



## A Collaborative Organization Structure for Ensuring Security in Academic Campuses

D.S. Bhilare

School of Computer Science & IT,  
Devi Ahilya University, India

---

**Abstract** - Across the world Academic Campus Networks face similar Information Security threats as generally they have common set of vulnerabilities. Most of the educational institutes in developing countries do not have adequate resources to identify and respond to these threats. Therefore, a collaborative approach is required, where security incidents, its analysis and solutions are stored using a common protocol. The proposed framework provides a structured way for institutes of higher education to collaborate with each other on security issues in key areas including incident response, attack mitigation, and preventive measures. This would also avoid duplication of efforts and an early solution can be found, based on past experience.

**Keywords**- Information security, collaborative organization, incident handling, alert, academic campus

---

### I. Introduction

Security related threats have become not only frequent and diverse but also financially damaging and disruptive [4,5]. New types of security related incidents emerge every day. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and quickly restoring the IT services [12]. Building an effective Incident Response Mechanism is very challenging, it requires substantial planning and resources. Continuous monitoring and control through threat detection and prevention systems and other mechanisms is essential. Establishing clear procedures for assessing the current and potential business impact of incidents is critical [7]. Equally important is implementing effective methods of collecting, analyzing, and reporting data. Building relationships and establishing suitable means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g., other incident response teams, law enforcement) are also vital [8].

### II. Related Work

Earlier research on distributed threat management has focused mainly on the exchange of data within a single organization. Focus was on distributed collection and centralized correlation [11]. The DShield project [15] is an example of a centralized repository that receives intrusion alerts from many distributed sources. Cuppens and Mieke [1], [2] discuss methods for cooperatively correlating alerts from different types of intrusion detection systems. Cyber Threat report of GTISC believes strongly that a proactive and collaborative approach to understanding emerging threats will help us develop more effective information security technologies and strategies[6]. A major driving force for institutions to join a collaboration group is that the participants can implement mitigation strategies against threats they otherwise would not have known about. A study showing resources needed to counter worm propagation, concludes that a response needs to be mounted in 2-3 minutes and that participation of nearly all nodes required to be effective [7]. They also suggest that the Internet by its inherent weaknesses is not effective in preventing and containing worm outbreaks. Their results suggest that both technological and administrative issues must be addressed before any effective defense can be mounted against such Internet-wide threats. While these numbers are specifically derived in the context of quarantining Internet worms, their results show that current and foreseeable threats demand a cooperative and collaborative approach to achieve desired level of security. The OAI-Protocol for Metadata Harvesting (OAI-PMH) defines a mechanism for harvesting records containing metadata from repositories[3][10] [14]. In order to provide services, the harvesting approach must be combined with other mechanisms [9].

A browser interface is very difficult to build when the metadata to be browsed is distributed across a number of repositories. Therefore, the preferred approach would be to get all the metadata records together in one place.

### III. Proposed Framework

The proposed framework for implementing a collaborative distributed inter university incident handling mechanism is built around open source OAI-PMH protocol[13]. The overall structure is divided into three key modules: Incident Data Capture Module, Metadata Generator Module, and Service Provider Module.

#### Design of the Incident Database

The proposed incident database stores the following information about the each incidence:

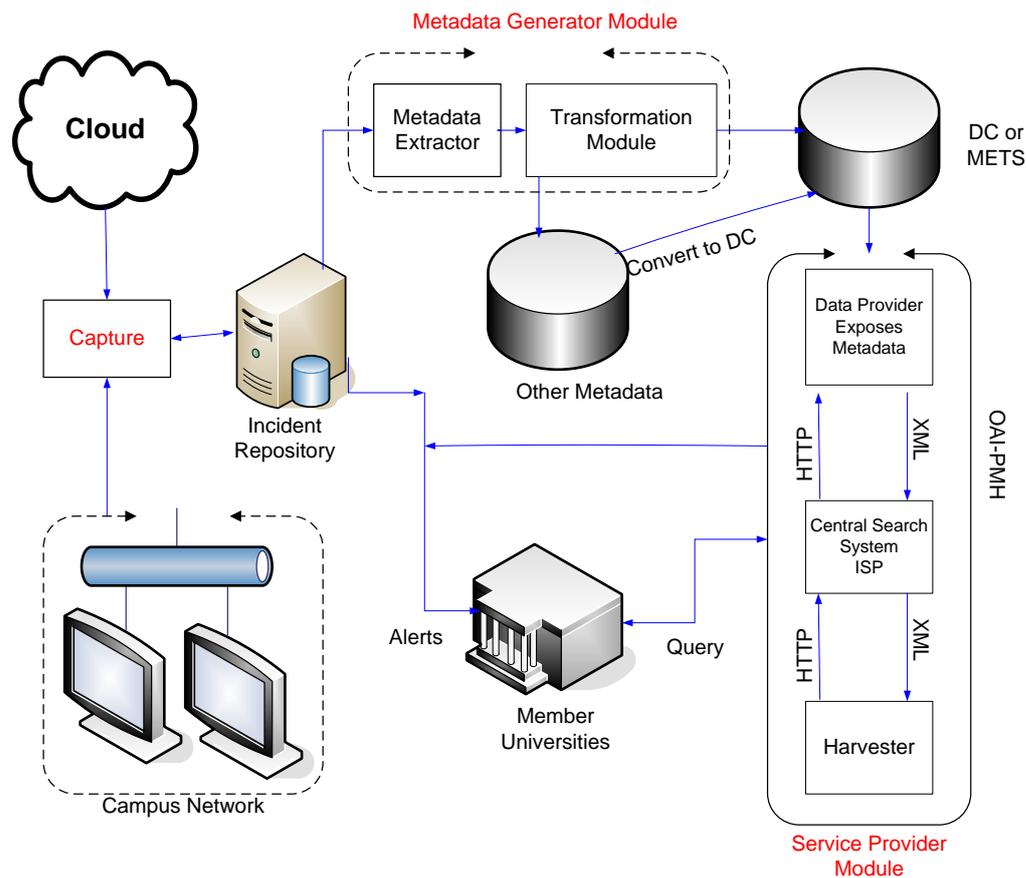
- Incident ID.

- University/College ID
- Date and Time the Incident Occurred
- Date and Time when the problem resolved
- Total Number of Staff hours consumed
- Total Number of hours lost
- Who attacked?
- Why was the reason of attack?
- How the attack was executed?
- What steps are being taken to prevent future occurrences?

**A. Components of the Framework**

The complete framework is illustrated in the Fig. 1. There are three key modules as shown below:

- Incident Data Capture Module
- Metadata Generator Module
- Service Provider Module



**Fig. 1: A Framework for Collaborative Organization Structure for Securing Academic Campuses**

**B. Incident Data Capture Module**

The “Capture” module interacts with the environment, which includes the External World and Campus Network. Whenever any new input or suspicious activities is detected, it is recorded in the incident database in the pre-decided format, if it is not already recorded. Under certain circumstances, the incident database is also updated manually, as sometimes the “capture” module is unable to detect all the incidents.

The “capture” module also maintains a log of all the incidents, so that it can be used by the administrator to formulate the policies for the incident management and reporting.

**C. Metadata Generator Module**

The Metadata Generator Module (MGM) module continuously gathers input from the incident database and generates corresponding metadata. These incident databases belonging to member institutes are pre-registered and authenticated before every access. The MGM, manages the mapping relationships between the information present in the incident database to the standards like DC (Dublin Core) or METS (Metadata Encoding and Transmission Standard).

This metadata is generated depending on the contents of the incident database and other input. This is carried out by checking how frequently a term is used in the incident reporting text. The mapping is thus completely dependant on the contents of the text.

The metadata thus generated by the Extractor sub module forms raw input to the Transformation sub module. The Transformation sub module separates metadata formats recognized by the OAI-PMH in a separate repository, which mainly contains DC and METS. The remaining formats are transferred to other formats, which later on converted to accepted format using available metadata conversion tools. Finally, these metadata formats which are essentially in XML format are made available to the Data Provider.

#### **D. Service Provider Module**

Whenever a member university or college requires some information from the member community, a request is fired by local client having software called harvester. The harvester software is required to issue the OAI-PMH request for fetching the metadata of incident databases. This request is first sent to the central service provider. The Service Provider tries to resolve the request using local repository, after proper authentication of the user. If required information is not available locally, then it is passed to the member repositories. There is a module called "data provider" at the local database end which exposes this metadata to the harvester via the same service provider.

Hence in OAI-PMH, it is the data provider who does the job of exposing the metadata to the harvester. Any institute that wants to be a member of the collaborative incident databases group has to first ensure that they follow the same protocols to expose their metadata information to the central service provider. In order to address the issue of reliability and integrity of the information shared by the member institute, service provider module maintains a reliability rating for each member institute, which is updated based on the feedback from other institutes and past record. This rating is also provided along with incident information to the requesting member. However, this does not ensure the reliability of the information, but gives some idea about the trust-worthiness of the source of the information.

### **IV. Implementation**

#### **A. Implementation Strategy for OAI-PMH Grammar**

In order to access OAI-PMH repositories for harvesting metadata use of the Perl based toolkit, Net::OAI::Harvester (Summers, 2004) is proposed. Implementation code for one verb of OAI-PMH is given below. Similarly, remaining verbs can also be implemented:

The OAI-PMH is essentially a set of request/response messages which may be sent over HTTP to retrieve metadata that is encoded in XML. So one can construct a familiar URL and get back an XML document containing the required metadata. From a programming perspective there are several issues that arise when writing a OAI-PMH harvesting program: HTTP requests need to be URL-encoded for safe transmission; error conditions can arise which must be handled gracefully; resumption tokens may be used to break up a response into chunks. Of greatest concern here is that all responses are arbitrarily large XML documents.

Net::OAI::Harvester is a Perl module that abstracts away all the details of generating the HTTP request, handling error conditions, and parsing XML so that extracted data can be easily used.

After installing Perl, Net::OAI::Harvester can be installed with one command:

```
perl -MCPAN -e 'install Net::OAI::Harvester'
```

#### **B. Implementation of "Identify" verb:**

Using the following script, identification of the repository can be obtained:

```
1 use Net::OAI::Harvester;
2 my $var0 = Net::OAI::Harvester->new(
3   baseURL => 'http://archive.upper.net/cgi-bin/mph1' );
4 my $identity = $var0->identify();
5 print $identity->repositoryName(),"\n\n";
```

#### **OUTPUT:**

Central Library D.A. University OAI-PMH Repository

Thus we can implement the proposed framework using open source protocols and tools.

### **V. Conclusion And Future Work**

The proposed framework improves institutions capability to manage Information Security threats, as more informed decisions are taken. Institutions are able to take preemptive actions without having been directly attacked. Since most of the educational institutes have limited resources to detect and respond to these threats, the proposed approach allows sharing of information related to these attacks and possible solutions. The participating members of these cooperative can find information about measures taken in case of similar incidents taken place in other institutes. This would avoid duplication of efforts and an early solution can be found out based on past experience. Future research may focus on data analysis towards predictive security measures and methods for low cost alert distribution and broadcast. Another issue would be development of a metric for ranking the threat level for particular verticals, or groups of organizations.

#### **References**

- [1] Cuppens, F. and A. Mieke, (2002). "Alert Correlation in a Cooperative Intrusion Detection Framework," in IEEE Security and Privacy.
- [2] Cuppens, F, (2000). "Lambda: A language to model a database for detection of attacks," in Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID 2000), (Toulouse, France), October 2000.

- [3] Dublin Core Metadata Initiative, (2005). DCMI Abstract model. <http://purl.org/DC/>
- [4] Gordon, L.A., M. P. Loeb, W. Lucyshyn, and R. Richardson (2006). CSI/FBI computer crime and security survey.
- [5] Junginger, M., A. Balduin v., and H. Krcmar, (2003). Operational Value at Risk und Management von IT-Risiken. WISU - Das Wirtschaftsstudium, (3):356–364.
- [6] GTISC, (2009). <http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf>
- [7] ISO/IEC. ISO/IEC 27001:2005 (2005). Information technology security techniques information security management systems requirements.
- [8] Nist Publications, (2008): computer security resource centre, SP800-61, <src.nist.gov/publications/nistpubs/>,
- [9] Bhilare, D. and Kawale Jai, (2005), "An architecture for cooperative digital libraries". CSI Computing 2005, Indore.
- [10] Open Archives Forum. (n.d.), (2007). OAI for beginners, the Open Archives Forum online tutorial. 2. History and development of OAI-PMH. Retrieved April 21, 2007, from <http://www.oaforum.org/tutorial/english/page2.htm>.
- [11] Stolfo, S., (2004). "Worm and Attack Early Warning: Piercing Stealthy Reconnaissance," IEEE Privacy and Security, May/June 2004.
- [12] Soo Hoo, K.J., (2000). How much is enough? A risk management approach to computer security. <http://iisdb.stanford.edu/pubs/11900/soohoo.pdf>, June 2000.
- [13] Summers, Ed, (2004, Jan 30). "Building OAI-PMH Harvesters with Net::OAI::Harvester" , Publication: Ariadne Issue 38 <http://www.ariadne.ac.uk/issue38/summers/intro.html>
- [14] The Open Archive Initiative. <http://www.openarchives.org>
- [15] Ullrich, J., (2004). "Dshield home page." <http://www.dshield.org/>.