TD10 – Usages, sécurité et société

{Emmanuel.Godard, Yann.Esposito}@lif.univ-mrs.fr

17 décembre 2005

☞ Dans ce TD nous essayerons de réfléchir sur les usages qui sont fait des réseaux informatiques, dans quelle mesure réelle la sécurité est appliquée. Nous essayerons de réfléchir aux implications sociales de l'apparition de ces réseaux.

1 Usages et sécurité

1.1. Qu'est-ce qu'un VPN ?

Un VPN (Virtual Private Network) ou Réseau Privé Virtuel. Il s'agit d'utiliser internet pour relier plusieurs réseaux comme si les ordinateurs étaient sur un même réseau local. La communication devant se faire de la manière la plus sécurisée possible.

(a) Quelle différence y-a-t'il entre l'utilisation de SSH et l'utilisation d'un VPN standard ?

Protocoles de tunneling pour VPN :
- PPTP (Point to Point Tunneling Protocol) protocole de niveau 2 (liaison de données) développé par Microsoft, 3com, Ascend, US Robotic et ECI telematic.
- L2F (Layer Two Forwarding), protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est obsolète.
- L2TP (Layer Two Tunneling Protocol) est un protocole de niveau 2 développé par l'IETF (Internet Engineering Task Force http://www.ietf.org) s'appuyant sur PPP.
- IPSec est un protocole de niveau 3, issu des travaux de l'IETF permettant de transporter des données chiffrées pour les réseaux IP.

SSH est un protocole de niveau 4. Il ne permet donc pas de proposer des services de niveau inférieur.
De plus, dans un VPN, l'administrateur peut sniffer les paquets et avoir accèss aux emails par exemple. Ce qui n'est pas le cas avec SSH.

1.2. Quelles sont toutes les qualités d'une connexion entièrement sécurisée ?

1. même si la connexion est écoutée une tierce personne ne doit pas pouvoir comprendre ce qui a été dit (**chiffrement**) ;
2. les protagonistes doivent pouvoir être certain de parler à la bonne personne (**signature**) ;
3. on doit être certain que l'envoi d'une information a bien été reçue par la bonne personne ;
4. personne ne peut savoir que la communication à lieu à l'exception des protagonistes (**stéganographie**) ;
5. tout écoute doit être décelée (possible très bientôt avec les communications quantiques) ;

(a) Que peut-on rajouter si on parle de **communication** sécurisée au lieu de connexion sécurisée ?

Par communication, on peut aussi entendre diffusion d'information. Dans ce cas, il y a de multiples raison de vouloir rester anonyme. L'anonymat implique alors des notions contradictoires avec les qualités d'une connexion sécurisée.
– l'identité de l'émeteur d'une information doit être certifiée ;
– personne ne doit savoir qui envoi des informations ;
– personne ne doit savoir qui récupère des informations ;
– personne ne doit pouvoir détruire ou modifier une information ;

1.3. Voici une liste de qualités pouvant être attribués à des protocoles :
- facilité de mise en œuvre ;
- facilité d'accès (grand public) ;
- efficacité ;
- connexion/diffusion ;
- qualités de sécurité ;

Comment notez vous les protocoles suivants :
- ethernet, WIFI ;
- IPv4, IPSec, IPv6 ;
- DNS, POP, SMTP, IMAP ;
- POPS, Mail avec cryptosystème ;
- TELNET, RSH, SSH, TLS ;
- FTP, FTPS, HTTP, HTTPS ;
- P2P centralisé (eMule, eDonkey, Kazaa, BitTorrent...) ;
- P2P décentralisé (Gnutella) ;
- P2P protégé (ANT, MUTE) ;
- P2P parnoïaques (Freenet, GNUNet...) ;
- Routage en oignon, Mixes (TOR, Projet, JAP) ;

Protocole	Facilité	accessibilité	efficacité	C/D	Séc. conn.	Séc. diff.
ethernet	+	+	+	C	-	x
IPv4	+	+	+	C+D	-	-
IPSec	+	+	+	C+D	+	0
IPv6	-	0	+	C+D	+	0
DNS	+	+	+	D	x	-
POP/SMTP/IMAP	+	+	+	C+D	-	-
POPS	+	0	+	C+D	+	0
Mail avec cryptosysètme	-	-	+	C+D	+	0
TELNET/RSH	+	0	+	C	-	x
SSH/TLS	+	+	+	C	+	x
FTP/HTTP	+	+	+	D	x	-
FTPS/HTTPS	+	+	+	D	x	0
P2P centralisé	+	+	+	D	x	-
P2P decentralisé	0	+	+	D	x	-
P2P protégé	0	+	0	D	x	0
P2P paranoïaque	-	-	-	C+D	+	+
TOR, Mixes	-	0	0	C+D	0	0

2 Usages et société

2.1. Quel est l'état actuel de conservation des logs ?

voir http://www.assemblee-nationale.fr/12/rapports/r2681.asp#P481_132534
Projet de loi relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et au contrôles frontaliers. Votée le 29 novembre : Extension des personnes qui ont une obligation de maintenir des logs ; comme avant les FAI, mais aussi maintenant, les cybercafés, les compagnies tels les hôtels, les compagnies aériennes... Mais aussi les fournisseurs d'accès à des réseaux de communications électroniques accessibles via une borne WIFI.
Les logs :
– informations permettant d'identifier l'utilisateur ;
– données relatives aux équipements terminaux de communications utilisés ;
– caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
– les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
– les données permettant d'identifier le ou les destinataires de la communication.
Aucune obligation quant au contenu des communications.
Changement majeur du projet de loi : *les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée, placée auprès du ministre de l'intérieur.* (... désignée par la cncis et nommée par le ministre de l'intérieur ...) Cette personnalité aura en charge de vérifier la réalité des motivations de chaque demande de recherche des logs.
Ce n'est donc pas un juge qui prend la décision d'observation des logs pour des raisons de luttes contre le terrorisme.
Le projet de loi européen (directive 2002/58/EC) que vous pouvez trouvez à l'adresse suivante :
http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0438en01.pdf
Ce projet de loi impose à tous les fournisseur d'accès public de maintenir des logs.
Member States shall ensure that the following categories of data are retained under this Directive :
(a) data necessary to trace and identify the source of a communication ;
(b) data necessary to trace and identify the destination of a communication ;
(c) data necessary to identify the date, time and duration of a communication ;
(d) data necessary to identify the type of communication ;
(e) data necessary to identify the communication device or what purports to be the communication device ;
(f) data necessary to identify the location of mobile communication equipment.
The types of data to be retained under the abovementioned categories of data are specified in the Annex.
Toutes ces données devant être conservées 1 an (article 7).

2.2. Usages de l'internet selon différents points de vues : grand public, informaticiens (professionels ou amateurs), administrateur, organisation publique.
Les administrateurs et les organisations publiques ont souvent intérêt à pouvoir conserver les logs pour diverses raisons.

(a) Est-il facile ou difficile pour le grand public de passer au travers des systèmes de logs ? En particulier, est-il facile pour le grand public de faire en sorte de cacher ses activités internet à un FAI ? à une organisation publique comme les renseignements généraux ?

L'information sur comment passer au travers du système de log est assez difficile à obtenir et encore plus à comprendre pour le grand public qui n'est surtout pas sensibilisé à la question des informations restant sur leur activités numériques.

(b) Est-il facile ou difficile pour un informaticien, professionel ou amateur de cacher ses activités à un FAI ? à une organisation publique ?

De nombreux systèmes sont possible pour passer au travers du système de log. Nottament, encore aujourd'hui en France, il suffit de faire passer toutes ces communications par un proxy situé dans un pays où les logs ne sont pas obligatoires pour passer au travers.
Plus grave, les hacker utilisent en général des zombis ; c'est-à-dire des ordinateurs privés comme proxy à l'insu de leur propriétaire. Par exemple en infectant ces ordinateurs avec un virus.
Ainsi, c'est le propriétaire de l'ordinateur qui aura des ennuis judiciaire et non pas le hacker. Même en retrouvant les connexions entrantes, il s'agira certainement d'une autre victime mais pas du hacker.