

Trabajo Práctico Nº1: Wiretapping

Alvaro Jose Fernando, Barbeito Nicolás, Brum Raúl, Nieves Yésica

Resumen—Our premise is ...

I. INTRODUCCIÓN

A. Paquetes ARP

El protocolo ARP (Address Resolution Protocol) permite mapear direcciones de nivel de red a direcciones físicas. La idea de este protocolo se basa en el envío de paquetes que pueden ser de preguntas o respuestas. El emisor del paquete que pregunta por una dirección, envía un mensaje broadcast sobre la red local, siendo respondido por un mensaje unicast por aquel al que pertenece la dirección consultada. Mediante el envío de estos paquetes ARP se construyen las tablas que mapean direcciones de red con direcciones físicas.

B. Entropía de una fuente

Para poder definir la entropía de una fuente, necesitamos la definición de información que aportan los símbolos emitidos por dicha fuente. Se define información de un símbolo s como

$$I(s) = \log(1/P(s))$$

siendo $P(s)$ la probabilidad de ocurrencia de dicho símbolo. De esta manera, puede calcularse la información media suministrada por una fuente de información de memoria nula (los símbolos emitidos son estadísticamente independientes) como

$$\sum_S P(s_i) I(s_i) \forall s_i \in S$$

Esta cantidad media de información por símbolo de la fuente, recibe el nombre de *entropía* $H(S)$ de la fuente de memoria nula.

$$H(S) = \sum_S P(s_i) \log(1/P(s_i))$$

Debido a que la entropía de una fuente depende de la probabilidad de los diferentes símbolos que la componen, se puede demostrar que para una fuente de información de memoria nula con un alfabeto de q símbolos, el valor máximo de la entropía es precisamente $\log q$, alcanzándose solamente si todos los símbolos son equiprobables.

C. Fuente S

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 $[t_i, t_f]$:

$$P_{ti,tf} = \{p_1 \dots p_n\}$$

siendo p_i el i -ésimo paquete transmitido en la red entre los instantes de tiempo $[t_i, t_f]$.

Alvaro Jose Fernando, LU: 89/10, email: fer1578@gmail.com
Barbeito Nicolás, LU: 147/10, email: nicolasbarbeiton@gmail.com
Brum Raúl, LU: 199/98, email: brumraul@gmail.com
Nieves Yésica, LU: 340/05, email: yesica.nieves@gmail.com

Los paquetes p_i pertenecientes a 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:

$$S_{ti,tf} = \{s_1 \dots s_n\}$$

siendo $s_i = p_i.type / p_i$ perteneciente a P entre los instantes de tiempo $[t_i, t_f]$.

D. Propuesta de una nueva fuente S_1

Para analizar la entropía de la red en base a los paquetes ARP observados realizamos una nueva tool en base a la anterior que nos permitiera obtener datos de los campos de dichos paquetes. Se propone como nueva fuente S_1 el conjunto de símbolos conformado por las distintas direcciones IP destino:

$S_1 = \{s_{11} \dots s_{1n}\}$ siendo s_{1i} el valor del campo *pdst* correspondiente a la ip destino del paquete

Al igual que para la fuente S , realizamos el cálculo de la entropía como fue requerido, como la probabilidad e información de sus símbolos.

II. MÉTODOS Y CONDICIONES DE CADA EXPERIMENTO

En esta sección describiremos brevemente las redes elegidas para realizar las escuchas mediante las herramientas indicadas en el enunciado del trabajo practico.

A. Home Lan

Esta medición fue realizada en la Lan de una casa por un intervalo de 2 horas. La misma cuenta con una computadora corriendo un sistema operativo Linux la cual es el router de la Lan y provee a las demas computadoras de acceso a internet ademas de otros servicios de red (proxy, dns, dhcpd, etc). A la misma se encuentran conectadas mediante un switch 4 computadoras cableadas y 2 access point inalámbricos. A estos últimos se encontraban conectados al momento de la medición una notebook y varios celulares. Ademas una de las computadoras cableadas corre una maquina virtual con ip propia independiente y otra de las computadoras cableadas posee otro isp para conectarse a internet por lo que no utiliza a la primera computadora como gateway.

B. red 2

C. red 3

D. red 4

III. RESULTADOS

A. Cálculos y observaciones sobre la Entropía de las fuentes

A continuación se adjuntan algunos los resultados obtenidos:

- "Muestra 1" (*captura1.pcap*):
 - Entropía Fuente S:
 - Entropía Fuente S₁:
- "Muestra 2" (*captura2.pcap*):
 - Entropía Fuente S:
 - Entropía Fuente S₁:
- "Muestra 3" (*captura3.pcap*):
 - Entropía Fuente S:
 - Entropía Fuente S₁:
- "Muestra 4" (*captura4.pcap*):
 - Entropía Fuente S:
 - Entropía Fuente S₁:

B. Protocolos y nodos distinguidos y proporción de paquetes ARP

IV. GRÁFICOS Y ANÁLISIS

A continuación haremos un análisis de cada una de las redes de las cuales capturamos su tráfico. Para ello, haremos uso de distintos gráficos que nos ayudarán a visualizar mejor la información del tráfico en cada red.

A. Analizando tráfico de captura1" (captura1.pcap)

B. Analizando tráfico de captura2" (captura2.pcap)

C. Analizando tráfico de captura3" (captura3.pcap)

D. Analizando tráfico de captura4" (captura4.pcap)

V. REFERENCIAS