Secure Access Control System for Digital Repositories - DSpace as a case study

By
Hirra Anwar
2010-NUST-MS-CCS-18

Supervisor
Dr. Muhammad Awais Shibli
Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Computer and Communication Security (MS CCS)

In
School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(May 2013)

Abstract

Digital Repositories serve the purpose of storage and long term preservation and access of digital content. With the growing trends towards digital repositories, the access issues, privacy and confidentiality concerns of content stored in repositories have increased manifolds. The digital content stored in repositories is exposed to high-profile data losses. Storage and preservation of digital content raises the concerns of content security and its need based access. It must be ensured that sensitive digital data is appropriately protected and kept secure from unauthorized access and consequently its misuse.

Considerable work has been done over the last few years over the authentication & authorization issues of digital repositories; however the policy and access issues of repositories still emerge with the changing trends. The access control trends have now shifted to be more fine-grained, policy based and external to applications. A stringent and effective access control mechanism can ensure restricted access of the digital content stored in the repositories. Since repositories comprise data of varying security levels, access on such content requires fine grained authorization which elaborates context aware constraints for restricting access.

In this thesis, we explore and address the security requirements of digital repositories and propose a generalized standard based security system for digital repositories which ensures flexible policy definition, security of data, extensible policy enforcement, and seamless integration with standard based systems. Our proposed system ensures granular level authorization based on OASIS standard XACML technology and Advanced Encryption Standard based encryption of digital content to ensure confidentiality of data stored in repositories. As a test case, we have enhanced the authorization of DSpace institutional digital repository system. DSpace currently follows a primitive authorization mechanism which we have updated according to the latest security trends. In addition to this, we have introduced the feature of encryption of stored documents which ensures confidentiality of DSpace content.

We have rigorously evaluated our work through test cases and NIST defined Qualitative and Quantitative criteria which are used to analyze the

security aspects of the system. Threats have been identified pertinent to DSpace and their mitigation has been devised through proposed mechanisms. The evaluation shows that there is a significant enhancement in the security of DSpace including granular level access and secured digital content.