RESUMEN ANALÍTICO EN EDUCACIÓN - RAE -	UNIVERSIDAD CATÓLICA de Colombia Vigilada Mineducación RIUCaC

FACULTAD DE INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C.

LICENCIA CREATIVE COMMONS:

Atribución		Atribución no comercial	X	Atribución no comercial sin derivadas	
Atribución no comercial compartir igual		Atribución sin derivadas		Atribución compartir igual	

AÑO DE ELABORACIÓN: 2020

TÍTULO: Seguridad de la Información en Dispositivos Smartwatch

AUTOR (ES):Escobar Corredor, Gina Julieth y Hernández Velásquez, Laura Paola

DIRECTOR(ES)/ASESOR(ES):

Osorio Reina, Diego

MODALIDAD:

Trabajo de investigación

PÁGINAS:	48	TABLAS:	6	CUADROS:	0	FIGURAS:	14	ANEXOS:	0

CONTENIDO

RESUMEN ANALÍTICO EN EDUCACIÓN - RAE -	UNIVERSIDAD CATÓLICA de Colombia Vigilada Mineducación RIUCaC

DESCRIPCIÓN:

La tecnología IoT con el paso del tiempo ha impactado al mundo positivamente, Los Smarwhatch han sido diseñados para permanecer en interacción con el usuario teniendo en un solo dispositivos todas las funcionalidades necesarias para permanecer conectados y actualizados, es por esto que conocer las caracteristas de seguridad que ofrecen y contar con una serie de recomendaciones para su adquisición y uso es cada vez más necesario.

METODOLOGÍA:

Para el desarrollo del proyecto se contemplaron 4 fases, principalmente, el levantamiento de información, seguido del análisis documental, la ejecución de las pruebas técnicas y del análisis de riesgos para llegar a la definición de las recomendaciones, tomando como insumo el resultado de las fases previas.

Se toma como técnicas e instrumentos el análisis documental de la información recolectada de fabricantes, proveedores, artículos, estándares de la industria, legislación y diferentes fuentes, las cuales se convierten en el insumo más importante puesto que es el camino para la definición de las recomendaciones de seguridad para los consumidores de los dispositivos SmartWatch.

Con la evaluación de riesgos y con la ejecución de diferentes pruebas tecnicas, se llegó a la definición de las recomendaciones de seguridad para el cumplimiento del objetivo.

- Revisión documental de los manuales y características de cada fabricante seleccionado para la investigación
- Análisis comparativo
- Consulta de la información de fabricantes de SmartWatch, proveedores, artículos y diferentes fuentes expuestas en internet.
- Herramientas para husmeo de tráfico

PALABRAS CLAVE:

SMARTWATCH, IOT, WEARABLE, WIFI, BLUETOOTH, SEGURIDAD, RECOMENDACIONES

CONCLUSIONES:

Es posible observar e interpretar los datos que puede recolectar el Ubertooth One y en un ambiente más desarrollado generar ataques dirigidos a cada dispositivo

A pesar de la facilidad para adquirir herramientas de husmeo de tráfico, el uso de estas como el Ubertooth One requieren de conocimientos avanzados de hacking, sistemas operativos y redes.

Los dispositivos U8 y *AONYSTAR DINA+,* son limitados en características, de difícil configuración y requieren de un software intrusivo en permisos para poder sincronizar las notificaciones de los dispositivos celulares.

La data de todos los dispositivos Apple se encuentra cifrada tanto en tránsito como en reposo de acuerdo con lo publicado en la página web del fabricante.

El resultado de la investigación deja establecida una incertidumbre en cuanto a la data transmitida por el Galaxy Watch dado que no se pudo validar a nivel documental o técnica esta característica.

La complejidad en el uso de las herramientas como el Ubertooth reduce la probabilidad de un ataque o de la visualización de los datos ya que es necesario contar un alto conocimiento técnico para lograr el objetivo.

Las pruebas deben ejecutarse en diferentes escenarios para finalmente lograr la captura de la data.

No se evidenció por parte de los fabricantes información clara respecto a los mecanismos de cifrado utilizados para la data que se transmite a través del SmartWatch y su entorno.

Dada la incertidumbre en cuanto al cifrado de los datos en tránsito y en reposo del Galaxy Watch se abre la puerta para siguientes investigaciones que partiendo de la información técnica encontrada profundicen en el esclarecimiento de este interrogante.

Al contar con la herramienta de husmeo bluetooth el presente proyecto deja la puerta abierta para que siguientes proyectos profundicen en el análisis de la

información en tránsito, la verificación de la seguridad de la información que viaja cifrada y la inyección de paquetes que planteen engaños a los dispositivos objetivo.

No es clara la información expuesta por los fabricantes en cuanto a la eliminación de información en caso de robo o pérdida del SmartWatch de forma remota.

El AppleWatch cuenta con un factor de seguridad superior en comparación con los demás SmartWatch elegidos para esta investigación, dado que es no es posible emparejarlo con otro dispositivo si este ya se encuentra vinculado con una cuenta de ICloud.

En caso de robo o pérdida del AppleWatch es posible a través de la cuenta de iCloud.com realizar el bloqueo inmediato.

El Galaxy Watch y AppleWatch se encuentran alineados y en cumplimiento con la ley 1581 de 2012 relacionada con la protección de datos personales en Colombia y sus políticas se encuentran publicadas en un sus sitios web.

Los marcas de SmartWatch U8, *AONYSTAR DINA+,* no cuentan con sitio web oficial en el que se pueda verificar el cumplimiento de las leyes colombianas.

Las funciones de ubicación de estos dispositivos deben ser tenidas en consideración para la asignación de los permisos que solicitan las diferentes aplicaciones.

La información de estos dispositivos se almacena en mayor medida en la nube, lo que hace difícil entender el gobierno que se maneja en el momento de su uso.

Cada día se ven en el mercado dispositivos con mayores recursos en capacidad de almacenamiento, recursos de memoria, y a los fabricantes líderes invirtiendo en la seguridad de la información de estos.

FUENTES:

[1] RODRIGUEZ NAVARRO, Carlos. **"**Qué se espera del IoT en los próximos años". En línea. 22 octubre de 2019 disponible en: (https://soloelectronicos.com/tag/para-que-sirve-el-iot/).

[2] ANSCOMBE, Tony. "Legislar la seguridad de los dispositivos IoT: ¿es realmente la solución?" en línea. 6 mayo de 2019. Disponible en: (https://www.welivesecurity.com/la-es/2019/05/06/legislar-seguridad-dispositivos-iot/).

[3] PORTAFOLIO, "Seguridad del IoT se convierte en megatendencia" en línea. 23 mayo de 2019. Disponible en: (https://www.portafolio.co/tendencias/seguridad-del-iot-se-convierte-en-megatendencia-529872).

[4] PUENTE GARCIA, Miriam. "Riesgos y retos de ciberseguridad y privacidad en IoT", en línea. 22 diciembre de 2017. Disponible en: (https://www.incibe-cert.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-IoT).

[5] SIGNALS IOT, "Relojes inteligentes liderarán ventas de wearables hasta 2022", en línea. 18 diciembre de 2018. Disponible en: (https://signalsIoT.com/relojes-inteligentes-lideraran-ventas-de-Wearables-hasta-2022/).

[6] Ibíd, p. 7,15. DISPOSITIVOS WEARABLES, "¿Que es Wearable? – Los dispositivos vestibles" en línea. disponible en: (http://www.dispositivosWearables.net).

[7] Ibíd, p. 7,18. COLOMBIA, CONGRESO DE LA REPUBLICA. Ley estatutaria 1581 de 2012. (octubre 17) Por la cual se dictan las disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587 de 18 de octubre de 2012

[8] CCN-CERT, "EL FBI advierte sobre dispositivos de Internet de las Cosas (IoT) comprometidos" en línea. 07 agosto de 2018. disponible en: (https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/6717-el-fbi-advierte-sobre-dispositivos-de-internet-de-las-cosas-iot-comprometidos.html).

[9] CRESPO, Adrián, "Los smartwatch son un peligro para la seguridad de los datos de los usuarios, o al menos de momento" en línea. 12 diciembre de 2014.

Disponible en: (https://www.redeszone.net/2014/12/12/los-smartwatch-son-un-peligro-para-la-seguridad-de-los-datos-de-los-usuarios-o-al-menos-de-momento/).

10 Ibíd, p. 8, 17 ENISA, “Internet de las cosas (IoT)” en línea. disponible en: (https://www.enisa.europa.eu/topics/IoT-and-smart-infrastructures/IoT).

[11] MEREDYDD Williams, Jason R.C. Nurse, CREESE Sadie. Computers in Human Behavior: Encouraging privacy-protective behavior in a longitudinal study. Volume 99, October 2019, Pages 38-54

[12] ACOSTA, Victor Manuel. “Seguridad en Smartwatch: claves para protegerlo de posibles hackers” en línea. 23 julio de 2018. Disponible en: (https://revistadigital.inesem.es/informatica-y-tics/seguridad-en-SmartWatch/).

[13] RACHARLA, Kavya, NAROPANTH Sumanth. “Securing your in-ear fitness coach: Challenges in hardening next generation wearables” en línea. agosto 2018. Disponible en: (https://i.blackhat.com/briefings/asia/2018/asia-18-naropanth-racharla-In-ear-fitness.pdf).

[14] GARCIA, Maria. “IoT - Internet Of Things” DELOITTE, en línea. disponible en: (https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html).

[15] LOPEZ, María de los ángeles, Albanese, Diana Ester, Sánchez Marisa Analía. Contaduría y Administración: Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la República Argentina. Volume 59, Issue 3, October–December 2014, Pages 61-88

[16] EBSCO. IoT Device risk assesssment. En línea. disponible en: (http://eds.b.ebscohost.com/eds/detail/detail?vid=2&sid=76aaa9e0-4008-4c8f-94b0be73c3247c21%40sessionmgr103&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZQ%3d%3d#AN=87322980&db=ers).

[17] SCIENCE DIRECT. Wireless broadband standards and technologies. Ahmadi, in Academic Press Library in Mobile and Wireless Communications, 2016. En línea. disponible en: (https://www.sciencedirect.com/topics/engineering/bluetooth/pdf)

[18] Ibíd, p. 13,16. CHOI, Jaewon, KIM Seongcheol. Computers in Human Behavior: Is the smartwatch an IT product or a fashion product? A study on factors affecting the intention to use smartwatches. Volume 63, October 2016, Pages 777-786

[19] SANMARTIN MENDOZA, Paul, AVILA HERNANDEZ Karen, VILORA NÚÑEZ, Cesar, MOLINARES JABBA, Daladier. “Internet de las cosas y la salud centrada en el hogar”. En línea. 29 de abril de 2016. Disponible en: http://www.scielo.org.co/pdf/sun/v32n2/v32n2a14.pdf

[20] PRESS, Gil. “Internet of Things by the numbers: market estimates and forecasts, en línea 22 agosto de 2014. Disponible en: (https://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/#5976d2cb9194).

[21] CASTRO, Diego, CORAL William, CABRA, José. “Survey on IoT applied to healthcare”. en línea. 12 octubre de 2017. Disponible en: https://www.redalyc.org/jatsRepo/496/49655603024/index.html

[22] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. (enero 5) por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial No. 47.223 de 5 de enero de 2009

CAICEDO, John. “Internet de las cosas y la seguridad”. En línea.16 octubre de 2017 disponible en: (https://www.johncaicedo.com.co/2017/10/16/internet-de-las-cosas-y-la-seguridad/).

CHUAH, Stephanie Hui-Wen. Telematics and Informatics: You inspire me and make my life better: Investigating a multiple sequential mediation model of smartwatch continuance intention. Volume 43, October 2019, 101245

HSIAO, Kuo-Lun, CHEN, Chia-Chen. Telematics and Informatics: What drives smartwatch purchase intention? Perspectives from hardware, software, design, and value. Volume 35, Issue 1, April 2018, Pages 103-113

HA, Taehyum, BEIJNON, Bjorn, KIM, Sangyeon, LEE, Sangwon, KIM, Jang Hyun. Telematics and Informatics: Examining user perceptions of smartwatch through dynamic topic modeling. Volume 34, Issue 7, November 2017, Pages 1262-1273

TSUNG-Chien, Lu, YAO-Ting, Chang, TE-Wei, Ho, YI, Chen, YI-Ting, Lee YU-Siang, Wang YEN-Pin, Chen, CHU-Lin, Tsai, MATTHEW, Huei-Ming, Ma, CHENG-Chung, Fang, FEIPEI, Lai HENDRIKA W., Meischke, ANNE M.Turner.

Resuscitation: Using a smartwatch with real-time feedback improves the delivery of high-quality cardiopulmonary resuscitation by healthcare professionals. Volume 140, July 2019, Pages 16-22

MATIN, Kheirkhahan, PhD, SANJAY, Nair, ANIS, Davoudi, Parisa, Rashidi, AMAL A., Wanigatunga, DUANE B., Corbett, TONATIUH, Mendoza, TODD M., Manini, SANJAY, Ranka. Journal of Biomedical Informatics: Volume 89, January 2019, Pages 29-40

MEREDYDD, Williams, JASON R.C.Nurse, SADIE, Creese. International Journal of Human-Computer Studies: (Smart)Watch Out! encouraging privacy-protective behavior through interactive games. Volume 132, December 2019, Pages 121-137

PHILIP, Menard, GREGORY J., Bott. Computers & Security: Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. Volume 95, August 2020, 101856

VINCENT, Dutot, VEERA, Bhatiasevi, NADIM, Bellallahom. The Journal of High Technology Management Research: Applying the technology acceptance model in a three-countries study of smartwatch adoption. Volume 30, Issue 1, May 2019, Pages 1-14

LIANG-Hong, Wu, LIANG-Chuan, Wu, SHOU-Chi, Chang. Computers in Human Behavior: Exploring consumers' intention to accept smartwatch. Volume 64, November 2016, Pages 383-392

Sangeun, Jin, Minsung, Kim, Jihyeon, Park, Minsung, Jang, Kyuseok, Chang, Daemin,Kim. Applied Ergonomics: A comparison of biomechanical workload between smartphone and smartwatch while sitting and standing. Volume 76, April 2019, Pages 105-112

LEE, HC, LEE DM, Conferencia Internacional 2020 sobre inteligencia Artificial en Información y Comunicación, ICAIIC 2020: Modelo de aprendizaje automático para algoritmos de localización en interiores con GPS y reloj inteligente. Artículo 9065245, Febrero de 2020 Páginas 735-737

SAMSUNG ELECTRONICS COLOMBIA S.A. "Política De Tratamiento De Datos Personales" En línea. 25 Junio de 2013 disponible en: (https://www.samsung.com/co/proteccion_de_datos/).

APPLE Inc, “Política de Privacidad” En línea. 31 Diciembre de 2019 disponible en: (https://www.apple.com/legal/privacy/es/).

APPLE Inc. “Información general sobre la seguridad de iCloud” En línea. 17 Abril de 2020 disponible en: (https://support.apple.com/es-es/HT202303).

ENISA, “Sobre ENISA” En línea. disponible en: (https://www.enisa.europa.eu/about-enisa)