Article in T-110.501 Seminar on Network Security 2001 ISBN 951-22-5807-2
Publications in Telecommunications Software and Multimedia TML-C7 ISSN 1455-9749
Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory

http://www.tml.hut.fi/Studies/T-110.501/2001/papers/index.html

Analysis of E-book Security

Guoyou He
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
ghe@cc.hut.fi

Abstract

E-book is a new publication technology raised in recent years. It has a number of advantages for both providers and consumers. From the standpoint of providers, E-book can distribute publication in a large range efficiently and economically. From the consumers' point of view, they can read E-books immediately, without having to wait for the title to be shipped to them. Many E-books can be taken anywhere by the customers in their laptop, or PDA, etc. To protect the rights of both providers and consumers with security mechanisms is one of critical issues in development of E-book technology. Currently, E-books are secured using different security mechanisms in their publishing and distributing process. This paper makes a survey on main E-book standards, application architectures and security mechanisms. The security strength and weakness of the investigated E-book systems are analyzed and presented.

1 Introduction

E-book - electronic book, is a book in electronic format. An E-book can be stored in one or several digital files and distributed via Digital Rights Management (DRM) systems[1], which define the way for E-book distribution and consumption. A DRM system is mainly composed of E-book servers and readers[1, 5]. E-books can be downloaded from E-book servers of different providers to a consumer's reader system, which includes reading device (e.g. laptop, PDA, PC, or dedicated E-book reading device) and reading software (e.g. Adobe PDF file reader and Microsoft E-book reader) through Internet. Of course, E-books can also be stored and distributed via storage medias such as disk and CD-ROM. In fact, E-book is very familiar for all of us. It simply can be in any electronic file format such as PDF, OEB[19], HTML, XML, LIT[16], Doc, even plain Text, depending on the requirements on richness of the contents and security of the E-book systems. For example, E-books in PDF format can provide rich contents, and the corresponding E-book system, Adobe Acrobat, provides several levels of security[12]; HTML can provide multimedia effects for an E-book, if the E-book is compiled with a HTML compiler, the publication can not be modified, the print and copy functions can also be disabled[4]; files in plain Text format only provide contents in ASCII format, if they are opened with a general text file reader, the contents can be freely modified, copied and distributed, but if the plain text files converted into .lit files with eBook Express[16], user rights can be restricted.

Compared to a traditional book, E-book can be distributed in large scale with very low cost instantly. E-book also has the advantages of low material consumption, high portability in weight, volume and little room occupation. But E-book may never have

some advantages of traditional book, such as easy usage for all kind of people, no need of reading devices, no need of power consumption except light when reading. The transaction processes of traditional books mostly are in physical. A lot of trust such as protection of the copyright and the rights of a consumer is involved in the physical transaction implicitly. But the main disadvantages, format incompatibility and security issues, of E-book have raised a lot new requirements and technologies, especially for restricting free duplication and distribution. To tackle these issues, many organizations and companies have involved in developing E-book standards and technologies including Digital Rights Management (DRM) for E-books[1], Electronic Book Exchange (EBX)[5], MPEG-21[15], Open E-book Publication Structure (OeB)[19], Open Digital Rights Language (ODRL)[14], and Extensible Rights Mark Up Language (XrML)[8], etc.

In the E-book market, the e-commerce processes are implemented mainly by DRM systems via Internet, though it can also be done by storing E-books in storage media such as disk and CR-ROM, and distributed by distributors and retailers. Making a secure DRM system on Internet is critical for the E-book business. Following, I will only concentrate on DRM systems on Internet, and review the requirements and architecture for implementing secure DRM system and the security mechanisms currently used in DRM system for E-books.

2 The Scope of E-book Security

E-book is a kind of asset in digital format. In the E-book market, it should be securely stored, transferred and used against free duplication and distribution. The E-book business is implemented via DRM system for E-books. A DRM system is mainly composed of E-book servers, reading systems, transmission facilities, E-book contents and related information[1, 2, 5]. In a DRM system, E-book contents and related information are stored in the E-book server and/or the E-book reading systems; the transmission is mainly carried out via Internet[5]. To keep an E-book free from unrestricted duplication and distribution, we have to make the E-book storage places and transmission processes secure, i.e. making the E-book system secure against free duplication and distribution. So I define E-book security here as maintaining E-book system secure and restricting free duplication and distribution of E-books.

3 Digital Rights Management for E-books – DRM

DRM for E-books[1, 2] is being developed by the Association of American Publishers, Inc. (AAP) and other participants in the publishing and e-commerce industries. DRM for E-books is intended to promote the use of E-books and to facilitate the development of E-book related technology. DRM for E-books specifies the functionality of DRM system, foundation of DRM application architecture, interoperability issues of different DRM solutions and DRM system requirements in the aspects of technology, legislation, Rights Specification Language (RSL)[1], electronic package control, file format and trust infrastructure. It aims to provide a standard specification of DRM for different E-book system vendors. The first version of DRM for E-books was released in December 2000[1].

3.1 Typical DRM Application Models

DRM application models are classified as E-book market model and E-book electronic package model[1]. The E-book market model requires DRM system supporting all the activities in the publishing stages of the E-book market. This model defines the E-book market as five phases including create and publish, market and distribute, sell to consumer, consume content and support consumer. The implementation of DRM system should support all the activities involved in these phases[1]. This model is a business model describing the DRM system mainly in the market point of view. The E-book electronic package model describes the DRM system in the technique point of view[1]. It specifies the basic technology for publishing, transmitting and consuming digital E-book contents in the DRM system.

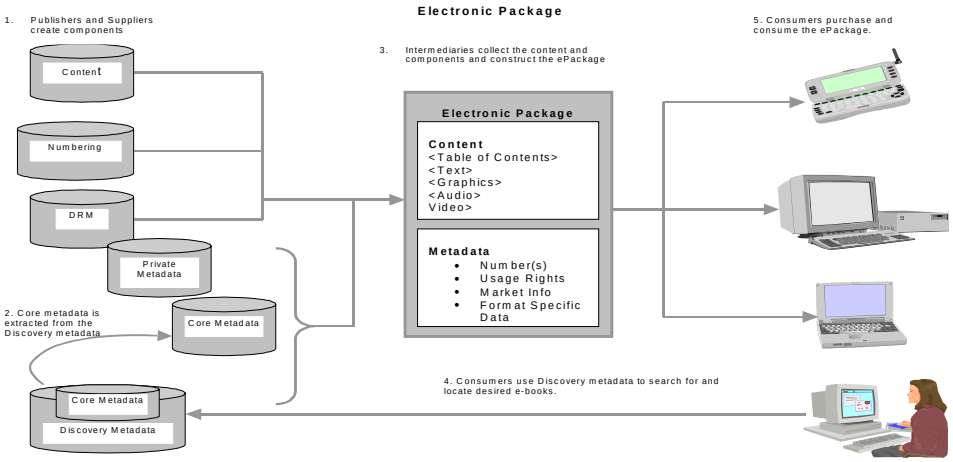

Figure 1: E-book Electronic Package Model of DRM[2]

The E-book electronic package model contains the components of a DRM E-book system and describes the activities of E-book business.

The components of a DRM system include:

- *DRM E-book system server of publisher and suppliers:* the E-book contents, metadata[2], information of DRM and numbering[3, 13] are stored in this server. Metadata is classified as Discovery Metadata, Core Metadata and Private Metadata. Discovery metadata provides the information to help consumers locate and purchase desired title and to help service providers creating market opportunity to sell a title. Discovery metadata is public information, which contains information such as the title, the author, the cover image, the E-book description etc. Core metadata is a part of the ePackage. It is also public information such as the title, the author, the category, the contributor information, the file size etc. used for cataloging and creating digital libraries. Private metadata is not for public consumption. It contains information for helping publishers, distributors and retailers to manage the E-book selling process. Private metadata includes: RSL, which is information necessary to support the DRM solution and specify the terms, conditions and fee structure associated with a particular E-book; format specific information, which is unique and required information to create the ePackage for specific –book format; return

metadata, which is the information potentially sent back by consumers in the process of exchanging services. DRM contains usage rights information specified with RSL. The information includes the rights of using E-book such as distributing, printing, copying, disposing, etc. Numbering contains the information for identifying E-books[2].

- *Reading and searching systems:* These systems are used for locating and consuming E-books. The deal of E-books is negotiated between the system server and the reading/searching systems securely.

- *Transmission facilities:* The E-book content and related information can be transmitted via any communication networks such as Internet, WAN, LAN, or wireless networks.

During the E-book dealing process, the information Core metadata, private metadata, DRM, numbering for specific E-book is compressed, encrypted with the content of E-book in ePackage and distributed from provider's DRM system server to consumer's reading system.

3.2 Functionality and Secure Mechanisms of DRM

Contrasts to the physical book commerce, E-books are traded mainly via Internet with digital technology. The E-book sellers and buyers are invisible each other in most cases. Can they trust each other? How can the commerce transaction be done securely? DRM tackles most of the security issues for the E-book market though some problems still present.

Protection of digital content

DRM provides protected digital contents with encryption. DRM recommends that DRM system solutions encrypt content and metadata with standard symmetric encryption algorithms such as DES, RC4, etc[1]. Currently, multiple DRM systems and content file formats co-exist. So DRM solution should allow publishers or authors to have the option of specifying or selecting different encryption algorithms and key lengths. A publisher uses a DRM publisher utility software encrypting specific E-book title with a single randomly generated encryption key. At the same time, a voucher is generated for the title. The voucher encrypts the content encryption key using the publisher's public key. During the distribution process, the voucher is decrypted with the publisher's private key first. Then it is encrypted with a retailer/consumer's public key and transferred to the retailer/consumer[5]. The encrypted contents and metadata can be decrypted with the encryption key. So proper key management is critical for DRM.

Except encryption, digital watermarking technologies, though it can't prevent unauthorized access to E-book contents, can be used in DRM solutions to trace and prevent unauthorized and illegal distribution of unencrypted E-books for additional level of security[1].

Secure E-book distribution

DRM system can distribute E-books via Internet or CD-ROMs. When CD distribution is used, the decryption key and usage rights specification can be delivered with the CD, but DRM uses different secure mechanisms for Internet distribution.

In the process of E-book distribution from publisher/retailer to consumer or from publisher to retailer, the critical issue is that the decryption key distribution. DRM uses asymmetric encryption method to distribute the decryption key[1]. An E-book provider encrypts the E-book decryption key with a retailer/consumer's public key and sends it to the retailer/consumer. It can be decrypted with retailer/consumer's private key. Then the DRM system uses the decryption key to decrypt the E-book. The strength of the encryption depends on key length used in the encryption.

Personal lending in DRM system is done via setting loan right and making a loan copy. The loan right can specify the loan period. The right to make a copy of loaned work is governed by the loaner copy. If there is a copy right, the right can be exercised. Except restricting to make copy from loaned work, DRM also prevents consumers making unauthorized copy by specifying copy right on E-books via RSL, for example[1]:

VIEW = YES
PRINT = YES
COPIES = 3
DELETE = NO
SUPERDISTRIBUTE = NO.

Institutional lending is time based multiple lending used within library or corporate. All the copy rights, loan rights and usage rights are specified via RSL in DRM system. Giving is similar to personal lending, but no time limit for returning. The access of E-book on the original consumer's reading device is terminated.

Using RSL, a publisher can specify the rights of superdistribution and distributor copies such as prices and number of copies for consumers and retailers.

In addition, the rights to secure using E-books such as creating backups, deleting works, transferring works, modifying works and creating unprotected copies, etc. are specified via RSL in DRM systems.

Content authenticity

In DRM system, the E-book contents can be authenticated using message digest to assure that consumers get what they really want. Content provider generates a message digest with one-way hash function and stores it in a safe place available to consumers. The Consumers can authenticate the E-book contents with the message digest[1].

Transaction non-repudiation

DRM provides transaction non-repudiation with digital signature. Using the private key of a transaction participant encrypts a digital signature with the transaction. Anyone can decrypt the signature with the public key and verify that the private key holder participated in the transaction[1].

Market participant identification

Participants are identified with digital certificates in DRM system for E-books[1]. Detailed information refers to the trust model in section 4.1.

Cryptographic technology makes DRM having many useful capabilities for E-book security, but it still has some limitations, broader perspectives on digital content protection are needed.

3.3 Multiple DRM Perspectives Required for Protection

In the technology aspect, DRM can't ensure securing E-book content absolutely. To optimize protection, DRM requires multiple perspectives of protection in technical, legal and social[1].

Technical DRM Perspective

The technical perspective includes rights specification language, electronic package controls, hardware and software[1]. The technical DRM perspective has a number of elements based on cryptography. They are usually used in combination to secure E-book contents. These elements include encryption, public/private keys, digital certificates, watermarks, access control, authentication, secure communications protocols, secure content storage, rights specification language, and trust infrastructure as discussed above. Based on the technologies mentioned above, it will help to mitigate threats and illegal copies, and further enforces implementing programs and services in DRM systems to identify and audit copyright violations. It also enforces monitoring and responding to activities and programs of attempting to break DRM system security, unauthorized reproduction and distribution of E-books. AAP has already implemented an Internet monitoring program used for searching pirated E-book contents over Internet[17].

Legal DRM Perspective

The full name of DRM is Digital Rights Management. The rights here is closely related to law and legal issues. The legal perspective involves legislation, compliance, investigation and enforcement. The watermark in technical perspective is the promise for legal perspective. Digital watermarking can not prevent illegal distribution of E-book contents, but it can help to detect illegal copies and enable compliance, investigation and enforcement of legislation. The technical and legal perspectives can't guarantee completely secure digital contents. It is possible that any secure system can be defeated under certain condition. When the contents of E-book are delivered to market, protecting the E-book contents becomes a social issue[1].

Social DRM Perspective

In the emerging field of E-book, authors and publishers have more opportunities to publish contents. More and more materials including books, magazines, newspapers and other online contents are available to consumers. The consumers may get high-quality illegal copies of E-book or other copyrighted works without compensating the copyright holders. Securing copyrighted works against unauthorized use in digitized format becomes increasingly critical in worldwide. So it becomes a social issue that making consumers to know the distinction between E-book downloading and freeloading,

legislation on copyright, value of using legal E-books and the risks of using pirated digital contents. Content providers can also mitigate piracy by providing superior support added values only available to legitimate users. Some possibilities are warranty support, problem resolution, update, enrich contents with multimedia and special offer, etc. Making more people understand the value of being legitimate users. The aim is to keep honest people honest and create more honest people[1, 19].

Compared to the technical and legal perspectives, strengthening the activities in social perspective can create more legitimate consumers, relatively it decreases the number of illegal users. It means that amount on pirated E-books is decreased, threats are mitigated and DRM system security is increased. Creating more legal consumers in social perspective means the decrement of the efforts on investigation and enforcement on preventing unauthorized use of E-books, relatively the legal perspective is enforced.

3.4 Security Requirements for DRM

The security requirements of DRM are mainly related to two aspects. One is electronic package control, and the other is trust infrastructure.

Security Requirements for Electronic Package Control (EPC)

Electronic Package control refers to encryption and related packaging technology required to support the DRM system. The requirements on the EPC include multiple objects, encryption, transmission, numbering, metadata and search[1].

- Multiple objects – EPC should support multiple digital objects both themselves and that made by other digital objects. EPC supports creating E-books as collections of objects contained in a single electronic package and segmenting large E-book into multiple electronic packages to distribute.

- Encryption – EPC should support standard encryption algorithms. Publisher can have the option to select preferred algorithms.

- Transmission – EPC should ensure error free transmission.

- Numbering – EPC supports E-book identification system, e.g. ISDN of E-book.

- Metadata – Safely package E-book metadata, securely encrypt private metadata, protect and authenticate EPC content and metadata. Non-private data can be accessed easily.

- Search – Easily access and locate E-books at object level.

Security Requirements for Trust Infrastructure (TI)

Trust infrastructure is the part in a DRM system. It makes the whole system work. The requirements on it are critical for the system. They are listed following[1]:

- Interoperability – TI supports multiple vendors' E-book reading devices.

- Security – Use reputable, third party independent security practices. TI should be demonstrated secure.

- Consumer privacy – TI must support protection of consumer privacy and information.

- Miscellaneous Security requirements – TI should support multiple levels security, such as authentication, digital signatures and watermarking.

It is required that new DRM specification should be based on standard encryption algorithms for encryption, standard compression and packaging techniques for packaging. Internet standards such as ODRL, XrML and XML should be used for DRM rights specification languages and communication protocols.

4 Electronic Book Exchange System – EBX

EBX system[5] is being developed by the EBX working group. It defines the way of secure E-book distribution from publishers to booksellers, from booksellers to consumers, between consumers, and between consumers and cooperates. In this section, we'll discuss the functionalities and security related issues of EBX system.

4.1 EBX System Models

EBX system is specified in two models, functional model and trust model based on the functionalities of the system components and interactions of the trusted components in the system respectively. They are described in following.

Functional model

This model defines the EBX system in the sequence order from E-books creating, publishing, distributing to consuming.

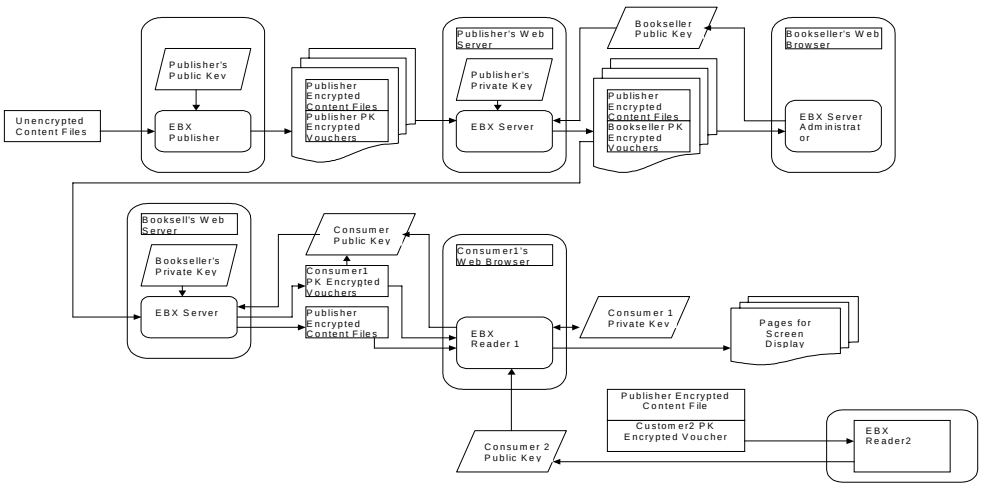

Figure 2: EBX Functional Model

The whole procedure is shown in Figure 2 which includes publishing, distributing to booksellers/distributors, delivering to consumers/libraries, and transferring between consumers, between consumers and libraries. The vouchers in the figure are digital objects that describe transmission and usage permissions and copyrights of E-books.

Publishing: Publisher formats each E–book title into specific format of file and encrypts the content file using the EBX publishing utility licensed from a certified EBX software vendor. Voucher template is created for the content file by encrypting the content-encryption key, which is generated by the EBX publishing utility using the publisher's public key. The encrypted content files and the corresponding vouchers are added to the publisher's EBX server, which is plug-in software to publisher's Internet Web site for use by authorized booksellers and distributors.

Distributing to booksellers or distributors: Any E-book can be downloaded from publisher's Web site to bookseller/distributor's EBX server by using EBX server administrator equipped browser. Both the EBX server and the EBX Server administrator equipped browser are licensed from certified vendors. In the downloading, the publisher's EBX server decrypts the desired voucher using the publisher's private key, sets the bookseller/distributor's permissions and copy count, and re-encrypts the voucher using the bookseller/distributor's public key. Then the encrypted voucher is transferred to the bookseller and the encrypted content file is added to the bookseller/distributor's on-line Internet bookstore Web site.

Delivering to consumers: A consumer can purchase and download the E-books what he wants from the bookseller's Web site using his EBX reading system, which is licensed from a certified vendor. During the downloading, the bookseller's EBX server decrypts the content file's corresponding voucher using the book seller's private key and creates a new voucher combined with the applicable permissions for consumer (e.g., 1 copy, lending, giving allowed, printing not allowed). The new voucher is encrypted with the consumer's public key and transferred to the consumer. The consumer's EBX reading system can then use the consumer's private key to decrypt the voucher. The vouchers containing content decryption keys are always encrypted using the consumer's public key and stored on the consumer's reading device. To decrypt the E-book, the reading system using the corresponding voucher decrypts each encrypted page.

Trust model

As we mentioned in the functional model, EBX reading systems and servers consist of EBX networks made up of different vendors' products. For two components in the network to interoperate, they need to communicate and find what they have in common such as encryption algorithm, key length, and the format of the content file. In order to ensure the integrity of the overall network and avoid giving away secret information to potential attackers, the participants in communication need to trust each other. All the services carried out between trusted parties are trust services, which specifies the services of each component must perform correctly to both manage the digital rights of protected content and preserve the integrity of the system. It requires mutual authentication of clients and servers. The authentication mechanism of trust services is Public Key Infrastructure (PKI), which performs the identification, certification, and authentication functions required by the trust mode. The overall EBX Certificate Authority (CA) architecture is given in Figure 3[5].

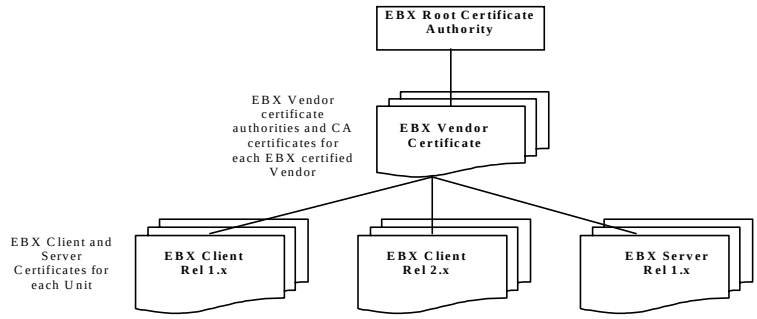

Figure 3: EBX Certificate Authority Architecture[5]

The EBX CA architecture consists of root CA and related systems, vendor CAs and related systems, and certificate processing services implemented by vendors.

The EBX root CA issues X.509 v3 certificates to vendor CAs. Each vendor CA in turn issues X.509 v3 certificates to client and server instances implemented by the vendors. A vendor CA certificate issued by the EBX Root CA is delivered via e-mail to the vendor. Then the vendor installs the certificate to the vendor's own CA. The key requirements to the vendor CA are that it issues a unique certificate to each client and server instance, the trust level indicated by the certificate must be at or below the maximum trust level approved for the client or server implementation, and the certificate conforms to the format specified in the EBX specification.

The vendor certificate services are done in the process that an EBX client builds a PKCS#7 certificate chain and sends it to an EBX server where the service is requested. The EBX server receives, decomposes and verifies the PKCS#7 certificate chain sent by the client. After the certification, the client public key is extracted from the authenticated client certificate, and the content encryption key is encrypted in the voucher with client's public key.

In an EBX system, there are many different components including hardware and software. Based on the role and functionality of a component, which can be assigned to a trust level. The EBX trust model specified six levels of trust[5]:

- Level 0 –No protection: Creating content and distributing it for viewing with no protection for titles, no proof of origin, no assurance regarding integrity of Infrastructure, copying allowed and unregistered reader (lacks a unique ID).

- Level 1 – Signed by author/publisher: Cryptographically signed by author or publisher binding in attributes, rights, integrity and origin; copy allowed; registering reader is optional.

- Level 2 – Book personalized to purchaser: Cryptographically signed by author/publisher binding in attribute, rights, integrity, origin; purchaser ID bound to individual copies cryptographically; copy subjected to rights; registering reader is optional.

- Level 3 – Software DRM with strong encryption: Specified and enforced range of rights; protecting content with strong encryption; individually registered; voucher servers individually revocable; implemented in unprotected software.

- Level 4 – Software or hardware DRM for high value content: Resistant to the well equipped lone hacker; resistant to sniffing tools and defendant to virus and Trojan horse attacks with component's private key and other credentials; decryption of content occurs in a secure, trusted environment; revocation procedures in place for rogue devices and content servers.

- Level 5 – Industrial Level Hacking / Cryptanalysis Required: Coercion more serious threat; hardware must have tamper detection and appropriate shutdown procedures; password guessing shall be detected and the component shall have appropriate shutdown procedures; hardware must have provisions to protect secrets in all modes of operation.

In the EBX system, a number of the servers and end user readers from different vendors cooperate to enforce digital rights. They provide persistent copyright protection through secure authentication, secure transfer and controlled exposure of the vended content according to the trust levels defined for the system and rights associated with each particular digital title. An example is shown in Figure 4.

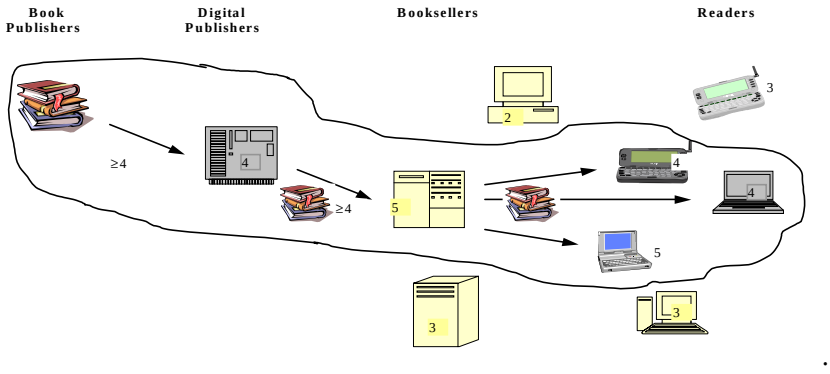

Figure 4: Subset of components that can handle a trust level 4 set by publisher[5]

In this example, the book publisher requires the E-book service should have at least trust level 4. It is available for those components having trust level greater than or equal to 4 in the EBX system. The others are excluded from the service.

5 Revealed Flaws of E-book security

Currently, a lot of E-book sellers are doing E-books business over Internet[9]. The big E-book market has been driving many vendors implementing different electronic publishing and reading solutions[20, 21]. The software E-book leaders are Adobe Acrabat PDF and Microsoft Reader LIT. But it was reported that the security flaws in both of them have been revealed recently.

On DEF CON Nine, July 13th, 2001, Russian cryptanalyst Dimitry Sklyarov presented Adobe's Acrobat e-book reader security mechanisms and the security flaws what he found in Adobe's Acrobat e-book reader[10].

In Adobe's E-book DRM system, the file encryption and key management are handled by third parties developed security handler plug-ins, which include Standard security handler, Rot13 security handler, FileOpen security handler and SoftLock security handler. An Adobe DPF file viewer takes document encryption key from a security handler and decrypts E-book content[10]. The cryptographic algorithms used in the security handlers are critical for the security of the Adobe's E-book DRM. Unfortunately, all these third parties developed security handlers have security flaws as revealed by Sklyarov.

The standard security handler uses RC4 steam cipher encrypting file content with a unique encryption key. The encryption key is encrypted and stored in the PDF file's encryption dictionary. Either the user password or owner password can recover the encryption key and decrypt the file content. The passwords can be enumerated with reasonable efforts[10]

Rot13 security handler is very weak. It encrypts all documents with a fixed key. The key is stored in the plug-in and can be found easily[10].

FileOpen security handler uses variant keys, but all the keying materials are contained in the encrypted document. Attackers can easily reconstruct the keys[6, 10].

The other third party plug-ins, *SoftLock security handler* and *eBook Pro compiler*, used in Adobe Acrobat can be easily broken as Sklyarov mentioned[10].

Except the flaws mentioned above, a software product, Advanced Ebook Password Remover (AEBPR) was marketed via Internet by ElcomSoft before. AEBPR can remove user password even 128-bit RC4 and all encryptions of a PDF file. It can also remove security put in place by third party security handlers[12, 20].

After the security issues, Adobe Acrobat eBook reader was updated. Elcomsoft was asked to cease selling AEBPR immediately by Adobe's Anti-Piracy Enforcement Team on June 25, 2001. Sklyarov was arrested due to violating the Digital Millennium Copyright Act (DMCA)[23] in the U.S. after the DEF CON computer security conference.

In addition to security flaws of Adobe Acrabat, it was reported that the Microsoft eBook reader security was also broken recently. One decryption program can defeat Microsoft eBook reader level five protection and convert E-books to unprotected files that can be viewed on any Web browser[7].

6 Strength and Weakness of the E-book System Security

For analyzing the strengths and weakness of the E-book system security presented above, let us consider following four common attacks based on [11]:

Attack the content server

This kind of attack enables access to and alteration of E-book content on publisher or E-book seller servers. It may also deny services. To mitigate this kind of attack, measures have to be taken on securing operating system and using firewalls. From previous discussion, we can see that E-book technologies have to create the E-book system in

distributed environment. In the DRM system for E-books, consumers mostly have the services via bookseller's server or publisher's server. These servers can be under special care such as securing operating systems and using firewall. The communication between clients and servers are under certification and authentication control. All critical information stored and transferred under encryption on provider's server. So the security of provider's server in a DRM system is relatively easy to be fulfilled, and the possibilities of being defeated are relatively low.

Attack the encrypted content

It includes the attacks of cracking the encrypted E-book content and making it possible to distribute copyrighted content illegally. This kind of attack is the most dangerous threat on DRM systems. Attackers can easily get necessary information for reconstructing encryption keys from broadly spread reader systems. The key reconstruction can be done using current powerful calculating facilities with reasonable efforts. The critical solution for mitigating this attack is use proper cryptography technology.

Attack the reader system

Reader systems are distributed in very large scale and different environments. Reader system can be used to decrypt documents. All or part of encryption key related information of an E-book is stored on reader devices. Attackers can easily access critical information for cracking the system on the distributed reader systems. This attack is difficult to defend.

Impersonate a legitimate customer

In a DRM system, the mechanisms of verification and authentication can be implemented for keeping network integrity. It can restrict impersonation, but can't completely prevent it. Any person, no matter an attacker or not, can be a legitimate customer.

From technical point of view, E-book system is a very complicated and widely spread system. Correspondingly, the security implementation in this system is extremely difficult. The critical issue to make the E-book security possible is use proper technologies and properly implemented third party plug-ins. The cracking of Adobe Acrobat is a typical example.

7 Conclusion

In this paper, the newly emerged E-book technologies are presented. They are intended to promote publishing revolution in secure way. All organizations and vendors try to overcome security issues and make their systems perfect. But in the face of complexity of communication and distribution, technology limitation, and the strength of attack, it's almost impossible to fix all flaws from attack. The typical verification is the revelation of security flaw in Microsoft E-book Reader and the cracking of Adobe's Acrobat eBook system. It's difficult to say any E-book can ensure absolute security. Of course, E-book business is a newly emerging field, to make E-book systems secure, we have a long road ahead. The improvement in technology perspective is still the key for security issues. Currently, the critical technology used in E-book security is cryptography technology. The common method cracking encryption is key reconstruction. As we have identified attack on revealing the encryption key is the most dangerous threat on E-book security.

Using proper cryptography technology is the first thing first need to be considered in design and implementation of DRM system for E-books. The second main threat is reader system attack. Proper implementation of reader system is the key to maintain secure and integral DRM system. It should be considered using comprehensive measures including legal and social perspectives to keep E-book secure, but it is the way of no way in technical view. Another important aspect in E-book security is monitoring and tracing. It is important to help the system vendors finding the security flaws and fixing it.

References

[1] AAP – Association of American Publishers, Inc., Digital Rights Management for Ebooks: Publisher Requirements, Version 1.0, New York, 2000.
<http://www.publishers.org/home/drm.pdf>

[2] AAP – Association of American Publishers, Inc., Metadata Standards for Ebooks, Version 1.0, New York, 2000.
<http://www.publishers.org/home/metadata.pdf>

[3] AAP – Association of American Publishers, Inc., Numbering Standards for Ebooks, Version 1.0, New York, 2000.
<http://www.publishers.org/home/numbering.pdf>

[4] Bersoft, How to choose your HTML eBook compiler, June 22, 2001 [referred 8.11.2001]
<http://www.bersoft.com/comparing.htm>

[5] Book Industry Study Group Inc., The Electronic Book Exchange System (EBX) Version 0.8, July 2000.
<http://www.ebxwg.org/pdfs/spec.pdf>

[6] Bruce Perens, Dimitry Sklyarov: Enemy or friend?, August 2, 2001 [referred 8.11.2001]
<http://www.zdnet.com/zdnn/stories/comment/0,5859,2800985,00.html>

[7] CNET News.com Staff, Microsoft E-book security in doubt, 31.8.2001 [referred 8.11.2001]
<http://news.cnet.com/news/0-1005-200-7026815.html?tag=rltdnws>

[8] ContentGuar,: XrML: Extensible rights Markup Language, 2000.
<http://www.xrml.org/>

[9] EBook Connections, eBook Best Seller List, November 18, 2001 [24.11.2001]
<http://www.ebookconnections.com/bestsellers/b_home.htm>

[10] ElcomSoft, eBooks Security – theory and practice, 13.7.2001, [referred 8.11.2001]
<http://www-2.cs.cmu.edu/~dst/Adobe/Gallery/ds-defcon/sld001.htm>

[11] Global Integrity Corporation, E-book Security Assessment, 1999 [referred 8.11.2001]
<http://www.publishers.org/home/press/global.html>

[12] Guignard Bryan, How Secure is PDF? White paper, 23.7.2001 [referred 8.11.2001]

<http://www-2.cs.cmu.edu/~dst/Adobe/Gallery/PDFsecurity.pdf>

[13] International DOI Foundation, The DOI Handbook, Version 1.0.0 February 2001. <http://www.cs.rit.edu/usr/local/pub/jeh/courses/731/DOI-Handbook-v1_0_0.pdf>

[14] IPR Systems Pty Ltd, Open Digital Rights Language (ODRL), 2001. < http://odrl.net/0.9/ODRL-09.pdf>

[15] Jan Bormans, Keith Hill: MPEG-21 Overview, Sydney, July 2001.

[16] Microsoft, How to Make an eBook, October 01, 2001 [referred 8.11.2001] <http://www.microsoft.com/ebooks/tools/make_how.asp>

[17] Microsoft, Message from the AAP and Microsoft, 2000 [referred 8.11.2001] <http://www.microsoft.com/piracy/epub/default.asp>

[18] Noring Jon, Finding the balance for End-user, DRM and the DMCA, July 26, 2001 [referred 8.11.2001] <http://planetebook.com/mainpage.asp?webpageid=199>

[19] Open eBook Forum, Open eBook Publication Structure 1.0.1, July 2001

[20] Planet eBook, Adobe Acrobat eBook Reader updated after security issue, June 28, 2001 [referred 8.11.2001] <http://www.planetebook.com/mainpage.asp?webpageid=157>

[21] Planet eBook, eBook Software, July, 2001 [referred 8.11.2001] <http://www.planetebook.com/mainpage.asp?webpageid=14&TBCategoryID=9>

[22] Planet eBook, ePublishing & Converting, July, 2001 [referred 8.11.2001] <http://www.planetebook.com/mainpage.asp?webpageid=14&TBCategoryID=7>

[23] U.S Copyright Office, The Digital Millennium Copyright Act of 1998, Oct. 28, 1998 <http://loc.gov/copyright/legislation/dmca.pdf>

Analysis of E-book Security Guoyou He Helsinki University of Technology Telecommunications Software and Multimedia Laboratory Abstract E-book is a new publication technology raised in recent.Â Transcription. 1 Analysis of E-book Security Guoyou He Helsinki University of Technology Telecommunications Software and Multimedia Laboratory Abstract E-book is a new publication technology raised in recent years. It has a number of advantages for both providers and consumers. From the standpoint of providers, E-book can distribute publication in a large range efficiently and economically. From the consumers point of view, they can read E-books immediately, without having to wait for the title to be shipped to them.