Projet S5 SE « Déploiement d'une sonde réseau embarquée sur un routeur IP»

Contexte:
Actuellement plusieurs routeurs et bornes sans-fil 802.11 peuvent embarquer des OS de type Linux. Les projets Open-WRT et DD-WRT sont deux exemples parmi d'autres, qui permettent de remplacer l'OS original d'un routeur par un OS Linux minimaliste. Avec cette ouverture des systèmes d'exploitation des routeurs, différentes fonctionnalités avancées non disponibles dans les firmwares d'origines peuvent être implémentées.
Le but de ce projet est d'identifier, de comparer, et d'installer une ou plusieurs sondes réseaux sur un routeur sans fil linux afin d'inspecter le trafic qui passe par le routeur. La technique Deep Packet Inspection (DPI) est largement utilisée dans les réseaux d'entreprises et récemment sur Internet en France (depuis la loi Hadopi) pour avoir une visibilité sur le type de trafic passant par les infrastructures réseaux. Cette technique est capable de reconnaître plusieurs protocoles et attributs protocolaires pour retranscrire le plus fidèlement possible l'activité du réseau.

Objectifs du projet :
L'objectif de ce projet est de maîtriser les systèmes d'exploitation Linux embarqués sur routeur sans fil et la manipulation de compilation croisée pour les architectures ARM. Les étapes nécessaires à la création des firmwares, la mise à jour des firmwares, l'installation et la désinstallation de logiciels sur routeurs, la compilation croisée (Cross-compilation) seront largement abordés durant ce projet.
L'objectif étant d'identifier un outil pertinent pour mettre en place la technique DPI afin d'afficher les statistique d'utilisation de la bande passante d'un routeur, de remonter des alarmes automatique lorsqu'un protocole est utilisé (exemple alarme lorsque le protocole P2P est utilisé) ou tout simplement pour monitorer le trafic passant par le routeur. Plusieurs outils simples existent sur un système linux complet : tcpdump avec quelques scripts, le filtrage L7, Snort, etc. Le travail demandé durant ce projet, est d'identifier l'outil qui permet d'atteindre l'objectif fixé, de le déployer, et de mettre en place quelques scripts et scenarios de tests.

Logiciels : DD-WRT, OpenWRT, tcpdump, L7-Filtring, Snort.
Matériels disponibles : Routeurs linksys
Pré requis : maîtrise de la compilation C, notion de cross-compilation
Encadant : Toufik Ahmed
Email : tad@labri.fr
Mots-clefs : Routeur Linux embarqué