Providing security for eLearning

Frank Graf*

Department Security Technology, A8, Fraunhofer IGD, Institute for Computer Graphics, Fraunhofer Str 5 (Rundeturmstr.6), Darmstadt 64283, Germany

Abstract

This paper discusses the specific security requirements of Internet-based learning (eLearning). Two concrete solutions for improving the degree of security achievable are shown. First, a framework for secure testing is introduced. This framework prevents manipulation from the side of the students during learning thus allowing a reliable control of learning success. Second, solution presented deals with the problem of confidentiality and protection of copyright. By establishing a lifelong control of the copyright owner over his documents it prevents illegitimate access and redistribution.

Keywords: Secure learning; Internet and intranet security; Watermarking; Biometry; Encryption; Intellectual property

1. About eLearning

Although eLearning has gained most of its popularity in the recent years, the idea of using the computer for learning can be traced way back to the early years of computing, especially to the time when ‘Personal Computer’ emerged. Some examples are the work of van Dam [1] and Bork [2].

The emergence of the WWW was an important turning point for eLearning. Seen from a technical perspective, the WWW is merely an open and extensible platform for accessing multimedia material in a network. But its major importance lies in the impact it had on the Internet. Before the emergence of the WWW, the Internet was almost exclusively used by universities and some corporations to exchange data. The WWW brought a new style of working where the location of the data no longer mattered. Further on, it became the driving force for the explosive growth of the Internet and made the WWW and the Internet a part of everyday life for the general public. The new medium WWW was almost immediately adopted for teaching and attracted a considerable amount of research and development activities; ‘virtual university’ became a widely used buzzword. As a matter of fact the WWW has today become the de facto standard platform for eLearning.

As often, security was not an issue in the early development phases of the WWW and was only added on later when it became obvious that for real-life application scenarios, as e.g. for eCommerce and eLearning, security is an essential issue. Due to the close relation to the WWW many of the security problems in eLearning are similar to ones of the general WWW and therefore at least some of the solutions developed there will also apply to eLearning. However, there are certain aspects, which are specific to eLearning.

This paper shows how to solve some of the security problems of eLearning.

2. Why eLearning needs security?

Why security is a crucial issue for eLearning becomes obvious if one looks at the following facts.

2.1. Knowledge becomes an important means of production

The speed of technical development is continuously getting faster. New knowledge emerges and must be
mastered and incorporated in ever shorter periods of time. As a result of this, continuous, lifelong training will become a necessity not only for the success of an individual but also for corporation as a whole. On the conceptual level, this implies that the concept of “learning for life” will be replaced in many areas by “learning on demand”. From a practical point of view, the implications are: Learning must be done more frequently and—since it is becoming more and more part of the normal work—it must be integrated as seamlessly as possible in the working process. Currently, training is often performed in a remote classroom environment, where besides the cost for training there might also be considerable costs for traveling and accommodation. New forms of professional training, like eLearning, where training can be provided at the workplace immediately when the demand arises are needed to meet the future requirements in a time and cost-efficient way.

That knowledge is becoming an important resource for the success of a company is also indicated by the increasing importance of licenses, patents and standards and how they are used to secure market position.

2.2. Knowledge as product

Since knowledge has become a crucial resource for the success of a company, it has also become a product and an object of trade. Therefore there is also a substantial market for eLearning. In a study [3] from May 2000 IDC forecasted a 12% annual growth rate in revenues for IT-based training from $19.4 billion in 1999 to almost $34 billion in 2004. With this amount of money at stake there is definitely also the need to protect the knowledge, especially in the case of eLearning where the learning material, which is the carrier of knowledge, is exposed to the broad public.

2.3. Knowledge as a key for personal success

The most important issue from the security point of view, however, is the fact that knowledge is also the key to personal success. Since there is no instant test to evaluate the knowledge, respectively, the skills of an individual, certificates, as e.g. university diplomas are a cornerstone of user evaluation. Since such certificates are the basis for the decisions over the progress of the student’s professional life, the achievement of such a certificate is of utmost importance for him. Thus a student will do everything he can to obtain a certificate. This includes the various forms of cheating. Therefore learning has a long history of cheating and for the traditional forms of learning there are established ways to prevent cheating. eLearning introduces new ways of learning. The students, however, are still the same, they will cheat if given the opportunity. Since eLearning is still in its early phase of development, mechanisms to prevent cheating have yet to be established.

3. Security issues in eLearning?

3.1. Protection against manipulation

From what has been said above it is obvious that an eLearning system must be secured against manipulation from the side of the students. Protection against manipulation is also an issue in normal WWW and several solutions have been developed for this, e.g. encryption, digital signatures, TSL, firewalls and virtual private networks (VPN). The problem with these solutions is that they are directed against attacks from the outside while the user is being trusted. In eLearning, the users are the students and as said before one cannot trust them. However, this does not imply that the security mechanisms mentioned above are not needed for eLearning. In fact, these mechanisms are still needed to prevent manipulations from a third side but one needs additional mechanisms against manipulation from the side of the legitimate users.

Maleficient users are also a security hazard in normal application scenarios—in fact it is said that around 80% of attacks are done by an insider—but the difference in an eLearning scenario is the quantity. In normal application scenarios it needs some criminal energy and additional effort to gain personal advantages from a manipulation, therefore, the vast majority of the users will stick to the rules. In eLearning users will directly benefit from their manipulations and the results of their learning will be of utmost importance for their future career. Because of this there is a much higher readiness to cheat.

But even if one could be sure that no student had the intention to manipulate the result of the learning one should provide mechanisms to prevent cheating, otherwise students could cheat themselves (e.g. time limits for tests or look up the solution while a test is running) (Fig. 1).

With respect to security the underlying client-server architecture of the WWW is a big asset. Due to this it is possible to isolate the sensitive parts (e.g. test evaluation) of the learning material into entities which are kept on the server. Only learning material without any sensitive information is delivered to the students. During the learning phase this material interacts with the sensitive entities on the server. The advantage of this approach is, that since the server is under the control of the trainings provider he can take all necessary precautions against manipulations. If the students cannot freely access the sensitive entities or not at all this will dramatically reduce the potential for attacks. This approach requires some discipline from the
learning material authors, since they must split up their material into a sensitive and a non-sensitive part and enable them to interact. Currently, JavaScript is commonly used for programming course material including the computation of test results. Although JavaScript gives the author an easy way of programming it is highly insecure since it is interpreted on the client-side.

3.2. User authentication

A reliable identification of the user is an elementary feature for an eLearning system because it is the basis for

Access control. Usually access to the eLearning system is granted only to registered students but even their access might be restricted to a certain subset of the learning material.

Billing. Especially if eLearning is offered on a commercial basis there is a need for remuneration. There are numerous accounting schemes but almost all of them are in some way related to the actions of the individual users.

Maintenance of learning material. Information which students used regarding which material and how well the training worked out, provides the training provider with some insight into what the assets and the deficits of his learning material are and allow him to improve his portfolio.

User profiles. If the learning success of the a user is recorded, this information on his current level of knowledge can be used to optimize a course for his pre-existing knowledge, his preferences and/or his learning goals.

Certification. In case the learning results in some kind of certification (e.g. a diploma), it is essential that the records on which the certificate is based on can, without ambiguity, be attributed to a specific student.

How to handle certification and user profiles in collaborative learning is an interesting topic, which raises new problems. This paper will ignore these problems and focus only on the problems of user authentication in individual learning. Currently, there are three major categories of techniques for user identification.

Passwords are still the standard in user identification. No special hardware is required for their realization. In a networked environment the secure transmission of passwords is a crucial issue.

Smart cards use cryptographic mechanisms, namely public-key encryption, to provide authentication and identification. The security of the smart card does not depend on the computer it is used with, and smart cards can be designed to resist tampering. They provide efficient means of identification and authentication with a two-factor (knowledge and possession) mechanism that also ensures non-repudiation properties. In order to use smart cards, all clients must be equipped with special hardware and there must be the infrastructure to issue the smart cards. Currently, there is no universal standard for smart cards and smart card readers are not standard equipment on today's computers. Therefore smart cards are not a viable alternative for eLearning except in environments placing emphasis on security and being able to pay for this added security.

Biometric Identification has recently gained much attention. Here unique, invariable biological characteristics of a person (fingerprints, voice, face, handwriting, etc.) are used to authenticate a user. The idea behind this is that if the user itself is the key there is no longer the possibility of stealing or duplicating the key. However, binding the authentication to personal characteristics raises concerns about privacy. With regard to standards the situation is even worse as with smart cards. All biometric systems need some hardware to read in the biometrical characteristics. Part of them uses rather
exotic hardware (e.g. finger or iris scanner) while for others more common hardware like microphones or cameras is sufficient. Since microphones and cameras can be used to realize audio/video conferences with other students or a tutor one would prefer such biometric systems for eLearning which require only these. The development in the area of biometric systems is still in an early state. In a study [4] initiated by the Bundes-kriminalamt (BKA, Federal Criminal Investigation Office) and the Bundesamt für Sicherheit in der Informationstechnik (BSI, German Information Security Agency) several of the twelve systems tested showed unsatisfactory recognition rates and almost half of the systems could be duped without much effort.

Even if all these methods would work perfectly there is still a conceptual problem which none of them can overcome. In the best case a training provider can ensure that a certain user has been involved in a particular learning activity. What he cannot ensure is that recorded actions of the user are original to this specific user and he had not used illegitimate resources. In order to guarantee this learning has to be done in an environment, over which the training provider has full administrative control. However, this contradicts the core principles of eLearning (time- and space-independent learning). But traditional learning as well is not done exclusively in environments the teacher has total administrative control over (take for example homework or writing a thesis). As a consequence, there is no absolute security nor will there be such a thing, but over the years procedures have been established which give an adequate amount of security. The same will happen for eLearning. Possible approaches are:

Legal steps. Here the student must submit an affidavit stating that he made no use of illegitimate resources. Any certificate is granted under the condition that this statement is true. Although with this approach cheating cannot be prevented it provides much better leverage for legal actions once illegitimate actions are uncovered. This approach is independent from any technical provision, thus it can and ought to be used in parallel to technical means.

Separation of learning and certification is another well-known approach from traditional learning which can also be adapted to eLearning. Here one distinguishes between a learning and an explicit testing phase. The eLearning system can be used in both phases, but while the learning can be done in a time- and space-independent fashion, the testing is done in a controlled environment. User actions are recorded in both phases, but only the reliable data from the test phase are used for certification. This approach allows a high degree of security, although there are some disadvantages. Testing is additional effort for the student although it ideally should lead to the same results that could be derived from the learning phase. The fact that there is an upper limit for the duration of a test also has consequences. First, the actual performance of the student on the day of testing may not be representative of the student’s capabilities. Then there is also an upper limit to the complexity of the problems that can be used in the test. So only a subset of the entire course content can be tested. Although the tester will try to select a subset which is as representative as possible, there are aspects which cannot be tested in such a setting.

Integrated testing. Instead of distinguishing between learning and testing eLearning could go into the opposite direction. All the information concerning the learning success gathered during the entire learning process is used for certification. In this way the entire performance of the user can be taken into account. However, for this the gathered information must be of higher granularity than just simple test results. Essential for this approach are tools which assist the tutor in analyzing user profiles, evaluate the students learning success and detecting suspicious learning patterns. It cannot be guaranteed that every piece of information describes the situation accurately, either because the student tried to manipulate or because he was distracted. If the interpretation is done with care and over a longer period of time, this should result in an accurate overall evaluation. However, there will always be a certain amount of insecurity. In case the tutor has some doubts, he can revert to explicit tests. In this case the information available gives good hints on what to test.

Innovative course design. A very fascinating approach, but very challenging for the authors, would be to find course material or forms of learning where the user cannot cheat. As one example the user could be given a concrete task. In order to find the solution he must—effectively as a side effect of the course—acquire the desired knowledge and the course is designed in a way such that he is guided towards this information. Collaborative elements, in which the student is forced to present his solution might also be an interesting possibility here. Since the tutor evaluating the presentation will obtain a good impression in this way of his actual knowledge the student is obliged to learn in order give a good presentation of his solution.

3.3. Confidentiality

Due to the fact that learning material by its nature must be distributed to the outside, industrial espionage and data theft are not major problems in eLearning. However, in certain scenarios this is also of relevance. Take for example a company, which uses eLearning for in-house training. In this case the learning material might contain sensitive information and confidentiality and restricting flow of information to well-defined groups is definitely an issue. Aside from counter-measures against physical theft of storage devices,
diligent security administrators have to set up countermeasures against electronic theft such as the installation of firewalls and intrusion detection mechanisms to hamper attackers from the outside. This will cover only part of the risk that confidential data could be stolen. Confidential material can be leaked from a perfectly protected intranet—stolen by insiders, having legitimate access to the data in question.

3.4. Copyright protection

The creation of learning material will always need a substantial amount of human expertise and cannot be automated to a significant degree. So learning material will always represent a high amount of expertise and work and therefore the copyright holders of learning material have a strong interest in protecting their learning material from illicit use and distribution.

The major drawback for copyright protection in eLearning is that the copyrighted material must be made available in digital form to the students. A training provider can and will restrict access to learning material only to registered students and the learning material can be delivered in encrypted form to the customer to prevent illicit users from getting hold of the data during the transmission. But once the data has reached the customer, the training providers depend on the goodwill of its students in terms of security issues. With digital data giving a user ready access to data always implies giving him the opportunity to copy and redistribute the data at will. Withholding the learning material until appropriate payment for the purchased goods is confirmed does not solve this problem, since it does not prevent one paying customer from redistributing illegitimate copies of the learning material.

A good way of reducing the costs for learning material is to reuse learning material created by others. Besides preventing the same content from being re-implemented over and over again a training provider can so gain access to material for content outside its own domain. If training providers exchange learning material, this will normally be done on the basis of some kind of agreement and typically there will be some kind of reimbursement. For this reason training providers require a way to prevent other training providers from using their material in ways other than covered by the agreement.

If learning material is composed from existing learning material or other copyrighted material, e.g. includes material from other authors into new courses, secondary copyright becomes an issue. Here the problem arises as to who the copyright holder of the composition is.

3.5. Shortcomings in the functionality of the WWW

The WWW was designed as unifying mechanism for the retrieval and presentation of various internetworked resources and provides sufficient mechanisms for delivery and presentation of learning material, but it has some shortcomings, when it comes to learning specific functionality.

In the WWW paradigm a user can at any time navigate to an arbitrary resource reachable by the client. In a learning application scenario one wishes to restrict1 this freedom of the user. But, since all standard browser applications implement this navigation metaphor in their user interface it is very hard to realize such restricted navigation functionality. In particular, it is almost impossible to realize a WWW-based user-interface, which prevents the student from using the native navigation functionality of the browser.

Further on, the WWW does not provide the degree of interactivity, exactness, reliability and security which is needed for effective monitoring of the learning success of students. Due to the statelessness of HTTP, there is no way to guarantee that either all test-relevant or none of the learning material is delivered to a student; even if all learning material has been delivered to the student there is no well-defined point in time for the start of the test. Today, JavaScript is commonly used for implementing learning-specific functionality such as timing control, test evaluation, and feedback in learning material. Although from a programmer’s perspective this is a very elegant and easy to use approach, the fact that the human readable source code is executed on the client side jeopardizes security. Since there are, despite all those problems, good reasons for using standard WWW browsers in eLearning, is a good approach to look for ways to augment the standard functionality of the WWW by learning specific ones. One example of such an augmentation is the open test frame work [5–7], which has been developed at Darmstadt University of Technology and provides secure implementations2 for the following:

- secure delivery of test material,
- reliable timing control,
- reliable and secure recognition and evaluation of user actions,
- tamper-resistant evaluation of tests,
- secure creation and delivery of feedback.

---

1 So the user should not be able to leave tests, nor should he be able to look up the correct solutions.
2 The security of the implementations comes from the fact that in this framework all security relevant functionality is realized on the server side.
The advantage of this approach is that only the functionality that the WWW is lacking, must be implemented. For the presentation of the learning material and the handling of the user interactions the already existing functionality of the WWW-browser can be reused.

4. Protecting intellectual property

As mentioned before the core problem with protecting digital data in the WWW is that the copyright holder loses the control over his material once it is delivered to the user. Since the material is represented as digital data, the user can make any number of copies without any loss in quality. One approach to protect intellectual property is therefore to extend the control of the copyright holder to the entire lifetime of digital data.

The CIPRESS\textsuperscript{3} system \cite{Ref8} (Fig. 2) is using this approach. The following sections will first give an overview of the system and then discuss how CIPRESS can be utilized for eLearning.

4.1. Overview of CIPRESS

The re-encryption technology is the key technology for preventing illegal distribution and allows exact monitoring of the usage of documents. The basic idea is that all data are stored in encrypted form on the storage devices of a client computer—CIPRESS uses the term client to denote a computer workstation which is used to access, display and alter documents. Whenever the document is accessed it must be decrypted. However, this decryption is only temporary so that the decrypted data of a document exists only in the volatile memory section of the computer. As soon as the document is saved to a storage device it is encrypted again. The crucial point here is that CIPRESS does not reuse the encryption key but creates a new personalized key specific to the document whenever the document is written. Key creation is done by a central key storage facility, the so-called Key Center, which is located in a secured facility. In CIPRESS, keys are exclusively generated in the Key Center, therefore the keys needed for decryption of a document must be retrieved from the Key Center. Thus the Key Center is involved in every access of the document data and therefore can monitor and document every usage of the documents. Furthermore, if the Key Center does not deliver any keys for the document the user cannot access its content. For practical usage this implies that an attacker from the outside might steal the data or even the entire storage device or computer but all he gets is the data in encrypted form. In order to view the document’s content he would have to contact the Key Center and authenticate himself to obtain the keys needed. If he uses his own user ID for this the Key Center would detect this illicit usage and not deliver the key. Therefore it is not sufficient to steal the data, the attacker must also have the authentication of a user who has sufficient access rights. However, the Key Center will in any case log the access, so that it is impossible to access the data

\textsuperscript{3}The acronym CIPRESS stands for “Cryptographic Intellectual Property Rights Enforcement System”. This is the internal code name for a joint development of the Mitsubishi Corporation, Tokyo, Japan and the Fraunhofer Institute for Computer Graphics based in Darmstadt, Germany to protect intellectual property from illegal usage and also to expedite reuse of copyrighted material for new content creations by combining patented re-encryption and watermarking technology.
without leaving a trace. The fact that by inspecting the records of the Key Center the entire usage trail of a document can be reconstructed becomes an essential feature when the copyright holder finds a pirated copy of one of his documents since it will help him to prove his ownership and to identify the security leak.

All this encryption and decryption is transparently handled by specific CIPRESS system components. These CIPRESS components exploit the cryptographic hash (a.k.a. digest) of a document in order to retrieve the corresponding key from the Key Center. A digest can be seen as a quasi-unique identifier. The numerical value is calculated in a way which ensures with sufficient probability that for two different documents (even if differing only by a single bit) the same digest will never be calculated. For CIPRESS this means that once a user alters the content of the document the modified content will be treated as a new document. Having to register all system files or application programs and reregister them whenever the file has changed, would create a lot of network traffic and a tremendous overhead of data in the Key Center, especially since during the login a lot of system files will be altered. This is the reason why CIPRESS also supports local documents on the client’s storage devices for non-shared usage. Like CIPRESS documents, they are automatically encrypted and decrypted but instead of using the re-encryption approach and obtaining the keys from the Key Center, a machine-specific key, the so-called master key, is used. This master key encryption is specific for every CIPRESS client. Therefore a master key encrypted document can only be accessed on the in which computer it is created. Once a document is completed and should become generally available, the document must be registered with CIPRESS. From then on the document will be encrypted using the keys from the Key Center and thus will become subject to the Key Center’s usage control and permanent surveillance. Registration must be done at a Content Server. In CIPRESS Content Servers are used to provide centralized and persistent storage of digital documents. Documents can be in any form of multimedia material such as text, audio, video or image data. The user can retrieve documents from a Content Server either using a CIPRESS specific application, which is also used to register documents, or alternatively they can use a WWW front-end and access the data via any WWW browser on a CIPRESS client. The encrypted material can also be made available on standard file servers.

From a technical vantage the CIPRESS system consists of lower layer extensions to the operating system.\(^4\) Thus CIPRESS provides an application-inde-\(^4\)Such operation system extensions have been developed for Microsoft Windows NT 4.0, Microsoft Windows 2000 and Solaris.
watermarks. The watermarking technology used by CIPRESS for images and video is unique in the point that it allows the embedding of hierarchical watermarks [9,10]. Since every watermark leads to a slight decrease in quality and these losses accumulate, CIPRESS uses a maximum of five watermarks (Fig. 3). The first one is a public watermark. This watermark is embedded immediately when the document is registered and holds the ID of the copyright holder. By reading out this public watermark everyone can determine the copyright holder for a given document. This is of utmost importance for the copyright holder since he can prove his claim in court. The other four watermarks are secret ones. Whenever a user accesses a document CIPRESS adds a further secret watermark holding the ID of the accessing user. In case a document already contains the maximal number of five watermarks a new watermarking cycle starts, i.e. CIPRESS will retrieve a new version of the document from the Content Server containing only the public watermark. Only a CIPRESS administrator knows the secret keys which are necessary to read out the information from the secret watermarks and is therefore capable of determining the most recent user of the image. Since the KeyCenter keeps record of who accessed the document the entire line of document users can be retrieved. The watermarks will stay in the information even when it leaves the media computer and is stored on different media and survive most common transformations. CIPRESS can detect its watermarks even if they are scanned in from printouts, up to 90% of the original image has been discarded, or the image is converted to a grayscale image.

Although watermarking cannot prevent the illicit distribution and usage of copyrighted material it is of utmost use once a copyright violation is to be proved in court. Also in case an insider was involved in the data theft, this malicious user can be identified and legal steps can be taken against him.

By combining all the above techniques, CIPRESS provides a secure environment since it covers all possible channels for an attack.

CIPRESS distinguishes between local and registered documents. This classification is based on technical issues (what type of encryption is used). In CIPRESS a document can either be registered as a normal or a Data Linkage document. This conceptual classification allows CIPRESS to correctly deal with the issue of copyright and secondary copyright. In the case of a normal document, CIPRESS assumes that the owner of the document is also the copyright holder for the content. According to the Data Linkage concept a user, if he wants to include foreign material in his material, is not allowed to embed this foreign material in his material. Instead he must use an external reference. The user then registers the new material as a Data Linkage document with himself as the copyright holder. Since composition of material is an intellectual work of its own right this is an appropriate way to handle the copyright problem. Since used material is always referenced but never embedded, the original of the referenced material must also be accessed whenever the composition is accessed. This guarantees that the copyright protection cannot be circumvented.

4.2. eLearning in a CIPRESS environment

The major advantage of CIPRESS is that since it is implemented transparently at the operating system level, it provides the required security features in a transparent way and can therefore be combined with any learning environment. So using standalone eLearning applications poses no problem at all and, due to the integrated WWW front-end, CIPRESS can also immediately be adopted for WWW based eLearning. In this case all the students must have installed on their computers—besides CIPRESS—a WWW browser. CIPRESS will take

![Fig. 3. CIPRESS watermarking scheme.](image-url)
4.2.1. Life-long usage control of learning material

In a CIPRESS environment the student can access learning material only if he has authenticated him against the CIPRESS system and the Key Center has provided the key, required to decrypt the learning material for this particular student. The important issue here is, that this key retrieval is not performed only once when the learning material is being delivered to the student, but with every access to learning material. Since the students cannot manipulate the Key Center, which is located in a secure facility, in a CIPRESS environment only legitimate users will be able to access the learning material. As a consequence, even sensitive or confidential information can safely be included in the learning material. If an intruder steals the learning material or even the entire hard disk, all he gets is the encrypted data. In order to see the content he would need a key from Key Center. In the same way, CIPRESS prevents illicit re-distribution even for learning material located on the students' PCs. If a legitimate student forwards the learning material, he has access to, to a different student, the data will be transferred in encrypted form and this other student will be able to access this learning material only if the Key Center delivers the appropriate keys. Since the keys used in CIPRESS are specific for every combination of document and user a student cannot reuse the keys of another student. Thus, due to the combination of re-encryption and watermarking access control does not end within CIPRESS once the learning material is delivered to the student. Instead, access control is extended to the entire life span of a piece of learning material and, since CIPRESS is embedded into the operating system and not only into a learning system, students even cannot access the learning material outside a learning session

The fact, that in CIPRESS the Key Center is involved in every access and thus can keep track of the user actions, has additional benefits besides security. The usage information gathered by the Key Center can be used for the following:

- Performance tuning and quality management. The information regarding how many students have accessed the system is important information for the training provider, since it allows him to optimize the overall performance of the system. The information on which learning material is accessed and to what extent this occurs helps the training provider to cover the needs of his customer and also provides some insights for quality management.
- Accounting and billing. Accounting and billing is in the one or other form always connected to the actions of the students. Since the CIPRESS Key Center keeps record of every key delivery all the basic data needed for accounting and billing are readily available at the Key Center. Large-scale accounting and billing like operating a Key Center in a secure and reliable way require resources which probably exceed the capabilities of small or medium enterprises. Therefore it would be a reasonable business model that an internet provider or telecommunication company, which has the technical and administrative resources, operates the key center and, as a service to their customers, will do billing for them. Then a training provider could concentrate on the creation and maintenance of learning material and other learning-related services such as tutoring or certification. This would give small and medium enterprises the opportunity to become a training providers, without having heavily to invest in hardware and accounting personnel. With its distinction between Content Servers and Key Center, CIPRESS is especially well suited for such a business model.
- User-profiling. As mentioned before maintaining user profiles allows significant enhancement in the course quality. Since CIPRESS detects and records the access to material at any time and not only when the user learns, one can reach a much higher level of accuracy of the user profiles, if the learning system is given access to information gathered by CIPRESS.

4.2.2. New learning features

By giving the owner permanent control over his learning material, CIPRESS effectively prevents the illicit re-distribution of learning material from the side of the student. Besides this, the lifelong control in conjunction with the CIPRESS user administration allows some beneficial features, which are not possible in conventional learning environments.

- Pay per use. From the access logs at the Key Center one can easily derive, what learning material a student has used. This is an essential feature for realizing learning on demand scenarios. In such a scenario the student can potentially access every piece of learning material, but will be billed only for the material he actually used. The advantage for the student is that he can immediately access the learning material, when the need arises, without having to undergo any subscription procedure. The advantage of CIPRESS is, that the Key Center will become aware of any access, independent from the distribution channel used. With CIPRESS every type of
material, even full-grown applications, can be used in pay per use mode.

- Time-restricted use of learning material. Normally a student can once the material is delivered to him access the learning material as long as he keeps the data. With CIPRESS the owner of the learning material or the training provider can by setting the CIPRESS permissions at any time cause the Key Center to no longer distribute any keys for a specific piece of learning material. With this feature a training provider can restrict the student’s usage of the learning material to exactly the time span the student has paid for.

- Ease of maintenance. Also, this feature is very beneficial for keeping the software up to date. Suppose the training provider decides that a specific piece of learning material should no longer be used, because the content has become obsolete, is faulty or for some legal or political reason. With traditional systems the training provider had no means to make sure that the students will not continue to work with the material delivered to them. With CIPRESS all he has to do is set the CIPRESS access rights so that the Key Center will no longer deliver keys for this learning material.

- Delivery in advance. Although learning material will normally be delivered on demand via the WWW, there are certain scenarios where using a different distribution makes sense. Using CIPRESS and a WWW-based training system requires in any case the existence of an online connection for obtaining the keys from CIPRESS and sending back control information (user feedback) to the course control system. These information are relatively small amounts of data, so sending them causes almost no delay. Other considerations apply to multimedia material, especially high-quality video, which is retrieved on demand from the server. The training provider might send the learning material in advance on a CD-ROM. Then the learning material could be loaded from the file-system and so avoid significant delays which disturb the flow of learning and high communication bills. When doing this, it must be guaranteed that the student cannot access the material (exercises, tests) before he is supposed to do so. When using CIPRESS this is no problem at all. All that the owner—or even the learning system automatically—has to do is set the CIPRESS access rights accordingly. When the material arrives on CD-ROM the student has no rights, therefore receives no keys and cannot access the material. Immediately before the student should access a piece of learning material, the learning system grants the rights and the student can access the material.

- Personalization. Different students have different backgrounds, different learning goals or simply have paid for a different level of support. So ideally, there should be a specific set of learning material that each student needs. The training provider must on the one hand ensure that a student can access all the learning material he needs or is entitled to, but on the other he does not want to give the student access to material he is not entitled to. When the learning material is delivered via CD-ROM this is a major problem since it is not practical to create for each student a personalized CD-ROM. With CIPRESS the training provider can send the same CD-ROM, containing all the available learning material, to each student. Since the learning material is encrypted, the training provider controls which learning material a student can access by granting the access rights. It is also not a problem later on to give the student access to more material or imply further restrictions. Again, it is only a matter of changing the access rights. No new CD with material must be delivered to the student.

The conceptual support for secondary copyright (Data Linkage) comes in handy in case learning material authors are paid based on how often their learning material is used. Since it is the CIPRESS philosophy not to merge material from different copyright holders but use Data Linkage instead, the royalties for the copyright holders can easily be derived from the logs of the Key Center.

5. Conclusion

Although the WWW does not cover all the security requirements of eLearning there are ways to overcome many of the problems and reach an acceptable level of security.

The test framework demonstrates how highly interactive test material can be integrated in WWW based training in a way that guarantees secure and reliable monitoring of the students’ learning success. The framework is fully operational and can easily be adapted and extended. Therefore it can serve as a good test bed for exploring new forms of learning especially suited to the WWW, and which can better handle the specific requirements of the WWW.

In an environment with a trusted administration of the client computers it is even possible to prevent illegitimate access and redistribution of course material.

References


