Security Architectures for Controlled Digital Information Dissemination*

Jaehong Park Ravi Sandhu

The Laboratory for Information Security Technology (LIST)
ISE Department, MS4A4
George Mason University, Fairfax, VA 22030
{jaehpark, sandhu}@ise.gmu.edu, www.list.gmu.edu

James Schifalacqua†

SI International, Inc.
8484 Westpark Drive, McLean, VA 22102
jschifalacqua@si-intl.com, www.si-intl.com

Abstract

Besides securing transmission of digital information at lower layers, several application-level security solutions for controlled dissemination of digital information have been developed using cryptographic, watermarking or use-control technologies. These dissemination control solutions have been designed for different business purposes. Little research, if any, identifies security architectures for controlling or tracking digital information dissemination in general. The identification of such will provide a foundation for developing appropriate security solutions for organizations' secure dissemination of digital information, and provide a better understanding of current application-level security solutions.

In this paper, we identify eight application-level security architectures based on the following three elements: Virtual Machine, Control Set, and Distribution Style. Some of the architectures provide control and tracking capabilities for dissemination and usage of digital information, while others provide only tracking capability. We describe the architectures and compare their capabilities, merits, and demerits. In addition, we review briefly some of the required mechanisms, including watermarking and use-control technologies. Also, we relate some of commercial solutions to our security architectures in order to provide insight on the current availability of our solutions architectures.

1. Introduction

As we start the new millennium we find ourselves accustomed to the pervasive and convenient availability of digital information. The proliferation of inexpensive digital equipment (i.e. computers, network facilities, printers, scanners, cameras, and copiers) and the Internet has expedited this availability to a scale scarcely imagined a few years ago. Along with this digital revolution, unauthorized dissemination of digital content has emerged as one of the most problematic and challenging issues in information security.

Instances of this issue abound, and are divided into two types based on their purposes: Payment-Based Type (PBT) and Payment-Free Type (PFT). In PBT, a payment function is required in order to access digital information. In PFT, dissemination of digital information does not require payment, but must be controlled nonetheless to satisfy confidentiality or other security requirements. In this paper we focus on security solutions for PFT dissemination. Our solutions for PFT dissemination do not necessarily exclude support of payment functions. It may be possible to overlap payment functions onto PFT security solution architectures.

Unlike the Commercial mass-distribution environment, there are situations in which payment function is not required and higher distribution security is the primary concern. For example, in the Intelligence community digital information is often disseminated to organizations in various countries. The White House may wish to distribute a document in digital form to the South Korean government in such a manner that the received digital information is not revealed either intentionally or accidentally, to the North Korean government. Similar situations can exist in the commercial sector. In recent business-to-business (B2B) e-commerce, it is common for a hub organization to distribute information digitally to its several smaller partners. The challenge is to prevent further distribution of the digital information by the small partners to others. For instance, General Motors could disseminate several different technical descriptions in digital form to different suppliers who provide the specific parts of GM

* This research has been partially supported by Lockheed Martin Management and Data Systems at George Mason University.

† Work done while at Lockheed Martin Management and Data Systems.

motor vehicles. However, GM would like to prevent the leakage of digital information amongst suppliers regardless of their intention or possession of the digital information.

The characteristics of digital information of the PFT environment differ significantly from characteristics of digital information of the PBT environment. In the latter environment, a small amount of information leakage is acceptable and even desired [COX96][‡], while this may not be acceptable for the PFT environment. The number of legitimate copies of a single digital item in PBT is typically greater than that of PFT copies. In general, the objective in the PBT environment is to distribute as many copies as possible and to extract payment for each copy. In the PFT environment, it is the distribution itself which needs to be limited. Therefore, solutions and research for Payment-Based mass distribution purposes may not be directly applicable to the PFT environment, i.e. in Intelligence community or B2B Transactions.

In PBT, security breaches of digital assets result directly in financial loss. Re-distribution of illegally obtained digital information does not reduce its quality or worth to the consumer. Consequently, digital content providers have put much effort into protecting digital information from unauthorized distribution. However, no systematic study has been done for controlling digital information dissemination.

Hence, studies for more generalized security architectures that can provide secure environments for PFT digital information dissemination should be considered. Identifying generalized security architectures for controlled digital information dissemination is important in order to provide a cornerstone for developing proper security solutions that satisfy an organization's requirements for secure and controlled dissemination of digital information, as well as for better understanding the current application-level security solutions.

In this paper we first discuss security objectives, followed by security architectures, and the related mechanism. The objective section articulates "what to do" while the mechanism section addresses details about "how". The architecture section gives formal structural ways in which appropriate mechanisms can be implemented to achieve defined objectives. This layered approach provides a practical way to acknowledge, analyse, and develop effective security solutions. In addition, we apply some of present COTS solutions to our security architectures to show the commercial availability of our security solution architectures.

2. Security Objectives

Today in an organization, many documents and products are in digital form. They are often disseminated to other organizations by means of electronic transmission, floppy disks, or CDs. Many of these digital objects need to be well protected from accidental and malicious attacks, even when the digital information has left the control of the originating organization.

Consequently, *studies for controlling dissemination of digital information* have gained increasing attention from both commercial and non-commercial uses. Controlled dissemination of digital information means that the distributor or rights holder can control recipients' access to the digital information. The recipients of digital information need to gain access rights to access the digital information. Even after the access to digital information, there are certain restrictions, such as that the recipients cannot modify the digital information, or cannot apply print-screen, copy, and save-as functions to the digital information.

Because there may still be some undesirable leakage of digital information, in addition to the controlling mechanisms, additional *studies about tracking technologies for disseminated digital information* should be conducted. The tracking of disseminated digital information means the original distributor or rights owner can trace re-dissemination of the disseminated digital information, so as to find who has re-disseminated or from what place re-dissemination occurred.

The main objective of this paper is to identify a secure environment for digital information dissemination by defining the security architectures that can provide control ability on the disseminated digital information. Also, the security architectures should support tracking ability on the disseminated digital information. More specifically, proposed security architectures should make it difficult or useless for recipients to re-disseminate the received digital information if not authorized, regardless of their intention. In addition, they should make it difficult for new recipients to access the illegitimately re-disseminated digital information that they possess.

3. Security Architectures

In this section we identify several different security solution architectures for PFT, based on available technologies and commercial solutions. These architectures may or may not satisfy all the stated security objectives. The classification of these architectures has been done somewhat exhaustively to

[‡] In superdistribution, the electronic information itself is freely distributed to everyone who wants it. So copying is not restricted. Rather, copying and distribution are encouraged for marketing purposes. However, the electronic information is wrapped up with digital strings, and can be accessed only where special software (e.g. virtual machine on recipient's computer) is available. Also, electronic information usage is monitored and controlled by appropriate authorities.

cover all possibilities. Each architecture provides different advantages and disadvantages. This section defines these architectures based on the following three factors and discusses their merits and demerits in terms of our security objectives.

3.1 Three factors of security architecture

There are three major factors that distinguish the security architectures. They are *virtual machine (VM), control set (CS),* and *distribution style.* The combination of use of each factor results in different security architectures. For better understanding of these architectures, first we have to understand these three factors.

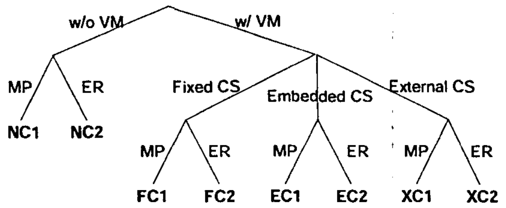
The virtual machine is software that runs on top of vulnerable computing environment and employs control functions to provide the means to control and manage access and usage of digital information. For instance, Adobe Acrobat Reader with Web Buy plug-in is virtual machine while Acrobat Reader alone is not virtual machine because it does not employ control functions to control access to digital content. The existence of a virtual machine on the client side is one of the most influential factors of the architecture, and it provides the foundation of use control technologies. It also implies the need for specialized client software.

The control set is a list of access rights and usage rules that is used by the virtual machine to control a recipient's access and usage on digital information. We recognize three styles of control sets: A *fixed control set* is hardwired into the virtual machine and applies uniformly to all digital information documents and all users. An *embedded control set* is inextricably bound to each digital document and is carried along with it. An *external control set* is separate and independent from the digital document (and can be transported separately or together with the document). Embedded and external control sets can apply different controls to each document and each user.

Message push (MP) and *external repository (ER)* are two possible distribution styles. In message push style, digital information is sent to each recipient. In external repository style, each recipient obtains the digital information from a dissemination server on the network.

3.2 Architecture Taxonomy

Based on these three factors, we identify eight application-level architectures for controlling and tracking dissemination of digital content. The following diagram illustrates the taxonomy of these architectures. We use the term "no control" to mean the lack of a virtual machine. The term "fixed control" means that the only control is that which is fixed in the virtual machine. The terms "embedded" and "external" control mean variable control as discussed above. They may coexist with fixed controls in the virtual machine.



VM: Virtual Machine
MP: Message Push
ER: External Repository
CS: Control Set

NC1: No control architecture w/ MP
NC2: No control architecture w/ ER
FC1: Fixed control architecture w/ MP
FC2: Fixed control architecture w/ ER
EC1: Embedded control architecture w/ MP
EC2: Embedded control architecture w/ ER
XC1: External control architecture w/ MP
XC2: External control architecture w/ ER

Figure 1. Security Architectures

Each of these architectures is described in the following sub-sections. Non-Encapsulated digital information dissemination architectures are described here as basic architectures for comparison purpose and only satisfy part of our objectives. Encapsulated digital information dissemination architectures are our main concern. Even though we have distinguished and defined these architectures, there can be real world security solutions that combine more than one security architecture. The diagrams for each of the architectures do not explicitly show encryption mechanisms or watermarking mechanisms. Encryption and watermarking mechanisms are required in all of these architectures.

3.3 Non-Encapsulated Architectures

3.3.1 No Control Architecture w/ Message Push (NC1)

No control architecture with message push (NC1) is a classic architecture for digital information dissemination. In this architecture, the distributor of digital information directly sends a copy of the digital content to each recipient. Each recipient stores the copy at his/or her storage device.

After distribution is done, the distributor has no direct means to control the distributed digital information, so the likelihood of deliberate re-dissemination or theft is increased. The recipient can either keep the digital information or delete it from his or her storage device.

After the digital information is deleted, there is no way for recipient to access the digital information. To access the saved information from multiple computers, the recipient needs to transport the information.

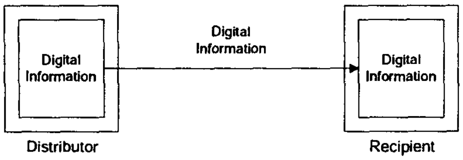


Figure 2. No Control Architecture with Message Push (NC1)

3.3.2 No Control Architecture w/ External Repository (NC2)

No control architecture with external repository (NC2) has similar features to NC1, except that in NC2 digital information is sent to an external repository server for distribution. A recipient must connect to the external repository to access and retrieve the digital information. Once a recipient has received the digital information, the distributor has no way to control or manage access rights or usage rights. Since this architecture does not have a virtual machine, there is no control set.

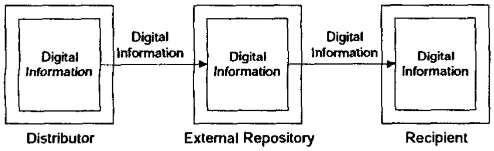


Figure 3. No Control Architecture with External Repository (NC2)

3.4 Encapsulated Architectures

3.4.1 Fixed Control Architecture w/ Message Push (FC1)

In the fixed control architecture with message-push (FC1), the control set is included in virtual machine. Since the control set is encoded into a virtual machine, the control set cannot be changed after the distribution of the virtual machine. Digital information is encapsulated in a *digital container* that does not allow the recipient to access digital information without using special application software (virtual machine). Therefore, a recipient only can access digital information through a virtual machine. Access is based on the control set encoded inside the virtual machine. This control set will contain rules which the virtual machine enforces, such as preventing storage of the cleartext digital information on the recipient's non-volatile storage. Re-dissemination of the digital container in this case would be accessible only by someone who has the virtual machine.

This architecture has the message-push distribution style. Each recipient must maintain the received digital container on his or her storage device for further access to it.

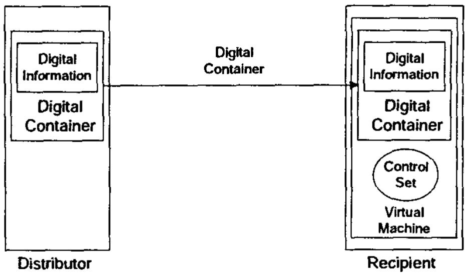


Figure 4. Fixed Control Architecture with Message Push (FC1)

3.4.2 Fixed Control Architecture w/ External Repository (FC2)

The Fixed control architecture with external repository (FC2) has basically same characteristics as FC1 except for the distribution style. In this architecture, digital information that is encapsulated within a digital container is sent to external repository for distribution. A recipient must connect to the external repository to access or download the digital container. The recipient can access digital information encapsulated within the digital container through a virtual machine using the control set encoded in the virtual machine. In general, architectures based on external repositories facilitate access to the information by a single recipient from multiple computers.

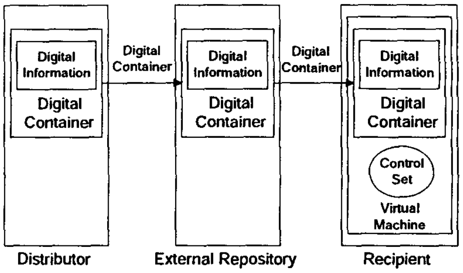


Figure 5. Fixed Control Architecture with External Repository (FC2)

3.4.3. Embedded Control Architecture w/ Message Push (EC1)

In the embedded control architecture with message-push (EC1), the control set is embedded in the digital information and always comes with the digital information within its digital container. The distributed digital information will be controlled based only on the pre-set access rights and usage rules on the digital information. Because there is no external control center function, the distributor cannot change the control set of the distributed digital information. In this and all subsequent architectures, the control set applied to the digital container may be in addition to a fixed control set in the virtual machine.

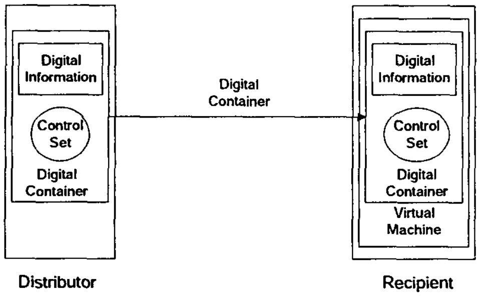


Figure 6. Embedded Control Architecture with Message Push (EC1)

After a recipient has received a digital container, he or she can access the digital information without any network connection, if he or she has proper access rights. This means that there is no additional access control (i.e. changing access rights after dissemination) for the distributed digital information. In addition, there can be only pre-set revocation. In other words, there is no revocation function available, which can be applied after distribution of the digital container.

In this architecture the control set can prevent storage of cleartext digital information on the recipient's non-volatile storage. Storage of the digital container by the recipient would be required for future access. However, the control set can prevent someone else from opening the digital container if it is re-disseminated to them.

3.4.4 Embedded Control Architecture w/ External Repository (EC2)

The embedded control architecture with external repository (EC2) also has fundamentally the same features as EC1, except for its distribution style. In this architecture, digital information is encapsulated within a digital container and sent to the external repository server. In addition to the controls that can be imposed in EC1, in this case the control set can further prevent the recipient from storing the digital container on the recipient's non-volatile storage. If the encapsulated digital container cannot be locally stored then this architecture enables the distributors to revoke a previously granted access.

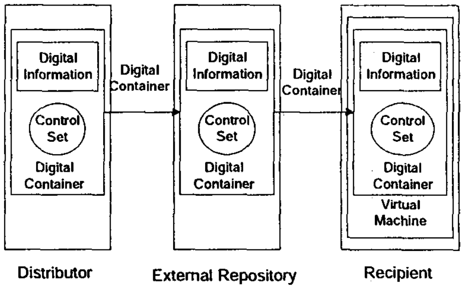


Figure 7. Embedded Control Architecture with External Repository (EC2)

3.4.5 External Control Architecture w/ Message Push (XC1)

In the external control architecture with message push (XC1), digital information is freely available in the form of digital container, but only those who have valid access rights can open the digital information in it. The recipient gets access rights by connecting to the *control center*. These access rights can be encapsulated in a digital container with or without the original digital information. This means that access rights can be distributed independently and that access rights can be encapsulated in a digital container with other digital contents that are not related to the access rights. In this architecture, distributors can control and manage recipients' access rights on the digital information, including causing the revocation of previously granted rights. Both senders and recipients must trust the control center.

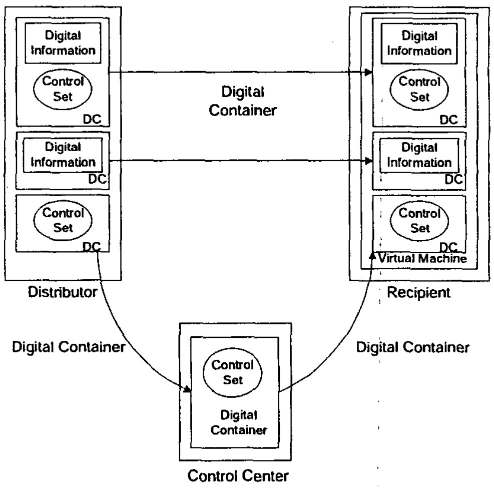


Figure 8. External Control Architecture with Message Push (XC1)

There are two options based on the usage rule information. In first case, every time a recipient wants to open an item of distributed information, he or she must access the control center. In second case, the recipient does not have to access the control center every time, but he or she should access the control center from time to time to get the proper usage rights, based on the usage rights policy. The recipient may have to access the control center based on the usage time, the number of access, or fixed time period. In latter case, there can be a one-time only connection to the control center if the recipient receives an unlimited (no expiration) set of access rights that do not require any further connection. The distributors should decide very carefully before distributing any control set that does not require any further connection, lest they forfeit their power to revoke access.

3.4.6 External Control Architecture w/ External Repository (XC2)

The external control architecture with external repository (XC2) has mainly the same characteristics as XC1 except that it includes an external repository. Encapsulated digital information is stored at the external repository for distribution. The information may or may not be freely available. This architecture can provide separation of content and access rights. This architecture may have four possible options based on the usage rule information. Note that there are two digital containers in this architecture. In reference to figure 9, the digital container at the top carries the digital information, whereas the one at the bottom only carries a control set. Each of these digital containers may or may not be storable by the recipient. This gives us four combinations as follows.

In first case, both the encapsulated digital information and the encapsulated control set can be stored on a recipient's local storage device. In this case, a recipient does not have to connect to either an external repository or a control center every time he or she wants to access the digital information. The recipient may have to connect to the control center from time to time to renew the control set (as explained in XC1). Alternately, only a one-time connection to the control center is all that is required for the recipient to access the digital information forever.

In the second case, a digital container that includes digital information is freely available, but the control set digital container cannot be locally stored. In this case, a recipient can save the encapsulated digital information in local storage and does not have to download it every time he or she wants to access it. However, the recipient must always connect to the control center to get the control set that is required to access the information. This case can be very useful when the size of the digital information is huge.

In the third case, the encapsulated digital information cannot be locally stored, but the encapsulated control set can be stored. Finally, in the fourth case neither digital container is locally storable. These last two cases may allow greater control over information dissemination. For example, the digital information can be completely withdrawn.

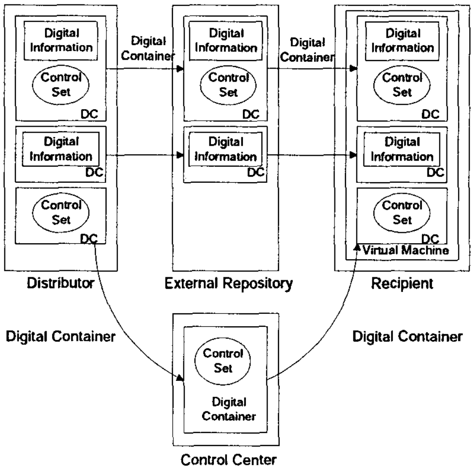


Figure 9. External Control Architecture with External Repository (XC2)

4. Related Mechanisms

Mechanisms are sets of technologies that support the solution architectures. Implementation of each of the architectures may require a different mix of mechanisms. In this section we give a list of mechanisms that are potentially useful in achieving the security objectives and goals. Use-control mechanisms cannot be applied to NC1 and NC2 architectures. Cryptographic techniques are not included here as unique dissemination control mechanisms, and they are typically used for the secure transmission of digital information, or as integrity protection mechanisms.

4.1 Watermarking Mechanisms

In most cases, digital watermarking means invisible watermarking. In some cases, a watermark can be divided into visible and invisible watermark. In this section, we consider only invisible watermarking, because visible watermarking is not applicable for our objectives.

Digital watermark, or fingerprint[§] is used to mark the identity of the objects (digital information) with information such as the author's name, recipient's name, distribution date, or usage rights. This is done to identify, rather than to protect the digital information from unauthorized access. Digital watermarking can thus provide a tracking capability to illicit distribution of digital information [KOB97, ZHA97]. Digital watermark (invisible) can only be detected by special software. In context of our project, digital watermarking technologies are required to enable tracking of disseminated digital information. The detailed description of the characteristics of digital watermarking technologies and linguistic techniques are out of our project scope. Watermarking mechanisms can be implemented into all of our security solution architectures.

Digital information can be in several formats such as text, image, audio, and video format. Watermarking technologies are dependent mainly on the type of digital information where the watermarks are to be stored. Each of image, video, audio, and text content needs different watermarking technologies.

The size range of digital information can vary widely, but the size needs to be large enough to facilitate watermarking. If this cannot be guaranteed, padding technologies may be needed. This issue is important because if the typical size of a type of digital information is too small (for example, small text email messages), there might not be any means to store watermarks in it, and then we cannot implement watermarking technology in our security solutions. The size of digital information also influences the security architectures. If the size of digital information is too big, downloading may not be a good way to access the digital information.

For tracking purpose especially, each copy of the originally disseminated digital information needs unique watermarking information (a "fingerprint") so as to identify the sender's and receiver's identities. Embedding different watermarking information in each copy of the originally disseminated digital content, however, is not yet realistic for cases of mass dissemination [DWO99].

4.2 Use-Control

The Use-Control mechanism is originally based on the superdistribution concept. As stated earlier, superdistribution is a concept that electronic information is available freely, but access to the information is controlled. In the use-control mechanism, digital information is encapsulated into a cryptographically protected electronic container called a *Digital Container*. This encapsulated digital information is only accessible by using special application software called a Virtual Machine, with approved access rights that are stored in a *Control Set*. This mechanism can be applied to all architectures except NC1, NC2.

4.2.1 Virtual Machines on recipients' computers

In the DVD industry, to prevent illicit copying and distributions, several security features have been developed (e.g. regional restriction, copy control restriction). These features are embedded in DVD players. Each DVD title is burned with one or more security configurations based on these features. Because of these security features, a DVD title can only be played or copied within its allowed restriction boundary.

Similarly, we can use a secure and tamper-resistant virtual machine (application software) on top of a vulnerable computing environment such as PCs. So, digital information can be only accessible within the virtual machine. By using a virtual machine, we can restrict the access privileges. For instance, we can disable the print function, save function, and save-as function within the virtual machine. Virtual machine mechanisms that reside on recipient's computer can be implemented in all architectures except NC1, NC2.

4.2.2 Digital Container

The digital container [SIB95, KAP96] is a key feature of use-control technologies. A Digital container is a tamper resistant electronic envelope that is designed to protect digital information and to control usage by wrapping it up with cryptographic mechanisms. Digital containers can be implemented using either a control set or watermarks for controlling usage rights. Control set technology is a typical configuration for digital containers while there are optional watermarking approaches.

- Controlling by using Control set

A digital container can contain digital information and control sets. A control set is a collection of usage rules and rights information. Control sets can be encapsulated in a digital container with or without digital information. For instance, when a recipient tries to access digital information, client software will check the control set to verify that the recipient has the correct usage rights.

- Controlling by using watermark

Instead of using a control set, there is another possibility to control access to digital information by using watermarking technologies. In this case, the digital container encapsulates digital information, which is watermarked with controlling information such as the

[§] A watermark is called a fingerprint when a watermark embedded in an object distinguishes the object from others uniquely.

recipient identity and usage rules. Client software will check the watermarks of the digital information and verify the authorizations and usage rights. If a watermark is used for the digital container, the digital container always includes digital information and watermark. So, usage rules cannot be encapsulated alone without digital documents. This means that digital information cannot be distributed independently from usage rules.

4.2.3 Control Center

In general, a control center exists for controlling and managing the access rights, usage rules, and even usage history. A control center holds security policies (control sets) that govern usage of digital information and a database of senders and recipients. Generally, the purpose of the control center is to provide access rights on digital container to correct users, so users can access the digital information. To achieve this, client application software (the virtual machine) will check the control set in a digital container or virtual machine, and if necessary, it will communicate with the control center for additional information such as granting access rights to certain digital information. In the commercial world, the control center can be also responsible for payment functions, access to the digital information can be granted/revoked based on payment.

5. Discussions

In this paper we have identified several possible security architectures for controlling the dissemination of digital information and tracking its re-dissemination, along with some required or related mechanisms to enforce the security architectures. In this section we analyze these architectures and give the findings of our study.

5.1 Solution Approaches

Our paper has focused on two major security objectives: controlling dissemination of digital information and tracking its re-dissemination. The fundamental ideas of these security objectives are as follows.

In a security perspective, there can be two types of attacks: identified attacks (known) and unidentified attacks (unknown). Figure 10 shows a logical diagram for security attacks and protections. By implementing use-control mechanisms in our security architectures, we have tried to protect digital information from these attacks. Our solution architectures with use-control mechanisms can protect known attacks and some unknown attacks. However, as shown at Figure 10, there can still be some other unknown attacks. These attacks are likely to break through our architectures and thus access the digital information. If this cannot be avoided, there should be well-defined methods to trace the attackers (and hence the watermarking techniques).

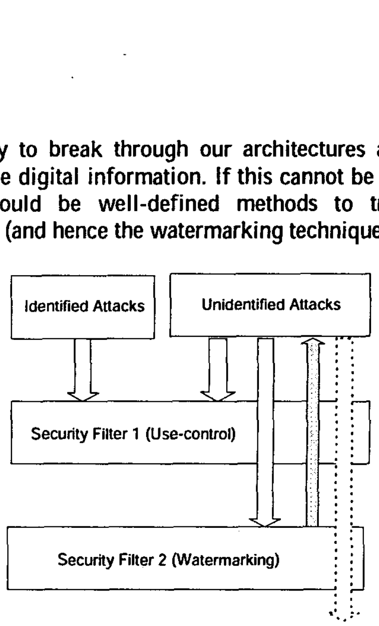

Identified Attacks
Unidentified Attacks
Security Filter 1 (Use-control)
Security Filter 2 (Watermarking)

Figure 10. Security attacks and protections

Security architectures with use-control mechanisms do not have any tracking features per se. However, in addition to use-control, by implementing watermarking mechanisms into our security architectures, we can achieve reasonable tracking methods. In Figure 10, the gray arrow shows tracking action using watermarking technologies. However, current watermarking technologies are still premature to guarantee the tracking of dissemination and re-dissemination of digital information. If the attackers have tampered the watermarked digital documents, the likelihood of successful tracking of watermarked information will be significantly reduced. The dashed line in Figure 10 shows those attacks that subvert watermark tracking.

In this paper, we have defined security architectures, which can include use-control mechanisms for protection of disseminated digital information (security filter 1), and also which can include watermarking mechanisms for tracking methods (security filter 2). Also, we have identified related mechanisms that can be implemented into the security architectures.

5.2 Characteristics of Security Architectures

We have proposed eight security architectures to accomplish our security goals. These security architectures have different characteristics. These characteristics are important features for choice of a security solution in a particular context. Table 1 shows security and functional characteristics of our security architectures. These characteristics can be merits, demerits, limitations, or requirements of the architectures, depending on the environment in which the architectures are deployed.

	Characteristics	NC1	NC2	FC1	FC2	EC1	EC2	XC1	XC2
C1	Disseminator can control access and usage of disseminated digital information			Y	Y	Y	Y	Y	Y
C2	Disseminator can change recipients' access rights after dissemination						Y	Y	Y
C3	Re-disseminated digital information can be protected			Y	Y	Y	Y	Y	Y
C4	Special client software (virtual machine) is vulnerable to attacks			Y	Y	Y	Y	Y	Y
C5	Tracking re-disseminated digital information is possible	Y	Y	Y	Y	Y	Y	Y	Y
C6	Disseminated digital container is reusable for other recipients by re-dissemination							Y	Y
C7	Digital information does not have to be on recipient's storage		Y		Y		Y		Y
C8	Digital information can be accessible from any machine if it is connected to network		Y		Y		Y		Y
C9	Recipient should carry digital information to access it from multiple machines	Y		Y		Y		Y	
C10	Special client software (virtual machine) is required			Y	Y	Y	Y	Y	Y
C11	In case of large digital information, download time can be significantly costly		Y		Y		Y		Y
C12	Every access to digital information requires network connection.								
C13	The architecture can be supported without network connection	Y		Y		Y			
C14	Control center trusted by both distributors and recipients is mandatory							Y	Y

Note: C1 ~ C5: Security characteristics, C6 ~ C14: Functional characteristics

Table 1. Characteristics of Architectures

5.3 Available COTS Solutions for the Architectures

The Table 2 shows the currently available COTS solutions which belong to one of our security architectures.

For Example, Adobe PDF Merchant & Acrobat Reader (v4.05) with Web Buy plug-in belongs to the first case of XC2. PDF Merchant generates a cryptographically encapsulated PDF file and a Voucher file. The encapsulated PDF only can be accessed through Web Buy plug-in. Acrobat Reader with Web Buy is Virtual Machine (VM) in our security architectures. Voucher file is Control Set (CS) in our architectures It grants the right to access the PDF. Both files can be stored at local storage. Therefore there is no network connection required every time recipients want to access digital content. It also provides an option for binding content to CPU ID, storage device ID, network ID, e-mail address, or time, so the recipients only can access within certain environments such as a specific hardware or time period.

Some of the architectures have not been used in any COTS solution because of their different security characteristics and functional characteristics.

Solution	Organization	NC1	NC2	FC1	FC2	EC1	EC2	XC1	XC2
PDF Merchant & WebBuy	Adobe								X
PageVault	Authentica							X	
SoftSEAL	Breaker Technologies								X
Confidential Courier	Digital Delivery, Inc.					X			
DocSPACE	DocSPACE Co.		X						
CIPRESS	Fraunhofer Institute for Computer Graphics & Mitsubishi Co.								X
Cryptolope	IBM							X	
InTether	Infraworks Co.					X			
InterTrust	InterTrust Technologies Co.							X	
RightMarket	RightMarket.com Inc.							X	

Table 2. Architecture of COTS solution

6. Conclusion

In this paper, we first identified our security objectives. We then identified eight security architectures for our security objectives: to provide a PFT secure environment for controlling digital information dissemination and tracking its re-dissemination. Each architecture's main characteristics, merits, and demerits have been discussed. We described some related mechanisms such as watermarking technologies, and use-control technologies that can be implemented in these security architectures. In addition, we have related our security architectures to COTS solutions to show commercial availability of the security architectures.

The study performed in this paper is the first systematic study of this topic. In particular, the architectures we have identified have not been previously defined in this manner in the literature. Also the security objectives and mechanisms have not previously been so clearly articulated. Nevertheless, this paper is fundamentally a starting point. It provides the basis for future research and development for controlling and tracking dissemination of digital documents. Further research on our architectures and mechanisms will lead to practical solutions for our security objectives.

This paper has focused only on Payment-Free Type digital information dissemination. Even though our solutions may also provide the basis for Payment-Based Type solutions, different objectives may require different security solutions.

References

[COX96] Cox, Brad. Superdistribution, MA: Addison Wesley, 1996.

[DWO99] Dwork, Cynthia, Copyright? Protection?, The Mathematics of Information Coding, Extraction, and Distribution, The IMA Volumes in Mathematics and its Applications, vol. 107, pp. 31-47, 1999. NY: Springer-Verlag.

[KAP96] Kaplan, Marc. IBM Cryptolopes, Superdistribution and Digital Right Management, 1996, Online, Available: http://www.research.ibm.com/people/k/kaplan/cryptolope-docs/crypap.html.

[KOB97] Koblin, Jens., Kockelkorn, Michael. The IMPRIMATUR Multimedia IPR Management System, 1997, Online, Available: http://www.imprimatur.alcs.co.uk/newstore.htm.

[SIB95] Sibert, Olin. et al. The DigiBox: A self-Protecting Container for Information Commerce, In Proc. of USENIX Workshop on Electronic Commerce, New York, July, 1995.

[ZHA97] Zhao, Jian. Applying Digital Watermarking Techniques to Online Multimedia Commerce, In Proc. of the International Conference on Imaging Science, Systems, and Applications, Las Vegas, June, 1997.

— *Notes* —