The Ethics of Key Escrow for Computer Encryption

In this day and age of technology we rely on the internet for almost all facets of daily life. Commerce, shipping and communication all revolve around the internet in some way. We also depend on computer encryption and security to keep our confidential information safe and away from prying eyes. Would we feel safe if the Government had the keys to this technology able to read trade secrets and monitor electronic money transfers. If we look at it in this light, we would most likely protest this invasion of privacy and fight against this idea.

However. from the government's point of view, this is also the age of terrorism where threats range from nuclear 'dirty-bomb' attacks to the release of a biological-weapon, an event that could bring the country to its knees by killing or seriously harming the majority of the workforce. Terrorists are spread out across the globe and have covert communications network to convey their plans. They use common encryption algorithms to keep their communications secure and out of the hands of law enforcement. Would it be justified for the major Governments around the world to have a copy of the private key to open any digital lock, to intercept and decrypt enemy communications. Would it be better to know that the law enforcement agencies of the world had the tools to read any terrorist plot, or would it seem worse, knowing that your credit card number was readable by foreign governments, where corrupt officials might be harvesting them for their own purposes. Is it ethical for law enforcement agencies to have a master key for all strong computer encryption algorithms? This paper will try to weigh out these differences in this paper and also give readers a background information of both computer encryption and

how it is the backbone of the internet. This paper will be divided into a few discrete portions: the history of encryption and its many uses today, a brief overview of the technology behind encryption algorithms, the issues regarding the topic, the ups and the downs of both sides and finally will conclude on the issue, state my opinion and come to a close.

The cryptography of today has evolved immensely from its roots. The earliest know use or some sort of system to obscure text dates back to around 1900 BC when Egyptian scribes used a made up hieroglyphic alphabet to keep the text secret (Depuis). It then advanced, through the time of the Greeks, the Romans, and into today. This progression of the strength of cryptography has been necessary to keep one step ahead of those who are trying to break the code (Depuis).

Encryption has many uses in today's world. It is used in many applications from Today, encryption is used for almost everything to do with computers. When you log on to an e-commerce site you get forwarded to a secure site that uses 128-bit Secure Socket Layer encryption. Your web browser and the web server trade public keys (explained later) and all further communications (credit cards, social security numbers) are secured with a 128 character password. If a cracker (computer criminal) were to sniff the packets (or monitor all the data) between the computer user and the server all that he would see would be gibberish.

Computer encryption is also relied upon by businesses around the world. Today, more and more people from around the world are using the internet to communicate amongst themselves. They use encryption algorithms such as Pretty Good Privacy (PGP), Multipurpose Internet Mail Extensions (MIME) and other encryption systems to keep

their now ideas and financial agreements out of the hand of their competitors. The most popular method of communication is e-mail, with millions of messages being sent everyday and almost everyone of them is like an open book. They are transmitted in the clear (readable by all) and are stored on most of the mail servers that they hop from. People who are tech savvy, or have need for high e-mail security can use PGP or MIME to encrypt and sign their messages to ensure that only the intended recipient can decode and read the email and any attachments.

The final use of encryption is for data security. To protect from burglary and corporate espionage many companies have policies to make sure that their employees keep all private files under lock and key. so to speak. When enterprise's back up their data, they encrypt it in case of data theft. If for example, a cracker were able to compromise the main file server at company X and access all of company X's files the files would be useless because they would be encrypted. Some commercial products encrypt your data so that if the hard drive of a computer is stolen the data is useless.

Many people of today's generation have experimented with codes and secret agent type activities when they were young. However, computer encryption is much different. There are two main types of encryption, symmetrical and asymmetrical. The former means that the same password used to encrypt the data is used to decrypt it. This type is used mostly for data security as normally the same person is trying to decrypt the information as the one who encrypted it. A common encryption algorithm that uses symmetrical encryption is known as Blowfish. Blowfish is completely public domain and open source. It is used in many security products, both commercial and open source (Schneier).

The latter type of encryption, asymmetrical, is quite a bit more complex. It allows two people to encrypt data for the other one to read without sharing passwords. Each user can have their own password and using something called a 'Public Key'. This type of encryption is used much more common. It is used when sending e-mails, digitally signing files and text and browsing secure sites. When you encrypt a file (which could be text) you use your 'Private Key' and the intended recipient's Public Key to encrypt the data. This generates a cypher text, (encrypted text files encased in special headers and footers called armor) that can be deciphered by the recipient's Private Key. One can encrypt data to multiple Public Keys, allowing for one person to send an email containing secure information to many people, and have all of them decrypt the data with their own passphrase.

All of these examples show a typical encryption model without the use of key escrow. Key escrow has been a topic of hot debate in the past decade. The idea behind key escrow is that when a key is generated a copy of the private key is sent to a trusted third party (in this case, the government) where it be kept safe and you could recover it in case you lost the key. However, by doing so, you grant the government access to your key. This key can be used to forge documents and decrypt and encrypted data that is encrypted with the key. Naturally, these keys would not be used unless there was a warrant. The next section of the paper will discuss these issues (NRC).

These days the media and our government highlights the threat of attack from rogue states and terrorist factions. The government uses a multitude of methods to try and protect its citizens, ranging from offensive to the covert. This includes the interception of encrypted communications. Without key escrow, the cracking of codes is relegated to

super computers that try every possible password. This is a very slow and tedious process with no guarantee for success. This is not a good situation for the law enforcement agencies around the world. Most of the communications intercepted are time critical and need to be decrypted before the encrypted data becomes obsolete. If law enforcement had the private keys to these messages, they would be able to decipher them almost instantly. From those intercepted and decrypted messages they could discover troop movements and know what planned attacks are coming. Key escrow could in theory reduce the threat of terrorism.

On the other hand, many online privacy advocacy groups like the Electronic Privacy Information Center (EPIC) and the Electronic Frontier Foundation (EFF) have been against the use of key escrow from the start. They claim that it is an invasion of privacy and is unlawful (in the US at least). They claim that this could used recklessly. For example, the government could screen emails from people the law enforcement doesn't have warrants for. It would be easy for governments abuse this power, and hard for privacy watchdog groups to monitor.

There have been attempts in the past to monitor online communications, such as the famed Echelon project. This project was headed up by the National Security Administration (NSA) in the late 1940s to monitor all communications around the globe. It claimed to only monitor suspects, however, no source code for the programs were ever released, nor was there enough information to ensure that only suspects with warrants were being monitored. Because of this, internet users have no idea if all of their communications were being watched, or only those of criminal suspects. The project has since been claimed to have been shut down by the NSA (Poole).

The most widespread attempt to bring key escrow to the masses has been project Clipper Chip and project Capstone. These two are very similar and use the same encryption algorithm (the secret, non-disclosed Skipjack algorithm), but the former is for voice communication and the latter is for data security and online communication. The principle is simple. A small micro-chip is used to encrypt all data (voice or packets), this encrypted data also includes a short section called the "Law Enforcement Access Field" (LEAF) that contains the chip's hard-coded serial number and the hard-coded unit key. The LEAF is encrypted with the key escrow's public key. When the law enforcement agency come across an encrypted communication, then could then decrypt it. The advantages of this system is it let users get a stronger encryption algorithm (80 character long password for Skipjack vs. the 56 character password DES that was currently allowed for civilians) so their communications and data were more secure, and allow for the government to be able to decipher these more secure communications (NRC).

Now that a good background of the changes that key escrow will bring about has been established, both sides of the argument can be evaluated. On the positive side of this debate, in countries where the use of strong cryptography is not permitted, it would allow for citizens to protect their financial and other confidential data using a stronger algorithm. It would also allow for the government to be able to intercept and decrypt rogue communications. This would cut down on crime both on the internet and off it. It would also give law enforcement agencies the upper hand in predicting and stopping terrorist threats.

The pros of this idea are apparent from the government's point of view. They can give their citizens a stronger sense of security from rogue states and terrorist factions.

They also have the ability to crack encrypted communications almost instantly if the need arises. In nations that are not allowed by the US government to use strong encryption, the citizens can protect their online communications better than they could without key escrow. If the government needed to monitor terrorist suspects email, it is an option with key escrow. Without the need to crack terrorist communications, the government would have less resource requirements, leading to a lower defense bill. It would also give the armed forces more accurate and timely warning about strikes and troop movements. This would again lead to less guesswork in military operations, making war and safer and more exact occupation.

However, as with all proposed changes, there are aspects of this idea that can be seen as negative. Firstly, who would own the central key server. There is already plenty of debate about who will own and manage the central servers that provide the pillars of the internet. If the US proposed to control the key escrow servers, then they would have a huge advantage. They would be able to monitor nations that they disagreed with and basically do what they pleased. The second main objection to the proposal is if key escrow were to become a reality, could the governments in power be trusted to only use the master private keys for lawful practices. With almost unlimited possibilities to gain from exploiting such a resource, would the population feel safe. Because of this threat, computer scientists and mathematicians might team up to create another encryption algorithm that would be without the government's key escrow. The third and last issue with key escrow is the possibility of server compromise. With goal of decrypting and reading all internet communications, a team of highly skilled crackers could perhaps get access to the key escrow servers and steal the private key. Once this happened, all current

encryption algorithms would be unsafe and new ones would have to be developed, a daunting and difficult task.

This debate about key escrow has been ongoing for many years. Programs like the Clipper Chip program have been created and unsuccessfully tried in the United States. Factors which have led to the downfall of these pilot programs include the rejection by the EU to use key escrow and the widespread distrust of many in the computer industry (EPIC). Originally the private keys were to be kept by the government but this proposal was widely rejected. In response, the government then proposed to designate a few private companies to be the "trusted third parties" that would keep the keys for recovery. With this scenario, in the event that the government needed the private keys for an investigation, the keys could be requested from the escrow service. Thus the people who used the escrowed system could use stronger encryption algorithms and be free of most export regulations. After this change to the key escrow program was proposed, resistance died down. However, before this could be implemented, the private sector created even stronger algorithms, which were released as open source. As a result the government lost their foothold in this issue and consequently relinquished most efforts to implement key escrow.

To conclude, I believe that the negative aspects of key escrow outweigh the benefits. While the short-term financial savings of key escrow would be appealing, the possibility of an internet-dictatorship or a data compromise would be a far worse outcome. Consequently, my opinion is that a non-regulated internet is the only way to ensure privacy and freedom of speech for all. Nonetheless, since this choice will change the way all people use the internet, it should be discussed broadly both among world

leaders and within the general population.

Works Cited:

Abelson, Al et al. “The Risks Of "Key Recovery," "Key Escrow," And "Trusted Third-Party" Encryption | 1998”. Center for Democracy and Technology. 1998. CDT. 13 Oct. 2005 <http://www.cdt.org/crypto/risks98/>.

CNN. “Bush: Secret wiretaps have disrupted potential attacks”. CNN.com. 17 Dec. 2005. CNN. 31 Dec. 2005. <http://www.cnn.com/2005/POLITICS/12/19/nsa/index.html>.

Computer Security Department. “Encryption Key Recovery”. NIST. 2005. NIST. 15 Oct. 2005 <http://csrc.nist.gov/keyrecovery/>.

Depuis, Clement. “A Short History of Crypto”. Crypto Machines. 2005. 14 Oct. 2005 <http://www.jproc.ca/crypto/crypto_hist.html>.

EFF, The. “Key Escrow, Key Recovery, Trusted Third Parties & Govt. Access to Keys”. Electronic Frontier Foundation. 2005. EFF. 24 Sept. 2005 <http://www.eff.org/Privacy/Key_escrow/>.

EPIC, The. “Cryptography Policy”. Electronic Privacy Information Center. 2005. EPIC. 24 Sept. 2005 <http://www.epic.org/crypto/>.

Mao, Wenbo. “Publicly Veriable Partial Key Escrow”. Hewlett-Packard Laboratories. 1997. 14 Oct. 2005. <http://scholar.google.com/scholar?hl=en&lr=&q=cache:_rQ04c0SpgMJ:www.ussrback.com/cryptopapers/1997/www.hpl.hp.co.uk/people/wm/papers/pvpke.ps+key+escrow>.

Mao, Wenbo. “Veriable Escrowed Signature”. Hewlett-Packard Laboratories. 1986. 14 Oct. 2005. <http://scholar.google.com/scholar?hl=en&lr=&q=cache:iQxAk8k3EI0J:www.ussrback.com/cryptopapers/1997/www.hpl.hp.co.uk/people/wm/papers/escr-sig.ps+key+escrow>.

NRC, The. “Cryptography's Role in Securing the Information Society”. Electronic Privacy Information Center. 30 May 1996. 14 Oct. 2005. <http://www.eff.org/Privacy/Key_escrow/Clipper_III/9605_nrc_cryptopolicy_draft.report>.

Poole, Patrick. “Echelon: America's Secret Global Surveillance Network”. Patrick S. Poole. 2000. 29 Oct. 2005. <http://fly.hiwaay.net/~pspoole/echelon.html>.

Roach, Russel. “Cryptography: Code is the Key”. Cyberarmy Privacy Commision. 2005. CPC. 24 Sep. 2005 <http://www.cpcnet.org/pwatch/index.php?Release=4&PHPSESSID=6e30d15c5681f1bb7179bc6e64554e8c>.

Schneier, Bruce. “The Blowfish Encryption Algorithm”. Counterpane Internet Security. 27 Apr. 2005. 16 Oct. 2005. <http://www.schneier.com/blowfish.html>.