Task 1B Certificates

- What are digital certificates used for?

Digital certificates are used to verify the identity of a person, device, or server. They are used in a variety of applications, including:

Secure websites: Digital certificates are used to create secure connections between web browsers and web servers. This is known as HTTPS, and it is used to protect sensitive data, such as credit card numbers and passwords, from being intercepted by attackers.

Email signing and encryption: Digital certificates can be used to sign and encrypt emails. This helps to ensure that emails are authentic and have not been tampered with in transit.

Code signing: Digital certificates can be used to sign code, such as software applications and operating system updates. This helps to ensure that the code is authentic and has not been tampered with.

Network security: Digital certificates can be used to authenticate devices and users on a network. This helps to prevent unauthorized access to the network.

- Why are certificates important for online payments and banking security?

Online payments and banking are highly sensitive activities, and it is important to protect the data that is transmitted during these transactions. Digital certificates play a vital role in this protection by providing a way to verify the identity of the parties involved in the transaction.

For example, when we make an online payment, your web browser will use a digital certificate to verify the identity of the website that you are visiting. This ensures that we are not sending our payment information to a fraudulent website.

Similarly, when we log in to our online banking account, our web browser will use a digital certificate to verify the identity of the bank's website. This ensures that we are not entering our login credentials into a phishing website.

- What other uses do certificates have?

Digital certificates can also be used for:

Digital signatures: Digital certificates can be used to create digital signatures. Digital signatures are electronic signatures that can be used to sign electronic documents, such as contracts and invoices.

Electronic document security: Digital certificates can be used to protect electronic documents from unauthorized access, modification, and disclosure.

Software distribution: Digital certificates can be used to sign software applications and operating system updates. This helps to ensure that the software is authentic and has not been tampered with.

IoT security: Digital certificates can be used to authenticate IoT devices and secure communications between IoT devices.

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

TLS mitigates a variety of attacks, including:

Man-in-the-middle attacks: A man-in-the-middle attack is when an attacker intercepts communications between two parties and impersonates one of the parties. TLS prevents this by encrypting the communications so that the attacker cannot read them.

Eavesdropping attacks: An eavesdropping attack is when an attacker intercepts communications between two parties and listens to them. TLS prevents this by encrypting the communications so that the attacker cannot hear them.

Packet sniffing attacks: A packet sniffing attack is when an attacker captures network packets and analyzes them to steal sensitive data. TLS prevents this by encrypting the packets so that the attacker cannot read them.

TLS is important for online banking because it helps to protect sensitive data, such as account numbers and passwords, from being intercepted by attackers.

- How do browsers use certificates for ensuring browsing security?

When we visit a website, our web browser will use a digital certificate to verify the identity of the website. This is done by checking the certificate's signature, which is issued by a trusted certificate authority (CA). If the signature is valid, the browser will establish a secure connection with the website.

The browser will then use the certificate to encrypt the communications between your browser and the website. This ensures that any sensitive data that you send to the website, such as your credit card number or password, is encrypted and cannot be intercepted by attackers.

  - What does the warning in the picture above mean?

It means that my browser can't establish a secure connection with the website. The reason is that my browser is unable to confirm that the site has a valid SSL certificate. Also `NET::ERR_CERT_COMMON_NAME_INVALID` means that the certificate’s domain name doesn't match the address bar..

Certificate Authorities

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

Because it could allow an attacker to impersonate any website and steal users' personal information. If an attacker compromised a certificate authority that was trusted by a user's browser, they could create a fake certificate for a popular website, such as a bank website. When the user will visit the fake website, their browser would think that it was the real website and would send their personal information to the attacker.

- Why is certificate transparency important?

Certificate transparency is important because it helps to prevent fraudulent certificates from being issued. By making all certificates public and easy to audit, certificate transparency helps to ensure that only valid certificates are used.

Task 3 PSD2 Analysis

- Write further analysis on the effects of PSD2 on payment security for Task 3 (max 250 words)

One of the key effects of PSD2 on payment security is the introduction of strong customer authentication (SCA). SCA requires payment service providers (PSPs) to authenticate customers using two or more independent factors before authorizing a payment. This can include factors such as a password, PIN, or biometric identifier.

Another positive effect of PSD2 on payment security is the increased oversight of PSPs. PSD2 requires PSPs to have robust security measures in place to protect customer data and prevent fraud. This includes measures such as data encryption, access controls, and security monitoring.

PSD2 also led to the development of new and innovative payment solutions, many of which are more secure than traditional payment methods.

Although, PSD2 is a complex and multifaceted regulation, but its impact on payment security is positive. PSD2 has made it more difficult for fraudsters to succeed, promoted the development of new and innovative payment solutions, and increased competition in the payments industry.

- Write a short (max 500 words) analysis on the effects of emerging AI-technologies on online banking frauds and biometric authentication with at least two examples where it has already been used in frauds or other criminal activities.

Emerging AI-technologies are having a significant impact on both online banking frauds and biometric Analysis on the Effects of Emerging AI-Technologies on Online Banking Frauds and Biometric Authentication.

Artificial intelligence (AI) is rapidly transforming the online banking landscape, both for the better and for the worse. On the one hand, AI-powered technologies are being used to develop innovative solutions to detect and prevent online banking fraud. On the other hand, criminals are also increasingly exploiting AI for their own nefarious purposes.

One of the most promising applications of AI in the fight against online banking fraud is in the area of anomaly detection. AI-powered systems can be trained to identify patterns in customer behavior that may indicate fraudulent activity. For example, a system might be trained to flag transactions that are unusual in terms of size, frequency, or timing.

Another way that AI is being used to combat online banking fraud is through the use of natural language processing (NLP). NLP systems can be used to analyze customer communications, such as emails and chat transcripts, for signs of fraud. For example, an NLP system might be able to identify suspicious language patterns or inconsistencies in the customer's story.

Biometric authentication is another area where AI is having a major impact. Biometric authentication systems use unique physical characteristics, such as fingerprints, facial features, or voice patterns, to identify individuals.

AI is being used to develop new and more sophisticated biometric authentication systems. For example, AI-powered facial recognition systems are now able to identify individuals with a high degree of accuracy, even in challenging conditions such as low light or poor image quality.

Overall, the effects of emerging AI-technologies on online banking frauds and biometric authentication are complex and multifaceted. On the one hand, AI is being used to develop innovative solutions to combat online banking fraud. On the other hand, criminals are also finding ways to exploit AI for their own purposes.

It is important for the banking industry and law enforcement to work together to stay ahead of the curve and develop new ways to mitigate the risks posed by AI-enabled fraud.

Examples of AI-enabled fraud

1. In 2020, four Florida men were charged with bank fraud conspiracy for allegedly defrauding banks and stealing what turned out to be $24 million from government COVID economic relief payments. Prosecutors said in 2021 that the men used fake identities and fake companies they had set up in the past, to receive millions of dollars from the Payroll Protection Program.

2. In early 2020, a branch manager of a Japanese company in Hong Kong received a call from a man whose voice he recognized—the director of his parent business. The director had good news: the company was about to make an acquisition, so he needed to authorize some transfers to the tune of $35 million. The manager, believing everything appeared legitimate, began making the transfers. What he didn’t know was that he’d been duped as part of an elaborate swindle, one in which fraudsters had used “deep voice” technology to clone the director’s speech.

- Summarize what is subdomain takeover and what measures can an organization take to protect itself from it (max 250 words)

A subdomain takeover is a type of cyberattack in which an attacker gains control over a subdomain of a targeted website. This can happen when a subdomain is no longer in use and the DNS record for that subdomain is still pointing to an active server. The attacker can then register the subdomain and host malicious content on it.

Subdomain takeovers can be used to launch a variety of attacks, such as:

Phishing: The attacker can create a fake website on the subdomain that looks like the legitimate website. When users visit the fake website, the attacker can steal their personal information, such as login credentials and credit card numbers.

Malware distribution: The attacker can distribute malware to users who visit the subdomain. The malware can be used to steal data, spy on users, or damage their computers.

Denial-of-service (DoS) attacks: The attacker can flood the subdomain with traffic, making it unavailable to legitimate users.

Organizations can protect themselves from subdomain takeovers by taking the following measures:

Regularly review DNS records: Organizations should regularly review their DNS records to identify any unused subdomains. Once an unused subdomain is identified, the DNS record should be removed.

Use strong passwords: Organizations should use strong passwords for their DNS accounts and other cloud resources. This will help to prevent attackers from gaining unauthorized access to these resources.

Enable DNS monitoring: Organizations should enable DNS monitoring to detect any unauthorized changes to their DNS records. This will help to identify subdomain takeovers early, before the attacker can launch an attack.

Use a web application firewall (WAF): A WAF can help to protect against subdomain takeovers by filtering traffic to subdomains. The WAF can be configured to block traffic from known malicious IP addresses and to block suspicious requests.

In addition to the above measures, organizations should also educate their employees about subdomain takeovers and other cyber threats. Employees should be trained to identify phishing emails and to be suspicious of any unexpected changes to websites.