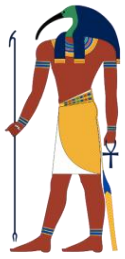

Píldora nº 7: ¿Qué son los Principios de Kerckhoffs?

Escena 1: La figura de Auguste Kerckhoffs

Auguste Kerckhoffs fue un lingüista y criptógrafo holandés que nace en 1835 y fallece a los 68 años en 1903. En enero y febrero de 1883, siendo profesor de alemán en París, publica en el *Journal des Sciences Militaires* el artículo *La cryptographie militaire*, un importante tratado sobre la criptografía en el que, entre otras cosas, establece lo que se conoce como Postulados o Principios de Kerckhoffs.

Escena 2: Principios de Kerckhoffs

En su traducción literal, los seis principios de Kerckhoffs aplicados a la criptografía son:

1. El sistema debe ser en la práctica indescifrable, en caso de que no lo sea matemáticamente.
2. El sistema no debe ser secreto y no debe ser un problema que éste caiga en manos del enemigo.
3. La clave del sistema debe ser fácil de memorizar y comunicar a otros, sin necesidad de tener que escribirla; será cambiable y modificable por los interlocutores válidos.
4. El sistema debe poder aplicarse a la correspondencia telegráfica.
5. El sistema debe ser portable y su uso no deberá requerir la intervención de varias personas.
6. El sistema debe ser fácil de usar, no requerirá conocimientos especiales ni tendrá una larga serie de reglas.

Escena 3: Matizando e interpretando algunos principios

Excepto el cuarto principio, que no es directamente aplicable a la criptografía actual y que deberemos matizar, puesto que hoy en día la correspondencia es en general digital y no telegráfica, todos los demás principios siguen siendo válidos 131 años después.

En cuanto al primer principio que establece que en la práctica el sistema de cifra debería ser indescifrable, hoy se interpreta a que éste sea computacionalmente seguro. En otras palabras, que por limitaciones en la capacidad de cálculo de los actuales ordenadores, el sistema de cifra resista todo tipo de ataques, en tanto el tiempo necesario como el esfuerzo económico para que dichos ataques fuesen viables sería inmenso y, por lo tanto, no abordable.

Escena 4: ¿Cuál es la aportación más importante de los Principios de Kerckhoffs?

La aportación más importante de los Principios de Kerckhoffs es la segunda, que dice: el sistema no debe ser secreto y no debe ser un problema que éste caiga en manos del enemigo. Hoy en día hemos simplificamos su enunciado, diciendo simplemente que la seguridad del sistema debe recaer sólo en la clave.

Profundizando algo más, como se lee en la entrada Lema de Kerckhoffs del Glosario y Abreviatura de la Guía de Seguridad de las TIC del profesor Arturo Ribagorda, publicada por el Centro Criptológico Nacional de España en 2009, este postulado establece que “la seguridad de cifrado debe residir, exclusivamente, en el secreto de la clave y no en el desconocimiento del algoritmo de cifrado. Antes bien, este último debe ser de general conocimiento por la comunidad criptográfica, para que pueda ser criptoanalizado y descubiertas sus vulnerabilidades si las hubiere”.

Madrid, octubre de 2014

Autor del guion: *Jorge Ramió Aguirre*
Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*