Imperial College London
Department of Computing

Network Security (430)
Tutorial 1
Exercises for the *Introduction*

Discuss your ideas/solutions with the tutorial helpers.

1. Give 10 or more examples of assets that an organisation may wish to protect. Include both tangible assets (easy to measure/quantify) and intangible assets (harder to quantify).

2. Give 10 or more examples of threats to the assets identified in question 1. What do you think is the biggest threat?

3. Give 10 or more examples of countermeasures that could be adopted to protect against the threats identified in question 2.

4. Give some examples of what an adversary could do to messages passed between two parties communicating over an insecure channel?

5. What measures can be taken to prevent or detect eavesdropping?

6. The following are additional security functions that are needed in some circumstances. Try to work out what they might provide. *Signatures*, *witnessing*, *timestamping*, *receipt*, *anonymity*, *certification*, *revocation*, *ownership*.

7. What techniques might be used to detect degradation in availability?

8. Attempt a ranking of confidentiality, authentication, integrity, and availability in order of importance for each of the following organisations: (i) a *bank*, (ii) the *military*, (iii) a *university*. Give reasons for your rankings.

9. If you received a letter in the mail, how would assure yourself that the letter was authentic? Imagine the letter was from (i) your mother, (ii) your bank, (iii) the lottery office. What if the communication was by phone? What techniques could you employ to fabricate a letter or perform a phone call masquerade?

10. If you were the head of security at Amazon.com and were told that Amazon.com's home page had suddenly changed to that of a porn site, what would you do in the next 24+ hours to handle the situation?

Imperial College of Science, Technology and Medicine
Department of Computing

Network Security (430)

Notes on Solutions – *Introduction*

1. Assets. Possibilities include (in no particular order): Data including archives. Computers, disks, tapes. Communications kit: routers, switches, modems, patch panels, phones, faxes. Air-conditioning systems. Alarm systems., network bandwidth. Manuals. Printouts: reports, letters, emails, contracts. Configuration information, personal data, medical data, passwords. money, CPU time, file space, access to services. Intellectual property. Reputation. Public Image. Staff morale. Anonymity. Safety and health of staff, privacy of users, customer/client goodwill, share price, domain name.

2. Threats. Possibilities include: Unreliable software, software bugs. Malicious software: viruses, worms, bombs, trojan horses, password crackers. Cryptanalysis. Microsoft. Open Source. Pirating. Reverse engineering. Disgruntled, blackmailed, bribed employees or ex-employees. Hackers. Government agencies, military and industrial spies, criminals, terrorists. ISPs. Backbone providers. Illness, flu-epidemics, death, strikes, resignations, badly-trained staff. Loss of phone/network service. Loss of utilities (water, electricity), garbage disposal. Lightning, flood, fire, bombs, ransom demands, vendor bankruptcy. Economic downturn. Bad press. Fringe groups. Legal action. Faulty computers/equipment. Bad practice, misconfiguration. Misuse of resources
Biggest threat? One survey of security incidents found the following: 55% due to human error, 10% due to disgruntled employees, 10% to dishonest employees.

3. Countermeasures. Protect buildings, equipment and people from unauthorised access and natural disasters. Use fibre optic cabling. Shield equipment & cabling. Use reliable H/W & S/W, Shredder. Keep backups & standby systems. Define and enforce security policies, disaster recovery procedures. Use "good" cryptography. Dongles. Use firewalls, simulated attacks. CERT. Use good password admin, virus checkers, intrusion detection s/w, auditing software, biometrics. Isolate network. Increased bandwidth. Counter-intelligence, Ethical hackers, Security guards, Good Lawyers. Patents, copyrights, contracts. Employ trustworthy staff, background checks. Train/educate staff. Keep staff happy (good food, computers, gym, pool). Insure. Take security seriously (planning, administration, risk assessment, cost/benefit analysis, paranoia level). Splendid Isolation.

4. Read, modify, delete, delay, replay, redirect messages. How might such actions be usefully used by an adversary? Ideally we would like to prevent such actions otherwise to detect them if they do occur.

5. Encryption. For traffic analysis: padding messages, inject spurious messages, selective routing of messages. Covert channel analysis. Fibre-optic cabling, Quantum communication.

6. Signatures - Bind info to an entity. Witnessing - verify creation or existence of info by an entity, Timestamping - record the time of creation, update etc. Receipt - acknowledge that info has been received. Anonymity - conceal id of sender/receiver. Certification - endorsement of info by a trusted entity. Revocation - retraction of certification or authorisation. Ownership - provide entity with legitimate right to use or transfer.
Note: techniques are available to implement each of these functions securely using cryptography.

7 Measure CPU load, transmission rates. Request-reply times. Compare with thresholds. etc..

8. Note: there is no correct answer. For example, a case for each of the following could be made.
In banking one might normally consider Integrity and Authenticity as more important than Confidentiality and Availability. The military would probably consider Confidentiality as paramount with Availability as the least important function. A university would probably consider Integrity and Availability as the more important functions. Many would say all are equally important.

9. Possibilities include: Mother: context, personal details, handwriting recognition. Bank: Letter head, correct bank account details. Lottery Office: No idea. By phone: voice recognition, convincing banter (dangerous though).

10. The list of things to do is endless. It is important to recognise that such attacks can and do happen and ideally we should have pre-thought out some contingency measures. Overall one needs to identify what happened? When? Who did it (not often possible)? How they did it? Why they might have done it? Consult/report to superiors/colleagues/authorities. Close off internet. Shutdown systems (can be dangerous though if extent of attack is not determined). Ensure attack cannot happen again. Recover (possibly with degraded functionality).