2019 4th International Conference on Education and Social Development (ICESD 2019)
ISBN: 978-1-60595-621-3

Granular Data Encryption and Application Research in the Forensic Blind Area

Li-zhi LIN[1,a,*], Fa-jian XU[2,b] and Long-tian FU[1,c]

[1]FuZhou University of International Studies and Trade, Fuzhou, Fujian, China

[2]FuJian Police College, Fuzhou, Fujian, China

[a]hilychee@126.com,[b]908140143@qq.com, [c]253601337@qq.com

*Corresponding author

Keywords: XRQL; Digital Signature; Blind Area of Forensics; Safety Management and Control of UAV.

Abstract. RDF query language XRQL is easy to be combined with XML digital signature. By using XRQL query results and its localization, XML digital signature can encrypt the granular data of the whole document. This way will also lead to the blind area of electronic evidence, the forensics blind also need to be broken by XRQL technology. These technology can also be applied to the safety control of UAV airborne information.

Introduction

In 2001, the concept of electronic forensics was introduced from abroad. From intrusion detection and evidence collection to data recovery and electronic evidence, electronic forensics technology played an important role in evidence and identification, but there were also many problems. For example, there are many forensic blind spots that make the validity of electronic physical evidence questionable. Therefore, we need to conduct in-depth research on technologies such as memory dynamic storage, BITLOCKER, etc., which will generate electronic forensic blind spots, and find techniques and application countermeasures for cracking electronic forensic blind spots.

Encryption and data preservation technologies for electronic data are emerging one after another. This is also an important reason for the production of electronic forensic blind spots. In particular, fine-grained granular data encryption technology will generate a large number of electronic forensic blind spots. Only by analyzing these technologies, problems can be discovered. Find specific countermeasures to break through the blind spot of electronic evidence collection. Therefore, it is first necessary to analyze the basic concepts and related technologies of RDF, XRQL and digital signature related to granular data encryption.

The Basic Concepts of RDF, XRQL and Data Security

Metadata is the data of organizational data. It is a complete set of coding systems. It can describe the basic characteristics of any digital information resources, especially network information resources and their interrelationships, so as to ensure that these digital information resources can be automatically discerned, decomposed, extracted and analyzed by computers and their network systems. The Resource Definition Framework (RDF) is a metadata standard published by the W3C. It is an architecture that can encode, exchange, and reuse structured metadata. It provides an operational carrier for metadata. There are many techniques for querying RDF documents. RDF_QL is a kind of query. The query for RDF is basically similar to the query for XML. It only expands some RDF-specific query methods, which is more complicated than SQL. Similar query languages include the RQL ICS-FORTH RDF Suite for RDF metadata developed by the Greek ICS-FORTH organization, the open RDF query language Versa, and the RDF query language RDQL defined in the Jena project developed by Hewlett-Packard. There is also a query language that combines XML and RQL called XRQL, which is the product of the combination of Xquery and RQL, which is also an important direction for the development of RDF query [1].

The security of data includes the following aspects: confidentiality guarantee, integrity guarantee, authenticity guarantee, and anti-denial guarantee. Digital signature refers to some data attached to a data unit, or a cryptographic transformation of a data unit. This data or transformation enables the recipient of the data unit to confirm the source and integrity of the data unit; and to protect the data. Prevent being forged by people (such as recipients). The traditional digital signature technology is implemented by the confidentiality of the private key in the public key encryption algorithm, because this private key is not known to anyone except the owner, so it can be used to uniquely identify the user. The information encrypted with a private key can only be unlocked with the corresponding public key, so that signature authentication can be achieved, and the non-repudiation and unforgeability of the signature can be guaranteed. Digital signatures are completely independent of data encryption. Data can be signed and encrypted, or only signed or encrypted.

Data protection, data security and other issues exist in the description, publication, management and utilization of information resources. Digital encryption is an important method for protecting data information in the network. The network also gains more trust and wider application because of encryption technology. XRQL makes the query result of RDF flexible, so it is very simple to add RDF query information or query results or even partial result information to digital signature, which enhances the function of XRQL query and expands its application effect.

XML digital signatures are also widely accepted and used because of their widespread use. One of the strengths of the XML language is explicit search, and there is no ambiguity. If a portion of a document, including tags, is encrypted as a whole, the ability to search for data related to those tags is lost. In addition, if the tags themselves are encrypted, once they are leaked, they will be exploited for a plain text attack on the cryptography employed. These issues are all related to XML digital signatures. So when you need to perform different encryption processing on different parts of a document, you need to ask for XML. Whether you can successfully encrypt the different parts of the document depends on whether you can accurately locate the location of the granular data in the document. Although it is also possible to encrypt the entire RDF document directly with an XML digital signature, XRQL can actually perform local granular data operations in RDF applications, so the combination of XML digital signature and XRQL can fully utilize and exploit the advantages of both, and can semantically parse the document to meet the encryption needs of some special cases.

The Principle of Granular Data Encryption and the Production of Evidence-based Blind Spots

The general digital signature is to calculate the information to be signed with the private key, obtain the signature of the information and attach it to the original information, so as to ensure the integrity of the data, the authentication of the information source and the non-repudiation of the sender of the information. However, in the case where multiple participants are required to sign, this signature mechanism requires all participants to sign in turn, the latter person verifies the signature of the previous person, and then uses the private key for the signature of the previous person to perform operations. And then pass the obtained signature result to the next signer until the signature of the last signer is completed, thus realizing the signature of a person by a plurality of people, achieving multi-party non-repudiation, but in this case, except that the first person knows the content of the information he signed, the rest of the people do not know what they signed, which is unreasonable in reality. They cannot ask others to sign the document without the contents of the unknown file. Moreover, in general, in the case where multiple people are required to sign, the signer only signs and bears the corresponding responsibility for the part that he is responsible for, and is not responsible for the rest of the document. After these analyses, we found that general digital signature techniques cannot implement signing only specific parts of a document. The XML-based digital signature technology can effectively solve the above problem by signature protection of the granular data. When multiple people sign a file, each person can only sign the part of the local data segment that he should be responsible for (granules), no responsibility for the rest of the document [2].

XRQL can locate the found information, which is beneficial to separately encrypt and sign the

result of the query information or the local granular data of the result, so as not to affect other parts of the information, especially the file frame structure of the RDF document. So sometimes the purpose of the query becomes to determine the exact location of the target in the document. The advantage of XML digital signature is the encryption of local data. It is also a W3C product with RDF and XRQL. There is no problem in cooperation and compatibility, which can meet various aspects such as intellectual property protection, value proof, and data security. Demand [3]. Digital signature can be directly used in XML, but XRQL can be used to deeply penetrate RDF applications. Therefore, it is proposed to combine the digital signature of XML with XRQL to fully utilize and exploit the advantages of both, and the signed local data is also Become a blind spot for electronic forensics. The combination of XML digital signature and XRQL can penetrate the internal implementation of RDF to encrypt the content and improve the level of protection. XRQL's query result positioning and XML digital signature sign and encrypt the element-level object, which completes the encryption function and expands the purpose of the query.

The Analysis of the Blind Spot Problem of the Data Encryption of the Granular Data and Its Application in the Safety Control of the Unmanned Aerial Vehicle

The use of metadata and RDF technology to organize management and identify and utilize important electronic files is an important method. In these fine-grained encryption applications, the electronic collection security level is greatly improved, which is also a cause of the electronic forensic blind spot. Taking network resources as an example, many network resources and services are not free. For charging information and services, password accounts are used to control management. Due to the inherent defects of password accounts is easy to be stolen or shared, intellectual property rights and various resources and services are not well protected. But if you combine the fine-grained granular data encryption technology to sign and encrypt important query and information services, it effectively protects the key information in these resources. It also adding a lot of trouble to electronic forensics.

In the forensic analysis of electronic evidence, it is difficult to screen, filter, query, analyze and collect electronic documents encrypted with granular data. It is necessary to understand and master the corresponding fine-grained encryption principles and methods before they can crack the electronic forensics blind zone. Therefore, it is of great significance to study the XML digital signature and the granular data encryption technology in XRQL to crack the electronic forensic blind zone.

The problem of blind spot in electronic forensics is a niche direction in electronic forensics technology, which deserves in-depth research and open application. For example, it can be applied to the “authentication” problem of the unmanned aerial vehicle, which can force the loading and running of the “answering machine”, the aircraft file, the flight parameters and the control data file during the flight start of the aircraft, and allow the personnel with the corresponding authority to access and get relevant information. Of course, this information needs to be encrypted at different levels for granular data, and then publicly released; for example, "answering machine", the flight parameters are general grades, allowing the general personnel to access the parameter information related to the current flight record of the aircraft; the aircraft file is ranked higher, It includes personal privacy information such as aircraft owners and users, so this information is generally only open to management personnel; flight control data files are the highest level, mainly open to law enforcement officers and senior management personnel, and this information allows law enforcement personnel to crack the aircraft control data to obtain the control password and then seize control of the aircraft from the aircraft remote control when it in critical situations.

Summary and Prospect

Metadata, RDF technology and XRQL query language are originally used to organize, manage and utilize electronic resources, but if combined with XML digital signatures it can solve data security problems in many special cases, using XRQL query result positioning plus encrypted

object at element level, which can perform local search, location and fine-grained encryption of the local particle information of the resource document, and is also a way to protect the metadata information.

Because the encryption of the granular data is the protection of the fragmented information, it is highly concealed and easy to be neglected in the electronic forensics to create a forensic blind spot. Even if it is discovered by the electronic forensic software, the corresponding decryption technology is still needed to crack the encrypted granular data. Therefore, in the electronic forensics, we must conduct continuous research on the blind spot of evidence collection, not only to discover new blind spots for evidence collection but also to study the corresponding techniques for cracking the blind spot of evidence collection. It is very meaningful to strengthen the security and control of unmanned aerial vehicle. We can also use it to improve the anti-interference ability and enhance the robustness of unmanned aerial vehicle.

References

[1]M.L. Yang: *Design,* The Research and Implementation of The RDF Data Storage and Query based on Graph (MS., Bei Jing Jiaotong University 2015), pp. 7-8.

[2]M. Zhu: *Design,* Research on RDF Data Storage and Query Based on Base (MS. Nanjing University 2013), p. 6.