La sécurité, problème majeur pour les plates-formes de diffusion de flux multimédia adaptables

Ahmed Reda Kaced and Jean-Claude Moissinac

GET-ENST-CNRS UMR 5141
37-39 Rue Dareau 75014 Paris {kaced, moissinac}@enst.fr

Résumé La diffusion multimédia bouleverse actuellement l'Internet et les réseaux d'entreprise. Les plates-formes de diffusion de contenus multimédia se vulgarisent de plus en plus (P2P, VoD, vidéosurveillance, imagerie médicale, etc.). Les techniques de communication et les moyens d'accès se diversifient en conséquence. Néanmoins, ce développement rapide se voit entravé par l'absence de politiques de sécurité assez fiables, l'un des obstacles majeurs est certainement la gestion des droits (DRM) et les risques de piratage, problème qui s'amplifie encore dans les cas de flux multimédia adaptables sur des réseaux hétérogènes.

Cet article a donc pour but d'expliquer les vulnérabilités généralement exploitées par les pirates pour s'introduire dans les systèmes de diffusion de flux multimédia et pour s'approprier les contenus échangés. Il ne vise pas à expliquer comment compromettre un système mais à comprendre la façon dont il peut l'être afin de mieux pouvoir s'en prémunir. En effet, la meilleure façon de protéger un système est de procéder de la même manière que les pirates afin de cartographier les vulnérabilités du système. Ainsi cet article ne donne aucune précision sur la manière dont les failles sont exploitées, mais présente les vulnérabilités et les attaques qui les ciblent, permettant de déterminer des moyens efficaces pour les contrer.

Un prototype de plate-forme d'échange de documents multimédia totalement sécurisée est décrit brièvement à la fin de cet article pour valider les solutions proposées.

Mots Clés : Diffusion multimédia, sécurité, adaptation de contenu, piratage.

1 Introduction

Le potentiel de transmission de fichiers multimédia (musique, des jeux vidéo, des séquences de films, des émissions télévisées, etc.) en temps réel, ainsi que d'autres contenus multimédias numériques sur les terminaux mobiles (téléphones portables, PDA, etc.) a déclenché une activité fébrile sans précédent. Actuellement, dans la communauté multimédia, beaucoup de travaux visent l'accès omniprésent aux contenus en ligne [13][24][10]. L'objectif est d'offrir des services partout, n'importe quand, sur n'importe quel terminal. Les difficultés

traitées sont généralement la diversité des documents et contenus multimédia [24], l'hétérogénéité des réseaux d'accès et la variété des terminaux [14]. Ceci a conduit à l'apparition de plates-formes de diffusion multimédia pour les échanges de ces contenus entre des terminaux de différents profils, selon des architectures Peer to Peer (P2P) ou Client-serveur.

Une problématique très importante reste néanmoins récurrente dans ce type de services : il s'agit de l'exposition de ces contenus aux risques d'attaque ou de piratage sur les réseaux lors des opérations de transfert et d'adaptation (*section 3*), ainsi que sur les terminaux à faibles ressources (*section 5*), et la difficulté de la gestion des droits numériques (DRM [12][17], *Digital Right Management*).

Dans cet article, nous nous proposons d'aborder les plates-formes de diffusion multimédia sous l'angle général de la sécurité et des risques d'attaque (des comportements, des ressources disponibles, etc.). Différentes déclinaisons de cette même approche sont proposées :

- types d'attaques envisageables sur les contenus mono ou multimédia échangés (images, vidéos, audio, etc.) ;
- risques liés aux opérations d'adaptation des documents ;
- vulnérabilité des terminaux mobiles.

La suite de l'article est articulée comme suit. Nous commencerons dans la section 2 par présenter l'architecture des plates-formes de diffusion multimédia ainsi que les formats des documents concernés par notre étude. Dans les sections 3, 4 et 5, nous décrirons les risques liés à ces services de diffusion et transactions effectuées sur ces architectures. Nous donnerons ensuite, dans la section 6, quelques solutions envisageables pour résoudre ces problèmes de sécurité et pour se prémunir contre ces attaques. Nous terminerons par la section 7, avec la description de notre plate-forme d'échanges de documents multimédia sécurisées pour valider les solutions proposées.

2 Topologie d'une plate-forme de communication multimédia

Nous distinguons deux types d'architectures de plates-formes de diffusion multimédia selon la nature (adaptabilité) des flux échangés entre les fournisseurs de contenu et les récepteurs. Nous différencions donc les plates-formes où les fournisseurs produisent des flux non adaptables et proposent des versions multiples de leurs contenus, chacune destinée à un profil matériel donné, et les plates-formes reposant sur l'envoi de flux adaptables (*section* 2.2), où une même version sera envoyée à tous les récepteurs, des opérateurs d'adaptation (*proxies*) s'occupant ensuite de fournir le bon format à chaque récepteur selon son profil.

2.1 Plate-forme de diffusion multimédia adaptative

Dans cette étude nous nous sommes intéressés aux plates-formes dites *adaptatives*, c'est à dire utilisant des proxies qui adaptent dynamiquement les données

transmises, de façon à ce que les terminaux récepteurs puissent les exploiter efficacement, sans surcoût lié à leur manipulation.

Les proxies bénéficient de mécanismes d'adaptation comme des filtres (transformation vidéo, modification automatique d'images, redimensionnement, recadrage, etc.), des mécanismes de transcodage (changement de format vidéo/ audio/ images), etc. Les données sont adaptées en fonction des caractéristiques du terminal récepteur et des préférences de l'utilisateur [15].

Les composants qui interviennent dans ce système de diffusion constituent une *plate-forme de communication multimédia adaptative*. La Figure 1 illustre ces composants ainsi que leur organisation physique (clients, serveur, proxies, etc.). L'objectif d'un tel système est de restituer à chaque client l'information générée par le serveur, tout en satisfaisant aux besoins et aux contraintes définis par le contexte de ce client (format, taille d'écran, langue, etc.).

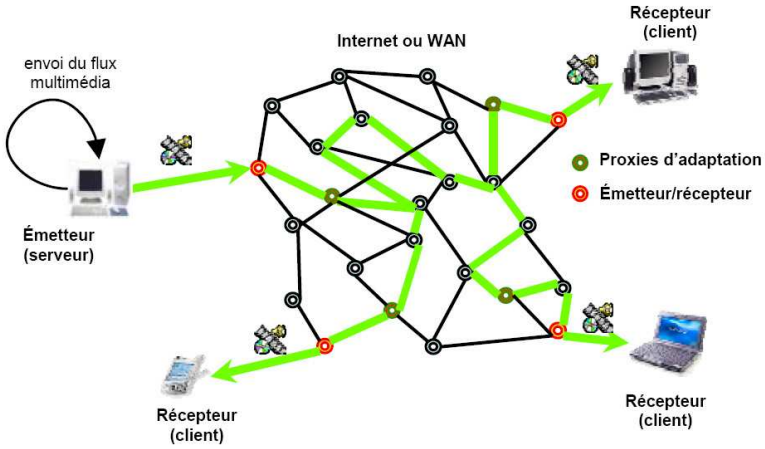

Fig. 1. Topologie de la plate-forme de communication

Émetteur (Serveur) Le serveur a pour tâche de produire les fichiers multimédia adaptables, sous un format bien défini. Il le transmet ensuite, selon la politique de communication, au proxy le plus proche en spécifiant le ou les destinataires.

Récepteurs (Clients) Ce sont des terminaux hétérogènes qui permettent de lire le flux multimédia émis par le serveur. Dans une topologie P2P, ces derniers peuvent aussi jouer le rôle de serveurs.

Proxies Un proxy représente une entité logique placée sur des nœuds intermédiaires dans la plate-forme. Son rôle consiste à récupérer les données des émetteurs, à déterminer les adaptations qui doivent être employées et à envoyer les données adaptées aux autres proxies ou directement aux clients.

La fonction principale de cette plate-forme de communication, qui la différencie d'un système de communication classique, est de confronter les présentations multimédia auxquelles un utilisateur accède avec le contexte l'environnant. Le résultat de la confrontation, c'est-à-dire l'adaptation des présentations multimédia au contexte de l'utilisateur, est la production d'une présentation qui correspond aux besoins et aux contraintes du contexte du récepteur.

En termes de sécurité, la plate-forme de diffusions doit garantir :

- l'authenticité du document multimédia transmis de bout en bout malgré l'adaptation (qui l'a envoyé ?) ;
- l'intégrité des données du document multimédia (ont elles été modifiées durant la transaction ?) ;
- la non-répudiation du document (son auteur ne peut démentir l'envoi du document original, non adapté).

2.2 Document multimédia adaptable

Nous appelons *document multimédia adaptable* tout document structuré composé d'un ensemble de médias de différents types : textes, images, animations, vidéos synthétiques ou réelles, sons synthétiques ou réels, et dont la présentation comporte une composante spatiale, hypertexte éventuellement, mais aussi temporelle, et permettant l'adaptabilité de ces médias à différents types de terminaux. Un tel document multimédia peut se présenter sous forme d'un :

- fichier textuel, écrit dans une forme déclarative (HTML, SMIL [1], etc.) ou non, additionné à un ensemble de médias séparés ;
- fichier binaire (AVI, MPEG, etc.).

Il existe ainsi plusieurs formats de flux multimédia adaptables (MPEG-4, MPEG-21 [17], SMIL, SVG, Flash), et notamment une grande variété dans les documents structurés. Notons que depuis ces dernières années, les flux utilisant des métadonnées XML sont de plus en plus utilisés. C'est sur ces derniers que nous avons axé notre étude ci-présente.

Le standard XML, défini par le W3C [21][22], est en effet apparu comme le plus adéquat pour atteindre les objectifs de l'adaptabilité. Le principe de ce format est le même que pour tous les formats de documents structurés : les éléments de structure sont délimités par une balise de début d'élément et une balise de fin d'élément. Chaque balise de début d'élément contient le type de l'élément et éventuellement ses attributs. Le contenu de l'élément est situé entre les deux balises.

3 Risques liés à la plate-forme de communication

Tout composant du système de communication dans une plate-forme de diffusion est potentiellement vulnérable à une attaque visant à récupérer le flux multimédia, le modifier, se l'approprier, etc., ou perturber le fonctionnement du système adaptable. Ces attaques sont en réalité généralement lancées automatiquement à partir de machines du système adaptable infectées (virus, chevaux de

Troie, vers, etc.), à l'insu de leur propriétaire, ou encore activées par des pirates informatiques.

Si l'on considère une plate-forme de diffusion utilisant des communications via Internet. L'acheminement des flux sans itinéraire préconçu fait qu'il est impossible de savoir par où passent les données, et donc d'avoir la garantie que le chemin emprunté est sans danger. En effet, les informations envoyées d'un ordinateur à l'autre peuvent passer par un certain nombre de machines avant d'atteindre leur destination. Rien n'empêche un utilisateur de ces machines intermédiaires d'intercepter le trafic qui transite par elles. Plusieurs techniques d'attaques réseaux sont envisageables pour récupérer les flux transitant, Sniffing, Spoofing, Deny Of Service, etc.

Dans notre contexte, nous distinguons deux niveaux d'attaques réseau éventuelles sur la plate-forme :

3.1 Scénario 1 : Attaque pré-adaptation

Dans ce cas de figure, le pirate est positionné entre le serveur et les proxies d'adaptation ; il a pour objectif de récupérer les flux multimédia transitant avant les opérations d'adaptation, afin d'exploiter l'aspect adaptable du document multimédia qui le rend vulnérable, pour le modifier, se l'approprier ou le diffuser illégalement.

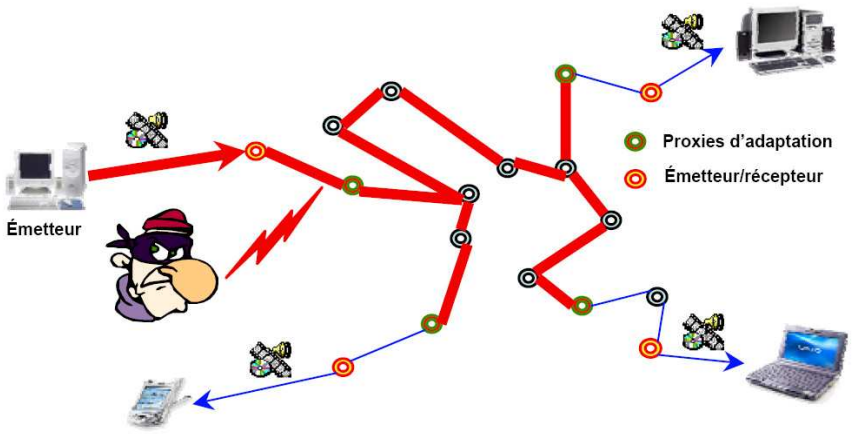

Fig. 2. Attaque Attaque pré-adaptation

3.2 Scénario 2 : Attaque post-adaptation

Ici le pirate est positionné sur le réseau entre les proxies d'adaptation et les clients, ou attaque directement le terminal récepteur ; il peut aussi récupérer le flux multimédia transitant afin de le copier et le diffuser illégalement.

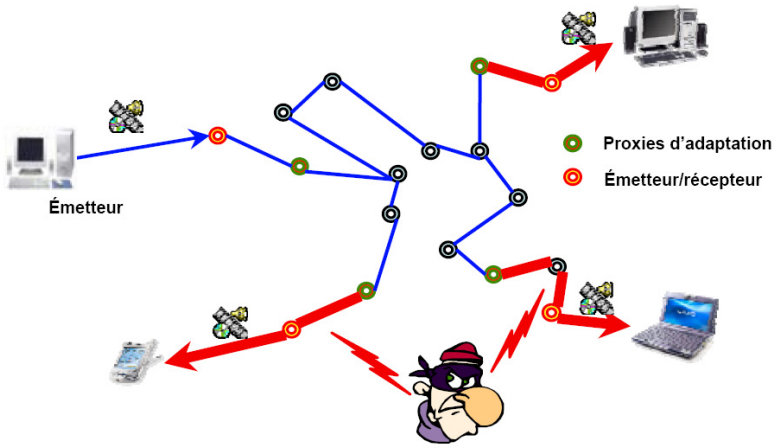

Fig. 3. Attaque post-adaptation

Pour garantir l'intégrité et la confidentialité des flux transmis et palier les failles de sécurité sur les liens de communication, une solution serait la mise en œuvre de méthodes de chiffrement des flux transmis, évitant les risques de piratage de ces derniers tout en préservant leur aspect authentifiable.

Pour assurer l'authentification et la non-répudiation des documents multimédia, une solution classique est de mettre en œuvre des mécanismes de signature numérique. Une vérification réussie de la signature numérique permet au récepteur de confirmer l'identité de l'expéditeur et empêche l'expéditeur de répudier le document.

Ces mesures de signature/chiffrement « classiques » sont très pertinentes dans le cadre de diffusion de flux non adaptable. Nonobstant, dans notre contexte les contenus doivent autoriser les opérateurs d'adaptation à effectuer les changements nécessaires sur le document avant sa diffusion. Toute signature sera donc invalidée après une opération d'adaptation. Nous présentons dans la section 7 une solution fondée sur un chiffrement « lien à lien » des données transmises et un mécanisme de signature autorisant les opérations d'adaptation.

4 Attaques possibles sur les flux multimédia

Comme nous l'avons cité dans le paragraphe 2.2, la forme standard d'un document multimédia adaptable est l'association d'une description métadonnée et d'un ensemble de médias (images, fichiers audio, fichiers vidéo, texte, etc.).

Si la signature numérique du flux multimédia permet l'authentification de son émetteur, il existe d'autres techniques plus « persistantes » pour la sécurisation des flux média le constituant. Le tatouage numérique ou, *watermarking* [6] se présente comme la solution ultime de protection des données média. Son principe est d'insérer une marque imperceptible dans les valeurs de la donnée. Dans le cadre de la protection des droits d'auteurs, la marque insérée, appelée « *watermarque* » correspond au code du copyright qui permettra alors d'identifier le propriétaire. Ce type de tatouage doit répondre à des contraintes fortes en termes de robustesse. Idéalement, quelles que soient les transformations (licites ou illicites) que la donnée tatouée subit, la marque doit rester présente tant que la donnée reste exploitable. De plus, la présence de la marque ne doit être détectée que par des personnes autorisées (possédant une clef de détection privée).

De nombreux algorithmes ont étés présentés récemment et certains produits sont même commercialisés, cependant, aucun d'eux ne satisfait pleinement au cahier des charges idéal pour les flux adaptables. Nous présentons dans ce qui suit quelques types d'attaques envisageables sur des flux médias numériques tatoués visant à contourner cette méthode de sécurisation. Pour plus de détails vous pouvez consulter [6], [7] et [9].

- Attaque par **cropping** : elle consiste à extraire un morceau non tatoué d'un flux média pour le réutiliser. Pour être résistant à ce type d'attaque, le tatouage doit être présent sur tout le média. La même situation se produit dans le domaine fréquentiel du média où la marque doit être partout présente afin d'éviter une destruction par **filtrage** passe bande.
- Les algorithmes de **compression** peuvent être des attaques particulièrement dangereuses pour les processus de tatouage puisque leur objectif est exactement l'opposé de celui du tatouage. On veut en effet, par l'utilisation de ces algorithmes ne garder du média que les composantes essentielles à leur compréhension.

Des méthodes plus complexes cherchent à retirer « chirurgicalement » la marque du signal tatoué. Cette opération peut être très facile dans un cas particulier : si l'implémentation de la marque ne dépend pas du média. Dans ce cas, un pirate possédant plusieurs médias différents contenant la même marque pourra enlever celle-ci. En effet, un simple **moyennage** des médias donnera une estimée de la marque, qu'il pourra alors retrancher aux médias tatoués. Cette situation peut par exemple avoir lieu si l'on marque une séquence de film. On imposera donc que l'étape d'implémentation de la marque soit dépendante du média, on dira que le tatouage est statistiquement imperceptible.

- L'attaque de **l'impasse** inhibe directement le protocole de tatouage. Cette attaque est due à un défaut d'injectivité de l'application d'implémentation de la marque.

- Attaque par **collusion** : L'attaquant possède plusieurs copies du même contenu avec quelques différences provenant de l'individualisation des watermarques. Il les combine ensuite pour obtenir des documents qui ne contiennent plus aucun signal de tatouage. cette attaque peut être utilisée pour perturber les marques individualisées de type *fingerprint* qui permettent d'identifier le client.
- L'attaque par **surmarquage** consiste à tatouer à nouveau un média déjà tatoué. Pour certains schémas, en particulier si les lieux de tatouages sont fixés, cette attaque peut être très dangereuse. Certains protocoles de tatouage se protègent en vérifiant, avant de distribuer une clef, que le média original proposé n'est pas tatoué. Cette protection n'est utile que si le schéma de tatouage demeure inconnu. En effet, s'il est connu, un pirate peut ajouter une marque de sa fabrication qui invalidera la détection.
- L'attaque par **recopie** consiste à recopier une marque obtenue préalablement (par exemple par estimation) sur un média non marqué. Le détecteur validera alors le nouveau média comme étant tatoué.

Il existe aussi d'autres attaques spécifiques aux différents types de média (images, vidéos, etc.), nous n'avons pas fait ici une description exhaustive de toutes les attaques existantes. Néanmoins, les avancées récentes dans le domaine du tatouage numérique présentent plusieurs solutions et algorithmes de tatouage qui permettent d'éviter ou de contrer ce type d'attaques. Furht présente dans [9] un panorama complet sur ce sujet.

Une des conclusions de cette étude globale sur les attaques sur le tatouage est d'accorder une grande importance à la sécurisation des médias constituant le document multimédia, en plus de la sécurisation de la description métadonnées de ce dernier. Les attaques sur les médias tiennent une place très importante dans le cahier des charges d'un processus de sécurisation puisqu'elles définissent la robustesse d'un système.

5 Vulnérabilité des terminaux mobiles

De plus en plus d'utilisateurs commencent à télécharger diverses applications et contenus multimédia sur leurs PDA et téléphones portables, dont beaucoup fonctionnent avec des systèmes d'exploitation ouverts de type Symbian [18] ou Microsoft. Étant équipés d'un système d'exploitation, il est inévitable que ces terminaux deviennent plus vulnérables aux attaques. Le manque de mécanismes de sécurité protégeant la valeur du contenu numérique sur ces terminaux portables étant un frein majeur pour l'explosion du multimédia mobile.

Ni l'industrie des portables ni les propriétaires de contenu n'ont trouvé une solution qui leur convienne mutuellement pour protéger ces terminaux portables contre les « maladies électroniquement transmissibles ». Parmi les questions qui restent en suspens on peut citer : où mémoriser le contenu chiffré et comment le protéger ? Quel composant doit être chargé de mémoriser un code privé qui déverrouille et déchiffre le contenu ? Comment transmettre en toute sécurité le contenu numérique déchiffré à un lecteur multimédia intégré au terminal mobile

pour le décodage MP3 ou H.264 ? Comment faire appliquer les règles d'utilisation du multimédia numérique sur un terminal mobile d'une manière efficace et conviviale ?

Les attaques sur ce type de terminaux se font souvent via une interface réseau sans fil : liaisons Wi-Fi ouvertes, failles dans Bluetooth (*BlueSnarfing, Backdoor, Bluejacking.*.) [19], les PDA et Pocket PC posent aujourd'hui des problèmes de sécurité spécifiques, les programmes malfaisants (virus, chevaux de Troie), se propageant via ces interfaces.

La menace s'est matérialisée pour la première fois l'année dernière lorsqu'un programme malfaisant pour téléphones mobiles, un ver, appelé Cabir, a été lâché dans la nature par le groupe de hackers ¡¡ 29A ¿¿. Leur but affiché n'était que de prouver la faisabilité du concept et d'alerter le monde. Depuis, Cabir s'est métamorphosé en un peu plus de 15 variétés et sa trace a été retrouvée dans 14 pays.

La vulnérabilité des terminaux mobiles aux attaques réseaux ou virales s'explique en partie par la prédominance d'une seule plate-forme informatique. La première vague d'attaques visant les terminaux mobiles a choisi pour cible le système d'exploitation Symbian. Heureusement, les mobiles ne sont pas aussi homogènes que les PC : une faille affectant des appareils Symbian laisse des millions d'autres appareils indemnes. Mais il n'y a guère de raison de se satisfaire de la situation.

Dans les architectures actuelles, concernant les attaques visant à récupérer les flux multimédia, une fois qu'un fichier numérique est transmis puis déchiffré sur le processeur, il est transféré « en clair » vers un lecteur multimédia sur le terminal [23], exposant ainsi la liaison lors de laquelle les informations internes du DRM peuvent être copiées. Il existe des solutions techniques à ces problèmes. Le plus dur est de faire la part des choses en ce qui concerne le coût, la sécurité, la commodité et les bénéfices pour les opérateurs, les propriétaires de contenu et les utilisateurs.

Quelques constructeurs veulent mettre en œuvre la gestion des droits numériques (DRM) [12] sur une carte à puce. D'autres, poussent pour un DRM intégré à un moteur de sécurité câblé, sur une bande de base ou sur un processeur d'applications. D'autres fournisseurs de puces, proposent des solutions DRM similaires au niveau des processeurs, combinant matériel et logiciel. Ils proposent également des solutions DRM alternatives, et même concurrentes conçues spécifiquement pour les cartes SIM (téléphones) ou pour les cartes flash amovibles (PDA, etc.). L'utilisation de ces cartes flash représente la troisième méthode, qui permet d'enregistrer et d'exécuter les agents DRM sur des cartes multimédia sécurisées, telle que la carte ¡¡ SecureMMC ¿¿ [23].

6 Proposition d'un schéma de sécurisation

Compte tenu des vulnérabilités susmentionnées et des nombreux aspects liés à la sécurité, à l'authentification et aux autorisations, à la confidentialité et à l'intégrité des données, et compte tenu du fait que les communications classiques

sur Internet ne mentionnent pas la sécurité, il est aisé de dire que les communications dans une plate-forme de diffusion « ne sont pas sûres !¿¿. Pourtant, examinons de plus près les services de communication sur Internet. Actuellement, la création de services de communication sécurisés n'est pas chose impossible.

Lorsque l'on aborde la question de la sécurité des communications, il faut examiner les points suivants :

- qu'essayons-nous de réaliser ? Restreindre l'accès à un service à des utilisateurs dûment habilités, éviter que les documents multimédia transmis ne soient lus par des indésirables, etc. ;
- comment allons-nous y parvenir ? Par le réseau, la couche transport, le système d'exploitation, un service ou une application ;
- quel niveau d'interopérabilité recherchons-nous dans le cadre de notre solution ? Un niveau local ou global.

Comment donc sécuriser les communications sur la plate-forme proposée ? En répondant à ces questions et en appliquant les mêmes techniques que celles que nous employons pour sécuriser n'importe quelle autre application, notamment :

- par la sécurisation des connexions ;
- par l'authentification et l'autorisation des interactions.

Comme nous allons le voir, ces techniques offrent des solutions élaborées qu'il est possible de combiner pour optimiser les résultats. Par exemple, il est possible d'utiliser un pare-feu avec un service Web XML [4] afin de limiter l'accès à certaines fonctionnalités (méthodes) en fonction de la nature du client et de stratégies préétablies.

Pour plus de clarté, commençons par examiner chacune des solutions actuellement disponibles pour sécuriser l'infrastructure.

6.1 Sécurisation de l'infrastructure

Un service de communication sûr repose sur une infrastructure sécurisée. Il existe diverses technologies qui, intégrées dans un plan de sécurité global, permettent d'assurer la sécurité de l'infrastructure d'une plate-forme de communication. Le processus de planification relatif à sa mise en œuvre suppose :

- une identification approfondie des risques potentiels liés à l'environnement (virus, pirates, etc.) ;
- une analyse des conséquences d'une violation de la sécurité et des mesures préventives à envisager ;
- une stratégie d'implémentation soigneusement planifiée pour intégrer les mesures de sécurité à tous les niveaux du réseau (clients, proxies, serveurs), en fonction de l'identification et de l'analyse préalablement réalisées.

6.2 Sécurisation des connexions

Une des solutions les plus faciles pour sécuriser ces services de diffusion est d'assurer la fiabilité de la connexion entre le client et le serveur. Pour atteindre cet objectif, plusieurs techniques sont possibles, selon la portée du réseau et le

profil d'activité des interactions. Citons, parmi les plus répandues et les plus accessibles, les techniques suivantes : des règles qui reposent sur l'existence d'un pare-feu, le protocole SSL (Secure Sockets Layer), Kerberos et aussi les réseaux privés virtuels (VPN, Virtual Private Network), .

Si nous savons exactement quels ordinateurs doivent accéder à la plate-forme de communication multimédia, nous pouvons appliquer des règles de pare-feu afin de limiter l'accès sur la base d'adresses IP connues. Cette technique s'avère utile lorsque nous souhaitons restreindre l'accès aux ordinateurs au sein d'un réseau privé, LAN ou WAN par exemple, et que le contenu des flux n'est pas un secret (par conséquent, pas de chiffrement). Les pare-feu tels que ISA Server (Internet Security and Acceleration) [5] offrent éventuellement un ensemble de règles reposant sur des stratégies et permettent de limiter, à des degrés divers, l'accès aux ordinateurs par les clients, en fonction de leur origine ou de leur identité.

Le protocole SSL permet d'établir des connexions sécurisées sur des réseaux non sécurisés (tels qu'Internet). Bien qu'il constitue une solution tout à fait efficace en termes de sécurisation des communications, il pèse sur les performances d'une façon non négligeable. Les services Web XML peuvent gérer le protocole SSL intégré aussi bien au niveau du client que du serveur.

Kerberos est un protocole réseau qui permet aux utilisateurs de s'authentifier par l'intermédiaire d'un serveur sécurisé. Des services comme l'ouverture de session et la copie à distance, la copie sécurisée de fichiers entre systèmes et autres fonctionnalités à haut risque deviennent ainsi considérablement plus sûrs et contrôlables. Ce protocole fonctionne sur un contrôle de l'identité des clients, qui peuvent obtenir par la suite des tickets pour s'authentifier auprès des différents services présents sur le réseau. Toutes les transactions passant par Kerberos sont chiffrées, ce qui résout un ensemble de problèmes de sécurité

Un réseau privé virtuel (VPN) est une extension d'un réseau privé qui assure des connexions sur des réseaux partagés ou publics comme Internet. Via un VPN, vous pouvez envoyer des données d'un ordinateur à un autre sur une connexion sécurisée. Semblable par bien des côtés au protocole SSL, le VPN est une connexion point-à-point à long terme. Aussi exige-t-il une connexion à long terme pour que le gain en termes d'efficacité soit sensible.

6.3 Sécurisation des documents multimédia

La sécurisation de ces documents passe par la sécurisation de toutes les entités constituant le document.

Pour les métadonnées XML, le W3C avec l'IETF ont mis en place deux groupes de travail (XML Signature WG [22] et XML Encryption WG [21]) qui ont pour but de développer une syntaxe XML permettant :

- de représenter une signature de tout ou partie d'un document référençable par une `http://www.w3.org/Addressing/`URI;
- de chiffrer/déchiffrer des documents électroniques (y compris tout ou partie d'un document XML) ;

– d'utiliser une syntaxe XML pour représenter le document signé et les informations permettant de le décoder.

On pourra renforcer cette sécurisation par la sécurisation des médias intervenant dans un flux multimédia en utilisant des techniques de DRM, tatouage, stéganographie, et fingerprinting [3].

6.4 Authentification et autorisations

Authentification : l'authentification est le processus qui consiste à vérifier l'identité d'une personne (ou, plus généralement, de ¡¡ quelque chose ¿¿). Cette ¡¡ personne ¿¿ ou ce ¡¡ quelque chose ¿¿ est l'entité. L'authentification nécessite des preuves, autrement dit des informations d'identification. Par exemple, une application cliente peut fournir un mot de passe comme information d'identification. Si elle présente des informations correctes, le système suppose qu'elle est bien ce qu'elle prétend être.

Autorisations : une fois que l'identité de l'entité est authentifiée, des autorisations peuvent être accordées. Pour qu'il y ait accès à un système, les informations concernant l'entité sont comparées avec des informations de contrôle des accès, par exemple avec une liste ACL (Access Control List). Les accès peuvent varier selon les clients. Ainsi, certains clients ont un accès total au service, alors que d'autres n'ont accès qu'à certaines tâches. On peut accorder à certains clients un accès complet à l'ensemble des données, à d'autres un accès à un groupe limité de données, ou encore un accès en lecture seule.

Une solution parmi les plus simples pour authentifier les accès à un service de diffusion de documents est d'utiliser les fonctionnalités d'authentification du protocole employé pour l'échange des messages. Pour la plupart des services de communications, il s'agit d'exploiter les fonctions d'authentification du protocole HTTP. Des solutions sous forme de services Web XML telles qu'Internet Information Server (IIS) et ISA Server proposent plusieurs mécanismes d'authentification sur HTTP.

7 Plate-forme de diffusion proposée

L'objectif de cet article étant de présenter les risques liés au processus de diffusion de flux multimédia adaptables, nous allons présenter sommairement notre plate-forme de diffusion. Plus de détails peuvent être trouvés dans [13].

Ainsi, pour valider les propositions présentées dans les paragraphes précédents nous avons réalisé SEMAFOR (*SEcure Multimedia Adaptation platFORm*) un prototype de plate-forme de diffusion multimédia (Figure 6), utilisant des Services Web XML. Nous avons aussi opté pour le format des flux multimédia SMIL (descriptions métadonnées XML), qui semble être le plus approprié pour la validation de nos travaux.

SEMAFOR implique deux niveaux de sécurisation :

– sécurisation des documents, qui consiste à fournir un mécanisme de signature de documents autorisant les opérations d'adaptation, tout en préservant l'intégrité des flux échangés ;

– sécurisation des transactions, qui consiste à renforcer les transactions et les messages échangés entre les différents intervenants de la plate-forme.

7.1 Signature des documents multimédia

Nous utilisons dans SEMAFOR un schéma de signature de documents multimédia XML reposant sur la technique de *Tiger-Tree Hashing* (TTH) [2], en représentant le flux à signer sous forme de feuilles d'un arbre binaire de Tiger. Chaque composant est représenté par une feuille, en rajoutant de nouvelles feuilles qu'on appelle *FreeLeaves*, chaque *FreeLeaf* va se positionner à coté d'une feuille correspondant à un média adaptable (Figure 4). Ces *FreeLeaves* permettent l'insertion dynamique d'éléments dans l'arbre de Tiger, et sont instanciées en utilisant des fonctions de hachage à sens unique.

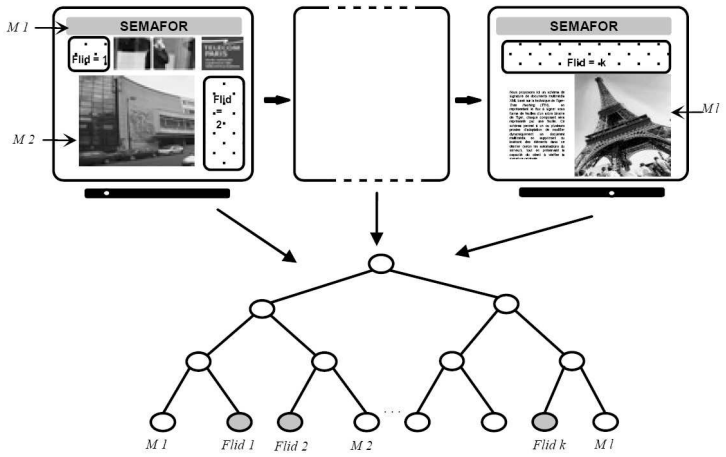

Fig. 4. Représentation du document en Tiger-arbre

Pour la signature de ses feuilles, nous avons adopté la recommandation du W3C sur la signature XML, XML-DSIG, cette recommandation définit un processus pour chiffrer des données et représenter le résultat en XML. Les données peuvent être arbitraires, un document XML, ou une portion de document XML. Le résultat du chiffrement est un élément XML qui contient une référence sur les données chiffrées. Cette technique permet donc, lors d'une diffusion de flux multimédia :

– de garantir l'authenticité du document multimédia de bout en bout malgré l'adaptation ;
– d'assurer l'intégrité des données du document multimédia ;
– d'obtenir la non-répudiation du document.

Ce schéma permet à un ou plusieurs proxies d'adaptation de modifier dynamiquement un document multimédia en supprimant ou insérant des éléments

dans ce dernier (selon les autorisations du serveur), tout en préservant la capacité du client à vérifier la signature originale.

7.2 Sécurisation des transactions

En s'inspirant de bibliothèques de sécurisation de transactions d'e-Commerce reposant sur XML, nous avons défini pour SEMAFOR le protocole XSST (*Xml Secure Semafor Transaction*). XSST est un format de message sécurisé pour les transactions effectuées sur la plate-forme SEMAFOR. Il est décomposé en plusieurs définitions : d'une part la structure des messages et d'autre part les différentes définitions et interactions.

La base d'XSST est le format de message XML utilisé pour l'encapsulation sécurisée des transactions. Le choix d'XML s'est imposé pour deux raisons majeures : d'une part, l'évolution de XML qui permet d'ajouter des éléments dans les versions supérieures sans remettre en question le *parsing* des anciens formats et d'une autre part, la portabilité entre les différentes architectures informatiques. Le format se présente sous cette forme :

```
<XSST xmlns...>
<encryption type="0-2-0-8" id="example" ...>
...
<data type=.../>
...
</data>
<signature type="1-4-1" id="example" ...>
dNGQnaD...
</signature>
</XSST>
```

Fig. 5. Format d'un message XSST

Il y a trois grandes parties dans la structure-même du message XSST :
- *encryption ;*
- *data ;*
- *signature.*

L'élément *encryption* peut apparaître de 0 à n fois dans un même message XSST. Il définit le type de chiffrement de l'élément *data* via l'attribut *type* ainsi que

la clé symétrique via un id (*keyId*) ou la clé de session (*symmetricKey*). La définition du type se fait via une table de correspondance concernant le choix de l'algorithme cryptographique, ainsi que les méthodes de ¡¡*padding*¿¿ mais aussi le mode de fonctionnement en tant que système cryptographique hybride ou non.

L'élément *data* ne peut apparaître qu'une fois dans un même message XSST. Il contient les données, (souvent) chiffrées. L'attribut *encoding* permet de définir le type d'encodage de cette partie (par exemple : Base64). L'attribut *type* définit le type du message. Les types ne sont pas décrits dans le standard de base mais dans des bases complémentaires. Ce type peut être un autre message XSST mais aussi des données spécifiques. Il existe souvent aussi deux sous-éléments à *data* : *tid* et *timestamp*. Ils sont localisés dans cet élément car le chiffrement est effectif à l'intérieur de l'élément *data*. D'autres sous-éléments peuvent apparaître suivant le *type* du message lui-même.

L'élément *signature* peut apparaître de 0 à n fois dans un même message XSST. Il contient la signature de la partie *data*. Le type et la méthode de signature sont contenus dans l'attribut *type* qui est décrit dans une table correspondance équivalente à la partie *encryption*.

L'ensemble du format de message est décrit dans le schéma XML XSST principal. Ce format de message exprime le strict minimum de la transaction, ce sont les utilisations propres des types qui étendent la syntaxe et les échanges.

7.3 Implémentation

Fonctionnellement, le prototype s'organise autour des trois composants : serveur, proxies intermédiaires et clients.

Serveur Le serveur est un peer équipé d'un système d'édition de flux multimédia (SMIL, SVG, etc.), d'un analyseur de métadonnées qui génère la représentation du flux en arbre de Tiger, et des modules de signature XML-DSIG [22] et XML-ENC [21] pour la signature et le chiffrement des médias et du document XML. Ces modules permettent aussi au serveur de signer ces transactions selon le format XSST avec des certificats X509. Il dispose ainsi d'un module de gestion de clés (partagée, privée, secrète) selon la politique de sécurité fixée au niveau du proxy.

Proxy On dispose au niveau du proxy de plusieurs modules :

- un mécanisme d'adaptation de documents multimédia (transformation, transcodage, etc.) ;
- une base de données pour la gestion des profils des différents clients reliés à la plate-forme ;
- un module de communication qui gère les transactions sous le format XSST ;
- des modules de signature et de chiffrement de documents XML pour les documents adaptés et les transactions XSST ; ils permettent la validation de

signatures et de certificats, et ont aussi la charge de vérifier complètement les signatures, de les horodater, et éventuellement les rejeter ;
– et d'un module pour la gestion de la politique de sécurité entre les clients, les serveurs, et le proxy (gestion des clés, vérification, authentification, etc.).

Cette approche permet d'introduire très simplement des fonctions de confiance, l'intervention dans les services de la plate-forme se limitant à rajouter des modules dans les politiques d'adaptation et de sécurité au niveau du proxy.

Client Le client selon ses capacités et son environnement, dispose d'un outil de visualisation de fichier adapté. Il dispose des modules nécessaires pour le déchiffrement et la vérification de signature des documents qu'il reçoit, un module qui gère les transactions XSST, ainsi que les outils nécessaires pour la gestion des clés utilisées lors de ces opérations. La réalisation de cette plate-forme s'appuie sur les travaux réalisés dans l'équipe dans le domaine de l'adaptation de flux multimédia. L'objectif de nos travaux en cours est d'améliorer et d'optimiser le schéma de sécurisation lors de la diffusion des flux multimédia adaptables décrits en XML.

8 Conclusion

Nous avons présenté dans cet article une étude globale des problèmes de sécurité dans les plates-formes de diffusion de flux multimédia, plus particulièrement sur des architectures P2P ou client-serveur, utilisant des proxies d'adaptation quand le flux échangé n'est pas chiffré lors d'une partie ou de tout le long du processus du transfert.

Nous avons pris le cas des flux multimédia adaptables, et nous sommes intéressés aux risques liés à la diffusion de ces flux avant et après adaptation. Nous avons distingué les différents niveaux de risque et les vulnérabilités exploitées à chaque fois. Nous nous sommes ensuite penchés sur les attaques visant les médias eux-mêmes, qui ont comme objectif de contourner les tatouages présents sur ces média. Un dernier niveau de vulnérabilité a été étudié et qui concerne les risques liés aux terminaux clients plus particulièrement les terminaux léger de type téléphone ou PDA.

Les différentes attaques présentées montrent la nécessité de penser la conception des algorithmes de sécurisation en termes d'applications (adaptabilité, transmission, etc.) : une fois ces applications définies, il devient possible d'anticiper les attaques qui seront utilisées et de les contrer.

À partir des ces différentes études, nous avons présenté, pour conclure, un système de diffusion de documents multimédia, permettant la signature et le chiffrement de ces derniers suivant les recommandations W3C, sur une architecture d'adaptation utilisant des proxies.

Les extensions futures et les approches de recherches complémentaires seront importantes. Nous espérons pouvoir compter sur plusieurs apports pour faire évoluer les approches proposées et les différents développements.

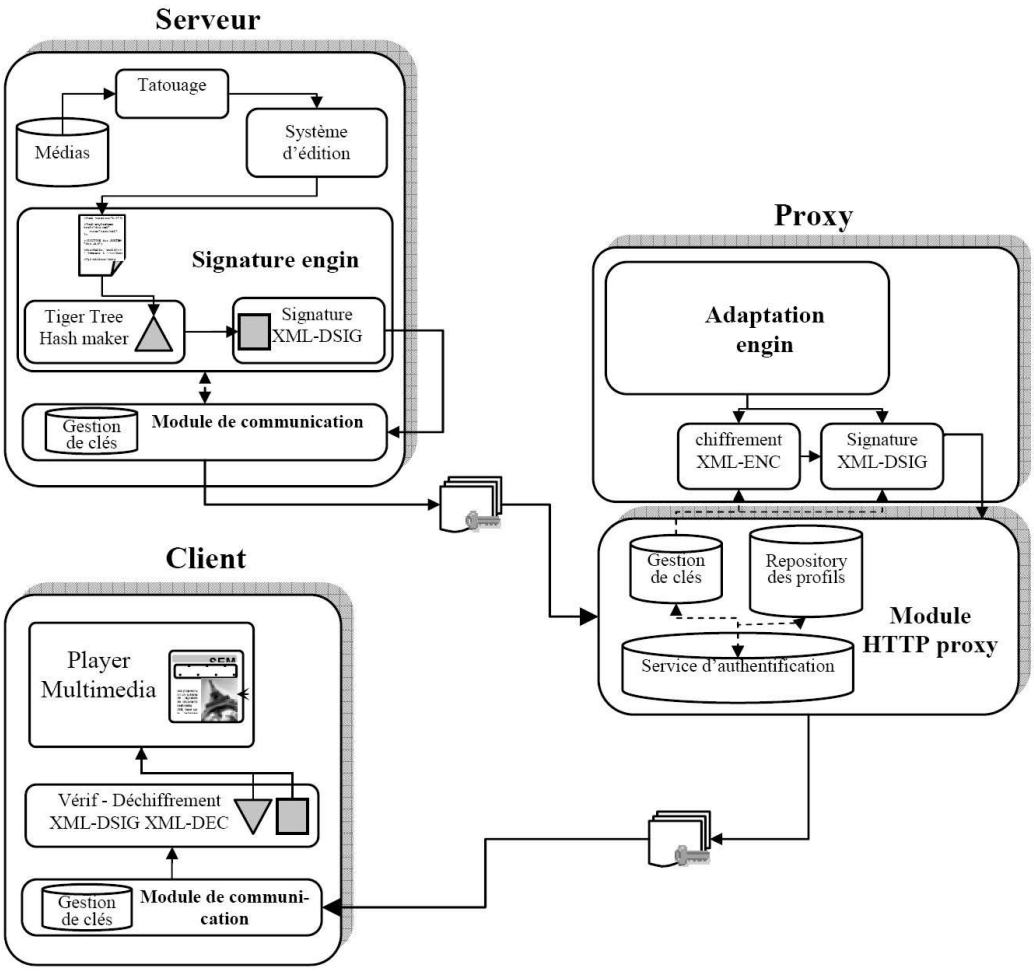

Fig. 6. Schéma fonctionnel de la plate-forme d'adaptation

Références

1. "*Synchronized Multimedia Integration Language (SMIL) 2.1 Specification W3C Recommendation 2005*". Available at : `http://www.w3.org/TR/REC-smil`.
2. Anderson. R, Biham. E, *Tiger : A Fast New Hash Function*, Fast Software Encryption - FSE'96, LNCS 1039, Springer-Verlag (1996), pp. 89–97.
3. Atluri, V., Adam, N., Gomaa, A., and Adiwijaya, I. *Self-manifestation of composite multimedia objects to satisfy security constraints.* ACM Symposium on applied computing. March 2003.
4. Daniel J. Polivy, Roberto Tamassia. *Authenticating distributed data using Web services and XML signatures.* Proceedings of the 2002 ACM workshop on XML security November 2002.
5. Datta, A., Dutta, K., Thomas, H., VanderMeer, D., Suresha, and Ramamritham, K. *Proxy-based acceleration of dynamically generated content on the world wide web : an approach and implementation.* In Proceedings of the 2002 ACM SIGMOD.
6. Davoine, F. and Pateux, S. *Tatouage de documents audiovisuels numériques.* Traité IC2 – Information, Commande, Communication. Hermès-Lavoisier. ISBN 2-7462-0816-4. 2004.
7. Doërr, G. *Security issue and collusion attacks in video watermarking.* Thèse de doctorat. EURECOM, 2004.
8. Fox, A. and Gribble, S.D. *Security on the move : Indirect authentication using kerberos.* In Proceedings of the Second ACM International Conference on Mobile Computing and Networking - Mobicom'96, pages 155-164, New York, USA, 1996.
9. Furht. B, Muharemagic. E, Socek. D, *Multimedia Encryption & Watermarking,* Book, Springer, ISBN : 0387244255, September 2005.
10. Hagimont D., Layaïda N., *Adaptation d'une application multimédia par un code mobile*, Technique et Science Informatiques (TSI), vol. 21, n ° 6, 2002.
11. JPEG 2000 Medical Imaging Ad Hoc Group. *Jpeg 2000 for medical imaging applications*, November 2002.
12. Julie, E. Cohen. *DRM and Privacy.* Communication, ACM 46(4), 46-49. 2003.
13. Kaced, A R., Moissinac, J C. *Sécurisation des flux multimédia adaptables - Proposition d'un schéma de signature sur des proxies*, UbiMob'05, Grenoble, Juin 2005.
14. Kirsch-Pinheiro, M., Gensel, J., Martin, H., "*Awareness on Mobile Groupware Systems*", In : A. Karmouch, L. Korba, E.R.M. Madeira (Eds.), MATA 2004.
15. Layaïda, O., Ben Atallah, S, Hagimont, D., *Adaptive Media Streaming Using Self-Reconfigurable Proxies.* In Proceedings of the 7th IEEE International Conference on HSNMC 04. June 2004 - Toulouse, France.
16. Lemlouma ,T., Layaïda, N., *Adapted Content Delivery for Different Contexts,* SAINT 2003 Conference, Orlando, Florida, USA, January 27-31, 2003. IEEE Computer Society publication. pp. 190-197.
17. *MPEG ISO/IEC. Jtc1/sc29/wg11.mpeg-21 overview (version 4.0).* document n4801. `http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm`, May 2002.
18. Harrison. R, Northam. P, Eds. 2003 *Symbian OS C++ for Mobile Phones.* John Wiley & Sons, Inc.

19. Technologies mobiles *: Des GSM Bluetooth vulérabvles.* `http://awt.wallonie.be/web/mob/`, Février 2004.
20. Ford. W, Hallam-Baker. P, Fox. B, Dillaway. B, LaMacchia.B , Epstein. J and Lapp. J, *XML Key Management Specification (XKMS).* `http://www.w3.org/TR/2001/NOTE-xkms-20010330/W3CNote,March2001`
21. W3C Recommendation. *XML-Encryption.* `http://www.w3.org/TR/xmlenc-core/`
22. W3C Recommendation. *XML-Signature Syntax and Processing.* `http://www.w3.org/TR/xmldsig-core`
23. Yoshida, J. *La sécurité fait caler le multimédia mobile.* EE Times, May 2005. `http://www.eetimes.fr/ed/news/showArticle.jhtml?articleID=162100421`
24. Zhang H., *Adaptive Content Delivery : A New Research Area in Media Computing*, Proc. Of the 2000 Int. Workshop on Multimedia Data Storage, Retrieval, Integration and A Applications, Hong Kong, 2000.