Secure Software Design & Engineering(CY-321)

Threat Modeling & Risk Assessment

Anti-Phishing Browser Extension

Group Members

1. Shameer Awais (2022428)
2. Rooshan Riaz (2022506)
3. Naqi Raza (2022574)
4. M. Yasir (2022455)

Submission Date: 14/03/2025

Ghulam Ishaq Khan Institute of Engineering Sciences and Technology

Attack Vectors & Risk Levels

To ensure the security and reliability of the Anti-Phishing Browser Extension, we employ the STRIDE threat modeling framework. STRIDE helps identify key risks such as Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. By applying this framework, we systematically analyze potential attack vectors, assess their impact, and develop targeted mitigation strategies to protect users from phishing threats.

Attack Vector	**Description**	**Risk Level**
Phishing Sites Bypassing Detection	Attackers may create sophisticated phishing sites that evade the ML-based detection algorithms.	High
Data Leakage	Sensitive user data (e.g., URLs, browsing history) could be leaked if the extension is compromised.	High
Reverse Engineering	Attackers may reverse engineer the extension to understand its detection mechanisms and bypass them.	Medium
Man-in-the-Middle (MITM) Attacks	If communication between the extension and backend servers is not properly encrypted, attackers could intercept data.	High
Malicious Code Injection	The extension could be exploited to inject malicious scripts into web pages, compromising user security.	High
User Consent Bypass	Attackers could manipulate the extension to bypass user consent mechanisms, leading to unauthorized data collection.	Medium
Session Hijacking	If the extension includes user authentication, session tokens could be hijacked.	Medium
Input Validation Flaws	Lack of proper input validation could lead to injection attacks or other vulnerabilities.	Medium
Third-Party Service Compromise	If the extension relies on third-party services for phishing database updates, these services could be compromised.	Medium

Table 1: Attack Vectors and Risk Levels

Security Mitigation Strategies

To address the identified threats and ensure the robustness of the Anti-Phishing Browser Extension, we propose the following mitigation strategies. These measures are designed to protect users from phishing attacks, safeguard their data, and maintain the integrity of the extension. Each strategy is tailored to counter specific attack vectors and align with secure software design principles.

Attack Vector	**Mitigation Strategy**
Phishing Sites Bypassing Detection	Continuously update the machine learning model with new phishing patterns. Use heuristic analysis alongside ML to detect new phishing sites.
Data Leakage	Implement strict data access controls. Only collect necessary data (e.g., URLs) and ensure it is encrypted both in transit and at rest.
Reverse Engineering	Use code obfuscation and signing to prevent tampering. Regularly update the extension to patch any vulnerabilities.
Man-in-the-Middle (MITM) Attacks	Ensure all communication between the extension and backend servers uses HTTPS (SSL/TLS encryption). Implement certificate pinning to prevent MITM attacks.
Malicious Code Injection	Follow secure coding practices to ensure the extension does not inject malicious scripts. Regularly audit the code for vulnerabilities.
User Consent Bypass	Implement robust user consent mechanisms. Ensure users can easily opt out of data collection and sharing. Regularly audit consent mechanisms for vulnerabilities.
Session Hijacking	Use secure session management practices, such as short-lived session tokens and secure cookie attributes (e.g., HttpOnly, Secure).
Input Validation Flaws	Implement strict input validation and sanitization for all user inputs. Use libraries or frameworks that automatically handle input validation.
Third-Party Service Compromise	Use trusted third-party services and regularly audit their security practices. Implement fallback mechanisms in case of service compromise.

Table 2: Security Mitigation Strategies