Dynamic Encryption

Background

For many years it was claimed that the NSA, the US intelligence agency, are listening in to (all) the communication in the world. In 2013, Edward Snowden told the world that this is in fact the case.

In the early 70s IBM started working on encryption algorithms for computers, and IBM submitted their algorithm, Lucifer, as a candidate for a call of proposals from the National Bureau of Standards (now NIST). Lucifer encrypts 64 bits of data using a 128-bit key. NSA changed this design in various ways, most importantly, the key size was reduced to 64 bits, of which eight bits are not used. The standard was named DES, Data Encryption Standard and published 1975.

The cryptographic community increased their knowledge in symmetric encryption in the late 80s, and in particular in the early 90s, a number of young researchers came to the field. By the mid 90s the community was able to construct very strong encryption algorithms that the government agencies were not able to break. Still it is conceivable that the these agencies at that time were ahead of the academics, in particular in terms of decrypting knowledge and capabilities.

Clipper Chip

In 1993, the US government (Clinton administration) tried to introduce, the so- called key-escrow systems. These are strong encryption systems that were public but constructed such that the government was able to decrypt the encrypted data. The NSA developed a chipset, named the Clipper chip, intended to be adapted into all telephones. Skipjack was the name assigned to the encryption algorithm inside the system. At first Skipjack was classified and kept secret, but it was later declassified and published by the NSA in 1998. The academic community reacted strongly against such systems, and after some years of debate, the escrow systems were abandoned (or skipped!).

Advanced Encryption Standard

In 1997, the US government announced a competition to supply the next federal encryption system, to be called the Advanced Encryption

Standard, short the AES. In 2001 the winner was selected and the standard was ready to go November 2011. At first it may seem strange that the US government initiates the development of a strong encryption algorithm for public use. But by a second thought, this was probably a very good move.

The cryptology researchers were getting very good at constructing strong encryption algorithms, that no agency could break. So the development and employment of the AES would get everybody (or most) people to use the same algorithm. This is very beneficial for agencies, since they would only have to try to cryptanalyse one algorithm, but maybe even more important, they would only have to invest in decrypting hardware for just one algorithm. It is known that practical attacks on AES or similar algorithms, involve breaking the key generation algorithm rather than the encryption algorithm and exploiting non- randomness in the keys exchanged. With the same encryption algorithm used everywhere, testing potential values of the keys would become much easier.

Dynamic encryption

To establish a secure connection between two parties, the involved parties must generate a good cryptographic key and exchange this key between them in a secure manner. It is a well-known security advice to change the value of the keys as often as possible. In addition, the parties should change the encryption system often, possibly for every new communication.

In the dynamic encryption approach, the sender chooses an encryption algorithm and transmits the algorithm to the receiver. Then they act like in a traditional encryption setup. For maximum security the parties should change the key frequently along with changing the cryptosystems.

The exchanged cryptosystems do not have to be kept secret, but to avoid attackers modifying the transmitted encryption systems, one should add an authentication tag to the cryptosystems. It is possible to construct a dynamic encryption system, such that all encryption algorithms ever used are at least as secure as the AES, but inarguably much more secure. If implemented correctly, such a dynamic

encryption system is practically unbreakable. The concept of dynamic encryption was invented at the Technical University of Denmark (DTU) by Professor Lars R. Knudsen (patent pending).

LRK. 2019.