Project Design
Phase-ISolution
Architecture

Date	25 September 2023
Team ID	Team 2.6
Project Name	Project – Malware Detection and Classification
Maximum Marks	4 Marks

Solution Architecture:

Solution architecture is a complex process – with many sub-processes – that bridgesthe gap between business problems and technology solutions. Its goals are to:

1. **Continuous Monitoring of Certificates**

SSL certificates have a limited lifespan, typically one to three years. It is important to monitor SSL certificates for expiration and to renew them before they expire. Otherwise, visitors to your website will receive an error message and may be unable to access your site.

In addition to monitoring for expiration, it is also important to monitor SSL certificates for mismatches. A mismatch occurs when the common name (CN) on the certificate does not match the domain name of the website. This can happen if the certificate is issued for a different domain name, or if the domain name is changed after the certificate is issued.

Mismatches can be exploited by attackers to perform man-in-the-middle attacks. In a man-in-the-middle attack, the attacker intercepts traffic between the user and the website and impersonates the website. The attacker can then steal sensitive data, such as login credentials or credit card numbers.

A continuous monitoring system can detect SSL certificate expiration and mismatches in real time. This allows you to take corrective action immediately, before attackers can exploit these vulnerabilities.

2. **Multi-Factor Authentication (MFA) and Access Controls**

MFA adds an extra layer of security to your website by requiring users to provide two or more factors of authentication to log in. This can include a password, a one-time code from a mobile app, or a fingerprint scan.

MFA makes it much more difficult for attackers to gain unauthorized access to your website, even if they have compromised a user's password.

In addition to MFA, it is also important to implement strict access controls on your website. This includes limiting who has access to sensitive areas of your website, such as the admin dashboard and database.

You should also use strong passwords and regularly change them.

3. **Regular Updates and Patch Management**

Software vulnerabilities can be exploited by attackers to install malware on your website. This malware can then be used to steal data, redirect visitors to malicious websites, or launch attacks on other websites.

It is important to keep your website software up to date, including the SSL certificate management software. Software updates often include security patches that can help to protect your website from known vulnerabilities.

You should also have a process in place for regularly patching your website software. This process should be automated if possible.

Conclusion

By implementing these security measures, you can help protect your website from SSL certificate attacks. Continuous monitoring, MFA and access control, as well as regular updates and patch management are all essential elements of an overall website security strategy.

Solution Architecture Diagram: