CHIP CLIPPER

Armesto Diana
diarcar25@gmail.com
UNIVERSIDAD PILOTO DE COLOMBIA

Resumen — Este documento hace referencia a eventos de Ciberterrorismo usados en la historia como una herramienta de vigilancia y control político por parte del gobierno de E.E.U.U donde la idea principal era imponer el uso de un chip en los dispositivos en los que se puede utilizar cifrado como son los PC, módems, televisores, y teléfonos, y con esto realizar investigaciones y controlar por medio del algoritmo, la seguridad del país, utilizando técnicas para descifrar los mensajes almacenados con estos equipos.

Índice de Términos — criptografía, información, seguridad, vigilancia.

Abstract — This paper refers to events in the history when the Cyberterrorism used as a tool of surveillance and political control by the U.S. government, where the main idea was to impose the use of a chip on devices that can use encryption such as PCs, modems, televisions, and telephones, and with this research and control by the algorithm, the country's security, using techniques to decipher the messages stored on this equipment.

Palabras Clave – Custodia, integridad, información, control, seguridad.

I. INTRODUCCIÓN

En la década de los 80 se estaba presentando conflictos en todos los medios de comunicación en E.E.U.U., a raíz de estos inconveniente el gobierno de ese país hizo un pequeño invento criptográfico llamada Chip Clipper, destinado a proteger las comunicaciones privadas del gobierno con la posibilidad de que una entidad certificadora obtenga las llaves electrónicas necesarias para descifrar las comunicaciones previa autorización de la autoridad competente.[1] Este chip utiliza una llave de 80 bits para cifrar voz y datos y fue utilizado en los equipos del gobierno de E.E.U.U. para protegerse de intrusos que habitualmente están violentando la seguridad de los sistemas.

En 1984 el presidente Ronald Regan decreto la controversial decisión de otorgar a la Agencia de Seguridad Nacional (NSA) el control de todos los sistemas computacionales que contienen información sensible no calificada, tanto del gobierno como no gubernamental. Seguido a esto la Computer Security Act reafirmo que la NIST[1] era la responsable de los sistemas de computación que contengan información sin clasificar de origen militar o estatal y le quito el poder a la NSA[2].

Luego de esto la NSA en el año de 1989 volvió a retomar el control de los sistemas, iniciando con esto el proyecto de Chip Clipper, destinado a encriptar llamadas telefónicas, módems, televisores, fax y computadores, y esto estaba bajo la custodia de dos agentes quienes conservaban las llaves privadas de ciudadanos bajo vigilancia de algún organismo de seguridad. Este chip en especial no podía ser abierto, de forma que no podían estudiar su diseño interno.

La propuesta del Chip Clipper no fue bien recibido por empresas ni por entidades estatales, porque lo asociaron como una herramienta de espionaje y no como un diseño fuerte de Encriptación.

[1] NIST..National Institute for Standars and Technology
[2] NSA National Security Agency

II. DEFINICIÓN

A. TERRORISMO

No existe una definición única y universalmente aceptada, de terrorismo. El terrorismo se define en el Código de Regulaciones Federales como "el uso ilegal de la fuerza y la violación contra personas o propiedades para intimidar o coaccionar a un gobierno, la población civil, o cualquier otro segmento del mismo, en cumplimiento de los objetivos políticos o sociales"[FBI (Federal Bureau of Investigation)].

B CIBERTERRORISMO

Mark Pollit, agente del FBI quien se ha dedicado a estudiar este fenómeno, define el "*Ciberterrorismo como un ataque premeditado y políticamente motivado contra la información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no cambiantes por parte de grupos subnacionales o agentes clandestinos*" [FBI (Federal Bureau of Investigation)].

C CHIP CLIPPER

A finales de la década de los 70, el gobierno de los Estados Unidos publicó el Data Encryption Standard (DES) para sus comunicaciones de datos sensibles, pero no clasificados, en 1993 el gobierno americano promueve una nueva iniciativa de criptografía encaminada a proporcionar a los civiles una alto nivel de seguridad en las comunicaciones; el proyecto *Clipper* se basa en dos aspectos fundamentales:

- Un chip cifrado a prueba de cualquier tipo de análisis o manipulación (el Clipper Chio o EES (Encrowed Encryption Standard)).
- Un sistema para combatir las claves secretas que, en determinadas circunstancias, otorgaría el acceso a la clave maestra de cada chip y permitiría conocer las comunicaciones cifradas por él [1].

No obstante, el primer gran conflicto que existió en las telecomunicaciones en torno con la privacidad y la violación de la intimidad sucedió en la década de los 80, y fue a través del *Chip Clipper*, que era un pequeño chip criptográfico destinado a proteger las comunicaciones privadas pero dejando abierta la posibilidad de que agentes gubernamentales obtengan las "llaves electrónicas" necesarias para descifrar las comunicaciones tras obtener una autorización legal.

Fig.1. Mykotronx MYK-78T ("Clipper") Escrowed Encryption Chip

El *Chip Clipper* (Fig. 1) también conocido como MYK-78T diseñado por el físico Mykotronx (EE.UU), de diseño anti – manipulación (a prueba de falsificaciones) del tipo VLSI (Very Large Scale Integration), dicho chip fue pensado para la encripción de llamadas telefónicas, donde dos agentes de custodia gubernamentales conservarían las llaves necesarias para que el gobierno pueda descifrar los mensajes de aquellos ciudadanos bajo vigilancia del FBI u otro organismo de seguridad. El Chip Clipper usaba un algoritmo de cifrado de datos conocido como Skipjack para transmitir información y algoritmo de Diffie – Hellman para distribuir llaves criptográficas de sesión entre los usuarios del microprocesador.

La iniciativa clipper (sistema de claves depositada) buscaba proporcionar a los usuarios un alto nivel de seguridad en las comunicaciones fortaleciendo la confidencialidad y la encripción.

Esta práctica se baso en dos elementos:

1) Chip cifrador: a prueba de análisis o manipulación.
2) Sistema de depósito claves secretas, administrado por el gobierno.

Cada clave secreta se divide en dos componentes que se entregan a dos agencias estatales independientes para su custodia, solo en el caso de que se necesitara la interceptación de la comunicación y tras gestionar la autorización judicial , la policía podría conseguir de las dos agencias los dos componentes de cifrado que permiten descifrar la comunicación.

Como base de uso se estipulo el Protocolo de interceptación de comunicaciones que consistía en:

1) Si durante una escucha programada legal se detectan comunicaciones cifradas mediante clipper, se solicita a las dos agencias encargadas (entidades certificadoras) que entreguen a los agentes las dos partes de la clave.
2) Las dos agencias depositarias extraen los componentes cifrados de la clave y lo entregan a los agentes. Las dos partes de la clave se unen para ser descifrada, teniendo la clave se procede a descifrar la comunicación.
3) Al terminar la escucha se solicita el borrado de la clave del procesador de cifrado (clipper), una vez borrado se genere y envía un certificado de la destrucción de la clave a las agencias depositantes.

D. Algoritmo de Cifrado Simétrico o de Clave Secreta

El cifrado simétrico consiste, un método criptográfico en el cual la clave de cifrado y la de descifrado son la misma; donde las dos partes que intervienen en la comunicación se ponen de acuerdo sobre la llave o clave que van a usar; una vez ambos tienen el acceso a la llave o clave, el remitente cifra el mensaje usando la clave, y lo envía al destinatario, esté lo descifra con la misma. Figura No 1.

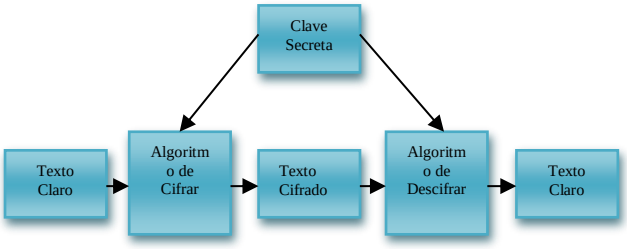

Fig. 2 Cifrado Simétrico (Clave Secreta)

E. Algoritmo DES (Data Encryption Standard) y SKIPJACK

El algoritmo DES (Data Encryption Standard) emplea una clave de 56 bits y opera sobre bloques de 64 bits y realiza 16 procesos sucesivos. El tamaño efectivo de la clave de DES puede aumentarse mediante cifrado múltiple.

El algoritmo SKIPJACK el cual ha sido implementado en el Chip Clipper, es un algoritmo diseñado por la NSA (National Security Agency), para apoyar la tecnología de depósito de claves; SKIPJACK emplea una clave de 80 bits que opera sobre bloques de datos de 64 bits y realiza 32 procesos sucesivos.

La clave, generada y programada en el *chip* después de que éste ha sido fabricado, se divide en dos partes que son cifradas y entregadas a dos agentes de claves que deben guardarlas por separado garantizando su seguridad [2].

F. Algoritmo de Cifrado Asimétrico o de Clave Pública

Los algoritmos asimétricos o de clave pública fuero introducidos por *Diffie – Hellman* y se basan en usar un par de claves o llaves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave o llave pública que puede entregar a cualquier persona, y la otra clave o llave privada que solo es del propietario y ninguna otra persona puede tener acceso a esta Figura No 1.

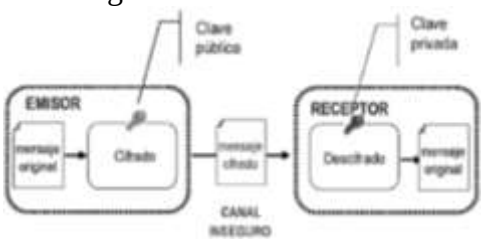

Fig.3. Cifrado Asimétrico (Clave Pública)

El clipper fue un estándar de cifrado voluntario para las comunicaciones telefónicas que se pretendía convertir en un estándar de cifrado capaz de velar por los intereses de particulares y el estado garantizando confidencialidad y aplicaciones de la ley.

Fig. 4 Interior del teléfono TSD-3600-E

El Chip está presente en el interior del teléfono encriptador TSD-3600-E por parte de AT & T. El chip está soldado directamente a la placa (es decir, no enchufado) y se pensaba que era a prueba de altas temperaturas. El AT & T TSD-3600 fue el primer y único teléfono encriptador que aparece con el chip Clipper instalado.

Fig.5 Teléfono TSD-3600-E

El algoritmo fue clasificado inicialmente como secreto, por lo que no podía ser examinado en la forma habitual por la comunidad científica de encriptación. Después de mucho debate, el algoritmo Skipjack finalmente fue desclasificado y publicado por la NSA el 24 de junio 1998. Se utiliza una clave de 80 bits y un algoritmo de cifrado simétrico, similar al DES.

G. CONTENIDO DEL CHIP

El algoritmo utiliza claves de 80 bits (en comparación con 56 para el DES) y tiene 32 rondas de codificación (en comparación con 16 para el DES). Es compatible con todos los 4 modos de operación del algoritmo DES. Adicionalmente, tiene 32 ciclos de reloj, y se ejecuta en modo de 12 Mb por segundo. Cada chip incluye los siguientes componentes:

Algoritmo de cifrado Skipjack
F, familia de claves de 80 bits que es común a todos los chips
N, un número de serie de 30 bits (esta extensión está sujeta a cambios)
U, una clave secreta de 80 bits que abre todos los mensajes cifrados con el chip
K, clave específica para determinada conversación de 80 bits
M, el mensaje

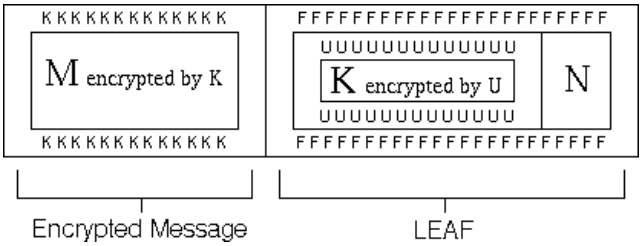

Fig.6 Diagrama del paquete de datos del chip clipper

III. VENTAJAS

1) El Chip Clipper se podía usar como dispositivo de cifrado/descifrado.

2) Clipper incluye una capa adicional de protección, ya que cualquier persona que desee llevar a cabo una intervención telefónica debe adquirir también un procesador especial y descifrar las claves de los agentes de depósito en garantía.

IV. DESVENTAJAS

1) El proyecto CLIPPER fue tomado como una amenaza potencial contra la libertad individual por parte del estado, quedando como un intruso en el derecho de cada ciudadano a la vida privada.

2) También se argumentó que las entidades certificadoras o agencias depositarias estarían expuestas a ataques demostrados que eran vulnerable perdiendo valor en su factor de encripción, dando cabida a mejora técnicas de encripción como PGP.

3) El gobierno pretendía crear una puerta trasera en las comunicaciones encriptadas de la sociedad de entonces, así que cualquier teléfono puede tener al espionaje estatal dentro.

V. CLASES DE CHIP CLIPPER

1) Existieron cinco diferentes modelos de Chip Clipper TSD-3600 modelos elaborados en año 1992 que en el mismo año produjo su cancelación del producto, utilizaba el algoritmo de cifrado.

2) La TSD-3600d originalmente utilizó el algoritmo DES con una clave de 56 bits.

3) El 3600F fue un modelo exportable que utilizaba un cifrado de 40 bits. Fue un chip débil incluso teniendo en cuenta la combinación de teclas.

4) El 3600P utilizaba la propiedad de 56 bits de cifrado similar a DES.

5) El 3600E fue el primer dispositivo de seguridad avanzada utilizando el algoritmo skipjack.

6) El modelo 3600, incluye un chip Clipper, interoperable para el cifrado F o P cuando se comunica con esos modelos.

A. Tendencias actuales de encriptación.

Desde el surgimiento y posterior declive del Chip Clipper hasta la actualidad, el problema de seguridad en comunicaciones se ha mantenido, lo cual ha permitido la aparición de nuevas tecnologías de encriptación en chips robustos y desarrollo de software de encriptación de alto nivel.

B. Algunos ejemplos son:

1) Tecnología IPHONE-SHIELD

La solución avanzada de IPHONE-SHIELD encabeza la industria en tanto que proporciona seguridad en multi-niveles a fin de establecer una llamada encriptada de óptima calidad entre dispositivos móviles confiables. IPHONE-SHIELD utiliza EMCP (Encrypted Mobile Content Protocol - Protocolo de Encripción de Contenido Móvil), un conjunto de protocolos basados en estándares tecnológicos, con el fin de optimizar el intercambio de contenido entre teléfonos celulares en tiempo real y a través de redes inalámbricas con bajo ancho de banda.

Certificado por el Ministerio de Defensa de los Estados Unidos de Norteamérica bajo la norma FIPS 140-2 del NIST (Cert# 1310)

2) Criptografía y Generación de Números Aleatorios

Criptografía de Clave Pública (RSA de 2048 bits y ECDSA utilizando curvas con módulos primos de 384 bits).

El RSA y ECDSA son utilizados para la autenticación. Los pares de la clave se generan en el teléfono durante la instalación y son únicos para cada aparato telefónico. Una clave privada jamás se comparte. Los algoritmos de Curva Elíptica Diffie-Hellman (ECDH) y los algoritmos RSA se utilizan para el intercambio de claves. La clave de sesión es válida para una sola llamada y se destruye de forma segura al finalizar su uso.[9]

3) Criptografía Simétrica

(AES y RC4 ambas de 256 bits) Ambos algoritmos de encriptación se utilizan al mismo tiempo. El paquete de datos se encripta primeramente con RC4 y el texto cifrado resultante se encripta nuevamente con AES en modo de operación "Contador" (CTR). Ambos algoritmos se inicializan con el intercambio de clave de sesión.

Algoritmos Base "Hash" (SHA512, MD5) Dos algoritmos base "Hash", estándares en la industria, son utilizados para obtener una mayor garantía en la integridad de la encriptación.

4) Generación de Números Aleatorios

Durante el proceso de instalación se genera una base inicial de valores numéricos de 2048 bits que se actualiza periódicamente.

El valor inicial se obtiene del input del micrófono.[9]

VI. MARCO LEGAL

CONSTITUCIÓN POLÍTICA COLOMBIANA 1991

ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan

interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar.

Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

LEY 599 de 2000 Por la cual se expide el Código Penal

Título III. Capítulo VII

Artículo 192. *Violación ilícita de comunicaciones*. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya delito sancionado con pena mayor.

Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de dos (2) a cuatro (4) años.

Artículo 193. Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. El que sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.

Artículo 196. Violación ilícita de comunicaciones o correspondencia de carácter oficial. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida comunicación o correspondencia de carácter oficial, incurrirá en prisión de tres (3) a seis (6) años.

Artículo 197. *Utilización ilícita de equipos transmisores o receptores*. El que con fines ilícitos posea o haga uso de aparatos de radiofonía o televisión, o de cualquier medio electrónico diseñado o adaptado para emitir o recibir señales, incurrirá, por esta sola conducta, en prisión de uno (1) a tres (3) años.

La pena se aumentará de una tercera parte a la mitad cuando la conducta descrita en el inciso anterior se realice con fines terroristas.

La pena descrita en el inciso anterior se aumentará hasta en una tercera parte cuando la comunicación o la correspondencia esté destinada o remitida a la Rama Judicial o a los organismos de control o de seguridad del Estado.

LEY 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Artículo 269 A. Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 B. Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269 C. Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

VII. CONCLUSIONES

- La palabra Ciberterrorismo hace referencia al terrorismo digital y su ataque es por los medios informáticos.
- El Chip Clipper está orientado a un hardware criptográfico que implementa un cifrado simétrico, con una táctica de seguridad para que intrusos no lograran abrirlo y verificar su diseño interno.
- El chip Clipper se utilizó para escuchar y grabar las conversaciones realizadas por los civiles en U.S.A violando la privacidad.
- Las entidades privadas y estatales no están preparadas para dar a entidades específicas el control de la información, que día a día se genera en sus medios de comunicación; medidas como el clip clipper ponen en sobre aviso a la sociedad de las intenciones del estado y de la capacidad tecnológica que podría tener para de una manera u otra tener el manejo de la información.
- Aunque la propuesta pública de chip clipper no fue aceptada por las entidades privadas y estatales no es descartable que se haya implementado.
- Con el fin de preservar la seguridad y de tener información almacenada que pueda ser utilizada en investigaciones puntuales, los gobiernos ven la necesidad de almacenar información referente a conversaciones telefónicas o transferencia de datos electrónicos. Sin embargo, el hecho de realizar desarrollos tecnológicos enfocados a este tipo de necesidades, no solo implica la parte de hardware y algoritmos, sino que se debe realizar un estudio detallado de las garantías de seguridad que se ofrecen, para así evitar que con la implementación, se dejen agujeros que pueden causar problemas más grandes que el inicial.

REFERENCIAS

[1] [RINCON CARDENAS, Erik. Manual de derecho de comercio electrónico y de internet Colección lecciones de jurisprudencia. Editor Universidad del Rosario, 2006.

[2] CALLE GUGLIERI, J. A. Reingeniería y seguridad en el ciberespacio. Edición Ilustrada, Editor Ediciones Días de Santos, 2005.

[3] CURTIN, Matt. Brute force: Cracking the data encryption standard. Interhack Corporation. 2005

[4] GODWIN, Mike. Cyber Rights: Defending free speech in the digital age. Extremely Reliable. 2003.

[5] GOMEZ VIEITES, Alvaro. Enciclopedia de la seguridad informática. Alfaomega Ra-Ma,2007.

[6] DENNING, Dorothy E. The Case for Clipper (Clipper Chip offers escrowed encryption). (en la web) MIT's Technology Review (07/1995). http://encryption_policies.tripod.com/us/denning_0795_clipper.htm>

[7] AT&T TSD-3600 Telephone Security Device (Clipper Chip). (en la web) http://www.flickr.com/photos/21746901@N08/sets/72157603948664464/

[8] DENNING, Dorothy E. The clipper chip: A technical summary. (en la web) Abril 21, 1993. http://catless.ncl.ac.uk/Risks/14.52.html#subj1

[9] Tecnología Avanzada en medidas y Contra Medidas Electrónicas http://www.espionaje.org/celular-cifrado-encriptador-telefonico_17.htm

AUTOR

Diana Eileen Armesto Camayo, soy egresada de la Universidad Nacional Abierta y a Distancia (UNAD) de la ciudad de Sogamoso, Actualmente vivo en la ciudad de Duitama, me he desempeñado como docente de la UNAD de Soata, actualmente trabajo como independiente.