Indian Journal of Science and Technology, *Vol 10(39), DOI: 10.17485/ijst/2017/v10i39/119866,* October *2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Highlighting Issues Relevant to Encryption Algorithms and Security Schemes

Abdelrahman Altigani[1,2]* and Siti Mariyam Shamsuddin[1,2]

[1]UTM Big Data Centre. Ibnu Sina Institute for Scientific and Industrial Research, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia; a.altigani@gmail.com
[2]Faculty of Computing, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia

Abstract

Cryptography provides a security backbone for most Electronic-Services (E-Services). Computer systems' users trust encryption techniques and protocols as robust mechanisms that deliver the required security services. Therefore, security researchers should act proactively to identify and resolve potential threats in current security schemes in order to preserve this relation of trust between average users and Secure E-Services. This research paper aims to address some of the potential threats in order to urge scholars to take action towards discussing and resolving them.

Keywords: Certification Authority, Cryptography, Cryptanalysis, Information Security, Security Breaches

1. Introduction

Computer Networks and Information Systems have dramatically changed our lives in many respects. It is not required anymore to list the advantages of Data Based or Web Based systems over Paper Based systems. When computer networks were first introduced, scientists and engineers focused mainly on providing and optimising connectivity. It did not take long to realise that all these efforts would be deemed worthless unless decent security was achieved. Accordingly, information security has become a vital research area. Researchers from all over the world have contributed significantly to the field of information security. However, there is still a considerable need for further enhancement of security mechanisms. To support this claim, a report was published by McAcfee in 2014 stating annual losses of an estimated 400 billion US dollars due to cybercrimes[1].

Information security is usually subdivided into different security services. For instance, according to the International Telecommunication Union[2], security services include Data Confidentiality, Data Integrity and Non-Repudiation. Each one of these services can be provided by using the appropriate mechanism or mechanisms. For example, to provide a confidential security service, encryption can be used.

Encryption algorithms are the main mechanism used to provide confidentiality[3]. Encryption algorithms can be classified into Asymmetric and Symmetric Encryption Algorithms[4]. Asymmetric Encryption Algorithms require two different keys. One key is used for encryption (i.e. encoding), while the other is used for decryption (i.e. decoding the encrypted data). In contrast, Symmetric Encryption Algorithms have only one key for both encryption and decryption operations[4]. It is worth mentioning that Symmetric Encryption Algorithms are the main approach used for encrypting a bulk of data. This is because although Asymmetric Encryption Algorithms solved the *key distribution* problem that exists in the Symmetric Encryption Algorithms, the performance of the Asymmetric Encryption Algorithms is generally quite poor compared to symmetric ciphers, as they rely heavily on mathematical problems that require too much time to encrypt or decrypt the data. It has been noticed that both symmetric and asymmetric ciphers can be integrated in many fashions to utilise the good qualities and overcome

*Author for correspondence

the deficiencies of each scheme. As an example, to send confidential data we can:

1. Encrypt the data (payload) using a symmetric cipher.
2. Encrypt (envelop) the symmetric key using the recipient's public key.
3. Send the encrypted message along with the encrypted key.
4. The recipient will decrypt the key using his/her private key.
5. Finally, the recipient will decrypt the message using the recovered key.

Similarly, to preserve the integrity of the message we can use either the Message Authentication Code (MAC) or the Digital Signature depending on our scenario.

Digital Signature is the mechanism most often used to provide both integrity and non-repudiation security services. To generate the Digital Signature, we need to fetch and use the public key of the recipient (e.g. Bob). However, we need to grant that this public key really belongs to Bob. The typical mechanism used to preserve this trusted binding between Bob and his public is called the *Digital Certificate*. The Digital Certificate is a digitally signed data structure that has been issued and signed by a trusted Certification Authority (CA). The data mentioned in the Digital Certificate includes the public key of the subject and the name (Distinguished Name) of the subject, along with other information. A valid certificate will grant the correctness of the binding between the subject and his public key[5].

Cryptographic mechanisms, such as encryption and Digital Signature, can be utilised in several ways to achieve a specific goal or set of goals. For example, the reputable Secure Socket Layer Protocol (SSL Protocol) is used every day to secure a considerable number of websites. This protocol is subdivided into four different protocols, which include the SSL Handshake protocol. The SSL Handshake protocol operation includes:

1. Checking the Digital Certificate of the website in the client side. The checking process involves validating the CA Digital Signature in the certificate.
2. Public Key Encryption: to encrypt the symmetric key (session key) that will be used to encrypt all the messages between the client and the website in a given session.
3. Symmetric Encryption: which will be used along with the session key to encrypt all the messages in a given session.

Cryptographic techniques are the skeleton for most security services. Without these security services, the connectivity service provided by computer networks would be significantly hazardous. These are only a few examples of the areas in which cryptography is vital:

- Electronic Banking (E-Banking) Services, Money Transfer, Mobile Banking, Electronic commerce (E-commerce), etc.
- Electronic Government (E-Government) transactions.
- To protect our business data or to run our business efficiently by using data clouds for better availability and mobility.
- To Create Virtual Private Networks (VPNs), so we can utilise the Internet efficiently to establish our own private networks.
- To protect the confidentiality and integrity of our medical records and facilitate Electronic Health(E-Health).
- To protect academic records and make Electronic Learning tools efficient.
- Secure emails, secure social network accounts.

The following section will cover some issues related to security schemes and encryption algorithms. Then a brief conclusion will be provided.

2. Highlighting Some Issues in Security Schemes and Encryption Algorithms

2.1 The Use of Standard Ciphers

Historically, the cipher design and internal operation considered a national security. Currently, ciphers are standardised. Scholars and developers are encouraged to study the internal design and operation of the Advanced Encryption Standard (AES), RSA and all other ciphers. This has dramatically increased interoperability. Secondly, experts from all over the world can check the soundness of the cipher, and if a weakness exists, they can directly report or publish it.

On the other hand, and apart from ethical aspects, why should anyone report any leak in the cipher, while they can utilise it for their own purposes? Is getting the credit for reporting a significant leak in a cipher or encryption protocol to be considered of equivalent value to utilising it for collecting confidential data or making money? C. B. Röllgen raised a similar concern when he said, "Popular ciphers are always those that have been certified by authorities whose job mainly consists of gathering intelligence. There is a clear conflict of interests for these government organisations. These professionals clearly know about the blatant deficiencies of the encryption algorithms that they certify"[6].

2.2 The Use of Open Source Technology

Currently, the trend is to use open source technology for providing security services. Clients choose not to fully trust the security service provider. Instead, they want to see how this service is provided. This business decision might be derived from the instinctive desire of business owners to control their business, or attempt to avoid the possibility of malicious code segments within the code. Another more practical reason is the relative ease of customising and obtaining support for open-source systems compared to proprietary systems.

On the other hand, this opens up a wide range of potential threats, which relies on the implementation deficiencies. The opponent knows not only the design of the encryption algorithm or encryption protocol; they also know how this algorithm or protocol is implemented. As an example of potential damage, in April 2014, a bug called Heartbleed (formally known by CVE-2014-0160) in the reputable cryptographic library OpenSSL was reported[7,8]. This bug was not in the SSL/TLS protocol logic; rather it was in the package implementation for this protocol, but the worrisome fact was that it was believed that this bug was known and exploited by others for a long time before it was reported[8].

2.3 Side Channel Attacks

As a logical result of using standardised ciphers and encryption protocols plus using open source technology, several attacks can be launched on ciphers and encryption protocols. These kinds of attack are known as side channel attacks and include timing attacks, power analysis attacks, fault attacks, and electromagnetic analysis attacks, among others[9].

These kinds of attacks involve looking at the problem from a very different point of view. Accordingly, there is no feasible approach to predict all the possible holes in your design.

2.4 Trust Your Instinct

In[10], the author states that moving the hosting service of your business to the public cloud is not as scary is it might sound. Under the subtitle "Untrustworthy instincts", he urges the reader to trust the public cloud service because so much effort has been put into protecting it from potential security threats. He also makes a comparison between the use of public cloud and air travel: "because flying is instinctively scary, so much has been spent to make it safe that you are less likely to die on a flight than you are driving the same journey in the 'safety' of your own car"[10]. This is not completely correct. Clouds are more exposed to hacking attempts, and opponents are developing their tools and techniques all the time to find only one hole. This is not analogous to travelling by air, in which we have specific laws of physics which we adhere to. Furthermore, the same mechanisms that are used for protecting the public cloud can be utilised for protecting your own network and data, without exposing your data to the same risk.

2.5 Advances in Computation Power and Quantum Computing

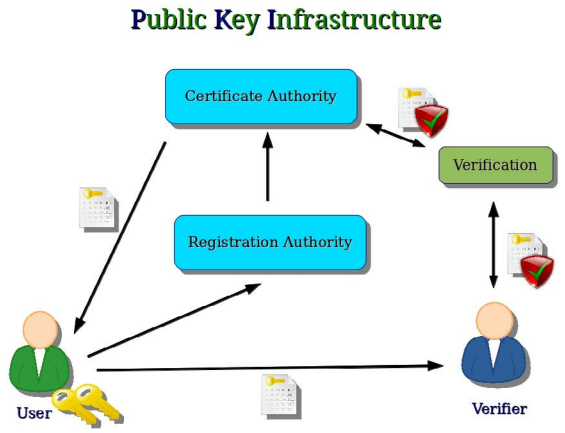
Shor algorithm was introduced in the mid of nineties as an algorithm that could run on quantum computers and solve the problem of large integer factorisation efficiently[11]. The large integer factorisation problem is at the heart of the RSA cipher as well as other asymmetric ciphers and, if solved, RSA as well as many other asymmetric ciphers will be deemed obsolete. Although several attempts have been made to come-up with quantum cryptography schemes to counter the potential threat, the maturity of these schemes is still questionable[12].

2.6 Certification Authorities Operation

Public Key Encryption is a key utility in most encryption schemes and protocols. However, a trusted bond between the subject and their public key should be establishing before any secure communication can take place. As stated before, the CA, or formally speaking the Public Key Infrastructure (PKI), is the entity that provides this

trusted bond. Figure 1 depicts an overview of the certification and verification processes in a typical PKI.

On the other hand, it has been proved that not all trusted CAs are necessarily operating in a completely ethical or professional manner[13,14]. Therefore, this bond is not necessarily always accurate. The reader is invited to imagine the cost of scenarios in which the internet surfer provides their secret information to an untrustworthy website that has a valid digital certificate.



3. Conclusion

More light needs to be shed on a few concerns relating to encryption algorithms and protocols to make things transparent and more robust. Overlooking such concerns is never a solution. However,identifying, analysing and perhaps proposing alternatives (if necessary) are steps in the right direction. Finally, it worth mentioning that in 1917 an article in the magazine Scientific American stated that the Vigenère cipher was impossible to cryptanalyze[15]. Now we all know that this was untrue. Therefore, we need to keep reminding ourselves of this incident before jumping to conclusions, such as this protocol or cipher is totally secure.

4. References

1. Arief B, Adzmi B, Azeem M, Gross T. Understanding cybercrime from its stakeholders' perspectives: Part 1-Attackers. IEEE Security & Privacy. 2015; 13(1):71–6. Crossref
2. International Standards equivalent in technical content–CCITT Recommendation X. 800 (1991). Security architecture for Open Systems Interconnection for CCITT applications.
3. Pawar SB, Tandel LL, Zeple PK, Sonawane SR. Survey of Cryptography Techniques for Data Security. International Journal of Science, Engineering and Computer Technology. 2015; 5(2):27.
4. Altigani A, Barry B. A hybrid approach to secure transmitted messages using Advanced Encryption Standard (AES) and Word Shift Coding Protocol. 2013 International Conference on Computing, Electrical and Electronics Engineering; 2013.
5. Adams C, Lloyd S. Understanding PKI: Concepts, standards, and deployment considerations: Addison-Wesley Professional; 2003.
6. Röllgen CKB. Block cipher. Google Patents; 2010.
7. Durumeric Z, Kasten J, Adrian D, Halderman JA, Bailey M, Li F. The matter of heartbleed. Proceedings of the 2014 Conference on Internet Measurement Conference; 2014. Crossref
8. Schneier B. Heartbleed. Schneier on Security. 2014; 9.
9. Zhou Y, Feng D. Side-Channel Attacks: Ten years after its publication and the impacts on cryptographic module security testing. IACR Cryptology ePrint Archive. 2005; 2005:388.
10. Zhang H. Bring your own encryption: balancing security with practicality. Network Security. 2015; 2015(1):18–20. Crossref
11. Bernstein DJ, Buchmann J, Dahmen E. Post-quantum cryptography: Springer Science & Business Media; 2009. Crossref
12. Scarani V, Kurtsiefer C. The black paper of quantum cryptography: real implementation problems. arXiv preprint arXiv:09064547. 2009.
13. Fisher D. Final Report on DigiNotar Hack Shows Total Compromise of CA Servers. Retrieved September. 2012; 8:2013.
14. Arnbak A, Asghari H, Van Eeten M, Van Eijk N. Security collapse in the HTTPS market. Communications of the ACM. 2014; 57(10):47–55. Crossref
15. Stallings W. Cryptography and network security: principles and practices: Pearson Education India; 2006.