Targeted Exerciser for Android Malware and Grayware

Master Thesis

Author: Mario Herreros Díaz

Mentors: Juan E. Tapiador, Guillermo Suárez-Tangil

Master in Cybersecurity

September 27th, 2016

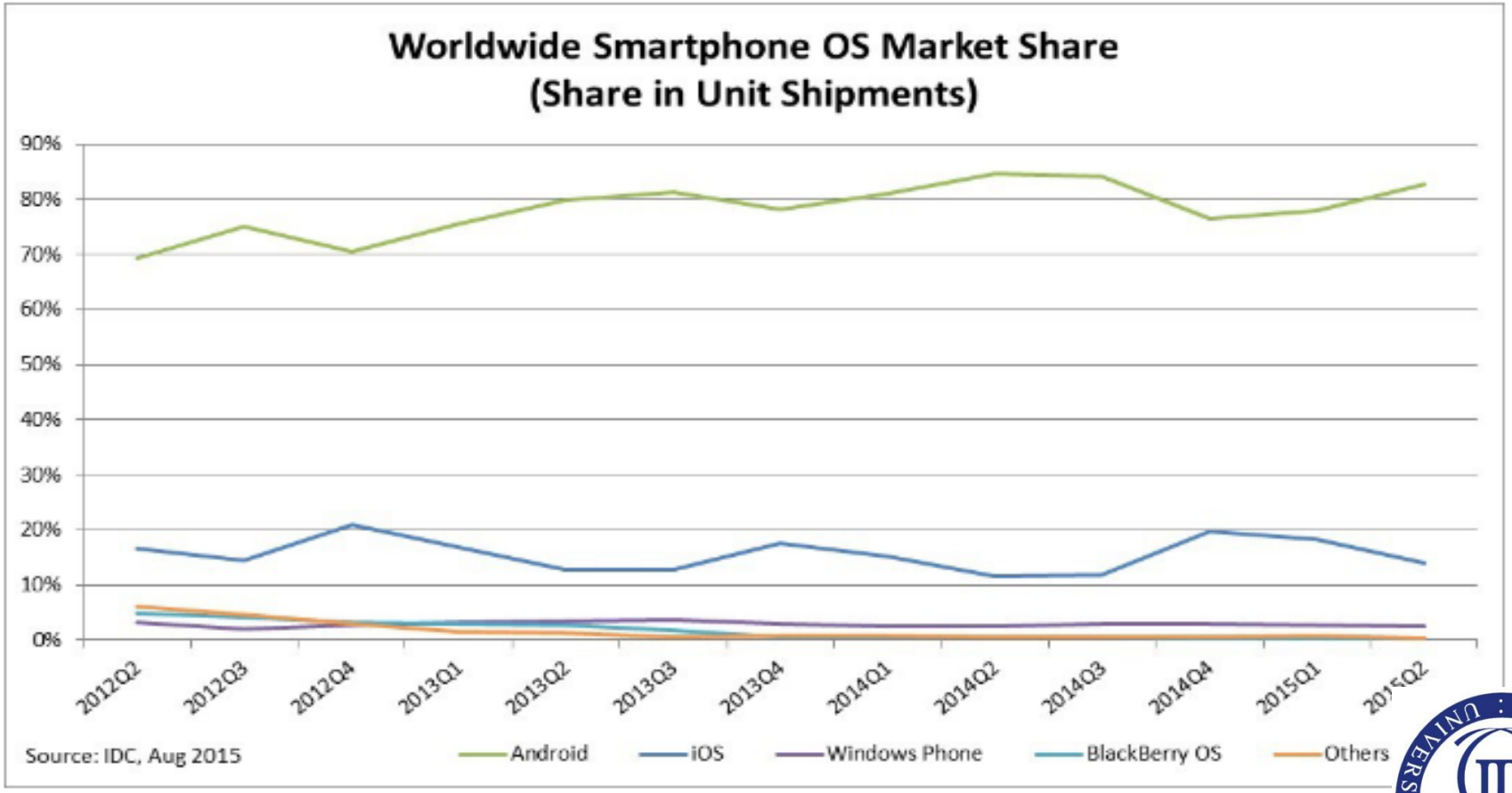
Índice

- Introducción
- Targetdroid
- Extendiendo Targetdroid
- Arquitectura
- Casos de estudio & Demo
- Conclusiones

Introducción
Motivación

- Fuerte incremento de *malware* en sistemas Android
- Causas:
  - Líder de ventas en el mercado global de dispositivos móviles
  - Vulnerabilidades existentes en el sistema de seguridad de Android
- Presencia de malware cada vez más especializado y complejo (ofuscación, bypassing, …)
- **Targeted Malware**

Introducción
Motivación

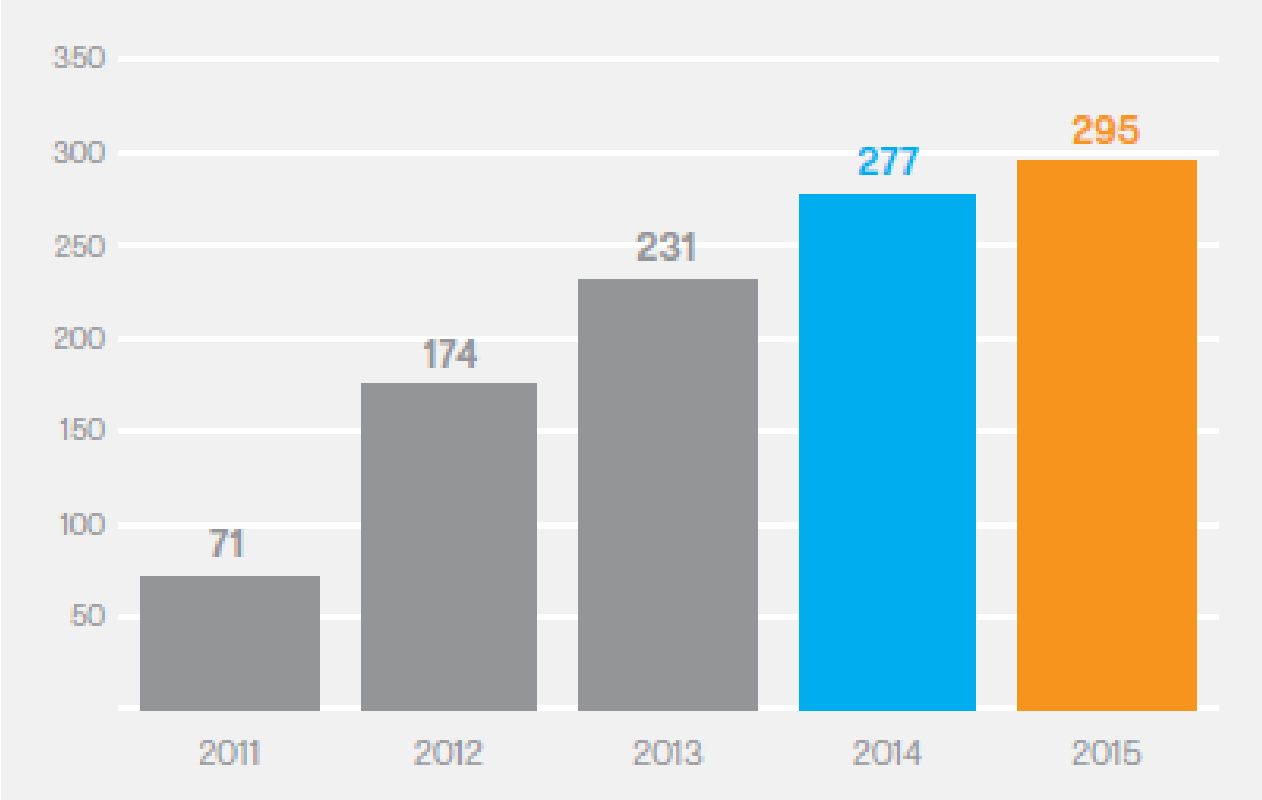


Introducción
Motivación

Cumulative Android Mobile Malware Families

Symantec

- *The number of Android malware families added in 2015 grew by 6 percent, compared with the 20 percent growth in 2014.*

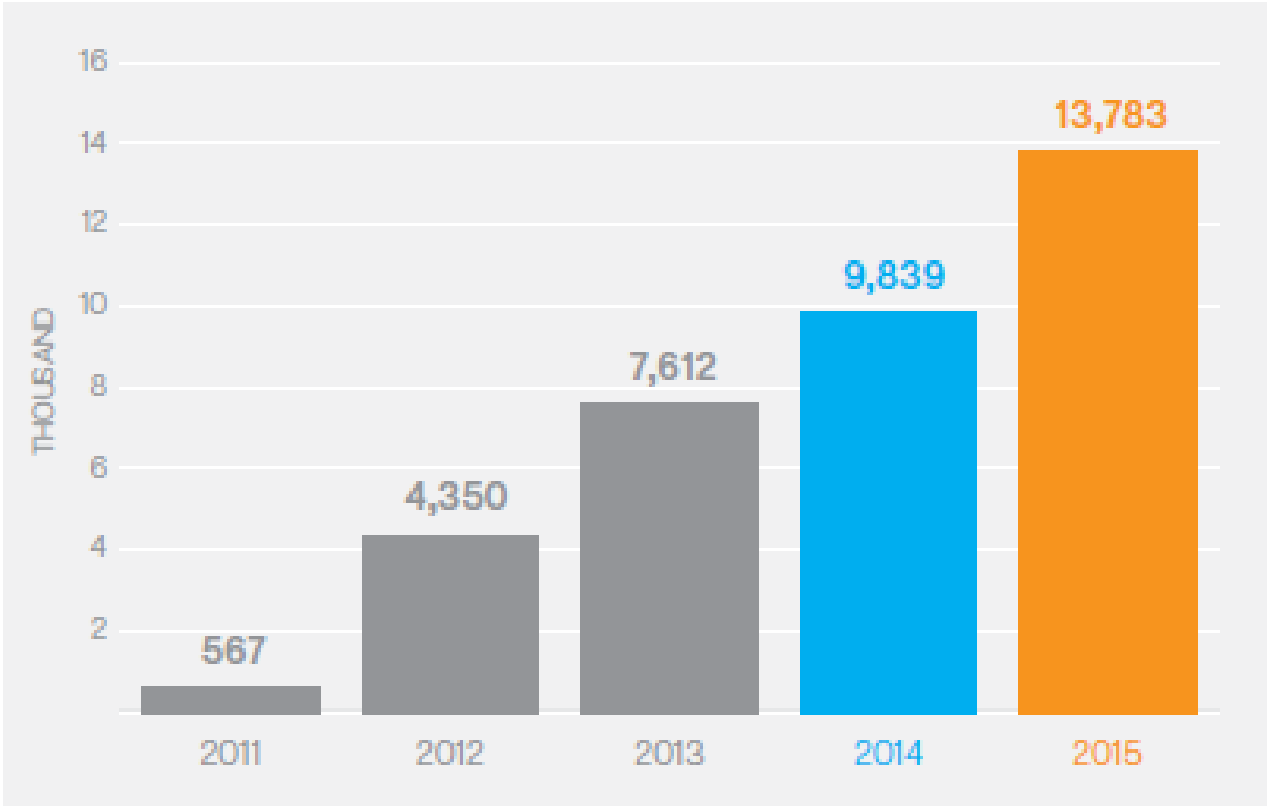


Introducción
Motivación

Cumulative Android Mobile Malware Variants

Symantec

- *The volume of Android variants increased by 40 percent in 2015, compared with 29 percent growth in the previous year.*



Introducción
Targeted Malware/Greyware

- Tipo de malware avanzado y complejo.
- Su ejecución maliciosa depende de:
  - Comportamiento del usuario.
  - Otros factores relativos al usuario (localización, modelo de dispositivo, aplicaciones instaladas, …).
- Su detección supone un gran reto:
  - Condiciones específicas de activación.
  - Gran número de escenarios posibles.

Introducción
Targeted Malware/Greyware

- **Stuxent**: estuvo latente hasta que se instaló una aplicación concreto y fue usada en cierta localización, teniendo como objetivo las plantas nucleares iraníes.
- **Eurograbber**: troyano cuyo objetivo era los usuarios de banca online.
- **Dendroid Remote Access Toolkit**: permite configurar el tipo de usuarios a los que atacar.

Targetdroid
Modelo estocástico

- Basado en el estudio *Detecting Targeted Smartphone Malware with Behavior-Triggering Stochastic Models.*
- Generación de contextos basados en **comportamientos de usuario**.
- Versión inicial basada en el uso de **modelos estocásticos**.
- **Limitación**: generación de un gran número de contextos para poder alcanzar el escenario deseado.

Extendiendo Targetdroid

- Definición de un lenguaje nuevo para representar distintos conjuntos de comportamientos relativo al usuario.
- Basado en :
  - Escenarios.
  - Contextos.
  - Eventos.
- Creación de un nuevo módulo para Targetdroid.
  - Interpretación del lenguaje definido.
  - Generación de eventos.
  - Análisis dinámico.

Extendiendo Targetdroid Behavioural User Language

- Define distintos escenarios que representan comportamientos de usuario y otros factores.
- Basado en el formato de texto JSON.
- Estructurado en:
  - **Scenario**
  - **Context**
  - **Event**

Extendiendo Targetdroid Behavioural User Language Scenario

- Es la agrupación de un conjunto de contextos.
- Permite compartir mismos contextos entre distintos escenarios.

Extendiendo Targetdroid Behavioural User Language Context

- Describe todos los posibles eventos que pueden ser realizados durante la simulación del comportamiento del usuario.
- Asociados a un momento en el tiempo.
- Tres tipos de contextos:
  - **Emulator configuration context**
  - **OS configuration context**
  - **Execution context**

Extendiendo Targetdroid Behavioural User Language Context

- Emulator configuration context:
  - Definición de las propiedades del entorno.
  - Configuración del emulador usado como sandbox.
  - Configuración previa a ser ejecutado el emulador.
  - Momento en el tiempo: t = -1.
  - Ejemplos:
    - Modelo del dispositivo móvil
    - Presencia de cámara delantera
    - IMEI del dispositivo

Extendiendo Targetdroid Behavioural User Language Context

- OS configuration context:
  - Definición de las propiedades del sistema inicializado.
  - Configuración del emulador Android a nivel de sistema operativo.
  - Configuración realizada en el momento en el que el emulador ha arrancado.
  - Momento en el tiempo: t = 0.
  - Ejemplos:
    - Nivel de batería
    - Aplicaciones instaladas

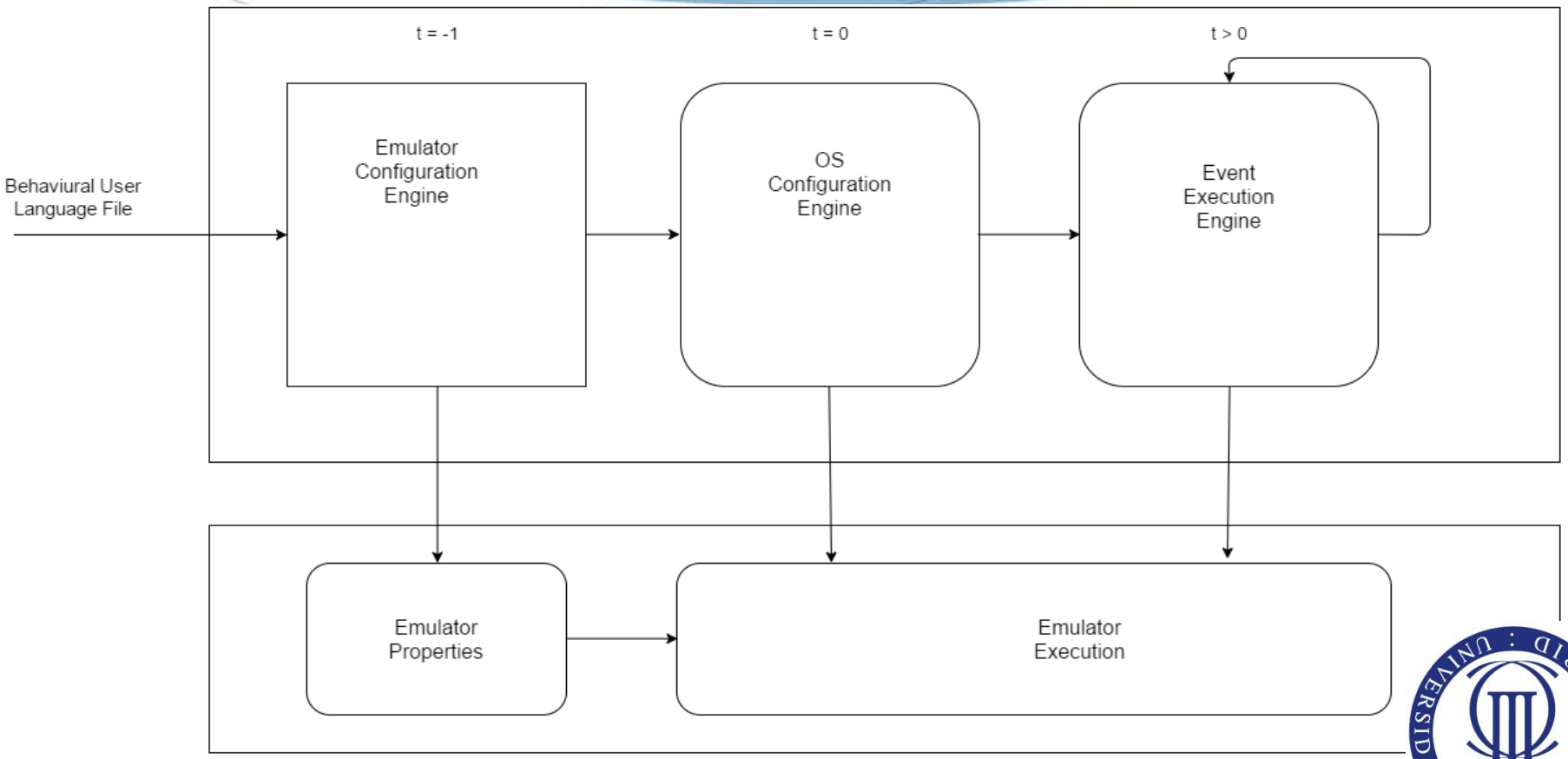
Extendiendo Targetdroid Behavioural User Language Context

- Execution context:
  - Eventos relativos a la interacción del usuario con el sistema.
  - Momento en el tiempo: $t > 0$.
  - Ejemplos:
    - Envío de SMS
    - Recibir una llamada
    - Ejecutar una aplicación
    - Generar una localización

Extendiendo Targetdroid Behavioural User Language Event

- Define cada una de las posibles acciones que pueden ser realizadas en el sistema.
- Es la unidad atómica del sistema desarrollado.
- Diferentes tipos de eventos:
  - Telnet
  - Configuración de properties
  - adb

Extendiendo Targetdroid
Arquitectura



Extendiendo Targetdroid Emulator Configuration Engine

- Fichero properties.ini del emulador de Android.
  - Define las propiedades del dispositivo virtual.
- Opciones a través de línea de comando.
  - Al ejecutar el emulador.

Extendiendo Targetdroid
OS Configuration Engine

- Instalación de aplicaciones
  - Uso de adb.
- Inyección de eventos de configuración de OS
  - Zona horaria.
  - Estado de a batería y la conexión de electricidad.
  - Uso de Telnet.

Extendiendo Targetdroid
Event Execution Engine

- Intents
  - Invocación de componentes y servicios del sistema Android.
  - Uso de adb.
- Comandos ADB
  - Usar adb para realizar acciones específicas.
  - Tomar captura de pantalla, subir/bajar volumen, etc.

Extendiendo Targetdroid Event Execution Engine

- Comandos Telnet
  - Uso del protocolo Telnet.
  - Envío de comandos para generar eventos en el emulador.
  - GSM, batería, llamadas, SMS, localización.
- Monkey tester
  - Acepta la entrada de scripts para realizar monkey testing.
  - Genera eventos relativos a la interfaz de usuario.

Extendiendo Targetdroid Event Execution Engine

- Comandos Telnet
  - Uso del protocolo Telnet
  - Envío de comandos para generar eventos en el emulador
  - GSM, batería, llamadas, SMS, localización.
- Monkey tester
  - Acepta la entrada de scripts para realizar monkey testing.
  - Genera eventos relativos a la interfaz de usuario.

Extendiendo Targetdroid Event Execution Engine

- Comandos Telnet
  - Uso del protocolo Telnet.
  - Envío de comandos para generar eventos en el emulador.
  - GSM, batería, llamadas, SMS, localización.
- Monkey tester
  - Acepta la entrada de scripts para realizar monkey testing.
  - Genera eventos relativos a la interfaz de usuario.

Casos de estudio
Dormant Malware/Grayware

- Uso del malware AndroRAT.
- Condiciones de activación del malware:
  - Presencia de cámara trasera en el dispositivo → t = -1
  - Nivel de batería superior al 65% → t = 0
  - Localización específica → t > 0
  - Estado del WiFi: conectado → t > 0

Casos de estudio
Anti-analysis Malware

- Uso del malware AndroRAT.
- Condiciones de activación del malware:
  - IMEI del dispositivo: 123456789 → t = -1
  - IP del dispositivo: 192.168.111.224 → t = -1
  - Nivel de batería distinto a 50% → t = 0
  - Estado de la conexión a la red eléctrica desconectada → t = 0

DEMO

- Vídeo:

Conclusiones

- Evolución de la complejidad del malware: Targeted malware.
- Los sistemas de detección actuales son insuficientes.
- Necesidad de la creación de un sistema de detección basado en el comportamiento de usuario.
- Agilidad en la generación de escenarios y contextos distintos.

Conclusiones
Líneas futuras

- Integración con sistemas Cloud.
- Integración con Big Data.
- Extender el sistema a otros sistemas operativos y dispositivos.
- Enriquecer el lenguaje definido con nuevos eventos y artefactos.

Targeted Exerciser for Android Malware and Grayware

¿Cuestiones? ¿Dudas? ¡Muchas gracias!

Presentación realizada por:

Mario Herreros Díaz 100275558