

Assignment 1

Security Products

Value: 20%

Due: At the end of the lecture 10th September 2003 (week 7)

There are many security products available. It is important to be able to select the correct product for your organisation's needs.

Imagine that you work for an organisation and your boss knows that you have done a computer security course. Your boss wants to buy a computer security product and wants you to recommend one. To make it a little easier I'm letting you choose the type of product (you wouldn't get that in the real world).

You are to

- Select a type of computer security product. The following are suggestions. You are free to choose an area not on the list but if you wish to choose another type, check with me first
 - Password security
 - Intrusion detection
 - VPN security
 - Firewalls
 - Digital Certificates
 - Digital Signatures
- Locate information on two products that provide a security service for your chosen area.
- Describe the two products chosen
- Compare and contrast them and come to some conclusions about which may be superior (perhaps one will be superior in some circumstances and the other in other circumstances).

Your entire submission should be no more than 8 pages in length and no less than 4. Be careful in your assessment of the two products. While all you will normally have to base your assessment on is the manufacturer's material, remember that this will be designed to present the product in the best possible light. Do not be taken in.

Michael Hitchens

August 2003

Assignment 1

Cryptography Products

Value: 20%

Due: At the end of the lecture 10th September 2003 (week 7)

Imagine that you work for an organisation and your boss knows that you have done a computer security course. Your boss wants the organisation to acquire a cryptographic library for its programming and wants you to select and evaluate one. To make it a little easier I'm letting you choose the programming language (you wouldn't get that in the real world), although it must be one of Python, Java, C, or C++.

Part 1

See if the system (whichever one you use) already has a cryptographic library for your language of choice. If it does not, locate one (probably from the web) and either install it your self or get the system administrators to install it for you.

Part 2

You are to write two pieces of code. They are to run on two separate machines. The first piece of code takes a string, typed in by the user, encrypts it using DES and sends the ciphertext to the second piece of code. The second piece of code decrypts the string and prints the plain text to the screen.

The two pieces of code can know the key in any way you choose. You could

- Hard code it into them
- Type it in when they each start running
- Have it stored in a file
- Etc.

Part 3

You are to write two pieces of code. They are to run on two separate machines. The first piece of code takes a string, typed in by the user, encrypts it using RSA (or some other asymmetric key algorithm) and sends the ciphertext to the second piece of code. The second piece of code decrypts the string and prints the plain text to the screen.

The two pieces of code can know the keys in any way you choose. They could be

- Hard coded into them
- Typed in when the programs each start running
- Stored in a file
- Etc.

Part 4 Report

For each of parts 2 and 3 you should hand in print outs of the two source files, information allowing me to compile them if necessary, accompanying documentation and sample runs.

You must also hand in a two page report which details

- How you found the library (it is acceptable to say that you found out about it from someone else doing the course)
- Your evaluation of the library:
 - how good is its documentation
 - how easy is it to program with
 - does it just implement the algorithms or does it offer other facilities, such as CBC, OFB, MIC, hashing, digital signatures, multiple algorithms, etc
 - any other observations

Michael Hitchens

August 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.