University of Essex

Online

MSc Cyber Security

Research Methods and Professional Practice

(RMPP_PCOM7E)

Unit 10 – Research Proposal Presentation Transcript

03 April 2023

Securing VoIP using TLS and SRTP: A practical study in Service Provider networks.

By: Zihaad Khan

Student ID: 12688015

Table of Contents

Slide 1 – Cover

Hello everyone, my name is Zihaad Khan and today I will be going through a research proposal presentation. I am currently pursuing a Master of Science (MSc) degree in cyber security at the University of Essex Online. As part of my studies, I am undertaking a module called Research Methods and Professional Practice (RMPP). One of the objectives of this module is to deliver a presentation on a chosen topic. The topic for discussion today is "Securing VoIP (Voice over IP) using TLS (Transport Layer Security) and SRTP (Secure Real Time Protocol): A Practical Study in Service Provider Networks".

Slide 2 – Agenda

The agenda for today will be as follows:

We will start by introducing the project title and explaining its significance in today's world. Then, we will move on to the research problem and the formulated research question, which will lead to the aims and objectives of the study. Next, we will review the current literature to identify research gaps and opportunities for positive contributions to this field of study. The research methodology and ethical considerations will be discussed, followed by the description of the artefacts that will be produced. Finally, we will end with the proposed timeline for conducting primary research and provide the relevant references for the papers studied.

Slide 3 – Project Title

The project title is: Securing VoIP (Voice over IP) using TLS (Transport Layer Security) and SRTP (Secure Real Time Protocol): A practical study in service provider networks.

Before proceeding any further, let me begin by explaining what Voice over IP, TLS and SRTP is:

Slide 4 – VoIP, TLS & SRTP

VoIP is a popular and cheap technology for making phone calls over the internet instead of traditional telephone lines (Muhammad & Muhammad, 2017). To make VoIP possible, a protocol called SIP i.e., Session Initiation Protocol (SIP) is a commonly used. This is a signalling protocol used for setting up and tearing down VoIP calls (Chakraborty et al., 2019). SIP is a text-based protocol that is used to initiate, modify, and terminate multimedia sessions, such as voice and video calls (IETF, 2012). However, the use of SIP introduces security challenges, such as eavesdropping and tampering of messages (Kumar & Roy, 2021).

This is where Transport Layer Security (TLS) comes in. This is a protocol that is used to encrypt communication over the internet. Specifically in this research, it is used to encrypt VoIP calls. TLS provides confidentiality, integrity, and authentication to the communication channel between two endpoints, basically between two telephones (IETF, 2008). When SIP is used over TLS, the signalling messages are encrypted, which prevents eavesdropping and tampering (Kumar & Roy, 2021).

Now that we have understood, VoIP, Signalling (SIP) and TLS, let’s move onto to Secure Real Time Protocol (SRTP). SRTP is a protocol that is used to encrypt the voice and video data transmitted (media stream) over the internet (Alexander et al., 2009). SRTP provides confidentiality, integrity, and protection to the media stream. When SIP is used with SRTP, the voice and video data are encrypted, which prevents eavesdropping and tampering (Alexander et al., 2009).

To recap, the use of SIP over TLS and SRTP can significantly improve the security of VoIP calls. TLS is used to secure signalling while SRTP is used to secure media. However, the configuration and deployment of these security mechanisms can be complex, varies between networks and requires careful consideration.

Slide 5 - Research Problem: Significance and Contribution to the Discipline

This research aims to address the increasing demand for securing VoIP communication in service provider networks. The focus will be on enhancing performance and security of VoIP networks by implementing TLS and SRTP. The study intends to contribute to the existing literature by evaluating the effectiveness of TLS and SRTP in securing VoIP communication. Furthermore, practical recommendations for service providers to improve the security of their VoIP networks will be provided.

Slide 6 - Research Question

The following research question was formulated, how effective is the implementation of TLS and SRTP in securing VoIP communication in service provider networks?

The effectiveness will be measured from a security and performance perspective, discussed in detail under research methodology.

Slide 7 - Aims and Objectives

By analysing the literature, various gaps in research or lack of research thereof were identified, these can translate directly into the aims and objectives of this research.

The aims and objectives are structured into three areas' viz. Evaluate, Analyse and Provide Recommendations:

- Evaluate - To evaluate the impact of implementing TLS and SRTP on the performance and security of VoIP communication in service provider networks.
- Analyse - To analyse the effectiveness of TLS and SRTP in securing VoIP communication against potential security threats.
- Provide Recommendations - To provide practical recommendations for service providers to improve the security of their VoIP networks.

Slide 8 - Literature Review

VoIP has become a popular means of communication due to its cost-effectiveness, flexibility, and scalability (Muhammad & Muhammad, 2017). However, its use has also introduced security risks, such as eavesdropping, call hijacking, and denial-of-service attacks (Suthar & Rughani, 2020). To mitigate these security risks, various security protocols have been developed for VoIP, including SIP over TLS and SRTP (Neacşu & Şchiopu, 2020).

Several studies have evaluated the effectiveness of these protocols in securing VoIP traffic. For example, Kumar and Roy (2021) found that SIP over TLS and SRTP provided high levels of security against eavesdropping and message tampering. This view is echoed by Alexander et al. (2009) as well as Suthar and Rughani (2020). However, the authors also noted that the implementation of these protocols required careful configuration to ensure their effectiveness. There is also a gap in the studies of analysing the effectiveness of these protocols in a service provider network.

Similarly, the paper by Suthar and Rughani (2020) provides an overview of VoIP security threats and their mitigation techniques. The authors discuss various security threats that VoIP faces, such as eavesdropping, denial-of-service attacks, call hijacking, and phishing attacks. They also provide a comprehensive overview of various VoIP security mechanisms, including encryption, authentication, access control, and intrusion detection and prevention systems. However, the study could have been more comprehensive by including real-world case studies of VoIP security and the challenges that it brings to the industry. Further experiments could also be conducted in test service provider networks.

The paper by Alexander et al. (2009) evaluates the performance of SRTP in VoIP communication. The authors conduct experiments to measure the impact of SRTP on call quality and call setup time using several open-source tools. They find that SRTP adds a security layer to VoIP and has a negligible effect on voice quality. However, the experiment was performed between two endpoints in an internal network and the same conclusion cannot be applied to a service provider network. The authors suggest that further research is needed to find a balance between security and performance in VoIP communication (Alexander et al., 2009).

Overall, the literature indicates that SIP over TLS and SRTP can provide effective security for VoIP traffic, but their implementation requires best practices to ensure their effectiveness. There are also potential vulnerabilities associated with these protocols which need to be addressed to maintain their security. Furthermore, as mentioned, gaps in research exist around the performance impacts and the implementation of TLS and SRTP in service provider networks. This study hopes to address the gaps identified as well as provide service providers with recommendations around the implementation of TLS and SRTP in service provider networks.

Slide 9 – Research Methodology

So, how can we achieve this? The research methodology will involve designing and setting up a test environment to simulate VoIP communications using SIP over a service provider network. Appropriate testing scenarios will be selected to ensure that the simulated VoIP communications are representative of real-world usage. The testing scenarios will involve different types of calls, such as one-to-one calls, conference calls, and calls with different codecs (which is a compression technology) to ensure a comprehensive evaluation of the impact of security measures on call performance and quality.

The SIP over TLS and SRTP configurations will be performed using best practices to ensure that the setup is accurate and representative of real-world deployments. The network traffic generated during the testing will be captured using packet capture tools like Wireshark and analysed to measure the call setup time and quality.

To ensure the accuracy, reliability and repeatability of the results obtained, the testing will be repeated multiple times, and the results will be averaged to obtain more accurate measurements. Additionally, statistical analysis techniques will be employed to compare the results obtained with and without TLS and SRTP and to determine the statistical significance of any differences observed.

The quantitative analysis will involve a subjective assessment of call setup time and call quality using the Mean Opinion Score (MOS) rating system. MOS is a widely used and accepted rating system for voice call quality, and it will be used to provide an overall assessment of call quality with and without TLS and SRTP (Alexander et al., 2009).

Overall, the research methodology will involve a comprehensive and rigorous evaluation of the effectiveness of SIP over TLS and SRTP in securing VoIP communication in a service provider network.

Slide 10 - Ethical Considerations and Risk Assessment

The project and researcher will comply with ethical guidelines such as the ACM Code of Ethics (ACM, 2018) and the BCS Code of Conduct (BCS, 2022), including obtaining the necessary permissions and consent from any service providers involved in the research. The research will not involve any sensitive or personal data, and measures will be taken to ensure the privacy and confidentiality of the participants (if any). Literature obtained and analysed will be cited and referenced accordingly. No risk assessment is required to be performed in this research.

Slide 11 - Description of Artefacts

The research will include simulated SIP call flows with and without TLS and SRTP to demonstrate the effectiveness of the implementation in securing VoIP communication. Practical recommendations for Service Providers to improve the security of their VoIP networks will also be provided.

Slide 12 - Proposed Timeline

It is assumed that the project module must be completed in 28 weeks. The infographic represents an estimate timeline. The proposed timeline for the project will involve a literature review and research question refinement in weeks 1 - 4, followed by the design and setup of the test environment in weeks 5 - 8. Weeks 9 - 12 will involve the configuration and testing of SIP over TLS and SRTP as well as capturing data. Weeks 13 - 16 will be devoted to analysing and interpreting results. Week 17 - 22 will be reserved for finalising the discussion and completing the project report. Lastly, Week 23 - 26 will be used to work on the artefacts and presentation. Two weeks has been allocated for unforeseen circumstances that may affect the timeline.

References

ACM (2018) Association for Computing Machinery. ACM Code of Ethics and Professional Conduct. Available from: https://www.acm.org/code-of-ethics [Accessed 12 March 2023].

Alexander, A, Wijesinha, A, & Karne, R. (2009) 'An evaluation of Secure Real-Time Transport Protocol (SRTP) performance for VoIP', Third International Conference on Network and System Security, Queensland, Australia, 19-21 October. USA: Towson University. 95-101. Available from: https://www.researchgate.net/publication/221204875_An_evaluation_of_Secure_Real-Time_Transport_Protocol_SRTP_performance_for_VoIP [Accessed 16 March 2023].

BCS (2022) Code of Conduct for BCS Members. Available from: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 14 March 2023].

Chakraborty, T., Misra, I, S., Prasad, R. (2019) *VoIP Protocol Fundamentals. In: VoIP Technology: Applications and Challenges.* 1st ed. New York City: Springer, Cham. Available from: https://link.springer.com/chapter/10.1007/978-3-319-95594-0_2 [Accessed 18 March 2023].

Internet Engineering Task Force - IETF (2012). Session Initiation Protocol (SIP). Available from: https://tools.ietf.org/html/rfc3261 [Accessed 25 March 2023].

Internet Engineering Task Force – IETF (2008). Transport Layer Security (TLS). Available from: https://tools.ietf.org/html/rfc5246 [Accessed 25 March 2023].

Kumar, V, & Roy, O, P. (2021) Security and Challenges in Voice over Internet Protocols: A Survey. *IOP Conference Series: Materials Science and Engineering* 1020(1): 1-10. Available from: https://iopscience.iop.org/article/10.1088/1757-899X/1020/1/012020/meta [Accessed 16 March 2023].

Muhammad, Z, H & Muhammad, Z, H. (2017) Collective Study On Security Threats In VOIP Networks. Available from: https://www.researchgate.net/publication/335442373_Collective_Study_On_Security_Threats_In_VOIP_Networks/citation/download [Accessed 22 March 2023].

Neacşu, E, & Şchiopu, P. (2020) 'An Analysis of Security Threats in VoIP Communication Systems,' *12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Bucharest, Romania, 25-27 June. Piscataway, NJ:

IEEE. 1-6. Available from: https://ieeexplore.ieee.org/document/9223162 [Accessed 16 March 2023].

Suthar, D, & Rughani, H, R. (2020) ‘A Comprehensive Study of VoIP Security’, *2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN).* Greater Noida, India, 18-19 December. Piscataway, NJ: IEEE. 812-817. Available from: https://ieeexplore.ieee.org/document/9362943 [Accessed 16 March 2023].