The University of Queensland
School of Information Technology and Electrical Engineering

Semester 2, 2017

COMS3000/7003 – Tutorial 4, Answers

Q1) Explain what "false accept" (False Match) and "false reject" (False Non Match) errors are for an authentication system.

A false accept error occurs when the verifier accepts the claimant's evidence, but the claimant is NOT, in fact, authentic. (Acceptance of an impostor.)

A false reject error occurs when the verifier rejects the claimant's evidence, even though the claimant is, in fact, authentic. (Rejection of a genuine user.)

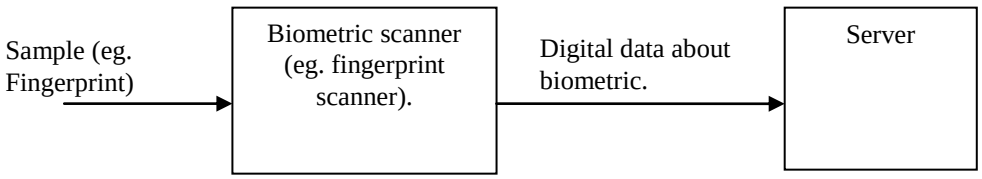
Q2) Compare the biometrics 'hair colour' and 'fingerprint' according to the following criteria:

- Universality
- Distinctiveness
- Permanence
- Performance
- Acceptability
- Circumvention

Use the labels High, Medium, and Low.

	Hair Colour	Fingerprint
Universality	L (Relatively large percentage of bald people)	H/M (Relatively small percentage of people with no fingers or lacking sufficiently strong pattern)
Distinctiveness	L (Relatively small number of distinct hair colours)	H
Permanence	L (can easily be changed)	H
Performance	H (accurate and fast reading is possible)	H
Acceptability	H (Scanning process is not intrusive, similar to face recognition)	M (Physical contact is required)
Circumvention	H (e.g can easily colour hair or use a wig)	M (circumvention is possible, e.g. with "Gummy fingers")

Q3) Draw a block diagram of a biometric authentication system that includes the biometric scanner (measuring device), a communications link, and a server containing a template database. Explain two ways in which a biometric authentication system might be vulnerable to a replay attack at different points in this diagram.



It may be possible to acquire a copy of a valid fingerprint, from a door say, and replay that fingerprint to the biometric scanner (the left arrow). It may also be possible to eavesdrop valid information that is transmitted from the scanner to the server, and later to replay that information.

Q4) A biometric device can be used in *identification mode* or *verification mode.* In which situation will we have a higher False Match Rate?

a) Explain your answer using an intuitive argument.

The higher error rate will occur when the device is used in identification mode. The intuitive argument is that when the biometric system tries to match your sample against just one record in the database, there's only one chance for a false accept error. If it tries to match your record against every record in the database (because you're not independently identifying who you are), there are many more chances for a false accept error.

b) Use a simple mathematical argument. For this you can make the following assumptions:

We can model both identification and verification as random processes. Let P_1 be the probability of a False Match (false accept) in a verification trial, where we have a 1-to-1 match problem. We now want to find P_N, the probability of a False Match in an identification trial, searching through a database of size N. The identification process (1-to-N match) can be modeled as N independent verification processes (1-to-1 matches)

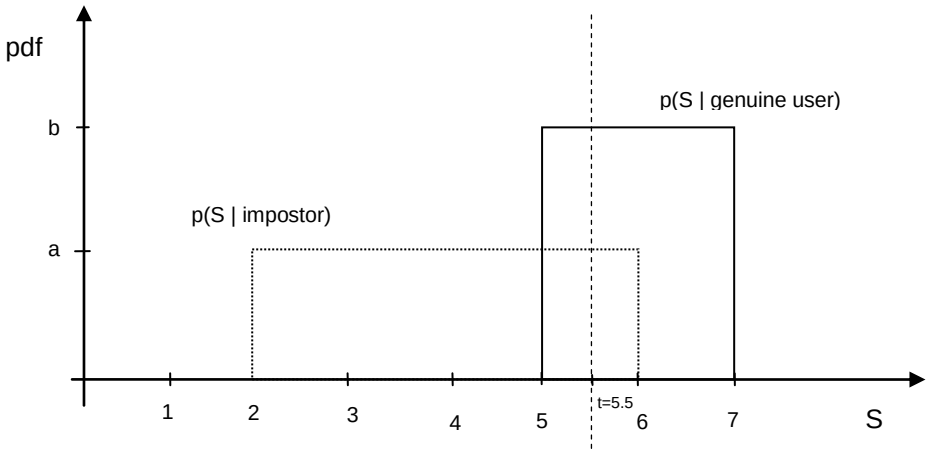
The probability of *not* getting a False Match in a single trial is $(1-P_1)$.
The probability of *not* getting any False Matches in N independent trials is $(1- P_1)^N$
For an identification trial to fail, at least one of the N verification trials (1-to-1 matches) needs to fail.
The probability of getting at least one False Match in N independent trials is:
$P_N=1 - (1-P_1)^N$

For small P_1 and large N, P_N is significantly larger than P_1.

For example: $P_1=0.001$ (99.9% correct rejection)

- N=200: $P_N=18\%$ (chance of false accept)
- N=2000: $P_N=86\%$
- N=10,000: $P_N=99.995\%$

Q5) Consider a biometric system with the following (somewhat unrealistic) conditional probability density functions for the matching score S for an impostor and a genuine user.



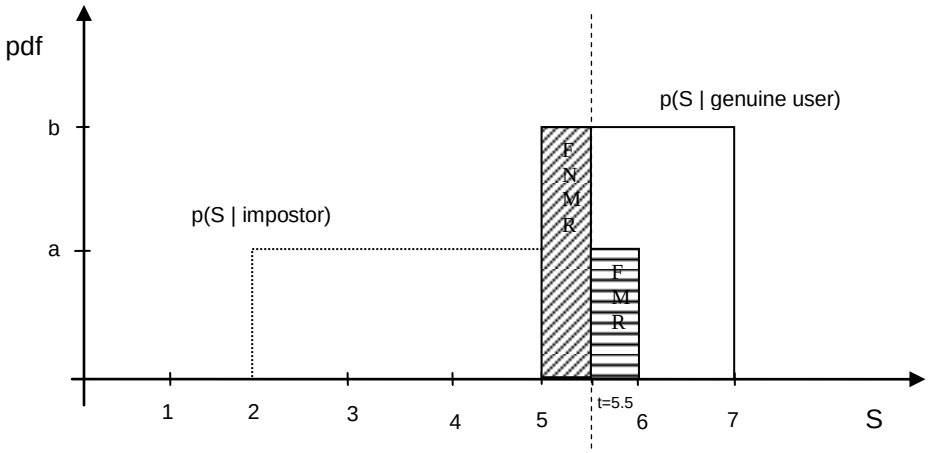
a) For a threshold of *t*= 5.5, what are the parameters FAR (FMR) and FRR (FNMR)?

Knowing that probabilities always need to add up to 1, i.e. the area under a probability density function must be equal to 1, we can find *a* and *b*.
a*4=1 → a=0.25
b*2=1 → b=0.5

The parameter FMR is equal to the probability that an impostor gets accepted, which is the same the probability of p(S | impostor) > t. (See illustration below.)

We have to calculate the area under the curve p(S | impostor) for S > t.
Therefore we have FMR = 0.5 * a = 0.5 * 0.25 = 0.125 = 12.5%

The parameter FNMR is equal to the probability that a genuine user is rejected. This is the same as saying the probability p(S | genuine user) < t.
Therefore we have FNMR = 0.5 * b = 0.5 * 0.5 = 0.25 = 25%



b) You are asked to adjust the system so that FNMR=2.5%. Where do you need to set the threshold *t* to achieve this? What is the resulting FMR?

FNMR is the area under the curve p(S | genuine user) for S < t. The width of the FNMR rectangle is t-5 (for t>=5) and its height is b=0.5. The area, i.e. FNMR is therefore (t-5)*b = (t-5)*0.5
FNMR needs to be 2.5%, so we can solve the equation for t.
(t-5)*0.5=2.5% = 0.025
→ t = 5.05

The resulting FMR for this value of t is the area under the curve p(S| impostor) for 5.05 < t < 6.
Therefore we have: FMR = 0.95*a = 0.95 * 0.25 = 0.2375 = 23.75%

c) What is the Equal Error Rate (or Crossover Error Rate or crossover accuracy) of the system?

The Equal Error Rate is the error rate for which FNMR = FMR.
FNMR = (t-5)*b = (t-5) * 0.5 (for 5<t<6)
FMR = (6-t)*a = (6-t) * 0.25 (for 5<t<6)
Since FMR=FNMR, we have:
(t-5) * 0.5 = (6-t) * 0.25
Solving for t gives t = 5 1/3

Therefore, FNMR=FMR=(t-5)*0.5=1/6 ≈16.7%

Q6) Consider a computer system with three users: Alice, Bob and Charlie. Alice owns the file *alice.sh* and Bob and Charlie can read it. Charlie can read and write the file *bob.sh* which Bob owns, but Alice can only read it. Only Charlie can read and write the file *charlie.sh*, which he owns. Assume that the owner (and only the owner) of a file can execute it. None of the three mentioned permissions implies any of the others. For example, execute access does not imply read access.

a) Given the above information, create the corresponding Access Control Matrix

	alice.sh	**bob.sh**	**charlie.sh**
Alice	{execute}	{read}	-
Bob	{read}	{execute}	-
Charlie	{read}	{read,write}	{execute,read, write}

b) Charlie gives Alice permission to read *charlie.sh* and Alice removes Bob's ability to read *alice.sh*. Charlie has gained superuser power and has now unrestricted access to all files. Show the new Access Control Matrix.

	alice.sh	**bob.sh**	**charlie.sh**
Alice	{execute}	{read}	{read}
Bob	{}	{execute}	-
Charlie	{read, write, execute}	{read, write, execute}	{read,write, execute}