PRETTY GOOD PRIVACY & CLIPPER CHIP & ITAR

By Yaman Akdeniz

MA Research student at the Criminal Justice Studies of the Law Faculty of University of Leeds, Leeds LS2 9JT.

E-mail: lawya@leeds.ac.uk.

Please cite as Yaman Akdeniz, "Pretty Good Privacy & Clipper Chip & ITAR" August 1996, Cyber-Rights & Cyber-Liberties (UK) at http://www.leeds.ac.uk/law/pgs/yaman/pgp&itar.htm.

The purpose of this short paper is to explain what is PGP, Phillip Zimmerman's powerful encryption software and the US government's proposed encryption tool, the Clipper Chip. This will be helpful for the UK readers to understand the encryption debates in the United States. US export regulations are also examined with links to recent cases.

PGP and Phillip Zimmerman

Pretty Good Privacy ("PGP") is a cryptography software which works on the same principle that public key systems use, but has many more features (1). PGP is the most used encryption tool by the Internet users because it is widely available on the Internet for free and it is considered for the present unbreakable. PGP is based on the RSA algorithm and it is by today's computing standards uncrackable. Philip Zimmerman, the creator of, PGP, explains it as:

> "well featured, fast, with sophisticated key management, digital signatures, data compression, and good ergonomic design." (2)

In April 1993, while Zimmerman was preparing to release the initial version of PGP, the US government announced its own public key cryptographic software, the Clipper Chip. Zimmerman completed and released PGP hoping that it would be seen as a good alternative to the government's proposal but he had been under investigation for alleged violation of export regulations, with a grand jury hearing evidence for about 28 months, which ended in January 1996 (3). He was under investigation because the disclosure or transfer of cryptographic software to a foreigner constitutes export under the ITAR (4). But Zimmerman never exported the PGP, he created it, encouraged its use and distributed to friends and colleagues, one of whom posted it to an Internet Usenet discussion group (5). The Federal Government decided not to prosecute Mr. Zimmerman and did not explain why they dropped the investigation (6).

US Clipper Chip

Clipper chip is an escrowed encryption project proposed by the Clinton Administration first time in April 1993. This Escrowed Encryption Standard ("EES") uses a classified symmetrical algorithm developed by the National Security Agency ("NSA"). Escrowed encryption means that two government agencies, the

National Institute of Standards and technology ("NIST") and the Department of Treasury, each hold half of the encryption key. The Clipper chip is available on hardware and not on software and the US Government's initial idea was to install the chip in every telephone, fax machine and modem and make it a national standard. By creating a national standard on this basis the US law enforcement agencies would be able to decrypt any messages encrypted by using the Clipper Chip upon due authorisation. The Clipper Chip was opposed by many civil liberties groups on the ground that it would infringe the privacy of users by the fact that the government has access to the keys. The image and fear of an Orwellian (7) style Big Brother Watching emerged.

According to the FBI, wiretapping is crucial to effective law enforcement:

> "If the FBI and local police were to loose the ability to tap telephones because of the widespread use of strong-cryptography, the country would be unable to protect itself against terrorism, violent crime, foreign threats, drug trafficking, espionage, kidnapping, and other crimes." (8)

The US Government in December 1995, presented a revised version of their Clipper Chip proposal which keeps in place the current export ban on strong encryption tools but allows for the export of moderately stronger, 64-bit key systems with key escrow systems (9). This new proposal known as Clipper II, does not go far away from the initial proposals.

In May 1996, the US Government came with a new proposal, "*Achieving Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure*" (10) which would establish a new public key infrastructure for encryption. Such a public key infrastructure proposed by the new proposal already dubbed as Clipper III, would enable users of encryption to clearly identify the people they are communicating with, and is widely viewed as an important prerequisite for the widespread use of secure electronic communications. However, as the Center for Democracy and Technology argues, Clipper III will not meet the privacy and security needs of Internet users because all users of the new system would have to ensure government access to their encryption keys through an approved key escrow agent (11).

It will be difficult to find a foreign market and foreign users for these products with the key escrow system, whatever their length is, because Big Brother will be watching abroad as well (12). Clipper Chip proposal would also limit the survival of some dissident movements where anonymity is an essential feature (13). Cryptography allows unprecedented anonymity both to groups who communicate in complete secrecy and to individuals who use anonymous e-mailers over the Internet to hide all traces of their identity when they communicate (14). Key escrow and the clipper chip threatens this kind of anonymity on the Internet (15). The government agents will be able to identify the content of e-mails and the destination of the messages.

Arms Export Control Act (16) & International Traffic in Arms Regulation (17)

Export of cryptography software with encryption keys over 40 bits long generally cannot be exported from the United States for reasons of security under the Arms Export Control Act ("AECA") (18) and the International Traffic in Arms Regulation ("ITAR") (19). The AECA was enacted to permit the Executive Branch to control the export and import of certain items in order to further "world peace and the security and foreign policy" of the United States (20). Cryptography software is included in the United States Munitions List ("USML") (21). Section 121 XIII(b)(l) includes:

> "Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems..."

The ITAR clearly considers cryptographic software as weapon whose export is illegal if not authorised by the American Department of State.

There has been a recent amendment to the ITAR provisions in February 1996. The new amendment establishes an exemption for the temporary export of cryptographic products for personal use. This would cover US citizens and lawful permanent residents who for example need or take their cryptographic software with them in their laptop computers when they go abroad for brief periods of time (22).

Senators Conrad Burns (R-MT) introduced the *Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996* on May 1996 to relax the restrictions prohibiting the export of strong encryption technology.

> "Any encryption software, or hardware incorporating such software, that is generally available (23), as is, and designed for installation by the user or purchaser, or that is in the public domain, would be exportable, regardless of key lengths."

Many of the popular web browsers, Pretty Good Privacy, or encryption in other widely available software would all be exportable with unlimited key lengths once made publicly available in the U.S.

The export controls with respect to cryptographic software were the subject matter of two recent contrasting decisions. See:

Philip Karn v. US department of State and Thomas E. McNamara No. 95-1812 (CRR) (U.S. District Court for the District of Columbia), March 22, 1996.

Daniel J. Bernstein v U.S. Department of State et al., U.S. District Court, Northern District of California 1996, No. C-95-0582 MHP.

Endnotes:

1. E.g. a user can select the amount of security that PGP provides. The user can decide on the length of the key where a shorter one is quicker but less secure and a long one provides better security but it is slower. A user can also sign a message with his own secret key, amking it impossible for others to change the message. See Jonathan Wallace & Mark Mangan, *Sex, Laws, and Cyberspace*, Henry Holt: 1996, page 47 for the explanation of the authentication feature in the PGP.
2. Philip R. Zimmerman, *The Official PGP User's Guide*, MIT Press, 1995.
3. See the CDT Policy Post Number 34, January 12, 1996 at http://www.cdt.org. See also [1996] CUD 8, 5 at http://www.soci.niu.edu/~cudigest
4. 22 C.F.R. art. 120.17.
5. See Jonathan Wallace & Mark Mangan, *Sex, Laws, and Cyberspace*, Henry Holt: 1996, page 42.
6. See the Web site dedicated to him and his legal defence fund at http://www.netresponse.com/zldf/
7. George Orwell, *1984*, Penguin, 1990.
8. FBI Director Louis Freeh, Address at the Executives' Club of Chicago, Feb. 17, 1994, at13.
9. See Center for Democracy and Technology, "Clinton Administration Continues to Push For Flawed Crypto Export Policy" from the Clipper II Archieves.
10. See the proposal at http://www.epic.org/crypto/key_escrow/white_paper.html
11. See the CDT Preliminary Analysis of "Clipper III" Encryption Proposal, May 21, 1996 at

http://www.cdt.org. See also Senator Conrad Burn's Response to the proposal, "Burns: Clipper III Strikes Out".

12. Leonard Doyle, "Spooks All Set to Hack it on the Superhighway" Independent, May 2, 1994 reports that: "The US plan for a Clipper Chip has raised fears among European businesses that sensitive information would no longer be secret if it were vetted by the CIA or the FBI."
13. A. Michael Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution" [1995] U. Penn. L. Rev. 143, 709-897, at 817.
14. ibid. at 818.
15. The Supreme Court in *NAACP v. Alabama ex rel. Patterson* 357 U.S. 449 (1958) at 462 stated that "inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association". In McIntyre v. Ohio Elections Commission, 115 S.Ct. 1511, (1995) the Supreme Court states that "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment" and "the anonymity of an author is not ordinarily a sufficient reason to exclude her work product from the protections of the First Amendment." See Michael A. Froomkin, "Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases" which states that Despite these ringing words, whether there is a right to be anonymous in the US remains unclear as a general matter, since difficult cases are precisely those in which exceptions are made to fit facts that sit uncomfortably within the rules that apply "ordinarily." For a contrary view that "McIntyre will prove to be dispositive" in providing First Amendment protections to anonymous political speech, see Richard K. Norton, Note, McIntyre v. Ohio Elections Commission: Defining the Right to Engage in Anonymous Political Speech, 74 N. Cal. L. Rev. 553 (1996).
16. 22 USC ss 2751-2796d.
17. 22 C.F.R. ss 120-130.
18. 22 U.S.C. 2778(a)(1) authorises the President to control the import and export of defence articles and defence services by designating such items to the United States Munitions List ("USML").
19. 22 C.F.R. Sections 120-30, were promulgated by the Secretary of State, who was authorised by executive order to implement the AECA. 22 C.F.R. 120.4(a) allows for a "commodity jurisdiction procedure" by which the Office of Defense Trade Controls ("ODTC") determines if an article or service is covered by the USML when doubt exists about an item.
20. See 22 U.S.C. 2778 (a) (1).
21. 22 U.S.C. 2778(b)(2) provides that once an item is on the USML, and unless otherwise exempted, a defence article or service requires a licence before it can be imported or exported.
22. See the Personal Use Exception to the ITAR, 61 FR 6111, February 16, 1996. An online copy is available from Michael Froomkin's web site at http://www.viper.law.miami.edu/~froomkin
23. Generally available software includes encryption software distributed over the Internet, widely offered for sale or transfer in the U.S. (including software disseminated as shareware or freeware), or preloaded on computer hardware.