Encryptsy – An AES Encrypted System for voice/data over Internet using DigiKey and VPN

Kazi Sanam
Professor
Information Technology Department
M.H. Saboo Siddik College of Engineering

Kazi Neha
Information Technology Department
M.H. Saboo Siddik College of Engineering

Mun Alifiya
Information Technology Department
M.H. Saboo Siddik College of Engineering

Chachiya Shahanawaz
Information Technology Department
M.H. Saboo Siddik College of Engineering

ABSTRACT
Safety is a major concern in public network data handling, correspondence, delivery of messages, and electronic transactions. Encryption is to ensure sensitive information is secure. The focused area of study at VoIP is related to Voice data privacy and quality of service. In these areas VoIP encryption and voice data confidentiality transforms into a difficult one. As VoIP sends the voice/data packet through the public internet, there is risk of voice data confidentiality. Furthermore, the exchange of cryptographic keys to encrypt the media stream is vulnerable to attacks such as MITM (Man in the Middle Attack). Hence, there is a need for stronger key management. For the same purpose, a physical key will be used for the encryption/decryption. This will avoid sharing of keys over the Internet and symmetric encryption will be done on voice/data packet and will be passed over VPN.

Keywords
Encryption, QoS, VoIP, VPN, MITM, Physical Key.

1. INTRODUCTION
Since the Internet began to be knowns by the public through the Web later in 1980, it has become a communication network that connects the globe. Software and networking have become a very helpful human necessity to complete many jobs easily, correctly and effectively. Recently, data protection and privacy have been of significant concern and vital for different communications networks, in this scenario almost all data is distributed over a network, such as a LAN or the Internet, so that unauthorized parties cannot access or use it. Back then when PSTN (Public Switched Telephone Network) where used for communication, there was a problem of wiretapping. In order to prevent such a situation VoIP (Voice over Internet Protocol) was introduced. Among them all, Voice over Internet Protocol (VoIP) using the Internet through the advancement of Internet-based voice transmission technology is evolving rapidly to the degree that it can replace the Public Switched Telephone Network (PSTN). There are many ways that can be used to provide security to data that is being communicated with cryptography.

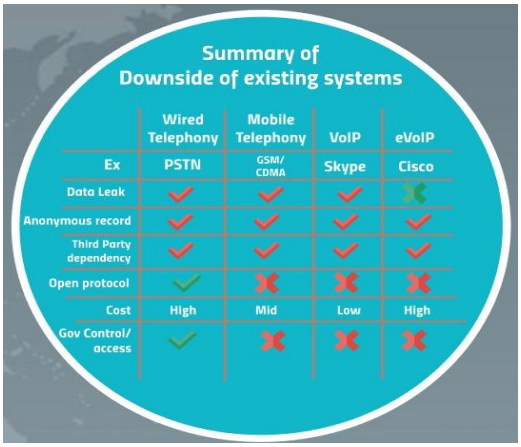

Figure 1 Comparison of Methodology

Cryptography (secret script) is the science and art of transforming messages to secure and resist attack-resistant information [1]. Encryption algorithm executes replacements of bytes and matrix transformations on the plaintext (original message before encryption) and converts it to cipher text (jumbled message). The VoIP service has a variety of security vulnerabilities, such as DoS (Denial of Service), VoIP SPAM, and eavesdropping. PSTN has a closed network infrastructure which offers physical line switching contact. Therefore, in order to access the traffic, the attacker must have knowledge of the qualified PSTN signal mechanism. The IP network is therefore available to any Internet user. It is therefore necessary to protect VoIP call confidentiality.

1.1 Symmetric vs asymmetric.
In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. Whereas in asymmetric encryption there is a set of private and public key for encryption/decryption. The key should be distributed before transmission between entities. The other advantage of symmetric over asymmetric is that Asymmetric encryption techniques are nearly 1000 times slower than Symmetric techniques, because they require more power to process computations [2].

1.2 AES.
The AES algorithm is proven to be highly secure, faster and strongly encrypted and is known for great skills and ease. It has 128, 192 or 256 bits variable key length; 256 by default. AES (Advanced Encryption Standard), [3] which is a very good symmetric key algorithm, is also a block cipher

algorithm which uses replacement, permutation, and number of rounds on each block which will be encrypted.

1.3 TCP v/s UDP.

The VOIP can be implemented using two protocols namely TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Today, most Internet telephony systems use either TCP or UDP to perform their Voice-over-IP (VoIP) operations. The results suggest that UDP tunnel allows more effective use of the connection and offers a radically improved transfer times and speed compared to TCP tunnel [4]. This option may be problematic, because TCP is not ideal for interactive traffic. Sending data packets on the internet can be vulnerable to various attacks. Hence use of VPN (Virtual Private Network) is suggested. Since VPN operates with its own private network, in essence of its functionality it has the advantages over other security techniques and security VPN also works without dropping or delaying calls. To avoid sharing of key online on the internet we will be using a physical key. This will avoid MITM (Man in The Middle) Attack.

1.4 Quality of Service (QoS).

QoS analysis is a crucial issue in obtaining desired quality of voice. Observing end-to-end delay and loss behaviours of packets and jitter are the parameters related to QoS. In VoIP, jitter is the variation in time between arrivals of packets and is usually caused by waiting in router queues which is caused by congestion or a change in path. No jitter occurs where a network has no variation in packet arrival times [5].

2. PROPOSED METHODOLOGY

The main contribution of this paper is that it highlights that the adversary does not initially have to be on the route of VoIP traffic to execute the MITM attack. We are proposing a separate VOIP program for the network. In order to avoid unauthorized access, the very first user has to connect to the device. Authentication can also be done using a fingerprint detector on a physical key.

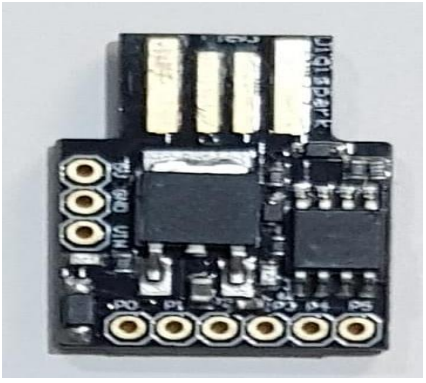

Figure 2 DigiKey

Digikey(Physical Key):The high-performance, low-power Microchip 8-bit AVR RISC-based microcontroller combines 8KB ISP flash memory, 512B EEPROM, 512-Byte SRAM, 6 general purpose I/O lines, 32 general purpose working registers, one 8-bit timer/counter with compare modes, one 8-bit high speed timer/counter, USI, internal and external Interrupts, 4-channel 10-bit A/D converter, programmable watchdog timer with internal oscillator, three software selectable power saving modes, and debugWIRE for on-chip debugging. The device achieves a throughput of 20 MIPS at 20 MHz and operates between 2.7-5.5 volts. By executing powerful instructions in a single clock cycle, the device achieves throughputs approaching 1 MIPS per MHz, balancing power consumption and processing speed [6].

The user then has to dial the number. The connection begins once the call is signed in. The man-in - the-middle attack (MITM) has proved to be one of the most serious threats to the security and trust of current VoIP protocols and systems. In our network real-time communication is achieved where voice data packets are sent from one device to another. To avoid confidentiality, integrity and data availability, the live voice data packets end up encrypted using AES 256 (Industry Gradient Encryption Algorithm).

The encryption algorithm is symmetric in that Symmetric is faster than asymmetric The VoIP uses VPN technology to improve security and QoS. OpenVPN provides high velocity, reliable and secure connection. One of the common mistakes when considering Voice over IP Security is to view this technology and its applications like all other network-based applications and use traditional security measures as a result. This approach fails to consider the fundamental property that distinguishes VoIP from conventional network-aware technologies. Mostly in encryption and decryption methods, the key is exchanged over the internet using key exchange algorithms such as deffie-helmen key exchange etc. Once the key is shared on the internet, the middle attack is highly likely and cannot be avoided. Therefore, to take security at another level we will be providing a Physical Key. So, we will never exchange the key over the internet to prevent this, instead the key to contact encryption will be kept on physical key. The key must be plugged into the system to start the communication user and the system will automatically retrieve the key from the physical key and encrypt data using that key. The receiver also has to plug in the physical key to receive the call. The system will automatically pick up the key and decrypt the data packets, as the communication key is never shared on the internet, there is no chance of key dropping and man in the middle attack. If the host is infected, then the call from the infected host can be tapped to. The user must boot the Linux from live Operating System (OS), and then start the VOIP system. The user then has to attach the physical authentication key and provide the contact key. Once the call has been completed the key can be removed and the system can be shut down. Since the OS are alive, there will be no changes in OS if somebody tries to harm them.

3. ALGORITHM

The algorithm works on 2 sides namely sender and receiver.

(A) Sender:

1. Start
2. Authenticate the user
3. Check physical key and fetch encryption from physical key.
4. Make a connection using VPN.
5. Take an audio packet from the mic.
6. Encrypt audio packets using AES-256.
7. Send encrypted packets via VPN.

(B) Receiver:

1. Start
2. Authenticate the User
3. Check physical key and fetch encryption from physical key

4. Make a connection using VPN
5. Receive audio packets and decrypt it
6. Play decrypted audio using speaker.

4. FLOWCHART

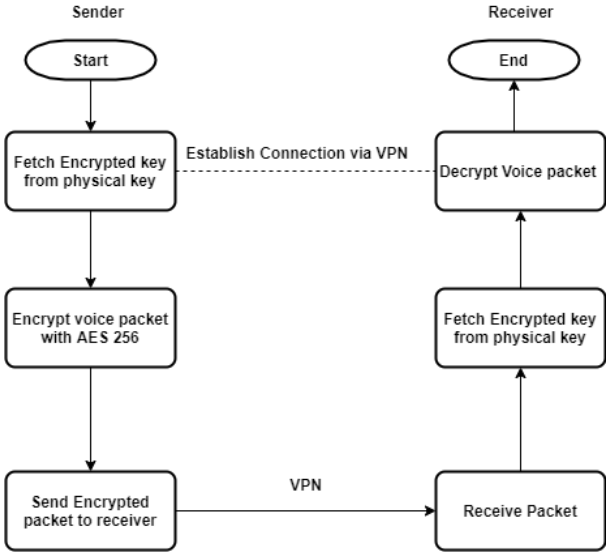

Figure 3: Flowchart of Encryptsy

The above diagram depicts the flow of system. The sender (caller) has to first attach the physical key and then dial the secure ID. The connection between sender and receiver will establish via VPN. The receiver will receive the encrypted packet and will decrypt is using DigiKey of the receiver.

5. IMPLEMENTATION

5.1 Attach the physical key

Figure 4 Screenshot for attaching physical Key

Attach the DigiKey (Figure 3.1 DigiKey) for authentication purposes which contains encryption and decryption key**.**

5.2 Enter the Secure ID

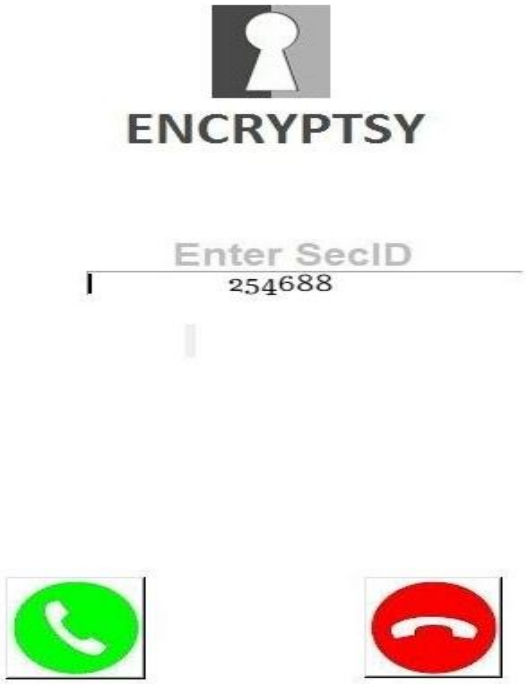

Figure 5 Screenshot for entering Secure ID

Enter the unique secure ID to initiate communication. In the backend the database will be maintained that will include the user's network IP and it is dynamically updated.

5.3 Connection is established.

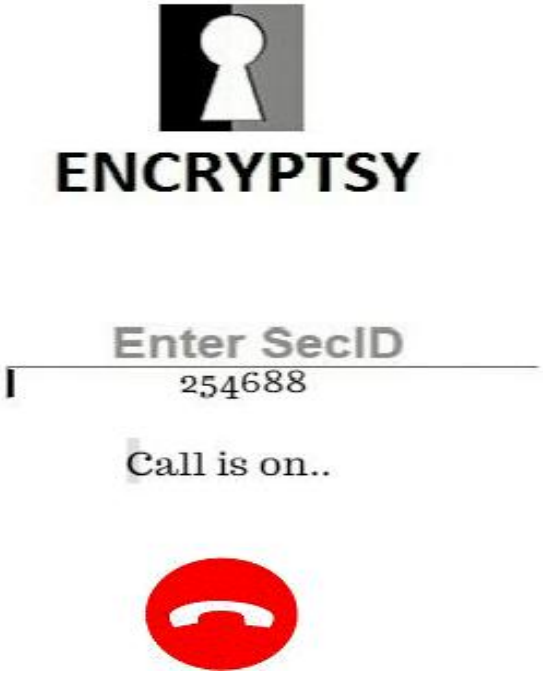

Figure 6 Screenshot for established connection

As soon as the unique secure ID is entered the connection will be established between the two clients,

6. RESULT ANALYSIS

The following are the result analysis for our system:

(1) The MITM attack on VoIP is much more realistic than previously thought. Hence, the system has features such

as Military grade encryption, Encrypted audio call, Encrypted conference call

(2) Extended security via VPN since securing all nodes along the path of VoIP traffic is not adequate to prevent MITM attack on VoIP.

(3) The implemented system is platform and third-party independent and use open source protocol to avoid vulnerabilities of non-VoIP-specific protocols (e.g., DNS) that can indeed lead to compromise of VoIP.

7. CONCLUSION

After conducting study, implementing and result analysis of VoIP, it is clear that VoIP security is in an incipient phase at the moment. Security for a VoIP system should begin with solid security on the internal network. It should be protected from the threats of attached hostile networks and the threats of the internal network. The load of the VoIP system should be accommodated by the network and the servers involved, ensuring that proper resources are in place and available. The key contribution of this paper is that it demonstrates that the adversary does not have to be initially in the path of VoIP traffic to conduct the MITM attack. The system should be protected from attacks and provide Confidentiality and Integrity. Striking a balance between security and the business needs of the organization is key to the success of the VoIP Deployment.

8. FUTURE Scope

Taking into account the importance of encryption, especially on the Internet, it is clear that a balance needs to be found between high performance and high protection. More studies such as the feasibility of using selective encryption to reduce the delays caused by cryptography must be performed and further performance parameters must be included.

9. REFERENCES

[1] Abdalbasit Mohammed Qadir Software Engineering Department,"A Review Paper on Cryptography "

[2] Monika Agrawal Department Of Computer Science,"A Comparative Survey on Symmetric Key Encryption Techniques ",Monika Agrawal et al. / International Journal on Computer Science and Engineering (IJCSE)

[3] Ria Andriani Magister Teknik Informatika Universitas AMIKOM Yogyakarta Yogyakarta,"Comparision Of AES 128, 192 And 256 Bit Algorithm For Encryption And Description File ",2018 3rd International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia

[4] Horia Vlad Balan International University Bremen,"An Experimental Evaluation of Voice Quality over the Datagram Congestion Control Protocol ",IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2007 proceedings.

[5] Ehsan Faghihi Engineering Department IRIB University,"QoS Parameters Analysis in VoIP Network Using Adaptive Quality Improvement",SPIS2015, 16-17 Dec. 2015, Amirkabir University of Technology, Tehran, IRAN

[6] microchip.com/wwwproducts/en/ATtiny85

[7] Sulafa Khaled Talha Faculty of Mathematical Sciences University of Khartoum Khartoum, Sudan," Evaluating the Impact of AES Encryption Algorithm on Voice over Internet Protocol (VoIP) Systems", 2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE)

[8] Stefan Hofbauer Danube Data Center GmbH, Network Department, Floridsdorfer Hauptstrasse 1, 1210 Vienna, Austria," CDRAS: An approach to dealing with Man-in-the-Middle attacks in the context of Voice over IP", 2011 Sixth International Conference on Availability, Reliability and Security