

Cryptology: Privacy or Terrorism in the Digital Age

1. What is the problem itself?

In the age of the Internet with instantaneous communication and purchases being made every second of every day, there needs to be some form of security in place to prevent private information from falling into the wrong hands. There are various programs and algorithms that have been developed to encrypt data to keep information private, but these steps forward have fallen under attack from law enforcement agencies as being tools for terrorists and drug dealers to keep their plans from being uncovered. Here arises a problem; how to protect the transactions and communications of innocent civilians, while uncovering the plots of criminals.

The problem of web security can be corrected, for the most part, with the advancement of one application: Web Browsers. Web browsers are the central application for the transmission of data across the Internet. A current limitation on the encryption standards in web browsers prevents the increase in security needed to maintain total privacy.

2. What are the problem's effects?

- (1) Encryption prevents law enforcement agencies from finding out about criminal intentions.

(2) Lack of encryption would destroy online trading and purchasing.

3. What are the problem's causes?

The encryption standard, RSA, is based on one-way mathematical functions and prime numbers. One-way mathematical functions are named in such that they are easy to compute, but difficult to reverse. This is enhanced when large prime numbers are added to the equation. In this case, three keys are needed: two large private keys, and one large public key. The private keys are used to compute the public key. Since there exists no fast and easy way to factor prime numbers, large prime numbers are used as the private keys. Because of the nature of the RSA algorithm, any information encrypted with the algorithm becomes impractical to attempt to decipher. Any average citizen can therefore protect themselves from their data being stolen over communication lines, but criminals can also keep their secrets well hidden.

The current generation of web browsers use 128-bit encryption to pass secure data across the Internet. The security associated with the RSA algorithm is dependent on the length of the keys used to encrypt and decrypt the messages. With the current growing power of computers, the ability to factor large numbers – while faster algorithms have not been found – is increasing because of the computation speed of modern processors. For complete security, it is estimated that current keys need to be at least 1024 bits long to make it impractical for people with access to large clusters of computing power to attempt to break the keys. Current encryption laws restrict the lengths of keys that can be used in encryption software, thus guaranteeing that the government, with its computational resources, can break any encryption scheme available on the market today.

4. What, if anything, is being done to solve the problem – and does this create further problems?

The government has taken on the job of finding a middle ground solution to the privacy concern. Their idea, Key Escrow, would follow in the RSA footsteps, but would keep a copy of one of the private keys in a government agency and the other key in a separate agency. Their thoughts were that law enforcement agencies can petition the key holding agencies to obtain the keys and there for decipher the information needed. This process is similar to the petitioning of the courts to obtain permission to perform wire taps on suspected criminals.

Opposition to this method has arisen from privacy groups such as the Electron Freedom Foundation (EFF). Their argument parallels the keeping of private keys to allowing the government to keep a copy of your house key. Allowing the government to keep a copy of your house key would allow them access to your house if they suspected you of wrong doing, but also carries the possibility of a bad cop taking your key and entering you house any time they please. Giving the government copies of private keys would allow them access to all the information they want, reason or not.

5. What kind of thing is needed to solve the problem?

There needs to exist the guarantee of privacy over normal everyday communications methods, while allowing law enforcement agencies the ability to read the information if there exists evidence that the information being transmitted is of criminal intent; or one of the sides needs to give in for the better good for the whole.

6. What are the possible solutions?

(1) Government's Key Escrow is placed into effect in all new technology. The location of the data must be well secure and accessible via court order only.

(2) Encryption technology grows without government intervention. Enhance the security for people and corporations to conduct business in a secure environment.

(3) A middle ground is found that satisfies both parties.

7. Which solution is the best?

The middle ground is found. Since this option is not in the foreseeable future, encryption technology should be allowed to grow without interference.

Microsoft should take the lead in implementing an increase in web security with their Internet Explorer web browser. Microsoft is a big corporation, a leader in the software industry, and with leadership comes responsibility. Microsoft should set the standard by raising the bar on Internet security by increasing their encryption keys from 128 to 256-bit. This increase in number of bits in the encryption keys is not perfect, but would delay decryption by an exponential factor and start the ball rolling on the bigger picture, the elimination of encryption restricting laws.

8. How should the solution be implemented?

Microsoft could release the new browser as part of a standard upgrade, or could wait until the release of their new operating system and roll out an entire package based on an increased encryption key size.

9. What is the background to the problem?

Types of ciphers: Substitution, Random, Symmetric, and Asymmetric.

- Substitution Cipher – replace each word or letter with another symbol. To decrypt, simply reverse the cipher. Examples include: ASCII, Enigma, and the Caesar Cipher
- Random Substitution – message is broken down into equal blocks. Pseudo-random numbers are computed from a seeded number generator. Each block has a pseudo-random number added to its ASCII value to mask the message. The message is decrypted using the same seed value in the number generator and subtracting from the message blocks. Examples include: Word processor encryption schemes.
- Symmetric Cryptosystems – messages are broken down into equal blocks. Bits within the blocks are scrambled and XOR'ed with a key value (64-256 bits long). The blocks are then put through a series of substitutions before the final encrypted message is completed. The message is decrypted with the key value. Examples include: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Windows XP key validation, and the Japanese cipher Camellia.
- Asymmetric Cryptosystems – One way mathematical formulas are used to encrypt a message. The key difference separating asymmetric schemes from symmetric schemes is that the key used to encrypt a message with the asymmetric cipher is not the key used to decrypt the message.

Examples include: Web browsers (128-bit key encryption), Rivest-Shamir-Adleman (RSA) algorithm.

Prime numbers – numbers in which are divisible by only two numbers: one and itself. Prime numbers are the keys used in Asymmetric Cryptosystems (most famously in the RSA algorithm) and selected because of the difficulty in factoring numbers and the unpredictability of prime numbers.

Key Escrow – An arrangement in which the keys needed to decrypt encrypted data (messages) must be held by a third party – only to be delivered after the fulfillment of specified conditions – so that government agencies can obtain the keys to decrypt messages which they suspect the data to be relevant to national security.

Cryptology – the science of analyzing and deciphering codes and ciphers.

Target Audience: Microsoft Corporation, Web browser division.

Report Type: Recommendation Report

Resources:

Singh, Simon. *The Code Book: the Science of Secrecy from Ancient Egypt to Quantum Cryptology*. New York: Anchor Books, 1999. 411 pages.