Generating and Distributing Encryption Keys

by Steve Tassio
15 September 2013

The purpose of this document is to give the reader an overview of what takes to effect secure personal Internet communications by using the SDC Private Messenger. By inference the reader will discover that personal communications have never been secure on the Internet.

The primary encryption algorithm used in the Private Messenger is known as 256 bit AES. The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The 256 bit nomenclature specifies the length of the encryption key. AES is known as a symmetric algorithm. That means the encryption key and the decryption keys are one and the same.

A brute force attack upon AES is an attack wherein each and every key is tried until the encrypted data is recovered. With a 256 bit key that means 2^{256} (1×10^{77}) number of attempts. The only known method to short circuit brute force reduced the number of attempts to $2^{254.2}$. A reduction for sure but what does this mean in practical terms? After all 256 bit AES is authorized for Top Secret DOD/government documents.

Using a faster supercomputer (as per Wikipedia): 10.51 Pentaflops = 10.51×10^{15} Flops [Flops = Floating point operations per second] and the assumption that a DES 56 bit key could be recovered in one second it would take approximately 3.31×10^{56} YEARS to try all the keys. Given that this is not a practical way to recover encrypted data how do adversaries hope to succeed in their attacks?

The first thing that comes to mind is via the Hollywood style bribery, beatings or burglary techniques to acquire the keys. If for the sake of argument we say that the adversary Mallet has coerced a key from Bob to find out what he has sent to Alice. And if Bob and Alice have correctly designed their key handling protocols Mallet may discover he has just blown his cover and obtained yesterday's session

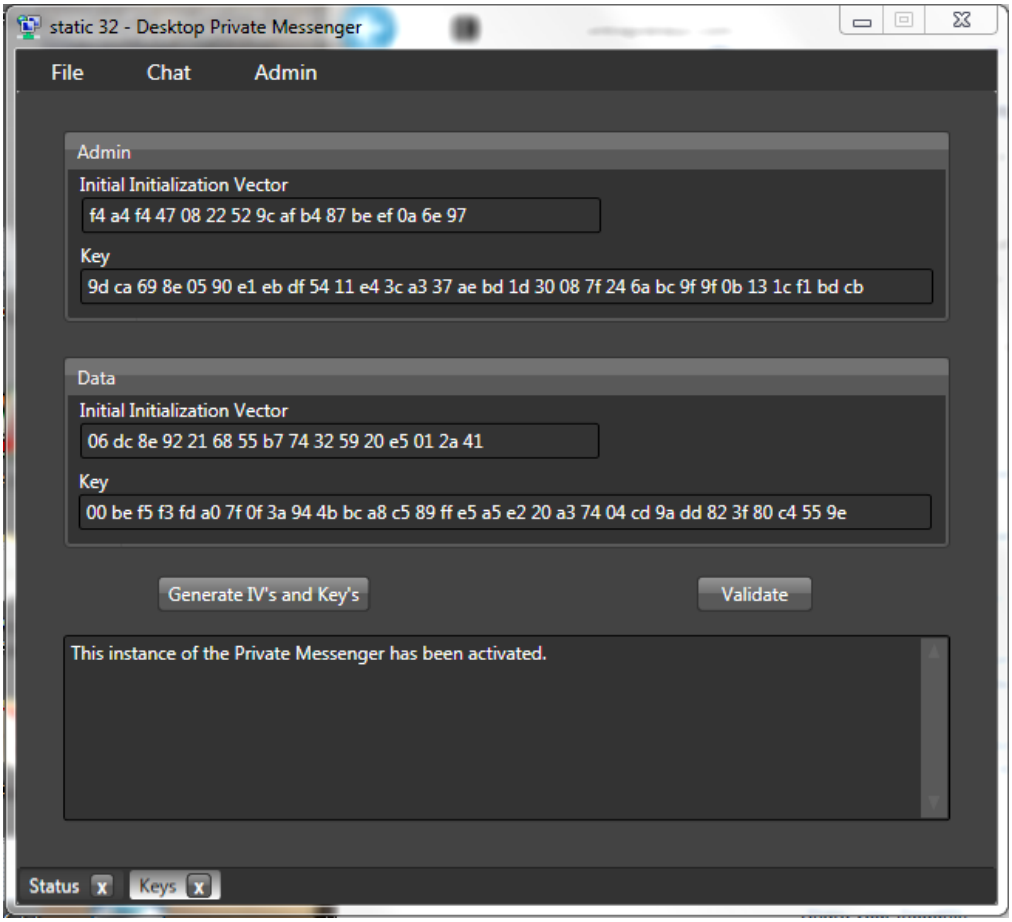
key or at best todays. Alice is alerted via their protocol by something that didn't happen and therefore the current session key is compromised and she takes appropriate counter measures.

If Mallet purchased or stole a key from Bob such that Alice was unaware then other countermeasures outside the communications channel must alert Alice to the danger. It's hard to imagine that the average Joe has information that men of incredibly small minds deem valuable but world headlines have established that type of lust as an on ongoing daily ritual for government agencies paid for by average Joe to protect his life and property.

If Bob is honest and he and Alice have correctly distributed and protected their keys where is the weakness now? It lies in the generation of the key values. If keys are based upon passwords or pass phrases then the possible combinations of key values is a microscopic subset of the total available key values. Suddenly searching for a key in such a small region of the 'number space' becomes a viable thing with present day computing power.

The Private Messenger utilizes a cryptographically strong random number generator as the basis for the keys it generates. Such a technique requires no input from the user and hence is not subject to any kind of bias or preference from the user. Randomness however does not mean that the generated sequence of numbers contains wildly varying numbers. Two 256 bit random numbers can be different by only one bit but look very different to the eye. In other words the two keys can be related by their portions that are identical and not separated by the one different bit.

To help prevent this relationship the Private Messenger takes the random 256 bit key and passes it through a one way hash called SHA-256. A one way hash is a cryptographic function that transforms one or more bytes of data to a fixed length output block of data in this case 256 bits long. A one way hash is just that. One way. The hash output cannot be used to recover the input data. In the Private Messenger this is valuable because it can never be determined what the original keys were let alone if the original generated keys are related.



This view of the Private Messenger shows keys and initial Initialization Vectors that have been generated by the Private Messenger. Note the two Group Boxes labeled ‘Admin’ and ‘Data’. Because the Private Messenger does not rely on servers for the orchestration of chats the administration of the chat sessions is handled by each Messenger in the current group. This house keeping is called ‘Admin’ and is also encrypted by the 256 bit AES hence the key. Having separate keys for Admin and Data divides the Private Messenger into two main functional pieces that cannot communicate with each other.

Note the ‘Initial Initialization Vectors’ for each key. These are cryptographically random values. The AES algorithm uses an IV with each operation whether encrypting or decrypting. The IV is ‘mixed’ with your message data before being output in its encrypted form. This mixing is needed because the

AES is what is known as a block cipher. In this case the output block is 128 bits long. A block cipher will produce the same cipher text for the same plain text and key inputs. This can allow estimates of the plaintext to be made because of the repeating patterns. By mixing random data the output from block to block is completely different. The rules for the IV are that it must be unique and random for each block operation. It does not need to secret. The IV doesn't aid in the encryption process. It is itself part of the encrypted data. The Private Messenger generates a new IV for each chat message sent and the recipients use it to add with the key and cipher text to the decryption process.

The Private Messenger provides the user with the means to generate competent keys and use them with a competent algorithm. What can go wrong now to give Mallet the upper hand? The only thing left is that Bob and Alice do not share and protect their keys competently. This is where paranoia and creativity combine together to form the key protection and distribution protocol. The creativity part is where Bob and Alice devise the means to distribute keys from time to time on a predetermined schedule. The paranoia part specifies the degree of covertness in key transfers and the frequency of the transfers.

Cryptography is about the value of thing protected. For ordinary citizens the value is assessed by the person to whom the secret belongs. Some people may feel that governments and other adversaries have no right to their weekend BBQ plans. Others may feel that social banter does not need encryption. This type of evaluation reveals what needs to be encrypted. The next consideration is how often is the valuable communication to occur? The frequency and volume of encrypted traffic can help estimate how often keys should be changed. Generally the less time a key is valid is better. This reduces losses if Mallet gets his hands on a key. This is also why the golden rule that new session keys are never transmitted in the current session.

Then to go one step further in key distribution scenarios, at random intervals change the protocol that is used to effect the actual transfer of the keys.

Built into the Private Messenger is the ability to distribute the keys that it generated or the user entered and distribute them securely over the Internet. This is accomplished by using the Elliptic Curve Diffie-Hellman key exchange protocol. This method is used by governments, banks, corporations and others to avoid the logistics of physical key distribution protocols. In the DH protocol two users exchange public keys (not to be confused with RSA public keys) the DH process combines the each users private key with the others public key. This creates an identical Key Encryption Key on each user's computer. This KEK never leaves the users machine and is used only once before disposal. One of the parties designated as the Keymaster uses his KEK to encrypt new keys then sends them to the remote user. The remote user decrypts the new keys with his KEK. This ends the life cycle of the KEK. Each user sets the new session keys both Admin and Data as the current session keys and chatting resumes after all of the users in the group have re-registered.

To transfer keys physically there are several types of password protected, encrypted, tamper proof USB sticks to use as the transfer medium. Some have serial numbers so that each one can be protected with its own unique cryptographically strong password. The user is free to select any means or a combination of means to transfer all or parts of the new key. The keys must never be stored on the computer in use. It must be 'ok' to lose the computer. Without the keys the Private Messenger is literally like that old pay phone in the booth. The Private Messenger retains no records of contacts or messages like the pay phone. The Private Messenger only works when it is in use nothing of the past can be recovered from it in the event of computer tampering or theft.

By now it is obvious that Internet communications have never been secure for the ordinary citizen. Freedom and security are not conditions that occur in nature. Both are procured and maintained by conscious willful effort. While the information lost to adversaries on the Internet to date cannot be recovered and protected with the SDC Private Messenger chosen new communications are protected from prying and undeserving eyes.

for more info: stephen.tassio@topsecretcommunications.com

www.topsecretcommunications.com