Facultad de Ciencias Exactas
UNIVERSIDAD NACIONAL DEL CENTRO DE LA PROVINCIA DE BUENOS AIRES

TRABAJO PRÁCTICO: 'ABSTRACT'

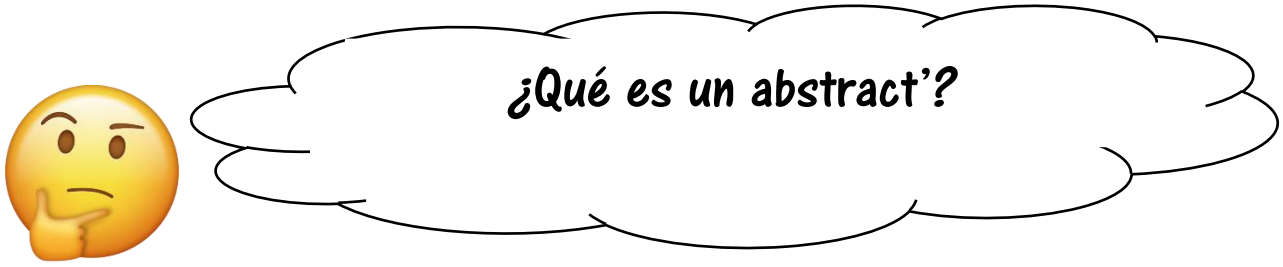
SISTEMAS, TUPAR, TUDAI Y TUARI

➢ Actividades de pre-lectura

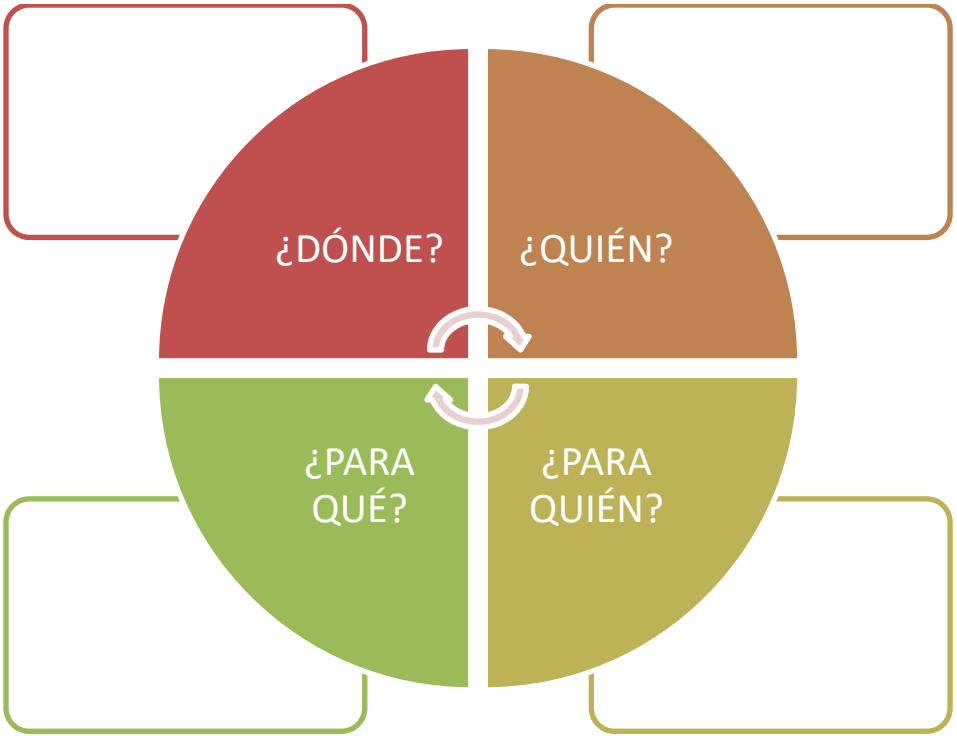
Como parte de la formación tanto en la universidad como en el desempeño de la actividad laboral, los ingenieros y desarrolladores recurren a diferentes fuentes de información. En algunos casos será necesario hacer una selección de que es lo que realmente necesitamos leer o eventualmente escribir trabajos de investigación o una tesis.

Como estrategia de lectura es importante poder entender un resumen académico ó 'abstract'.

Los invitamos a ver el **apunte teórico** correspondiente, en la plataforma. Luego complete las actividades propuestas.



1. En grupo, **COMPLETEN** el cuadro con la información apropiada.



- **Actividades de lectura.**

1- REALICE un barrio de lectura del texto en la página 3 y complete el cuadro.

TíTULO DEL ARTICULO	
NOMBRE DEL AUTOR/ES	
INSTITUCIÓN DE AFILIACIÓN DEL O LOS AUTOR/ES	
PALABRAS CLAVE	
NOMBRE DE LA PUBLICACIÓN	
FECHA DE PUBLICACIÓN EN LÍNEA	

2- ¿Qué resulta relevante a la hora de determinar el tema y la disciplina a la que corresponde? **JUSTIFIQUE.**

J Intell Inf Syst
DOI 10.1007/s10844-010-0148-x

"Andromaly": a behavioral malware detection framework for android devices

Asaf Shabtai · Uri Kanonov · Yuval Elovici · Chanan Glezer · Yael Weiss

Received: 22 August 2010 / Revised: 27 October 2010 / Accepted: 17 November 2010

Abstract This article presents Andromaly—a framework for detecting malware on Android mobile devices. The proposed framework realizes a Host-based Malware Detection System that continuously monitors various features and events obtained from the mobile device and then applies Machine Learning anomaly detectors to classify the collected data as normal (benign) or abnormal (malicious). Since no malicious applications are yet available for Android, we developed four malicious applications, and evaluated Andromaly's ability to detect new malware based on samples of known malware. We evaluated several combinations of anomaly detection algorithms, feature selection method and the number of top features in order to find the combination that yields the best performance in detecting new malware on Android. Empirical results suggest that the proposed framework is effective in detecting malware on mobile devices in general and on Android in particular.

Keywords Mobile devices · Machine learning · Malware · Security · Android

1 Introduction

Personal Digital Assistants (PDAs), mobile phones and recently smartphones have evolved from simple mobile phones into sophisticated yet compact minicomputers

A. Shabtai (✉) · U. Kanonov · Y. Elovici · C. Glezer · Y. Weiss
Deutsche Telekom Laboratories at Ben-Gurion University, Department of Information Systems Engineering, Ben-Gurion University, Be'er Sheva 84105, Israel
e-mail: shabtaia@bgu.ac.il

U. Kanonov
e-mail: kanonov@bgu.ac.il

Y. Elovici
e-mail: elovici@bgu.ac.il

C. Glezer
e-mail: chanan@bgu.ac.il

Published online: 06 January 2011

OBSERVE el texto nuevamente y **DECIDA** si las siguientes oraciones son verdaderas o falsas. **JUSTIFIQUE** las falsas.

a) El título incluye una idea de la temática del libro.
b) Los autores trabajan en un Asia.
c) Las palabras claves permiten a los buscadores identificar textos por su relevancia temática
d) El texto es parte de un texto académico más extenso.
e) El 'abstract' incluye toda la información que el científico considera necesaria publicar.
f) 'Andromaly' es una versión actualizada de Android.
g) El 'abstract' es un resumen del contenido de un trabajo de investigación.
h) Los autores proponen herramientas de 'ML' para identificar aplicaciones maliciosas.
i) Los usuarios de dispositivos Apple desarrollaron esta aplicación.
j) 'Andromaly' resultó efectivo en dispositivos Android.

El resumen académico o `abstract`

"El abstract debería ser considerado como una mini-versión del artículo" (Day 1991). Por tanto, se recomienda preservar la estructura IMRaD en él, describiendo los objetivos del estudio, la metodología usada, los resultados principales del trabajo y sus conclusiones fundamentales. Un `abstract` generalmente tiene un único párrafo y menos de 250 palabras y debe "permitir a los lectores identificar el contenido básico del documento rápida y fielmente, con el fin de determinar la relevancia del mismo para sus intereses y, por tanto, para decidir si necesitan leer el documento en su totalidad" (definición del American National Standards Institute).

LAS PARTES DE UN ABSTRACT

La extensión de este tipo de textos puede variar dependiendo de qué estemos resumiendo; y en algunos casos, el contenido puede variar de una disciplina a otra. En las ciencias de la computación, se espera que el resumen que precede a un trabajo de investigación contenga la siguiente información en el orden propuesto.

MOTIVACIÓN: Razones por las que el problema y los resultados son importantes.

PROBLEMA: El problema al que se intenta dar respuesta y el alcance de la investigación.

ENFOQUE: Determinación del enfoque o manera en la que se ha encarado el tema. En caso de un experimento, la metodología o instrumentos

RESULTADOS: La respuesta que se propone para el problema planteado

CONCLUSIONES: Las implicaciones de esta respuesta que se propone.

3- **RELEA** el resumen de la página 3 e identifique las diferentes partes:

MOTIVACION / PROBLEMA/ ENFOQUE/ RESULTADOS/ CONCLUSIONES

¿Todas las partes están presentes?

4- **IDENTIFIQUE** y **TRANSCRIBA** las frases que se usan para introducir las secciones del resumen.

5- Lea la siguiente lista e **INDIQUE** en qué sección del resumen podrían usarse.

	1) *This….is based on findings..*		2) *…the problem/ issue/question of hacking….*
	3) *…users have experienced difficulties with….*		4) *For the purpose of this work…..*
	5) *We carried out a procedure…*		6) *Security is an intrinsic part of…..*
	7) *Integration appears to pose a challenge …*		8) *.. the framework revealed shortcomings in…*
	9) *Several techniques were employed….*		10) *This experimental study replicates…..*
	11) *In an attempt to address this problem….*		12) *User's experiences are integral to….*
	13) *We conclude that…*		14) *In order to find a solution/ alternative….*
	15) *The answer to the problem lay in……*		16) *… the next stage in the process….*
	17) *…by means of a computer simulation….*		18) *Twenty-five devises were selected from…*
	19) *The application of the algorithm produced some interesting results….*		20) *Process automation appears to impact on….*
	21) *….brought about fundamental changes…*		22) *….obtained more accurate results….*
	23) *To summarize….*		24) *To bring this paper to a close…*
	25) *As we have seen…*		26) *…we may draw the following conclusions…..*
	27) *Stated briefly….*		28) *In this paper we propose….*
	29) *We apply the technique to a set of ….. and find that……*		30) *We evaluate the efficacy of*

6- Estilo académico en inglés. **OBSERVE** esta lista y **MARQUE** las características como propias del estilo académico (AC) ó no académico/general (NC/ G).

	Términos específicos: framework, users, monthly		Términos generales: things, people, sometimes
	Palabras acortadas, formas contraídas, y siglas populares: LOL, lab tests, gonna study.		Palabras completas y siglas explicadas: laboratorio experiment, we intend to study

	Oraciones cortadas: Well, kind of… they seem to affect each other, up and down they go!		Oraciones claras y completas: Evidence suggests a correlation between A and B.
	Signos de puntuación para expresar emotividad: Come on! Seven servers this guys and no sound?		Signos de puntuación para organizar ideas: Despite redundancy, interruptions in streaming occurred.

7- A continuación, encontrará una serie de textos breves para trabajar en grupo. Los textos han sido cortados y mezclados. **LÉANLOS** detenidamente y **PROPONGAN** correcto para cada uno.

a. **DECIDAN** cuáles de ellos son resúmenes académicos y **JUSTIFIQUEN**.

8- **IDENTIFIQUEN** la temática de cada uno de ellos y **CONSIGNEN** posibles palabras clave en el cuadro.

	TEMA	**PALABRAS CLAVE**
TEXTO A		
TEXTO B		
TEXTO C		
TEXTO D		
TEXTOE		
TEXTO F		

9- INDIQUE qué título le asignarían a cada texto

a. An Android Application Sandbox System for Suspicious Software Detection
b. AndroidLeaks: Automatically Detecting Potential Privacy Leaks in Android Applications on a Large Scale
c. Virtual Objects on the Internet of Things
d. Android Permissions Demystified
e. What is IoT?
f. History of IoT.

10- PROPONGA una forma en castellano para cada uno de los títulos.

	TEXTO A
	MIT professor Neil Gershenfeld's book, When Things Start to Think, also appearing in 1999, didn't use the exact term but provided a clear vision of where IoT was headed.
	Wanting to bring radio frequency ID (RFID) to the attention of P&G's senior management, Ashton called his presentation "Internet of Things" to incorporate the cool new trend of 1999: the internet.
	Kevin Ashton, co-founder of the Auto-ID Center at MIT, first mentioned the internet of things in a presentation he made to Procter & Gamble (P&G) in 1999.

	TEXTO B
	Both the sandbox and the detection algorithms can be deployed in the cloud, providing a fast and distributed detection of suspicious software in a mobile software store akin to Google's Android Market. Additionally, AASandbox might be used to improve the efficiency of classical anti-virus applications available for the Android operating system.
	In this paper, we propose an Android Application Sandbox (AASandbox) which is able to perform both static and dynamic analysis on Android programs to automatically detect suspicious applications. Static analysis scans the software for malicious patterns without installing it. Dynamic analysis executes the application in a fully isolated environment, i.e. sandbox, which intervenes and logs low-level interactions with the system for further analysis.
	This makes it harder to detect and react upon malware attacks if using conventional techniques.
	Smartphones are steadily gaining popularity, creating new application areas as their capabilities increase in terms of computational power, sensors and communication. Emerging new features of mobile devices give opportunity to new threats. Android is one of the newer operating systems targeting smartphones. While being based on a Linux kernel, Android has unique properties and specific limitations due to its mobile nature.

	TEXTO C
	Based on the problems this paper proposes a structure that supports the generic construction of virtual objects irrespective of their business logic and their integration with other applications and "things"
	Digital objects like physicists should be part of Internet of Things but the different structures of these digital objects causes in most cases these digital objects can interact only with specific applications that know the specific format
	As technology advances more and more "things" began to appear in digital format, such as: tickets, agendas, books, electronic purses, etc. Internet of things encourages communication and integration of physical objects with each other and people to automate tasks and improve efficiency.

	TEXTO D
	We built Stowaway, a tool that detects overprivilege in compiled Android applications. Stowaway determines the set of API calls that an application uses and then maps those API calls to permissions. We used automated testing tools on the Android API in order to build the permission map that is necessary for detecting overprivilege.
	We apply Stowaway to a set of 940 applications and find that about one-third are overprivileged. We investigate the causes of overprivilege and find evidence that developersare trying to follow least privilege but sometimes fail due to insufficient API documentation.
	We study Android applications to determine whether Android developers follow least privilege with theirpermission requests.
	Android provides third-party applications with an extensive API that includes access to phone hardware, settings, and user data. Access to privacy- and security-relevant parts ofthe API is controlled with an install-time application permission system.

	TEXTO E
	As mobile devices become more widespread and powerful, they store more sensitive data, which includes not only users' personal information but also the data collected via sensors throughout the day. When mobile applications have access to this growing amount of sensitive information, they may leak it carelessly or maliciously.
	To combat this problem, we present AndroidLeaks, a static analysis framework for automatically finding potential leaks of sensitive information in Android applications on a massive scale. AndroidLeaks drastically reduces the number of applications and the number of traces that a security auditor has to verify manually.
	AndroidLeaks examined these applications in 30 hours, which indicates that it is capable of scaling to the increasingly large set of available applications.

	We evaluate the efficacy of AndroidLeaks on 24,350 Android applications from several Android markets. AndroidLeaks found 57,299 potential privacy leaks in 7,414 Android applications, out of which we have manually verified that 2,342 applications leak private data including phone information, GPS location, WiFi data, and audio recorded with the microphone.
	Google's Android operating system provides a permissions-based security model that restricts an application's access to the user's private data. Each application statically declares the sensitive data and functionality that it requires in a manifest, which is presented to the user upon installation. However, it is not clear to the user how sensitive data is used once the application is installed.

	TEXTO F
	This adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate without a human being involved, and merging the digital and physical worlds.
	Thanks to cheap processors and wireless networks, it's possible to turn anything, from a pill to an aeroplane, into part of the IoT.
	The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, collecting and sharing data.

11- RELEA los textos y **SELECCIONE** con cuál/es se relacionan las siguientes oraciones.

a. Detectar software malicioso en Android es difícil
b. Propone una aplicación para escanear dispositivos móviles.
c. Propone el uso de una aplicación desde la nube para mejorar la seguridad de Android.
d. Analiza el acceso a la información del usuario que tienen las aplicaciones instaladas en los dispositivos móviles.
e. Propone una aplicación para preservar la privacidad usuarios de aplicaciones en Android.
f. La aplicación propuesta duplica los resultados de los análisis humanos.
g. Los objetos y artefactos digitales evidencian incompatibilidades.
h. Los autores proponen la construcción de objetos virtuales genéricos.
i. Los costos de producción hacen posible que más objetos estén conectados a redes wifi.
j. Los objetos inteligentes pueden conectarse sin mediación humana.
k. Internet de las cosas fue un concepto inventado para vender un sistema de identificación por radiofrecuencia.

12- **EXPLIQUE** la siguiente frase: "*Google's Android operating system provides a permissions-based security model that restricts an application's access to the user's private data.*"

.....

.....

.....

.....

➢ Actividades de escritura

Los resúmenes presentan las ideas principales de artículos de divulgación más extensos. ¿Cuál de los artículos le interesaría leer? **EXPLIQUE** y **JUSTIFIQUE** con información de los resúmenes.

➢ Referencias

Bailey, S. (2015) *Academic Writing: A Handbook for International Students* (4th Ed.) New York. Routledge

Hyland, K. (2006) *English for Academic Purposes: An advanced resource book.* New York .Routledge

McCarthy, M & O'Dell, F. (2008*) Academic Vocabulary in Use.* Cambridge. Cambridge University Press

Schelppegrell, M.J. (2004) *The Language of Schooling: A Functional Linguistic Perspective*. London. Lawrence Erlbaum Associates

Van Geyte, E. (2013) Writing: Learn to write better academic essays. London. Harper Collins Publishers

Academic articles

Blasing,T; Batyuk, L; Derrick Schmidt,A; Camtepe, S.A; & Albayrak.S. (2010) "An Android Application Sandbox System for Suspicious Software Detection*". 5th International Conference on Malicious and Unwanted Software*. Disponible en: https://ieeexplore.ieee.org/document/5665792 (Retrieved 17/11/2018)

Espada, J.P; Sanjuán Martinez, O; Garcia-Bustelo, B.C. P; Cueva Lovelle, J.M. (2011) 'Virtual Objects on the Internet of Things'. *International Journal of Artificial Intelligence and Interactive Multimedia, Vol. 1, Nº 4. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3867814*(Retrieved 17/11/2018)

Gibler. C; Crussell,J; Erickson, J. & Chen, H. (2012) "AndroidLeaks: Automatically Detecting Potential Privacy Leaks In Android Applications on a Large Scale". *International Conference on Trust and Trustworthy Computing* pp 291-307. Disponible en: https://link.springer.com/chapter/10.1007/978-3-642-30921-2_17 (Retrieved 17/11/2018)

Porter Felt, A; Chin, E; Hanna, S; Song, D; Wagner, D. (2011) "Android Permissions Demystified". *CCS '11 Proceedings of the 18th ACM conference on Computer and communications security* Pages 627-638. Disponible en: https://dl.acm.org/citation.cfm?id=2046779 (Retrieved 17/11/2018)

Shabtai, A; Kanonov, U; Elovici, Y; Glezer, C. & Weiss, Y. (2010) "Andromaly": a behavioral malware detection framework for android devices**".** *Journal of Intelligent Information Systems*

Volume 38, Issue 1, pp 161–190. *Disponible en:* **https://link.springer.com/article/10.1007/s10844-010-0148-x** (Retrieved 17/11/2018)

On-line magazines

Ranger, S. (2018) *ZDNET*. Disponible en*:* https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/ (Retrieved 17/11/2018)

Rouse, M. (n/d) *TARGETTECH.*, Disponible en: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (Retrieved 17/11/2018)