Los Estados Unidos tienen una larga historia en cuanto a restringir la exportación de criptografía, conforme a la teoría que la criptografía es una suerte de "munición". Antes de diciembre de 1998, sólo se podían exportar legalmente desde es país, productos criptográficos para el empleo general que no usaran más de 40 bit para cifrado simétrico y 512 bit para el cifrado asimétrico.

El tamaño de clave de 40 bit es extensamente reconocido por ser vulnerable a los ataques y por ser aún muy utilizado. En 1996, Damien Doligez, un estudiante en Francia, usó una red de terminales de trabajo para intentar un ataque por fuerza bruta[1] sobre 40 bit SSL, la llave había sido fijada como un desafío para descifrar [Doligez96]. La búsqueda con su red tomó 8 días.
Otro ataque por fuerza bruta distribuido por un grupo más tarde en el mismo año, encontró que "rompía" el SSL en 32 horas.

Desde entonces los ordenadores se han hecho más rápidos y más baratos. Una métrica estándar calcula en 10x cada cinco años el aumento de poder/dólar (ver datos del año 1995 y dividir por diez)[2].
Ya que pasaron más de cinco años desde el desafío original sobre SSL, una estimación muy elemental sería que la misma rotura tomaría entre 19 horas (usando el sistema de Doligez) y 3,2 horas (usando el sistema del segundo grupo).

Posteriormente, grupos públicos construyeron motores de fuerza bruta dedicados. En 1998, un grupo apoyado por el EFF (Electronic Frontier Foundation) lanzó el "Deep Crack" un motor para "crackear" el DES [EFF98]. Con un coste (en 1997) de aproximadamente 210.000 u$s ellos construyeron una máquina capaz de emplear la fuerza bruta ("quebrando") una llave sola de 56 bit DES en alrededor de 56 horas (casualidad)[3].

[1] Se define como ataque por fuerza bruta a aquel método que para determinar la combinación exacta prueba todas las posibles hasta que "acierta" con la correcta.
[2] Tiempo promedio en 1995

	40 bit	**56 bit**	**128 bit**
100 K$	2 seg.	35 hs.	10e19 años
100 M$	0,002 seg.	2 min	10e17 años
100.000 M$	0,000002 seg	0,1 min	10e13 años

[3] Desafío I: tiempo para romper la llave = 41 días
Desafío II: tiempo para romper la llave = 56 horas
Desafío III: tiempo para romper la llave = 22 horas 15 minutos, el 18.01.1999 EFF ganó un premio de 10.000$. Para obtenerlo utilizó 100.000 PC trabajando simultáneamente sobre Internet, las que probaban 245.000 millones de claves por segundo!

Tuve la suerte de conocer a uno de sus creadores John Guilmore, también fundador y líder de EFF (http://www.eff.org) y empleado de Sun Microsystems, con oportunidad de la Conferencia Anual de RSA en San José (California), quien me obsequió su libro "Cracking DES", donde describe paso a paso cómo construir su Deep Crack, demostrando lo inútil de la inversión de aproximadamente 30 millones de dólares, hecha por el gobierno de EE.UU. para el desarrollo de DES, argumentando que se tardarían miles de años en descifrar su algoritmo.

Tratando de poner algo de luz, recordamos que el número posible de llaves en 56 bit es 2^{56} o aproximadamente 72 por 10^{16} (72.057.590.000.000.000). En 40 bit es decir 2^{40} es aproximadamente 1.099.511.000.000, lo que representa 1/65536 del número de llaves que hay en una clave de 56 bit.

Si el "craker" de DES de EFF fuera aplicado a una mucho más pequeña llave de 40 bit, en aproximadamente 4 segundos la quebrarían, es decir obtendrían dicha llave.

La criptografía asimétrica (también llamada criptografía de clave pública) también puede ser víctima de ataques mediante la fuerza bruta. El más famoso es el Crypto Desafío de RSA.
Uno de los más recordados fue el factoreo de dos números primos en una llave de 512 bit RSA en agosto de 1999 [RSA99]. La solución del Desafío tomó aproximadamente 5.2 meses utilizando 292 ordenadores extendidos sobre Internet.

Por consiguiente, RSA Laboratories ahora recomienda al menos 768 bits para la seguridad en PKI, en realidad hoy la seguridad se obtiene con 2048, lo cual es una exageración para la mayoría de los requerimientos. Al presente vemos autoridades de certificación con llaves de 4096 y cosas por el estilo, lo que ocurre que siempre debemos pensar en mantener un sano equilibrio, por cuanto no es gratis el empleo de este tipo de seguridad. El tiempo que se emplea para encriptar y desencriptar con claves asimétricas de tamaña magnitud es muy grande.

Las restricciones finalmente fueron vencidas, en especial por la presión ejercida por las mismas empresas de seguridad estadounidenses que veían cómo perdían mercado ante sus similares del resto del mundo, que re-construía algoritmos de encripción fuerte y llaves de 128 bit mientras ellos miraban cómo se le evaporaba el negocio.

Todo en este tema no es blanco o negro, lo que si es claro que en el mundo de las comunicaciones seguras, las transacciones comerciales mediante SSL requieren si o si claves de 128 bits para poder afirmar que estamos "seguros" y que en el ambiente de Infraestructuras de Clave Pública (PKI), no se puede bajar casi en todos los casos de claves de 1024, que ya se han convertido en un estándar.

Pero tengamos algo en claro, como siempre la cadena se corta por el eslabón más débil: lo que significa que de nada servirá que la tienda virtual a la que estoy comprando tenga un servidor con llaves de 128 bits, si yo en el otro extremo estoy empleando un browser que me permite manejar 40 bits!, por lo tanto además de lo expresado anteriormente no olvidemos: verificar las características de seguridad del site al que ingreso, haciendo clic en el candado o en la llave y mantener actualizado mi navegador al último release con 128 bits.

Ing. Jorge Bernardo