Veton Abazovic
NetID: va187

Computer Security

Assignment 9

Question 1

What are minutiae points in a fingerprint?

Answer: Minutiae points in a fingerprint are major features in a fingerprint. The minutiae points are used to determine the uniqueness of a fingerprint image.

Question 2

How does invisible reCAPTCHA (reCAPTCHA v3) work?

Answer: Invisible reCAPTCHA (reCAPTCHA v3) monitors the traffic and looks for any suspicious activity and it does this by using adaptive risk analysis to score traffic. With this website owners can then determine how to handle the activity.

Question 3

How does reCAPTCHA adapt for mobile devices?

Answer: ReCAPTCHA adapt for mobile devices by instead of having t insert many characters, on a mobile device the user would have to pick a series of pictures that match the category given such as pick all the pictures with a car in it.

Question 4

What does the author state as the main problem of using a biometric for combined identification and authentication?

Answer: The main problem that the author states as the main problem of using a biometric for combined identification and authentication is that biometric is public information thus if at the wrong hands can be used against you. People can obtain your biometrics or access the system by spoofing and when authentication is stolen there is no way to provoke it and there is also no actual evidence that all claim that all biometrics are unique,

Question 5a

How does U2F operate without a shared secret?

Answer: U2F operate without a shared secret by generating a new pair of keys for every service. It sends this new key to the server and validates it with the public key during registration and only the service stores the public key.

Veton Abazovic
NetID: va187

Question 5b

What is the technique that U2F uses to authenticate with the server?

Answer: The technique that U2F uses to authenticate with the server is that the server generates a challenge and then sends the challenge to the key attached with the checksum. After that the security key then generates a private key from the registration then uses the checksum to check the device is valid or Is the original. Then the device signs the challenge from the server and private key and the server verifies the signature using the public key.