Name of the Scholar- Antriksh Johri

Name of the Supervisor – Prof(Dr) Kum Kum Dewan

Department – Mathematics

Title of the thesis - ***A Prescriptive Framework to develop Secured Cyber Applications: A Design Phase Blue Print***

ABSTRACT

Cyber security, once an issue of interest for Intelligence Agencies of the various countries, has gained importance in almost all sectors of life wherever the new technology based advancements have taken place around the globe. Governments, Universities, Business houses, all have become vulnerable in one way or the other in today's cyber era where terrorism (w.r.t. violence as well as economic terrorism) has also become a prime issue of concern. The gravity of the threat has been well realized by all and a great effort is being put in developing methodologies and framework so that the newly developed cyber application provide good security while ensuring the authorized access to appropriate valid users. This thesis presents the ongoing efforts and development of Framework for the Development of Secured Cyber Application.

To make significant progress in the magnitude of cyber, security must be built into systems from the step one. New architectures containing new hardware designed to include embedded cyber security monitoring and processing capabilities and even especially designed to accommodate new cyber security analysis and new encryption and decryption techniques are needed.

At present, the cyber security comes up as a reaction to an attack and mostly it is achieved manually. Threats and vulnerabilities are defined and addressed only after they appear, are then identified, analyzed and distilled into well defined behaviors and even digital signatures. Definitely, today, sophisticated and intelligent systems are required which can detect and protect from threats based upon more than just tabulated data, using sophisticated, predictive mathematical models to "stay ahead of the curve".

Software with good security features is efficient enough to repel most attacks, tolerate the maximum no. of attacks which it cannot repel and is also able to recover quickly with a minimum of damage caused from the attacks it cannot tolerate. Development of high assurance security software requires knowledge and techniques which are not usually known or used in practice by most software developers.

Usually in a customary Software Development Life Cycle (SDLC), security is taken up as the last issue to be covered and all its scenarios like probabilities, estimation and solution are resolved at the very end after the software has been developed. Vulnerabilities are an emergent property of software which appears throughout the development phases.

When the security aspect is ever considered during the system life cycle, they are in general, features like password protections, firewalls, virus detection tools, and so on. These are, in fact, not security requirements at all but rather implementation mechanisms that are intended to satisfy unstated requirements, such as authenticated access. Thus, system specific security requirements which provide protection to essential services and assets are often overlooked. Even the view point of attackers is not calculated. So, the net result is that the security features, even which are present, are inadequate. Thus, a scientific approach dealing step by step with the security requirements will help to avoid the problem of generic lists of features and to take into account the attacker's perspective.

Including security at the beginning of the SDLC is often considered the most cost effective approach for two reasons (1) it is usually more difficult to add functionality into a system after it has been built, and (2) it is frequently less expensive to include the preventive measures to deal with the cost of a security incident.

Chapter 1 gives the foundation of this research work and talks about frameworks both theoretical as well as conceptual, besides narrating objectives and goals of the research work. Detailed survey of various issues has been discussed at length.

Chapter 2 details out various names and their criminal acts which have taken prominence in the history of Cyber Security. This chapter also details out most popular instances in Cyber Security breach. It also gives some statistical facts.

Chapter 3 deals with various types of risks as outlined by OSWAP such as Injection, Cross Site Scripting, Broken Authentication and Session Management, Insecure Direct Object References, Cross Site Request Forgery, Security Misconfiguration, Failure to Restrict URL Access, Invalidated Redirected and forwards, Insecure Cryptographic Storage and Insufficient Transport Layer Protection. It also suggests prevention from such risks.

Chapter 4 is about Cyber Applications Vulnerabilities, their classifications such as Design Vulnerabilities, Implementation Vulnerabilities, Operational Vulnerabilities and Overlapping nature of Vulnerability Type. This chapter also presents some statistical interpretation of various types of vulnerabilities.

Chapter 5 talks about Security Metrics Framework of the Web Applications. In this chapter, malicious cyber attacks, and the extent to which attackers can damage has been scripted. This also elaborates the need of standard and secure metrics besides the need for securing the Software Development Life Cycle at Design Phase, Deployment Phase and Run Time Phase. The chapter constructs metrics for various type of vulnerabilities such as Unvalidated Input, Broken Access control, Broken Authentication and session management, Cross Site scripting, Buffer Overflow, Injection flaws, Improper Error handling, Insecure storage, Application denial of service, Insecure configuration management etc.

Chapter 6 is about various Security Threats to Cyber Application and counter Measures for a Secure Design. The various threats as mentioned above have been taken into account and their counter measure at design phase has been detailed out. This chapter gives a fair idea to take complete control of the access of the site. It is pertinent to mention that security requirements will keep on changing in response to changed environment. However, as per present scenario, the counter measures have been suggested in this chapter for various threats.

Chapter 7 gives live examples of various security features incorporated in an application which got developed for online registration of examinees and generation of various reports in CBSE. The security features introduced are at Data Validation stage, (to prevent SQL injection attack), stored procedures for data queries, prevention of direct URL execution, prevention of automated login attempts from bots and, hiding of run-time execution error from the user. This chapter also suggests security checklist comprising of both black Box checking and white Box checking etc.

Chapter 8 brings out prescriptive framework to develop secure cyber application. In this chapter, a Secure Software Development Life Cycle (SSDLC) has been introduced. The complete road map for web application security has been proposed. Besides this, a secure Software Development Model has been designed. A general SDLC is discussed that includes the following phases: initiation phase, acquisition / development phase, implementation phase, operations / maintenance and disposition phase. In addition to above, a complete IT Security in the Software Development Life cycle has been put forward. Finally, a complete Application Security Lifecycle model has been proposed.

Chapter 9 presents conclusion and future scope. Though in every chapter recommendations and / or conclusions have been proposed, in this chapter, however, a consolidation has been done.