ABI SOFTWARE DEVELOPMENT

Written by: Adam Berent

Regulating Cryptography **v1.4**

In light of recent events new concern has arisen on the general availability of strong encryption software, and how this software might be abused for illegal or immoral actions. There is new fear that terrorists may enjoy access to strong cryptographic devices to communicate with total privacy. One of the suggested solutions is to force regulation of cryptography there by weaken the encryption software we are all allowed to use.

Regulating or banning strong encryption will weaken our position to defend ourselves from criminals and terrorists. Week encryption will mean that we can read their files but it will also mean that they have the possibility to read ours. Considering that the number of legitimate users far outweighs the illegitimate ones, this is not a good prospect.

The government has proposed to implement a key escrow encryption system, which would allow a backdoor to access your secured data. Key escrow does not work, simply because there is nothing stopping a terrorist from using non-key escrow software written outside of the U.S.

There are thousands of businesses that produce strong cryptography outside of the U.S. There will be nothing stopping a terrorist from circumventing our laws and purchasing a product from a country that does not have a ban on strong cryptography.

Cryptography is math. It is impossible to ban math. There will always be material available to the public on the various cryptographic algorithms available hence making the creation of strong cryptographic software a possibility.

The public is often not aware the possibility to circumvent the encryption software by using tools such as keystroke sniffers Trojan Horses or viruses. There are hundreds of tools available and being written daily that will allow not only large government agencies but also any knowledgeable person's access to encrypted data. What good is 448 bit encryption if you capture the key as the user types it? Just not long ago U.S. District Judge Nicholas Politan ruled that it was perfectly acceptable for FBI agents armed with a court order to plant a keystroke sniffer in gangster's Nicodemo S. Scarfo's office, and monitor his PC's output. By doing this the FBI successfully circumvented the encryption software called PGP that Scarfo used to encrypt his documents. Strong encryption will not prevent law enforcement agencies from doing their job; it simply means that they have to use software tools as advanced as their opponents.

Strong cryptography can be abused, but the benefits far outweigh the risks. We often forget that our banking transactions, medical information and computer networks are protected by encryption. Human rights workers and reporters in third world countries often use cryptography to protect information that can be dangerous to their lives. Encryption prevents criminals from accessing our data. We can continue to enjoy these benefits or we can jeopardize our own security by banning or hindering strong encryption.

 If you would like to contact me feel free to do so at aberent@abisoft.net or visit www.abisoft.net.