Deep packet inspection

En informatique et en télécommunications, le ***deep packet inspection*** (***DPI***), en français **inspection des paquets en profondeur**, est l'activité pour un équipement d'infrastructure de réseau consistant à analyser le contenu (au-delà de l'en-tête) d'un paquet réseau (paquet IP le plus souvent) de façon à en tirer des statistiques, à filtrer ceux-ci, à les prioriser ou à détecter des intrusions, du spam ou tout autre contenu prédéfini. Le DPI peut servir notamment à la censure sur Internet ou dans le cadre de dispositifs de protection de la propriété intellectuelle.

Il s'oppose au *Stateful Packet Inspection*, qui ne concerne que l'analyse de l'en-tête des paquets. Le DPI peut provoquer un ralentissement sensible du trafic là où il est déployé.

Sommaire

Principes

Le DPI mêle les fonctions des systèmes de détection (IDS) et de prévention (IPS) d'intrusions à celles d'un pare-feu à état : cette combinaison permet de détecter certaines attaques que les IDS/IPS et le pare-feu ne peuvent révéler à eux seuls. Si le pare-feu à état peut voir le début et la fin d'un flux de paquets réseau, il ne peut pas remarquer des événements inadéquats pour une application en particulier. Les IDSs peuvent détecter les intrusions, mais sont peu utiles pour les bloquer ; enfin les DPI sont employés pour prévenir les attaques par virus ou vers, et s'avèrent plus spécifiquement utiles contre des attaques par dépassement de tampon, par déni de service (DoS), ou par l'emploi de vers qui tiennent dans un seul paquet.

Le DPI permet de lire les couches 2 et 3 du Modèle OSI, voire dans certains cas jusqu'à la couche 7, ce qui inclut à la fois les *headers* (en-têtes), les structures des protocoles et la charge, le contenu du message lui-même. Il peut par ailleurs identifier et classer le trafic à partir d'une base de données de signatures, c'est-à-dire à partir des données contenues dans le paquet lui-même (ce qui permet un contrôle plus efficace que s'il était uniquement basé sur les informations des en-têtes) ; un chiffrement des points de sortie est donc généralement nécessaire pour échapper à une inspection de type DPI. Un paquet classifié peut être redirigé, marqué/taggé, bloqué, voir son débit limité, et bien sûr être rapporté à un agent du réseau : dans ce genre de cas, plusieurs types d'erreurs HTTP peuvent être identifiées et transférées pour une analyse ultérieure. Beaucoup de dispositifs DPI peuvent analyser des flux de paquets (plutôt que procéder à une analyse paquet par paquet), ce qui permet un contrôle sur des flux cumulés d'informations.

Utilisations

Par les entreprises

Jusqu'à récemment la sécurité des connexions internet en entreprise était une discipline annexe, où la philosophie dominante consistait à tenir à l'écart les utilisateurs non autorisés, et à protéger les autres du monde extérieur : l'outil le plus utilisé était alors le pare-feu à état. Ce dernier permet un contrôle efficace des accès extérieurs au réseau interne (limités à certaines destinations), tout en autorisant l'accès à des serveurs extérieurs si la requête en a été faite précédemment. Cependant, des vulnérabilités existent au niveau du réseau qui demeurent invisibles aux yeux du pare-feu ; de plus, le recours devenu fréquent aux ordinateurs portables rend difficile la prévention de menaces telles que les virus, les vers et les logiciels espions, dans la mesure où ces appareils se connectent souvent à des réseaux peu protégés (connexion sans fil à domicile ou dans des lieux publics). Par ailleurs les pare-feux ne peuvent faire la distinction entre un usage légitime ou prohibé d'une application ; le DPI permet donc aux administrateurs et aux agents de sécurité d'établir des règles et de les renforcer à tous les niveaux, y compris à celui de l'application et de l'utilisateur, dans l'optique de combattre ces menaces. Enfin le DPI peut être utilisé en entreprise pour éviter les fuites d'informations (*Data Leak Prevention* ou DLP) : lorsqu'un utilisateur tente d'envoyer un fichier protégé par e-mail, il peut alors recevoir une notification sur la manière de procéder à un tel envoi de manière sécurisée.

Par les gouvernements

En plus d'utiliser le DPI pour renforcer la sécurité de leurs réseaux, les gouvernements d'Amérique du Nord, d'Europe et d'Asie l'utilisent pour différents usages comme la surveillance et la censure. Ainsi, l'Iran utilise un tel système depuis 2008, fourni par Nokia Siemens Networks (NSN)[1].

Les premières tentatives de contrôle des communications se sont traduites par la création d'un *Traffic Access Point* (TAP), un serveur tiers (proxy) connecté à un appareil de surveillance gouvernemental ; mais ces techniques ne sont plus d'actualité dans le cadre des nouveaux réseaux. Le DPI fait donc aujourd'hui partie des techniques de substitution qui remplissent des fonctions équivalentes, et peuvent être mises en œuvre par décision d'une cour de justice pour accéder aux flux de données d'un individu en particulier. Aux États-Unis, cet usage est soumis au CALEA (*Communications Assistance for Law Enforcement Act*).

Le dictateur Mouammar Kadhafi a utilisé le système Eagle de la société Amesys pour repérer et espionner ses opposants[2].

Ce système de surveillance massive et d'interception de communications électroniques serait également utilisé en France, selon le site reflet.info[3] ainsi que owni.fr[4]. La Syrie de Bachar el-Assad a fait appel à Area, société italienne en contrat avec la société allemande Utimaco, elle-même sous contrat avec Qosmos[5]. Le programme de recherche qui était en train d'être développé en Syrie a été interrompu par Area en novembre 2011[6]. Par ailleurs, la société Qosmos a déclaré s'être retirée totalement du projet de manière unilatérale dès octobre 2011 et a toujours dit qu'aucun de ses logiciels n'a jamais été opérationnel en Syrie[7].

Par les fournisseurs d'accès à Internet

Le DPI peut être mis en place par les FAI sur les réseaux fixes et les réseaux mobiles pour sécuriser leurs réseaux internes ; mais cette technologie peut aussi s'appliquer aux clients eux-mêmes, pour intercepter des communications illégales, pour mettre en place de la publicité ciblée, pour améliorer la qualité du service, pour offrir des services tiers, ou dans le cadre de la protection de la propriété intellectuelle.

- Parce qu'ils acheminent tout le trafic de leurs clients, les FAI peuvent en effet surveiller leurs habitudes de navigation de manière très détaillée et connaître ainsi leurs centres d'intérêt (puis revendre ces informations à des entreprises spécialisées dans la publicité ciblée comme Phorm, NebuAd).
- L'usage du DPI a aussi été envisagé par le Parlement néerlandais dans un rapport de 2009 en tant que mesure qui aurait été ouverte aux parties tiers pour renforcer la surveillance du respect de la propriété intellectuelle, visant plus particulièrement à réprimer le téléchargement de contenu protégé sous copyright. À la suite de critiques émanant d'ONG, cette proposition devrait être abandonnée[8]. En France, après l'arrivée de l'HADOPI et de la mise en route de l'analyse des échanges peer to peer, le DPI est évalué, mais l'HADOPI ne montre pas (pour l'instant du moins) la volonté de l'utiliser dans le cadre de son activité[9].
- Des fournisseurs d'accès affirment que les échanges de type *peer-to-peer* (P2P) posent un problème de trafic ; typiquement, dans le cadre du partage de fichiers (musique, vidéos, documents), la large taille des fichiers transférés nécessite une capacité accrue des réseaux. Le DPI leur permet de vendre l'idée d'une répartition plus juste de la bande passante, et d'éviter les congestions du réseau... En complément, la priorité peut être accordée à des services comme la VoIP ou les appels en vidéo-conférences, qui nécessitent un temps de latence moindre. Cette approche est privilégiée pour une attribution dynamique de la bande passante.

- Le recours au DPI par les FAI pose le problème du respect d'un certain niveau de service (service level agreement) dû aux clients (le contrôle des données ralentissant les débits entrant/sortant), et celui du respect de la vie privée (le DPI permet de connaître le contenu de tous les paquets transférés, des e-mails envoyés ou reçus aux sites web visités, en passant par les partages de musique, de vidéo ou de logiciels ; il permet aussi d'interdire les connexions à certaines adresses IP ou l'usage de certains protocoles, d'identifier certains usages ou le recours à certaines applications).

Critiques de l'usage du DPI

Les partisans de la neutralité du net et défenseurs des libertés sur Internet trouvent le DPI intrusif du point de vue de la vie privée[10] et, selon l'usage qui en est fait, contraire au principe de non-discrimination du trafic internet et du droit d'accès à Internet[11].

Notes et références

1. "Iran's Web Spying Aided By Western Technology" (http://online.wsj.com/article/SB124562668777335653.html)
2. VIDÉO. J'ai rencontré des blogueurs libyens torturés grâce à du matériel français (http://leplus.nouvelobs.com/contribution/426918-video-j-ai-rencontre-des-blogueurs-libyens-tortures-grace-a-du-materiel-francais.html), Le Plus du Nouvel Observateur, .mercredi 14 mars 2012
3. Un Eagle d'Amesys en France… Mais pour quoi faire ? (http://reflets.info/un-eagle-damesys-en-france-mais-pour-quoi-faire/), blog Reflets.info, mardi 13 mars 2012.
4. Amesys surveille aussi la France (https://owni.fr/2011/10/18/amesys-surveille-france-takieddine-libye-eagle-dga-dgse-bull), owni.fr
5. Internet massivement surveillé (http://owni.fr/2011/12/01/spy-files-interceptions-ecoutes-wikileaks-qosmos-amesys-libye-syrie/), 1er décembre 2011.
6. https://www.bloomberg.com/news/2011-11-23/italian-firm-exits-syrian-monitoring-project-repubblica-says.html
7. http://www.qosmos.com/qosmos-confirme-qu-aucun-de-ses-logiciels-na-jamais-ete-operationnel-en-libye-ou-en-syrie/
8. EDRI, Dutch copyright working group strikes deep packet inspection (http://www.edri.org/edrigram/number8.8/bof-on-deep-packet-inspection) 21 avril 2010
9. PC Inpact, Filtrage par DPI: les réponses de l'Hadopi et celles de PC INpact (http://www.pcinpact.com/actu/news/59866-hadopi-dpi-reponses-pcinpact-filtrage.htm), 16 octobre 2010
10. ReadWriteWeb, Le Deep Packet Inspection pour mieux vous asservir (http://fr.readwriteweb.com/2010/01/12/analyse/deep-packet-inspection-censure-filtrage/), 12 janvier 2010
11. "Une contre-histoire de l'Internet" Un documentaire de Jean-Marc Manach (@manhack) et Julien Goetz (@juliengoetz) réalisé par Sylvain Bergère, coproduit par ARTE et Premières Lignes Télévision. (http://lesinternets.arte.tv/42/)