1.

The main event of this report is that a cyber attack compromised customer data of EBay Inc. The involved data are email addresses, encrypted passwords, birth dates, mailing addresses and other information but not contain financial information. The breach was because the attacker obtained login credentials of employees which allowed them to access EBay’s corporate network. The exact number of compromised accounts is unknown, but it is a large number. The response of EBay Inc is urging users to change their passwords and investigate the breach. According to the investigation, there is no one responsible at this time. There are three responses outside the EBay Inc, the first is the market, EBay shares were down 0.2 percent after the attack. The second one is the security experts advised customers to be on the alert for fraud, especially if they used the same passwords for other accounts because it can be used in credential-stuffing. The third one is the research analysts said there was not enough information to assess if EBay had been negligent.

2.

a) In encrypted file transmission, especially in peer-to-peer file transmission, a cryptographic hash function is used to verify the integrity of the file. If a hash function fails to provide compression, the hash value will be long, same as its size. Therefore, it is the same as sending the file two times, which is double the transmission time.

b) In some encrypted database software or retrieval applications, a cryptographic hash function is used to map the key space to the storage space. If a hash function fails to provide efficiency, the computing time of the hash value will be long, especially when the data volume is large. Therefore, the search function or the computing time of new keys in modified databases will be inefficient.

c) In password systems, a cryptographic hash function is used to encrypt original password text. If a hash function fails to provide one-way, then attackers can obtain x with a known hash algorithm . By inverting this process, the original password text is no longer safe.

d) In digital business, especially such as digital contracts. A cryptographic hash function is used in digital signature generation and verification. If a hash function fails to provide collision resistance properties, others are able to forge digital signature and verification. Therefore the digital signature and verification will not be unique, which can be a security breach.

3.

a) By adding photos on credit cards, it becomes a biometrics method of authentication. The photo represents “something you are”, and “you are your key”. In the information security area, biometics are a more secure alternative to passwords. When a thief is using someone else’s credit card which has a photo on it, if the merchants have questions like “Who are you?”, “Are you who you say you are?”, the thief is highly likely unable to prove those questions. In other words, this is a one-to-one comparison. If the thief claims he or she is the owner of the photoed credit card, the only comparison is the thief and the photo on the card. Besides, comparison can’t be made between a person and credit cards without photos. Therefore, it has a lower error rate due to the small number of comparisons that must be made, because more comparisons required, the higher the error rate. In conclusion, based on these reasons, although most people can’t distinguish photos very nicely, including photos on credit cards can lower the error rate. In this case, the fraud rate drops significantly.

b) Because it is a two-factor authentication which requires both “something you have”(the plastic card) and “something you are”(the photo appears on a screen), which are the two out of the three “somethings”. Simply putting photos on plastic cards is less safe because others can forge similar plastic cards with their own photo. However, a photo appearing on a screen can be recognized as a password generator inside the plastic card, which is harder for others to forge or duplicate. Therefore, this approach is better than putting the photo on the card.

4.

a) Since there is only one password for n accounts, and the probability that a password appears in Trudy’s dictionary is given which is . Therefore, the probability that the password appears in Trudy’s dictionary is .

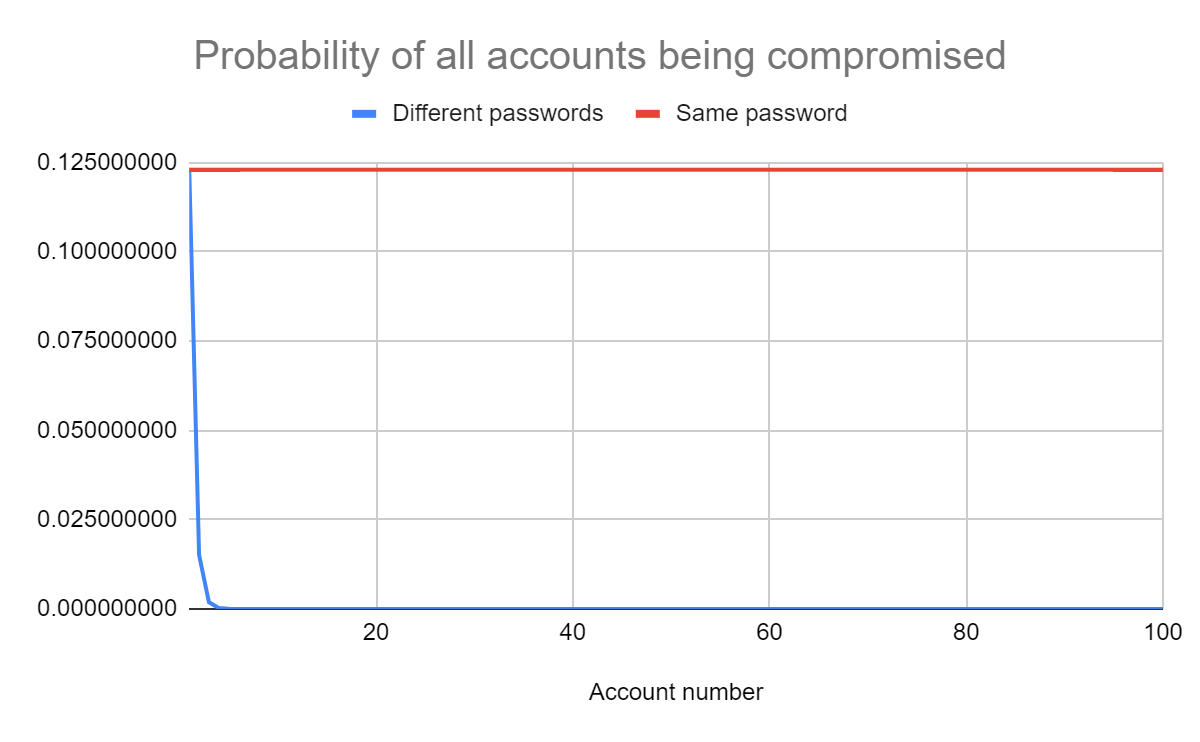
b) If the probability that a password appears in Trudy’s dictionary is p, then a password that doesn't appear in Trudy’s dictionary is , for n distinct passwords for n accounts, the probability of those passwords that doesn’t appear in Trudy’s dictionary is . Therefore, the probability of at least one of your passwords appears in Trudy’s dictionary is .

When , which agrees with the answer to part a.

c) It is more secure than choosing different passwords for each account.

It is because the probability of all passwords appears in Trudy’s dictionary is . When is given, as , while using the same password for each account still have probability that all accounts are being compromised.

For example, for a random probability number :



X axis is the account numbers , Y axis is the random probability , the probability of all accounts being compromised decreased very quickly to 0 when using different passwords, while using the same password still has probability .

5.

a) Yes, Alice authenticates Bob.

After Bob sends and to Alice, Alice can calculate session key by hash function . So she can decrypt by using session key , to verify the constant value .

b) Yes, Bob authenticates Alice.

After Bob sends to Alice, Alice sends to Bob, which means Bob can decrypt the message by using shared symmetric key which only Alice and Bob know. Furthermore, after receive from Alice and decrypted , Bob can calculate session key by hash function , in order to verify the constant value .