TP1: Wiretapping

Teoría de las Comunicaciones

Departamento de Computación
FCEN - UBA

25.08.2015

1. Introducción

El objetivo de este trabajo es utilizar técnicas provistas por la teoría de la información para distinguir diversos aspectos de la red de manera analítica. Para ello, sugerimos el uso de dos herramientas modernas de manipulación y análisis de paquetes: Wireshark [2] y Scapy [3].

2. Normativa

- Fecha de entrega: 23.09.2015
- El informe deberá haber sido enviado por correo para esa fecha con el siguiente formato:
  to: tdc-doc at dc uba ar
  subject: debe tener el prefijo [tdc-wiretapping] y contener en numero de grupo
  body: nombres de los integrantes y las respectivas direcciones de correo electrónico
  attachment: el informe y el código desarrollado. El nombre de los archivos debe contener el numero de grupo.

3. Enunciado

Cada grupo deberá resolver las consignas que siguen a continuación, tomando como referencia lo explicado en clase.

3.1. Primera consigna: capturando tráfico

Sea P la fuente de información generada a partir de todos los paquetes Ethernet que se transmiten en una determinada red entre los instantes de tiempo $[t_i, t_f]$:

$P_{t_i,t_f} = \{p_1 \cdots p_n\}$ siendo p_i el i-esimo paquete transmitido en la red entre los instantes de tiempo $[t_i, t_f]$.

Los paquetes $p_i \in P$ encapsulan diferentes protocolos, que se pueden identificar a través del campo *type* del frame de capa 2 (*p.type* en Scapy). Por lo tanto, con el objetivo de distinguir los protocolos utilizados en una red, se define otra fuente de información S de la siguiente manera:

$$S_{t_i,t_f} = \{s_1 \cdots s_n\} \text{ siendo } s_i = p_i.type \ / \ p_i \in P \text{ entre los instantes de tiempo } [t_i, t_f].$$

Se pide:

1. Implementar una herramienta que simule la fuente de información P para redes locales. Es decir, la herramienta debe escuchar pasivamente los paquetes Ethernet transmitidos en la red local durante un tiempo $t_f - t_i$ y quedarse solo con los símbolos de la fuente correspondiente.
2. Adaptar la herramienta del punto anterior para estimar la probabilidad y la entropía de la fuente S para la red local.

3. Proponga una fuente de información S_1 con el objetivo de distinguir, en lugar de los protocolos como hace S, los nodos (hosts) de la red. La distinción de S_1 debe estar basada *únicamente* en paquetes que utilicen el protocolo ARP.

4. Utilizando la herramienta, realizar experimentos (uno por integrante) capturando paquetes en redes de acceso compartido. Las capturas deben ser lo más extensas posibles ($t_f - t_i \geq 10$ minutos). En la medida de lo posible, intentar capturar en al menos una red que no sea controlada (en el trabajo, en un shopping, etc.).

3.2. Segunda consigna: gráficos y análisis

Presentar un informe científico donde se analice, para cada experimento, las fuentes S y S_1 y a partir de ello determinar:

(a) Los protocolos distinguidos.

(b) La proporción de paquetes ARP sobre el total de la información transmitida.

(c) Los nodos distinguidos.

Los resultados de esta consigna deben estar basados en conceptos formales de la teoría de la información. O sea, se debe analizar qué símbolos son estadísticamente significativos en cada red, analizando la información de cada símbolo con respecto a la entropía de su respectiva fuente.

El informe debe seguir la estructura de un informe científico: somera introducción, métodos y condiciones de cada experimento, resultados y conclusión. La presentación de los resultados debe efectuarse mediante gráficos y su correspondiente análisis. Sugerimos, entre otros, histogramas (de IPs y protocolos) con cortes en los valores de entropía. Se valorará especialmente en esta consigna la creatividad y el análisis propuesto. Recomendamos, pués, pensar cómo resultará más efectivo presentar la información recopilada.

Referencias

[1] RFC 826 (ARP) `http://tools.ietf.org/html/rfc826`

[2] Wireshark (página web oficial) `http://www.wireshark.org`

[3] Scapy (página web oficial) `http://www.secdev.org/projects/scapy/`

[4] OUI (IEEE) `http://standards.ieee.org/develop/regauth/oui/oui.txt`