



BOND UNIVERSITY

2010 May Semester

Mid-Semester Examination

INFT13-347, INFT73-347

System Security

Time: 1 Hour
Date of Examination: Wednesday, 7th July, 2010

SID:

Instructions to the Candidate:

1. **Please ensure that your student id number is filled in on this cover!**
2. Answer all questions in this booklet in the spaces provided.
3. You may use any course material, a dictionary and a calculator.
4. For multiple-choice questions any number of correct answers is possible (zero, 1, ..., all). Negative marking applies.
5. For text questions answer the question in a few sentences.

Question 1

(15%)

Tick the correct statements about PGP/GPG:

- It is infeasible to compute the private key if one has only the public key.
- Ownertrust in a key requires validity of the key itself.
- Validity of a key requires ownertrust in the key itself.
- Publishing a key revocation certificate guarantees that that key is no longer used.
- To verify signatures the signer's private key is required.

Question 2

(10%)

Briefly describe the differences between the classic Unix permission model and POSIX ACLs.

Question 3

(12%)

Under what circumstances is XOR-encryption (= bit-wise XOR of message and key) absolutely uncrackable and why? Give a brief explanation.

Why is this guaranteed secrecy of little practical relevance?

Question 4

(12%)

Tick all correct statements about disk/volume encryption:

- Watermarking attacks affect some block cipher modes when applied to disk encryption.
- Disk encryption is performed on each disk block (512 bytes) separately.
- For each disk block a separate key is required.
- Disk encryption hides the existence of files.
- Disk encryption hides the content of files.
- Disk encryption protects the integrity of files.

Question 5

(15%)

Tick all correct statements about authentication methods:

- Two-factor authentication always involves one-time passwords.
- Dictionary attacks affect all authentication methods.
- All One-time password schemes require time synchronization between client and server computers.
- Challenge-response schemes (except public key crypto and S/Key) are susceptible to server database disclosure.
- Two-factor authentication means having two separate passwords.

Question 6

(12%)

Assuming there is already a corporate firewall shielding your organization, why does it still make sense to have a firewall filter active on an individual server? Which security principle does this relate to?

Question 7

(12%)

Tick all correct statements about hardening a computer system:

- Hardening involves minimizing the installed or active software.
- The purpose of hardening is to improve efficiency of the computer.
- Hardening reduces the chance of a successful attack.
- Only a system that doesn't provide any network services can be considered hardened.

Question 8

(12%)

Describe three situations where the security of your computer system relies heavily on trust in something.

Is trust an inherent aspect of computer security (in other words: can there be computer security without trust)? Briefly justify your answer.

End of Paper.