International Journal of Database Theory and Application
Vol.9, No.7 (2016), pp.297-304
http://dx.doi.org/10.14257/ijdta.2016.9.7.26

Security Measures in Overcoming Mobile IPv6 Security Issues

Jasmine P. Valera, Sunguk Lee*

Department of Multimedia, Hannam University, Daejeon, Korea
jas_12394@naver.com, sulee0612@hnu.kr
**Correspondent Author: Sunguk Lee* (sulee0612@hnu.kr)*

Abstract

With the remarkable progressions in network communications and modern day technology, Mobile IP became very significant as people nowadays have mobile devices with them. If one network goes down, the other connected networks are affected. However, Mobile IP makes this problem practically non-existing. Wherever the user's location is with his/her mobile device, a unique IP address of its own exists consistent with their device. Mobile IPv6 advanced features compared to MIPv4 are optimized to reduce packet loss. Herein, issues on security threats alleviates in the mobility of wireless networks. This paper focuses on MIPv6 mobility support by proposing enhanced methodologies in providing secure communication.

***Keywords:** Mobile IPv6, Mobility Support, MIPv6 Security, Binding Update, Cryptography*

1. Introduction

The successor of MIPv4, introduced by the IETF (Internet Engineering Task Force) known as Mobile Internet Protocol version 6 (MIPv6) developed its opportunities and brought higher quality features that integrates the birth of Fast Mobile Internet Protocol version 6 (FMIPv6), Hierarchical Mobile Internet Protocol version 6 (HMIPv6) and Proxy Mobile Internet Protocol version 6 (PMIPv6).

MIPv6 aims to enable nodes move and reach their destinations flexibly and transparently while in move or changing their location in the wireless environment. Additionally, it is exclusive for homogenous media mobility maintaining existing connections among mobile nodes as it communicates to each other [1].

This study was summarized as follows: Section 1 will discuss the architecture of MIPV6 and its standard mobility procedure, Section 2 highlights the issues followed by Section 3, presenting measures on dealing with several existing threats. Finally, the allover impact of proposed techniques was concluded.

2. Mobile IPv6 Basic Operation

Mobile IPv6 solves the issue on routing problems when mobile nodes connect and transmit data to other nodes while keeping the same IP address. Through the proposed routing schemes, the ability of network nodes to reach other nodes while mowing flexibly is achieved wherever the network location is. To address hosts efficiently and predict the greatest potential path for receiving and sending packets over network serves as main purpose of Mobile IPv6.

This transmission of data is governed by rules and domains. The fundamental elements of Mobile IPv6 starts with the Mobile Node (MN) which uses Home Agents (HA) in reaching other nodes known as Correspondent nodes (CN) represented by two main address; Home Address (HoA) and Care-of-Address (CoA).

ISSN: 2005-4270 IJDTA

In the cycle of MIPv6, the Home Address carries a stable IP address allowing Mobile Nodes reachable making the Home Address as the permanent address of the mobile node within the mobile node's network. Another characteristic ability of Mobile Nodes is having multiple Home Addresses which occurs when multiple Home Addresses are in the Mobile Node's home connection. This is how the Care of Address and Home Address are related. Whenever an unattached Mobile Node is away from its home, this becomes now the foreign network. The movement of Mobile Node as it transmits data to one network from another foreign network creates an address which is temporary or subnet prefix of a foreign network. It is referred to Care-of-Address (CoA) wherein revealed by the Mobile Node as its present Care of Address to its Home Agent and Correspondent Nodes.

The method in which these addresses are exist is called the binding management which includes Binding Update (BU), Binding Acknowledgement (BAck) and Binding Request (BReq). The first one previously mentioned is the Binding Update. When the Mobile Node connects to another network link, it sends its Care of Address to its Home Agent via Binding Update process. After the Home Agent and Correspondent Node received the Binding Update, it now performs the Binding Acknowledgement and sends Binding Requests from Home Agent and Correspondent Node to Mobile Node in restoring the present binding updates. Figure 1 below summarizes the binding management process.

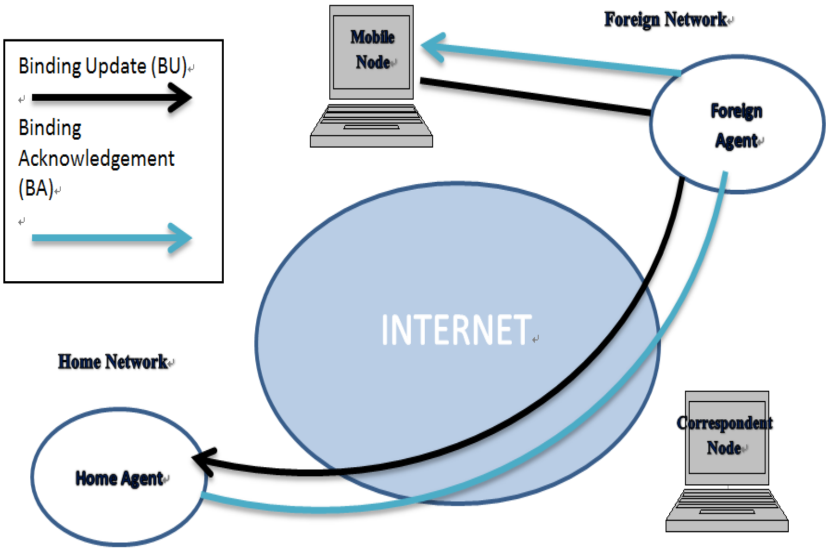

Figure 1. Mobile IPv6 Binding Update Process

These binding messages are packets routed to the Mobile Node's home network diverting them through tunneling mode back to the Mobile Node. Then, if the packets are received already, the Mobile Node informs the Correspondent Node of its current address or location. When the binding updates have been made by the Correspondent Node amongst Home of Address and Care of Address, there is an exchange of Correspondent Node to the Mobile Node simultaneously.

The routing header is an address used by nodes in sending packets. When the Correspondent Nodes sends packets to Mobile Nodes, the IP routing header is established. It shows the destination location as Care of Address while the Home Address appears in the routing header. Also, the destination address is changed when the Mobile Nodes receives packets right before moving on to the next layer protocol. However, the Mobile Node uses a Home Address signifying as the true sender to the Correspondent Node when the Correspondent Node forwards packets directly as well as by Care of Address being the packet's source address [2].

Mobile IPv6 must be transparent in communicating packets and entering protocol layers as standard operation process. The mobility feature without any issues when connecting nodes in whichever layer requires strong security. Thus, the following threats and security issues will be discussed on the following sections.

3. Modes in Forwarding Data Packets

There are two possible ways between the mobile node and a correspondent node in transmitting packets as shown below.

3.1. Bi-directional Tunneling Mode

Also known as Symmetric Mobility Tunneling, this mode is enabled by default only in which the channeled information traffic occurs in both directions from entry-point to exit-point node. In this mode, MIPv6 support from the CN is not required and uses the reverse tunneling. The HA uses proxy Neighbor Discovery to divert any packets addressed to the MN's home address(s) on the home link. Each diverted packet is tunneled to the MN's primary CoA using IPv6 encapsulation.

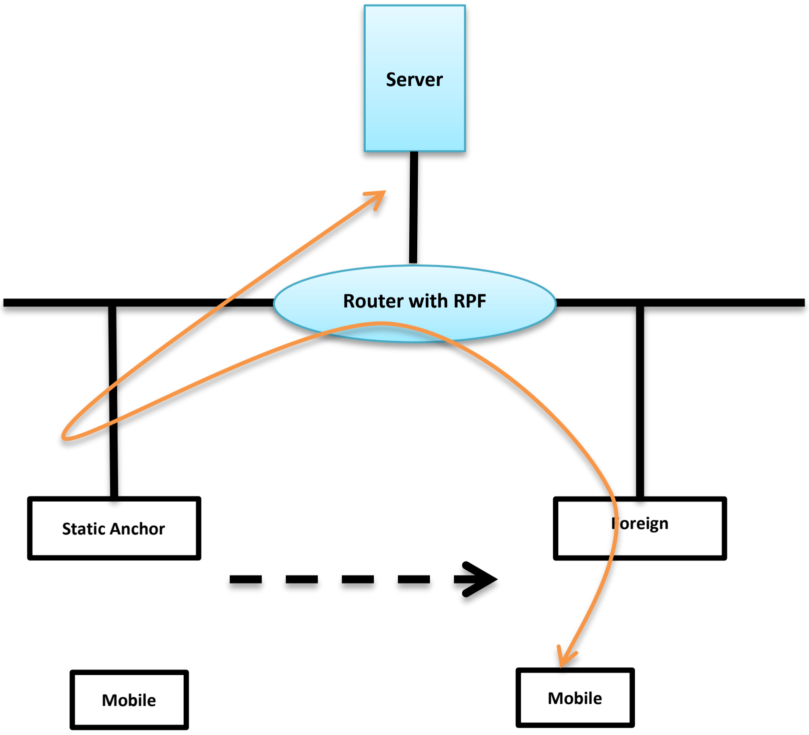

Figure 3. Bi-directional Tunneling [3] et al. *Cisco*

In consideration of security, the degree of confidentiality processed on both directions is based on the kind of security header constructed in the tunnel's Security Association [4].

3.2. Route Optimization Mode

This mode enables more effective data packets communication than the previous mode. In order to create and restore from time to time a bidirectional security between Mobile Node and Correspondent Node, Routing Optimization needs a considerable amount of mobility signaling messages [5]. Figure 4 below illustrates the basic structure.

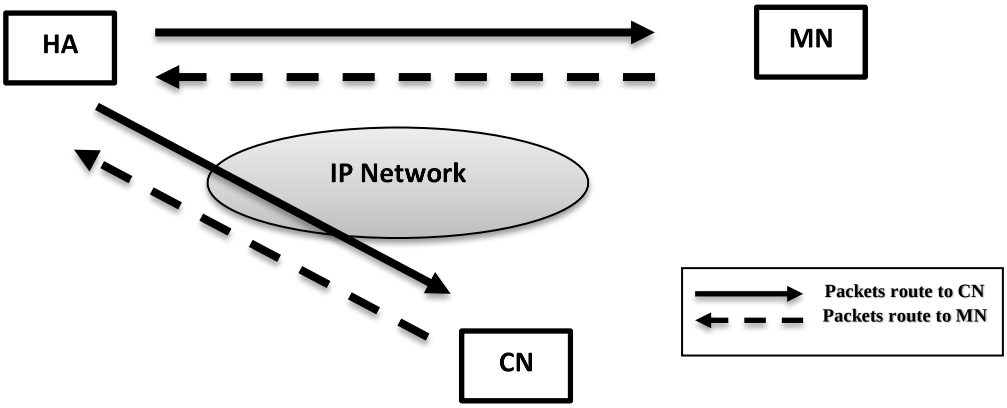

Figure 4. Routing Optimization [6] et al. *Shanzhi Chen*

The Correspondent Node checks binding cache if any entries for the destination location of such packet is present before transmitting packets. If an entry is already present, this packet is sent to the Mobile Node via Care of Address. Then, using the Home Address as the destination location, the Correspondent Node forwards these packets [6].

Compared to the Bi-Tunneling Mode, Routing Optimization removes cramming at the Mobile Node's Home Agent and Home Network and also reduces any probable failures of the networks on both directions.

However, problems continue to arise like securing Neighbor discovery, binding update authorization process, poor unity of Mobile IPv6 and firework and dual stack architecture and interoperating among Mobile IPv4 and Mobile IPv6 when roving.

4. Security Issues

Although Mobile IPv6 has a lot of advanced features compared to Mobile IPv4, there are still loopholes and inefficiencies arising especially in terms of data security. As development in Mobile IPv6 grows, these issues correspondingly existed and the following are common samples.

4.1. Man-in-the Middle Attack (MITM)

This is one of the challenges in Mobile IPv6 security which takes advantage of a weak authentication process by interacting networks. Herein, the intruder attacks by interfering data through backdoor and impersonate successfully each end points as treated the real node. When this occurs, false binding updates from the malicious nodes spoof data packets inserting fake Home Address. Also attacker has the ability to redirect data packets to suspicious or any random address to destroy transmission between valid nodes.

Some examples of MITM Attacks include, ARP Cache Poisoning and Hijacking of SSL and Sessions. This issue was proposed by numerous countermeasures to minimize the attacks such as hardening of host, designing a network from a secure basis and on-time upgrades and updates of operating system on networks [7].

As shown in Figure 5, the traffic can be redirected through a malicious node through false Binding Updates. Herein, the malicious intruder is on a two-node communication line which disrupts the transmission of data by changing the packet contents.

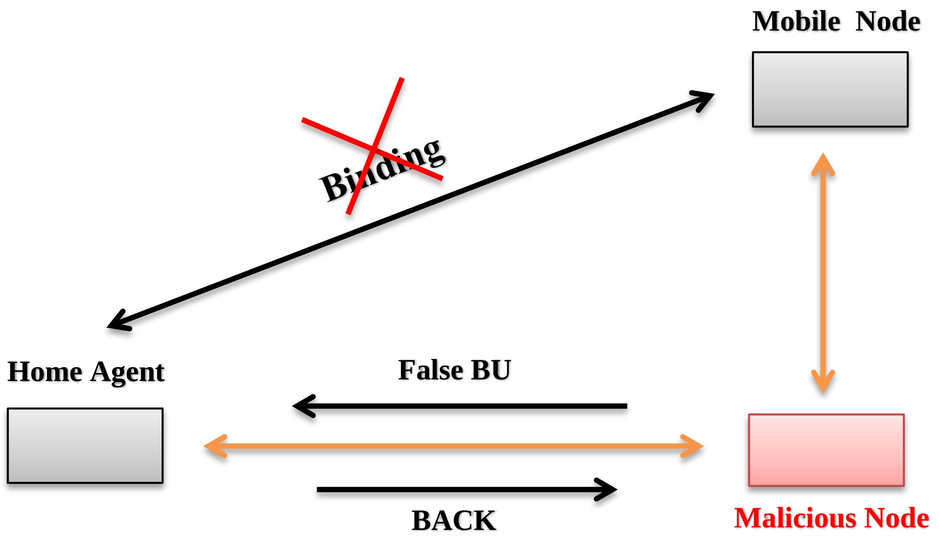

Figure 5. MITM Attack

Due also to the visible network forwarding of packets, this security objective is at high risk. Binding message authentication on various entities has related security concerns. If one network connection is attacked, consequently the other involved systems will fall at risk too. To ensure the validity and authentication in order to overcome the malicious node impersonation attack, a proposed scheme will be discussed later.

4.2. Denial-of-Service (DoS)

The Denial-of-Service attack takes place when the real node was service denied. This can be in many forms even not under the presence of Mobile IPv6. Usually, this kind of attack claim that the Mobile Node is located on another address through fake binding updates or the attacker denies service to the Mobile Node's packet and thus dropping it off. Also, this attack has the ability to saturate the Correspondent Node's memory with many invalid Binding Updates to the nonexistent Home Address [8].

4.3. Binding Update Spoofing

In Binding Update Spoofing, usually, the attacker has the willpower to do whatever it wants to stress the Mobile Node such as retrieving its traffic, forbidding it to communicate, or redirecting the traffic to a target to perform a Denial of Service.

4.4. Traffic Injection

Traffic Injection occurs when a Mobile Node's Home Address is recognized and visible to anyone and can be stored in the DNS. However, if an "intruder" has knowledge of the address, he can "steal" it to redirect traffic to himself by sending a Foreign Binding Update to the Correspondent Node. In this setup, the data traffic that was originally meant for the Mobile Node is taken away by the intruder and possibly also that the intruder could steal the Mobile Node's connection to a Correspondent Node, which could act then as the current Mobile Node. But maliciously all the while, the intruder is not even on the Mobile Node and the Correspondent Node path. As shown in Figure 6, the tunnel is unsafe between the Correspondent Node and Mobile Node.

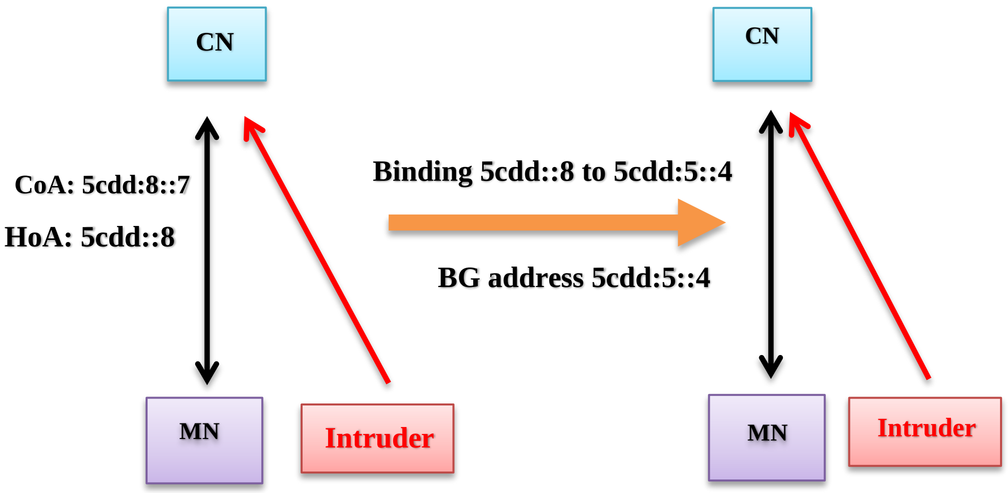

Figure 6. Stealing Traffic Showing Intruder Attack

The intruder can disrupt freely the transmission pf packets between Mobile Node and its Home Agent. This scenario is not protected, and the attacker keeps sending fake Binding Updates by replacing fake destination addresses of mobile nodes. As easily the attacker inject data packets into the tunnel and pretend to send traffic from the Home Address [9].

4.5. Return Routability Procedure

This does not provide any protection against an attacker based on the visited network: the threat is, in this case, independent of Mobile IPv6, and equivalent to an attacker eavesdropping traffic on a non-protected Wi-Fi hotspot.

5. Security Measures for Addressing MIPv6 Security Issues

There are several proposals that were defined by the IETF to solve these security threats and attacks aiming to secure and reduce the loss of signaling packets sent from MN to HA.

In the advanced research studies, the number of proposed protocols includes Hierarchical Mobile IPv6 (HMIPv6) which makes mobility within an operator's network transparent to correspondent nodes through a pyramidal hierarchy of home agents. However, Proxy Mobile IPv6 (PMIPv6) does not require any host-based mobility stack in the MN, irrespective of the handoff frequency. On the other hand, Fast Handovers for Mobile IPv6 (FMIPv6) is a different approach to reduce packets losses during handovers. Besides these proposed developed protocols in MIPv6, the following security mechanisms are designed for the better understanding of serious challenges in MIPv6.

5.1. Cryptography

Cryptography handles mobility management issues in Mobile IPv6. To achieve encryption confidentiality, integrity nonrepudiation and authentication, cryptography was designed which ensures the confidentiality in sending the packets through a network. Herein, the sender follows a certain encryption algorithm that encrypts the plaintext message to produce ciphertext. In addition, this is composed by two kinds; the asymmetric and symmetric key cryptosystem.

5.1.1. Asymmetric Key Cryptosystem

This cryptosystem is used in public key cryptography uses two keys called public and private key. The public key is used for encryption and the private key is used to gain confidentiality.

In Figure 5, the message of Anna is encrypted into code using John's public key. However, only John who has the private key can decrypt the message.

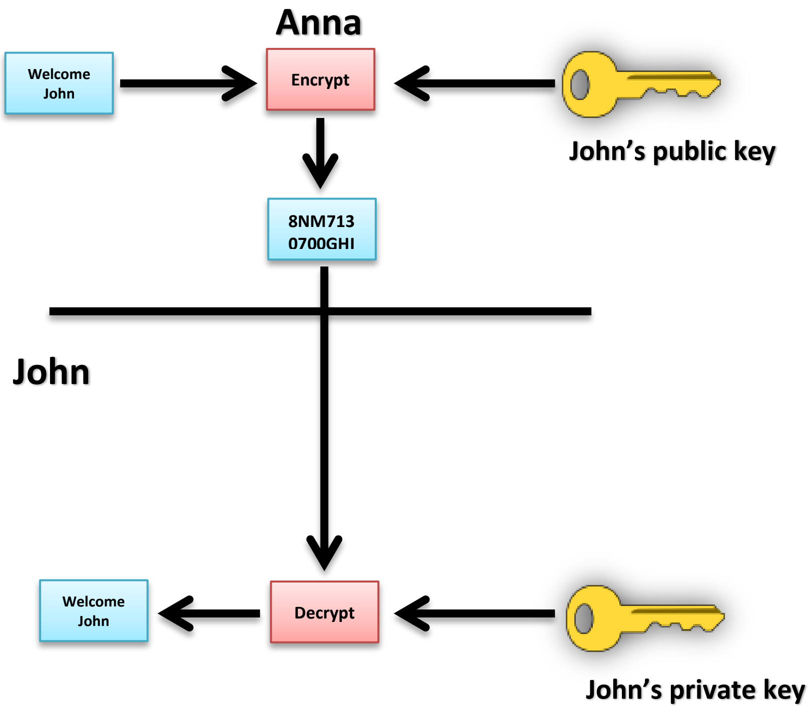

Figure 5. Asymmetric Key Encryption Key [11] et al. *Wikipedia*

For instance, in a pair of key used for digital signatures compose of a private signing key and a public verification key. The public key may be widely dispersed, while the private key is recognized only to its owner. The keys are related accurately, but the parameters are selected so that calculating the private key from the public key is unattainable [10].

5.1.2. Symmetric Key Cryptosystem

Opposite to the asymmetric, this one is secretly known only to one entity (both sender and receiver). This is likely used as simple way to communicate securely since its use is limited by the need to exchange keys securely.

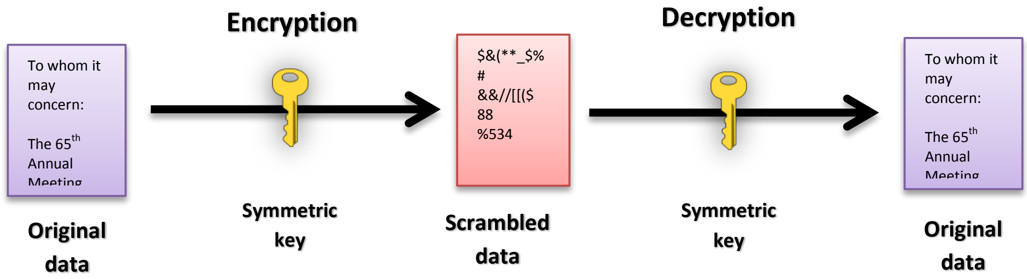

Figure 6. Sample Symmetric Key Cryptography [12]

However, the problems alleviate in terms of involvement of third parties or more in sharing the same.

5.2. Dynamic Home Agent Address Discovery (DHAAD)

This function allows mobile node to discover home agent addresses while located in a foreign link. Here, MIPv6 attacks are considered non-existing when using DHAAD. Here, the attacker cannot send an authenticated binding acknowledgement to the MN harmlessly.

6. Conclusion

The widespread of Internet usage in communications, banking, research and everyday lifestyle of people become more fundamental wherein security is a critical issue in managing Internet privacy. The focus of this paper on security risks and threats are summarized with respect to the different vulnerabilities and attacks in MIPv6 as well as and presenting several security measures to overcome these problems such as Cryptography, Encryption and Dynamic Home Address Authentication Discovery.

Acknowledgements

This paper has been supported by the 2016 Hannam University Research Fund.

References

1. A. K. Tripathi, A. Srivastava, H. Pal, S. Tiwari and S. Pandey, “Security Issues in Mobile IPv6, National Conference on Development of Reliable Information System, Techniques and Related Issues (DRISTI) 2013.
2. T. Koskiahde, “Security in Mobile IPv6”, Tampere University of Technology, April 18, 2002.
3. http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010010110.html
4. https://tools.ietf.org/html/draft-conta-extensions-ipv6-tunnel-01
5. https://tools.ietf.org/html/draft-haddad-mext-mobisoc-04.html
6. S. Chen, Y. Shi, B. Hu and M. Ai, “Mobility Management: Principle, Technology and Applications”, Springer 2016, p. 207, 210.
7. https://arxiv.org/ftp/arxiv/papers/1504/1504.02115.pdf
8. H. Modares, A. Moravejosharieh, R. B. Salleh and J. Lloret, “Enhancing Security in Mobile IPv6”, ETRI Journal, Vol. 36, No. 1, February 2014, p.52.
9. J. Arkko, V. Devarapalli, F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents”, IETF, RFC 3776, June, **(2004)**.
10. https://en.wikipedia.org/wiki/Public-key_cryptography
11. https://upload.wikimedia.org/wikipedia/commons/thumb/f/f9/Public_key_encryption.svg/525px-Public_key_encryption.svg.png
12. https://www.ibm.com/support/knowledgecenter/SSB23S_1.1.0.12/gtps7/ssldig01.gif