International Journal of Advances in Computer Science and its Applications – IJCSIA
Volume 4 : Issue 1 *[ISSN 2250 – 3765]*
Publication Date : 09 January 2014

Data Leak Prevention Using a New Hybrid Security Model

[Kamran Morovati, Sanjay Kadam]

***Abstract*: This paper introduces a new security model which reduces the risk of unauthorized data disclosure in an organization's network. This model will protect confidential information against unauthorized disclosure. The model is effective at preventing intentional and/or unintentional data propagation (e.g. by a disgruntled employee or by means of malware, etc.)**

The proposed model is a combination of traditional cryptographic-based security methods and Meta-data embedding. The model uses the public key infrastructure cryptosystem and document watermarking technique to attach auxiliary security features (e.g. hash value) into the sensitive documents in order to prevent users from disclosing them without authorization.

***Keywords*— Data Leakage Prevention, Public Key Infrastructure, Digital Certificate, Document Watermarking, Security Models.**

I. Introduction

In cyber security, information leakage means unauthorized transmission of data (or information) from within an organization to an external destination or recipient. The data leakage may happen intentionally by a company's employees who have authorized access to an organization's network, system, or sensitive data or it may happen inadvertently due to an employee oversight or more commonly through a malware attack. An insider threat is known as one of the most important causes of confidential data breach. Simply put, 'insider threat' means the exposure of proprietary or confidential information of the company or organization by dishonest employees from within the company itself. Valuable data such as the source codes, financial or medical records, trade secrets or more mundane items such as company strategies and future business initiatives can be exposed, allowing competitors to gain an unfair advantage in business operations. Many insiders who stole or modified information were actually recruited by outsiders, including organized crime, foreign organizations or governments. (1)The insider threat is a major problem that organizations must be aware of and proactively prevent since it may result in data leakage and security breaches.

Kamran Morovati (IRAN)
Computer Science Department, Pune University
k.morovati@gmail.com

Sanjay Kadam, CDAC-Pune (INDIA)
Computer Science Department, Pune University
sskadam@cdac.in

The threat is attributed to legitimate users who abuse their privileges, and given their familiarity and proximity to the sensitive data, can easily cause significant security violation. In an organization's network, the focus is mainly on guarding the perimeter since external attacks have a higher incidence. Consequently, internal resources are left largely exposed with only the basic access control mechanisms. Due to the lack of tools and techniques, security analysts do not correctly perceive the threat, and hence consider the attacks as unpreventable.

II. Background

This section briefly describes the concepts and techniques that we have used in our proposed model:

Cryptography is the art of secure data communication between two parties in the presence of adversaries. It has two main categories:

1. Symmetric cryptography: Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key.
2. Asymmetric cryptography: Also known as *public key cryptography* refers to a cryptographic system requiring two separate keys, one of which is secret (private key) and one of which is public (public key). Although both keys are mathematically related, it is computationally infeasible to deduce the private key from the public and vice versa.

A *key* is a binary value that works with a cryptographic algorithm to produce a specific cipher text. Keys are very huge numbers, which are measured in bits. In cryptography, the bigger the key means the resultant cipher text is more secure.

A *hash function* **H** is a transformation that takes a variable-size input **m** and returns a fixed-size string, which is called the hash value **h** (that is, **h = H(m)**). The basic requirements for a cryptographic hash function are:

1. The input can be of any length.
2. The output has a fixed length.
3. **H(x)** must be one-way which means that given a hash value **h**, it must be computationally infeasible to find some input x such that **H(x) = h**.
4. **H(x)** must be collision-free. That is to say, it must be computationally infeasible to find any two messages x and y such that **H(x) = H(y).**

A *digital signature* is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such

that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). (2) Using PKI, the private-key signs (creates) signatures, and the public-key verifies them. Figure 1, illustrates the process of digital signature creation and verification.

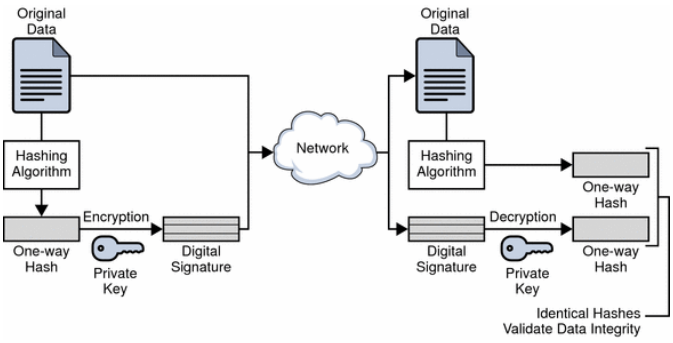

Figure 1: Digital Signature Creation and Verification[i]

One issue with PKI cryptosystems is that users must be constantly vigilant to ensure that they are encrypting to the correct person's key. In a public key environment, it is vital that you are assured that the public key to which you are encrypting data is in fact the public key of the intended recipient and not a forgery. (3) A *digital certificate* solves this problem. A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity (information such as the name of a person/object, their address, etc.). The certificate verifies that a public key belongs to an individual. X.509 is the most common standard for producing digital certificates. It has a fairly flexible format hence it could be issued for various purposes. Table 1, shows the general fields of a X.509 certificate.

Version Number
Certificate Serial Number
Signature Algorithm Identifier
Issuer X.500 Name
Validity Period
Subject X.500 Name
Public Key Information
Public Key Value
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Certification Authority's Digital Signature

Table 1: Structure of X.509 Certificate (version 3)

A *watermark* stored in a data file refers to a method for embedding/attaching auxiliary information to the original data for many reasons such as tamper detection, message authentication, ownership proof, copyright protection and traitor detection. Digital watermarking enables companies and owners to embed a unique digital ID into confidential documents. The data contained in the watermark can include security features such as the recipients of data or an advanced access control list (ACL). Therefore, use of digital watermarking could help in sensitive data dissemination deterrence or any information that is inadvertently or intentionally leaked out is easily traceable. Additionally, companies can use network detectors and email filters to check for digital watermarks within documents and images, providing notification if an attempt is made at uploading to the web or forwarding via email outside the company.

III. Current Data Leak Prevention Techniques

Data leak/loss prevention (DLP) is an approach to ensure that end users do not send sensitive or critical information outside of the corporate network. The term is also used to describe tools that help a network administrator control what data end users can transfer. Most of the available data leakage prevention (DLP) techniques are based on the monitoring, logging, network traffic analyzing and access control based countermeasures. Nowadays, many data loss prevention solutions are available in the market, which work based on the aforementioned techniques. However, they generally lead to inconvenience because of their high false alarm rate.

Technically current DLP solutions are classified as the following (4):

a) Network-Based DLPs focus on protecting data while it is in motion. Network-based DLP solutions are installed at the 'perimeter' of enterprise networks. They monitor network traffic to detect sensitive data that is being leaked or sent out of the enterprise. Solutions may investigate email traffic, instant messaging, social media interactions, web 2.0 applications, SSL traffic and more. Their analysis engines are looking for violations of predefined information disclosure policies, such as data leaks.

b) Storage-based DLPs focus on protecting data at rest within an organization's datacenter infrastructure such as file servers, SharePoint, and databases. These DLP solutions discover where confidential data resides and thereby enables users to determine why it is there. When confidential information is resident on insecure platforms it is usually an indicator of problematic business processes or poorly executed data retention policies.

c) End-point based DLPs focus on monitoring end point systems (laptops, tablets, POS, etc.) for all actions such as print or transfer to CD/DVD, webmail, social media, USB transfer, and more. End-point based solutions are typically event driven in that the agent resident on the end-point is monitoring for specific user actions, such

[i] Image depicted from: http://docs.oracle.com/cd/E19852-01/820-0382/aakfx/index.html

as sending an email, copying a file to a USB, leaking data or printing a file.

d) Content-aware DLPs address the risk of accidental exposure of sensitive data outside authorized channels, using monitoring, blocking and remediation functions. These tools enable the enforcement of company policies based on the classification of content.

In network based DLPs, two common architectures (5) that can implement data extrusion prevention include:

I. Use of a proxy server that views traffic on a specific protocol on a specific port (Application Layer of the OSI model)

II. Use of a network sniffer that observes all traffic at the network layer (Data Link Layer of the OSI Model.)

According to (6), data leakage prevention can be viewed from different perspectives. Technology based mitigation may include methods such as the secure content management and filtering approaches while data classification and user education could be considered as policy and process based mitigation.

In (7) a new security model according to the theory of insider threat assessment is presented. First, a modeling methodology which captures several aspects of insider threats has been described and subsequently, a threat assessment methodology to reveal possible attack strategies of an insider is proposed.

Theraography (patented by Advestigo[i]) is another helpful data filtering mechanism. It is a new content recognition technology based on the extraction of an information summary from multimedia content. It can be applied to a variety of file formats to generate a digital "fingerprint" based on file content. Content fingerprints are independent of file types and encoding. In this way, a document is represented by one or more fingerprints which allow all or parts of the content to be traced even after substantial modifications - cut and paste into other documents, changes of format or coding, additions or deletions.

The above mentioned solutions can mitigate the data leakage problem partially. For instance, most of the DLPs cannot sniff encrypted traffic so using cryptographic methods may simply bypass the DLP. As an example DLP solutions cannot prevent an information security vulnerability or attack like SQL Injection. Therefore, the need for further research in this domain is obvious.

IV. A Hybrid Security Model to Prevent Data Exfiltration

In this section, a new hybrid security model has been presented which effectively prevents company employees from unauthorized propagation of confidential data. The cornerstone of this innovative approach is the full integration and verification of security policies into the sensitive files that are intended to be protected. After identifying the sensitive files, a particular unit known as watermark control center (WCC) which will be discussed later, attaches additional security meta-data (watermark) such as an advanced access control list and the hash value of the document to the critical file, so it travels with it while the file is in-use (endpoint actions), in-motion (network traffic) or at-rest (data storage). WCC solves the problem of the metadata attachment and the information authentication based upon that metadata detection.

Many different data structures can be employed to attach the auxiliary data. In our model, we suggest adding metadata through the attachment of a customized digital certificate to the critical files. The extension field in X.509 (version 3) standard can store our extra security features. After being signed by the WCC's private key, this attached certificate can play the role of a digital watermark for tracking the important files. In our scenario, there is no need to make pair keys for sensitive files, instead only the public key of the WCC center will be mentioned in digital certificates.

The big advantage of using WCC's digital signature is that recipients can verify the file's authenticity and integrity simply by receiving the signed file.

Adding the Metadata

A digital watermark provides a guarantee that the digital data has not been tampered with and has come from the right source. It is created by embedding extra information, commonly in the form of digital patterns, into the computer files containing information which should be protected. For these watermarks to be effective, they need to be arranged in such a way that any attempt to remove or alter them is infeasible. In abstract view, the digital watermarking workflow consists of three activities. (8) Figure 2 illustrates the work flow of document watermarking.

Figure 2: Three phases of document watermarking

Embed: At one or more locations in the distribution channel, a digital watermark (digital certificate) must be attached to the sensitive files. In our model the watermark can be added to the source files at any point in the distribution chain such as completion of an authorizing transaction or further reproduction or distribution of the content. In the model the watermark control center (WCC) is the only authorized unit to perform watermark creation and embedding.

Detect: The counterpoint to Embed is the Detect phase, which forms the foundation for subsequent actions. The watermark could be detected at one or more locations in the content distribution workflow and in our model the detection can take place in the WCC or the company's gateway firewall.

[i]http://trademark.markify.com/trademarks/ctm/theraography/004282885

Response: Once detected, a wide variety of actions could be taken. In our case, the file sharing can be granted or the file may get dropped.

In our proposed model, the role of certificate generation, attachment and detection has been given to a particular unit known as the Watermark Control Center (WCC). According to the company's security policy, the WCC creates and attaches the watermarks into confidential files. This watermark includes additional information such as the document hash value, which preserves the document integrity, and a customized access control list, which shall determines whether the document can cross the organization gateway or not. WCC signs the document and the watermark with its private key.

The public key of the WCC is known to the users and also it is included in the certificate itself to prevent the use of fake keys. Hence, the users can decrypt the confidential data and the watermark if they have proper permission. The WCC private key is secret; therefore, no one else can create or alter the watermarks. This ensures that the watermark embedding cannot be done by anyone except the WCC.

In short, this procedure allows trusted users to access sensitive data, but on the other hand, it also hinders unauthorized data exfiltration. That is to say, although users may have access to data, it does not mean the data can be sent out without the necessary clearances (embedded in the watermark). In this scenario, an application layer firewall must be installed on the gateway to prevent the transmission of any document without watermark information. It also checks watermarked documents for proper permissions to decide whether they can leave the organization's network or not. Figure 3, illustrates the main components of our model.

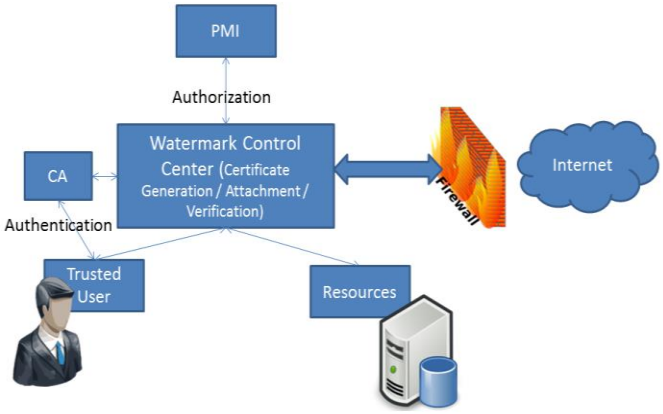

Figure 3: Components of the proposed data extrusion prevention model

The document protection procedure can be viewed as follows:

1. The user shows his identity to the access control module of the system and submits his request for resources to the WCC. (Both sides of information transmission including the information requestor and the information provider must have a valid digital certificate from Certificate Authority and subsequently their own public key and private key for data encryption and decryption)

2. After successful identity verification, the system confirms the authority of the trusted user to acquire the resource, and then provides the requested data (permission management). In this step, WCC investigates user privileges for the requested resource from Permission Management Infrastructure.

3. If the user is authorized to access the document, WCC generates a proper certificate according to a predefined security policy for the requested resource.

4. WCC signs and attaches the certificate first with his private key and then with the corresponding user's public key to ensure only the requesting user can decrypt the document. This ensures that data will not eavesdrop in between.

5. The user can access his requested files, but since the WCC's private key is secret, no one can create or alter the watermarks. On the other hand, the embedded message digest (hash fingerprint) in the watermark ensures that the digital watermark cannot be used for other documents.

Security Analysis

In a nutshell, the integrity of files is granted through the calculation and verification of the message digest which has been embedded in the watermark. The confidentiality of files is granted by employing PKI and finally the use of a digital signature grants the non-repudiation.

Conclusion

Data leakage perpetrated by insiders is a long standing security problem, but so far not much of an attempt has been done to counter the threat. The best security solution takes a layered approach, where complementary technologies are layered together to form a more complete defense. Digital watermarking and encryption provide the best security when working together. This paper presents a new hybrid security model which is effective in preventing illegal data extrusion that may be perpetrated by company insiders. This model integrates both a traditional cryptographic based security model and a document watermarking technique.

Future research may include the implementing and testing of access control mechanisms such as Role Based Access Control (RBAC) or the Chinese Wall security model in a network environment to prevent data leakage. Organizations may utilize other dissemination deterrence methods such as fingerprint analyzers and other metadata readers in addition to watermark detection and response techniques. This combination could empower the aforementioned data leakage prevention system.

Acknowledgment

A special thank of ours goes to Ms. Amy Da Silva for her editing assistance.

v. Bibliography

1. **Silowash, George, et al., et al.** *Common Sense Guide to Mitigating Insider Threats 4th Edition.* s.l. : Carnegie Mellon University, December 2012.
2. Digital signature. *Wikipedia.* [Online] August 10, 2013. http://en.wikipedia.org/wiki/Digital_signature#Definition.
3. Introduction to Cryptography. *PGP 6.5.1 documentation.*
4. **Glynn, Fergal.** Guide to Data Loss Prevention, Data Loss and Data Leakage. [Online] veracode. http://www.veracode.com/security/data-loss-prevention.
5. **Etue, David.** *Getting to Extrusion Prevention* . s.l. : Fidelis Security Systems, 2006.
6. *Data Leakage - Threats and Mitigation.* **Gordon, Peter.** s.l. : SANS Institute, 2007.
7. *Insider Threat Assessment: Model, Analysis and Tool.* **Ramkumar Chinchani, Duc Ha, Anusha Iyer, Hung Q. Ngo, and Shambhu.** s.l. : Springer, 2005.
8. **Group, P2P Digital Watermark Working.** *Digital Watermark Technologies, Applications in P2P Networks.* s.l. : Digital Watermarking Alliance (DWA).

About Authors:

Kamran Morovati is a senior network administrator and information security researcher. He is a Ph.D. candidate (computer science) in Department of Computer Science–University of Pune. He has a M. Tech. in Information Technology from Amirkabir University (Tehran Polytechnic) and BE in software engineering from Samsipour University of Technology (Tehran). His research interests include Information Security, Computer Networks, Soft Computing and Data Mining.

Dr. Sanjay Kadam works as a Joint Director in the Evolutionary Computing and Image Processing Group at C-DAC, Pune. He has a M. Sc. in Mathematics from Pune University, an M.Tech in Computer Science from IIT, New Delhi, and a Ph.D. in Computer Science from the University of London. His research interests include Image Processing, Parallel Processing, Neural Networks, and soft computing.