High-Performance and Cost-Effective VoIP Security Techniques for Operations on IPv4, IPv6, and IPv4/IPv6 Networks

Capstone Research Project

April 22, 2016

Moiz Hussain
Praniti Gupta
Shirin Bano
Vineet Kulkarni

Interdisciplinary Telecom Program
University of Colorado Boulder

Levi Perigo, Ph.D.
University of Colorado Boulder
Dan Williams
Firmware Engineer (Inovonics)

***Abstract*— Voice over IP (VoIP) is the new standard technology for telephony, gradually replacing the old Public Switched Telephone Network (PSTN). This research focuses on the security aspect of VoIP systems. Unsecured VoIP systems are vulnerable to malicious attacks. However, the overhead of the security techniques hampers the performance of VoIP systems. This research analyzes how a VoIP system performs with different security techniques. The performance of the VoIP system is analyzed on different types of data networks such as IPv4, IPv6, and IPv4/IPv6 mixed networks and in scenarios such as with and without network traffic. Additionally, the research includes a cost-benefit analysis of the security techniques, to determine their cost effectiveness. Based on the performance analysis and cost-benefit analysis, this research proposes three security techniques that can be applied to VoIP systems deployed on IPv4, IPv6, and IPv4/IPv6 networks.**

Keywords— VoIP, security, performance, cost-benefit analysis

I. RESEARCH QUESTION AND PROBLEM SETTING

What are the techniques that can secure a VoIP system operating on IPv4, IPv6, or IPv4/IPv6 networks, and also provide an optimum performance and cost-effectiveness, both on uncongested and congested networks?

VoIP is a technology that transmits voice as IP packets. In the near future, VoIP will be used by home users, businesses, and government organizations [1]. VoIP will be used for diverse purposes such as normal calls, emergency calls, business calls, and calls with important data. VoIP systems use the Internet as their underlying infrastructure. Since the Internet is a public platform carrying private VoIP calls, it becomes imperative to secure VoIP systems so that they are usable for all types of users and purposes. The downside of adding security to any system is that it also adds processing overhead, which can adversely affect the performance of the system. Therefore, there is a trade-off between desired security and performance. This research aims to address this trade-off issue for a VoIP system, by determining the techniques that provide an optimum level of security and performance.

IPv4 is a protocol used to transmit packets through various networks on the Internet. IPv4 uses a 32-bit address scheme, which limits the number of addresses that can be used on the Internet. To avoid complete exhaustion of usable addresses, a new protocol named IPv6 was developed. New organizations are being allocated IPv6 addresses while organizations with existing IPv4 networks are trying to migrate to IPv6 networks. However, the transition to IPv6 addresses is a time-consuming process, as it includes reconfiguring the entire network with new addresses. These organizations are gradually migrating to IPv6, and hence, they have networks with both IPv4 and IPv6 addresses. Therefore, the future VoIP systems for the old and new organizations will be deployed on IPv4, IPv6, or IPv4/IPv6 mixed networks. This research determines the effect of security on the performance of these VoIP systems, helping the organizations make a decision about the security techniques they want to deploy.

This research considers network traffic while analyzing the performance of the security techniques, in order to gauge the effect of security on the performance of VoIP systems in real-world networks. In addition, this research considers the cost-effectiveness of the security techniques, to make sure that implementing these techniques is a feasible investment for organizations. This research is based on the results and analyses of the past work conducted in the VoIP security field, and extends further in determining high-performance and cost-effective security techniques for future VoIP deployments.

II. RESEARCH SUB-PROBLEMS

To answer the research question, it is broken down into three sub-problems –

1. **What are the security techniques that provide an optimum performance to a VoIP system operating on uncongested IPv4, IPv6, and IPv4/IPv6 networks?**

The aim of this research sub-problem is to analyze the performance of a VoIP system with various security techniques, on an uncongested network. The performance of the VoIP system without any security is considered as the benchmark. Security techniques are applied one by one to the VoIP system and the performance of the VoIP system is observed with each technique and this process is performed for the three types of data networks. Since the network is uncongested, the performance of the system associates directly to the security technique being deployed.

This research sub-problem answers the first part of the research problem, that is, which security techniques provide an optimum level of performance to a VoIP system running on uncongested IPv4, IPv6, and IPv4/IPv6 mixed networks.

2. **What are the security techniques that provide an optimum performance to a VoIP system operating on congested IPv4, IPv6, and IPv4/IPv6 networks?**

The first sub-problem gives the benchmark of how a VoIP system performs with various security techniques when there is no network traffic. However, real-world data networks will not only carry VoIP traffic but also web traffic, email traffic, and traffic generated due to uploads and downloads of files. Though the network might not be fully congested, the performance of the VoIP system can be affected.

Therefore, the second sub-problem aims to analyze the performance of a VoIP system on a congested network, with different security techniques. The performance of the VoIP system without any security is considered as the benchmark. Security techniques are applied one by one to the VoIP system and the performance of the system is observed with each technique and this process is repeated for the three types of data networks.

Adding to the first sub-problem, this sub-problem answers the second part of the research problem, that is, which security techniques provide an optimum level of performance to a VoIP system running on congested IPv4, IPv6, and IPv4/IPv6 networks.

3. **What are the costs and benefits associated with the high-performance security techniques?**

It is important to understand the costs and benefits associated with the high-performance security techniques, because, it may not be a reasonable investment for an organization to implement a high-performance security technique if it is not cost-effective. Accordingly, the third sub-problem aims to determine the cost-effectiveness of these security techniques.

The first two sub-problems address the performance aspect of the security techniques and the third one addresses the cost-benefit aspect of the high-performance security techniques. Therefore, when all the sub-problems are solved, they determine the cost-effective security techniques that deliver an optimum performance and security to a VoIP system operating on uncongested and congested data networks.

III. LITERATURE REVIEW

Legacy voice system or PSTN has advantages such as no packet loss and high performance. However, PSTN also has disadvantages that limit its use. PSTN is a circuit-switched technology, which means that the connection between the endpoints of a call is established before the call is placed. In order to establish a connection beforehand, PSTN uses a dedicated channel for each call. Therefore, there are issues such as bandwidth wastage and high costs associated with PSTN, which is one of the reasons why PSTN is being replaced by VoIP [2].

VoIP is a packet-switched technology, which means that the connection between the endpoints of a call is established once the call is initiated. Since packet-switched networks share the available bandwidth, VoIP saves bandwidth. Since VoIP systems operate on the existing Internet infrastructure, installation and operational costs for VoIP systems are low. VoIP phones can be software based, and therefore, are portable. VoIP offers a plethora of features such as presence, voicemail, Interactive Voice Response (IVR), and caller-ID functions [3]. Presence technology helps in locating and identifying VoIP devices. IVR enables interaction between computers and humans, to automate repetitive and lengthy processes and to improve the user experience. Since VoIP systems are simple to implement and maintain, they are being used extensively.

Figure 1 shows, how a VoIP call is established between two phones, using the Session Initiation Protocol (SIP) for signaling. SIP is a protocol used by VoIP to establish a connection between the endpoints of a call. There are various messages exchanged using SIP, which enable the endpoints to recognize each other, negotiate the parameters of the call, and establish a channel to exchange audio or video media.

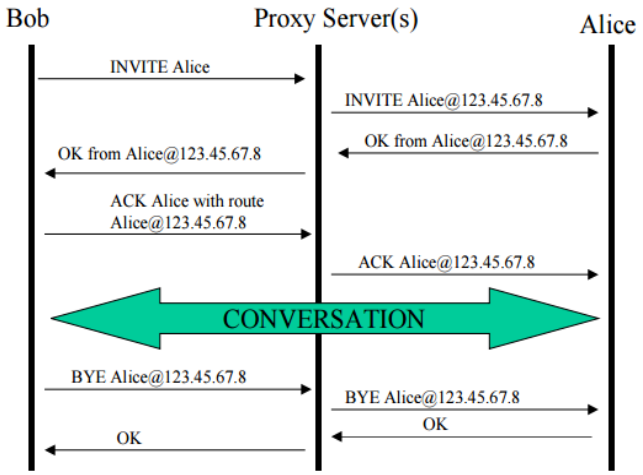

Figure 1: VoIP call setup [4]

As seen in the figure, there are two parts to a VoIP call – signaling and media. Past research has tried to identify the attacks to which an unsecured VoIP system is vulnerable. These attacks can be divided into four domains; viz. – attacks on VoIP signaling, attacks on VoIP media, attacks on the data network on which a VoIP system works, and attacks on a functioning VoIP system. Some of the attacks on VoIP signaling are SIP registration hijacking, SIP message modification, and SIP redirects [5-7]. In the SIP message modification attack, attackers intercept SIP messages and modify them to exploit vulnerabilities in a VoIP system. In attacks such as SIP registration hijacking and SIP redirects, attackers reroute SIP messages to themselves and collect private information about a call, such as the called party and calling party, information about the SIP devices, and what type of media will be exchanged. Research has also been conducted to identify the media attacks on a VoIP system. VoIP uses Real-time Transport Protocol (RTP) to transport the media. Some common attacks that have been identified on VoIP media are RTP payload malformation and RTP tampering [5] [6]. In these attacks, attackers modify RTP packets to exploit vulnerabilities in a VoIP system. This RTP modification also affects the confidentiality of a call. The third set of attacks is identified to affect the underlying data network. It is important to prevent these attacks, as, without a data network, the signaling system in VoIP will not work. Some of the attacks that affect the data network functionality are IP spoofing, MAC spoofing, Transmission Control Protocol (TCP) SYN flood, and TCP and User Datagram Protocol (UDP) replay attacks [4] [8]. TCP is a transport layer protocol used for services requiring reliability, such as web browsing, while UDP is a transport layer protocol used for services requiring high speed, such as domain name resolution. With the help of attacks such as IP spoofing and MAC spoofing, the attackers can pose themselves as legitimate entities of the VoIP system and can intercept all the VoIP messages. TCP SYN flood and TCP/UDP replay attacks involve sending a high number of packets to a data network, such that it consumes network resources to an extent where the data network goes down. The last domain of attacks is the attacks on a functioning VoIP system. These attacks can bring down a working VoIP system. A whitepaper by Xin and a research paper by Perez-Botero and Donoso have identified the attacks on a functioning VoIP system. Some of the attacks are Denial of Service (DoS), eavesdropping, and spam over VoIP [4] [6] [9]. Attacks such as DoS and spam over VoIP, burden the network with excessive and unnecessary traffic, leading to packet loss and resource consumption on network devices. Attacks such as eavesdropping, affect the confidentiality of the VoIP system. Considering the domains of attacks, there are four parts to VoIP security – securing VoIP signaling, securing VoIP media, securing the data network, and securing a functioning VoIP system.

Another method of studying the attacks on a VoIP system is by classifying the attacks based on the network layers they affect. This classification helps in developing security algorithms which are restricted to a particular layer or a set of layers. The paper by Coulibaly and Liu presents the types of attacks in the VoIP system and the layers they affect [8].

In a research paper based on VoIP security mechanisms, Shan and Jiang discuss some of the existing security mechanisms in VoIP [10]. The current security mechanism for SIP messages is the use of Transport Layer Security (TLS), which encrypts all SIP signaling messages. Similarly, to secure the media, a secure version of RTP called Secure RTP (SRTP) is used [6].

Apart from applying security to VoIP signaling or media, implementing security at the IP layer or the Network layer secures the data network on which the VoIP system works as well as the VoIP traffic. Research has shown that deploying VoIP over IPsec tunnels or Virtual Private Networks (VPNs) secure the data network as well as the VoIP system [11]. IPsec tunnels or VPNs are virtual overlay networks over the Internet that connect two private networks, such as internal networks of an organization. IPsec tunnels secure the traffic flowing through them by encryption and authentication techniques.

To gain from the benefits of VoIP, it is important to maintain the performance of the VoIP system, even with an added element of security. Accordingly, research has been carried out to study the performance of VoIP in IPv4 and IPv6 environment. For instance, Ahmed et al., discuss the effect of Quality of Service (QoS) for VoIP over IPv4 and IPv6 [12]. However, the research does not comment on the performance of a VoIP system, when security is added. Similarly, Rahangdale et al., talk about SIP security, but not about the performance of a VoIP system when SIP security is implemented [13]. Two separate studies discuss the performance of SIP with IPv4 and IPv6 IPsec tunnels but do not evaluate and compare the results with other security techniques [14] [15]. The research that analyzes the performance of TLS on a VoIP system presents a comparative analysis of the performance of the VoIP system with and

without TLS. However, the research does not encompass other security techniques [16-18]. Research has been conducted to identify techniques to secure VoIP media. The research focuses only on the media domain, not other domains of a VoIP system [19]. None of the previous research has considered the cost-effectiveness of the security techniques. Overall, there has been minimal research conducted to find high-performance and cost-effective security techniques for VoIP systems working on IPv4, IPv6, and IPv4/IPv6 networks.

The methodology used in the past research involves building a testbed of a VoIP system and analyzing its performance with security techniques. The testbeds used were either pure IPv4 or pure IPv6 networks. Few researchers used a mixed network, comprising of both IPv4 and IPv6 addresses. None of the past work considered all security techniques in one research paper. Therefore, the previous research does not implement an exhaustive and detailed research methodology. It does not analyze all the security techniques on all types of data networks.

This research used a methodology similar to the previous research, that is, to setup a testbed of a VoIP system. In addition, for this research, the VoIP system was deployed over all types of networks – IPv4, IPv6, and mixed IPv4/IPv6. In this research, all the security techniques were applied; both individually and in combination. The performance was measured with respect to parameters such as signaling delay, media delay, and jitter [20]. Moreover, a cost-benefit analysis was performed as a part of this research, to understand the cost-effectiveness of the security techniques. The methodology was designed to overcome the shortcomings in the methodology used in previous research.

IV. RESEARCH DESIGN AND METHODOLOGY

This research was based on testing a VoIP system running on different data networks with different security techniques applied, and then evaluating the results of all the tests. The research included an analysis of costs and benefits of the security techniques. The research was designed such that the performance tests were carried out for each security technique and each type of data network. The cost-benefit analysis was performed for the three high-performing security techniques for each type of data network.

To address the first two sub-problems, we had to conduct the performance analysis of the security techniques on a testbed of a VoIP system. For the testbed, we decided to use the following hardware and software components –

Hardware	Software
Dell Desktop Cisco 3825 Router HP Laptops Dell Laptops	PhonerLite Softphones Asterisk Private Branch Exchange (PBX) Wireshark iPerf Tool

Table 1: Hardware and software components

The components of the testbed were as follows –

a. Softphones – There were two softphones used to initiate VoIP calls. Softphones are software tools which can be used as phones. The softphones were installed on two HP laptops. We used PhonerLite softphones, as they support both IPv4 and IPv6, and all the security techniques
b. Asterisk PBX – To enable the VoIP functionality in the two softphones, they were registered to the two Asterisk PBXs. PBX is a device that enables call routing and other VoIP functions for the VoIP phones. We used Asterisk as it is an open source PBX and it supports all the security techniques. The Asterisk PBX software was loaded on two Dell Desktop machines
c. Cisco 3825 Routers – The two Cisco routers were used as data routers, to connect two Local Area Network (LAN) segments. The Cisco 3825 routers were loaded with a software that supports VPN configuration
d. Capturing PCs – All the VoIP traffic on the network was captured on the two capturing PCs running Wireshark. Wireshark is a software tool that can be used to sniff network traffic. Two Dell desktops were deployed as capturing machines
e. Traffic Generating PCs – These PCs were used to generate network traffic, required for the second sub-problem. Two Dell laptops were used to generate traffic, using the iPerf tool. iPerf is a software tool that is used to generate network traffic. It can generate multiple types of traffic. The amount of traffic and duration for which the traffic is sent can be adjusted as required.

We used the above components to build a testbed as shown in the following figure –

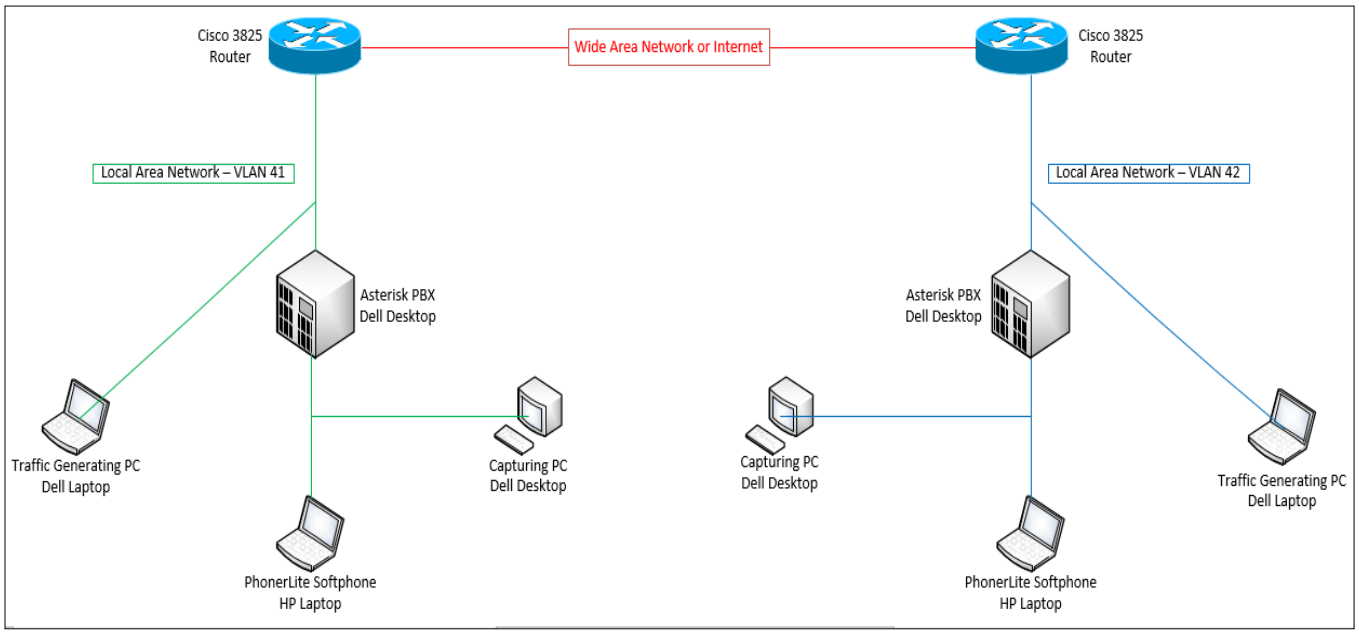

Figure 2: Network diagram

In this research, we considered the following security techniques –

a. VPN
b. SRTP
c. TLS
d. VPN-SRTP
e. VPN-TLS
f. SRTP-TLS
g. VPN-SRTP-TLS

The three main techniques that we considered were VPNs, SRTP, and TLS. We deployed these techniques individually, as well as in combinations with each other.

We analyzed the following parameters for each call –

a. Signaling Delay – Time taken to establish a VoIP call between two phones
b. Media Delay – Difference between the time when the phone number is dialed and the first RTP packet is received. Media Delay is the most important delay from a user's perspective
c. RTP Media Delay – Maximum delay between two RTP packets
d. RTP Jitter – Mean jitter seen in RTP packets. Jitter is the variation in the time taken for packets to traverse a system.

The first performance test was carried out on an uncongested network. Firstly, we deployed the VoIP system without any security, on a pure IPv4 data network. We initiated five calls from each softphone. The call duration was 30 seconds each. Simultaneously, all the call traffic was captured on Wireshark running on the capturing PCs. The captures were analyzed to find the values of the performance parameters. Secondly, we deployed the VoIP system with the security techniques, on the pure IPv4 data network. We repeated the performance tests with each security technique. All the captured call traffic was analyzed and the performance of the VoIP system with each security technique was determined. Thirdly, we configured the network as a pure IPv6 network. The performance tests and analyses were repeated exactly as conducted on the IPv4 network. Lastly, the network was configured as a mixed IPv4/IPv6 network. The performance tests and analyses were repeated as above.

The second performance test was carried out on a congested network. The network was not congested to a full 100%. Rather, we generated traffic to fill the network between 40%-60%, in order to simulate a real-world network. We used the iPerf tool on the Traffic Generating PCs, in order to generate a bi-directional UDP and TCP traffic. Initially, we deployed the VoIP system without any security, on a pure IPv4 data network. We generated UDP traffic and initiated three calls from each softphone. Then we generated TCP traffic and initiated three calls from each softphone. All calls lasted 30 seconds each. Simultaneously, all the call traffic was captured on Wireshark running on the Capturing PCs. The captures were analyzed to determine the performance of the VoIP system. Similar tests were performed with each security technique. All Wireshark captures were analyzed and the results were compiled. The above tests were repeated exactly with a pure-IPv6 network and an IPv4/IPv6 mixed network.

When using a VoIP system, users base their experience on the time required to setup the call and hear the audio, which is represented by the Media Delay parameter. The RTP delay

and jitter are on the orders of few milliseconds and are almost the same with any security technique and any data network. Therefore, for this research, we determined high performing security techniques based on the Media Delay parameter. We determined the three fastest security techniques, for each type of data network, and for uncongested and congested networks.

We performed a cost-benefit analysis for each of the three security techniques. We considered the following factors for the cost-benefit analysis –

a. How is the user experience of the call with the security technique?
   We considered the Media Delay parameter to quantify the user experience of the VoIP system.

b. What is the cost of deploying the security technique on a new installation of a data network similar to our testbed?
   To determine the cost of deployment, we considered the cost of building a new data network similar to our testbed and implementing the security technique on it. We considered the hardware and software costs required to build such a network and deploy the security technique.

c. How easy is it to deploy the security technique?
   We determined the ease of deployment of the security technique based on the configuration required to implement that technique. Furthermore, we considered whether the security technique is a plug-and-play type of technique or is it a technique wherein configuration changes and maintenance is required.

d. How secure is the security technique?
   To determine the level of security provided by the technique, we analyzed whether the security technique itself is strong enough or can be easily compromised.

e. What is the complexity of troubleshooting the VoIP system with the security technique?
   The complexity of troubleshooting is important from the post-deployment point of view. We considered a variety of scenarios that could occur if there are issues in the functioning of the data network or the VoIP system. Considering these issues, we determined the complexity of troubleshooting the data network or the VoIP system, with the security technique applied.

The above factors determine how beneficial it is to implement a security technique and what cost factors are associated with it. We have considered tangible and intangible cost factors for each security technique. After analyzing all the results, we have, for all types of data networks, and for uncongested and congested networks, the three fastest security techniques and the costs and benefits associated with them.

V. RESEARCH RESULTS

Following are the results of our analyses -

	VPN	**VPN-SRTP**	**SRTP-TLS**
Delay (seconds)	0.2625	0.268	0.268
Cost of Deployment (USD)	20100	20100	18100
Ease of Deployment	High	Medium	Low
Risk of Cracking	AES - No Risk	VPN - No Risk. SRTP can be easily decrypted	No Risk
Troubleshooting Complexity	Medium	Medium	High

Table 2: Uncongested IPv4

	SRTP	**VPN**	**VPN-SRTP**
Delay (seconds)	0.2618	0.2647	0.2661
Cost of Deployment (USD)	18100	20100	20100
Ease of Deployment	High	High	Medium
Risk of Cracking	High	AES - No Risk.	VPN - No Risk. SRTP can be easily decrypted
Troubleshooting Complexity	Low	Medium	Medium

Table 3: Uncongested IPv6

	VPN	**SRTP**	**VPN-SRTP**
Delay (seconds)	0.2588	0.2624	0.2639
Cost of Deployment (USD)	20100	18100	20100
Ease of Deployment	High	High	Medium
Risk of Cracking	AES - No Risk	High	VPN - No Risk. SRTP can be easily decrypted
Troubleshooting Complexity	Medium	Low	Medium

Table 4: Uncongested Mixed

	VPN-SRTP-TLS	SRTP	VPN-SRTP
Delay (seconds)	0.2507	0.2663	0.2674
Cost of Deployment (USD)	20100	18100	20100
Ease of Deployment	Low	High	Medium
Risk of Cracking	AES - No Risk	High	VPN - No Risk. SRTP can be easily decrypted
Troubleshooting Complexity	High	Low	Medium

Table 5: Congested IPv4

	VPN	SRTP	TLS
Delay (seconds)	0.261	0.2645	0.2671
Cost of Deployment (USD)	20100	18100	18100
Ease of Deployment	High	High	Low
Risk of Cracking	AES - No Risk	High	No Risk
Troubleshooting Complexity	Medium	Low	High

Table 6: Uncongested IPv6

	SRTP	VPN-SRTP	VPN
Delay (seconds)	0.2545	0.2601	0.2638
Cost of Deployment (USD)	18100	20100	20100
Ease of Deployment	High	Medium	High
Risk of Cracking	High	VPN - No Risk. SRTP can be easily decrypted	AES - No Risk
Troubleshooting Complexity	Low	Medium	Medium

Table 7: Congested Mixed

We determined the cost of deployment based on the following formula –
Cost of Deployment = (Cost of the Softphones) + (Cost of the Cisco Routers) + (Cost of the security software required to support VPN)

The costs for each component are as follows -
Cost of Softphone - $50
Cost of Cisco Router - $9000
Cost of Software License - $1000

The results are shown for all the data networks, and for congested and uncongested conditions.

VI. DISCUSSION OF RESULTS

The performance analysis shows that for all types of data networks, VPN, SRTP, or their combination, are the fastest techniques. Therefore, the user experience of a call will be the best if these techniques are used. However, in terms of costs and benefits associated with the technique, different organizations can use different security techniques, according to their requirements.

The cost of deployment for VPN is slightly more than the security techniques that do not involve VPN, because of the special software requirements for VPN. SRTP and TLS do not require a special software running on the Cisco router.

The configuration requirement for VPN is less than that for SRTP and TLS. However, VPN must be configured on both sides of the IPsec tunnel. If both sides are not managed by the same organization, there can be issues with configuration and management of the VPN. In terms of configuration, SRTP is slightly difficult than VPN, because, in order to configure SRTP correctly, a VoIP expertise is required. The network engineers in an organization can configure VPN, but only those who have a VoIP expertise can configure SRTP. The same applies to TLS. In addition, TLS requires a more complex configuration. The configuration not only depends on the organization but also on certain authorities, known as Certificate Authorities. These are normally managed by different organizations, and hence, there is a dependency in the case of TLS configuration. Therefore, TLS is the most difficult technique to deploy.

SRTP is easier to troubleshoot than VPN or TLS. SRTP only encrypts the voice traffic. The signaling traffic is still clear-text. Since most of the VoIP issues are due to incorrect signaling, the troubleshooting becomes easier with SRTP. For instance, common issues such as one-way audio or no audio are easier to troubleshoot with SRTP. TLS encrypts the signaling part., hence it becomes difficult to troubleshoot with TLS. Moreover, because of the complex configuration of TLS, if there are issues with the TLS configuration itself, it becomes a tedious task to troubleshoot. In the case of VPN, both the signaling and media is encrypted, which makes it difficult to troubleshoot VoIP issues. However, since VPN is simple to configure, issues with VPN configuration and operation are easier to troubleshoot.

The encryption key used in SRTP is transmitted in clear-text and can be sniffed through Wireshark. If TLS is used with SRTP, then the SRTP encryption key is encrypted. Therefore, SRTP is not secure if used individually [21]. However, VPN and TLS are extremely secure techniques. VPN uses Advanced Encryption Standard (AES) encryption, which cannot be compromised. Similarly, TLS uses advanced encryption methods and features that cannot be decrypted.

VPN can secure the signaling and media of the VoIP system. Therefore, it can protect the VoIP system from most

of the attacks on signaling, media, the actual data network, and a functioning VoIP system. However, VPNs are normally not deployed on the internal network of the organization. Therefore, the VoIP system is still insecure inside the organizational network. TLS can secure VoIP signaling on the internal network of the organization. However, it only secures signaling and it might not be implemented over the Internet. Similarly, SRTP secures only the media of the VoIP system and that too, only internal to the organizational network. As per an organization's requirements, any of the above security techniques can be used. For instance, if an organization does not prioritize securing its internal network, then it can use VPN to secure the VoIP system over the Internet.

We have shown the three fastest security techniques and the costs and benefits of using these techniques. The organizations that want to deploy VoIP systems can refer to the results of this research and, depending on their requirements and priorities, the organizations can choose one of these security techniques.

VII. CONCLUSION AND FUTURE RESEARCH

VoIP is an evolving technology in the telephony domain. There are various security issues related to VoIP. Although past research has analyzed security techniques, it does not cover all the security techniques on all types of data networks. This research has performed a comprehensive analysis of all the security techniques. It has considered all types of data networks, and scenarios such as uncongested and congested networks. Moreover, this research has considered the cost-effectiveness of all the security techniques. The results of this research should give an overview of which security techniques have high performance and what are the costs and benefits of using these techniques.

Future research can enhance the research methodology in terms of the number of calls and the duration of the calls. Future research can modify the testbed to suit a particular organization's needs. The modifications might include changing the existing hardware, increasing the hardware, or using proprietary devices. We expect to see future research considering these parameters, thus adding to the Book of Knowledge in the VoIP security domain.

ACKNOWLEDGEMENTS

We would like to sincerely thank Dr. Levi Perigo and Mr. Dan Williams for their insights on our project work and for reviewing our project results and updates. We would also like to extend our sincere thanks to Dr. David Reed and Irena Stevens for their continuous guidance and supervision throughout the project.

REFERENCES

[1] Sudip S. (2015, Jul 05). *"VoIP Services Market to Expand at 9.7% CAGR till 2020 Thanks to Increasing Adoption in Residential and Corporate Sectors"* [Online]. Available: http://www.transparencymarketresearch.com/pressrelease/voip-services-market.htm

[2] US-CERT, "Understanding Voice over Internet Protocol (VoIP)", 2006.

[3] A. B. Johnston, "SIP and the Internet," in *SIP: Understanding the Session Initiation Protocol*, 3rd ed. Boston: Artech House, 2009, ch. 1, pp. 1-23.

[4] National Institute of Standards and Technology, "Security Considerations for Voice Over IP Systems", NIST, Gaithersburg, MD, 2005.

[5] D. Butcher, X. Li and J. Guo, "Security Challenge and Defense in VoIP Infrastructures", IEEE Trans. Syst., Man, Cybern. C, vol. 37, no. 6, pp. 1152-1162, 2007.

[6] J. Xin, "Security Issues and Countermeasure for VoIP", Sans.org, 2007. [Online]. Available: https://www.sans.org/reading-room/whitepapers/voip/security-issues-%20countermeasure-voip-1701.

[7] G. Sonwane and B. Chandawarkar, "Security Analysis of Session Initiation Protocol in IPv4 and IPv6 Based VoIP Network", in *Advanced Computing, Networking and Security*, Mangalore, India, 2013, pp. 187-192.

[8] E. Coulibaly and L. Hao Liu, "Security Of Voip Networks", in *International Conference on Computer Engineering and Technology*, Chengdu, China, 2010, pp. 104-108.

[9] D. Perez-Botero and Y.Donoso, "VoIP Eavesdropping: A Comprehensive Evaluation of Cryptographic Countermeasures," in *International Conference on Networking and Distributed Computing*, Beijing, China, 2011, pp. 192-196.

[10] L. Shan and N. Jiang, "Research on Security Mechanisms of SIP-based VoIP System", in *International Conference on Hybrid Intelligent Systems*, Shenyang, China, 2009, pp. 408-410.

[11] R. Barbieri et al., "Voice over IPsec: Analysis and Solutions," in Computer Security Applications Conference, 2002 © IEEE. doi: 10.1109/CSAC.2002.1176297

[12] H. Ahmed et al., “Performance Analysis of VoIP Quality of Service in IPv4 and IPv6 environment” *International Journal of Digital Content Technology and its Applications*, vol. 8, no. 2, pp. 40–51, Apr. 2014.

[13] T. Rahangdale et al., “An Overview on Security Analysis of Session Initiation Protocol in VoIP network”, *International Journal of Research in Advent Technology*, vol. 2, no. 4, pp. 190–195, Apr. 2014.

[14] T. Hoeher et al., “Evaluating Performance Characteristics of SIP over IPv6”, *Journal of Networks*, vol. 2, no.4, pp. 40–50, Aug. 2007.

[15] R. Yasinovsky et al., “VoIP performance with IPsec in IPv4-IPv6 transition networks”, *Infocommunications Journal*, vol. LXV, pp. 15–23, 2010.

[16] C. Shen, et al., "The impact of TLS on SIP server performance," *IEEE/ACM Trans. Netw.*, vol. 20, no. 4, pp. 1217-1230, Aug. 2012.

[17] M. Ashraf et al., "*An Investigation into the Effect of Security on Performance in a VoIP Network*" [Online]. Available: http://www.glyndwr.ac.uk/computing/research/pubs/sein_adg.pdf

[18] M. Kulin et al., "SIP Server Security with TLS: Relative Performance Evaluation” in International Symposium on Telecommunications, 2012 © IEEE. doi: 10.1109/BIHTEL.2012.6412062

[19] A. Alexander et al., "An Evaluation of Secure Real-time Transport Protocol (SRTP) Performance for VoIP", in *International Conference on Network and System Security*, QLD, 2009, pp. 95-101.

[20] (Jan, 2014). *Testing Voice over IP (VoIP) Networks* (Rev B) Online: Available: https://www.ixiacom.com/sites/default/files/resources/whitepaper/voip-whitepaper.pdf

[21] A. Critelli. (2014, Jun 22). *Hacking VoIP – Decrypting SDES Protected SRTP Phone Calls*. [Online]. Available: https://www.acritelli.com/hacking-voip-decrypting-sdes-protected-srtp-phone-calls/

Appendix A – List of Figures and Tables

Appendix B – List of Acronyms

VoIP	Voice over IP
PSTN	Public Switched Telephone Network
IVR	Interactive Voice Response
SIP	Session Initiation Protocol
RTP	Real-time Transport Protocol
DoS	Denial of Service
TLS	Transport Layer Security
SRTP	Secure Real-time Transport Protocol
VPN	Virtual Private Network
QoS	Quality of Service
PBX	Private Branch Exchange
AES	Advanced Encryption Standard
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Appendix C – Explanation of Terms

VoIP	Technology that transmits voice as IP packets
IPv4	32-bit address scheme used to allocate network addresses to devices
IPv6	128-bit address scheme developed to replace IPv4
Mixed Network	A network consisting of both IPv4 and IPv6 addresses
Presence	A VoIP feature that enables locating and identifying VoIP devices
IVR	A VoIP feature that enables interaction between computers and humans, to automate repetitive and lengthy processes and improve user experience
SIP	A protocol used by VoIP to establish a connection between the endpoints of a call
SIP registration hijacking	An attack in which the attackers intercept the SIP REGISTER message and pose as legitimate endpoints. They can then intercept the actual calls
SIP redirects	An attack in which the attackers reroute SIP messages, affecting the confidentiality of the VoIP system
SIP message	An attack in which the attackers tamper

modification	SIP messages to intercept calls and to exploit the vulnerabilities in a VoIP system
RTP	A protocol used by VoIP to transmit the media, which can be either audio or video
RTP payload malformation and RTP tampering	RTP payload is the audio or video being exchanged through the VoIP system. If it is malformed, it affects the confidentiality of the calls
IP and MAC spoofing	Attacks in which the attackers pose as legitimate users by first intercepting and then spoofing the IP and MAC addresses of the user devices. This spoofing enables the attackers to play with the data being sent to and from the user devices
TCP	A transport layer protocol used for services requiring reliability, such as web browsing
UDP	A transport layer protocol used for services requiring high speed, such as domain name resolution
TCP SYN flood	An attack in which the attackers send high number of TCP SYN packets, consuming the resources of the network
TCP/UDP replay	An attack in which the attackers flood the network with same packets to exploit vulnerabilities
DoS	An attack in which the attackers flood the network with unnecessary but legitimate packets, consuming the network resources to an extent where the network goes down
Spam over VoIP	An attack in which the VoIP system is flooded with spam calls and messages, consuming the network resources
Eavesdropping	An attack in which the attacker intercepts all the VoIP messages, without the knowledge of the users at the endpoints
TLS	Security mechanism to encrypt SIP signaling messages
SRTP	Security mechanism to encrypt VoIP media messages
VPN	Virtual overlay networks that are built on the Internet and connect two private networks of same or different organizations
PBX	Devices that enable the VoIP functionality in VoIP phones
Softphones	Software based VoIP phones
Wireshark	A tool used to sniff network packets
iPerf	A tool used to generate different types of network traffic
Signaling Delay	Time taken to establish a call between two VoIP phones
Media Delay	Time taken to establish a call and hear the first audio
Circuit-Switched	Connection between the endpoints is established before the communication between them starts
Packet-Switched	Connection between the endpoints is established when the communication between them initiates
Jitter	Variations in the time taken by packets to transit the network