THE UNIVERSITY OF DODOMA

COLLEGE OF INFORMATICS AND VIRTUAL EDUCATION

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CSE)

FINAL YEAR PROPOSAL

ACADEMIC YEAR: **2023/2024**

TITLE: PENETRATION TESTING IN GSM AND VULNERABILITIES OF SS7 NETWORK

GROUP MEMBERS

STUDENT'S NAME	REGISTRATION NUMBER	PROGAMME
1. DAVID MKINA	T22-02-14529	Dip CSDF
2. JACKSON MKUNDE	T22-02-02886	Dip CSDF
3. EMILY SEVERINE	T22-02-10531	Dip CSDF
4. PASCHAL NAFTAR	T22-02-13406	Dip CSDF
5. AMANI MAHENA	T22-02-13404	Dip CSDF
6. MKAMI MWANISI	T22-02-10393	Dip CSDF

CHAPTER ONE

1. Introduction

1.1 Project Overview

The "Penetration Testing in GSM and SS7 vulnerabilities" project aims to assess the security posture of Global System for Mobile Communications (GSM) and Signaling System No. 7 (SS7) networks through comprehensive penetration testing methodologies. In recent years, the telecommunications industry has faced increasing threats from cyberattacks targeting vulnerabilities within these critical communication protocols. This project seeks to address these challenges by conducting thorough assessments and identifying potential entry points, weaknesses, and attack surfaces within GSM and SS7 networks.

1.2 Problem statement

GSM network structure is divided into a Network Switching Subsystem and a Base Station Subsystem. The Network Switching Subsystem (often called core network) is a wired backbone that allows mobile phones to communicate with each other and with mobile devices in other networks. The core network consists of Mobile Switching Centers (MSC) which are primary service delivery nodes responsible for handling voice calls and other services. A special type of MSC is a Short Message Service Centre (SMSC) which supports sending and receiving of text messages – SMS. Establishment and control of voice circuits in the telephone network is provided by signaling protocols, carried out-of-band, in separate signaling links that use message switching. Signaling protocols used in telecommunication networks worldwide are grouped in the Signaling System Number 7 (SS7) standard. The SS7 protocol stack defines protocols at several layers.

Signaling System no. 7 (SS7)

Signaling System No. 7 (SS7) is one of the mobile communication backend protocols mainly used for establishing the roaming interconnectivity across 2G/GSM mobile network operators. Besides roaming, SS7 has enabled a wide range of facilities such as Short Message Services (SMS), toll-free numbers, televoting and Local Number Portability (LNP). It was built during the time when mobile network operators used to be the trusted network of government-owned organizations and the security of the whole network were provided by denying access to external entities.

Being a four decades old protocol, SS7 have the following issues:

- Attackers can gain access to the SS7 based core network using other Internet protocols.
- Once they are inside the core network, they can exploit the routing layer to map the periphery of the network, scan for open ports and send hostile communication messages.
- Since there is no authentication check or any other cryptographic protection within the network, the attackers can impersonate as the network internal nodes and query for subscriber information from other nodes.
- SS7 protocol is not secure and can easily be compromised by hackers.

No established security system has been developed in the SS7 network protocol, so a hacker getting access to the SS7 network can listen to your phone calls, read your text messages and even track geographical locations.

- A hacker can even bypass the two-factor authentication by intercepting the SMS designated to a user. Furthermore, upon intercepting the SMS message, the hacker can gain access to the user’s social media platforms, online banking accounts. If the hacker intercepts your SMS verification messages through SS7 attack, it would be easy for the hacker to access your accounts.

This type of attack is considered to be a form of man-in-the-middle attack which puts the cell phone user at great risk.

1.3 **Objectives**

- Main objective.

To assess the security vulnerabilities, present in GSM and Signaling System No. 7 networks through penetration testing.

- Specific objective.

1. Identify and analyze potential entry points and attack surfaces within GSM and SS7 networks.
2. Conduct simulated attacks to exploit vulnerabilities in GSM and SS7 protocols.
3. Evaluate the effectiveness of existing security measures in protecting against penetration attempts.
4. Recommend strategies and countermeasures to mitigate identified vulnerabilities and enhance the security posture of GSM and SS7 networks.

1.4 **Project significance**

- **Security Risks:** GSM and SS7 vulnerabilities pose significant security risks. If exploited, attackers could compromise sensitive data like calls, texts, and location information.
- **Impact:** Successful attacks could have a devastating impact on individuals, organizations, and critical infrastructure.
- **Current Knowledge Gaps:** Existing knowledge about GSM and SS7 security has limitations. This project aims to address these gaps by uncovering vulnerabilities and recommending solutions.
- **Improved Security:** The project's findings can be used to strengthen GSM and SS7 networks. Potential outcomes include developing new security measures or raising awareness of existing vulnerabilities.
- **Future Research:** This project may pave the way for further research in GSM and SS7 security.

1.5 **Project scope**

Inclusions:

- Assessing vulnerabilities in GSM and SS7 networks.
- Penetration testing to identify weaknesses and attack surfaces.
- Evaluating existing security measures.
- Developing mitigation strategies and recommendations.
- Documenting findings, recommendations, and remediation steps.

Exclusions:

- Implementing security measures or system changes beyond testing.
- In-depth analysis of non-security aspects of the networks.
- Physical security assessments or hardware evaluations.
- Legal/regulatory compliance beyond security vulnerability assessment.

Constraints:

- Time constraints: Specify the project timeframe.
- Resource constraints: Briefly mention limitations in budget, personnel, or equipment.
- Access constraints: Discuss potential limitations in accessing relevant network environments for testing.
- Technical constraints: Acknowledge limitations in conducting specific penetration testing methods due to technical reasons or network operator restrictions.
  pen spark

CHAPTER TWO

2. Literature Review

2.1 Introduction

This chapter presents a comprehensive literature review on penetration testing methodologies for identifying vulnerabilities within GSM and SS7 networks. It explores the literature to determine the state of knowledge regarding security threats related to these important communication protocols.

2.2 Definitions of Key Terms

For a clear understanding, this section defines essential terms used throughout the project:

- **Penetration Testing:** The simulated practice of attacking a computer system to evaluate its security posture and identify potential weaknesses.

- **GSM Network Architecture:** The architecture of a GSM network consists of two primary subsystems:

    - **Mobile Switching Center (MSC):** A core network element responsible for handling voice calls and other services.
    - **Base Station Subsystem (BSS):** Manages the radio link between mobile devices and the network.

- **Signaling System No. 7 (SS7):** A signaling protocol used for establishing communication between network elements in telecommunication networks.

- **Vulnerability:** A weakness or flaw in a system's design or implementation that can be exploited by attackers to gain unauthorized access or cause harm. (Focus on vulnerabilities relevant to GSM and SS7)

- **Penetration Testing Methodologies:** Structured approaches for conducting penetration testing, which may involve various techniques like vulnerability scanning, social engineering, and exploit testing. (Specify methodologies relevant to your project)

- **a novel attack** is a method that has not been previously known or encountered, and is used to exploit vulnerabilities in networks or computer systems. Because these attacks have not been documented before, they are difficult to detect and defend against using traditional security measures.

- **tailoring** is the process of customizing security measures to meet the unique needs of an organization or system. This involves adapting security controls, policies, and procedures to address the organization's unique risks and vulnerabilities.

2.3 Theoretical Literature/Framework

This section explores theoretical frameworks that underpin the approach to penetration testing in GSM and SS7 networks. Here are some potential frameworks to consider:

- **CIA Triad:** This information security model emphasizes three core principles:

    - **Confidentiality:** Protecting sensitive information from unauthorized disclosure.
    - **Integrity:** Ensuring the accuracy and completeness of data.
    - **Availability:** Guaranteeing authorized access to information and systems.

The CIA triad can guide the identification of vulnerabilities that could compromise confidentiality (e.g., eavesdropping on calls), integrity (e.g., manipulating call data), or availability (e.g., denying service attacks).

- **Penetration Testing Methodologies:** Frameworks like PTES (Penetration Testing Execution Standard)
  or
- OSSTMM (Open-Source Security Testing Methodology Manual) provide structured approaches for conducting penetration testing. These methodologies can be adapted for specific contexts like GSM and SS7 network assessments.

Explain how your chosen framework(s) will be used to guide your project's methodology for assessing vulnerabilities.

2.4 Related (Similar) Work

A thorough literature review was conducted to identify existing research on:

- **Penetration Testing Methodologies for GSM/SS7:** Explore existing research on how penetration testing has been applied to identify vulnerabilities in GSM and SS7 networks. Analyze the methodologies used, their effectiveness, and any limitations identified.
- **Vulnerabilities in GSM/SS7:** Examine research on previously discovered vulnerabilities within GSM and SS7 networks. Categorize these vulnerabilities and their potential impact on network security.
- **Mitigation Strategies and Countermeasures:** Review existing research proposing strategies to address vulnerabilities in GSM and SS7 networks. Analyze the effectiveness of these proposed solutions.

Critically analyze the reviewed literature by summarizing key findings, methodologies used, and limitations of previous research.

2.5 Innovation/Research Gap

Building upon the comprehensive literature review, this project aims to address a critical gap in the existing knowledge regarding penetration testing methodologies for GSM and SS7 networks.

Here are the key areas where this project will contribute:

- **Advanced Penetration Testing Methodologies:**
    - The project could introduce novel penetration testing methodologies specifically tailored for GSM and SS7 networks.
    - These methodologies could incorporate cutting-edge techniques like machine learning for anomaly detection, fuzzing for protocol weaknesses, and social engineering simulations targeted at network personnel.
    - By employing such techniques, the project can achieve a more comprehensive and in-depth assessment of vulnerabilities compared to traditional methods.

- **Novel Attack Surface Identification:**
    - The project could propose innovative ways to identify and analyze potential entry points and attack surfaces within GSM and SS7 networks.
    - This might involve developing automated tools or algorithms that can efficiently scan and map the network architecture, including dynamic aspects like routing protocols.
    - Additionally, the project could explore advanced techniques like side-channel analysis to uncover vulnerabilities that might not be readily apparent through conventional methods.

- **Enhanced Security Measures:**
    - The project could recommend novel strategies and countermeasures to mitigate the identified vulnerabilities and enhance the security posture of GSM and SS7 networks.

    - These recommendations might include:
        - Implementing strong cryptographic algorithms to protect sensitive data in transit and at rest.
        - Designing robust authentication mechanisms that go beyond SMS-based two-factor authentication, potentially leveraging hardware tokens or biometrics.
        - Deploying intrusion detection and prevention systems (IDS/IPS) specifically tailored to identify and block suspicious activity within GSM and SS7 networks.

- **Future Research Directions:**
    - The project's findings can highlight areas that require further research and investigation.
    - This could include:
        - Exploring emerging threats and vulnerabilities in GSM and SS7 networks as attackers develop new techniques.
        - Investigating the development of more robust security architectures for mobile communication networks, potentially leveraging advancements in blockchain technology or secure multi-party computation.
        - Researching the feasibility of migrating to more secure communication protocols that are inherently less susceptible to attacks compared to GSM and SS7.

By addressing these gaps, the project has the potential to significantly improve the security posture of GSM and SS7 networks, making them more resilient against cyberattacks.

CHAPTER THREE

3. Methodology

3.1 Introduction

A methodology is a structured and systematic approach to conducting research. It outlines the steps and techniques used to gather data, analyze information, and draw conclusions.

3.2Research Approach

This project will adopt a **qualitative research approach**. Qualitative research focuses on understanding complex phenomena through in-depth exploration and analysis of non-numerical data, such as observations, interviews, and documents.

Here's why qualitative research is suitable for this project:

- Focus on identifying vulnerabilities: Penetration testing involves qualitative analysis of network behavior to identify weaknesses and potential attack vectors.

- Understanding attacker intent: Qualitative methods can help explore the motivations and techniques used by attackers targeting GSM and SS7 networks.

- Evaluating security posture: The project aims to assess the overall security posture, which involves qualitative judgment based on the identified vulnerabilities and existing security measures.

3.3Research Method

This project will employ a **penetration testing methodology** specifically tailored for assessing vulnerabilities in GSM and SS7 networks.

This methodology will involve several phases:

1. **Planning and Reconnaissance:** Gather information about the target network (GSM/SS7) and define the scope of the penetration testing.

2. **Scanning and Enumeration:** Identify potential entry points and attack surfaces within the network using various scanning techniques.

3. **Gaining Access:** Exploit identified vulnerabilities to establish unauthorized access to network resources.

4. **Maintaining Access:** Secure and maintain access to the network to conduct further exploration and analysis.

5. **Covering Tracks:** Conceal any evidence of the penetration test to minimize potential damage.

6. **Reporting:** Document findings, including identified vulnerabilities, exploited weaknesses, and recommendations for remediation.

3.4Study Area/Location

Specify the context or environment where the penetration testing will be conducted. This could be:

- A simulated GSM/SS7 network environment in a controlled lab setting.
- A test network provided by a willing network operator with appropriate permissions and safeguards in place.

Explain the rationale behind your chosen location.

3.5 Data Collection/Requirements Gathering

3.5.1 Data Collection Techniques/Methods

Data collection in penetration testing involves gathering information about the target network. Techniques might include:

- **Network scanning:** Identifying active devices, services, and protocols running on the network.
- **Packet sniffing:** Capturing network traffic to analyze communication patterns and potential vulnerabilities.
- **Social engineering:** Simulating social attacks to assess the human element of network security.
- **Vulnerability scanning:** Utilizing automated tools to identify known vulnerabilities in network devices and software.
- **Manual exploitation:** Employing penetration testing tools and techniques to exploit discovered vulnerabilities.

3.5.2 Data Collection Tools

The specific tools used will depend on the chosen penetration testing methodology and the target network environment. However, some common tools might include:

- **Network scanners:** Tools like Nmap, Nessus, or OpenVAS for network discovery and vulnerability assessment.
- **Packet sniffers:** Tools like Wireshark or tcpdump to capture and analyze network traffic.
- **Social engineering tools:** Phishing emails, pretext calls, or social media manipulation techniques (used ethically with permission).
- **Vulnerability scanners:** Tools like Metasploit or Acunetix for automated vulnerability identification and exploitation.
- **Penetration testing frameworks:** Kali Linux or Parrot OS provide pre-configured environments with various penetration testing tools.

3.6 System/Requirements/Data Analysis

Data collected during penetration testing will be analyzed to assess the identified vulnerabilities and their potential impact on network security. Analysis techniques might include:

- **Vulnerability assessment:** Evaluating the severity and exploitability of discovered vulnerabilities.
- **Risk assessment:** Estimating the likelihood and potential consequences of successful attacks exploiting these vulnerabilities.
- **Threat modeling:** Identifying potential attackers, their motivations, and the attack vectors they might employ.

3.7 Reporting

The project findings will be documented in a comprehensive penetration testing report that includes:

- **Executive Summary:** A concise overview of the project scope, methodology, and key findings.
- **Technical Details:** Detailed descriptions of identified vulnerabilities, exploited weaknesses, and proof-of-concept attacks.
- **Risk Assessment:** Analysis of the potential impact of identified vulnerabilities on network security.
- **Recommendations:** Clear and actionable recommendations for mitigating identified vulnerabilities and enhancing network security pen spark

3.8 System Requirements (Optional)

If your project involves any specific software or hardware requirements for conducting the penetration testing, you can include them in this section. However, for a pure penetration testing

CHAPTER FOUR

4. Project Timeline and Budget

4.1 Project Timeline

A project timeline is a crucial tool that visually represents the chronological order of events and tasks involved in a project. It helps to:

- **Plan and schedule project activities:** Define the start and end dates of each task, ensuring a realistic and achievable project duration.
- **Allocate resources effectively:** Assign personnel and equipment to tasks based on their timelines.
- **Track progress and identify potential delays:** Monitor project progress and identify any deviations from the planned timeline to take corrective actions.

4.2 Project Budget

A project budget is a detailed financial plan that outlines the estimated costs associated with completing a project. It helps to:

- **Secure funding:** Demonstrate to stakeholders the resources needed to complete the project.
- **Control project expenses:** Track actual costs against the budget and identify any deviations to prevent overspending.

4.3 References

[1] MobiSys'10, June 15–18, 2010, San Francisco, California, USA. Copyright 2010 ACM 978-1-60558-985-5/10/06

[2] R. Ahas, A. Aasa, et al. Evaluating Passive Mobile Positioning Data for Tourism Surveys: An Estonian Case Study. Elsevier Tourism Management, 29(3):469–486, 2008.

[3] S. Keshav. An Engineering Approach to Computer Networking: ATM Networks, the Internet, and the 253 Telephone Network. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997.

[4] ITU-T. Introduction to CCITT Signaling System No.7. ITU-T Recommendation Q.700, Mar 1993.

[5] G. Heine and M. Horrer. GSM Networks: Protocols, Terminology, and Implementation. Artech House, Inc., Norwood, MA, USA, 1999.

[6] Hacking 9. Practical Protection. It Security Magazine Vol. 12, No. 14 Open.

[7] SS7 – The Deadliest Attack. Author - Vasanth Vanan
https://medium.com/@vasanthavanan59439/ss7-the-deadliest-attack6423de7fe8c0

[8] Tobias Engel, SS7-Locate-Track-maniuplate, Presentation:
https://berlin.ccc.de/~tobias/31c3-ss7-locate-trackmanipulate.pdf

[9] Welcome to SigPloit (Wiki)
https://github.com/SigPloiter/SigPloit/wiki/1--Welcome-to-SigPloit

[10] Mobile Network Architecture (Wiki)
https://github.com/SigPloiter/SigPloit/wiki/2--Mobile-Network-Architecture

[11] How to use the SS7 module
https://github.com/SigPloiter/SigPloit/wiki/3--How-to-use-the-SS7-module

[12] Hacking, Practical Protection, IT Security Magazine, Vol.12, NO.14

[13] MELT'08, September 19, 2008, San Francisco, California, USA. Copyright 2008 ACM 978-1-60558-189-7/08/09

[14] 3GPP TS 29.002: Mobile Application Part (MAP).

[15] Q.700: Introduction to CCITT Signalling System No.7