Definición de características del tráfico de aplicaciones para la detección de malware

En este documento se presentan algunas de las características más relevantes que fueron propuestas por trabajos de investigación realizados por investigadores que han compartido sus hallazgos con el público. A continuación se dará un resumen de las características obtenidas en dichos trabajos, el método de clasificación usado y los resultados obtenidos.

1) **Malware Detection Using Network Traffic Analysis in Android Based Mobile Devices**

   Características obtenidas:
   - **Tamaño promedio de los paquetes**
   - Duración media del flujo
   - Intervalo de tiempo entre los paquetes enviados
   - **Relación entre los bytes entrantes y salientes**
   - Relación entre paquetes entrantes y salientes
   - **Promedio de Bytes Enviados por Flujo**
   - Intervalo de tiempo entre paquetes recibidos
   - Composición del tráfico (% de TCP)
   - **Promedio de Paquetes Enviados por Flujo**
   - **Promedio de Bytes Enviados por Segundo**
   - Número promedio de paquetes enviados por segundo
   - **Promedio de Bytes Recibidos por Flujo**
   - **Promedio de Paquetes Recibidos por Flujo**
   - Número promedio de bytes recibidos por segundo
   - Número promedio de paquetes recibidos por segundo
   - Relación entre el número de conexiones y el número de IPs de destino

   En este estudio las características más notables en el comportamiento de las aplicaciones maliciosas fueron las que sobresalen en las características anteriores (las que aparecen en negrilla).

   Método utilizado: Se utiliza un clasificador basado en reglas (se puede inferir que fue un árbol de decisión) para realizar la clasificación de una aplicación como maliciosa. En este método se definieron tres niveles de clasificación: bajo riesgo, mediano riesgo y alto riesgo, esta clasificación se hacía de acuerdo a las características obtenidas.

Resultados: El clasificador predijo correctamente 45 muestras del total de 48 muestras, con una precisión del 93,75%.

2) **DroidCollector: A High Performance Framework for High Quality Android Traffic Collection**

Características obtenidas: En este estudio la característica más relevante fue el tráfico HTTP, dado que HTTP es el protocolo predominante adoptado por la mayoría de las aplicaciones móviles, y la información de metadatos en las cabeceras de petición HTTP siempre contiene información valiosa. Estas características extraídas incluyen el campo del host, el campo Request-Uri, el campo Request-Method y el campo User-Agent.

Método utilizado: Para este estudio se utilizó un clasificador SVM(Support Vector Machine) para la clasificación de aplicaciones en benignas o maliciosas.

Resultados: En promedio, se consiguió un 98% de confianza en que estos paquetes de petición HTTP desconocidos se clasifican correctamente por el modelo de detección en sus categorías correspondientes.

3) **Mobile malware detection through analysis of deviations in application network behavior**

Características obtenidas:

- Promedio, desviación estándar, mínimo y máximo de datos enviados y recibidos en bytes.
- Promedio, desviación estándar, mínimo y máximo de datos enviados y recibidos en porcentaje de la cantidad total de datos transmitidos.
- Porcentaje de bytes enviados y recibidos.
- Estado de red (Celular, WiFi o "sin red").
- Tiempo (en segundos) desde que se enviaron los últimos datos de recepción de la aplicación.
- Modo de envío y recepción (eventual\continuo) derivado de "desde-última-envío y recepción-segundos"; es decir, si el último evento de envío o recepción de datos fue detectado hace menos de un número especificado de segundos, el modo correspondiente (envío o recepción) es continuo, de lo contrario es eventual.
- Dos estados de aplicación: el primero especifica si la aplicación se encuentra en primer plano o en segundo plano y el segundo especifica si la aplicación se encuentra entre las tareas activas o inactivas en el momento de la medición.

- Tiempo en el fondo anterior (en segundos y porcentaje): tiempo total que una aplicación ha estado en el fondo anterior desde que se inició la última monitorización de esta aplicación.
- Minutos desde el último tiempo de modificación activo de la aplicación.
- Minutos pasados desde el último evento de datos recibido por la aplicación.

Método utilizado: El análisis incluyó una validación cruzada y la aplicación de una regresión lineal, Tablas de decisión, Support Vector Machine para regresión, Gaussian Processes para regresión, Isotonic Regression, y Decisión/Regression tree (árbol de decisión, REPTree)

Resultados: Se pudo observar que para casi todas las aplicaciones maliciosas se detectó un alto nivel de desviación (80-100% de las instancias anómalas) del comportamiento original de la red.

4) **A First Look at Android Malware Traffic in First Few Minutes**

Características utilizadas: El principal enfoque de este estudio fue el tráfico HTTP y DNS. En el caso del el DNS se analizaron las consultas dns, tanto su tipo como el número de consultas. Para el caso del tráfico HTTP se tomó la longitud de los paquetes, Relación entre la cantidad de tráfico del enlace descendente (downlink) y del enlace ascendente (uplink), HTTP Request y el tráfico de anuncios.

Método utilizado: Para este caso se utilizó el análisis estadístico para detectar patrones de comportamiento del tráfico en las aplicaciones maliciosas.

Resultados: Se observó que más del 70% de los programas maliciosos generan tráfico malicioso en los primeros 5 minutos, la consulta DNS y la petición HTTP pueden utilizarse para identificar el malware, y la tasa de detección alcanza el 69,55% y el 40,89% respectivamente, el tráfico de anuncios puede afectar en gran medida a la detección de malware.

Conclusiones y trabajo a futuro