NTRU CRYPTOSYSTEM ANALYSIS FOR SECURING IOT

[1]Lela Mirtskhulava, [2]Nana Gulua, [2]Nugzar Meshveliani

[1]Iv. Javakhishvili Tbilisi State University, 3 University Str. Tbilisi, Georgia

[2]Sokhumi State University, 61 Politkovskaya str. Tbilisi, Georgia

Abstract

In the given paper, we analyse NTRU (Nth Degree Truncated Polynomial Ring Units) - the first lattice-based public key cryptosystem due to their advantages like lack the install base and long-term cryptanalysis. NTRU's cryptosystem is much faster than the algorithms like RSA or ECC. NTRU use one-off keys that makes possible to change keys after a few seconds of use. A cracker would need to obtain hundreds, or thousands, of keys rather than just one for cracking the encryption on a video files. The Internet of Things (IoT) is a network of thousands of smart interconnected devices like cars, smart medical equipment, industrial control systems, smart grid and etc. Security risks are growing with using increased number of connected vulnerable devices caused serious security threats. Through the vulnerable devices is the attacker can gain a sensitive information accessing the enterprise networks. Malwares, botnets and distributed denial-of-service (DDos) caused material damage in IoT systems. IoT security is an essential consideration of the given paper.

Keywords**:** *IoT security, wireless security, NTRU cryptosystem, encryption, decryption.*

1. Introduction

The Internet of Things (IoT) serves more than millions of people. A huge number of smart and connected devices support new possibilities to people on the globe, decreasing expenses of billions of dollars even. By the Internet of Things (IoT), we primarily understand cars connected to the Internet, TVs, surveillance cameras, robotic manufacturing, smart medical equipment, an power supply network and countless industrial control systems (turbines, valves, servo drives, etc.). IoT security needs special attention due to its security breaches. Cybercrime threats are increased with more PCs, smartphones or other devices connected to the Internet which becomes very crucial for security issues of our whole society. Millions of malicious threats are fixed in the telecommunication systems, Internet of Things (IoT), Wi-Fi and etc. Organizations suffer multiple malware and cyberattacks. Multiple new malware files are detected in every second. All the domestic appliances might be the secret spies listening and recording the conversations. Recently published CIA documents shocked with the news about that TVs connected to the Internet may record the conversations and microwave cameras might be spies. [1]

The Internet of Things is a set of various components that connect people, systems and software over Internet. Communication network is one of the important component enabled by IoT wireless technology which is the gateway between IoT devices and a software. Wireless Fidelity (Wi-Fi) is the go-to standard for transferring large amounts of data over a wireless network based on the IEEE 802.11 standards' family. Wi-Fi is a local area networking (LAN) technology that replaced wired Ethernet for peer-to-peer communications. Due to its popularity at homes and other environments, Wi-Fi has been selected as an IoT wireless technology for developers.

Wi-Fi networks play a significant role in today's communication world due to their mobility, inexpensiveness, flexibility and effectiveness [2]. They are integrated into every digital device like laptops, smartphones, PDAs and etc. Wi-Fi is one of the leading wireless technologies and played a significant role in IoT development because Wi-Fi coverage is ubiquitous. The applications of IoT requires diverse connectivity in data throughput, cost-effectiveness and energy efficiency [3].

However, wireless networks have many limitations such as reduced storage data and low-power consumption. But main challenge in using Wi-Fi networks is security issues. They are using radio waves which are usually prone to eavesdropping and it requires to keep the data transmitted through network nodes permanently encrypted in order to avoid unauthorized access to the Wi-Fi networks. WEP, WPA and WPA2 protocols designed for for securing Wi-Fi networks by handling communication management. The aim of the given study is to analyse the security issues in wireless networks. Main attention will pay to WPA2 protocol security issues discovered recently by Computer Science Scientists.

2. Wi-Fi protocols

Chronologically, 3 main wireless Security protocols: WEP, WPA and WPA2 were developed through the last two decades. Wireless Equivalent Privacy (WEP) was the first default IEEE 802.11 standard based encryption protocol developed in 1997 where the various technical failures were detected. WEP uses the RC4 encryption scheme and the CRC-32 for data integrity, and a shard secret key k of 5 to 13 bytes [4]. For producing a ciphertext C and its checksum ICV from a plaintext M, the key k is combined with an Initialization vector IV of 3 bytes through the formula (1):

$$C=M||ICV(M) \oplus RC4(K)||IV \quad (1)$$

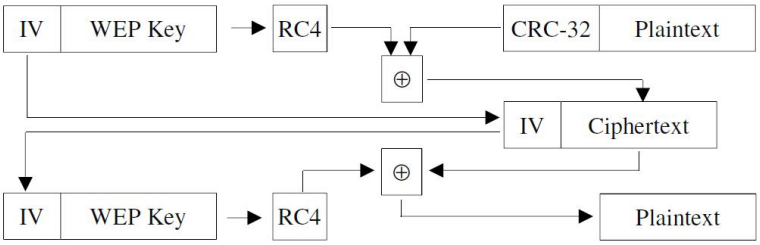

Fig. 1. WEP Encapsulation process [5]

WEP protocol and its cryptographic primitives have been found to be vulnerable on a several levels, what led to the second encryption standard protocol development WPA (Wi-Fi protected access) in order to solve most of the problems associated with WEP security issues. Wi-Fi protected access (WPA) was invented to solve the problems in the WEP cryptography method. Both WEP and WPA were used to secure wireless communications and due to their many proven vulnerabilities new protocol was implemented, WiFi protected access 2 (WPA2) protocol [5-6]. WPA2 also known as IEEE 802.11i standard is a revision to the 802.11 standard which specifying security techniques for wireless networks.

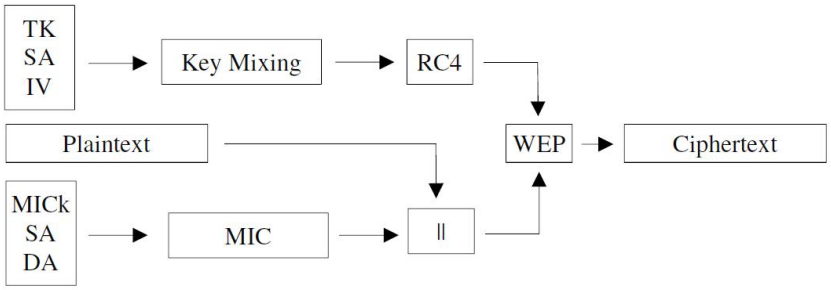

Fig. 2. WPA Encapsulation process

3. WPA2 vulnerabilities

The serious weaknesses were recently discovered in WPA2 (Wi-Fi Protected Access 2) by Computer Science Scientists. The KRACKs (key reinstallation attacks) were introduced to abuse design flaws in cryptographic protocols to reinstall an already-in-use key. Several types of

cryptographic Wi-Fi handshakes are affected by the attack. Main issue is the attackers can use this novel attack technique to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos that were previously assumed to be safely encrypted [7-8]. Depending on the network configuration, the attacker can inject and manipulate data in all modern protected Wi-Fi networks injecting ransomware or other malware into websites. NTRU's encryption routines lack the install base and long-term cryptanalysis and thank to this property NTRU's cryptosystem is much faster than either RSA or ECC. The most likely application for new cryptographic techniques lies less with displacing existing technologies and more with new applications. Use of NTRU's "disposable" keys makes it possible to change keys after even a few seconds of use. To crack the encryption on a music or video file, a cracker would need to obtain hundreds, or thousands, of keys rather than just one [9].

In October 2017, KRACK (Key Reinstallation Attack) attack on WPA2 were announced. The KRACK attack can affect all variants of the WPA protocol. WPA (Wi-Fi Protected Access) and WPA2 are security protocols developed by the Wi-Fi Alliance to secure wireless computer networks. They replaced their predecessor WEP (Wired Equivalent Privacy) because the serious weaknesses were found by researchers in the previous system [10]. This attack abused implementation flaws in cryptographic protocols to reinstall an already-in-use key. This resets the key's associated parameters such as transmit nonces and receive replay counters. Several types of cryptographic Wi-Fi handshakes are affected by the attack. Wi-Fi networks use the 4-way handshake for generating a fresh session key. Now, the 4-way handshake is vulnerable to a key reinstallation attack what is achieved by manipulating and replaying handshake messages [11].

"This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on," researcher Mathy Vanhoef, of the Katholieke Universiteit Leuven in Belgium wrote. "The attack works against all modern protected Wi-Fi networks. Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites" [12].

Every Wi-Fi client is vulnerable to CRACK attack against the group key handshake. This enables to replay broadcast and multicast frames. During the 4-way or fast BSS (Basic Service Set) transition handshake is attacked it is possible to decrypt frames and hijack TCP connections and thus the injection of data into unencrypted HTTP connections. Moreover, this attack to Android 6.0 completely void any security guarantees.

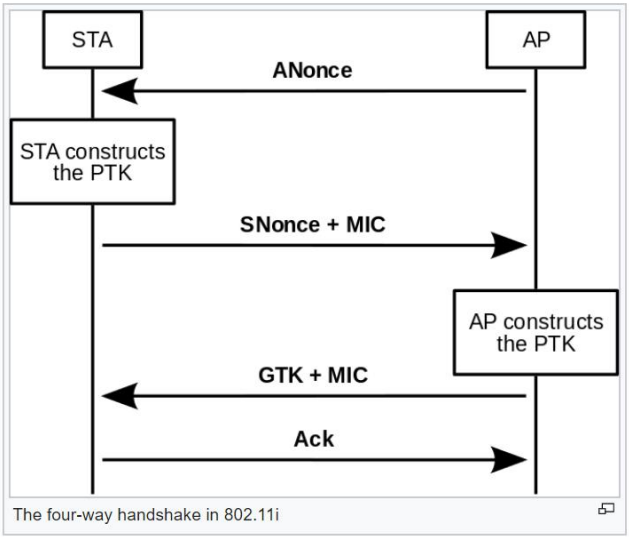

Fig. 3. Four-way handshake for Wi-Fi

The four-way handshake (Fig.3) enables the access point (or authenticator) and wireless client (or supplicant) independently prove to each other that they know the PSK/PMK (Pre-shared key/Pairwise Master Key), without ever disclosing the key. The access point and client both encrypt messages to each other—that can only be decrypted by using the PMK that they already share—and if decryption of the messages was successful, this proves knowledge of the PMK. The four-way

handshake is critical for protection of the PMK from malicious access points—for example, so that the client never has to tell the access point its PMK.

4. New Security WPA3 Protocol Invention

At the beginning of 2018, the WPA2 were replaced by new WPA3 protocol as Wi-Fi Alliance announced. New security standard differentiates Enterprise mode with 192-bit cryptographic strength and Personal mode with the use of CCMP-128 encryption algorithm [13]. Pre-shared key exchange protocol was replaced and simultaneous authentication and forward secrecy is used instead [14-15]. So, the WPA3 mitigates security issues caused by weak passwords [16]. WPA3 aims to bring new technologies to withstand the cracks that started to appear in WPA2 [17].

5. Four Main changes the WPA3 protocol brings to wireless security

5.1. Simultaneous Authentication of Equals (SAE): this is a new method authenticating a device trying to be connected to a wireless network. This kind of handshake as named dragonfly handshake uses cryptography preventing to guess a password during exchanging cryptographic keys. So, PSK also known as a four-way handshake has been replaced by SAE. SAE extended security feature and "forward secrecy" is used where an intruder can gain access to encrypted data sent by a router and guess a current password but decrypt only data that were transmitted after that time. SAE enables the encryption password to be changed every time when connection can be established [18].

5.2. 192-Bit Security Protocols: WPA3 (Enterprise) features 192-bit encryption. Wi-Fi currently features 128-bit security but the 192-bit security protocol will be optional setting for institutions requiring a strong level of cryptographic strength. For ensuring the entire network security, WPA3 will use a 256-bit for enterprise modeand a 384-bit mode of Hashed Message Authentication for key creation and confirmation.

5.3. Easy Connect: this is a way of recognition of plenty of connected devices in the world making that more intuitive. Easy Connect: this is a separate protocol which gives a way of recognition of plenty of connected devices in the world making that more intuitive. Where every connected device has unique Quick Response (QR) code functioning as public key. No password is used.

5.4. Enhanced Open: this is another separate protocol designed to protect your data against passive eavesdropping while you are connected to an open network using OWE (Opportunistic Wireless Encryption).

6. WPA3 Vulnerabilities

The vulnerabilities have been discovered in new launched security protocol WPA3. They make it possible to recover a wi-fi password through the “efficient and low cost” attacks. Research showed that the passwords may be accessible for hackers as the protocol contains two main types of flaws in design that can be used for attacks. The vulnerabilities found in WPA3 Personal implementation are known as ‘Dragonblood’ [18].

7. Cryptographic Solutions in Wi-Fi Security and Cryptosystems

For securing Wi-Fi networks the existing wireless protocols must ensure user authentication, message privacy and integrity. Cryptographic approaches are required in Wi-Fi networks for dealing with attacks providing integrity and confidentiality that effect on the Wi-Fi network performance. We can use cryptosystem as a set of three algorithms: for encryption, decryption and a key generation. Wi-Fi Infrastructure incorporates billions of digital devices and users. Every node in Wi-

Fi networks must be provided with cryptographic functions like symmetric and asymmetric cryptographic primitives for performing data encryption and authentication.

This work is intended to use secure and faster cryptographic solution for Wi-Fi networks security by using an open source public-key NTRU cryptosystem that uses lattice-based cryptography. NTRU can implement the NTRUEncrypt public key encryption algorithm in Java and C. NTRUEncrypt is lattice-based and known as unbreakable even with quantum computers. On the other hand, commonly used cryptosystems like RSA or ECC, can be broken by quantum computers. Therefore, NTRU is significantly faster than other public-key cryptosystems [19-24].

8. The NTRU cryptosystem

NTRU parameters and keys:

N - N-1 degree polynomials in the ring R
q - the large modulus
p - the small modulus
f - the private key (a polynomial)
g - a polynomial - generation of the public key h from f
h - the public key, (a polynomial)
r - the random polynomial
d – coefficient

The NTRU cryptosystem use three integer parameters (N, p, q) and four sets $L_f, L_g, L_\emptyset, L_m$ of polynomials of degree N-1 with integer coefficients. Note that p and q need not be prime, but we assume that gcd(p; q) = 1, and q will always be considerably larger than p. We note the ring R=Z[X]/(X^(N-1)). An element F∈R can be written as a polynomial or a vector,

$$F = \sum_{i=0}^{N-1} F_i\, x^i = [F_0, F_1, \ldots, F_{N-1}]$$

We write * to denote multiplication in R. This star multiplication is given explicitly as a cyclic convolution product,

$$F * G = H$$

where

$$H_k = \sum_{i=0}^{k} F_i G_{k-i} + \sum_{i=k+1}^{N-1} F_i\, G_{N+k-i} = \sum_{i+J \equiv k\ (mod\ N)} F_i G_i$$

When we do a multiplication modulo q, we mean to reduce the coefficients modulo q.

9. Key generation

To generate an NTRU key, Bob randomly chooses 2 polynomials f,g∈Lg. The polynomial f must satisfy the additional requirement that it have inverses modulo q and modulo p. For suitable parameter choices, this will be true for most choices of f, and the actual computation of these

inverses is easy using a modification of the Euclidean algorithm. We will denote these inverses by Fq and Fp, that is,

$$F_q * f \equiv 1 \ (mod \ q)$$

and

$$F_p * f \equiv 1 (mod \ p)$$

Bob next computes the quantity

$$h \equiv F_q * g \ (mod \ q)$$

Bob's public key is the polynomial h. Bob's private key is the polynomial f, although in practice he will also want to store Fp.

10. Encryption and Decryption

Suppose that Alice (the encrypter) wants to send a message to Bob (the decrypter). She begins by selecting a message m from the set of plaintexts Lm. Next she randomly chooses a polynomial L and uses Bob's public key h to compute

$$e \equiv p\phi * h + m \ (mod \ q)$$

This is the encrypted message which Alice transmits to Bob

Suppose that Bob has received the message e from Alice and wants to decrypt it using his private key f. To do this efficiently, Bob should have precomputed the polynomial Fp.
In order to decrypt e, Bob first computes

$$a \equiv f * e \ (mod \ q),$$

where he chooses the coefficients of a in the interval from -q/2 to q/2. Now treating a as a polynomial with integer coefficients, Bob recovers the message by computing

$$F_q * a \ (mod \ p).$$

11. Major NTRU advantages and Performance Analysis of cryptosystems

1. Fastest key generation
2. Efficient encryption
3. Efficient decryption
4. Low memory

If the parameters of NTRU N, p, q, d satisfy the following inequality q > (6d + 1) p, decryption doesn't fail. We can consider the following secure parameters: N=7, p=3, q=41, d=2 and according to inequality 41>39

Table 1. Performance analysis of cryptosystems.

Cryptosystems	Symmetric	Encryption	Decryption	Key generation
NTRU	Asymmetric	Fastest	Faster	Easy
DES	Symmetric	Faster	Fastest	Difficult
RSA	Asymmetric	Slow	Slow	Easy

12. Conclusion

In the given paper, we proposed NTRU-based encryption and key generation schemes for securing W-Fi since WPA2 and WPA3 protocols are no more providing secure connection between AP and STA. This approach is an alternative solution to support data integrity, confidentiality, authentication issues. NTRU was offered by evaluation of other asymmetric algorithms such as RSA, ECC. Main advantage of the proposed cryptosystems is their encryption, decryption and key-generation speeds as they are faster than the others.

NTRU doesn't suffer with factorization and discrete logarithmic problems what is main benefit achieving high speeds with lower power of computing. So, asymmetric key protocol with light weight as NTRU is better solution for securing Wi-Fi network.

References

[1] An Internet of Things: Reference Architecture. Symantec.
[2] Tahar Mekhazniaa, Abdelmadjid Zidania. Wi-Fi security analysis. Elsevier. Procedia Computer Science 73 (2015) 172 – 178.
[3] Nazmus Sakib, Shamim Ahmed, Samiur Rahman, Ishtiaque Mahmud & Md. Habibullah Belali. WPA 2 (Wi-Fi Protected Access 2) Security Enhancement: Analysis & Improvement. Global Journal of Computer Science and Technology Volume 12 Issue 6 Version 1.0 March 2012. Online ISSN: 0975-4172 & Print ISSN: 0975-4350. USA.
[4] Joseph Mwangi Dr. Wilson Cheruiyot Dr. Michael Kimwel. Security Analysis of WPA2. Control Theory and Informatics ISSN 2224-5774 (Paper) ISSN 2225-0492 (Online) Vol.5, No.5, 2015.
[5] Rivest R. The RC4 encryption algorithm. RSA Data Security. 1992.
[6] Microsoft Technet Library, How 802.11 Wireless Works, Technical Reference, Available: http://technet.microsoft.com/enus/library/cc757419(WS.10).aspx
[7] Paul Arana, INFS 612 – Fall 2006 “Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)”.
[8] Moen V, Raddum H and Hole K J. Weaknesses in the Temporal Key Hash of WPA. Mobile Computing and Communications Review, 2001. 76-83.
[9] Mathy Vanhoef, Frank Piessens. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. https://papers.mathyvanhoef.com/ccs2017.pdf.
[10] http://searchsecurity.techtarget.com/feature/Control-wireless-vulnerabilities-before-they-control-you.
[11] Kevin Beaver, Peter T. Davis, Devin K. Akin. Hacking Wireless Networks for Dummies. ISBN: 978-0-7645-9730-5. 2005.
[12] https://en.wikipedia.org/wiki/IEEE_802.11i-2004.
[13] https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/
[14] "Wi-Fi Alliance introduces Wi-Fi Certified WPA3 security | Wi-Fi Alliance". www.wi-fi.org. 2018.
[15] "Wi-Fi Certified WPA3 Program". https://www.wi-fi.org/discover-wi-fi/security. 2018.
[16] Wi-Fi Gets More Secure: Everything You Need to Know About
[17] WPA3.https://spectrum.ieee.org/tech-talk/telecom/security/everything-you-need-to-know-about-wpa3. 2018
[18] https://spectrum.ieee.org/tech-talk/telecom/security/everything-you-need-to-know-about-wpa3
[19] Mathy Vanhoef, Eyal Ronen. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd.

[20] Hoffstein J., Lieman D., Pipher J., Silverman J. "NTRU: A Cryptosystem", NTRU Cryptosystems, Inc. (www.ntru.com).
[21] Parasitism C, Prada J. "Evaluation of Performance Characteristics of Cryptosystem Using Text Files", Journal of Theoretical and Applied Information Technology, Jatit, 2008
[22] Hoffstein J., Pipher J., Silverman J. An Introduction to Mathematical Cryptography, New York, 2008, http://www.springerlink.com/content/978-0-387-77993-5#section=229331&page=4&locus=51
[23] Hoffstein J., Pipher J., Silverman J. " NTRU – A ring based public key cryptosystem"
[24] Hoffstein J., Lieman D., Pipher J., Silverman J. "NTRU: A Public Key Cryptosystem", NTRU Cryptosystems, Inc. (www.ntru.com).