



Unbreakability of Encryption & DLT Standard

Lawlesh Tiwari

Senior System Executive

Cognizant Technology Solutions

Pune, India

Abstract: Cryptography is taught with the basic rule that there is no such thing as an unbreakable encryption because "If someone tries enough keys he is bound to get the right one," which gives rise to the basis of the brute force attack. Brute force attack, or exhaustive key search, is a strategy that can, in theory, be used against any encrypted data. It involves systematically checking all possible keys until the correct key is found. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute-force attack against it. The so-called Landauer limit implied by the laws of physics sets a lower limit on the energy required to perform a computation of kT and the processing speed and memory requirements also set physical barriers. But with the exponential growth of computing industry supercomputers having computing capacities of 20 Peta-FLOPS and beyond have been made and a number of systems that were originally thought to be impossible to crack by brute force have nevertheless been cracked. A truly unbreakable code must not have an obtainable key. A theory for this is for the code breaker to not realize that he has broken the code even if he has the key. For example, the key and cleartext may change according to a random time variable so that even when the code has been broken the encrypted text could still represent any other meaning. This is however very impractical and has never been able to be put into effect. This paper discusses unbreakability of encryptions and proposes an encryption that can be called truly unbreakable. This paper also discusses a way of implementing an encryption that is contextually breakable and hence can only be used by random common users not criminals and terrorists because for them the code can be broken.

Keywords: Brute Force; One-Time Pad; Key size; Key space; Key Transportation

I. Introduction

Modern world is moving towards cyber globe. In an era where meetings, conversations, decision making, information sharing and even social aspects of life are moving online and offline on digital and cyber world, it is necessary to provide for security and privacy on cyber and digital world which is provided cryptography. The world of cryptography has come from historic roots where cryptography was a physical world phenomenon with no particular definition except communication with codes. In the modern era the cryptographic scenario has shifted and firmed. Modern Cryptographic principles state

- Principle 1. The first step in solving any cryptographic problem is the formulation of a rigorous and precise definition of security.
- Principle 2. When the security of a cryptographic construction relies on an unproven assumption, this assumption must be precisely stated. Furthermore, the assumption should be as minimal as possible.
- Principle 3. Cryptographic constructions should be accompanied with a rigorous proof of security with respect to a definition formulated according to principle 1, and relative to an assumption stated as in principle 2 (if an assumption is needed at all).

As with the physical world the cyber world has presented opportunities to the miscreants and has presented them a lot of them. With the physical world with lot of evolution and finally coming to term and controllability of antisocial elements the cyber world in its teenage is the prime meeting place and target of terrorists and other outlaws.

Criminals use encryption in four domains: voice, fax, and data communications; electronic mail; files stored on the computers of individual criminals and criminal enterprises; and information posted in public places on computer networks. They use tools for hiding crimes through anonymity: anonymous remailers, anonymous digital cash, computer penetration and looping, cellular phone cloning, and cellular phone cards and tools for concealing information: passwords, digital compression, steganography, remote storage, and audit disabling. It is well known that Al Qaeda has been specifically recruiting persons with a computer sciences background and has been training its operatives in computer sciences. The use of the Internet by other terrorist groups such as the ETA is also extensively documented.

In this cases many criminal & terrorist investigation law and security organization debate that it would be better if encryptions remain feeble so that they can be broken and thus not complicate the task of law enforcement as was the case in 1970s and 80s.

But Encryption is critical to building a secure and trusted global information infrastructure for communications and electronic commerce today. While the above demands may better defend our society, we

should also consider the costs of applying such measures. Such measures can hand authoritarian governments and agencies with little public accountability tools with which to violate privacy, curtail the free flow of information, and restrict freedom of expression, thus adding a heavy price in terms of diminished civil liberties to the high toll exacted by terrorism itself. Electronic Frontier Foundation published a report in January 2011 which states that since 9/11 there were approximately 40,000 violations of law and thus breach of user privacy. Verizon in its 2012 data breach report declared 855 incidents, 174 million compromised records of data espionage. EFF claims NSA is already listening to everything you say.

II. Brute Force and Breakability

A brute-force attack, or exhaustive key search, is a strategy that can, in theory, be used against any encrypted data. It involves systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire search space. Given a ciphertext c , the adversary can decrypt c using all keys $k \in K$. This gives a list of all possible messages to which c can possibly correspond. Since this list cannot contain all of M (because $|K| < |M|$.) The adversary can again try decrypting each of these ciphertexts with all possible keys until it finds a key k for which $\text{Dec}_k(c) = m$. However this m is the assumed clear text until there are a few cipher text and clear text pairs are known. Assumed cleartexts are the clear text that show meaning to the brute force machine according to the artificial intelligence program such as searching the clear text for most common parts of speech or a grammatical structure. Brute force attack is applicable to all encryptions and is bound to break all with enough resources and time.

III. Exceptions and Their Unviability

In 1917, Vernam patented a cipher that obtains perfect secrecy. Approximately 25 years later, Shannon introduced the notion of perfect secrecy and demonstrated that the one-time pad (sometimes known as Vernam's cipher) achieves this level of security. The one-time pad encryption scheme is defined as follows:

- Step 1. Fix an integer $l > 0$. Then the message space M , key space K , and ciphertext space C are all equal to $\{0, 1\}^l$ (i.e., the set of all binary strings of length l).
- Step 2. The key-generation algorithm Gen works by choosing a string from $K = \{0, 1\}^l$ according to the uniform distribution (i.e., each of the 2^l strings in the space is chosen as the key with probability exactly 2^{-l}).
- Step 3. Encryption Enc works as follows: given a key $k \in \{0, 1\}^l$ and a message $m \in \{0, 1\}^l$, output $c = k \oplus m$.
- Step 4. Decryption Dec works as follows: given a key $k \in \{0, 1\}^l$ and a ciphertext $c \in \{0, 1\}^l$, output $m = k \oplus c$.

One time pad provides perfect secrecy because for any cipher text c there are 2^l equally likely keys equally likely clear texts m and as long as the key is new at every use and completely random even know clear text attack cannot decode the key for future use. Unfortunately, this brings forward two important drawbacks of One-time pad to achieve perfect secrecy,

1. Storage and transport of a very long key and in case of unknown message length generation storage and transport of a key of unbound length.
2. One time usage of one key and thus fresh key transport at every new message.

The conditions themselves are not impossible but impractical and unviable for common user. The only use of one time pad (never officially confirmed) is known to be done by US and Soviet Presidents during cold war.

IV. Unbreakable Encryption DLT

A. Algorithm

1) Encryption Algorithm

- Step 1. Generate a permitted Character Space C_p .
- Step 2. Take the Clear Text (C_M) Length C_L .
- Step 3. From C_p generate a completely random key K of length C_L .
- Step 4. Generate Cipher text C_T by applying OneTime pad on clear text with K .
- Step 5. Append K at the end of C_T .
- Step 6. Take the text at the end of step 5 as clear text C_i for next encryption E_i with key K_i and generate cipher text C_f .

2) Decryption Algorithm

- Step 1. Take Cipher Text C_f and key K_i and applying decryption E_d generate C_i .
- Step 2. Split the C_i into two equal length texts. One is the Cipher Text C_T and other is key K .
- Step 3. Apply One-Time Pad and decrypt to Clear Text.

B. Analysis

1) Encryption

The encryption method is based on one time pad with a provision for easy transport of key. It will be analysed for resource load it puts on the user. The resource requirements can be calculated on the largest memory utilizing element in algorithm to be in memory at any instant and the required speed of processing. The largest memory utilizing element in the algorithm comes into action at step 6 so the total required memory on one go processing will be $L(C_i) + L(K_i) + M(E_i)$ (L represents length and M represents memory requirements) or $2L(C_M) + L(K_i) + M(E_i)$.

As $L(K_i)$ is too small in comparison to $2L(C_M) + M(E_i)$ and $2L(C_M)$ is an element dependent on the message so the only element deciding the memory requirements is the second layer of encryption and so the memory requirements are not very high because it is one of the market available symmetric encryption schemes with not exhaustive memory demands. Now to the processing resource, the processing resources are dependent on processing speed requirements. It can be calculate on the minimum processing speed for the processing of the largest operation to complete in the smallest possible time. The step that is largest can be one of the 2nd and 6th so the processing resource need not be extraordinary as both do not require a very high processing rate. The processors of a common PC today are capable of performing well beyond this requirement.

2) Decryption

The decryption method as in all symmetric schemes is the exact opposite of the encryption method it will be analysed for its resource requirements.

The largest memory utilizing element in the algorithm comes into action at step 1 which same as the output of the step 6 of the encryption algorithm so the memory requirements for the Decryption are same as that of Encryption.

The processing resources requirements of decryption are equal to or lower than the encryption and so within the reach of common user.

3) Brute Force

Brute force attack as already been mentioned has been taken as a standard for the strength of any encryption standard. Brute force analysis will pursue the angle of brute force strength of the standard.

The brute force attack against DLT standard will follow the steps as

Step 1. Take Cipher Text C_f and key K_{i1} and applying decryption E_d generate C_{i1} .

Step 2. Split the C_{i1} into two equal length texts. One is the Cipher Text C_{T1} and other is key K_1 .

Step 3. Apply One-Time Pad and decrypt to Clear Text C_1 .

Step 4. Check C_1 if it is a plausible clear text. If yes stop (in most cases) or list it as one clear text. If no repeat from Step 1.

Let's take the keyspace is K_i then total number of clear texts generated equals K_i . Let the probability of a meaningful clear text is be P_M . Let the Contextuality coefficient be C_X . Let T be the time interval it takes to search all of the keyspace

Case I: The most common cases of brute force machines terminate at the first hint of clear text and test the presence of clear text by looking for 3 letter combinations of most common part of English speech. The encryption is completely impervious to these machines as one time pad will produce so one such clear text every $T \cdot P_M / 0.4$ time interval.

Case II: If a highly configured and intelligent machine with brute force capability is asked to run against this standard. It will enlist $K_i \cdot P_M \cdot C_X$ number of clear text that would have to be manually analysed and research to find the right one.

C. Requirement for perfect secrecy

As the analysis presents that the breakability of the encryption can be stated by the number of possible outcomes that are possibly the clear text and thus the least number of possible keys. So the requirements to the unbreakability of the encryption with ambiguity being A

$$K_s \geq A / P_M C_X$$

This way the perfect secrecy requirements are dependent on contextuality and ambiguity requirements. Let's put the ambiguity to 1 million and for common user the contextuality coefficient is almost 1 as they are highly non contextual to the brute force attacker. This is a very trivial requirement as encryption standards with keyspace much greater than even 10^{20} are pretty common these days. A playfair cipher with 64 character space and key length of 11 characters is sufficiently capable of providing this.

D. Usage

The uses of the encryption standard are innumerable and are only dictated by the resource requirements. As the resource requirements and well within the reach of a common user as of this day and computer industry and allied sciences are not going back the use is restricted to no one. As the encryption stand will the best for many years to come and as it employs one encryption layer over one time pad to provide the condition for perfect secrecy with the small key and ease of its transport and exchange, it can be upgraded at whim as more of symmetrical encryption come to knowledge and even if no advances are made into the field, as of this day the

artificial intelligence schema and allied digital surveillance to counter the encryption and bare the life of common user is far from reality in the foreseeable future providing the standard users a guarantee of perfect secrecy for many decades to come.

V. Conclusion

The Cryptographic standard DLT provides for the common user, cyber rights cells as well as Security and Intelligence community. As a list of meaningful clear text is generated and based on the artificial intelligence program or the intelligence of the Analysts a contextual probability analysis can narrow down the list of clear texts considerably but a perfect answer can only be gotten if the clear text is highly contextual like in the case of criminal conversations else there are still a very large number of possible clear texts. So the encryption while providing security and privacy to the general noncriminal public does not considerably hinder the work of law enforcement and international security agencies. This cryptographic standard has been stated in the paper with all the three necessary principals of modern cryptography.

References

- [1] "Brute-force attack," [Online]. Available: http://en.wikipedia.org/wiki/Bruteforce_attack#Unbreakable_codes. [Accessed 02 07 2012].
- [2] J. K. a. Y. Lindell, Introduction to Modern Cryptography, CRC PRESS, 2007.
- [3] J. Dorothy E. Denning and William E. Baugh, "Hiding Crimes in Cyberspace," *Cybercrime*, vol. 2, no. 3, July 1999.
- [4] R. F. Perl, "Terrorist Use of the Internet: Threat, Issues, and Options for International Co-operation," Organization for Security and Cooperation in Europe, 2008.
- [5] Verizon, "2012 Data Breach Investigations Report," Verizon RISK Team, 2012.
- [6] EFF, "Patterns of Misconduct: FBI Intelligence Violations from 2001 - 2008," Electronic Frontier Foundation, 2011.
- [7] G. Weimann, "www.terror.net How do modern terrorist use the internet," United States Institute of Peace, Washinton, 2004.