la clé publique correspondant à la clé privée que Bob n'a révélée à personne.

Si vous avez bien suivi, il ne s'agit pas ici de chiffrer le document lui-même, la confidentialité d'un document n'ayant rien à voir avec sa signature.

Via son outil de vérification de signature Alice passe alors par les étapes suivantes :

- Elle sépare document et empreinte chiffrée ;
- Elle déchiffre l'empreinte avec la clé publique de Bob ;
- Elle calcule l'empreinte du document reçu par la même fonction de chiffrement à sens unique que Bob et obtient l'empreinte du document reçu ;
- Elle compare l'empreinte déchiffrée et l'empreinte recalculée par elle.

Si les deux empreintes sont les mêmes cela prouve :

- Que l'empreinte reçue a bien été chiffrée par Bob qui seul possède sa clé privée, et puisque Alice l'a déchiffrée avec la clé publique de Bob, cela établit l'authenticité du document : il vient bien de Bob.
- Que le document n'a pas été modifié au passage puisque l'empreinte recalculée n'aurait alors pas été la même que l'empreinte déchiffrée, ce qui établit l'intégrité du document

Le document reçu par Alice est alors réputé avoir été envoyé par Bob et n'avoir pas été modifié avant ou au cours du transfert. Ce document est alors dit « **signé électroniquement** » par Bob.

Mais cette clé publique de Bob, qui prouve à Alice que c'est bien celle de Bob ???

C'est là une excellente question et qu'il fallait soulever. Si on s'en tient à ce qu'on a dit jusque là, rien ne le prouve en effet, donc il manque quelque chose.

Il manque la notion de « **certificat** ».

Quand Alice récupère la clé publique de Bob, elle ne récupère pas en fait cette clé sous sa forme brute. Cette clé, qui rappelons-le n'est pas un secret (elle est publique) est contenue dans un **certificat numérique**. Ce certificat atteste que la clé publique récupérée par Alice est bien celle de Bob, que nous sommes dans la période de validité de cette clé publique et, surtout **ce certificat est signé**

électroniquement par une autorité à laquelle Alice fait confiance.

Signé électroniquement par une autorité de confiance ? Et oui, Alice possède la clé publique de l'autorité de confiance qui va lui servir à déchiffrer l'empreinte du certificat de Bob. Donc elle calcule l'empreinte du certificat puis le compare à l'empreinte déchiffrée, mais ce principe nous l'avons déjà expliqué quand nous avons parlé du document que Bob a envoyé à Alice.

Mais qui a délivré certificat et clés asymétriques à Bob et sur quels justificatifs ?

C'est sûr que si c'est moi qui vous délivre votre clé privée et votre certificat contenant votre clé publique correspondante, par e-mail, sans vous connaître, ce serait la porte ouverte à tous les abus. Mais si c'est une autorité de confiance, voire même une autorité officielle, qui s'assure que la personne, à qui on délivre la clé privée et le certificat contenant la clé publique, est bien celle qu'elle prétant être, alors les choses sont acceptables, et la signature électronique a même force de loi aujourd'hui en France que la signature papier ... si bien sûr le certificat a été obtenu de manière acceptable.

Que c'est compliqué !!! En tout cas pour l'utilisation, c'est très simple. D'ailleurs si vous avez déclaré vos revenus par l'Internet, c'est ainsi que vous avez procédé, bravo ! ;-)

Gérard Peliks, EADS et président de l'atelier sécurité de Forum ATENA

AGENDA

Cette rubrique vous permet de connaître les prochains rendez-vous de la profession que nous organisons ou pour lesquels nous sommes partenaires. Ils sont aussi l'occasion de nous rencontrer et de vous faire participer à ces échanges.

N'hésitez pas à consulter régulièrement la rubrique « Agenda » sur notre site web pour consulter les dernières mises à jour directement.

Les Rendez-vous de la rentrée

Mardi 3 octobre 2007

Solutions Demat avec l'intervention de Gérard Peliks, EADS et président de l'atelier sécurité de Forum ATENA

Certificat et signature électroniques : notions essentielles, applications et mise œuvre
mercredi 3 octobre 2007 de 10 h 30 à 12 h 30 au
Cnit Paris La Défense

Renseignements et Inscriptions :

Accès gratuit après inscription obligatoire sur
www.salons-solutions.com

Si vous souhaitez contribuer à notre prochaine édition, n'hésitez à nous faire part de vos suggestions à l'adresse redaction@forumatena.org

PUBLICATIONS

Retrouver sur le site www.forumatena.org nos nouveaux livres blancs que vous pouvez télécharger gratuitement.

Ce mois-ci, un livre blanc édité par l'atelier FTTH

<http://www.forumatena.org/LB73/WhyPON.pdf>