Oscar Velez Moncada 10123550
CPSC 329 Assignment 2

PART 1

Q1.1 Assuming the face database is public, what is the entropy of the passwords?

The entropy is $\log_2(9^5) = 15.85$ bits

Q1.2 What is the probability of an adversary guessing the password of a selected user?

Adversary has a 1/59049 chance of guessing the password

Q1.3 Would the security increase if the database was not public? Justify your answer.

The security will increase because the attacker does not know the amount of faces used in the system. If the attacker has his own database of faces the attacker won't know if they'll have all the faces used in the database

Q1.4 What is the probability of an adversary guessing the password if the system allows one incorrectly answered challenge?

There is an 11% chance of an adversary guessing the password

Q1.5 Describe two attacks that are more effective in Passfaces compared to traditional password systems. You may assume the attacker has access to a verification terminal (Passfaces, or password system) that blocks an account after 3 unsuccessful attempts.

Shoulder surfing, mouse logging

Part 2: Picture-based password system

Q2.1 Outline the calculations by Alice for both methods, and comment on her final verdict regarding the security of the system.

Out of 100 possible pictures you choose 20, therefore 100 C 20 ≈ 5.3598×10^{20}. If we take the entropy of that number it is roughly 69 bits. Assuming that an adversary doesn't face a system where it allows as many tries as possible for each challenge, the adversary has a 1 in 2 chance (50%) of guessing each challenge correctly. This means the adversary has a 1 in 1,048,576 chance of passing the challenges. Method 2 seems redundant as it doesn't actually test the security of the system if Alice is correctly responding every challenge. If she doesn't know the answer to each challenge, she still has a 50/50 chance of guessing correctly, and each challenge grows more exponentially in terms of guessing all the way until the final challenge,

giving her a 1/1,048,576 chance of impersonating a user and guessing correctly each challenge presented by the system.

Q2.2 Compare both the usability and security of this system with a Passfaces based system described in Question 1. Assume that both systems would lock an account after 3 invalid attempts. In particular, (i) compare the success chance of an adversary in an online attack, and (ii) comment on the security and usability of password selection method of the two systems. (in Passfaces, passwords are randomly selected by the system; in the picture-based system a user selects their favorite set).

Although humans are better able to recognize pictures compared to text, these graphical passwords are hard to "write down" and it takes longer to authenticate & memorize, along with the server being unable to store hashes of passwords. Another problem that arises is that it becomes a lengthy process to verify each user and not every user will remember their password. The security of both systems seems to be greater than text-based password but at the expense of usability (due to the amount of time it will take to log in every time). Assuming both systems would lock after 3 invalid attempts in an online attack, the adversary has a greater chance of correctly guessing all of the challenges in the Passfaces system, although the adversary has a greater chance of correctly guessing a challenge with the picture based password system (1/2 chance vs. 1/9). Both systems have really good security but the picture-based system has greater security because of the greater number of challenges the adversary has to go through. The usability is greater for the Passfaces system because there are less images to recall from, and it will take less time for the user to enter the system, enhancing usability.

Q2.3 Bonus question: Suppose an adversary has an unlimited access to a verification terminal, which will not block any accounts regardless of the number of unsuccessful attempts. Describe an effective algorithm that would allow the attacker to fully learn a user's password. Include an estimate of how many guesses the attacker would need. (5 bonus points)

Rainbow table would be the best algorithm as it's basically a large dictionary with pre calculated hashed and the passwords from which they were calculated. It would be 100 guesses to map each picture in the database

PART THREE

Consider the following simple protocol intended to allow an RFID reader to authenticate an RFID tag. The protocol assumes that the tag can store a 32-bit secret key 's', shared with the reader, perform XOR operations, and receive and transmit 32-bit values. The reader generates a random 32-bit challenge 'x' and transmits $y = x \oplus s$ to the tag. The tag computes $z = y \oplus s$ and sends it to the reader. The reader authenticates the tag if $z = x$.

Q3.1 Show that a passive eavesdropper that observes a single execution of the protocol can recover key s and impersonate the tag. Demonstrate this can be done by recovering the key s from y = 0x3344ffac, and z = 0x1100dd0d.

If $y = x \oplus s$, $z = y \oplus s$, then it follows that $z = x \oplus s \oplus s$. Therefore for two binary bits b_1 and b_2, we have XOR(b_1,b_2) = 0 which means z = x. The secret key s = 224422a1

Q3.2 Can a passive eavesdropper learn the secret keys from observing a single execution of the protocol?

I don't believe a passive eavesdropper can learn the secret key from observing from a single execution, unless the eavesdropper knows what y and z equal like the last question.

Q3.3 Does the answer change if the attacker can observe multiple executions of the protocol?

The answer changes because now the attacker can gather more data as to what the challenge is and compare answers, and figures out what the shared keys could be. The shared keys s_1 and s_2 will be the same, there is a chance that a user will send the same x (for example) multiple times. Therefore you compare that data with previous times a user sent that challenge.

PART 4

Q4.1 Discuss Attack 1 on Protocol 1. Would the attack work? If so, outline the steps of the attack as well as the minimum resources required to execute it.

The attack wouldn't work as the attacker isn't doing anything to the database.

Q4.2 Discuss Attack 2 on Protocol 1. Would the attack work? If so, outline the steps of the attack as well as the minimum resources required to execute it.

The attack would work as the adversary would send a challenge that's different than the regular tag

Q4.3 Discuss Attack 1 on Protocol 2. Would the attack work? If so, outline the steps of the attack as well as the minimum resources required to execute it.

The attack would work as the adversary can tamper and give a different r so it performs an XOR operation with a different challenge

Q4.4 Discuss Attack 2 on Protocol 2. Would the attack work? If so, outline the steps of the attack as well as the minimum resources required to execute it.

It wouldn't work as the adversary will receive a different reply and could pay more than what was intended

PART 5

Q5.1 Does Canadian e-passport store biometric data?

According to the slides, no it does not yet store biometric data. According to the government of Canada website the only biometric information stored is the photo of the passport holder's face

Q5.2 Outline two important security and privacy issues related to biometrics.

Privacy: Verification & identification/authentication. Security: Unauthorized reading and cloning

Q5.3 Is the RFID chip in the passport the same as those used in the retail sector (e.g. for clothes)?

Yes, but the chips on passports are encrypted and coded to make it difficult for unauthorized readers to obtain information, meanwhile retail doesn't include security in their chips

Q5.4 Does the cryptography conform to the ICAO standard? (Using publicly available information.)

The cryptography conforms to the ICAO standard

Report one security or privacy related incident related to electronic passports. You answer should be at most 2 paragraphs long, and include the following:

◦ the attacker and the victim;

The "attacker" was a Syrian immigrant Bashar Habib with the help of "No Borders" an activist group, and the victim was the airport in Greece and London and its security system including the workers and the security system

◦ a description of the attack in your own words;

The Syrian immigrant wanted to escape from Greece where he was living after Syria so that he could become a doctor and help people in Syria. After living in Greece after escaping Syria, No Borders, an anarchist group helped him out by giving him a passport belonging to a 24 year old Austrian Marius Brem, even though they looked nothing alike. Bashar was able to pass through all the security until he failed the security check in Stansted airport where his passport failed. Even though is innocent, it depicts how easy it is to pass through security despite having a passport belonging to someone else, and he could've been anyone else with different intentions.

◦ how the attack was detected/contained and what were the attack consequences;

Home Office detected what happened after seeing a selfie when Bashar landed in London. He was taken into custody and later released and taken to a hostel. Home Office proscribed No Border as it undermined national security

◦ motivation of the attackers;

Bashar wanted to escape the refugee camp in Greece for a better life and future

◦ link to the reported incident on a credible website;

http://www.dailymail.co.uk/news/article-3794575/I-cleared-FIVE-checks-fake-passport-jihadi-Anarchists-Syrian-migrant-bogus-documents-smuggle-UK-RYANAIR-FLIGHT.html

◦ two evidences that the source is credible.

Authors names are given and article is from September 2016