El secretismo no implica seguridad

Traducción de Textos

Curso 2007/2008

Versión	Cambio
1.5RC	Revisión de todo el texto
1.4	Primera traducción de todo el texto
1.3	Traduciendo el décimo tercer párrafo

Autor:

Rubén Paje del Pino

i010238

Índice de contenido

1. Primer párrafo (18-XI-07)

Existe una gran confusión entre los diferentes conceptos entre secretismo y seguridad lo que habitualmente causa una ausencia de seguridad y sorprendentes discusiones políticas. El anonimato a menudo contribuye a tener una falsa sensación de seguridad

2. Segundo párrafo (parcialmente corregido el 18-XI-07)

En junio de 2004, el departamento de seguridad del interior (equivalente a nuestro ministerio del interior) de EE.UU. instó a los administradores de TI a mantener la red sin pérdidas de información secreta. La comisión federal de las comunicaciones exige a las operadoras telefónicas informes de las caídas de su servicio y quiere extender esa medida a las líneas de datos de alta velocidad y las redes inalámbricas, ya que el ministerio del interior teme que tal información pudiera dar a los ciberterroristas un "mapa de carreteras virtual" para llegar a las infraestructuras críticas.

3. Tercer párrafo (18-XI-07)

¿Es útil dar a conocer la información de las vulnerabilidades de los ordenadores y las redes, o esto precisamente ayuda a los hackers? Esta es una pregunta común, ya que el software nocivo explota las vulnerabilidades del software después de conocerse.

4. Cuarto párrafo (18-XI-07)

El comentario de que el secretismo es bueno para la seguridad es bastante ingenuo, y siempre merece la pena refutarlo. Sólo es cierto en contadas circunstancias y ciertamente no lo es con respecto a la vulnerabilidad o fiabilidad de la información. La seguridad basada sólo en el secretismo es frágil, y una vez se dan a conocer ya no hay vuelta a atrás. Intentar basar la seguridad en el secretismo es simplemente un mal planteamiento.

5. Quinto párrafo (20-XI-07)

La criptografía se basa en secretos – claves – pero observe todo el trabajo que conlleva que las claves sean efectivas, además estas claves son cortas, fáciles de transferir y de actualizar y modificar; por otro lado es el único componente secreto de un sistema de criptografía. Con los algoritmos criptográficos se crean secretos difíciles de descifrar por esto que uno de los principios más básicos de la criptografía es asumir que el algoritmo es público.

6. Sexto párrafo (20-XI-07)

Una falacia acerca del secretismo es suponer que este funciona. ¿De verdad creemos que los puntos débiles de las redes son un misterio para los piratas incapaces de descubrir estas

vulnerabilidades?

7. Séptimo párrafo (20-XI-07)

Los partidarios del secretismo ignoran el valor que tiene la transparencia en el ámbito de la seguridad. El escrutinio público es la única forma eficiente de mejorar la seguridad. Anterior a que los fallos de los programas se dieran a conocer periodicamente, las compañías de software negaban su existencia y no se molestaban de arreglarlos, amparándose en la seguridad que el secretismo les daba. Y como los consumidores no tenían grandes conocimientos, compraban estos sistemas creyendo que tales sistemas eran seguros. Si volvemos a mantener secretos los errores de las aplicaciones, tendremos que las vulnerabilidades conocidas por unos poco pertenecientes a la comunidad de la seguridad y por muchos en el mundo de los hackers.

8. Octavo párrafo (20-XI-07)

El secretismo evita que las personas evalúen sus propios riesgos. El hacer público los cortes en las redes que forzaría a las operadoras telefónicas a mejorar sus servicio, lo que permitiría a los consumidores a comparar la calidad de las diferentes compañías y elegir luego la opción aquella que presta un mejor servicio para sus necesidades. Sin hacer público estos detalles, las compañías pueden ocultar sus puntos débiles.

9. Noveno párrafo (20-XI-07)

¿quién soporta el secretismo? Son los vendedores de software como Microsoft que quieren mantener su información vulnerable bajo secreto. Las recomendaciones del ministerio del interior tuvieron amplio eco por las operadoras telefónicas, ya que los intereses de esas compañías se sirven del secretismo, más que en el interés de los consumidores de los ciudadanos o de la sociedad.

10. Décimo párrafo (26-XI-07)

Tras el 11 de septiembre estamos viendo este conflicto del entre el secretismo y la transparencia ocurre en todo el mundo. El gobierno estadounidense está intentando mantener los detalles de muchas medidas anti-terroristas – e incluso las operaciones más rutinarias gubernamentales – en secreto: la información sobre la infraestructura de las plantas de energía, los edificios gubernamentales y la información de perfiles de consumidores utilizada para identificar a ciertos pasajeros de líneas aéreas; los estándares que utiliza el ministerio del interior codificados con colores de niveles de seguridad anti-terrorista e incluso la información sobre las operaciones gubernamentales que no tienen ninguna conexión con el terrorismo.

11. Undécimo párrafo (26-XI-07)

El secretismo mantiene a los terroristas en la ignorancia especialmente a los terroristas ineptos que por sí solos no serían capaces de encontrar esos fallos. Pero al mismo tiempo, la ciudadanía –

de la cual el gobierno es en última instancia responsable – no puede evaluar las contramedidas o comentar su eficacia; por tanto la seguridad no puede progresar porque no existe un debate público ni educación de la ciudadanía.

12. Duodécimo párrafo (26-XI-07)

Estudios recientes han demostrado que la mayoría de los sistemas de aguas, energía, gas, telefonía, datos, transportes y de distribución son redes libres de escala: siempre tienen conmutadores altamente conectados. Los atacantes saben esto intuitivamente y van tras estos nodos mientras que las víctimas están empezando a aprender como mejorar la seguridad de los nodos y ofrecer redundancia, ya que tratar de esconder el hecho de que una red tiene nodos concentradores es inútil, es mejor identificarlos y protegerlos.

13. Décimo tercer párrafo (26-XI-07)

Estamos más seguros cuando tenemos la información necesaria y así ejercer presión sobre los vendedores para mejorar la seguridad, mientras que estamos menos seguros si las vendedores de software no hacen públicas sus vulnerabilidades de seguridad, y si las operadoras telefónicas no tienen que hacer un informe de los problemas de su red. Los gobiernos que funcionan sin tener que dar cuentas sirven a sus propios intereses y no a los intereses públicos.