DESARROLLO DE CAPACIDADES DE DEFENSA Y SEGURIDAD CIBERNETICA

Lic. Walter Fabián Agüero
Director: Dr. Roberto Uzal [a]
Co directores: Dr. Daniel Macedo – [b] / Dr. Daniel Riesco – Dr. Germán Montejano [a]

[a] Universidad Nacional de San Luis, San Luis, Argentina. Facultad de Cs. Fco. Mat. y Nat. / Universidad Nacional de San Luis. Ejército de los Andes 950 – San Luis

[b] Universidad Federal de Minas Gerais, Belo Horizonte, Brasil. Av. Antônio Carlos, 6627 – Pampulha - Belo Horizonte - Brasil

wfaguero@gmail.com

Resumen

Es poco probable que cuando en EEUU se creó el proyecto de la DARPA (Defense Advanced Research Projects Agency) cuyo fin era buscar e intercambiar información entre los investigadores, científicos y militares, ubicados en distintos sitios distantes hubieran pensado en las dimensiones que hoy tiene Internet.

Sin lugar a dudas han sido varios los factores que han permitido el crecimiento de esta gran red: conectividad, prestadoras de internet y dispositivos tales como computadoras, tablet, celulares, etc.

Es probable que el Smartphone (imagen 1)[1] sea el dispositivo para tener una conexión constante e ininterrumpida a Internet.

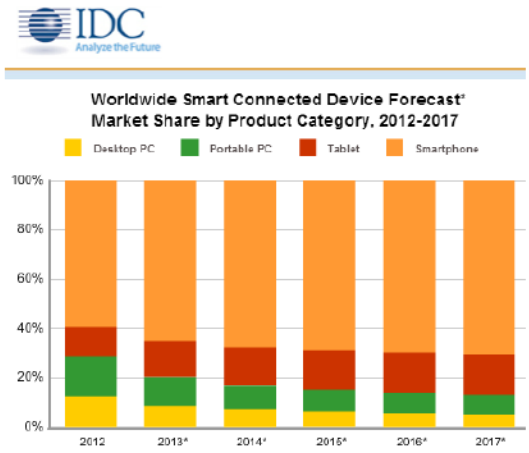

Imagen 1: Pronóstico de ventas con marcado

Muchos de los logros sobre esta red suelen verse empañados por vulnerabilidades que permiten el robo de información que maliciosamente suelen cometerse sobre datos, equipos, etc.

Los Smartphone generalmente poseen tecnología Bluetooth, cuya tecnología cobró protagonismo con una sofisticada ciberarma llamada Flame, descubierta por Kaspersky[2]. Una de sus funciones era

1 http://www.forbes.com/sites/louiscolumbus/2013/09/12/idc-87-of-connected-devices-by-2017-will-be-tablets-and-smartphones/

2 http://www.Kaspersky.com/about/news/virus/20

robar, desde una computadora, información de celulares que pasaban dentro de su rango de cobertura.

El crecimiento de ciberarmas está propiciando en distintos países ciberataques a infraestructuras críticas.

Por ello es necesario que nuestro país tenga la capacidad de desarrollar ciberamas que permitan contrarrestar este flagelo.

Palabras clave: Ciberdefensa, Seguridad Informática, Guerra Electrónica

Contexto

El proyecto está enmarcado en el Proyecto de Investigación de Ingeniería de Software, Conceptos, Métodos y Herramientas en un contexto de "Ingeniería de Software en Evolución" Facultad de Ciencias Físico-Matemáticas y Naturales, Universidad Nacional de San Luis."

Introducción

Después de cada nuevo lanzamiento tecnológico, son frecuentes las noticias que informan sobre vulnerabilidades detectadas en esos dispositivos que son aprovechados por la creciente ola de delincuencia informática.

Se puede observar también, la continua batalla que parece no tener fin donde por cada corrección de la vulnerabilidad encontrada, nuevas formas y métodos son llevados a cabo promoviendo nuevos agujeros de seguridad. Estas idas y vueltas, también se dan en muchas tecnologías, como por ejemplo en el caso del Bluetooth.

La gran demanda en adquisición de celulares (Smartphone), el bajo costo del acceso a internet, el creciente uso de la tecnología Bluetooth y la poca información sobre vulnerabilidades en equipos móviles, etc., convierten a las personas que usan esta tecnología en blancos potenciales del robo de información.

Los que llevan a cabo estos ilícitos no tienen en cuenta nivel social, cultural, etc., pudiendo encontrar víctimas en cualquier estrato social.

Una mayor conectividad a Internet aumenta el riesgo de ataques informáticos.

Los atacantes suelen encontrar vulnerabilidades que aprovechan para llevar a cabo sus ciberataques, los cuales suelen tener como destino, no solo personas, sino infraestructuras críticas de países o naciones.

Los ataques se van tornado en complejas armas cibernéticas como lo son Flame o uno de los más recientes malware descubiertos llamado Regin[3]. Estas ciberarmas, utilizadas para ciberataques utilizan Servidores de Comando y Control que llevan a cabo los ataques.

Mediante la detección de ataques que puede ser usando "Análisis de flujos de redes para detectar patrones de comportamientos compatibles con ciberataques[4]" sería posible saber

12/Kaspersky_Lab_Experts_Provide_In_Depth_Analysis_of_Flames_Infrastructure

[3] http://www.symantec.com/connect/blogs/regin-una-herramienta-de-ciberespionaje-que-permite-vigilar-sigilosamente?fb_ref=Default&fb_source=message

[4] Trabajo de la maestría en Ingeniería del Software. Lic. Claudio Baieli, Dr. Uzal, Dr. Berón, Dr.Montejano, Dr. Riesco (UNSL, San Luis, Argentina), Dr.Cunha (UFMG, Brasil)

inclusive la procedencia de la ciberagresión. Conocer el origen del ataque justificaría neutralizar el Servidor de Comando y Control de ese ataque, el que no solo protegería la infraestructura atacada sino que estaría enmarcado en el uso de legítima defensa pronunciado en el artículo 61 de Naciones Unidas.

Existen numerosos antecedentes a sobre ciberagresiones tales como: a) Rusia contra Estonia, b) el Banco Nacional de Giorgia hacheado por Rusia, c) Voladura de Planta de uranio en Irán, d) distintos casos de espionaje implicando el robo de secretos tecnológicos de China a Estados Unidos, entre otros.

El incremento en ciberagresiones motiva que nuestro país tenga la posibilidad de crear modelos de ciberarmas que puedan permitir la neutralización de ciberataques que pudieran estar llevándose a cabo contra nuestro país.

Se ha tomado como punto de partida e inspiración del presente trabajo suponer como Flame pudo robar información de celulares desde un equipo usando tecnología Bluetooth.

Encontrar y reproducir vulnerabilidades de la época ha servido para dar los primeros pasos en la gestación de las primeras armas cibernéticas que permitan el objetivo que se persigue.

Tal como lo sugirió el director[5] de este proyecto, es necesario ver a Flame como un bus donde el uso de la tecnología Bluetooth es tan solo uno de los componentes de mismo. Es necesario reproducir el resto de los componentes de ese bus tales como los módulos de autodestrucción, propagación, etc. Esto dará una idea más precisa del camino a recorrer para entender lo que se precisa para la generación de módulos de ciberdefensa.

Se debe tener presente que esta área de investigación no tiene precedentes o referencias bibliográficas concretas debido a que son líneas de investigación que países desarrollados utilizan en polos militares y cuyos logros son guardados en el secreto absoluto.

La línea de trabajo que se ha investigado no es inédita, ni tampoco una imitación, es algo que ha permitido dejar los primeros pasos teóricos y prácticos necesarios para la construcción de un modelo de ciberarma que permita neutralizar posibles ataques cibernéticos a nuestra infraestructura.

Líneas de Investigación, Desarrollo e Innovación

El lineamiento principal de la investigación tiene que ver con el desarrollo de capacidades de ciberdefensa y seguridad cibernética.

Trabajar con la tecnología Bluetooth y sus vulnerabilidades ha permitido entender las capacidades del funcionamiento y comportamiento de herramientas que aprovechan debilidades del protocolo de la pila Bluetooth.

Analizar vulnerabilidades y su impacto dentro de la pila de protocolo Bluetooth es una técnica que permitió identificar, clasificar y entender aspectos de ciberataques.

Resultados y Objetivos

Se ha logrado replicar el ambiente de trabajo de un ciberataque utilizando la tecnología Bluetooth de dos dispositivos previamente emparejados.

[5] Dr. Roberto Uzal. Director del Doctorado en Ingeniería Informática (UNSL) y Director de la Maestría en Ingeniería Informática (UNSL)

Mediante una herramienta que aprovecha una vulnerabilidad presente en Bluetooth a través del protocolo OBEX, cuya función es la transferencia de datos entre dos dispositivos previamente emparejados, se logró robar información a un celular Smartphone desde una notebook sin el consentimiento de la víctima. También se pudo transferir información hacia el celular sin que la víctima se diera cuenta.

Los pasos futuros serán trabajar modularmente para intentar replicar todo el bus del virus Flame.

Formación de Recursos Humanos

La estructura del equipo de trabajo está compuesta por Lic. Walter Fabián Agüero, Director Dr. Roberto Uzal (UNSL), y los co-autores Dr. Daniel Macedo (UFMG, Brasil), Dr. Germán Montejano (UNSL) y Dr. Daniel Riesco (UNSL).

La etapa investigativa se ha llevado a cabo en el marco de la Maestría en Ingeniería del Software que se dicta en la Universidad Nacional de San Luis (UNSL) y se relaciona directamente con la línea de I/D/I presentada.

Referencias

1. Specification of the Bluetooth system, v.1.2.Core specification, available from http://www.Bluetooth.org
2. Scott R. Fluhrer and Stefan Lucks. Analysis of the E0 encryption system. In Proc. 8th Workshop on Selected Areas in Cryptography, LNCS 2259. Springer-Verlag, 2001.
3. Scott R. Fluhrer. Improved key recovery of level 1 of the Bluetooth encryption system.
4. Cryptology ePrint Archive, report 2002/068,
5. available from http://eprint.iacr.org/ 2002/068/ , 2002. / 2014
6. Miia Hermelin and Kaisa Nyberg. Correlation properties of the Bluetooth combiner generator. In Information Security and Cryptology, LNCS 1787, pages 17.29. Springer-Verlag, 1999.
7. Markus Jakobsson and Susanne Wetzel. Security weaknesses in Bluetooth. In Proc. RSA Security Conf. – Cryptographer's Track, LNCS 2020, pages 176.191. Springer-Verlag, 2001.
8. Matthias Krause. BDD-based cryptanalysis of keystream generators. In L. Knudsen, editor, Advances
9. in Cryptology – EUROCRYPT'02, LNCS 1462, pages 222.237. Springer-Verlag, 2002.
10. Y. Lu and S. Vaudenay. Faster correlation attack on Bluetooth keystream generator E0. In Advances in
11. Cryptology – CRYPTO'04, LNCS 3152, pages 407. 425. Springer-Verlag, 2004.

12. Ophir Levy and Avishai Wool. A uniform framework for cryptanalysis of the Bluetooth E0 cipher. Cryptology ePrint Archive, Report 2005/107, 2005. http://eprint.iacr.org/2005/107
13. J. L. Massey, G. H. Khachatrian, and M. K. Kuregian. SAFER+. In Proc. First Advanced Encryption Standard Candidate Conference. National Institute of Standards and Technology (NIST), 1998.
14. Informe de la Ontsi (España, página 50) Observatorio Nac.de las Telecomunicaciones y de la SI. España. http://www.innovaxp.com/es/blog/el-auge-de-las-aplicaciones-movil-y-la-necesidad-de-estar-siempre-conectado/
15. Ciberespacio: http://www.ecured.cu/index.php/Ciberespacio
16. http://eprints.gla.ac.uk/78067/1/78067.pdf "El Problema de la Atribución Geiss & Lahmann, 2013.
17. http://43jaiio.sadio.org.ar/proceedings/SIE/16-SIE704.pdf
18. http://es.wikipedia.org/wiki/Defense_Advanced_Research_Projects_Agency
19. http://www.forbes.com/sites/louiscolumbus/2013/09/12/idc-87-of-connected-devices-by-2017-will-be-tablets-and-smartphones/
20. http://www.computerworld.com/article/2503859/desktop-apps/flame-s-Bluetooth-functionality-could-help-spies-extract-data-locally--researchers-say.html
21. http://arstechnica.com/security/2012/06/spy-softwares-Bluetooth-capabilty-allowed-stalk-of-iranian-victims/
22. http://www.crysys.hu/targeted-attacks.html
23. http://securelist.com/blog/incidents/34216/full-analysis-of-flames-command-control-servers-27/
24. http://www.engadget.com/2012/06/11/flame-malware-extinguishes-itself-microsoft-protects-against-fu/
25. http://www.bluetooth.com/Pages/what-is-bluetooth-technology.aspx
26. http://bibdigital.epn.edu.ec/bitstream/15000/55/1/CD-0024.pdf - http://es.wikipedia.org/wiki/Bluetooth
27. http://www.ericssonhistory.com/changing-the-world/Anecdotes/The-history-of-Bluetooth-/
28. http://www.intelfreepress.com/news/the-man-who-named-bluetooth/4078/ Por la unificación de compañías telefónicas (Nokia, Ericcson) con informáticas (Intel, Toshiba, IBM)
29. http://www.grc.upv.es/Software/bluefriend/BlueFriend%20Memoria25.pdf

30. Tecnologías Wireless y Movilidad en IPv4/IPv6XVII. Universidad Nacional de La Plata. Página 181

31. Universidad Politécnica de Cataluña. España. Bluetooth v4.0: la futura solución inalámbrica de bajo consumo página 4). http://upcommons.upc.edu/pfc/bitstream/2099.1/13249/1/memoria.pdf

32. http://www.ieee802.org/15/pub/TG1.html

33. Washington Univerversity (Dep.Computer Science and Engineering) http://www.cse.wustl.edu/~jain/cse574-06/ftp/wpans/index.html (apartado resumen, figura 6)

34. Unión Internacional de Telecomunicaciones http://www.itu.int/en/ITU-R/study-groups/workshops/RWP1B-SRD-UWB-14/Presentations/International,%20regional%20and%20national%20regulation%20of%20SRDs.pdf

35. Universidad Politécnica de Cataluña. España. Bluetooth v4.0: la futura solución inalámbrica de bajo consumo página 8). http://upcommons.upc.edu/pfc/bitstream/2099.1/13249/1/memoria.pdf

36. Universitat Politécnica de Catalunya. Escola d´Enginyeria de Telecomunicació i Aeroespacial de Castelldefels. Bluetooth v4.0: la futura solució inalámbrica de baix consum. Ricard Morales Pedro. Página 14.

37. Tecnologías Wireless y Movilidad en IPv4/IPv6. XV Escuela Internacional de Informática. UN La Plata. Luis Marrone | Andrés Barbieri | Matías Robles. (pág. 191)

38. Guide to Bluetooth Security. National Institute of Standards and Technology. Departamento. de Comercio USA (pág.14)

39. http://es.wikipedia.org/wiki/Espectro_ensanchado_por_salto_de_frecuencia

40. http://rose.eu.org/2012/wp-content/uploads/2012/03/Wireless-communication.pdf (pág. 12)

41. http://es.wikipedia.org/wiki/Modulaci%C3%B3n_por_desplazamiento_de_frecuencia

42. Escuela Politécnica Nacional. Estudio del estándar IEEE 802.15.4 Zigbee para comunicaciones inalámbricas de área personal de bajo consumo de energía y su comparación con el estándar IEEE 802.15.1 Bluetooth (pag. 65)

43. Johnson Consulting. http://www.swedetrack.com/images/bluet12.htm

44. Madrid, España. Universidad Pontificia Comillas. Esc.Técnica Superior de Ingeniería. Ing.Informática Estudio de análisis y rendimiento Bluetooth, página 16

45. Versión 4.2: https://www.bluetooth.org/en-us/Documents/Bluetooth4-2QuickRefGuide.pdf

46. Universidad de Lleida. José García Pique, Ignacio Lozano Almazan y Daniel Sanchez Garcia.

http://web.udl.es/usuaris/carlesm/docencia/xc1/Treballs/Bluetooth.Treball.pdf

47. Universidad de Lleida. Jose Garcia Pique, Ignacio Lozano Almazan y Daniel Sanchez Garcia. http://web.udl.es/usuaris/carlesm/docencia/xc1/Treballs/Bluetooth.Treball.pdf

48. Definición de Endian: http://es.wikipedia.org/wiki/Endianness

49. Tecnologías Wireless y Movilidad en IPv4/IPv6. XV Escuela Internacional de Informática. UN La Plata. Luis Marrone | Andrés Barbieri | Matías Robles. (pág. 191)

50. Universidad de las Américas, Puebla. México. (página 7). http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/archundia_p_fm/capitulo3.pdf

51. BlueFriend: Red Social Basada en Tecnología Bluetooth. Universidad Politécnica de Madrid. Pág.15

52. Universidad Politécnica de Cataluña. España. Bluetooth v4.0: la futura solución inalámbrica de bajo consumo página 18). http://upcommons.upc.edu/pfc/bitstream/2099.1/13249/1/memoria.pdf

53. Guide to bluetooth Security. National Institute of Standards and Technology – US Department of Commerce

Perfiles bluetooth https://developer.bluetooth.org/TechnologyOverview/Pages/Profiles.aspx

54. Universidad de Tel Aviv . Israel. http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/

55. Bluetooth Security Attacks. Comparative Analysis, Attacks, and Countermeasures. Springer Briefs in computer Science. 2013. Capítulo 2, página 3

56. Bluetooth Security . Department of Computer Science and Engineering. Helsinki University of Technology. Página 10 (http://www.yuuhaw.com/bluesec.pdf)

57. Security Threats and Countermeasures in Bluetooth-Enabled Systems. Department of Computer Science University of Kuopio. Página 37 (http://epublications.uef.fi/pub/urn_isbn_978-951-27-0111-7/urn_isbn_978-951-27-0111-7.pdf)

58. http://es.wikibooks.org/wiki/Seguridad_inform%C3%A1tica/Vulnerabilidad