Published on *LET* (http://let.iiec.unam.mx)

Why everything is hackable. Computer security is broken from top to bottom. As the consequences pile up, things are starting to improve

Enviado por Josue Garcìa Veigaen Vie, 06/02/2017 - 11:21
Cita:

The Economist [2017], "Why everything is hackable. Computer security is broken from top to bottom. As the consequences pile up, things are starting to improve", *The Economist*, London, 8 de abril, http://www.economist.com/news/science-and-technology/21720268-consequenc... [1]

Fuente:
The Economist
Fecha de publicación:
Sábado, Abril 8, 2017
Revista descriptores:
Estudios de caso: actividades - empresas [2]
Formas de la competencia entre grandes empresas [3]
Relaciones entre empresas estados y sociedad [4]
Tema:
Los costos de la seguridad informática
Idea principal:

En el mundo cibernético existe gran cantidad de hackers: los hay quienes se dedican a encontrar vulnerabilidades del sistema con el fin de implementar mejoras para el fin común, pero también existen aquellos que violentan el sistema con intenciones de extorsionar, robar y beneficiarse mediante acciones ilegales y criminales.

El artículo señala que este último tipo de pirateo cibernético está creciendo fácil y rápidamente en mercados altamente desarrollados y sofisticados que no requieren ya de expertos en el lenguaje de código. Lugares informáticos donde se comercializan datos de tarjetas de crédito robadas, las fallas en el código de distintos softwares para ser explotadas, traficantes de “ransomware”* y el uso de "botnents"** para saturar sitios en-línea exigiendo dinero a cambio de su liberación.

De acuerdo con la revista el costo total de esta red de pirateo informático ha ocasionado una gran cantidad de pequeños ataques y algunos grandes. Además se advierte que esto podría crecer al expandirse el margen de acción del hackeo con las nuevas innovaciones tecnológicas en puerta –Internet de las Cosas (IoT, por sus siglas en inglés).

Computadora, no está bien

Desde las bases de la tecnología informática, en la cultura del desarrollo de software, en el

crecimiento veloz de los negocios en línea, en los incentivos económicos de las empresas informáticas y los intereses estatales. Los nuevos y mayores daños ocasionados por la inseguridad informática están generando una mayor intervención desde las compañías privadas, los gobiernos y centros de investigación.

Los riesgos que asume el proceso de su fabricación son muchos, cualquier ligero error en alguna etapa o transición de una a la otra –diseño, manufactura, ensamblado de chips o de los sistemas operativos – puede resultar en un sistema completamente defectuoso o vulnerable a un ataque (*Dato Crucial 5*). Las empresas manejan grandes cantidades de códigos informáticos en sus productos (programas, chips, dispositivos) y lograr que interactúen adecuadamente con el resto no es tarea fácil. Los errores en las líneas de código abren la posibilidad de miles de virus en un programa (*Dato Crucial 7*). Un error podría significar resultados imprevistos.

Al existir distintas vías para que la computadora procese datos (información) como instrucciones –ambas son representadas al interior de la máquina en la misma forma: como secuela de dígitos–; sí los datos “desbordan” alguna parte del sistema ubicada en la memoria trasladándose a la parte donde la máquina espera instrucciones, los datos serán procesados como conjunto de nuevas instrucciones. Esto abre una gran vulnerabilidad posibilitando que los programas sean saturados intencionalmente.

Eliminar cualquier riesgo de abuso y/o alteración en las millones de líneas de códigos antes de que los usuarios hagan uso de ellos, es casi imposible. Se han encontrado vulnerabilidades hasta en los sistemas de armas del Departamento de Defensa de Estados Unidos(*Dato Crucial 8*).

Karma policiaco

La historia de la seguridad informática está relacionada estrechamente con los intereses de espionaje y seguridad nacional entre estados. Por ende ha sido tema recurrente trabajar en el desarrollo de una capa de software adicional para mantener los detalles de confidencialidad bajo resguardo. A pesar de ello cada año nuevas vulnerabilidades y debilidades son reportadas en esta capa de protección.

La inocencia e ignorancia de muchos usuarios sigue siendo motivo de preocupación. Desarrollar prácticas de seguridad tanto en los programadores, empresas y usuarios toma bastante tiempo. Esto preocupa el actual desarrollo del IoT.

Otro motivo, y quizá el más fuerte, de inseguridad son los incentivos económicos en los negocios de la informática. Para los programadores de software el desarrollar códigos de seguridad implica gastar tiempo y recursos, y ello a su vez implica mayores costos y no está añadiendo nuevos consumidores y por ende tampoco ganancias. Incluso la falta de una jurisdicción adecuada que obligue a las empresas a comprometerse legalmente con los servicios ofrecidos en sus programas permiten que la industria informática sea capaz de innovar productos a gran velocidad. Lo cual implica trasladar grandes costos a los consumidores.

Por su parte la postura de los gobiernos es ambivalente. En ocasiones están a favor de una mejor seguridad informática que resguarde la información privada de los ciudadanos tanto de sus propias operaciones. Pero por otra parte, las computadoras son herramientas de vigilancia y espionaje civil del cual pueden hacer uso los gobiernos.

Androide cada vez más paranoico

El riesgo es que las debilidades pueden ser aprovechadas por cualquiera. Algunas empresas y gobiernos están tratando de resolver de manera conjunta los problemas de seguridad con distintas acciones: recompensando la caza e identificación de fallas en los programas, la insistencia de actualizar los programas con sus últimas versiones (como lo hace Microsoft), desarrollo de protocolos de codificación reescribiendo desde arriba hasta abajo el código que conserva información privada (como Google y Amazon), plataformas de fuente abierta que le permita libre acceso al público, y sugerir mejoras, entre otras.

El Departamento de Defensa de Estados Unidos mediante su división de Agencia de Proyectos de Investigación Avanzados de Defensa (DARRPA, por sus siglas en inglés) financia proyectos para desarrollar innovaciones en el tema de seguridad. Un ejemplo es CHERI, un nuevo tipo de chip que busca fortalecer la seguridad en el hardware, garantizando que los datos (información) no puedan ser confundidos con las instrucciones. También permite que los programas individuales operen dentro de procesos aislados (sandboxes***) más seguros, limitando su habilidad para afectar otras partes de la máquina (o dispositivo). La idea es que estos chips sean agregados fácilmente a aquellos diseñados por ARM e Intel que se utilizan en teléfonos y laptops. El aislamiento de procesos actualmente ya se encuentra en uso por distintos sistemas operativos, buscadores en-línea y otros. Pero escribir procesos de aislamiento en programas enlentece el rendimiento. Otro proyecto de ARPA se centra en técnicas llamadas “métodos formales”, estos convierten los programas informáticos a enunciados gigantescos de lógica formal. Teoremas matemáticos que pueden ser aplicados para analizar y hacer pruebas con el comportamiento de los programas.

También el mercado de los seguros está cambiando. Las grandes empresas están recurriendo a los seguros informáticos (*Dato Crucial 9 y 10*). Este incremento en la demanda de seguros cibernéticos podría estimular una mayor innovación en programas más seguros.

Para la revista el futuro definirá nuevas responsabilidades a los productores de programas informáticos, en un mundo donde la computarización de todas las cosas es creciente y el riesgo asumido podría generar mayores daños. Lo cual no será tarea fácil. Sin duda habrá resistencia a mayores responsabilidades que impliquen mayores costos.

---

* Ransomware o bien “softwares de rescate” son programas utilizados para bloquear el acceso a determinados archivos del sistema infectado, con el fin de pedir un pago a cambio de retirar la restricción (https://es.wikipedia.org/wiki/Ransomware [5])

** Botnents: literalmente son “redes de máquinas infectadas” que son usadas para atacar a terceros, por ejemplo saturar sitios en-linea generando mucho tráfico, obligándolos a pagar un

rescate (https://mx.norton.com/botnet [6])

**Sandboxes: literalmente se traduce como “cajas de arena” pero en seguridad informática se le conoce como el mecanismo de aislamiento de procesos para ejecutar programas de manera aislada y más segura (https://es.wikipedia.org/wiki/Aislamiento_de_procesos_ [7] (inform%C3%A1tica)).

Datos cruciales:

1. En febrero de 2016 ciberdelincuentes robaron 81 millones dólares directamente del Banco Central de Bangladesh.

2. En agosto de 2016 la propia Agencia de Seguridad Nacional de Estados Unidos vio sus propias herramientas de hacking filtradas por todo el Internet ocasionado por un grupo autodenominado Shadow Brokers.

3. En octubre (2016) una pieza de un software llamado Mirai fue utilizado para inundar Dyn, una compañía de infraestructura en Internet, haciendo inaccesibles muchos sitios de Internet (como Twitter y Reddit).

4. Se hackeó el servicio de correos del Comité Democrático Nacional de Estados Unidos y la subsiguiente fuga de comunicaciones vergonzosas pudo haber sido parte de un intento para influir en el resultado de las elecciones presidenciales estadounidenses.

5. En 2011 se descubrió un defecto de manufactura en algunos de los transistores componentes de chips de ciertos helicópteros navales de Estados Unidos.

6. En 2015 Google reportó más de 2 mil millones de líneas de código en varios de sus productos, Linux 20.3 millones, Windows con 50 millones.

7. Una estimación calcula que los programadores de código informático realizan entre 10 y 50 errores en cada 1,000 líneas de código (Steve McConnell).

8. En 2015 una firma de seguridad privada encontró 14 vulnerabilidades en la aplicación promedio para celular (Trustwave).

9. El mercado de seguros cibernéticos está valuado alrededor de 3 y 4 miles de millones de dólares anuales. Y está creciendo 60% cada año (SentinelOne).

10. Un tercio de los negocios estadounidenses tienen servicios de seguros cibernéticos con cobertura de algún tipo, aunque sea por tiempo limitado (PwC, 2015).

Nexo con el tema que estudiamos:

Debilitar la seguridad privada puede incrementar el control no solo de los gobiernos sobre los usuarios sino también de las corporaciones o de quien acceda a esta información. Por otro lado, los tres mercados existentes en su estado actual generan ganancias: el desarrollo de software, el mercado ilegal y el mercado de seguridad. ¿Por ende quién está interesado en generar mayor seguridad? Una mayor seguridad informática debería generar más ingresos que los que

antes mencionados, o en su defecto, ¿quién asumirá la inversión de tiempo y recursos el consumidor, el fabricante o el gobierno? Por otra parte, también habría que introducir en este razonamiento los intereses de los usuarios, que no siempre son mercantilizables.

Bien es señalado por la revista: los intereses sociales podrían cambiar al ver que las consecuencias de los virus o hackers puedan traer mayores costos, ya no solo monetarios sino también en pérdidas humanas, u otras cuestiones.

Otras fichas sobre el tema de seguridad informática:
Safety last. How to manage the computer-security threat. The incentives for software firms to take security seriously are too weak [8]
Terror and the internet. Tech firms could do more to help stop the jihadists. [9]

Links
[1] http://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security
[2] http://let.iiec.unam.mx/taxonomy/term/16
[3] http://let.iiec.unam.mx/taxonomy/term/17
[4] http://let.iiec.unam.mx/taxonomy/term/20
[5] https://es.wikipedia.org/wiki/Ransomware
[6] https://mx.norton.com/botnet
[7] https://es.wikipedia.org/wiki/Aislamiento_de_procesos_
[8] http://let.iiec.unam.mx/node/1381
[9] http://let.iiec.unam.mx/node/1401