Analysis of the Security Vulnerabilities in Virtual Private Networks

Atiqa Zafar & Zaryab Khan
School of Electrical Engineering and Computer Sciences,
NUST Islamabad, PK

I. INTRODUCTION

Virtual Private Network (VPN) services have become increasingly popular as a cost-effective way of communicating private information securely over an insecure public network. Both organizations and individuals are rapidly joining the VPN usage bandwagon to securely enter an internal network to access resources, data and communications, or simply as a way to work around regional restrictions on content and anonymity. However, VPNs are not the impenetrable, secure systems that we believe them to be and are wide open to attacks such as IPv6 leakage, DNS hijacking, Offline Password Cracking, Man-in-the-Middle Attacks and Malware Infections etc. Over half of the 16 VPN services, looked into by a group of researchers from Sapienza University of Rome and Queen Mary University of London, used the Point-to-Point Tunneling Protocol with MS-CHAPv2 authentications, which makes them vulnerable to brute force hacks.

In this paper, we wish to investigate such potential security risks by studying the core VPN technologies. The work shall be extended by discussing a range of best practices and countermeasure techniques to deal with these vulnerabilities when implementing a virtual private network. This proposal report has been organized as follows. Section II highlights the importance of this research paper by discussing how VPNs make attractive target for security attacks. Section III marks out the objectives of this research, while the flow of work that is to be followed and the project schedule are discussed in Section IV and V.

II. IMPORTANCE

With the rapid increase in the usage of VPNs by both individuals and organizations to transmit sensitive information over an insecure public network, VPNs have become attractive target to hackers. VPN traffic is often invisible to IDS monitoring. This means the attacker can intrude without being picked up by the IDS. By VPN hijacking, the attacker can not only access the sensitive data being transmitted but can also get an access to the internal network resources. This can lead to massive security concerns.

III. AIMS AND OBJECTIVES

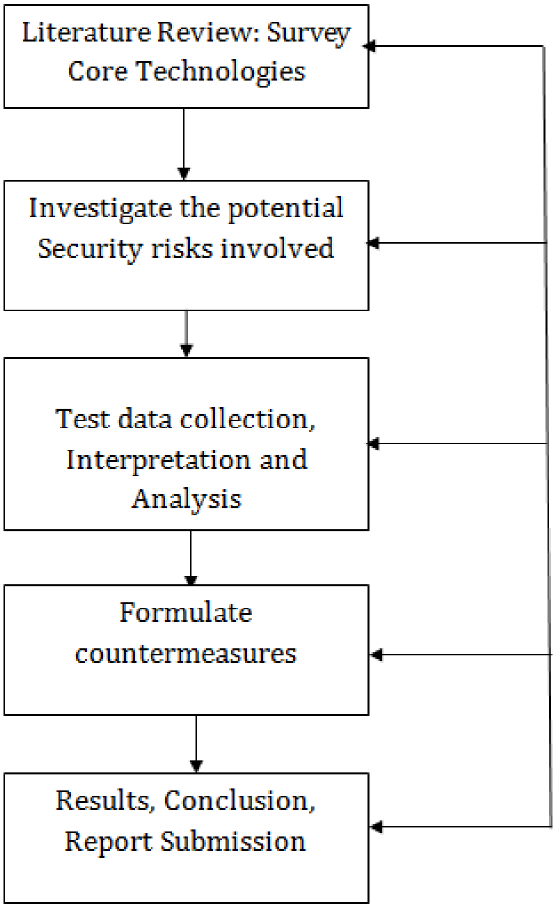
i. Survey the core technologies most commonly used by VPN service
ii. Identify and investigate the potential Security risks involved
iii. Identify countermeasures to solve the problem
iv. Evaluate the performance and security impacts of the countermeasures

IV. PROJECT PLAN

It is never easy to predict the workflow of a project while still being in the initial stages but nevertheless it is always an excellent idea to chalk out a proper plan of action that provides a direction and a way forward through all the stages of the project. Following is the work plan that we have formulated to organize our project efforts.
Each stage of the work plan will be associated with a milestone we aim to achieve.

A. Milestone 1: Literature Review

In Literature Review, we shall survey historic and recent research papers to understand the varying underlying technologies of VPN, like the security protocols IPSec, SSL, Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) involved. Once a clear understanding of these protocols is achieved, we shall investigate the potential security vulnerabilities they pose.


Literature Review: Survey Core Technologies
Investigate the potential Security risks involved
Test data collection, Interpretation and Analysis
Formulate countermeasures
Results, Conclusion, Report Submission

B. Milestone 2: Risk Investigation

After a thorough literature review, we shall investigate the potential security vulnerabilities such IPv6 leakage, DNS Hijacking etc in implementing VPNs.

C. Milestone 3: Countermeasure Formulation

This milestone consists of producing countermeasure techniques to eradicate the security risks involved in the VPN implementation.

D. Milestone 4: Conclusion

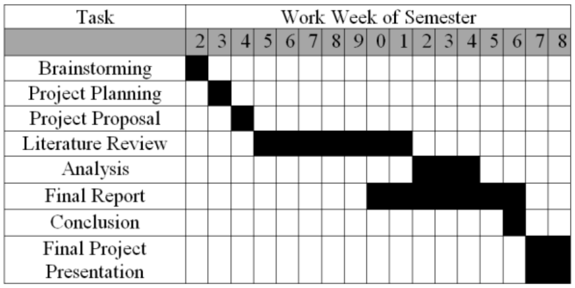
This is milestone is for narrating and interpreting results to draw conclusions.

Deliverables

This *Project Proposal* will be followed up by a *Literature Review* to provide historic and recent references for reading, and concise explanations of the contributions to our paper. The literature review shall be followed up by a *Final Written Report* covering all the technical details. The valuable findings will be summed up by a *Class Presentation* that is expected to last around 15 minute.

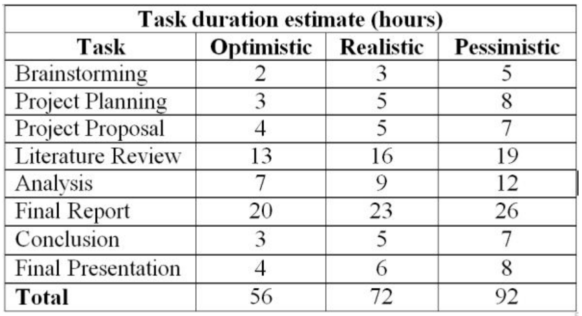
V. PROJECT SCHEDULE

This project is assigned to us as the semester project of the course Network Security. The time allotted to us for completion is 16 weeks.



Task	Work Week of Semester																
	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8
Brainstorming	■																
Project Planning		■															
Project Proposal			■														
Literature Review				■	■	■	■	■	■	■							
Analysis											■	■	■				
Final Report									■	■	■	■	■	■	■		
Conclusion															■		
Final Project Presentation																■	■

The Gantt chart provided above is the representation of the timeline. It must be noted however that there may be variations in the actual timeline as this chart only serves to organize our work efforts. Further complications down the line may affect the work progress. Further breakdown of the various tasks into the number of working hours is provided below:



Task duration estimate (hours)			
Task	**Optimistic**	**Realistic**	**Pessimistic**
Brainstorming	2	3	5
Project Planning	3	5	8
Project Proposal	4	5	7
Literature Review	13	16	19
Analysis	7	9	12
Final Report	20	23	26
Conclusion	3	5	7
Final Presentation	4	6	8
Total	56	72	92

VI. RISKS AND ETHICS

Most data that we will collected shall not raise any ethical concerns as we shall probe the public service through our own VPN accounts. However, if any data about other VPN users is collected to provide insight into wider privacy issues, we shall immediately delete all data after analysis. The data will be solely used for academic purpose of analysis.

References

[1] R. Hills, “Common VPN Security Flaws Whitepaper”, http://www.nta-monitor.com, January 2005.

[2] Wikipedia, "Virtual Private Networks" https://en.wikipedia.org/wiki/Virtual_private_network

[3] Vasile C. Perta*, Marco V. Barbera, Gareth Tyson, Hamed Haddadi, and Alessandro Mei, "A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients", 2015