Analyse de trafic réseau – Test Passif

Référence: MI20171103-002

Enseignant : Wissam Mallouli
Contact : wissam.mallouli@montimage.com
Mobile : +33 6 95 93 33 39 (urgence)

Description

Le Deep Packet Inspection (DPI), en français Inspection des Paquets en Profondeur, est l'activité d'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 ou à détecter des intrusions, du spam ou tout autre contenu prédéfini.

Dans le contexte du mini-projet, les étudiants seront amenés à étudier **un** protocole réseau de leur choix (les protocoles Ethernet, IP, TCP et UDP ne peuvent pas être sélectionnés). Ils devront programmer un logiciel pour extraire les différents champs protocolaires et les afficher en sortie.

En option, ils devront également analyser une ou plusieurs règles fonctionnelles applicables pour le protocole sélectionné (exemple : contraintes sur un ou plusieurs champs d'un seul paquet, contraintes sur des champs de différents paquets, contraintes sur les échanges Etc.).

Le langage de programmation sera choisi par les étudiants. Les langages C et C++ sont recommandés.

- Entrée du logiciel : un fichier pcap[1] contenant des paquets contenant le protocole choisi[2].
- Sorties du logiciel : les valeurs des différents champs du protocole + (optionnel) les verdicts d'analyse des propriétés fonctionnelles identifiées.

Connaissances pré-requises

Les étudiants doivent maitriser la programmation en C et avoir des connaissances avancées dans les réseaux de télécommunication (protocoles, analyse de paquets, test passif etc.).

Travail en groupe ?

Ce mini-projet pourra être fait individuellement, en binôme ou en trinôme. Il ne devra pas durer plus qu'une journée de travail. Google est votre ami.

[1] https://fr.wikipedia.org/wiki/Pcap

[2] https://wiki.wireshark.org/SampleCaptures

A rendre

Les étudiants doivent rendre par mail **avant le 31 décembre 2017 23h59**

- Le code du logiciel
- Un manuel d'installation et d'utilisation du logiciel (1 à 3 pages)
- Si vous avez choisi d'ajouter la partie optionnelle au logiciel (relative à l'analyse d'une ou plusieurs propriétés fonctionnelles), veuillez expliquer la/les propriété(s) que vous avez identifiée(s). Dans ce cas, le logiciel devra fournir en sortie –en plus des différents champs protocolaires– un verdict relatif au respect de chaque propriété.

Email :

- Titre : [M2-Info] mini-projet noté – « Nom du protocole »
- Destinataire : wissam.mallouli@montimage.com ou wissam.mallouli@gmail.com
- N'oubliez pas de mettre les membres du groupe dans le document « Manuel d'installation et d'utilisation »
- Un accusé de réception vous sera envoyé avant 1er Janvier 2018. Si vous ne recevez pas d'accusé, veuillez me contacter pour vérifier que j'ai bien reçu votre mini-projet.

Voici une liste de protocoles recommandés : SMTP, DHCP, IMAP, POP, HTTP, HTTP2, FTP, UDP-Lite, Telnet, SSH, SSDP, SNMP, SMB, RTSP (Realtime streaming protocol), NTP (network time protocol), NETBIOS, LDAP (Lightweight Directory Access Protocol), IGMP, ESP (Encapsulating Security Payload), AH (Authentication Header), MySQL, DECT (Digital Enhanced Cordless Telecommunications), LLDP (Link Layer Discovery Protocol), PPP (Point-To-Point), TFTP (Trivial File Transfer Protocol), UFTP (UDP based FTP - port 1044), BGP (Border Gateway Protocol), MGCP (Media Gateway Control Protocol), NDMP (Network Data Management Protocol), NNTP (Network News Transfer Protocol), OpenFlow, DNP3(Distributed Network Protocol)