

Assignment 2

Security Policy

Value: 20%

Due: 29-10-2003

Consider an organisation that is the investment arm of a bank. The organisation handles various forms of investments for its customers. For simplicity, assume that the all customers of the organisation are also customers of the bank.

The organisation (for simplicity) offers two types of product:

- Fixed term cash investments

- Mixed fund management (shares, real estate, cash, etc)

It has six divisions

- Sales

- Shares

- Real Estate

- Cash management

- Accounting

- Technical Support

Sales personnel are stationed in the branches of the bank. They have their own terminals in the branch, which connect both to the customer account systems of the bank and to the customer accounts of the organisation (so customer information can be recovered easily). All other divisions are centrally located. Each terminal in the central location is allocated to one of the four divisions. Only managers have their own private terminals, all others are open to use by any member of the appropriate division (tech support staff can access any terminal, although only tech support managers are allowed access to the terminals of managers of the other divisions). The terminals of each division are arranged in a LAN, and all five LANs are connected. There is network infrastructure, file servers, etc to support these LANs.

Sales staff are allowed access to the balance (only) of bank accounts and investment accounts of customers. They are also allowed to change the investment arrangements of customers, on the authority of the customer.

Accounting staff are responsible for transferring funds to the other divisions for investment and for distributing the results of investments to customer accounts. Accounts are also the only staff that can make debits from customer bank accounts (to add to investment accounts) or credits to customer bank accounts (to distribute earnings).

The cash, real estate and shares divisions all manage a number of holdings. They are entirely unaware of customer details, simply receiving money from accounts to invest and returning earnings.

The above does not give a full definition of such an organisation. When (not if) you get to a point where you have to make decisions about information not covered above you have two choices. You may either contact me (probably best by e-mail) to ask or you can decide for yourself. If you take the later option you **must** document your choice fully (so I know what it is you are writing policies about).

You are to define security policies for the organisation. Your entire submission should be no more than 12 pages in length and no less than 6. Obviously this is not enough room to write a complete security policy for the organisation. Part of your mark will be awarded on the basis of how well you choose example policies to define. Make sure that those policies which you do define are complete, in terms of their scope, meaning and the results of transgressions (see the lecture notes for details). You also need to include an implementation plan for your complete security policy proposal

You must include policies covering the following:

- The access to customer information
- The transfer of customer funds between the divisions
- The access of the technical staff to equipment and information

You will need to cover other areas as well in your sample policies, but that selection is up to you. Note that there is a marking scheme on the course website. You would be well advised to consult this in preparing your submission.

You are to submit a hardcopy of your assignment in the lecture in week 13.

Michael Hitchens

September 2003

Assignment 2

Public Key Infrastructure

Value: 20%

Due: 29-10-2003

You are to write a **simple** chat program, supported by a public key infrastructure and associated components.

The chat program must allow users to:

- Login, using a username and password
- Determine which other users are currently logged in
- Set up a chat session with a user who is not currently in one
- Send messages within a session
- End a session
- Log out

DO NOT make the interface to the chat program a GUI. It makes it too hard for us to mark. This is not an interface course. Instead, make it all text based.

Implementing the underlying public key infrastructure will require you to:

- Design a certificate structure (possibly derived from an existing definition)
- Design and implement a certificate authority which can issue such certificates
- Protect the certificate authority (probably via password)
- Determine some way of securely creating, storing and accessing the key pairs for principals
- Handle certificate distribution, certificate revocation and the public key of the CA(s).
- Implement and properly document an authentication protocol between principals based on the information held in the certificates
- Allow principals to securely agree on a symmetric session key

The above requirements for the PKI will require you to provide another interface, separate from the chat facility. This second, PKI management interface, will enable the issuing and revoking of certificates, addition and removal of users, replacement of keys, etc.

Note that the authentication and selection of a session key should be done for each session, but should be invisible to the users. The chat sessions within the chat program should be encrypted using the session key.

You are to write this in one of C, C++ and Java. As noted above your submission should employ text-based interfaces, not GUIs.

On the course website you will find a marking guide for this assignment. You are to provide a written report that *clearly* specifies which portion(s) of your code are responsible for each points of interest I have identified. Be precise. We will use your report to locate the pieces of code we wish to examine. If your report is unclear we may decide that it is too hard and that the code does not exist (which would mean zero marks for you for the code relating to that point).

You are to hand in both printed and electronic versions. Both are to include all source code you write, compilation instructions and your documentation. The printed version should also include a few sample runs and is to be handed to me in the last lecture. The electronic version should be submitted, no later than the above date, as a **single** zip or tar file e-mailed to michaelh@ics.mq.edu.au. We will only be looking at the electronic version if we wish to check something in the code. If we do not receive a printed version we will not be looking at the electronic version (ie, not submitting the printed version counts as not submitting the assignment).

Michael Hitchens

September 2003

School of Information Technologies
COMP4307/5327 Computer Security
General Assignment Information

Assignment 1 Due Week 7

Assignment 2 Due Week 13

Each assignment comes in two forms – essentially programming and non-programming.

Who does which assignment?

You get to choose.

However, I would strongly suggest you **not** choose the first non-programming and second programming assignment.

Assumed knowledge

Programming

- An undergraduate degree in computing
- The knowledge of how to write code to send messages between two machines on a network

Non-Programming

- A lay person's understanding of the internet and networks

Assessment

On the website you will find a marking outline for each assignment as it is set. It would be wise to consult the marking outline in the preparation of your submission.