aslam

by S S

Submission date: 26-Sep-2023 11:33AM (UTC-0700)
Submission ID: 2147482445
File name: Week_2_Part_1.docx (17.89K)
Word count: 1502
Character count: 8277

What are digital certificates used for?

Why are certificates important for online payments and banking security

Digital certificates are used globally to ensure security during data transmission between the website server and your systems. They have numerous applications in online payments and other applications in online payments and banking, and a few of them are listed below.

- They ensure data encryption during the data transmission over the internet as they ensure data transmission.
- They are used to identify any organization's individual, device or server as they ensure that the entity presenting the certificate is who they claim to be.
- In various online applications, digital certificates act as a means of identity verification and cryptographic assurance.
- In terms of online payments and banking security, certificates are essential. They assist in making sure customers connect to reputable banking websites and guard against unauthorized access to financial information.
- They also play a vital role in manual authentication between the customer and bank server, ensuring both are legitimate parties.
- They also ensure data encryption, which protects sensitive data from interception and tampering.
- They also guard' customers from phishing attempts. They can just check the certificate of the banking website to confirm its authenticity.

Other Uses of Digital Certificates

There are multiple uses of these certificates in other fields, and some are listed below.

- They are used to secure IoT systems to secure communication between the cloud and devices.
- They are also used in governmental institutions, such as filing tax document submissions.
- They also ensure secure data transmission in industries such as health care.
- They also play a vital role in controlling the system access and ensuring only authorized persons gain access to a restricted source.
- They are also widely used to sign a digital document to ensure authenticity.
- They also ensure the secured data transmission between apps and remote servers.

In conclusion, digital certificates are flexible data protection, internet security, and authentication instruments. They are crucial for safeguarding sensitive information, financial transactions, and online payments, but they are also helpful in many other fields and applications where security and trust are top priorities.

What kind of attacks does TLS mitigate and why is this important for online banking?

Transport layer security is today's standard as it helps to secure communication between a client machine and a website server and encrypts data during the transmission so that if a hacker even intercepts the data, he/she cannot read it and use it for beneficial purposes. It faces several types of attacks, a few of which are listed below.

Passive Attacks

Man in the Middle Attacks

It uses digital certificates to verify the originality of the server to the client, which prevents the hacker from intercepting and altering data in the transmission. If someone tries to enter the communication channel, the browser will automatically raise a red flag and warn about it.

Data Tampering

In this type of attack, hackers try to hack the data to tamper and modify data as it use cryptographic integrity checks to ensure secure data transmission between server and client. If any changes occur, it will generate an error and alert both parties regarding this.

Passive Attacks

In this attack, hackers try to extract the data from the intercepted data. As the data is encrypted during the exchange, they cannot extract sensitive information such as login credentials, account details, etc.

Session Hijacking

Data is encrypted using session keys using TLS as a mitigation measure. These keys are particular to each session and are negotiated during the opening handshake. Without the session keys, which are difficult to obtain, an attacker cannot decrypt the encrypted traffic even if they can intercept it.

It is essential in the banking sector, where much financial and sensitive data is transmitted every second and comprises such sensitive information. Compromising this information would provide unauthorized access to the banking accounts, leading to substantial financial loss. If it is compromised on a larger scale, it may also lead to the destruction of the country or specific geographic banking system. That is why it is essential to protect this data, its confidentiality, and its integrity.

How do browsers use certificates to ensure browsing security?

Browsers use the certificates to ensure browser security in multiple ways, and a few of them are given below.

When we visit a website over HTTP, the browser checks the domain name and public key of the server, checks the website certificate, verifies its authenticity through built-in Certificate authority and allows us to access the website only if the certificates are valid and trustworthy. In many cases, there is a chain certificate CA, and the browser checks the entire chain of trust and ensures that a trusted CA signs each certificate.
Browsers check to see if the certificate for the website has been revoked. Certificates may be revoked for several reasons, including the loss of the private key or a change in ownership. To verify the certificate's status, browsers employ the Online Certificate Status Protocol (OCSP) or certificate revocation lists (CRLs).
It also ensures the certificate's validity, and if it expires, it directly warns the user.
Browsers check to see if the certificate's domain name corresponds to the website's domain name the user is attempting to access. As a result, attackers cannot use a legitimate certificate for a different domain.

The warning in the shown picture means that the website certificate cannot be verified, which generates a warning to the user. It may be due to the following reasons.

- Either its certificate is expired.
- There is an issue in the certificate authority chain.
- Domain name and certificate name do not match with each other.
- The certificate may be revoked, due to which it is generating this error.

Certificate Authorities

Why would it be wrong if a trusted certificate authority was compromised?

If a trusted certificate authority is compromised, it will disrupt the chain of trust of certificates, which would lead to allowing the hackers and criminals to get access to the systems, just like what happened last year when MonPass was hacked, which allowed the hackers to get access to the backend client data. The following are the reasons why it should be avoided at any cost.

- If a CA is compromised, it can issue malicious digital certificates to hackers, which later can be used to impersonate websites and services, providing grounds for man-in-middle attacks in which sensitive data is compromised, which can be manipulated afterwards.
- A compromised CA would erode the trust between users and the organization, making them reluctant to share sensitive information or do online transactions.
- Few compromised certificates could influence millions of users globally as the hackers would use these certificates to launch attacks on a large scale.
- As certificates work in the chain, if a few of them are compromised and hackers take measures to hide their tracks, he/she can remain unnoticed for an extended period, allowing them to carry out their activities without even being noticed.
- E-commerce depends on sharing personal information and online transactions, so if any connections are compromised, it will lead to a vast business reputation and financial loss.
- If a CA is compromised and detected and certificates are revoked, users would still be reluctant to use certificates used by that CA, significantly impacting websites and services using those certificates.

- The compromised CA's reputation would suffer greatly, possibly with legal and financial repercussions. The CA might lose clients and customers and be sued or subject to regulatory sanctions.
- It takes much work to inspect the effects of a CA compromise. This involves taking time-consuming and expensive steps like revoking compromised certifications, performing forensic investigations, and putting in place additional security measures.

Certificate Transparency:

Certificate transparency is essential, and a few of the most important reasons are listed below.

- It creates a trustworthy environment between customers and websites. When customers know their connections are secure using certificates that have undergone multiple transparency checks before deployment, they feel safer, enhancing potential business growth.
- It is designed to enhance the level of security of HTTP and online communications by only allowing the issuance of digital certificates requested by legitimate website owners, which leads to the enhancement of trust in digital certificates.
- It is also quite helpful for detecting maliciously issued certificates and also helps us to detect whether it has no genuine owner, preventing unauthorized certificate issuance.
- Authentic certificates might not always be quickly detected by traditional certificate management. In order to protect against long-term risks, CT allows domain owners to keep track of the certificates granted for their domains.
- CT enables swift revocation if a certificate is compromised or misused by someone else. This rapid action method is beneficial in minimizing the potential damages.
- CT's presence promotes accountability inside the CA sector. CAs are driven to follow security best practices to protect their reputation and credibility.
- It ensures a very transparent system as all CAs are required to publically log all the certificates issued by them, which makes the system more transparent and auditable, and it holds CAs accountable for their actions.

aslam

ORIGINALITY REPORT

2%	1%	0%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Hertfordshire Student Paper	1%
2	docs.oracle.com Internet Source	1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		