International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

Review on usage Control Enforcement

Foram H. Shah
Computer Engineering Department,
St. Francis Institute of Technology,
Mumbai – 400103, India

Shamsuddin S. Khan
Computer Engineering Department,
St. Francis Institute of Technology,
Mumbai – 400103, India

***Abstract*— In today's computing era interaction between people and services provided by computer system plays vital role. Failure to them causes high damage to entity's. To avoid damage usage control policies are used. It is important to think about a way in which you will enforce those policies. Here reviews on some enforcement environment for distributed system, grid system where usage control policies are enforced using some enforcement model.**

Keywords*— Access control, Usage control, Policies Enforcement.

I. INTRODUCTION

Access control is ability to allowing, denying permission or rights regarding particular document in a system. Rights related to document includes read, write, execute, copy, transfer so on. In any system these rights need to be forwarded along with document when they are transferred from one machine to another, this happens with the help of policies enforcement. Policies are set of constraint or rules which needs to be defined by owner of the document and need to be enforced in each copy of that document. Access control deals with authentication, authorization not with obligation and conditions.

Usage control is extended version of access control which deals with obligation as well as condition in distributed environment, where system might separate geographically. Access control does not allow enforcement of policies in distributed system it loses its control to the data as soon as data leaves the originators machine but in distributed system policies enforcement on data is very much essential even if data gets propagated to other system or software. Usage control is related to end user who owns the data. End user needs to give some usage policies to his/her document. Which should be enforced to all copies of document as well as should get transferred on each document transferring transaction and should get enforced on the destination machine. For the same different policies enforcement model are there which propagates & enforces polices of document to destination machine also. Policies enforced can be like "open file ABC with note pad only", "delete file after 15 days","don't make more than 5 copies of file" & so on.

II. LITERATURE SURVEY

There are many access control enforcement models which act as policies manager of the document. Some of them are The Discretionary Access Control (DAC)model, The mandatory access control (MAC) model, Role-based access control (RBAC) model, The multilevel security (MLS) model, The BLP and BIBA models, The Clark-Wilson (CLW) Model, Key Management Models are discus in [8]. In this article pros & cons of each model is discus and compared. Not going much into detail of theses traditional models.

In this paper some usage control enforcement polices, models & Technics are discussed which includes, UCON model [1] . Usage Control on Grid Computational Services [2]. Enforcing Usage Control Requirements in Service-Oriented Architectures [3]. Usage control policy analysis [4]. Implementation policies of usage control [5]. Towards usage control in distributed system [6]. Usage control for distributed system [7], Security Enforcement Model for Distributed Usage Control [9]. State-based Usage Control Enforcement with Data Flow Tracking using System Call Interposition [10]. Datacentric Multi-layer Usage Control Enforcement: A Social Network Example [11].

The UCON model is described in the paper Towards Usage Control Models:Beyond Traditional Access Control[1]. Here new concept called usage Control for controlling access and usage of digital information objects is described. Main focus is given to the consolidated view of three areas such as traditional access control, trust management, digital rights management (DRM). The model Usage control (UCON) combines all of these three areas. The scope of model is shown in Fig 1. This is explained with payment options and different kinds of reference monitors. Traditional access control, trust management, digital rights management (DRM) handles and deals with their own targeted problems. UCON deals with all those targeted problem and covers issue such as security and privacy. Limitations of this models are: it do not cover the issues related to delegation of rights. Administrators issues are not described.

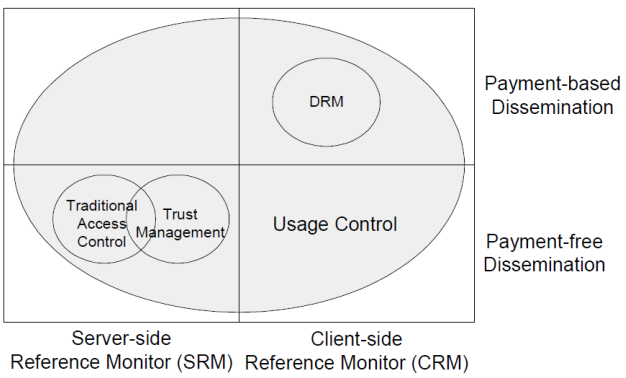

Fig. 1 UCON Scope [1].

In Grid environment usage control is done with different approach mentioned in Towards continuous usage control on grid computational services [2]. Security is one of the important factor in grid environment, since it supports the synergistic among very large and dynamic set of data,where trust relationship does not exist in prior. Approach to improve security of grid computational service includes integration of security architecture with new component that monitors behavior of grid applications. This component enforces a security policy which make apparent behavior of grid applications. (i.e sequence of operations that are allowed to perform).

This policies can be local or global. Aim of this policy is to precognition of threatening & malevolent behavior of the application that could reduce availability or could privilege unauthorized access to services.

Security policies specifies limits over the resource usage each rule of policy comes from repercussion of the composition of system calls, predicates and variable assignment. Here security module is paired with JVM to enforce security policy. Gmon a security tool dedicated to JVM implements continuous and fine grain application monitoring and improves security. This Gmon gets integrated with GRAM architecture within the globus frame work to protect grid computational services with fine grain usage policies.This model monitors system trace and stops execution when this violates the security policy. Detecting conflict in policy is one of the work which can be done based on above model.

Heterogeneity and openness of service oriented architectures (SOAs) pose a significant challenge on the enforcement of remote usage control policies [3]. SOA-based systems are open & non-proprietary system. The problem with it is, how to technically enforce usage control policies in SOAs based system that are not under direct control of data provider who request remote services and gives away sensitive data. Solution to this is given as model and enforce usage control policies for remote endpoints in SOAs. This approach combines concepts from three different areas such as web service & SOA security,trusted computing and usage control. The former checks for sufficient technology to enforce Usage control policies before a service provider sends data to requester needs to be perform. If technology related to data is not modified then the usage control policies are attached to the resources and transferred to requester. A dedicated enforcement component was configured with the policies at requester side . This approach makes use of model driven engineering technologies, which allows specifications of policies graphically after the transformations done. This transformations are used to configure the enforcement component of the architecture. Limitation of this approach is, it restrict general concepts of usage control in some ways such as applications that are not trusted are not allowed to run in the system.

Usage control requirements are described in terms of policies. There is a need of some approach to support analysis of problems related to policies. Which will check the problems such as is a policy steady i.e consistent? Is an conceivable usage control approach capable of enforcing given policy? Can we configure such approach by evaluating respective policies? Etc. To do so research is done in [4]. Where possible solutions of problems are enlisted by tool and then the solution are analysed by translating OSL(obligation specification model policies and abstract mechanism descriptions into a variant of LTL(linear time logic). This is done by using model checker and automatically analysis tool NuSMV. This approach gives complexity while using with heterogenious platforms.

Data may exist in various portrayal which reside at different layer of abstractions such as operating system,window manager,application level,DBMS etc.It is necessary that policy enforcement structures needs to be adapted and implemented at all the different layer to monitor & control data.For enforcement of policy at different layer the model has been implemented[11]. It enforces data related to the policies simultaneously at respective level and offers a multi layer enforcement & combines inter layer usage control enforcement. Reason for various multiple enforcement is that the data comes from different portrayal such as packets from network,object attributes,window content, etc. To protect those data enforcement is required at different layer where data is represented. It is suitable to protect data at higher level of abstraction. Architecture presented is built on top of main three blocks such as policy enforcement point (PEP), Policy information point (PIP) and policy decision point (PDP).This components are designed to communicate with network protocol and can deployed in distributed way. This architecture helps to enforce policy such as “any part of particular page can not be printed, or copied to the clipboard (not even in form of a screen shots)”.

It is necessary to undestand the actual meaning of policy, before applying or enforcing them, at user’s end semantics of basic operators, such as copy or delete, tends to vary according to the content. For this reason, they can be mapped to different sets of system events. The behaviour that user expects from system may differ from actual behaviour. In order to solve this problem, tool for automating the translation of specification level usage control policies into implementation level policies has been implemented [5]. The work presented gives two things. First, frame work that allows to define semantics of actions in terms of element of application specific domain models and translates the policy from there specification level syntax to event condition action (ECA) format. Second, it provides methodological guidance for the specification and translation of policy so that the complete process which is heavy when done manually is automated.

In this work, dynamic structure of system while translating policy have not been considered. Assumption is made that system is static.

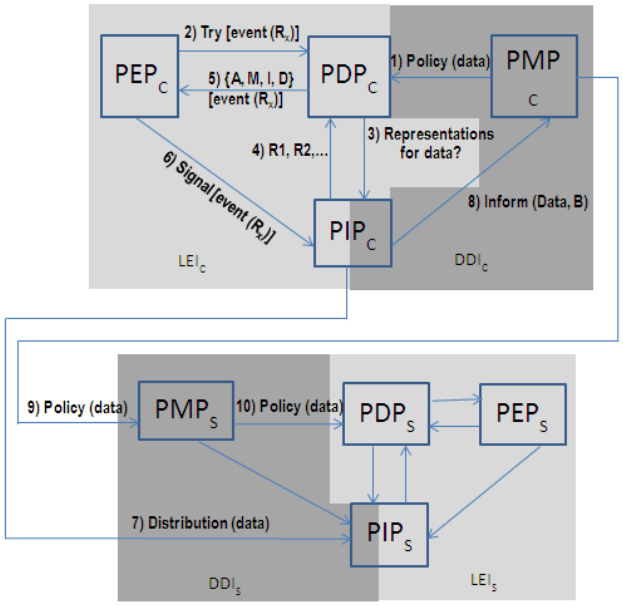

Fig. 2 Integration of LEI and DDI and interplay of DDI's components [7].

Distributed usage control related with data usage in distributed system enviornmentsare geographically distributed and communicate with each other with the help of internet. Due to this structure it is necessary to enforcement of policies to the data so even if data gets transfered to other machine it will be safe from unautorized usage. There are many ways to enforce usage policies in distributed environment some of them have been described earlier now we will have a look at some enforcement models which perform enforcement of usage control across all the distributed or system stored, processed data.

Research work is already done regarding these types of infrastructure. Generic data flow model[6] is one of them. Core component of distributed enforcement infrastructure are PIP and PMP (policy management point). PIP holds stae of information flowing through the system. PMP manages all usage control policy for data transfering, remaining and moving in the system. Other components PEP intercepts eactual events and transferes it to PDP which take decision whether to allow or not. This modle supports (1) Application and protocol independent dataflow tracking across different os instance, (2) sticking policies to upon sending it to another system and (3) policy enforcement at receiving site [6]. This infrastructure defeat weakness of traditional access control system but it do not take into account the fundamental distributed nature of data usage control enforcement.

Another upgraded model of generic data flow model is cross stystem data flow model [7]. It focuses on problem of establishment of usage control infrastructure that make sure that usage control policies are send along with data transfer and get enforced at recievers side. Compare to generic data flow model additional thing in this model is integration of LEI (Local enforcement infrastructure) and DDI (Data distribution infrastructure).Fig. 2 shows integration of LEI and DDI and inter play of the DDI's component. In this infrastructure focus is given to locally enforcable policies. Support for global information flow state is not there. Dynamic network structure is not considered. Some usage control applications,viz, multimedia streaming and voice over IP are not covered.

III. CONCLUSION

From the last two decades, security of data is becoming an important factor. Once data is transferredfrom one system to another system it is important to make sure that no undue advantage of data is taken. For the same, access control and usage control policy enforcement is done. As technology advancesthese enforcementmodels, also need to be changed in terms of security of data. There are some fields where usage control policies are not fully enforced or fully supported. Because of these shortcomings, this can be one of the upcoming research areas.

REFERENCES

[1] J. Park and R. Sandhu, "towards usage control models: Beyond traditional access control", in Proc. Of 7th ACM symposium on access control models and technologies, 2012.
[2] M. Colombo, F. Martineli, P. Mori, and A. Lazouski, "usage control for grid services".in International joint conference on computational science and optimization, pg. 47-51, Apr. 2009.
[3]A. Berthold, M. Alan, R. Breu, M.Hafner, A. Pretschner,J.-P. Seifert, and X. Zhang. "A Technical architecture for enforcement usage control requirement in a service-oriented architecture", in Proc of the 2007 ACM workshop on secure web services pg. 18-25, 2007.
[4] A. Pretschner. J. Ruesch, C. Schaefer, and T. Walter, "Formal Analysis of usage control policies", in International conference ARES'09, pg. 98-105, Mar. 2009.
[5] P. Kumari and A. pretschner, "Deriving Implementation-level policies for usage control enforcement", in Proc. 2nd ACM conference on data and application security and privacy, pg. 83-94, Feb. 2012.
[6] Florian Kelbert, Alexander Pretschner," Towards a Policy Enforcement Infrastructure for Distributed Usage Control", in Proc. of 17th ACM symposium on access control model and technologies , pg. 119-122, Jun. 2012.
[7] A. Pretschner and F. Kelbert, "Data usage control enforcement in distributed systems", in Proc. of3rdACM conference on Data and application security and privacy, pg. 71-82, Feb. 2013
[8] Anne V.D.M. Kayem et al. , "Adaptive cryptographic Access Control", in Advances in information Security, Springer, vol. 48, pg. 11-40,2010.
[9] X Zhang, JP Seifert, R Sandhu, "Security Enforcement Model for distributed usage control", in International conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pg. 10-18, Jun. 2008.
[10] M. Harvan& A. Pretschner, "State-based usage control enforcement with data flow tracking using system call interposition, in Proc. of 3rd;international conference on networl and system security pg.373-380, 2009.
[11] E. Lovat and A. Pretschnder, "Data-centric Multi-layer Usage Control Enforcement: A Social Network Example",in Proc. of 16th ACM symposium on access control models and technologies, pg. 151-152, 2011.