Chapter 1

Introduction

The importance of multimedia cannot be understated. Multimedia is considered to be a valuable form of communication, and its uses range from design, research, training, and education to the arts, entertainment, and visualisation. If used correctly, it helps to present information in a manner that is more understandable. For example, a pie chart of a company's success by department is usually easier to interpret than an equivalent set of statistics in number form. Multimedia has changed from its traditional form (paper, photograph, audio/video cassette, etc.) to an equivalent digital form in order to suit the needs of today's digital world. The three main types of multimedia are images, audio, and video; together these represent the audio and/or visual components of a multimedia presentation. A modern-day personal computer can normally be used to control the order in which these various components are combined and presented. A combination of these types of multimedia (called *hypermedia*) is often put together to enhance the desired message of the multimedia data.

Multimedia data must often be made public; the fact that multimedia data is in a digital form helps to increase its availability. This is because the data in this form can usually be easily duplicated, and can be accessed by many entities (even though the data itself may remain centralised). The security of all data in digital form has however been a concern, especially recently due to the exponential growth of public networks such as the Internet, and the increased sensitivity of the data made available (whether intentional or unintentional) through these networks. Information security has grown into a broad field, since the legitimacy of the actions taken upon this valuable asset should be ensured for *any* given computer system. The main information security services defined are identification and authentication, authorisation, confidentiality, integrity, non-denial, and availability. Although they are not always all essential, these services should be properly implemented, if they are required, to minimise the threat of an attack occurring on the data which is handled by that computer system, and to ensure that only authorised entities gain access to that data.

1.1 Problem statement

Although information security has received more attention recently, the underlying principles of its services were developed during the computer-based file systems era. These information security services were mainly aimed at ensuring the security of an entire data file as a single structure; only certain specialised systems restricted access to parts of a file depending on the security classification of the user making the request. The advent of the database has helped out with

this potential problem by allowing certain restrictions to be made on only specified structures within the database. The information stored within defined structures (such as a table within the relational database management system) can therefore be limited depending on who or what is requesting the data from the database.

Ensuring that proper security measures are taken for only parts of files, or based on the content of a particular file, may not have been an issue in the past for most computer systems. Certain types of electronic documents may still only need access to be restricted for the whole document. The requirements for multimedia data files (in particular) are different however; these files are often large and may not always need to be transmitted to a requesting entity in their entirety. The security of these file segments will most likely still be very important. Further, it may be the case that the actual “message” must be interpreted differently for each entity that makes a request for that multimedia data file. All the required changes must therefore be made to the relevant information security services in order to allow only parts of multimedia files to be classified if necessary.

The information security service of identification and authentication does not need to be changed since the process is the same whether the entire file is requested, or only a part of it. The authorisation information security service will be mostly affected because it is this service that has the vital responsibility of deciding what data a particular entity is allowed to access. As an example, a crime investigation department may be required to publicise (electronically) all photographs of crime scenes that took place within that city. The department may however prevent certain parts of these images from being included in the publicised image depending on who or what is requesting it, especially if the case is still in progress. An authorised entity must therefore be able to select parts of the image and classify them according to some prescribed security classification system (e.g. according to rank, or else public if not specified). Logical access control should therefore be ensured at *the content level* for multimedia data, allowing for a more dynamic security system. The other information security services may also need to be slightly modified to handle this, but the main changes that would need to be made would be for the authorisation information security service.

A large amount of research has gone into ensuring that unauthorised copying of a multimedia file that has a watermark embedded within it can be traced back to the original perpetrator, and if necessary the watermark can act as evidence in a court of law. Other areas of multimedia security have been researched, although this research is usually specific to the needs of a particular computer system and does not have a theoretical foundation that can be used for other systems in general.

Very little research has gone into ensuring logical access control at the content level for multimedia data. This dissertation will present a number of models that can be used to provide logical access control for images, digital video files, and digital audio files at the content level. The different models presented allow a more dynamic solution, since all of these models have their advantages and disadvantages. The best model can therefore be chosen depending on the needs of the particular computer system or application that needs to implement it. The models may even be combined in order to allow more choice depending on the particular multimedia file that is requested.

All of the secure multimedia database models that will be presented conform to a basic model structure. The actual multimedia data is securely stored in a repository (e.g. a file server). Security information associated with each image, audio file, or video file that includes the authorisation information is securely recorded in a database. The multimedia data can then be assembled, using the associated security information, according to the requesting entity's security classification. The process is divided into three phases for all of the secure multimedia database models presented. In the first phase, the security objects are created and associated with the multimedia data by an authorised entity. In the next phase, the collected security information is recorded and the multimedia data is securely stored. The aim for the third phase is to ensure that only the authorised parts of the requested multimedia data are sent to a requesting entity. A secure interface is used to allow an authorised entity to create the objects. Another secure interface is also used to make requests for multimedia data.

A prototype has been developed for one of the secure image database models that will be presented in this dissertation. The prototype will be used to provide some realistic examples of how the secure image database model can be used to ensure logical access control for images at the content level. The prototype will also be used to illustrate some potential problems that may occur for certain implementations. In addition, the prototype will provide important information regarding the issue of suspicion, which involves hiding the fact that the original multimedia data was modified, if this is necessary. The requesting entity should therefore not suspect that any changes were made (if possible), or at least the potential level of suspicion should be minimised.

Secure multimedia database models for the three main types of multimedia will be presented. Firstly, although these models can be combined to cater for requests made on all three of these types separately, this dissertation does not discuss logical access control for hypermedia or compound multimedia (e.g. HTML files).

Secondly, although text may be considered a form of multimedia, the main focus in this dissertation will be on images, video, and audio. The same basic model structure can however be used to ensure logical access control for text files at the content level (the difference is in the internal details of the model components).

1.2 How this dissertation is organised

The following chapters form the content of this dissertation:
Chapter 2 is an introduction to information security, and concentrates on the six information security services and the techniques used to implement them.
Chapter 3 provides a discussion on the different types of database systems that have been developed, starting with the history of computer-based file systems.
Chapter 4 discusses some important multimedia concepts that will be used in the explanation of the secure multimedia database models.
In chapter 5, previous work concerning multimedia security will be discussed, including an introduction to watermarks, the current main research focus within the multimedia security domain.
Chapter 6 presents a model for the development of a secure image database. A prototype based on this model will also be discussed, as well as a variation of the secure image database model.
Chapter 7 discusses some important issues regarding the secure image database model, including the potentially important issue of suspicion.
Chapter 8 presents a number of models and approaches that can be used for the development of a secure video database. Certain issues concerning this model such as suspicion will be examined at the end of this chapter.
Chapter 9 presents a number of secure audio database models. Certain issues regarding this model will also be examined at the end of this chapter.
Chapter 10 provides the conclusion to this dissertation, including possible future research work regarding secure multimedia databases.