

## EN BREF

## SÉCURITÉ

## CRYPTO : L'ALGORITHME HIME SERA UNE NORME ISO EN JUIN

Selon le *Nikkei Business Daily*, le système cryptographique à clé publique Hime développé par Hitachi accèdera au statut de norme internationale ISO au mois de juin prochain. Hime permettrait de crypter des données dix fois plus rapidement que l'algorithme RSA, tout en restant peu gourmand en ressources. Le gain en vitesse lors du décryptage serait, lui, compris entre deux et trois. P.A.

WWW.ELECTRONIQUE.BIZ

## ➔ L'UIT s'attaque à la normalisation de la TV sur IP

## ➔ Disques durs : bientôt plus d'octets par secteur

taper le titre dans la boîte "chercher"

## MODULES EMBARQUÉS

## LE LECTEUR RFID/NFC SE RÉDUIT AU FORMAT MINISD

Le Canadien Wireless Dynamics assure être le premier à lancer un lecteur-enregistreur de puces RFID et NFC (Near Field Communication) au format miniSD (21,5x20 mm). Insérable dans tous les PDA et smartphones équipés d'emplacements ad hoc, la carte intègre un processeur sécurisé SAM (Secured Access Module) et peut s'utiliser pour des opérations de paiement sans contact. P.A.

## LIAISONS SANS FIL

## UNE NORME IEEE À L'ASSAUT DU SPECTRE TV INUTILISÉ

En s'accordant début avril sur une proposition unique, le comité IEEE 802.22 a franchi une étape décisive dans la phase d'élaboration d'une future norme pour réseaux sans fil dits "régionaux", exploitant les canaux libres dans le spectre TV (voir *EIH* n°576). Sur chaque zone de couverture d'un émetteur UHF/VHF, bon nombre de canaux restent en effet vacants et pourraient être mis à profit par des réseaux radiocommuns fixes en point à multipoint. D'autant que des portées de 40 km sont envisageables à ces fréquences. P.A.

## TECHNOLOGIES AUDIO/VIDÉO

## La protection d'un contenu ne passe plus forcément par le cryptage

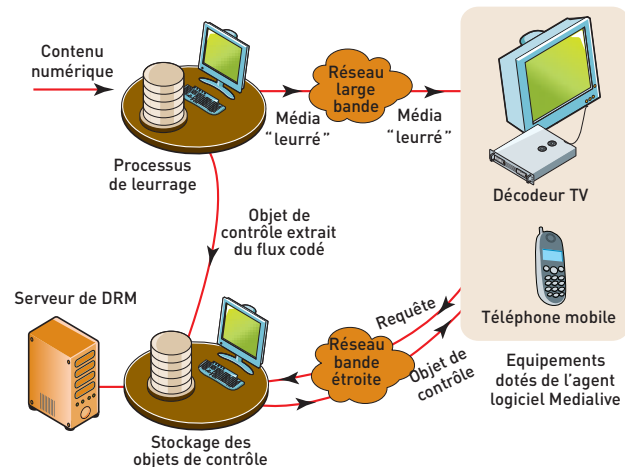
Le Français Medialive a inventé un procédé de protection des contenus multimédias numériques qui repose sur le remplacement d'une infime partie d'un flux codé original par des leurres. Cette technologie s'avère bien adaptée aux contraintes du marché des mobiles.

**A** l'heure où piratages divers et variés font perdre annuellement plusieurs milliards de dollars aux industries du disque et du cinéma, les technologies de protection des contenus multimédias numériques, et tout particulièrement celles utilisables de bout en bout (de la production à la diffusion et au stockage), ont le vent en poupe. Les techniques classiques de chiffrement, aussi sophistiquées soient-elles, affichent néanmoins quelques faiblesses : la gestion des clés reste une opération délicate et le risque qu'un éventuel pirate casse ces clés, ou le système qui les gère, n'est jamais à exclure. Mais existe-t-il vraiment d'autres alternatives ? Oui, comme l'affirme et le démontre le Français Medialive. Créée en 2000, cette jeune pousse a développé un procédé de protection – arrivé aujourd'hui au stade de la maturité industrielle – qui consiste non pas à crypter directement le contenu multimédia, mais à en soustraire une petite quantité d'informations pertinentes et à remplacer ces informations par des leurres.

## Une connaissance de la perception auditive et visuelle

Une grande partie du savoir-faire de Medialive, dont la technologie est couverte par une trentaine de brevets, réside dans une connaissance approfondie de la perception auditive et visuelle de l'être humain. Selon la société, il suffit en effet de retirer seulement 1 % des données incluses dans un flux codé – mais ce 1 % doit être judicieusement choisi(\*) – et d'échanger ces données par des valeurs aléatoires pour le rendre inexploitable... Membre des comités de normalisation ISO/IEC JPEG2000 et MPEG et, par conséquent, très au fait de la syntaxe des flux numériques multimédias, Medialive s'arrange également pour que le flux "leurré" soit strictement identique en taille et en format au flux original. Cette caractéristique évite toute surconsommation de bande passante et permet aux décodeurs audio/vidéo de fonctionner de manière habituelle, sachant que le rendu de l'image ou du son leurré est modulable. Dans la pratique, un serveur dit "de

## Remplacer 1 % du flux numérique par des leurres



Le 1 % vital extrait du flux numérique par le serveur de "leurrage" forme un objet de contrôle qui n'est transmis au récepteur qu'après paiement ou validation d'une autorisation d'accès. Intégré dans le récepteur, l'agent Medialive peut alors reconstituer le flux original.

leurrage", installé dans le réseau du fournisseur de services, se charge, après analyse du contenu, de retirer le 1 % vital du flux numérique à diffuser, à télécharger ou à émettre en *streaming* et d'y injecter des valeurs fausses. Les données extraites forment alors un "objet de contrôle" qui est stocké sur un autre serveur et qui n'est transmis au récepteur (PC, décodeur TV, téléphone mobile ou baladeur multimédia) qu'après paiement ou validation d'une autorisation d'accès. Le terminal, de son côté, doit intégrer un agent logiciel spécifique, "l'agent Medialive", de relativement faible empreinte mémoire (150 Ko). Cet agent a deux fonctions. D'une part, il détecte la réception d'un flux leurré et envoie les informations d'identification et d'authentification à un serveur de DRM chargé de vérifier les droits afférents. C'est lui, d'autre part, qui récupère l'objet de contrôle envoyé lorsque l'achat est validé, qui le synchronise avec le flux leurré, et qui recompose en temps réel le flux multimédia numérique original. Pour une sécurisation renforcée, l'objet de contrôle est lui-même chiffré selon l'algorithme AES 128 bits et décrypté à l'aide, éventuellement, d'une carte à puce.

A noter que l'envoi de l'objet de contrôle, du fait de son encombrement réduit, génère un débit assez faible et peut donc être véhiculé sur un réseau

à faible bande passante (GSM/GPRS notamment), distinct de l'infrastructure utilisée pour envoyer le flux leurré (DVB-T ou DVB-H par exemple).

## Utiliser des cartes SIM

Car, si la solution de Medialive est adaptée à tout type de réseau et fonctionne avec une grande variété de contenus numériques (MP3, AAC+, MPEG-2, MPEG-4, H.263, H.264, JPEG, JPEG2000, ...), c'est bien le marché des terminaux mobiles qui est dans la ligne de mire du Français. Aussi la société a-t-elle déjà entamé des discussions avec certains éditeurs de lecteurs multimédias pour téléphones mobiles évolués afin qu'ils intègrent l'agent Medialive au sein de leurs logiciels. Medialive, dont la solution est compatible avec les scénarios d'usage DRM 2.0 de l'Open Mobile Alliance, compte également se rapprocher des fabricants de cartes SIM. Avec leur capacité mémoire de plus en plus importante, celles-ci pourraient être utilisées pour stocker des objets de contrôle, voire des médias leurrés, ouvrant la voie à de nouveaux usages tels que la "super-distribution" de contenus.

PIERRICK ARLOT

(\*) Dans le cas d'un flux vidéo MPEG, Medialive remplace par des leurres certaines valeurs de vecteurs de mouvement et certains coefficients de blocs de chrominance et de luminance.