

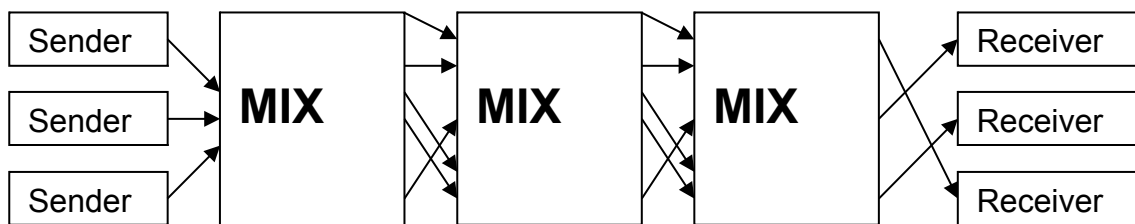
Examples of exam questions connected to the lecture on privacy

N.B. Sometimes Albin Zuccato is a guest lecturer on the subject of privacy. The nature of the lecture (and therefore the nature of exam questions) has been different over the years depending of whether Albin or Alan has presented the subject matter,

2008-10-22

Problem 4

The diagram below is illustrates the basic architecture of a privacy enhanced email system. Explain why it is an advantage to have a sequence of several mix nodes between sender and receiver. Explain furthermore how cryptography can improve the anonymity service.



2009-10-20

Problem 5

In practice an individual's need for privacy can be

- Culturally dependent
- Situation/Scope dependent
- Time dependent

Describe example situations that clearly illustrate how the need for privacy can vary according to these factors.

2010-10-22

Problem 5

There exists legislation (both Swedish laws and European directives) that uphold the privacy rights of individuals. Describe an example of a realistic situation where computer users might either regularly transgress against such legislation, or suffer the consequences of others who transgress against them. Indicate the essence of the legislation that is being transgressed (i.e., even though you may not know the name or designation of a law you should be able to characterise it).

2011-10-25

Problem 4

Describe each of the following IT security related terms. Also, for each of these terms further illustrate the concept by choosing a closely connected IT security concept and explaining the relationship between the concepts. Furthermore, give an example of an application of these tools/threats/concepts. Give concrete examples wherever possible. Structure each of your answers with headings *description*, *relationship to [your chosen related concept]*, and *example*.

Some students may find it helpful to use the pre-printed problem 4 answer sheet for their answer. Those who choose not to should take care to follow the above instructions extra carefully.

Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem

- Personal Firewall
- Public Key
- Prevention (as from the perspective of the basic goals of security)
- **P3P (Platform for Privacy Preferences Protocol)**

2011-12-19

Problem 4

Describe each of the following IT security related terms. Also, for each of these terms further illustrate the concept by choosing a closely connected IT security concept and explaining the relationship between the concepts. Furthermore, give an example of an application of these tools/threats/concepts. Give concrete examples wherever possible. Structure each of your answers with headings *description*, *relationship to [your chosen related concept]*, and *example*.

Some students may find it helpful to use the pre-printed problem 4 answer sheet for their answer. Those who choose not to should take care to follow the above instructions extra carefully.

Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem

- RSA
- **Spacial privacy**
- ACL (Access Control List)
- Integrity policy

2012-10-31

Problem 5

Though IT technology in general has introduced many threats to personal privacy, tools can and have been developed that enhance our ability to control what information about us is spread to others.

a) Describe in general terms what *remailers* do to enhance privacy, and explain why such services can

be assumed to be both good and bad for society.

b) Cryptography is an important element in remailers where a high level of privacy protection is necessary. Explain why and how.

2013-08-12

Problem 5

It is increasingly common these days for web-based service providers to request users to create an account with their organisation in order for users to gain full access to such web sites' functionality. IMDB, Google maps, YouTube are just some examples where creating an account and then authenticating your identity when accessing allows the sites to recall your previous configuration options and your previous interactions with that site. From the customer perspective this allows for a richer user experience than when visiting the same sites anonymously. Some sites even have agreements with such actors as Facebook and Google which allow you to use their authentication schemes, so you do not need to create a new account, but you just connect such accounts to your new service. In this way you do not only avoid having to create a new account (presumably with new password) but you can have increased functionality, such as automatically propagating information on what music you are listening to via Spotify to your "timeline" in Facebook in case it is of any interest for your "friends" in that system.

According to the subject matter covered on this course, discuss what are the principle security issues that might be considered a threat when using the functionality described above.

Discuss also what security mechanisms one might hope would alleviate such general threats as these, and comment on their presumed effectiveness when applied to this more specific scenario described above.