# Coimbra: Secure Web Access to Multimedia Content

Edgar Weippl
Software Competence Center Hagenberg
A-4232 Hagenberg
+43 7236 3343 - 837
edgar.weippl@scch.at

## ABSTRACT
In this paper, we describe various concepts how Web content can be published in a way so that copies cannot be illegally distributed. The required access control mechanisms are implemented using well-known cryptographic algorithms. A modified Web browser decrypts the content on-the-fly so that it is impossible for unauthorized users to copy and distribute the presented multimedia content.

## Keywords
Confidentiality, Discretionary Access Control, Security Model, Encryption

## 1. INTRODUCTION
Multimedia is today's buzzword when talking about Web content. The newest desktop computers now offer a performance unmatched even by workstations a couple of years ago. As a consequence both individuals and companies invest a lot of time and money into the development of multimedia content. Graphics, animation sequences and music are widely used on homepages of companies but also to convey information effectively e.g. in multimedia encyclopedias.

Due to the high cost of creating, distributing and updating Web-based multimedia content, security is a major issue. There are two aspects of security that we have focused on in this paper: confidentiality and some aspects of integrity. Confidentiality means that data objects are only accessible by authorized users, whereas integrity ensures that only authorized users modify content. A third aspect of security, we do not deal with, is availability, e.g. preventing denial-of-service attacks.


ACM Multimedia Workshop Marina Del Rey CA USA


## 2. RELATED WORK
Access Control for file systems and databases is probably one of the best-researched areas in computer science. In the 70s and 80s various security models have been developed to guarantee confidentiality and availability.

The Bell – La Padula model [1] [2] is the most famous security model. It considers the flow of information when a subject, e.g. user, observes or modifies an object, i.e. data. Basically, it prohibits users reading data that is classified at a higher security level ('clearance' in military terms) than they are and prevents them from writing data to security levels lower than those read from. These properties are also referred to as 'no read-up' and 'no write-down'.

The Bell – La Padula model is based on discretionary access control (DAC). This means that access control is at the discretion of the object's owner. On the contrary, mandatory access control (MAC) implies that access rights are assigned centrally [4].

The Biba model [3] can – at least to some extent – be considered to be the inverse of the Bell – La Padula model. It is mainly focused on guaranteeing integrity, i.e. to prohibit unauthorized modification of data.

Apart from using general computer security models restricting access and distribution of multimedia content, digital watermarking is an important approach to protect this kind of data. Yeung [11] gives an overview over existing techniques. However, even if perfect watermarking techniques existed, content could still be copied illegally causing considerable losses. MP3 copies of music distributed via Napster or Gnutella are a good example. In most cases, there is no doubt who holds the copyright of the songs but still thousands of copies are being distributed illegally.

Landwehr [5] present a comprehensive taxonomy of computer security issues. It provides a good introduction to the characteristics of security flaws and how they can arise.

# 3. COIMBRA

Coimbra was originally developed to allow university professors to securely distribute multimedia content for Web-based training courses. However, we soon realized that our technology could also be used in various other fields of application, e.g. multimedia encyclopedias or distributed authoring systems.

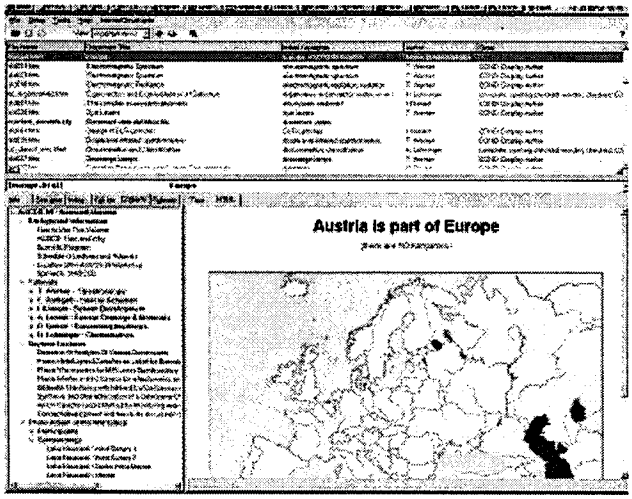


**Figure 1: Coimbra_admin is used to manage files on the Coimbra Server. The upper pane contains a directory listing with meta information on the files, the lower left pane shows a structured table of content and on the right a preview window displays the file.**

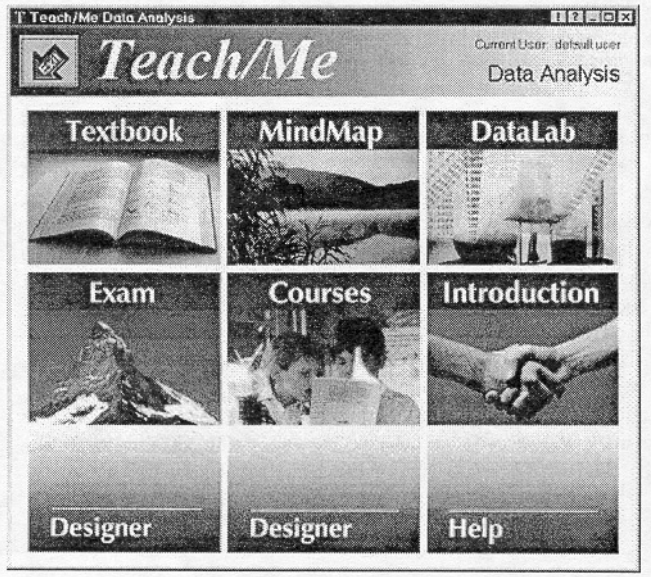


**Figure 2: This Figure shows the client browser displaying the main menu (an image map) of a WBT course.**

## 3.1 General Architecture

Unlike most other systems that publish Web content, Coimbra requires a special client, i.e. a slightly modified standard Web browser. Before being able to access multimedia content that has been published with Coimbra, users have to download the client software.

The content is stored on a Web server that supports both the HTTP and the FTP protocol. We strongly agree with Wilkinson [10]: "If sensitive information is to be included in a shared web, access controls will be required. However, the complex software needed to provide a web service is prone to failure. To provide access control without relying on such software, encryption can be used."

## 3.2 Encryption

Although the Coimbra system was never designed for high-security requirements, we still wanted to provide reasonable security. The first version of Coimbra compressed the files using the Zip algorithm with long passwords. Optionally the file could then be encrypted additionally by a fixed symmetric key using the simple XOR operation.

We always knew that the Zip encryption was not strong but we underestimated the resources that people are willing to invest to steal content. Within one month after starting the Beta tests, we noticed that the encryption had been broken. Therefore, we decided to use the Blowfish algorithm.

Blowfish is a symmetric block cipher that can be used as a replacement for DES (Data Encryption Standard). It was invented by Bruce Schneier [7],[8] in 1993 and is a freely available encryption algorithm. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. The Blowfish algorithm is has not been patented and can be used without license fees.

As the client software uses an open multilevel architecture, the files can be encrypted using a different algorithm instead of Blowfish, too. A promising approach is to use PGP as an additional layer. PGP implements asymmetric public key cryptography and is freely available at www.pgpi.com. Still, we need to add some additional logic to transparently manage the public and group keys required for public key cryptography.

## 3.3 Client Architecture

As shown in Figure 3 the client stores a downloaded file on the local disk. Copying this encrypted file to another system is possible but even with the same viewer the content can only be viewed after successfully connecting to the Coimbra server and entering login and password. Logging account accesses and IP addresses at the Coimbra server allows system administrators to easily detect multiple logins using a single account, i.e. the attempt to access information illegally. Locking this account, further illegal use can easily be prevented.

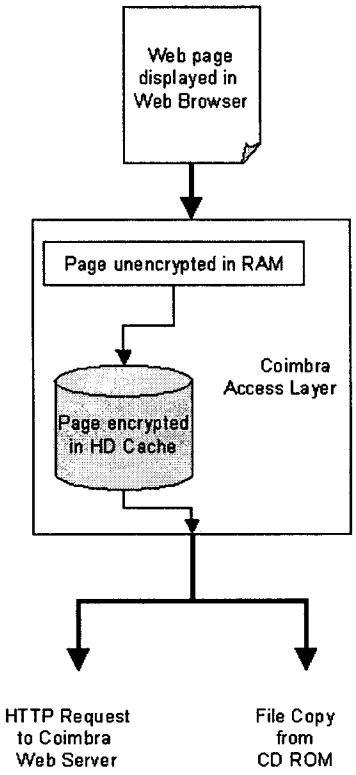


**Figure 3: The modified Web browser at the client side decrypts documents and optionally reroutes HTTP request to a CD ROM-based 'server'.**

If the user has read access to a file, she can view it. Depending on what the owner of the file specified, she might also be permitted to print it, save it or copy its content to the clipboard. We implemented a discretionary access control because managing access rights for every file by its owner is more efficient in distributed computing environments than a rigid mandatory access schema.

Let us now look at an example (see Figure 4). If a user creates a new file, e.g. a HTML page that includes references to graphics and movie files, she normally saves it to her local disk first. When she wants to publish it, our client software (Coimbra_admin) encrypts the file, uploads it via FTP and updates various index files. Optionally, the referenced graphic and movie files are also encrypted and stored on the server (or updated if they already exist).

Later on, other people want to view the newly created HTML page. They use their Coimbra clients to connect to the Web server and access this page. The page is downloaded via HTTP and stored locally in the cache. All files, i.e. HTML files, graphics, movies, etc. are only decrypted for viewing. As the viewer is a slightly modified standard Web browser, the content cannot be saved (as plaintext) unless the authors allowed doing so. Therefore it is very difficult to illegally copy the content of a Coimbra server.

## 3.4 Distribution based on CD ROM and Networked File Systems

Some readers may have already noticed that the only functionality of the Coimbra Web/FTP server was to allow retrieving documents via the HTTP and uploading via the FTP protocol. This is why – with very little additional effort – even a CD ROM can be a 'server'. As shown in Figure 4, the Coimbra Access Layer does not only take care of the encryption but also reroutes a http access to a simple file copy if the server happens to be a CD ROM or a networked file system. Obviously write accesses to a CD ROM fail but for networked file systems, the FTP call is replaced by file copy, too.

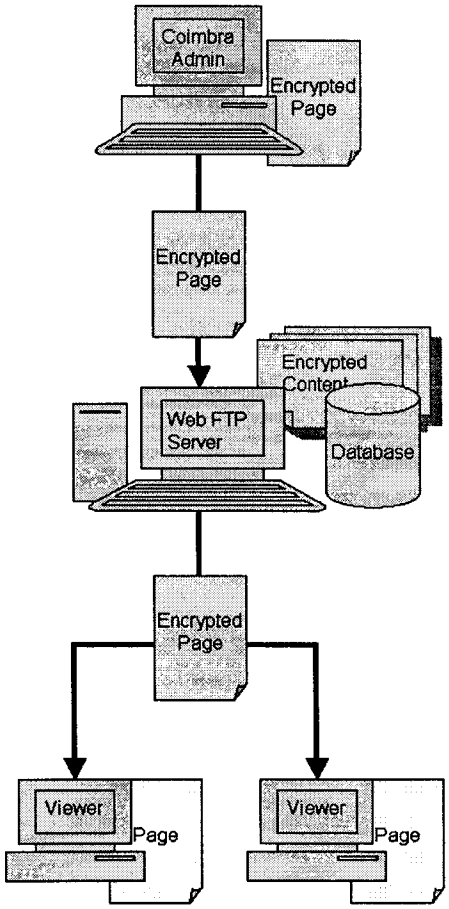


**Figure 4: Coimbra admin is used to administer the files on a Web and FTP server. The clients can connect to this server and download encrypted files that are only decrypted for viewing.**

# 4. SYSTEM ASSESSMENT / CONCLUSION

One of the major weaknesses of the current system is the fact that users need a special client to access Web pages published with Coimbra. This may be unacceptable for many e-commerce applications. However, for Web applications that are used on a

regular basis and that provide a lot of information that should not be copied, Coimbra is ideal.

We currently use the system to offer Web-based training courses and the German version of Teach/Me [7] is also based on this technology. Coimbra implements a security policy that is based on the Bell – La Padula model. Classified information cannot be 'written down', i.e. copied to a disk or to the clipboard without explicit permission. Obviously, information cannot be read without authorization (no read-up), either.

Our approach to secure multimedia content is orthogonal to watermarking techniques in the sense that it will protect all kinds of documents (whether watermarked or not) as long as the owner does not allow users to save them decrypted. In comparison to watermarking, Coimbra also prohibits illegally copying the content.

## 5. OUTLOOK

As mentioned before the most important weakness of Coimbra is that a modified browser is necessary. We currently explore options to integrate the Coimbra access layer in a Java Applet or an ActiveX control so that it can be executed within a standard Web browser environment.

## 6. ACKNOWLEDGEMENTS

Our thanks to Hans Lohninger, professor at the Institute of Analytical Chemistry at the Vienna University of Technology, who manages the project and implemented core layers of Coimbra.

## 7. REFERENCES

[1] Bell, D., and La Padula, L., "Secure Computer System: Unified Exposition and Multics interpretation". Technical Report ESD-TR-75-306, The MITRE Corporation, Bedford, MA, (1975).

[2] Bell, D., and La Padula, L., Mitre Technical Report 2547 (Secure Computer System): Volume II, *Journal of Computer Security*, 4 (2/3), p 239-263, (1996).

[3] Biba, K.J., "Integrity considerations for secure computer systems", Technical Report ESDTR-76-372, ESD,/AFSC, MTR – 3153, the Mitre Corporation, Bedford, MA, April (1997).

[4] Gollmann, D., *Computer Security*. John Wiley & Sons, (1999).

[5] Irvine, C., and Levin, T., "Toward a Taxonomy and Costing Method for Security Services". *Proc. 15th Annual Computer Security Applications Conference.* IEEE Computer Society. (1999).

[6] Landwehr, C.E., Bull, A.R., McDermott, J.P., and Choi, W.S., "A taxonomy of computer program security flaws", *ACM Computing Surveys*, 26. 211-254, (1994).

[7] Lohninger, H., *Teach/Me – Data Analysis*, Springer, (1999).

[8] Schneier, B., "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). Fast Software Encryption", *Cambridge Security Workshop Proceedings '93*. Springer, (1994).

[9] Schneier, B., "The Blowfish Encryption Algorithm – One Year Later", *Dr. Dobbs*, 1995

[10] US Department of Defense, DoD Trusted Computer System Evaluation Criteria (The Orange book). DoD 5200-28STD, (1985).

[11] Wilkinson, T., and Wiseman, D.H.S., "Trustworthy Access Control with Untrustworthy Web Servers". *Proc. 15th Annual Computer Security Applications Conference. ACSAC.* (1999).

[12] Yeung, M.M., "Digital Watermarking: Marking the Valuable while Probing the Invisible", *Communications of the ACM*, 41:31, (1998).