**System Security - Professional**

**Project Proposal**

**Group number:** 1

**Group members:**

1. **Lin Pengcheng -** 1008527
2. **Baskar Durga –** 1008534
3. **Harish Navnit -** 1008538
4. **Tang Fei -** 1008558

**Topic:** Trojan Source Attacks and Vulnerabilities in Software

**Main Paper:** "Trojan Source: Invisible Vulnerabilities" by Nicholas Boucher and Ross Anderson

**Main Idea/Contribution:**

The paper introduces a new type of attack called "Trojan Source" where source code is maliciously encoded to appear different to both compilers and human reviewers. The attack exploits text-encoding standards like Unicode to create source code with logically encoded tokens in a different order from their displayed order, resulting in hidden vulnerabilities that are not easily detectable by human code reviewers. The paper presents examples of Trojan Source attacks in various programming languages and proposes compiler-level defenses and other mitigating controls.

**Related Papers:**

1. "Securing the Software Supply Chain" by Brian Chess et al.: This paper discusses the importance of securing the software supply chain and highlights the risks associated with supply-chain attacks. It provides an overview of different types of supply-chain attacks and explores strategies and best practices for mitigating these risks.
2. "Compiler-based Security Vulnerabilities: A Survey" by Cristiano Giuffrida et al.: This survey paper provides an in-depth analysis of security vulnerabilities that can be introduced by compilers. It explores various categories of compiler-based vulnerabilities, their impact on software security, and existing techniques for detecting and mitigating such vulnerabilities.
3. "Unicode Security Considerations" by Mark Davis and Michel Suignard: This paper focuses on security considerations related to Unicode and text encodings. It discusses potential security issues that can arise from the use of Unicode, including character set manipulation, display issues, and bidirectional text vulnerabilities. The paper also provides recommendations for developers and implementers to mitigate these security risks.

**Project Plan:**

1. Familiarize myself with the main paper and related papers to gain a comprehensive understanding of Trojan Source attacks, supply-chain vulnerabilities, and compiler-based security issues.
2. Conduct further literature review to explore additional research and studies related to Trojan Source attacks and software vulnerabilities.
3. Identify common vulnerabilities introduced by Trojan Source attacks and analyze existing mitigation techniques proposed in the literature.
4. Evaluate the effectiveness of compiler-level defenses and other mitigating controls proposed in the main paper and related works.
5. Develop a plan to experimentally validate the effectiveness of the proposed defenses and controls.
6. Implement and conduct experiments to assess the robustness and practicality of the proposed defenses.
7. Analyze the results, draw conclusions, and identify potential areas for further research or improvements in defending against Trojan Source attacks.
8. Document the findings and prepare a research report or paper summarizing the study.