Task 2

Payments

Because chips are more secure than magnetic stripes, modern payment cards use chips. Chips possess dynamic data; every transaction would present different data, which makes the attacker difficult to clone or steal the information. Magnetic stripes possess static data, which is easily copied. This dynamic nature makes chips much safer.

An EMV certificate is a kind of digital signing that authenticates both the card and the terminal in any transaction. They protect the integrity of the payment by checking that both parties are real, and no fraud or tampering of any sort is going on. These certificates are essential in offering security for transactions.

Other payment card fraud includes card-not-present fraud, such as transactions not requiring physical cards-for instance, ordering goods via the Internet or over the phone. The convenience of contactless payments makes them very vulnerable to skimming, a process in which card information is captured from a distance by an attacker using special devices. Limits on the amount per contactless transaction reduce these risks.

MFA

MFA added new steps to banking security by asking users for more forms of proof, such as a password-something you know-a code sent to your phone, which is something you have-or biometrics like a fingerprint, which is something you are. In the event of an attack, this makes life more complicated for the attackers because now they have to compromise more layers.

MFA is a means of increasing security where an attacker-even if the password has been compromised-needs to bypass another layer, be it a code or a fingerprint, which is almost impossible. Thus, the possibility of fraud goes down.

Common MFA methods include one-time passwords via SMS, app-based authentications like Google Authenticator, and biometric ones such as fingerprint scanning. All these together provide additional layers of verification beyond passwords to make security tighter.

Attacks against 2FA focus on issues like stealing the time-based OTP generation key. SMS-based 2FA is also vulnerable to SIM swapping-a type of attack that allows the attacker to take control over a phone number with the intent of receiving authentication codes to later access accounts.