



La propagación de errores

Hace poco tiempo hablamos¹ de la conocida **Digital Milenium Act** americana pero no tratamos su infiltración en la administración europea desde el mes de mayo del año pasado en forma de borrador del Consejo de Europa². Ya vimos que el DMA es la última y poco imaginativa propuesta de la industria americana para negar cualquier tipo de publicidad y apoyo a la investigación y al análisis de los productos que lanzan al mercado y constituyen su fuente de riqueza.

La EUCD fue aprobada por el Parlamento Europeo el 22 de mayo de 2001 por lo que los gobiernos nacionales tienen hasta el 22 de diciembre de este año para incluir esta directiva en sus legislaciones nacionales suponiendo, claro está, que ningún país se niegue a ello. Lo más importante de esta directiva es su artículo siete en el que se prohíbe³, de forma universal, todo aquello que directa o indirectamente pueda terminar atentando contra los derechos de autor.

En su artículo sexto⁴, la EUCD convierte en ilegal cualquier procedimiento que pueda llevar a evitar medidas técnicas de protección, y ello sin tener en cuenta cómo consiga esa persona evitar dicha protección; por ejemplo, modificando activamente el sistema (atacándolo) o simplemente utilizando un fallo del mismo. Según esto, hacer una copia de uno de tus CDs para escucharlo en tu reproductor portátil de mp3 mientras vas de viaje en el coche es tan ilegal como poner esos regis-

El plazo para transcribir a los ordenamientos legislativos nacionales de la directiva del Parlamento Europeo de 22 de mayo de 2001 sobre la armonización de ciertos aspectos del *copyright* en la sociedad de la información, se está terminando. Esta versión europea del *Digital Millennium Act* americano trae asociada una amplia serie de limitaciones y censuras que pueden dañar seriamente la evolución de la Sociedad de la Información europea desde el punto de vista de los usuarios finales. Recientes incidentes con el protocolo SNMP ponen de manifiesto lo ineficiente de ese tipo de planteamientos para conseguir redes y sistemas informáticos mínimamente seguros e invitan a su abandono en aras de otras soluciones mas imaginativas.

tros a disposición de todo el mundo en sistemas tipo Naps-ter y, por supuesto, convierte en ilegal encontrar cualquier fallo en sistemas de seguridad de cualquier índole.

las recojan las compañías tecnológicas, nada europeas, que desarrollen los procedimientos técnicos de seguridad aplicados a los materiales sujetos a protección.

caso de dar con algo que las ponga en jaque, no se puede proceder a su difusión ya que con ello uno abandona definitivamente la legalidad.

SNMP

Afortunadamente no ha sido necesario esperar mucho tiempo para ver qué efectos reales tienen estas medidas intimidatorias, que tanto gustan a las compañías discográficas, sobre las actividades de la investigación en seguridad informática.

El SNMP es un protocolo para la gestión de los equipos que constituyen las redes y que se encarga de controlar y configurar *routers*, *switches* y demás elementos propios de las redes telemáticas. Miles de tales equipos constituyen el sistema circulatorio y la materia tangible de la actual sociedad de la información y la telemática.

El otoño pasado varios investigadores de la universidad de Oulu en Finlandia⁵ descubrieron múltiples debilidades⁶ en la implementación

Si se mantienen en secreto los errores de programación, algunas empresas afectadas, aún sabiéndolo, no se molestarán en corregir sus sistemas o productos ya que eso perjudicaría a los beneficios y porque confían ingenuamente en que la no publicidad del fallo va a impedir su utilización.

Siguiendo estas férreas limitaciones, siempre habrá que acceder a los materiales digitales a través del software y hardware proporcionados por el propietario comercial del objeto en cuestión, lo que siempre supondrá un clientelismo forzado. El mencionado artículo sexto de la EUCD pone toda la esencia de la protección de la propiedad intelectual en el software o hardware que la proteja.

Aceptando este artículo, los países de la Unión Europea se desentienden de legislar sobre el *copyright*, abandonando sus funciones para que

En este escenario, las investigaciones sobre la seguridad de los sistemas deben estar muy controladas y, en el

- 1 Jorge Dávila: ¿A la seguridad a través de la ignorancia? Revista SIC N°48* Febrero de 2002 pp. 66
- 2 301L0029 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of certain aspects of copyright and related rights in the information society. Official Journal L 167 , 22/06/2001 P. 0010 - 0019
- 3 Artículo 7: "Obligations concerning rights-management information" (RMI).
- 4 Chapter III - Protection of Technological Measures and Rights-Management Information: Article 6 - Obligations as to technological measures.
- 5 OUSPG = Oulu University Secure Programming Group <http://www.ee.oulu.fi/research/ouspg/>
- 6 CERT® Advisory CA-2002-03 "Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)" February 12, 2002 Last rev: May 16 2002

del SNMP que está presente en numerosos productos comerciales. Dichas debilidades permiten montar ataques por denegación de servicio (DoS) con sólo enviar a los enrutadores un solo paquete IP y, en algunos casos, permiten saltarse las listas de control de acceso y hacerse con el control total del equipo.

En aquel momento muchas compañías no tenían idea de si estaban afectadas por ese descubrimiento por lo que se incluyó un código de demostración⁷ para probar sus productos respecto a dicha debilidad⁸ y estuvo disponible en Internet. Desde el primer momento se mantuvo el sigilo que exigen leyes como la EUCD para dar tiempo a las casas comerciales para reparar sus distribuciones.

Las vulnerabilidades estaban en los procedimientos para la captura de mensajes de error y la llamada a funciones en el código⁹, y tienen su origen en errores cometidos en el código que debe tratar las estructuras escritas en ASN.1¹⁰ o en BER¹¹.

El código defectuoso encontrado en el caso del SNMP es tan básico que puede afectar a otros productos que nada tienen que ver con él. El problema con el tratamiento del ASN.1 puede afectar a muchas otras aplicaciones (¿OpenSSL¹²?) ya que no se limita al SNMPv1, que sólo es su manifestación pública mejor descrita.

El grupo de investigación de la Universidad de Oulu des-

cribió este problema en octubre de 2001, y decidió no publicarlo debido a que se trataba de un problema serio y extenso. El CERT asumió la coordinación de los diferentes afectados para resolver este incidente, y retrasó la publicación del *bug* hasta el 12 de febrero de este año, debido al amplio grupo de empresas con las que tenían que contactar. El CERT decla-

Es cierto que, si se dan las condiciones para que se realicen ataques y está disponible tal información, tarde o temprano será utilizada para tal fin.

ra que ha tenido problemas con algunas compañías que no se han tomado en serio el problema.

Aún siguiendo el mas puro estilo DMA, la publicación se adelantó en dos semanas respecto a lo previsto debido a las numerosas fugas de información que estaban dando lugar a un gran número de imprecisos y peligrosos rumores. Algunas compañías no tenían resuelto el problema en esa fecha aunque habían tenido varios meses para hacerlo, otras sólo se preocuparon del tema cuando se les informó de que iba a hacerse público.

A pesar de haberse distribuido, en contra del espíritu de las EUCD, un código demostrador de la vulnerabilidad detectada, no parece que haya sido utilizado para perpetrar ningún ataque; por el contra-

rio, la existencia de ese código y de una plena información sobre el problema del que se trata, ha permitido a muchas compañías tomar medidas de contención e instalarlas en sus redes o en las de sus clientes antes de poder eliminar realmente el fallo, y hacerlo todo ello en pocas horas.

Esta experiencia pone claramente de manifiesto que si se mantienen en secreto los

errores de programación, algunas empresas afectadas, aún sabiéndolo, no se molestarán en corregir sus sistemas o productos ya que eso perjudicaría a los beneficios y porque confían ingenuamente en que la no publicidad del fallo va a impedir su utilización.

Está claro que no son pocas las empresas que carecen de una adecuada ética profesional y que están dispuestas a no ver lo evidente hasta que se sienten amenazadas por la publicidad, única cosa que, al final, las mueve a corregir sus errores.

Otro asunto que queda claro en este caso es que la disponibilidad de códigos que demuestran la debilidad no implica inexorablemente la aparición de ataques basados en ese mismo código. Las razones que llevan a los atacantes a actuar no son tan sencillas e infantiles como la de hacer las cosas por el mero hecho de poder hacerlas. Sin embargo, es cierto que, si se dan las condiciones para que se realicen ataques y está disponible tal información, tarde o temprano será utilizada para tal fin.

El sigilo y la censura que imponen leyes como la DMA americana o la EUCD europea en ningún modo son soluciones para el problema que dicen afrontar. La pro-

tección de los derechos de autor no tiene rango suficiente como para que protegiendo a éstos, tengamos que renunciar al software de calidad o a la conveniente actualización y corrección de lo que cada día mas, constituye el esqueleto de la sociedad de la información en la que vivimos.

La única posibilidad de que esto realmente ocurra es que la investigación en temas de seguridad y calidad informática así como la difusión de sus resultados sea lo mas eficiente y pública posible.

Haber ocultado el expediente sobre el SNMPv1 habría sido una grave irresponsabilidad dejando abiertos flancos débiles a la espera de cualquier inoportuno ataque.

Es cierto que todavía no se ha encontrado el modo de reunir los diferentes puntos de vista y los diferentes intereses en este tema, pero el proceso se ha puesto en marcha y ya hay algunas propuestas mas conciliadoras¹³ que las planteadas por discográficas, empresas multimedia y de software.

Algún día dispondremos de una solución generalmente aceptada y que, con toda seguridad, no se basará en el oscurantismo, sigilo y censura que inspiran a muchos promotores empresariales de "guerras santas" representadas por el DMA y su traducción europea. Hasta entonces, quizá sea lo mas aconsejable no tomarse muy en serio la transcripción de la EUCD a las leyes nacionales europeas y frenar así un remedio que puede ser peor que la enfermedad. n

7 PROTOS test suite <http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/>

8 la PROTOS tool

9 Referencias CVE⁵: CAN-2002-0012 y -0013, respectivamente. de CVE = Common Vulnerabilities and Exposures en <http://cve.mitre.org/>

10 ASN.1 = Abstract Syntax Notation 1

11 BER = Basic Encoding Rules

12 Un reciente problema con el modulo mod_ssl del servidor web Apache también parece estar relacionado con el problema del ASN1.

13 Steve Christey & Chris Wysopal February 2002 "Responsible Vulnerability Disclosure Process" IETF Document <http://www.ietf.org/internet-drafts/draft-christey-wysopal-vuln-disclosure-00.txt>

JORGE DÁVILA MUÑOZ

Director

Laboratorio de Criptografía

LSIS - Facultad

de Informática - UPM

jdavila@fi.upm.es