Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

PRISM: A Public Repository for Information Security Material

Vincent Garramone, *Regis University,* and Dino Schweitzer, *United States Air Force Academy*

Abstract – To address a perceived lack of availability of educational resources for students and teachers in the field of information security, and advance the quality of information security education in general, our institutions have begun development of a web portal to house information security-related educational materials, research and virtual exercises, as well as provide links to other resources. This portal is termed the PRISM, Public Repository for Information Security Materials This paper details the initial vision for the PRISM repository, outlines user interface, technical, and personnel requirements, and discusses some of the more interesting aspects of implementation including access control provisioning, and protocols for content submission, review and classification. Current status of the project is also presented, followed by a brief overview of near-term future plans.

Index terms – Security education, active learning, educational resources

I. Introduction

As more of our lives come to depend on information technology, educating those who develop and manage those technologies about security concepts is crucial. Unfortunately, tuning existing mature educational programs to include a focus on security topics has proven not to be straightforward. Some institutions report success adding security-specific courses to existing curricula. However, for various reasons this is not always feasible [1]. As an alternative to adding a security-specific course, relevant activities and lessons can be integrated into existing courses to teach security concepts [2]. These added materials must be highly available, be able to be integrated into many different types of courses and curriculums, and have a high usability factor for students and teachers unfamiliar with the subject matter.

To help address these needs and advance the quality of information security education, our institutions have begun collaborative development on a web portal to house information security related educational materials, research and virtual exercises, as well as links to other resources. This website will serve as an online space for educators to discuss effective pedagogy, share tools, and collaborate on curriculum development.

This paper details the initial vision for the PRISM repository, outlines user interface, technical, and personnel requirements, and discusses some of the more interesting aspects of implementation including access control provisioning, and protocols for content submission, review and classification. Current status of the project is also presented, followed by a brief overview of near-term future plans.

II. Vision

The creators of the Public Repository for Information Security Materials (PRISM) website intend to make it a specialized resource for students and educators who are interested in information security education. Visualization tools, publications, educational materials, links to relevant websites, and research data (pertaining to the effectiveness of the tools and procedures offered on the site), are all potential types of material. Ideally, content will be contributed by a number of institutions. In addition, the site has the potential to eventually serve as a collaborative workspace where users discuss tools and teaching methods both asynchronously and in real-time, and have the opportunity to participate in educational games and online activities.

Although there are a number of websites that offer educational materials related to information security, no single site seems to exist that attempts to aggregate and classify these disparate pockets of resources. Merlot (http://www.merlot.org/), likely the most well known index of learning materials, has roughly twenty entries under information security heading, and just six cryptography related materials.

Furthermore, locating resources to match a particular need in the classroom is not straightforward in many existing repositories. When presenting security concepts, many higher education institutions have specific learning objectives they must address. For example, undergraduate and graduate information security program developers may be working toward compliance with requirements for a National Security Agency Center of

Academic Excellence[1] designation. Community colleges and professional schools, driven by job market requirements often strive to cover topics necessary to achieve industry recognized security certifications from companies like Microsoft, Cisco, and ISC[2]. High school teachers might not be so focused on domain learning, but instead wish to engage students by augmenting topics with hands-on exercises that require little preparation or technical skill. PRISM is being constructed to allow individuals in each of these situations to quickly locate resources that meet their teaching and learning objectives based on topical content, technology constraints, learner skill levels, and situational information (e.g. how much time is available for the exercise).

Our current focus involves determining the most useful way to classify and organize resources available on the site. Information security is a broad and complex field of study, and one can quickly become mired in results irrelevant to their interests when conducting keyword searches. Moreover, it may be difficult to identify those terms that will be most useful in locating specific materials within any given repository [3]. Currently, educational material repositories tend to use very general metadata definitions that lack the specificity required to effectively locate resources [4]. We anticipate a better method for locating relevant material will be realized through the use of carefully crafted taxonomies that allow for target location in a similar manner to that of large-scale online retailers. This is the focus of a related study currently being conducted at our institution.

III. Requirements

Prior to development, requirements-gathering efforts compiled the following list of essential features to satisfy our goals for the repository. At a high level, a publicly accessible website acts as an interface for educators and students to locate and make use of digital resources. A physical server is required to host the website, as is a reliable connection to the Internet with adequate bandwidth to support the PRISM user base. Finally, a plan for system administration and site maintenance is necessary to ensure continuous availability and integrity.

A. Front End

Certain characteristics and functionalities, driven by strategic goals of the project, were identified as vital to the utility of the PRISM website. These are some of the major considerations:

- An intuitive interface that allows students and educators to locate desired resources effectively and efficiently.
- A simple procedure to create new content to allow individuals of various technical proficiency levels to contribute meaningful content to the site.
- Access control levels to allow specification of permissions for anonymous users, authenticated users, content contributors, moderators, and site administrators.
- Flexibility in terms of site functionality to allow for growth and change inherent in a newly developed resource.
- Security sufficient to protect the site from attackers (especially important for an information security resources site!).
- A license compatible with the PRISM organization and budget.

B. Back End

Similarly, certain desirable conditions regarding hosting of the website that were considered.

- A carefully crafted framework for the organization and categorization of resources.
- A suite of supportive applications (database, web server, etc.) that are secure, reliable, manageable, and have educational institution-friendly licensing.
- Adequate server hardware to fulfill requests from visitors to the website at an acceptable level of performance.
- Secure configuration to protect from hackers or rogue applications.
- Redundant power, storage, processing, etc., to avoid a single point of failure.

C. Personnel and Procedures

Finally, personnel are required to monitor the hardware, maintain the site, and manage PRISM activity and administrative tasks.

- PRISM organizational leaders to provide direction, solicit participation, and support.
- Someone to develop and maintain the software powering the website.
- Someone to monitor and maintain the hardware, and somewhere to keep it.
- A site moderator to enforce site rules, preserve integrity and scope, and offer help to users and contributors.

[1] NSA CAE information page: http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

- An IA expert to configure the server, test software for vulnerabilities, and plan for failures and recovery.
- Rules and procedures for submitting and reviewing content, determining content appropriateness, and expiring content.

IV. Technical Execution

As with most projects, budget and availability of resources was a constraint in the planning and implementation of PRISM. Cost of hardware, software licensing or development, bandwidth and communications services, and maintenance of each component of the hosted website had to fit within the available budget. The primary source of resources for the PRISM project is donation-based. For this reason, among others, open-source solutions for software requirements were strongly preferred and ultimately implemented.

While an extended discussion regarding the pros and cons of open source software (OSS) is beyond the scope and intention of this paper, it is worth noting that given the "right set" of requirements and resources, OSS can offer many benefits over closed proprietary systems [6, 7]. For PRISM, the cost, security and performance requirements of the software, as well as the fact that a team of graduate IT students will manage the project for the foreseeable future made an open source solution both desirable and cost-effective.

A. Content Management System

After consideration and comparison of alternatives, Drupal was chosen as the content management system (CMS) for PRISM. The choice was mainly due to Drupal's flexibility in terms of appearance, administration and functionality, and its fairly respectable security record, all of which are driven by a large and active user/developer base that has fostered the creation of many customizations (called modules) and responsive security patching. A major benefit of this level of participation is that even those without skill in software development can benefit from its openness, and sidestep the lack of extensibility problem in proprietary systems which is discussed by Masuda, Murata, Yasutome, Shibuya and Nakanishi [8].

1. Access Control

Drupal also allows for fine-grained access and administrative controls. This allows the owners of the site to delegate site moderation and maintenance responsibilities to various groups participating in different ways. For PRISM, five primary levels of user access (called roles) are designated: anonymous users, authenticated users, trusted users, moderators, and administrators. Anonymous users can only view content, authenticated users can post comments and rate content, trusted users can access source code and create some types of primary content, moderators have the ability to edit and remove content posted by other users, and administrators have full control over the site. Figure 1 illustrates the nature of privilege allocation. Higher trust users have all of the privileges of users in lower-trust groups, as well as permissions to perform potentially higher-risk actions. The ability to create additional classes of users gives PRISM the ability to adapt to future needs as the site grows.

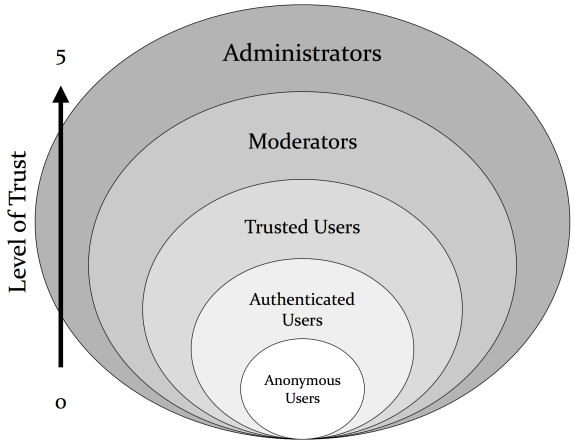

Figure 1. User class privilege sets

Because PRISM is a relatively small operation, the ability to publish content can be granted to just a few individuals within the organization without degrading site quality. This makes control easier, since most new content is submitted directly to moderators via web-forms for review before posting. Although this requires some up-front effort on the part of the moderators, it obviates the need to monitor the site for inappropriate postings (which can be tedious and time consuming) and is conducive to a healthy inverse relationship between set population and level of trust.

2. Extensibility

As PRISM will be a newly defined community resource, it is likely that changing requirements will be defined over time, and that initial requirements will become obsolete. Because of this, a platform for PRISM was chosen that has the ability to grow with the requirements of site users. Plug-ins or modules can be added or removed fairly easily by administrators to alter functionality. Components like forums, polls, chat, wikis, shopping carts, and social networking are not currently part of the site, but can be added with minimal to no programming knowledge.

Although installation of new functions (modules) is generally straightforward, configuration is often not, and sometimes requires considerable research and a good general understanding of the CMS to achieve the desired results. For example, creating views (content displays) based on content ratings requires manipulation of esoteric settings in various modules. The knowledge required to accomplish this task was garnered through the use of community-contributed how-to videos.

It should also be noted that with the addition of each module comes an increase in the complexity of site maintenance and operation, so it is important for administrators and designers to weigh benefits of each module installation, and only install and enable modules required for critical functions of the site.

3. Management

After modules are properly configured, actual maintenance of content within Drupal can be achieved without any programming experience. However, a strong working knowledge of HTML is beneficial for managing some types of content, and the ability to read, edit, and write PHP allows for the inclusion of functionalities not already captured in pre-packaged modules or snippets (small scripts written in PHP that can be included in content).

Updating the software itself is fairly labor-intensive, as there is presently no built-in update feature for core and add-on files. The next release of Drupal is expected to contain streamlined, automated updating of core files, modules and themes, and will further reduce maintenance costs. In the meantime, utilities like DRUSH (http://drupal.org/project/drush) can make management less time-consuming, but require command-line prowess. Again, the presence of technically inclined individuals in the participating organizations makes this disadvantage manageable for PRISM.

B. Software Stack

PRISM was also built upon free and open-source server technologies. Considerations for server software components included popularity, reputation, quality of documentation, and lab precedent (i.e., when possible, we utilized products already in use in the lab).

A fairly typical web server profile was configured using Linux (CentOS), Apache, MySQL and PHP (LAMP). Given general security concerns for public-facing web servers, each component was individually hardened prior to exposure to the Internet. Apache, MySQL and PHP were configured according to best-practices published by the developers. CentOS was secured according to the NSA Linux configuration guide[2].

We also decided to take advantage of the benefits virtualization has to offer (increased flexibility, reduced hardware and power consumption, and more efficient change management and disaster recovery) by installing the PRISM server on a VMware ESXi host. Consequently, PRISM can be co-located with other virtual servers on a single physical machine, and relocated to different geographic locations with minimal effort. Snapshot functionality allows administrators to roll back undesirable results from updates, intrusions or other unforeseen network events, and retention of up-to-date clones allows for quick recovery from catastrophic system failures. Finally, in the process of developing the PRISM site, a hardened, gold-master LAMP server was created, which can easily be repurposed for future projects that require a similar web-server configuration.

Figure 2 shows a summary of the software stack used for PRISM.

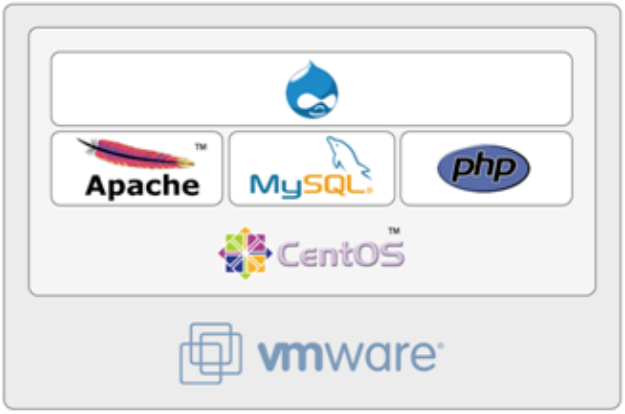

Figure 2. PRISM Software Stack

C. Hardware

Major hardware considerations were guided by ESXi 4 (http://www.vmware.com/resources/compatibility); essentially a 64-bit intel-compatible processor and supported storage adapter. Our solution was a Dell PowerEdge sc1425, with a RAID5 storage array. Although this configuration includes redundancy for storage devices and network interfaces, total failure of the server would result in a service outage. In the future, PRISM will likely be replicated at multiple physical locations for better resilience against environmental risks.

[2]http://www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml#linux2

V. Content Management

The major focus of PRISM is on categorizing content and presenting it to the end user in an intuitive way. In order for this to be accomplished, there must be clear protocols for content acquisition, and consistent methods of content categorization and review. There must also be measures in place to prevent abuse of the site through link spamming or the posting of malicious software.

A. Acquisition

Content for PRISM is acquired in one of two ways. It is either located by those who maintain the site, or submitted by end users and content developers. Content appropriated by PRISM staff is generally acquired in the form of links to external sites. In this case, we are responsible for evaluating the resource, attributing ownership, and categorizing appropriately.

Third parties can submit content directly to the site moderators, and it is subsequently handled in the same manner described above. Alternatively, a content developer can petition for special designation as a Trusted User on the site. This privilege level allows the user to upload and categorize materials autonomously, with final publication approval by moderators. This will ostensibly help to improve accuracy of metadata as the developer of a piece of content is likely the most qualified to describe it.

B. Categorization

The process of categorizing content is guided during the creation process within PRISM. Each content type (e.g. link, publication, activity, etc.) has a set of associated taxonomies that consist of pre-defined lists of meta-tags. Depending on the content type, some values are required in order to maintain a minimum level of organization on the site. Initial values are chosen at the time of creation, and can easily be updated by the creator or site moderators. Furthermore, any authenticated user has the ability to tag content, allowing a secondary organic categorical schema to develop within the site.

The overall structure and content of the aforementioned taxonomies is under development, and is the focus of an ongoing study at Regis University. In particular, input from users and usage statistics are being evaluated to determine which terms, taxonomies, and presentation styles generate the most universally relevant and useful search results.

Currently, a tailored subset of the Dublin Core[3] combined with additional elements is being used to organize PRISM content. Figure 3 shows a sample mapping of some of these metadata (the information available to match queries with results) to search drivers (those issues the user might want to address as they attempt to locate resources) in order to illustrate considerations we think are necessary to make information security teaching materials more available.

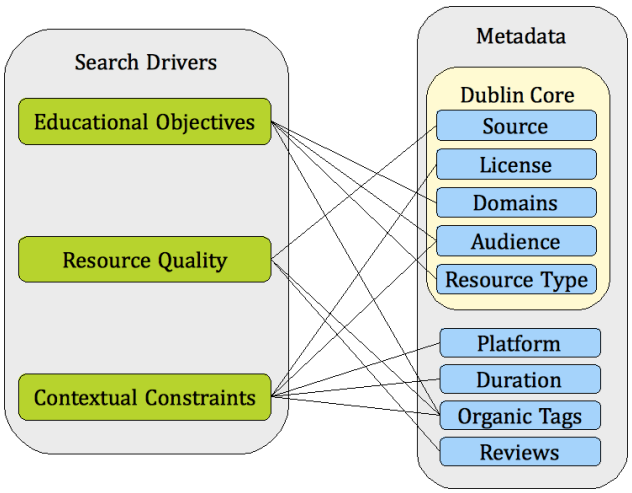

Figure 3. Search driver to metadata mapping

C. Review

There are two types of review that occur on the site that deserve note. First, site moderators review content submitted by entities who are not Trusted Users in order to determine suitability for posting. Relevance to information security education and completeness are considered, and scans are conducted on submitted files to identify software that could be dangerous to a user's system.

The second type of review is conducted by end-users. Currently, materials can be rated on the five-star basis and reviewed in the form of published comments. A slightly more fine-grained approach to content review is slated for implementation in the near future to allow for more information about the potential utility to be visually encoded with the materials.

D. Branding

Another major concern for developers is branding [5]. PRISM, like other repositories, provides full disclosure of ownership and copyright status. If the developer prefers,

[3] Dublin Core element guide: http://dublincore.org/documents/usageguide/elements.shtml

they can opt to host the material on their own servers, and link directly to the resource, or to their own descriptive content.

VI. Current Status

The PRISM site is fully functional and may currently be accessed at http://www.prismhome.org. Features and operations are constantly undergoing review and testing, and as previously mentioned, a study is being conducted to investigate the most effective method of organizing and presenting site materials for easy retrieval by an educationally oriented user-base. Furthermore, policy documentation is minimal, and its expansion would greatly ease the involvement of new site administrators, moderators and contributors.

Existing content consists of a selection of tools and papers from the sponsoring institutions, and links to a number of popular websites and resources that may be of interest to IS students and educators. As part of the initial set of tools available on the site, several visualization applets along with instructional materials and suggested exercises are available for viewing and download. They include:

- Passwords Web Lab
- Buffer Overflow Web Lab
- SQL Injection Web Lab
- Cipher Applets
    - Substitution
    - Shift
    - RSA
    - RC4
    - DES
    - Affine
    - Vigenere

These tools are designed to help facilitate active learning of information security concepts for students who may not have a strong background in computer science or security topics. The Web Labs are a series of web pages with embedded applets that allow the student to get hands-on experience with a concept in a controlled environment. Accompanying text provides instructions, background and context, suggested experiments, and challenges.

These tools also serve as models for those interested in developing educational materials to share with the community. The source code for each tool is available upon request for developers who would like to extend their functionality or use them as templates for related work.

Additional resources on the site include PowerPoint slides, a sample lab for Windows Vista security, security education publications, and links to various relevant websites.

Any user has the ability to contact site administrators and suggest material additions or modifications. However, in order for users to submit new material directly, account creation and login is required, and some level of trust must be established between the user and site moderators. This requirement is an effort to reduce spam and maintain the quality of site content.

Site content is currently tagged to express a number of attribute categories. Information security domain information is represented by ISC^2 CISSP common body of knowledge definitions. In order to provide educators with the necessary information to locate appropriate materials for their curricula and classroom capabilities, attributes such as exercise duration, grade level and platform compatibility have been added to a subset of the Dublin Core metadata element set.

Although all of the initial content has been tagged with relevant metadata, we hope users will take advantage of PRISM's built-in community tagging functionality to help make content descriptions relevant to a broad range of users. Figure 4 shows the current PRISM home page.

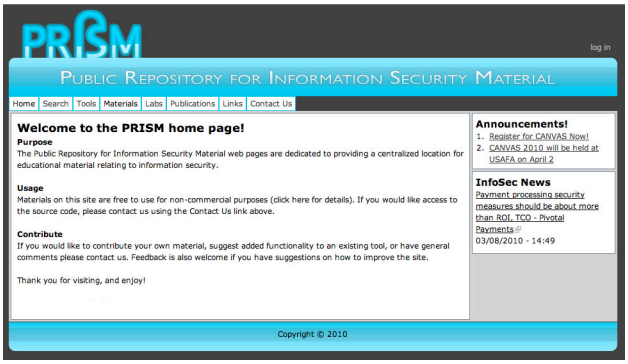

Figure 4. The PRISM Home Page

VII. Conclusions

Information security concepts are affecting an increasingly broad array of disciplines. We believe that integrating security topics into existing curricula would be more efficient and effective if a repository of educational materials existed that was easy to access, intuitive to navigate, and sufficiently stocked to address most common security concepts and contexts.

In order to realize this repository, PRISM has been developed as a portal to educational tools, publications, and other resources relating to information security education. Furthermore, a study is underway to develop a taxonomic structure capable of cataloging and describing

this content in a way that allows students and educators to find exactly what they are looking for with minimal effort.

As an educational resource, PRISM will only be successful with the support of the community. It is not intended to be a showcase of materials for a small number of institutions, but rather a community-wide collection of best practices, proven exercises, great ideas, and useful material. We encourage all security educators to make use of the site, submit their own material, and help make it a rich repository of teaching resources.

VIII. References

[1] Null, L. (2004). Integrating security across the computer science curriculum. *Journal of Computing Sciences in Colleges,* 19, 5, May 2004, pp. 170-178.

[2] Irvine, C., Chin, S., and Frincke, D. (1998). Integrating security into the curriculum. *Computer*, vol 31, no 12, 1998, pp. 25-30.

[3] Dicheva, D. and Dichev, C. (2006). Tm4l: Creating and browsing educational topic maps. *British Journal of Educational Technology*, 37(3), pp. 391 – 404.

[4] Wikiversity. (n.d.) *Classifying Educational Resources*. Retrieved from http://en.wikiversity.org/wiki/Classifying_educational_resources#Curriki

[5] Koppi, T., Bogle, L., & Bogle, M. (2005). Learning Objects, Repositories, Sharing and Reusability. Open Learning, 20(1), 83-91. Retrieved from ERIC database.

[6] Ellis, J. and Van Belle, J. 2009. Open source software adoption by South African MSEs: barriers and enablers. In *Proceedings of the 2009 Annual Conference of the Southern African Computer Lecturers' Association* (Eastern Cape, South Africa, June 29 - July 01, 2009). SACLA '09.

[7] Dedrick, J. & West, J. (2003) Why Firms Adopt Open Source Platforms: A Grounded Theory of Innovation and Standards Adoption. MIS Quarterly Special Issue Workshop, [Online], Available: http://www.si.umich.edu/misq-stds/proceedings/145_236-257.pdf.

[8] Masuda, H., Murata, K., Yasutome, S., Shibuya, Y., and Nakanishi, M. 2008. An integrated moodle system using VM technology to achive higher availability and lower TCO. In *Proceedings of the 36th Annual ACM SIGUCCS Conference on User Services Conference* (Portland, OR, USA, October 19 - 22, 2008). SIGUCCS '08.