Vision d'un opérateur sur la sécurité des réseaux

Mikaël SALAÜN, Patrick TRABÉ, Yvon GOURHANT

France Télécom R&D
2 avenue Pierre Marzin
22307 Lannion Cedex

{yvon.gourhant ; mikael.salaun ; patrick.trabe}@francetelecom.com

Résumé : La sécurité des infrastructures réseaux est le plus souvent considérée sous l'angle de la fiabilité et de la stabilité de l'architecture matérielle. A cette vision de l'opérateur s'est ajouté celle des utilisateurs qui cherchent à avoir l'assurance que les données transmises sont protégées des pirates. Les récentes attaques ont cependant montré que les équipements en bout de réseau ne sont pas les seuls victimes potentielles : le réseau dans son ensemble est sensible à des attaques. Cet article se propose de faire une étude de la situation en prenant en considération le point de vue d'un opérateur.

MOTS-CLÉS : sécurité, Internet, infrastructure réseau, réseau d'opérateur, DDoS, BGP

1. Introduction

Les opérateurs ont jusqu'à présent concentré leurs efforts sur la disponibilité et la stabilité de leurs réseaux. Ces deux objectifs sont naturellement liés à la sécurité puisque cette dernière apporte la garantie que le trafic est correctement acheminé. Elle revêt dans ce cadre des attributs de préservation de la qualité de service et de la surveillance des pannes matérielles pouvant survenir (routeur, liaisons,…).
La sécurité sur Internet repose le plus souvent sur les principes exploités en sécurité informatique. Elle se préoccupe de la résolution des problèmes de confidentialité et d'intégrité des données qui transitent. Dans ce contexte, le réseau est considéré comme un médium non sûr dans lequel des personnes malveillantes sont susceptibles de lire, modifier et supprimer les données qu'il achemine.

Les solutions développées et exploitées reflètent une vision locale de la sécurité qui prédomine aujourd'hui. L'utilisateur, le système et les données sont au centre des moyens de défense, et au final, seule la périphérie de réseau est concernée par la sécurité. Ainsi le contrôle d'accès à l'aide d'un pare feu ne se préoccupe que de protéger un réseau d'entreprise à son entrée. Une architecture sécurisée de bout en bout, un VPN à base d'IPSec par exemple, offre les cinq services de sécurité que sont l'intégrité, l'authentification, la confidentialité, le contrôle d'accès et l'anti rejeu. L'infrastructure sur laquelle repose le réseau virtuel peut être attaqué et rendu indisponible à tout moment, rendant de fait caduque l'architecture sécurisée.
Cette vision locale en bout de réseau de la sécurité s'est émoussée au fur et à mesure que sont apparues de nouvelles formes d'attaques tels que les Dénis de Service Distribuées (DDoS, Distributed Denial of Service). Les DDoS sont un important souci pour Internet. La prise de conscience de ce problème s'est faite avec les attaques contre de grands sites commerciaux en février 2000. Plus récemment, les serveurs racines du service mondial de DNS ont été les victimes d'un assaut de très grande ampleur qui aurait pu causer un blocage du Web. L'association de ces attaques avec des vers pour leur propagation a de nouveau montré la rapidité avec laquelle elles se mettent en place et l'extrême difficulté pour les bloquer.
Les moyens de défense traditionnels ne suffisent pas pour préserver l'infrastructure des attaques. Une analyse des ces nouvelles menaces ([MMR01], [PSW02]) montre qu'elles s'articulent autour de trois fondamentaux :

- *Aspect distribué*. Tout équipement connecté à Internet est susceptible de participer directement ou indirectement au réseau d'attaque. La nature d'un réseau d'attaque est donc distribuée et très fortement diffusée à travers Internet. La dualité entre la vue locale des moyens de défense et l'aspect global de ces attaques est la cause des difficultés actuelles pour s'en prémunir,
- *Utilisation et participation active du réseau à l'attaque*. Il n'est plus uniquement le support permettant au pirate d'accéder à distance aux équipements. Ses capacités sont détournées et exploitées afin de renforcer les nuisances de l'attaque,
- *Mise en danger du fonctionnement du réseau*. Les services fournis par les opérateurs sont non seulement des cibles potentielles, mais ils sont aussi détournés pour attaquer un équipement. Les protocoles de routage sont également concernés, avec des risques beaucoup plus élevés pour la stabilité du réseau.

Ces nouvelles attaques démontrent la présence de dangers quotidiens pour d'une part tous les équipements rattachés à Internet, et d'autre part pour les infrastructures des opérateurs dont les ressources peuvent être détournées, gaspillées, et bloquées.

Toute la chaîne des communications demande à être protégée, ce qui a pour conséquence de mettre en concurrence deux visions de la sécurité. La première est issue des besoins de l'utilisateur qui cherche à protéger les informations qu'il transmet. La seconde est propre à l'opérateur qui recherche la préservation de son infrastructure (bande passante, routeurs, services,…). Bien que les intérêts des deux protagonistes convergent vers une recherche de plus de sécurité, la résolution simultanée de leurs problématiques propres peut être à la base de conflits d'intérêts. Les attaques par DDoS illustrent très bien cela à l'image des dommages collatéraux qui peuvent être créés lorsque l'identification des flux responsable de l'attaque est erronée. L'opérateur est satisfait car l'élimination de ces flux préserve ses ressources. Les clients légitimes sont floués car leur trafic a été supprimé arbitrairement. La difficulté pour l'opérateur réside donc dans l'équilibre qu'il existe entre d'une part ses choix tactiques, et d'autre part, les politiques de sécurité qui gouvernent son architecture et ses relations avec ses clients et partenaires.

Cet article expose un constat des problèmes liés à la sécurité pour un opérateur et essaie de présenter des éléments de réponses. Il s'articule en quatre parties. La première situe le contexte réseau dans lequel évolue un opérateur. La seconde présente les problématiques posées à l'opérateur par le réseau Internet et ses interconnexions multiples. La troisième partie présente des travaux existants sur cette problématique. La quatrième partie conclut cet article.

2. Positionnement du réseau d'un opérateur

L'étude de la topologie d'Internet fait apparaître des nombreuses difficultés pour obtenir une vision claire et précise de l'organisation et des relations qui lient les réseaux interconnectés. Or la connaissance de ces caractéristiques est nécessaire afin de pouvoir répondre à la question "*qui* fait *quoi*, *en direction de qui*, et *comment*", et ainsi avoir la capacité d'appréhender correctement les attaques.

Internet est un réseau découpé en une multitude d'entités administratives : les Domaines Administratifs (AD), les Systèmes Autonomes (AS), les Fournisseurs d'Accès à Internet (FAI), et en périphérie les Utilisateurs. Chacun de ces quatre protagonistes va se définir par rapport aux relations qu'il entretient avec ses voisins. Ils sont circonscrits par rapport à leur frontière avec Internet[1] :

- Le *Domaine Administratif* (AD) définit une zone sous la responsabilité d'une seule et même autorité. Il constitue le niveau d'abstraction le plus élevé pour l'identification des différents types de domaines. Il permet de se soustraire aux détails internes qui le composent [WPSTT01]. Typiquement, un opérateur constitue un AD,
- Le *Système Autonome* marque l'usage de protocoles intra domaines en son sein, et de protocoles inter-domaines avec ses partenaires. Un AD est constitué de un ou plusieurs AS,
- Le *FAI* constitue généralement une AS. De cette manière, il est beaucoup plus aisé de gérer les interconnexions. Il se caractérise par les contrats et les accords d'échanges avec ses voisins :
    a. *Les accords de peering* sont une relation de libre échange de trafic, gratuite, et dans les deux sens.
    b. *Les accords de transit* créent une relation de dépendance entre le client et le fournisseur (les clients payent les fournisseurs pour pouvoir envoyer et recevoir du trafic),

[1] Internet Edge [Sta03]

- L'*Utilisateur* est en bout de chaîne et dépend directement du FAI. Plusieurs utilisateurs peuvent se "cacher" derrière ce qui semble être un unique utilisateur ; un NAT peut être la cause d'une telle confusion. L'Utilisateur ne maîtrise pas sa politique de routage qui est laissée à la charge de son administrateur.

La vision que possède l'opérateur sur son environnement est concentrique, avec en son milieu l'épine dorsale sur laquelle il s'appuie. Le AD de l'opérateur (représenté ici par une zone grisée Figure 1) peut ne comporter que le backbone, mais il est généralement accompagné de FAI et d'infrastructures dédiées à des services spécialisés[2] (pour les entreprises par exemple).

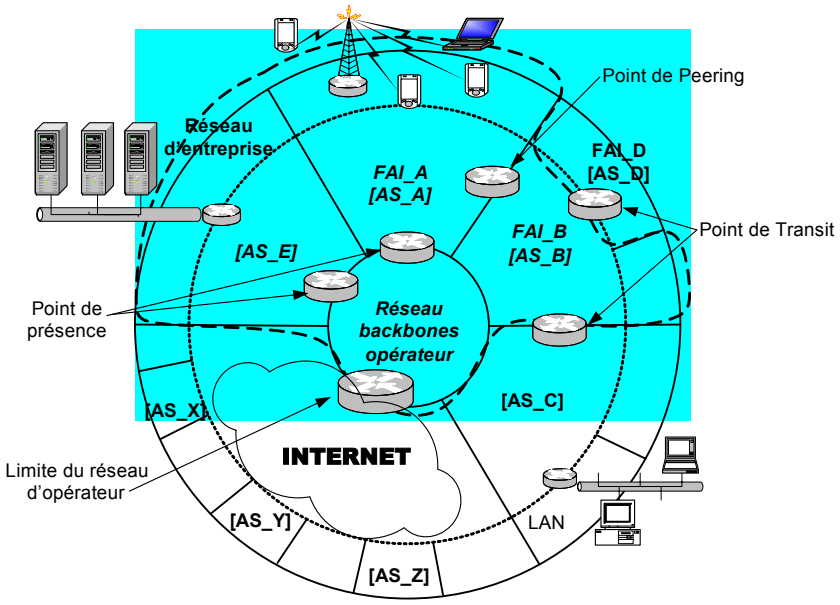

Figure 1 : Vision d'un opérateur sur son réseau et ses relations avec l'extérieur

3. Les problèmes rencontrés

Les effets des différentes attaques (succinctement résumées dans le Tableau 1) se traduisent par la dégradation des performances et la perte d'accessibilité. Elles concernent les plans de transferts et de commande, ainsi que les services mis à disposition sur le réseau. La nature des interconnexions sur Internet rend difficile un règlement de ces attaques [AJB00].

Les plans de transfert et de commande, les services

Les DDoS constituent le principal type d'attaque que rencontre le plan de transfert. Il est alors soumis à des problèmes de congestion. Les attaques du plan de commandes agissent sur le comportement du plan de transfert. Les protocoles de routages (BGP, OSPF,..) sont donc tout naturellement des cibles potentielles. Le pirate cherche à modifier les données exploitées pour l'aiguillage des paquets. Il peut pour cela s'attaquer directement au routeur, ou alors aux messages qu'ils s'échangent. La conséquence de ces attaques est une perte d'efficacité dans l'acheminement des paquets pouvant conduire à un DoS. La dangerosité de ses attaques est très forte car elles remettent en cause la stabilité du réseau, et elles peuvent potentiellement couper de larges portions du réseau.

[2] Nous ne considérons par la suite que ce cas de figure.

Les services particuliers disposés sur les réseaux constituent une troisième catégorie de cible (DNS par exemple). Ces attaques se singularisent par le fait qu'elles altèrent la disponibilité du service proposé, mais également qu'elles peuvent détourner l'usage du service pour perpétrer une attaque en direction d'une autre victime[3].

La lutte contre toutes ces attaques est difficile, tant au niveau de leur détection que de leur arrêt. Le chiffrement est une méthode souvent préconisée pour protéger les messages et les échanges d'informations. Des techniques ont été proposées à l'image de Secure-BGP [Lyn03] et de DNSSec [Eas99]. Cependant, elles accroissent la charge du réseau et augmentent la charge de travail du serveur avec la vérification des signatures. Le risque d'attaques de type DoS augmente. *L'ajout de sécurité au niveau de l'infrastructure a un coût qui peut impacter sur la sécurité locale*.

	Type d'attaque	**Cibles**	**Problèmes associés**
Plan de transfert	Congestion (DDoS)	• Lien • Routeur • Serveurs	Difficile à arrêter
Plan de commande	• Intégrité des données (Equipement, Protocole) • DoS et DDoS	Routeurs et protocoles associés	• Difficile à détecter • Chiffrement peut être dangereux
Services	• Détournement (RDDoS[3]) • DDoS	• DNS • Plateformes de services (H323, SIP,…)	• Le chiffrement peut être dangereux • Problèmes d'implémentation

Tableau 1 : classement des menaces suivant le plan auquel elles appartiennent

Dualité entre l'intra et l'inter-domaine

Il est très difficile de posséder une vue globale des interconnexions et des liens entre les domaines. L'analyse de la topologie inter-AS présentée par Govindan *et al.* [GR97] montre l'existence d'une hiérarchie qui s'est naturellement mise en place. Elle se compose de quatre niveaux qui sont définis par rapport à leur degré de connectivité. Le Tier 1 par exemple précise un domaine qui possède une très important connectivité[4]. La dénomination Tier 4 correspond à un domaine ayant une faible connectivité (<2). Mais les récentes mesures de Gao révèlent que les connexions latérales (entre AS de même niveau) augmentent plus que les interconnexions verticales [Gao00]. La hiérarchie s'estompe au fur et à mesure que croit le nombre d'interconnexion, ce qui est un handicap pour obtenir une vision structurée et hiérarchisée du réseau.
La connectivité des AS est cependant généralement limitée à 2 partenaires. La conséquence de ce constat est qu'*une attaque correctement dirigée contre quelques AS est susceptible de causer le blocage d'une partie d'Internet* [DN03].

Les routeurs BGP constituent la clef de voûte des échanges inter-AS. Une attention particulière s'est de fait portée sur ce protocole [Zdn03]. Bien qu'il soit difficile de réaliser des attaques contre les routeurs BGP, des risques existent et doivent être pris en considération

[3] RDDoS, Reflected Distributed Deny of Service [Pax01]
[4] Moins de 10 Tier de niveau 1 existent actuellement. Ils possèdent généralement plus de 200 liens vers l'extérieur.

[CCF03]. En plus des attaques classiques sur les implémentations de BGP, on compte quatre classes d'attaques :

- DoS sur un routeur,
- Réinitialisations de sessions qui conduisent à un DoS si celles-ci sont continuellement répétées,
- Le détournement de sessions,
- L'injection de routes qui peut conduire à la désagrégation des chemins, au détournement de trafic, ou encore à l'annonce de AS non existantes.

Les attaques sur les échanges entre routeurs sont difficiles à mettre en œuvre car elles demandent une parfaite connaissance de la communication. Les attaques directes sur l'équipement sont plus facilement réalisables (Figure 2).

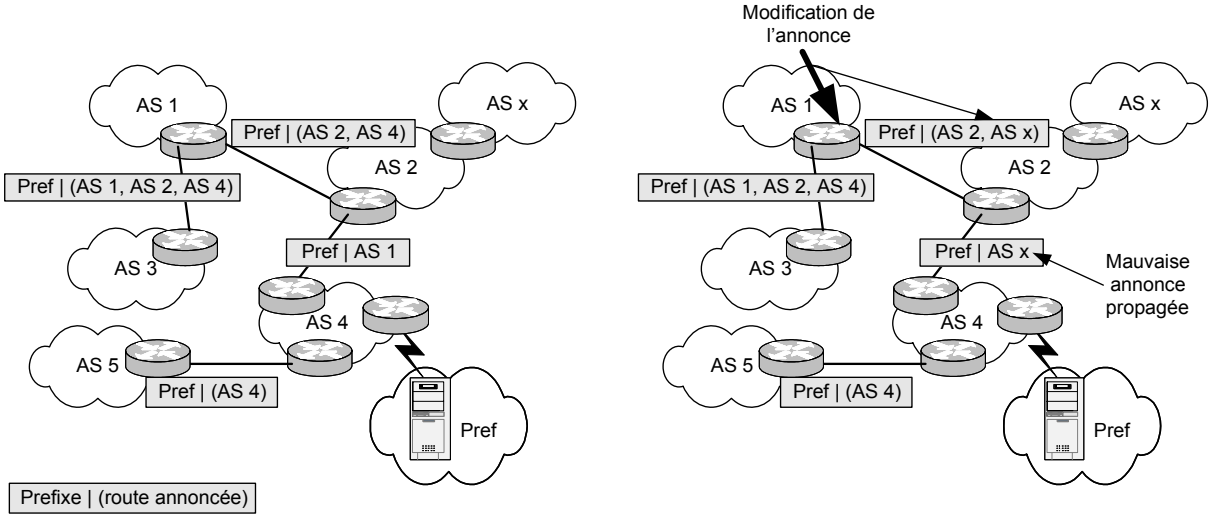

Figure 2 : illustration d'une attaque possible sur les annonces BGP

Les routeurs BGP possèdent une vision très juste de la topologie du réseau pour lequel ils travaillent, et ils ont une vue correcte du voisinage inter-domaine. Mais au-delà des points d'interconnexions, leur visibilité est extrêmement réduite.
Les accords existant entre les opérateurs et les FAI modifient l'accessibilité. Celle-ci peut être unidirectionnelle ou bidirectionnelle. Le trafic n'est pas donc obligatoirement symétrique. De manière généralement, *la connectivité entre deux réseaux n'assure pas l'accessibilité*. Tout ceci est laissé à la discrétion des opérateurs et aux politiques d'échanges qui les lient entre eux. Le routage BGP offre de très nombreuses possibilités dans l'application des politiques d'échanges de trafics. Ainsi la politique de routage du plus court chemin est souvent court-circuitée par la politique de routage de la "patate chaude" : le trafic du domaine partenaire est évacué vers le chemin de sorti le plus proche, avec pour conséquence un nombre de sauts et de routeurs traversés plus important. *Les parcours des échanges perdent leur symétrie d'origine*, compliquant un peu plus la perception des interconnexions directes et distantes.

Les Internet Edges déterminent les responsabilités et les obligations des entités sur le réseau, de telle sorte qu'ils définissent les différentes actions que l'opérateur peut mettre en place pour sécuriser son réseau. Au sein même d'une AD, les Internet Edges présents apportent des contraintes à l'opérateur telles qu'il ne maîtrise pas administrativement toute la chaîne de communication.

Internet a été conçu de façon à ce qu'il soit facile de s'y connecter. Une architecture aussi ouverte et flexible est donc tout naturellement en opposition avec une gestion et une administration cloisonnées. Les problématiques de l'inter-domaine naissent à ce niveau.

Le dialogue inter-domaines requiert une attention particulière. Il apporte l'extensibilité et une résolution correcte des attaques, mais ceci se fait au prix d'un compromis entre les droits et les devoirs respectifs de chaque opérateur.
Chang propose une solution de défense globale [Cha02] basée sur des échanges d'informations issues d'un système de détection global [WC02]. Mais la communication de données issues des analyses du trafic est très sensible. Elle doit être surveillée et filtrée à l'aide d'une politique de surveillance des échanges fixée par chaque autorité administrative. L'assurance que des données sensibles ne sortent pas du domaine est un impératif pour chaque domaine.
Barrère *et al*. [BBGLN03] ont proposé un modèle de collaboration qui permet un échange de politiques de sécurité. Mais la création de la collaboration s'appuie sur une volonté et un besoin de dialogue entre les partenaires. Dans un contexte de défense globale, la problématique diffère car un domaine qui ne participe pas à l'effort peut être impliqué dans l'attaque.
Le problème devient rapidement inextricable lorsque le nombre de partenaires ne participant pas à la coalition devient important. Paxson *et al.* ont amené l'idée [PSW02] que seule une "organisation centrale" peut être à la base du consensus indispensable entre tous les protagonistes pour régler définitivement le problème des attaques se produisant à l'échelle d'Internet.

4. Travaux en relation

C'est avec l'apparition des DoS (suivi ensuite des attaques par DDoS) que les recherches sur la protection des infrastructures de réseaux IP ont émergé. C'est pour cette raison qu'un grand nombre d'études se concentre sur cette problématique particulière. Dans ce contexte, le but n'est alors pas toujours de protéger l'infrastructure, mais plutôt de s'appuyer sur elle pour mettre un terme à l'attaque. En particulier les mécanismes de remontée à la source tire parti des ressources du réseau et de ses capacités d'analyse du trafic afin de retrouver les équipements responsables d'une attaque ([BC00], [BLT03], [SPSJTKS01]). Le contrôle du trafic contribue de manière beaucoup plus significative à l'assainissement des réseaux en bloquant le passage des trafics illégitimes ([PL01], [MBFIPS01]). Une troisième voie consiste à contourner les effets d'une attaque en la redirigeant vers des endroits déterminés sur le réseau ([YEA00], [Wei02]). Cette pratique est déjà couramment utilisée par les opérateurs lorsque le trafic illégitime est envoyé vers un trou noir (black hole).

Jayaram *et al*. ont proposé une taxonomie des menaces pesant sur les réseaux [JM97]. Cinq catégories ont été déterminées : la menace physique, le point de faiblesse, les programmes malignes, les droits d'accès, et les menaces basées sur la communication. Ils ont associé à chacune de ces menaces des mécanismes de sécurité (chiffrement, authentification, pare feu,..). Mais cette taxonomie n'entre pas au final dans le cadre d'une protection de l'infrastructure car le classement proposé considère les dangers sous angle de l'utilisateur, et non de l'opérateur.
Plus récemment, Chakrabarti et Manimaran ont présenté une taxonomie complète des problèmes de sécurité sur Internet. L'apport de leur travail est d'avoir proposé un classement des menaces en adoptant une vue d'opérateur, c'est-à-dire en considérant toute l'infrastructure de communication [CM02]. Quatre catégories d'attaques ont été proposées. La première

concerne le service de DNS qui est l'une des clés de voûte de l'Internet actuel. La seconde se rapporte aux tables de routages et aux attaques qui visent à les empoisonner. La troisième catégorie est constituée par un ensemble de menaces visant à apporter une mauvaise gestion des paquets. La quatrième et dernière catégorie est constituée par les attaques par DoS et DDoS, qui peuvent également résulter des deux types d'attaques précédentes.

5. Conclusion

Les mécanismes de défense actuels ne sont pas suffisamment adaptés à l'envergure et à l'aspect distribué des nouvelles attaques. Une résolution efficace et durable de ces attaques passe par un contrôle de l'infrastructure réseau de l'opérateur. Ce contrôle doit permettre d'anticiper dans la mesure du possible les attaques, et d'être suffisamment flexible pour pouvoir s'adapter à différents contextes d'attaques. Dans ce but, nous pensons qu'il est nécessaire de s'appuyer sur des techniques de détection et de filtrage distribué à différentes profondeurs du réseau. Des traitements du trafic à l'intérieur du réseau sont envisagés, toujours dans un but d'anticipation des attaques.
Dans une démarche similaire nous portons deux projets labellisés en 2003 : RNRT (ADSR) et IST (DIADEM). L'utilisation des réseaux actifs dans le cadre de ces projets permettra le déploiement et la mise en œuvre des moyens de lutte contre les DDoS, mais donnera aussi naissance à de nouvelles règles d'ingénierie réseau pour répondre aux besoins d'interopérabilité et de convergence des différents domaines traités par l'opérateur.
Nous espérons que cet article aura permis d'avoir une meilleure perception des problématiques liées à la sécurisation des infrastructures réseaux d'un opérateur.

[AJB00] R. Albert, H. Jeong, and A. Barabasi, "*Error and attack tolerance of complex networks*", Nature, volume 406, July 2000

[BBGLN03] F. Barrère, A. Benzekri, F. Grasset, R. Laborde and B. Nasser, "*Négociations de la politique de sécurité Inter-Domaine*", In Proceedings of SAR 2003, Nancy , 30 June - 4 July, France, 2003

[BC00] H. Burch, and B. Cheswick, *"Tracing Anonymous Packets to Their Approximate Source"*, In Proceedings of USENIX System Administration Conference, December 2000

[BLT03] S. Bellovin, M. Leech, and T. Taylor, *"ICMP TraceBack Message"*, Internet Draft : draft-ietf-itrace-04.txt, submitted February 2003, Expiration date : August 2003

[CCF03] S. Convery, D. Cook, M. Franz, "*An Attack Tree for the Border Gateway Protocol*", draft-convery-bgpattack-01, September 17, 2003

[Cha02] R.K.C Chang, **"***Defending against flooding-based distributed denial-of-service attacks: a tutorial***",** Communications Magazine, IEEE , Volume: 40 Issue: 10 , Page(s): 42 – 51, October 2002

[CM02] A. Chakrabarti and G. Manimaran, *"Internet Infrastructure Security: A Taxonomy,"* IEEE Network, vol.16, no.6, pp.13-21, Nov/Dec. 2002

[DN03] M. Decima, Q. Nguyen, "*Topologie de l'Internet : Exploration et représentation du réseau*", Note Technique FranceTelecom R&D, septembre 2003

[Eas99] D. Eastlake, "*Domain Name System Security Extensions*", RFC2535, March 1999

[Gao00] L. Gao, "On Inferring Autonomous System Relationship in the Internet", *In Proceedings of IEEE Global Internet*, San Francisco, CA, November 2000

[GR97] R. Govindan, and A. Reddy, "An Analysis of Internet Inter-Domain Topology and Route Stability", *In Proceeding of IEEE INFOCOM*, Kobe, Japan, April 1997

[JM97] N.D. Jayaram and P.L.R. Morse. Network Security, *"A Taxonomic View"*, In proceedings of European Conference on Security and Detection, School of Computer Science, University of Westmister, UK, IEE, 28–30 April 1997

[Lyn03] C. Lynn et al., "*Secure BGP (S-BGP*I)", draft-clynn-s-bgp-protocol-01.txt, July 2003

[MBFIPS01] R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, S. Shenker, *"Controlling High Bandwidth Aggregates in the Network"*, AT&T Center for Internet Research at ICSI (ACIRI) and AT&T Labs Research, Technique Report (Draft), Feb. 2001

[MMR01] J. Mirkovic, J. Martin, and P. Reiher, "*A Taxonomy of DDoS Attacks and DDoS Defense Mechanism*", UCLA CSD Technical Report CSD-TR-020018, 2001

[Pax01] V. Paxson, "*An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks*", In Proceedings of ACM SIGCOMM Computer Communications Review (CCR) Vol. 31, No 3, July 2001

[PL01] K. Park, and H. Lee, *"On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internet"*, In Proceedings of ACM SIGCOMM'2001, San Diego, CA, August 2001

[PSW02] V. Paxson, S. Staniford, and N. Weaver, "*How to Own the Internet in Your Spare Time*", In Proceedings of the 11th USENIX Security Symposium, August 5-9, San Francisco, 2002

[QPKHR02] Guangzhi Qu, Jayaprakash,Ramkishore Modukuri, S. Hariri, C.S Raghavendra, *"A Framework for Network Vulnerability Analysis"*, In Proceedings of Communications, Internet and Information Technology (CIIT 2002), St. Thomas, Virgin Islands, USA, November 18-20, 2002

[SPSJTKS01] C. Snoeren, C. Partbridge, L.A. Sanchez, C.E. Jones, F. Tchakountio, S.T. Kent and W.T. Strayer, "Hash-Based Traceback", In Proceedings of the ACM SIGCOMM conference, 2001

[Sta03] National security telecommunications advisory committee, *"Defining the Edge of the Internet"*, Internet security/architecture task force report, June 25, 2003

[WC02] K.K.K Wan, and R.K.C.Chang, "*Engineering of a global defence infrastructure for DDoS attacks*", In Proceedings of ICON 2002, 27-30 August, 2002

[Wei02] N. Weiler, *"Honeypot for Distributed Denial of Service Attacks"*, In Proceeding of IEEE WET Workshop on Enterprise Security 2002, June 2002

[WPSTT01] H. Wang, A. Prasad, P. Schoo, T. Tessier, O. Tirla, "*A Domain model approach to network security*", 2001

[YEA00] J. Yan, S. Early, and R. Anderson *"The XenoService A Distributed Defeat for Distributed Denial of Service"*, In Proceedings of the Information Survivability Workshop 2000, Massachusetts, October 24-26, 2000

[Zdn03] http://zdnet.com.com/2100-1105-990608.html