Task 1.B

Digital certificates are used to establish trust and secure communications over networks. They authenticate parties communicating with each other, encrypt data transmissions by providing public keys and make sure communications are secure and trusted. This is important for online payments and banking to make sure you are dealing with the correct entities and not criminals who want to drain your bank account. They can also be used for direct communication with other users to make sure that the users are legitimate and not someone posing as another.

TLS mitigates attacks like eavesdropping, man-in-the-middle attacks and replay attacks. Eavesdropping would allow an attacker to gain access to login credentials, MITM attacks could be used to modify the address user is trying to send money to and replay attacks can be used to force server to make actions that have already been taken.

Browsers use certificates to, well, ensure safe browsing. By authenticating websites through their digital certificate, the browser can make sure you are browsing the legitimate site and not that of an impostor. Digital certificates are also used by browsers to encrypt data and verify data integrity.

The warning in the picture complains about certificate naming. This means that the name in the certification does not match that of the domain.

Task 2.

Modern payment cards use chips rather than magnetic strips, simply because they are more secure. A strip stores a static data, which is a lot more easier to copy rather than the data that is contained on the chip. The chip also has cryptographic processes within it used for authentication, that create one-time codes used for transactions.

EMV certificates are used to secure communications between the card chip, payment terminal and the banks systems. All three need to be authenticated using certs and certs enable the use of encryption and secure data exchange that increase payment security.

Some attacks that are used against payments cards are eavesdropping, MITM and very obviously, scamming and phishing. With CNP, attacks are generally about getting the payment and card information, like keyloggers and phishing. For contactless payments, attacks are about eavesdropping, skimming or generally just stealing the card.

Multifactor authentication used by banks has two parts to it. First is the user information, like username or ID and password. Then the second authentication step is usually a confirmation through users mobile phone. The other, now less common way is to use a banking sheet or whatever the English name for it is, which contains a code of numbers for different transaction IDs. The user crossreferences the ID wanted by the banking app to the one on his sheet. The user then inputs the code written for that ID and gains access or makes the transaction.

MFA increases security by making sure that the user who is making the transaction is really who they claim to be. For example, if an attacker has managed to gain access to users username and password, they cannot do any transactions without bypassing the second authentication. The second authentication is also usually near impossible to break using brute-force methods, so attackers gain nothing.

MFA methods I use daily are secondary authentications through my phone, generally using codes or my fingerprint, when signing into different places.

Attacks against 2FA are usually phishing attacks, as only the user who has access to the 2FA applications/methods can provide the information required to break through them. However more sophisticated attacks do exist, like algorithm or seed compromises for TOTP, where an attacker has managed to break the algorithm or get the seed value for the TOTP and can then generate legitimate codes. For SMS attacks there are SIM swapping, where the attacker then gets all the SMS messages sent to the victim and SS7 attacks where the attacker can intercept SMS messages.

Task 3.

There are multitude of different card frauds, such as card-not-present, ATM and point-of-sale frauds. Within these categories there are multiple different kinds of frauds, like mail and telephone fraud, online fraud, counterfeit fraud, lost-and-stolen and card-not-received fraud. Geographically, most card frauds inside the SEPA are CNP frauds, with very few ATM and POS frauds. This is still the same outside of SEPA areas, but the number for ATM and POS fraud is bit higher. Places that have higher card markets (i.e.. cards per inhabitant) also experience more card frauds than places with less cards.

While CNP frauds are the most common frauds, this was not the case a decade ago. In 2007 CNP frauds were merely 48% of the frauds committed, while POS frauds measured a nice 33% and ATM fraud 20%. These types of frauds decreased over the years as EMV became the standard for banking cards. While EMV replaced the magnetic strip cards in SEPA quite fast, outside of SEPA ATM and POS frauds remained relevant for a longer time, as they were slower to adopt EMV.

Another notable change within the SEPA area is the amount of card purchases an individual does in a year. In 2010, a SEPA inhabitant owned 1.4 cards and made 63 transactions per year with them. However, this is rather skewed view on the subject, as a single Romanian made merely 14 card transactions in a year, while the average Finn made 200 transactions. These numbers are almost comically small compared to 2019 where the average SEPA inhabitant makes 8533 card transactions per year. The only country boasting less than 1000 card transactions per year is Bulgaria, with mere 306 transactions per inhabitant.

Over the years the use of cards for online shopping has risen drastically, but more than anything the use of cards for common purchases like grocery shopping has far exceeded everything else. The highest risk of fraudulent transactions are with e-commerce. This is simply because e-commerce is the easiest way to commit fraud and with the rising amounts of online transactions, the amount of frauds will rise in hand. Already in 2009 most of CNP frauds were done through the internet.

Ensuring that data breaches do not occur is important as a major data breach can cause the loss of card details to criminals who can use those details to commit fraud. This is why the tokenisation of accounting details would help majorly to lessen the effects of data breaches. Tokenisation is a security measure where the card details are replaced with unique digital identifiers that can have restrictions placed upon them. These restrictions can for example mean that the token can only be used a few times to pay or that that token can only be used for a specific merchant.