CPSC 329 W17 - Assignment 2

University of Calgary
Due March 10, 11:59 pm.
Individual assignment, no group work.

Each part is worth 20 points.

Part 1: Passfaces

The Passfaces based password system was described during lectures. Consider a Passfaces system with a database of faces containing 100 entries in total. A user of this system is given a set of 5 randomly chosen passfaces from the database to memorize as their password. During verification, a user is presented with 5 challenges. In each challenge the user is shown a 3 × 3 matrix of faces. Each matrix includes one passface from the user's password set, and also 8 decoy faces chosen randomly from the remaining 95 entries in the database. In each challenge the user is asked to identify the passface from their password set. If the user passes each challenge, the user is authenticated.

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

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

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

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

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.

Part 2: Picture-based password system

Alice wants to evaluate a picture-based password system. The system has a database of 100 different pictures. To select a password, the user is allowed to browse through the database of pictures and select 20 pictures as their password. To authenticate, the user is presented with 20 challenges. Each challenge consists of 2 pictures displayed to the user: one is randomly chosen from the user's password set, and the other is randomly chosen from the remaining 80 pictures. The user is asked to identify which of the two pictures is from their password set. If the user correctly answers all 20 challenges, the user is authenticated.

To analyze the security of this system, Alice will use two different methods:

Method 1: Alice will find the number of possible passwords, and use that to calculate the probability that an adversary could guess a user's password.

Method 2: Alice will calculate the probability of impersonating the user by correctly responding to the set of 20 challenges presented by the system.

After analyzing the system with the above methods, Alice will determine the level of security as the highest success chance of the two methods.

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

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)

Part 3: RFID with exclusive or

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 ⊕ s to the tag. The tag computes **z** = y ⊕ 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`**.

Now consider the following variation of the protocol. The reader and the tag share two different secret keys: s_1 and s_2. The reader sends to the tag a challenge y = x ⊕ s_1, and the tag responds with z = x ⊕ s_2 after recovering x = y ⊕ s_1.

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

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

Briefly justify all your answers. Note: "⊕" denotes a bitwise XOR of two binary numbers. For two bits b_1 and b_2, we have $XOR(b_1,b_2) = 0$ if $b_1 = b_2$ and $XOR(b_1,b_2) = 1$ if $b_1 \neq b_2$.

Part 4: RFID with hashing

Consider an RFID authentication system used in a clothing retail store, where readers send challenges to tags. Challenges are random strings, and tags are wireless transponders that respond to the challenges. Each tag has a unique identifying string *Id*. The system can be used in two modes: scanning mode (used for taking inventory) and individual mode (used for determining prices during checkout). In a scanning mode a reader broadcasts a challenge, and all tags in a short range from the reader will receive the same challenge and respond. Under individual mode, a tag will receive an individual challenge and will respond with its *Id*, which will be used to determine the price that the customer must pay.

There are two different communication protocols, and two different attacks to consider.

Protocol 1:

$Reader \rightarrow Tags$: r	– Reader sends a random challenge r.
$Tag_{Id} \rightarrow Reader$: $h(r \parallel Id), Id$	– Tag replies with a hash of r concatenated with Id, and Id.

Protocol 2:

$Reader \rightarrow Tags$: r	– Reader sends a random challenge r.
$Tag_{Id} \rightarrow Reader$: $h(Id \parallel k_{Id}) \oplus r$, Id	– Tag replies with $h(Id \parallel k_{Id}) \oplus r$ and Id.

where $\parallel$ denotes string concatenation, and k_{Id} is a unique *secret key* that a tag with Id shares with the reader.

Attack 1:

An adversary tampers with tags' responses during a scanning round, with the goal of corrupting the shop's database.

Attack 2:

An adversary tampers with the response during checkout, with the goal of paying less for the item.

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.

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.

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.

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.

Part 5: Canadian E-Passport

The following paper gives a summary of security issues related to electronic passports.

https://eprint.iacr.org/2005/095.pdf

Some technical details about Canadian e-passport can be found at the following links:

http://news.gc.ca/web/article-en.do?nid=847639
http://www.cic.gc.ca/english/passport/help/epassport.asp
http://www.cic.gc.ca/english/department/media/multimedia/video/e-passport/e-passport.asp

You may use other *credible* sources if needed in your answers to the questions below.

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

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

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

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

Q5.5 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;
- a description of the attack in your own words;
- how the attack was detected/contained and what were the attack consequences;
- motivation of the attackers;
- link to the reported incident on a credible website;
- two evidences that the source is credible.

Submission details:

1. Submit a single PDF file for the entire assignment. Use a text editor or a word processor to write your assignment, then convert to PDF. This is to ensure that handwriting will not impede marking and evaluation of your work.
2. Write your name, student ID and tutorial section on the first line of the submitted assignment and use the following naming convention to name your file.

   `A1-<surname>-<student id>-<tutorial section>.pdf`

3. Submit your PDF file to D2L submission system. Submit on time. Late submissions will not be possible!

General information about all assignments:

1. Due time: All assignments are due at 23:59 on the due date listed on the assignment. Late assignments or components of assignments will not be accepted for marking without approval for an extension beforehand. What you have submitted in D2L as of the due date is what will be marked.
2. Extensions may be granted for reasonable cases, but only by the course instructor, and only with the receipt of the appropriate documentation (e.g. a doctor's note). Typical examples of reasonable cases for an extension include: illness or a death in the family. Cases where extensions will not be granted include situations that are typical of student life, such as having multiple due dates, work commitments, etc. Forgetting to hand in your assignment on time is not a valid reason for getting an extension.
3. After you submit your work to D2L, make sure that you check the content of your submission. It's your responsibility to do this, so make sure that you submit your assignment with enough time before it is due so that you can double-check your upload, and possibly re-upload the assignment.
4. All assignments should include contact information, including full name, student ID and tutorial section, at the very top of each file submitted.
5. Assignments must reflect individual work. Group work is not allowed in this class nor can you copy the work of others. For further information on plagiarism, cheating and other academic misconduct, check the information at this link:

http://www.ucalgary.ca/pubs/calendar/current/k-5.html.

6. You can and should submit many times before the due date. D2L will simply overwrite previous submissions with newer ones. It's better to submit incomplete work for a chance of getting partial marks, than not to submit anything.
7. Only one file can be submitted per assignment. If you need to submit multiple files, you can put them into a single container. The container types supported will be ZIP and TAR. No other formats will be accepted.
8. Assignments will be marked by your TAs. If you have questions about assignment marking, contact your TA first. If you still have questions after you have talked to your TA then you can contact your instructor.