Sushma Shivshankar Nandiyawar

SNS Lab 5

Q1. How does VeriSign verify that a certificate signing request came from the correct entity for their "Secure Site" (not EV) certificates? What are two disadvantages/limitations to using method of validation?

Answer :

VeriSign, now under the Symantec umbrella, employs various techniques to authenticate a certificate signing request (CSR) for their "Secure Site" certificates. Here are some of the methods they utilize:

1. **Domain Validation:**
    a. Domain Validation VeriSign confirms that the domain name specified in the CSR corresponds to the domain name of the party seeking the certificate.
    b. This is achieved by sending an email to the registered administrative contact of the domain, requesting confirmation of the certificate request.
2. **Organization Validation:**
    a. VeriSign ensures the legitimacy of the entity seeking the certificate by examining their legal documents, including articles of incorporation, business licenses, or other government-issued records.
    b. They also confirm that the organization's name and address align with the details registered with the appropriate government agency.

Two drawbacks or constraints associated with using these validation methods are:

1. **Domain Validation** may be susceptible to email spoofing attacks, where a malicious actor could send a fraudulent email to the registered administrative contact of the domain, posing as the genuine certificate requester, and deceive them into validating the certificate request.
2. **Organization Validation** can be a labor-intensive procedure and is not always infallible: The process of authenticating legal documents and confirming an organization's identity can be a manual and resource-intensive task. Furthermore, achieving complete certainty regarding an organization's identity may not always be feasible, particularly in situations where the organization lacks a well-established presence or a clear ownership structure.

Q2. What are Extended Validation certificates? What are two advantages and disadvantages to using extended validation certificates?

Answer :

1. The most advanced SSL certificate is the Extended Validation (EV) certificate. This certificate guarantees the security and encryption of data.
2. However, they vary in terms of how rigorously the website owner's identity must be authenticated. By verifying the legal identification of a website owner, an EV certificate provides the utmost confidence in confirming digital identity.
3. An EV certificate signifies ownership of the domain by a registered legal entity, but it doesn't automatically mean that the website is trustworthy both in practice and under the law.

Benefits of employing Extended Validation certificates:

It provides a greater degree of trustworthiness compared to Domain Validation. The validation process for an EV certificate includes the following steps:

1. Confirmation that the individual making the request is authorized to utilize the domain.
2. Verification that the requestor has been given permission to issue the certificate.
3. Authentication of the requestor's actual existence and legal status.
4. Ensuring that the entity's identity matches the official documentation.
5. Moreover, it utilizes a 2048-bit signature and strong 256-bit encryption..

Drawbacks of employing Extended Validation certificates:

1. EV certificates rely significantly on user involvement, which may not be a wise approach for safeguarding your security.
2. It's not reasonable to expect users to consistently and precisely verify the domain owner's identity and the organization behind a website manually each time they visit a site.
3. To make Extended Validation certificates effective, certain technological limitations need to be imposed independently of the user.
4. They come at a higher price.
5. They often come with a limited validity period.
6. The validation process demands time and effort.

Q3. What steps could you take to ensure that you have the correct root certificate for VeriSign in your browser?

Answer :

1. Launch your web browser.
2. Access the privacy settings.
3. Choose security preferences.
4. Go to the certificate management section.
5. Verify on the official website that you are using the most up-to-date version of the root certificates.

On the authorities page, review and validate the VeriSign certificate.

Q4. Compare and contrast the OCSP and CRL approaches for certificate revocation.

Answer :

Certificate Revocation Lists (CRL):

1. Aggregate all certificates that have been revoked by a Certificate Authority (CA).
2. Require more time for certificate validation in comparison to OCSP.
3. Consume greater network resources when verifying a single URL, unlike OCSP.
4. Lack the capability to offer immediate, real-time updates for certificate revocations.

Online Certificate Status Protocol (OCSP):

1. Exclusively conveys the revocation status of the certificate for the requested website.
2. Speeds up the certificate verification process.
3. Demands fewer network resources compared to CRL.
4. Delivers real-time updates for certificate revocation details.

Q5. What X.509 field does a browser check to determine if a received certificate is allowed to be used for the site that sends it?

Answer :

The browser verifies the Common Name and Subject Alternative Name to determine if the certificate it receives is permitted for use by the website that sent it.

1. The Common Name :
    a. The Common Name usually includes the domain name or hostname for which the certificate is granted.
    b. The browser then checks whether the Common Name matches the domain name of the website it's trying to access, and if there's a match, the certificate is deemed valid for that site.
2. The Subject Alternative Name (SAN):
    a. The Subject Alternative Name (SAN) is an extension in the X.509 certificate that can contain various entries like DNS names, IP addresses, and email addresses.
    b. When a certificate includes a SAN extension, the browser not only verifies the Common Name (CN) but also examines the SAN field for a domain name or hostname that matches the website's domain.
    c. If such a match is found in the SAN field and aligns with the website's domain, the certificate is regarded as valid.

Q6. Why do certificates have an expiration date if there are other certificate revocation mechanisms (ie. OCSP and CRL)?

Answer :

1. CRL and OCSP mechanisms are essential for revoking certificates before they reach their expiration date. Nevertheless, there can be scenarios where these mechanisms experience failures or are unavailable.
2. In such instances, certificate expiration acts as an assurance that certificates will ultimately become invalid, ensuring their security even when real-time revocation checks are unfeasible or unreliable.
3. By setting expiration dates, a specific time frame is defined for certificate validation, reducing the associated risks of extended certificate usage.
4. Without these expiration dates, certificates could retain trust indefinitely, even if vulnerabilities are discovered.
5. Expiry necessitates organizations to regularly renew certificates, reducing their vulnerability to potential security issues.
6. The certificate's expiration ensures its continued compliance with up-to-date security standards. Certificate Authorities (CAs) incorporate the most current security measures when they issue new certificates.
7. Throughout the certificate's duration, any modifications to the website, like changes in the company's name or hosting location, necessitate obtaining a new certificate to accommodate these updates.
8. In essence, the expiration date acts as an extra layer of security and assists in resolving various practical and security issues, including adhering to security best practices, providing a

fail-safe mechanism, mitigating the persistence of outdated data, and simplifying operational processes.