Chiranthan Shadaksharaswamy

SNS Lab 5

Question 1: 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 part of Symantec, employs a range of methods to verify the authenticity of a certificate signing request (CSR) for their "Secure Site" certificates. Two of these methods include:

1. **Domain Validation**: VeriSign ensures that the domain name in the CSR matches the domain of the entity requesting the certificate. This involves sending an email to the registered administrative contact of the domain and requesting confirmation of the certificate request.
2. **Organization Validation**: VeriSign verifies that the organization applying for the certificate is a legitimate entity. This is done by scrutinizing legal documents like articles of incorporation, business licenses, or government-issued records. They also cross-check the organization's name and address with the information maintained by the relevant government agency.

Two limitations associated with these validation methods are:

1. **Susceptibility to Email Spoofing**:
    a. Domain Validation may be vulnerable to email spoofing attacks, where malicious actors send deceptive emails to the domain's registered administrative contact, masquerading as the legitimate certificate requester to trick them into confirming the certificate request.
2. **Time-Consuming and Potentially Imperfect**:
    a. Organization Validation can be a time-consuming process and may not offer absolute certainty.
    b. The process of verifying legal documents and confirming the organization's identity can be labor-intensive and may not always be foolproof.
    c. This challenge is particularly evident when dealing with less-established entities or those with less-defined ownership records.

Question 2: What are Extended Validation certificates? What are two advantages and disadvantages to using extended validation certificates?

Answer:

1. The most advanced level of SSL certificate is referred to as Extended Validation (EV). These certificates are designed to guarantee data integrity and encryption.
2. However, the primary distinction lies in the thoroughness of website owner identification. By verifying the legal identity of the website owner, an EV certificate provides the highest level of confidence in digital identity.
3. An EV certificate signifies that the domain is owned by a legally registered entity. It's crucial to emphasize that this does not automatically guarantee the reliability of the website, both in practice and from a legal perspective.

Advantages:

1. **Elevated Confidence:**
    a. EV certificates instill a greater sense of trust when compared to domain validation.
    b. The verification process involves multiple steps, including confirming the requester's authorization to use the domain, obtaining permission to issue the certificate, and ensuring their legal status aligns with official documentation.
2. **Robust Encryption:**
    a. EV certificates utilize a 2048-bit signature and strong 256-bit encryption, ensuring the security of data transmission.

Disadvantages:

1. **Reliance on User Action:**
    a. EV certificates heavily depend on user involvement. Entrusting users with the responsibility to verify the identity of the domain owner and organization each time manually and accurately they visit a website which may not be practical. Some technological constraints should be independently imposed to ensure the effectiveness of EV certificates.
2. **Limited Validity Period:**
    a. EV certificates often have a comparatively brief period of validity, necessitating more frequent renewals compared to other certificates.

Question 3: What steps could you take to ensure that you have the correct root certificate for VeriSign in your browser?

Answer :

1. Open the web browser.
2. Choose "Privacy" from the menu.
3. Select Security Preferences.
4. Navigate to the certificate management section.
5. Ensure that you are using the latest version of the root certificate by visiting the official website.
6. On authorities page the VeriSign certificate is available for inspection and validation

Question 4: Compare and contrast the OCSP and CRL approaches for certificate revocation.

Answer:

Certificate Revocation Lists (CRL):

1. Compile all certificates marked as invalid by a Certificate Authority (CA).
2. Take more time to validate certificates when compared to OCSP.
3. Place a greater strain on network resources when assessing the validity of a single URL, as opposed to OCSP.
4. Lack the ability to provide immediate, real-time updates regarding certificate revocations.

Online Certificate Status Protocol (OCSP):

1. Exclusively indicate the status of the requested website's certificate in terms of revocation.
2. Expedite the certificate verification process.
3. Consume fewer network resources in comparison to CRL.
4. Offer real-time updates on the status of certificate revocations.

Question 5: 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:
When a certificate is received by a browser, it places reliance on two crucial fields within the X.509 certificate to ascertain its suitability for the website it is connecting to are the Common Name (CN) and the Subject Alternative Name (SAN).

The Common Name :

a. The Common Name typically includes the domain name or hostname for which the certificate has been issued.
b. To validate the certificate's legitimacy, the browser cross-references the Common Name with the website's domain name it intends to access.
c. If there is a match, the certificate is considered valid for that specific site.

The Subject Alternative Name :

a. The Subject Alternative Name serves as an extension within the X.509 certificate and is capable of accommodating a variety of entries, such as DNS names, IP addresses, and email addresses.
b. When the certificate includes a SAN extension, the browser conducts a thorough examination, not only referencing the Common Name but also scrutinizing the SAN field.
c. If it discovers a domain name or hostname in the SAN field that aligns with the website's domain, the certificate is deemed valid.
d. In essence, the SAN field complements and fortifies the validation process, augmenting security measures.

Question 6: Why do certificates have an expiration date if there are other certificate revocation mechanisms (ie. OCSP and CRL)?
Answer :

1. Mechanisms like OCSP and CRL play a crucial role in revoking certificates before they reach their expiration dates.
2. However, there are situations where these systems might fail or become inaccessible. In such cases, certificate expiration acts as a fail-safe, ensuring that certificates will eventually become invalid.
3. By imposing a time limit on certificate validity, expiration dates serve as a protective measure against the risks associated with using certificates for extended periods.
4. When certificates lack expiration dates, trust can persist indefinitely, even if vulnerabilities are discovered.

5. The requirement for renewal due to expiration compels organizations to regularly update their certificates, reducing the potential for security issues.
6. Certificate expiration also ensures that certificates align with the latest security standards. Certificate Authorities (CAs) incorporate the most recent security updates when issuing new certificates.
7. Any changes to a website, such as alterations in the company's name or hosting location, during the certificate's validity period necessitate the acquisition of a new certificate to maintain security compliance.