Équipe Réseaux
Sujet Fingerprinting

Sujet de TER
2013–2014

Fingerprinting de routeur

Lieu	Équipe Réseaux, ICube (UMR CNRS 7357)
Encadrants	Jean-Jacques Pansiot (pansiot@unistra.fr) & Pascal Mérindol (pansiot@unistra.fr)

Contexte

Il est souvent utile de classifier les machines ou les routeurs connectés à Internet en classes plus ou moins homogènes, par exemple les PC tournant sous telle ou telle version d'OS, les routeurs de tel ou tel constructeur. Cela permet par exemple d'étudier l'impact de vulnérabilités, les parts de marchés (et leurs évolutions) de tel ou tel constructeur/plateforme logicielle. Le fingerprinting est une méthode qui permet, à partir des messages émis par une machine de déterminer sa signature (fingerprint) et donc lui associer une classe. Par exemple en analysant le comportement du protocole TCP on peut déterminer la variante de TCP utilisée (New-Reno, Cubic, Compound, ...) et en déduire l'OS de amnière plus ou moins précise. Le fingerprinting peut être purement passif (analyse du trafic existant) ou actif (on envoie des messages à la machine à tester) et plus ou moins agressif, voire intrusif.

Sujet

Il s'agit ici de développer un fingerprinting pour les routeurs et autres équipements réseau connectés à Internet. Une contrainte sera de rester "network friendly" donc peu agressif vis à vis du réseau et des équipements. Une première étude a déjà été menée dans l'équipe [1]. Dans un premier temps il s'agira de se familiariser avec l'outil `scamper` [2] et la plateforme internationale planetlab * qui ont servi pour cette étude. Celle ci a permis de dégager 3 classes principales : la première (et plus importante) contenant les routeurs Cisco, la deuxième les routeurs Juniper, et la troisième un ensemble d'autres plateformes. L'objectif est de raffiner cette classification par exemple en divisant certaines classes en fonction du modèle de routeur et/ou version de système. Dans un deuxième temps, il s'agira donc d'étudier d'autres critères de classification : par exemple la taille de certains messages d'erreur ICMP, le comportement à réception de certains messages (options IP, ICMP, etc) ou tout autre critère (non intrusif) à définir et tester. En particulier pour les routeurs activant MPLS [3], les messages ICMP obtenus en réponses à des paquets sonde sont plus riches (espace de label utilisé, TTL MPLS, nombre de labels). Une classification plus spécifique pour ces routeurs sera à étudier et ce type d'étude peut-être généralisé à tout attribut opérationnel spécifique à un routeur (BGP, multicast, etc). Une question complémentaire est la cohérence de cette classification : la signature d'un équipement est elle stable en fonction du point de mesure, du temps, etc ?

∗. http://www.planet-lab.org/

Référence clé (synthèse et critique de l'UE Initiation Recherche)

Des signatures de routeurs basées sur le TTL pour le fingerprinting réseau : [1]

Références

[1] Y Vanaubel, J-J Pansiot, P Mérindol, and B Donnet. Network fingerprinting : Ttl-based router signatures. ACM/USENIX Internet Measurement Conference, 2013. http://icube-web.unistra.fr/papr/docs/files/5085/IMC13-Vanaubel-preliminary.pdf.

[2] M. Luckie. Scamper : a scalable and extensible packet prober for active measurement of the Internet. In Proc. USENIX/ACM Internet Measurement Conference (IMC), November 2010.

[3] B. Donnet, M. Luckie, P. Mérindol, and J.-J. Pansiot. Revealing MPLS tunnels obscured from traceroute. ACM SIGCOMM Computer Communication Review, 42(2) :87–93, April 2012.