International Journal of Engineering Innovation & Research
Volume 1, Issue 2, ISSN : 2277 – 5668

# Design of Enterprise and Web Application Architecture for Secure Information System

**Dr. Banta Singh Jangra**
Associate Professor, Department of Computer Science and Engineering,
Haryana Institute of Technology, Bahadurgarh (Haryana) India
Email-ID: bsjangra@gmail.com, Mob: +91-9466724882

***Abstract*** **- In this paper we design and provide the tempering of systems can cause huge damage and hence it becomes extremely critical to understand all the aspects around avenues of security threats as well as understand the possible solutions to safeguard and secure the information flow. A Security Architecture Blueprint is must to bring focus to the key areas of concern for the enterprise, highlighting decision criteria and context for each domain. Security services provide confidentiality, integrity, and availability services for the platform. Security services are implemented as protection services, such as authentication and authorization, detection services, such as monitoring and auditing, and response services, such as incident response and forensics.**

***Keywords*** **- Design of Enterprise, SDLC, Vulnerability, Secure Information System, Application Architecture,**

## I. INTRODUCTION

A risk management centric approach allows for the security architecture to be agile in responding to business needs. Risk is a function of threats exploiting vulnerabilities against assets. The threats and vulnerabilities may be mitigated by deploying countermeasures. The risk management process implements risk assessment to ensure the enterprise's risk exposure is in line with risk tolerance goals. This does not mean that behavior is uniformly risk averse or risk seeking. The system should take on the appropriate level of risk based on business goals. Risk management, security policy and standards, and security architecture govern the security processes and defense in depth architecture through design guidance, runtime support, and assurance services. Security metrics are used for decision support for risk management, security policy and standards, and security architecture. The security architecture should have a reference implementation for developers and other IT staff to review what functions the security mechanisms performs, and how they do it.

## II. VULNERABILITY MANAGEMENT

The set of processes and technologies for discovering, reporting, and mitigating known vulnerabilities. The vulnerabilities may reside at any system layer – database, operating system, servers, and so on; specialized tools probe for known vulnerabilities. It is important to differentiate threat management and vulnerability management. The threat environment contains many unknown mysteries around attacker techniques and goals, attackers will identify currently unknown vulnerabilities (zero day attacks), but there are many known vulnerabilities that the security team can act on, while the threat landscape is inherently less predictable meaning security is reactive to threats and can be generally proactive towards dealing with known vulnerabilities. This has direct implications on staffing, prioritization, and investing in these areas, because vulnerability management has a more predictable lifecycle based on the known quantity of much vulnerability.

## III. APPLICATION SECURITY

It may deals with two main issues: 1) protecting the code and services running on the system, who is connecting to them, and what is output from the programs through a combination of secure coding practices, static analysis, threat modeling, participation in the SDL, application scanning, and fuzzing. 2) Delivering reusable application security services such as reusable authentication, authorization, and auditing services enabling developers to build security into their system. Security frequently collaborates with software architects and developers in this area to build security into the system.

## IV. ARCHITECTURE RISK ASSESSMENT

Assesses the business impact to critical business assets, the probability and impact of security threats and vulnerabilities. Since security is a system property, the architectural level is the proper level of abstraction to identify many of the most critical security flaws. The DHS Build Security In paper "Architectural Risk Analysis"6 defines a method for assessing the application's assets, threats, and vulnerabilities.

## V. SECURITY ARCHITECTURE AND DESIGN

Architecture and design of security services that enable business risk exposure targets to be met. The policies and standards, and risk management decisions drive the security

architecture and the design of the security processes and defense in depth stack.

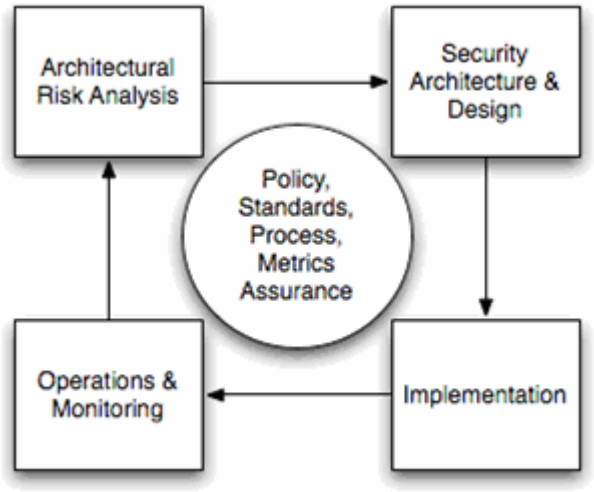


Fig. 1 : Security Architecture Lifecycle

## VI. IMPLEMENTATION

Security processes and services implemented, operational, and managed. Assurance services are targeted at verifying that the Risk Management, Security Policy and Standards, Security Architecture decisions are reflected in the actual runtime implementation.

Despite the "dot bomb" stock market debacle, most organizations continue to roll out new web-based business applications at a feverish pace. This phenomenon is not tied to a single vertical market. In fact, the trend toward web-based or true network computing spans both governmental and commercial organizations, and is evident in industries as diverse as insurance, banking, and finance to manufacturing, health care, pharmaceutical, and computers. Unfortunately, while there has been real progress in protecting corporate network infrastructure over the last few years, many organizations' web-based applications remain at very high risk.

To date, most security activity has emphasized securing the IT infrastructure. Certainly a secure network and systems infrastructure are critical to delivery of a secure web-based application. These include properly and securely configuring the base infrastructure elements such as servers, routers, switches, etc., and instituting changes and patches over time to remove new vulnerabilities. It also requires putting in place protective measures such as traditional firewalls, ensuring network- and system-level access controls, and appropriately protecting data and transactions through virtual private networks (VPNs) or other cryptographic measures. Infrastructure-level security also involves such measures as monitoring for potentially malicious activity or for denial of service conditions.

A comprehensive, systematic approach to implementing security from the very start of a new business application project is now considered to be the "best practice" approach. A standard firewall, for example, will fail to sufficiently protect a web-based application that was not designed with appropriate security in mind, or otherwise adequately protected. Security teams will have to work more closely with the architecture and design, application, infrastructure, IT, and business teams to ensure secure applications. While this is rather easy to state, META Security Group understands that designing and implementing the myriad of technical security controls, policies, processes, and procedures mentioned in summary form above can be an overwhelming task. Therefore we recommend, in keeping with a core META Security Group philosophy, a phased approach. Our recommended phasing takes into account often-present resource and budgetary constraints, and is designed to ensure the earliest initiatives have, from a risk reduction perspective, the highest return on investment (ROI).

### *Top 10 Challenges for Enterprise Security*

Every enterprise that relies on network-connected applications and services is subject to 10 key security realities:

1. The Internet was designed to share, not to protect.
2. Security is not optional.
3. The bad guys have good guns.
4. Security threats recognize no boundaries.
5. Security depends on people, process, and technology.
6. It's not enough to guard the front gate.
7. There's no stock blueprint.
8. Frisking everybody and everything takes time.
9. Grace under fire is a requirement.
10. Security is a closed-loop process with an open-ended date.

Financial institutions developing or reviewing their information security controls, policies, procedures, or processes have a variety of sources upon which to draw. First, federal laws and regulations address security, and regulators have issued numerous security related guidance documents.5 Institutions also have a number of third-party or security industry resources to draw upon for guidance, including outside auditors, consulting firms, insurance companies, and information security professional organizations. In addition, many national and international standard-setting organizations are working to define information security standards and best practices for electronic commerce. While no formal industry accepted security standards exist, these various standards provide benchmarks that both financial institutions and their regulators can draw upon for the development of industry expectations and security practices.

## VII. THE ENTERPRISE GOVERNANCE

Governance is achieved through the management structure, assignment of responsibilities and authority, establishment of policies, standards and procedures, allocation of resources, monitoring, and accountability. Governance is required to ensure that tasks are completed appropriately, that accountability is maintained, and that risk is managed for the entire enterprise. All aspects of institutional governance are important to the maintenance of a secure environment.

Information security is a significant business risk that demand engagement of the Board of Directors and senior business management. It is the responsibility of everyone who has the opportunity to control or report the institution's data. Information security should be supported throughout the institution, including the board of directors, senior management, information security officers, employees, auditors, service providers, and contractors.

Each role has different responsibilities for information security and each individual should be accountable for his or her actions. Accountability requires clear lines of reporting, clear communication of expectations, and the delegation and judicious use of appropriate authority to bring about appropriate compliance with the institution's policies, standards, and procedures.

## VIII. CONCLUSION AND FUTURE WORK

Data Security is the key concern and the top most priority for most of the organizations. For some of the organizations, Data is the only asset, so protecting it from competitors and outsider becomes extremely critical for the survival and viability of business. Organizations of today's generation start with keeping 'Data Security' as an integral part of their operational aspect. It's not considered as an additional and/or optional activity.

## REFERENCES

[1] A. Felt, "Defacing Facebook: A security case study," Jul. 2007, white paper. [Online]. Available: http://www.cs.virginia. edu/felt/fbook/facebook-xss.pdf

[2] A. Felt, P. Hooimeijer, D. Evans, and W. Weimer, "Talking to strangers without taking their candy: Isolating proxied content," in 1st International Workshop on Social Network Systems, Glasgow, Scotland, Apr. 2008.

[3] A. Nguyen-Tuong, S. Guarnieri, D. Greene, J. Shirley, and D. Evans, "Automatically hardening web applications using precise tainting," in 22nd IFIP TC 7 Conference on System Modeling and Optimization, Turin, Italy, Jul. 2005.

[4] A. V. Aho, M. Lam, R. Sethi, and J. D. Ullman. Compilers: Principles, Techniques, and Tools. Addison-Wesley, 2007.

[5] American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard –748–1998, Earned Value Management Systems, May 19, 1998, and reaffirmed on August 28, 2002.

[6] Andrea Bittau, Mark Handley, Joshua Lackey, "The Final Nail in WEP's Coffin," the 2006 IEEE Symposium on Security and Privacy, Oakland, CA

[7] Anirban Chakrabarti and G. Manimaran, Iowa State University, "Internet Infrastructure Security: A Taxonomy", IEEE Network.

[8] Anoop Singhal and Theodore Winograd, "Guide to Secure Web Services". NIST Draft (800-95), September 2006.

[9] Arconati, Nick. "One Approach to Enterprise Security Architecture." 14 Mar. 2002.

[10] Arun Kumar, Neeran Karnik and Girish Chafle, "Context Sensitivity in RBAC", ACM SIGOPS Operating Systems Review, 36 (3), July 2002.

[11] AusCERT, Computer Crime and Security Survey, 2006,

[12] http://www.auscert.org.au/images/ACCSS2006.pdf

[13] http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

[14] http://www.arctecgroup.net/secusecase.htm.

[15] http://www.cgisecurity.com/lib/ProtectingWebBased Applications.Pdf.

[16] http://www.filesonic.com/file/26012845/Information.Security.Architecture-0849399882.pdf

## ABOUT AUTHOR

**Dr Banta Singh Jangra**
MCA M.Phil, PhD in Computer Science, Presently working as Associate Professor in Department of Computer Science and Engineering in Haryana Institute of Technology, Bahadurgarh (HR). Member Editorial Board for Various International Journals.