Global Research Review in Business and Economics [GRRBE]

ISSN (Online) 2454-3217, ISSN (Print) 2395-4671
| Open-Access | Volume 8, Issue 02,
Pages 31-36 ||2022||

Data Confidentiality and XML Security Labelling

Asst.Prof. Dr. Nevzat Ünalan
Ufuk University, Vocational School, Ankara / Turkey

ABSTRACT

The aim of the study; is to emphasize the importance of security labeling to find a solution to the security problems that arise as a result of the electronic forms replacing traditional papers, and the need to ensure that not only the data itself but also the channels through which it is transmitted are secure.

Methodology; the study was conducted as a literature review questioning XML, labelling, XML security labelling and reviews were made on published books, articles and periodicals.

The findings of the research; the security labeling covers the principles of labeling, change management and processing, the electronic security label should have the information of the target environment where the data is intended to be transmitted, it should be shown that the integrity of the security information is not compromised when the data needs to be transferred between different security domains, the basis of the data confidentiality degrees is labeling, It reveals that electronic signature and timestamp are also used in evolved mechanisms.

As a result, security labelling and data protection should be handled with standard approaches that support data exchange between domains without affecting corporate security principles, newly developed technological concepts, and security features.

KEYWORDS- Confidentiality, Data, Labelling, Security, XML

1. INTRODUCTION

Attempts of business as well as administration processes dematerialization are mainly seen through introduction of electronic form replacing the traditional use of paper-based documentation. While issues of electronic form sustainability, usability, readability, accessibility, and integrity have already been addressed by various organizational and technology approaches, security labelling is becoming one of the most important research topics in the recent time. Technical approaches as well as technology recommendations have been introduced in the past with the proliferation of use of electronic messages and electronic messaging systems. Not only the data itself, but also the network on which the data is carried, must be secure. Therefore, it is necessary to find technical solutions that support the change of security parameters to prevent unauthorized disclosure of data located on different security networks.

Data security classification can be defined on various levels. National organizations follow internal or national wide classification policies, which are dictated by the laws implemented. The other international security organizations must follow common rules of interpreting security classification, while in business sector, security classification is a matter of internal policy when not dictated by the legal framework such as privacy protection laws.

It is necessary to take measures for the security of the data exchanged in an uncontrolled environment such as the Internet, the most important issue for this is the mutual understanding of the security measures taken by the parties making the data exchange and the secured data. One of the most important issues is the correct understanding of the security data classification information between the intermediary parties.

Although the degrees of secrecy can be easily used by the national defense units and can be regulated by law, when they are not placed in a legal framework in business life, they cannot go beyond the internal security policies of the companies. A framework that includes rules and techniques to define the degree of confidentiality of data should be essential among the units that will make secure data exchange.

Comprehensive studies are carried out on security studies, from simple data transmission to complex service-oriented infrastructures on data networks. New data formats such as XML are being created to support the SOA concept, efforts are underway to meet the security needs of multiple networks and to set standards for data processing and data security marking. Various standardization initiatives have already been undertaken to meet these requirements, such as RFC 2634 Advanced Security Services, FIPS 188 Standard Security Label for Information Transmission.

He introduction of the paper should explain the nature of the problem, previous work, purpose, and the contribution of the paper. The contents of each section may be provided to understand easily about the paper.

1.1 Methodology

The study was carried out as a literature review questioning XML, labelling, XML security labeling, and reviews were carried out on published books, articles, and periodicals.

2. DATA, INFORMATION AND KNOWLEDGE

Table1. The Data, Information and Knowledge

Data	Information	Knowledge
Symbols, Numbers	Statistical Tables Graphs	Encyclopedia, Book, Annual Statistics
Raw facts, Unprocessed figures	Processed data, Associated data	Organized information
	Who? When? Where? What?	How? (How will data and information be used?)
	External Objective	Internal (Personal) Subjective
Unstructured, Unintelligible facts and observations	Processed Data Associated Data	Knowledge is information which is organized, designed, and made meaningful by the reflection and synthesis of the human mind.

Descripted above table, data is one of the inputs of information. As it is known, the first stage of the scientific method is observation in ancient times, in the new age, and in the age of information. Data are raw symbols and numbers consisting of unstructured, meaningless observations.

Information is statistical tables and graphs made up of processed and associated data. Knowledge is a formalized information which is organized, designed, and made meaningful by the reflection and synthesis of the human mind (Osuga, S. et al., 1990).

3. DIGITAL DOCUMENTS, EXTENSIBLE MARKUP LANGUAGE AND SECURITY LABELLING

3.1 Digital Document

Documents produced through digital tools such as criminal records, stored under appropriate conditions by verifying with data matrix, barcode, verification number, stored for a long time or destroyed when the time comes are electronic documents. For an electronic document to be accurate and reliable, its content, context and structural elements must not be changed. In this context, information security is to protect the confidentiality, integrity, and usability of information, to preserve originality, accountability, non-repudiation, and reliability (ISO / IEC 27000: 2009). It is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and usability (CNSS, 2010)

3.2 Extensible Markup Language, XML

Extensible Markup Language (XML) is a data communication standard designed by the W3C (World Wide Web Consortium), a markup language that standardizes communication between platforms, enabling data exchange over the internet.

Before the emergence of XML technology, when the data in a database was transferred to another platform, it could not be carried out efficiently, in an accurate, holistic, and intact manner, and data transfer took a long time. XML technology developed to eliminate these negativities made the data flow between different systems and platforms carried out within a certain standard framework (Oudkerk and Bryant 2010, p.22.2).

Today, XML technology provides services in many areas such as transferring databases, organizing file systems, collecting financial data, and storing scientific content.

3.3 Labelling

The basis of data privacy degrees is labeling, which indicates elements such as database records, documents, data sources and data channels and must include:

- classification level,
- identification of data entity,
- identity of the person who owns the security tag,
- creation and storage time,
- identity of the person responsible for the security tag,
- audit trail and change log

One of the most important additional parameters are security policies references, such as security policy of originating domain in which a security label was originally created. When exchanging security classified data, it is of utmost importance to understand security parameters of originating domain and support proper interpretation when processing security label in targeted domain. Classification levels may differ from domain to domain and proper interpretation is needed when processing a label and associated data. Same principles may apply when security labels are used in private sector, such as confidential classification of data exchanged between enterprises.

3.4 Electronic Security Labeling

Three essential elements for electronic security labeling are labeling, change management and processing Fundamentals (Bridges and Jones, 2013);
Labelling – defines classification levels, classification marking rules and classification parameters,
Change management – interprets lifecycles of electronic labels and management of lifecycles including audit trails,

Processing instructions – defines electronic label relations to security policies of originating and targeted domain and security processing rules.
Technical as well as organizational approach must follow the above three basic principles when defining a syntax and processing rules of a security label.

3.**5 Security Label Requirements**

Examples of security services that may use security labels are a label-based access-control service, data integrity and/or data confidentiality service or non-repudiation of origin. Security attributes are attached to a data object, which can come in the form of a document, message, image, a communication channel, or any kind of embedded data. Electronic security tagging must meet multiple security field data exchange needs. An electronic security label should also have information of the target medium to which the data is intended to be transmitted (Sankari and Bose, 2014)

Examples of security services that can use security tags are tag-based access control service, data integrity, data privacy service or non-origin denial readability is preserved. Moreover, it is necessary to show that security components can change their original domains or even change over time, and that the integrity of the security information is not compromised when transferring between different security domains. It is essential to provide appropriate tools for changes and log audits and to develop supportive mechanisms for the propagation of changes in multi-domain environments.

General requirements for security labels;

- Deals with information, data objects and data communication channels,
- Keeps information about the security classification,
- Support for security attributes change management in multi-domain environments,
- Supports structured data object and machine processing,
- It supports the authenticity and integrity of the data.

Same as classified data, security labels may face change of content during the lifecycle. Classification level of a document may change from highly secret to classified category and such changes must be properly interpreted with the security label. Furthermore, security label mechanisms must propagate such changes through the whole infrastructure to where the original classified document was delivered in an efficient and trustworthy manner.
Whether the security label is embedded in the document or outside the document and in detachable form, a change to the confidentiality level of the document must be announced to make changes in other copies of the document. Changes made to the security principles of the source or target environment, which do not directly affect the security labeling, must also be included in the change management.

Confidential data can be shared in different security areas, and these security areas have their own consistent security principles. For the confidential data to be sent from the source area to the target area, the issues that the target area must meet;

- Processing the security label content,
- Determining a security basis associated with the security label,
- Acting on the security label and security principles.

Before sharing confidential data, it is necessary to understand the security principles of the target area and confirm that the adequate security level is met. If the target area does not meet this level of security, additional measures should be implemented to prevent data disclosure, such as the use of security guards.

3**.6 XML Security Labeling**

Meeting these requirements calls for introduction of an advanced, interoperable, and open syntaxes for security labelling. XML encoded security labelling proposes a format for expressing security labels using the XML. XML security tagging has replaced old data representations and formed the basis of new data manipulation techniques. Advanced, mutually intelligible, and public syntax must also be created to meet security needs (Thümmel and Eckstein, 2006)

The XML format replaces unstructured data representations such as many currently available ASN.1 and is the basis for a number of new data processing techniques, such as web services (WS), which are integral elements of service-oriented architectures (SOA) (Nadalin, 2006).

Security tags often carry access control information that is read by border control elements during the transition between two security areas. The XML format, on the other hand, is a generic method implemented by securely overlaying security information onto data objects

It is evaluated that the XML format will be compatible with the data object types that will emerge in the coming years. XML is supported by security standards such as cryptographic key management, encryption, electronic signing, access control. XML security tagging benefits from the growing community of XML standards-setting and easily adapts to existing technologies required for inter-domain communication.

The structure of XML security labels includes four basic elements: data classification attributes and attributes management, attributes processing rules, label binding information and label integrity demonstration. Classification information and bindings are the essential elements of XML security labels. An XML label may come in a form of an integral part of a structured data object or may simply present detached data object that is managed centrally and is exchanged between domains independently of classified data objects. A label can be associated with more than one data object and must support enough information for integrity (and authenticity) demonstration. For this purpose, XML digital signature syntax is used which supports referencing mechanisms label integrity and unambiguously links data object with security attributes using cryptographic mechanisms using strong hash and encryption algorithms (Eastlake at al, 2002).

XML security label include the following basic structure;

- Classification, category – defines classification level and author or owner of a security label,
- References – define unique or global relation to classified data,
- Audit trail – interprets changes of label lifecycle.
- In addition, a security label may also support the following information:
- Security policy – a reference to a policy on which creation of security label is based,
- Processing rules – supporting information for processing of a security label and classified data,
- Visualization – support for human readable format of security label content,
- Security assertions – information supporting security label ownership as well as security label authenticity, integration, and time existence (Blazic, 2010, p.4).

4. CONCLUSION

Confidential and private data of many people are kept and processed daily by public institutions and organizations in the finance, banking, education, health, and defense sectors, as well as the private sector. With the transfer of these written data from paper to electronic media over time, the processing, management, and security of personal data has gained a different dimension. The security of electronic data, which has increased rapidly in recent years, is defined as one of the most important technological challenges of today due to the difference of both environments.

A customized view of XML documents is enabled based on a security policy, and security tags are applied to XML nodes used by the security server to determine access to nodes within the document. An XML parser is an object manager that enforces access decisions on each XML node and on each transaction.

The use of XML format takes advantage of basic communication techniques in service-oriented architectures and has an impact on cross-domain solutions such as SOAP communication protocol introduced with web services. Furthermore, it can rely on XML based techniques for access control and security assertions management. An XML label can include security attributes for several data object or can bind to only a part of a structured document. Using detached security label type, data object is unaffected and may be handled through communication infrastructure independently from associated labels. Data disclosure is controlled on the fly and may affect only parts limited amount of data elements of a structured data object. Security attributes change management is performed centrally and expected changes can be propagated instantly through targeted domains (Blazic, 2010, p.6). The authenticity of a security tag can be demonstrated at any time using XML based long-term integrity techniques such as Evidence Record Syntax (ERS).

As a result, security labelling and data protection should be handled with standard approaches that support data exchange between domains without affecting corporate security principles, newly developed technological concepts, and security features.

REFERENCES

1. Blazic A.J (2010), XML Based Security Labelling, SETCCE, Slovenia
2. Bridges R., Jones C. (2013) Automatic Labeling for Entity Extraction in Cyber Security, Computational Sciences and Engineering Division Oak Ridge National Laboratory, Oak Ridge, TN 37830
3. Eastlake D., Reagle J., and Solo D. (2002) “(Extensible Markup Language) XML-Signature Syntax and Processing,” IETF RFC 3275, 2002
4. Nadalin A., Kaler C., Monzillo R., and Hallam-Baker P., (2006) “Web Services Security: SOAP Message Security 1.1 (WS-Security 2004),”
5. Osuga, S. et al. (1999) Knowledge Acquisition, Moscow, Mir, 1999 (in Russian)
6. SO / IEC 27000 2009 (E). (2009). Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Genel bakış ve kelime bilgisi. ISO / IEC.
7. Oudkerk S., Bryant I. (2010) A Proposal for an XML Confidentiality Label and Related Binding of Metadata to Data Objects, Norwegian Defence Research Establishment – FFI)
8. Sankari S., Bose S. (2014) Secure XML labeling for efficient XML content dissemination 2014 Sixth International Conference on Advanced Computing (ICoAC)Thümmel A., Eckstein K. (2006) "Design and Implementation of a File Transfer and Web Services Guard Employing Crypto-graphically Secured XML

Security Labels", Proceedings of the 7th IEEE Workshop on Information Assurance, U.S. Military Academy, West Point, NY, 21-23, IEEE, 2006

9. Ulusal Güvenlik Sistemleri Komitesi (2010) Ulusal Bilgi Güvencesi (IA) Sözlüğü, CNSS Talimat No. 4009, 26 Nisan 2010.