Advisory for Securing Different Assets of an Organization

Uttam Kumar Dash[1], Debnath Bhattacharyya[2] and Tai-hoon Kim[2]

[1]*Information Technology Department*
Heritage Institute of Technology
Kolkata, India
ud82@rediffmail.com

[2]*Hannam University*
Daejeon, Korea
debnathb@gmail.com, taihoonn@empal.com

Abstract

The organization trying to manage information security manually or automatically. The preliminary task is to first understand and identifying the security requirements, which generally includes everything starting from hardware, software and information assets, threats and vulnerabilities associated with them, different network connections and topologies used for transferring information to and from the enterprise.

Security infrastructure advisory is a specified set of entities, both physical as well as software, in order to implement the set of identified controls. It tells an individual/organization the details regarding the security tools and the exact location of security tools, required to mitigate the security risks of the organization. In this phase, the security infrastructure advisories for different assets and platforms are generated. After getting the security infrastructure specification, the organization decides on the particular infrastructure that it would like to implement..

Keywords: *Information, security, advisory, probability.*

1. Introduction

1.1. Enterprise Information Security Management (EISM)

Today's civilization is becoming more and more dependent on information infrastructure and this increasing dependency on information infrastructure is also the main reason behind rise of vulnerability breaches, threats, network attacks and cascading of pervasive failures. This is mainly because of lack of inherent security in new technologies, flaws in hardware and software products, poor information system design and management, lack of proper management of information systems and certainly lack of security awareness in the information system users. So, these flaws and weaknesses can be easily exploited to attack several enterprises like banking, telecommunication, energy, health and transportation etc.

Earlier, some sort of network security measures and were only taken into account to protect organization assets and information, but these types of security measures are not sufficient in case of today's dynamic and remote network infrastructures. Network or transport layer security is also not sufficient to protect organization from application level attacks.

So, security management will remain separate from network and systems management. But, security management will use network and systems for data collection, decision making and taking preventive and corrective actions.

1.2. Enterprise Information Security Engineering Lifecycle

The primary goal of securing enterprise information is to reach business goal by continuous business operations, but operations performed by the organization, its users, assets associated to this entire process are also major concern. Another important issue is that the need of securing information of any organization is not static but changes frequently depending upon the business requirement, technological and theoretical upgrades etc. Hence, a structured process for developing and deploying proper Information security infrastructure is necessary.

This leads to the concept of Information Security Engineering Life-Cycle, or simply "Security Engg. Life-Cycle" [shown in Figure 1]. Any process which needs to be survivable has to take a life cycle approach [11]. Following phases are considered to be of prime importance for this Life-cycle concept. Each phase can be implemented following the ISO 17799 code of practice.

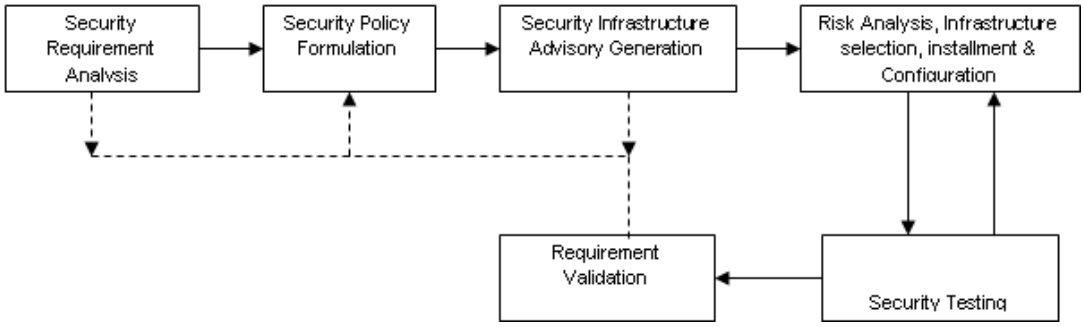

Figure 1. Security Engineering Life Cycle (SELC).

- Security Requirement Analysis: This is the very first step to be followed by the organization trying to manage information security manually or automatically. In this step, the preliminary task is to first understand and identifying the security requirements, which generally includes everything starting from hardware, software and information assets, threats and vulnerabilities associated with them, different network connections and topologies used for transferring information to and from the enterprise, different access control mechanism in place etc. In this phase the user enterprise is asked a set of questions to extract all the above mentioned information associated with the business.
- Security Policy Formulation: A security policy is used to translate, clarify and communicate management's position on security as defined in the high level security principles. A security policy manual can be defined as a set of high-level statements describing the objectives, beliefs and goals of the organization as far as security is concerned. It should not state how these controls are to be implemented. During this phase, the enterprise information which was collected in the previous phase, is analyzed and by following a well accepted information security standard, a set of controls are selected for the enterprise. Depending upon the selected controls, policy

manuals are prepared. The policies should be technology independent as much as possible and must not change frequently.

- Security infrastructure Advisory Generation Phase: Security infrastructure advisory is a specified set of entities, both physical as well as software, in order to implement the set of identified controls. It tells an individual/organization the details regarding the software necessary, the access rights of individuals, the exact location of security tools, etc., required to mitigate the security risks of the organization. In this phase, the security infrastructure advisories for different assets and platforms are generated. After getting the security infrastructure specification, a cost-benefit and detailed risk analysis is performed by the management of the organization concerned. Based on this, the organization decides on the particular infrastructure that it would like to implement.
- Security Testing and Validation: The main objective of the security testing would be to ascertain that the proposed security infrastructure is in place and working. Other than this, the system can be tested for faulty combination of software, known security holes and potentially dangerous application that can be compromised to breach the security infrastructure.
- Review and Monitoring: The Review process involves the review of the requirement, policy, infrastructure and testing so that the different entities do not become stale and create holes in the security framework. The Review may be triggered by changes in the Organizational Structure, Business goals and activity.

The outcome of the Review and Monitoring may re-initiate the activities of the Requirement analysis, Policy Formulation, Risk Analysis, Infrastructure updating and Testing & Validation. This is how the Security Engg. Life-cycle works.

2. Previous works

Web Security – I was a project funded by Department of Information Technology, Govt. of India and was developed by Department of Computer Science Engineering, Jadavpur University. The main purpose of the project was to develop a formal model of enterprise information security and to develop a set of metrics for management decision making on information security issues. Based on the above model and the metrics, a standard Framework for Enterprise Security Management was to be developed along with a number of component services integrated with the Framework to automate different phases of the Security Engineering Life-cycle.

The primary objective of the project was to develop the idea of systematic design and management process of Enterprise Information System Security (EISM). The team has put forward the idea of the Security Engineering Life-cycle comprising of the following phases:

a. Security Requirement Analysis phase
b. Security Policy formulation phase
c. Security Infrastructure Advisory phase
d. Security Testing phase.

The project work resulted into the following theoretical developments:

a. Security Requirement Analysis Methodology
b. An XML-based Language to express the Requirement Specification
c. Security Risk Analysis Methodology
d. Identification of Baseline Policies, Guidelines and Procedures
e. Methodology to generate infrastructure advisory

f. Methodology to generate the compliance test cases from the Requirement Specification

A major strength of the concepts developed is that all the concepts have been correlated with the ISO 17799 Standard on Best Practices for Information Security Management System.

During the lifetime of the project the members developed a suite of tools, which has been developed for partial automation of the security design and management activities of Enterprises, based on the concepts developed and the ISO Standard. The suite consists of the following tools:

a. A security requirement analysis tool
b. A security policy formulation tool
c. A security infrastructure advisory generation tool
d. An automatic test case generation and penetration testing tool

The Requirement Analysis Tool elicits the security requirement in the form of the IT Asset Register, the security requirements for each asset in terms of the parameters confidentiality, integrity, availability, authentication, non-repudiation and legal requirement. The tool analyses the objectives and control requirements, performs the gap analysis and initial vulnerability analysis. This is coupled with the Risk Analysis phase where the risk is calculated for each kinds of threat considering all the vulnerabilities exploited. This analysis classifies the assets into the high, medium and low risk categories to take suitable steps for the mitigation the threats.

The Policy development tool takes the requirement analysis report as input and generates the model baseline policy, guideline and procedure manuals for the enterprise.

The Infrastructure Advisory Generation Tool takes the requirement analysis and risk analysis report as inputs and generates the infrastructures necessary for the implementation of the selected controls.

The Security testing tool integrates two major requirements of automatic test case generation for control checking and compliance testing and penetration testing. The first sub-phase generates the test cases from the test plan repertoire for control and compliance checking from the Requirement Analysis report. This sub-phase also helps the test personnel to generate the test report in a multi-session mode. The second sub-phase of the tool has integrated the network mapping, the penetration testing, password cracking and traffic analysis tools for penetration testing from the same platform.

2.1. A web services based approach to EISM

2.1.1. Scope of application of Web Security – I: The outcome of the project Web Security – I was a systematic process for handling information security of an enterprise. But, before completion of Web Security – 1 there was no such automated tool in the market, integrating all the phases of security engineering lifecycle. The benefits are rapid development of the policies, comprehensive and detailed risk analysis, control-based infrastructure deployment and automated and integrated testing. The users of different sectors are already realizing the importance and benefit of such an approach.

Though the final output of Web Security – I was much appreciated and accepted by different Govt. and private organizations, it has some limitations due to the fact that it is a standalone application. As it is a standalone system, clients can use only the GUI provided by us and thus no client will be able to access the services of the system programmatically.

Though updating the system with changing business need is essential, in this case it is quite an impossible job for the service provider.

Due to all these problems, limitation and enhancement of the product of Web Security – I, the need of a web-based object-oriented framework is felt. In the next phase of the work, we have tried to prepare a web based information security management tool and Web-enabled Information System Security Design and Operational Management (WISSDOM) is the outcome of the work.

2.1.2. Need of WISSDOM: Due to the problems and limitations of Web Security – I discussed in the above section, the proposal for next phase of work Web Security – II was made. Following are the major requirements to be fulfilled in the second phase of work i.e. WISSDOM.

a. Even for any medium sized organization, managing the system is very difficult by human beings. In that case some formal models of the system are needed. In case of information security management also, we need some formal models to make the EISM automated. By following different formal models like Clark-Wilson model for integrity; Bell-La Padula Model for Database Access and different Access Control Models, it will be easy to validate the outputs of the system and thus customers can be served with more confidence.
b. Security design and management is becoming too complex with the increasing interplay among technologies, management, economics, social issues and large volume of data to be managed. Now, in case of information security management it is necessary to make the system always consistent with major changes in these fields. So we need to develop such a system so that organizations can get the upgraded version of the system to manage information security of their organizations. WISSDOM needs to be developed as a dynamic system with tools based on formal model.
c. In case of this phase of work, one of the primary objectives is to deliver a tool suite to support different phases of security engineering life cycle with in a web-based object-oriented framework so that the clients can get the services from anywhere of the world. By following this kind of framework rapid deployment and integration of newer version of the system will be easier.
d. Another objective of the work is to develop good quality training manual on the web.

To implement effective security architecture for WISSDOM, we need to first identify the components being used by WISSDOM that can be targeted by the attackers. Then we need to identify what are the existing vulnerabilities of the system that can be exploited by the external or internal entities. We need to also recognize the probable paths of attack or we can say the ways the attackers will try to attack.

As WISSDOM follows one or several information security standards to perform security analysis of the enterprise information, we have also tried to perform a risk assessment of WISSDOM by following security standards. According to most information security standards we follow in WISSDOM, the risk assessment for the assets we need to first identify the vulnerabilities of the system and the threats those exploits the vulnerabilities. After we get the list of threats and vulnerabilities associated with the system, we need to prepare a list of threat-vulnerability pair where each threat-vulnerability pair indicates which threat exploits

which vulnerability. Upon listing the threat-vulnerability pair list, we can plan for countermeasures to protect the threats. The basic steps for risk assessment are:

a. Identifying and prioritizing assets
b. Identifying Vulnerabilities
c. Identifying Threats and their probabilities
d. Identifying security tools for countermeasures

3. Our work

3.1. Identification and Classification of Resources, Threats and Vulnerabilities

3.1.1 Resources used: We classify our entire set of assets in 3 categories

a. Hardware Assets
b. Software Assets and
c. Information Assets

Hardware Assets: We can list the hardware assets as follows.

a. One Server used for deploying web server (to deploy the client application web module). This machine is to be connected to Internet
b. One Server used for deploying Business Services (Enterprise Java Beans (EJB) and Web Services) in an Application Server (Sun Java System Application Server). This machine is to be connected to the Internet.
c. One Server used for deploying Authorization and Authentication Services. This machine need not to be connected to the Internet, but need to be connected to the others.
d. One Server used for Databases.

Software Assets: Software assets associated or consumed are very important from the point of view of security. By the term software assets we don't mean only the software we have developed or the software we are using to run and deploy our application. It is the system software which we should also take care of. The operating systems and the system software are some inherent weaknesses which can be exploited by the hackers and that may cause the system to crash or overloaded. Although these vulnerabilities may not harm the business information directly, but by attacking the operating system the system may become unavailable for service.

The software assets associated are as follows:

a. Serverware: Sun Java System Application Server Platform Edition 8.1(SJSAS PE 8.1) as Application Server (EJB container and Web Container)
b. Database Server: Microsoft SQL Server 2000 as database.
c. Operating System: Microsoft Windows 2000 Professional.
   Microsoft Windows XP Professional/Enterprise Edition
   Linux Fedora Core 4
d. Application Software: Microsoft SQL server 2000 driver for JDBC

Information Assets: Information assets need to be secured for the sake of confidentiality and integrity of client information, business continuity and reputation of the organization. Several types of information are processed and stored in the database. Depending upon the type of information and the purpose of them, we can classify the set of Information assets as follows.

a. Client Information: In several form client information are processed but stored as database rows. During communication the client information are transmitted as XML (Simple Object Access Protocol (SOAP)) message. So ensuring security of these messages is as important as the information in the database.
b. Application Management parameters: This type of information is mainly related to proper functioning of WISSDOM. In fact, there are several information like the security standards, general threat and vulnerability information etc. are necessary while processing the client request for a particular service provided by WISSDOM. These information need to be secured for continuous and accurate performance of WISSDOM.
c. Logged Information: This information is stored to log information about several events occurring during processing client request. This information is useful to track the activities performed and in case of any malfunctioning it can be useful to detect the problem. One additional advantage is that the client cannot deny an activity that he/she has indeed performed. So, this information must be kept secured and must not be modified either by the administrator or by the client.

3.1.2. Identification of Vulnerabilities: Vulnerability is an inherent weakness in design, configuration or implementation of a network or a system that renders its susceptible to a threat. Mainly due to poor design, implementation and management of a system, several vulnerabilities are found in the system. While these are the sources of vulnerabilities, the vulnerabilities can manifest themselves in many ways.

We have identified some of the serious vulnerabilities and those are listed below.

a. Lack of Input size checking: Size of the input data sent by the client has to be checked prior to call a business method. In the database, each field is supported with a maximum length and if the data to be stored in that field crosses the upper limit, the business method will not be completed properly.
b. Lack of input data type checking: Every time a business method is to be invoked the type of the input must be checked in prior. As the client application sends data through a XML message, there is no way to determine the types of various data sent by the client application..
c. Lack of Input data format checking: Sometimes some of the information passed to a web service must be in a specific format. If that is violated the business method will not work properly and the system will behave accordingly.
d. Lack of Invalid character checking: During development of the system, some characters were used as special characters for different purposes. If the client data contains any of those special characters the system will not work accordingly. So the clients must be restricted to include those characters with in client data.
e. Inefficient encryption algorithm: If sufficient care is not taken during selection of encryption algorithm, the cryptographic module will not be able to guarantee desired level of confidence for the system users about the confidentiality of their messages.
f. Unsecured encryption algorithm and keys: In addition to an efficient encryption algorithm, efficiency of the encryption process depends on two parameters: security of the encryption algorithm and confidentiality of encryption keys (private). Normally those algorithms which are designed by new or inefficient designer or unpublished encryption algorithm or those which relies on random number generation but in fact a poor random number generator are considered to be unsecured.

g. Lack of enough Logging and auditing: Lack of enough logged information debugging and maintaining the system becomes harder. Auditing is essential for recording clients' behavior and audit trails are also very important for avoiding repudiation of request/response. In addition to this the logged information must be kept secured and in any case it must not be modified by anybody in the system.
h. Lack of proper administrative services and/or configuration Management: Controlled access to the system will enhance more security. If administrative services are not properly designed and developed then by breaking the service security anybody can perform some administrative operation intentionally or accidentally and can cause serious damage.
i. Lack of countermeasures for viruses and worms: Absence of industry standard antivirus is a major weakness of any important computation system explored to Internet.
j. Lack of load management of servers: Often potential hackers try to overload the system by running or invoking same application multiple times or by sending large messages as parameters etc. which consumes lots of CPU cycle, memory space and other resources and that may lead to system crash.
k. Lack of proper security policy for messages in transmission: Messages in transmission are very sensitive from security point of view because this is the time when the system is mostly attacked by hackers. If the messages are not properly secured then the message can be read by some third parties, which violates confidentiality property of the message. The message also may be altered during transmission, which violates integrity of the message.
l. Insufficient network boundary security control: If the network boundary of the system i.e. the boundary of the zone where the system is finally deployed is not properly secured then any non-legitimate person can get access of the system and can fetch confidential information from system storage.
m. Poor Exception handling: Exceptions that are allowed to propagate to the client can reveal internal implementation details that make no sense to the end user but are useful to attackers. Applications that do not use exception handling or implement it poorly are also subject to denial of service attacks.
n. Incorrect/Inefficient handling of media: If a database fails, for example, due to a hardware/software fault or an act of sabotage, this could have far-reaching consequences, depending on the function and significance of the database. In this case, the data in the affected database, are rendered unusable. As a result, users of this application can no longer perform some or all of the tasks [1].
o. Irregular or insufficient back-ups: Regular and sufficient backups are very much necessary for business continuity. Irregular and insufficient backups can lead to loss of data, database inconsistency, loss of data correlation [1].
p. Inefficient storage space: Once the maximum capacity of the storage medium is exhausted, the database might crash and result in a loss of data.. The capacity of the storage medium can suddenly be exhausted due to various reasons, e.g. due to errors in the application program, increased storage requirements of the users or a malicious attack intended to specifically reduce the existing storage space [1].
q. Poor Authentication Service.
r. Poor Authorization Service.

3.1.3. Identification and classification of threats: Literally a threat is anything that can disrupt the operation, functioning, integrity or availability of a network or system. There are several types of threat under consideration but In case of web service based applications we

have to look at from a different angle. Like any other computational systems there some common threats, like environmental threats, communicational threats, are associated with this kind of application. But we will look into a set of threats, which are specifically related to any web service based business application.

XML-based threats can be classified in many ways [10] but depending upon the effect of the attack on the web service based enterprise application, we can categorize the attacks as follows:

a. Identity based Attack: In this case, hackers try to steal identity of authentic users of the system and use that identity to interact with the system such that the system treats them as legal user.
b. Content based Attack: In case of Internet, it uses standard ports for all communications – generally port 80 for all HTTP traffic. The "port 80 problem" is that viruses and malicious content can get tunneled through port 80 to reach the inside of an organization. Once malicious content carried by XML is tunneled through this port, it arrives at enterprise servers, applications and databases and can weak havoc. Content-based attacks are also known as XML viruses or worms.
c. Application level Attacks: The third classes of XML web services attacks are operational. These attacks make services unusable for everyone and can bring the entire organization down.

While suggesting the security architecture, we'll be categorizing the threats in a different way. Firstly we take a look of a set of threats that are general in nature and we group them as General Threats. Secondly, there are a group of threats that mainly comes from external users of the system i.e. service consumers, intentionally or accidentally. We call these threats as External Threats. Similarly there are a group of threats called Internal threats, which normally imposed by the internal users i.e. group of administrators of the system. A set of threat which are imposed by communicational errors are also a serious concern as these kinds of threats causes loss of integrity and confidentiality of message during transmission. This group of threats is called as communicational Threats.

Following are a details description of some of the important threats those must be considered.

General Threats:

a. Buffer overflow [9]: In a buffer overflow situation, a long input data may not be gracefully handled by the service end point. If the receiving system is not prepared to handle unexpected field and message length, the application may be compromised. The application may be crashed, causing access to the system or possible downtime.
b. Denial of Service (DoS): These are the best known and particularly dangerous attacks. Denial of service means doing something to consume available resources such as memory, network, disk space or CPU cycles, without doing useful operations. As a result the attacked system spends time in working on useless messages. And hence it becomes unable to service legitimate requests.
c. Computer Viruses and Worms [1]: Like in case any other computational system, computer viruses and worms are a serious threat. In case of any web service application the source of viruses is mainly the messages those are used for web service producer-consumer communication.

d. WSDL Enumeration [5]: The WSDL file contains significant information available as to where a particular service is, what types of functions are called within the web service and how to interact with such a service. WSDL may also reveal what tools generated the web service providing attackers with more information on the environment. The attackers may successfully exploit some weaknesses of the environment in spite of proper authentication and authorization policy in place.
e. Cross-Site Scripting (XSS): SOAP and XML are standards used to wrap data for easy consumption. SOAP provides enveloping information to deliver messages in a seamless fashion between heterogeneous applications. Embedded characters or malicious code can be sent via the portion of the XML which will not be parsed. The receiving application may display or execute the data in unintended ways.
f. Coercive parsing [10]:. Parsing of the SOAP messages are required to extract parameters, determine which method to invoke, insert content into the database or perform some other functions. This basic operation is an easy target for a hacker to create a Denial of Service attack or degrade application performance. Web service and existing infrastructure do not provide protection for XML-based attacks. Putting in recursive relationships to create entity expansion, bogus parameters and significant amounts of white space can cause XML parsers to be overloaded or to perform unexpected problems.
g. SOAP attachments [9]: One important use of web services is to transmit large documents as attachments to smaller messages: so-called SOAP with attachments. This mechanism provides another way to transfer malicious content through the network – carried along with XML.
h. Mistake or alteration of encrypted data [1]: To maintain confidentiality, if SOAP messages are encrypted with private/public key encryption then successful decryption of the message at the either end is subjected to unaltered encrypted message otherwise it may lead to system overloading.
i. Failure of crypto module or insecure crypto-algorithm [1]: The failure of a crypto module can also result in various types of damage. It is no longer possible to protect a data transmission path using cryptographic procedures, making it temporarily impossible to preserve the confidentiality of the data. Encrypted data can no longer be decrypted until the required crypto module becomes available again.
j. Failure of a database: If a database fails, for example, due to a hardware/software fault or an act of sabotage, this could have far-reaching consequences, depending on the function and significance of the database. In this case, the data in the affected database are rendered unusable. As a result, users of the application can no longer perform some or all of the tasks assigned to them, unless these tasks can be carried out manually.
k. Loss of stored data: The loss of stored data can have a major influence on any other enterprise application. Loss or forgery of application data or customer databases could threaten the existence of private enterprises.
l. Loss of database integrity/consistency: A loss of database integrity or consistency means that, although data may still exist in a database, it has become corrupted or unintelligible. As a result, the data cannot be correctly processed any more. This could be due to a variety of causes, for example, inadvertent data manipulation

(e.g. unintentional modification of data), inadequate synchronization control of transactions or deliberate attacks.

m. Loss of data confidentiality: In the case of classified information (such as passwords, person-related data, certain business-related and official information, and research & development data) there is an inherent danger of the confidentiality of this information being impaired inadvertently or intentionally.

External Threats:

a. SQL injection [5]: It is a process of inserting malicious SQL statements into the XML in order to disrupt the normal operation of the system. If a web service connected to a database doesn't validate SQL, an incoming XML message containing rouge SQL statements could be used to obtain unauthorized information or to destroy data.
b. Parameter tampering [10]: Since the parameters of an operation are described within a Web Services Description Language (WSDL) document, the hacker can play around with different parameter patterns in order to access unauthorized information. The key to defending against malicious parameters is to validate all data.
c. Schema Poisoning: An attacker may attempt to compromise the XML schemas in its stored location and replace it with a maliciously compromised facsimile. DoS attacks against the XML grammar are straight forward if the XML schema is compromised. In addition, 'the door is opened' to manipulate content if data types are compromised.
d. Password Hacking: Password attacks are a common way to attempt to gain access to the system. This is one of the request authentication attacks, in which during requesting the service from the client side, the attacker masquerades as a legitimate identity through theft of a shared secret, username/password pair, Public Key Infrastructure (PKI) certificate, or other identity information.
   By repeatedly trying very common username and password combinations there is always a possibility to get access to the critical information stored in the enterprise system. This is commonly known as dictionary password attack.
e. Session theft (Impersonation of sender/receiver): Someone listening to an unencrypted conversion could hijack a session and send in new messages. In this way, session can be theft by the hackers by getting someone's session id and may perform illegitimate operations on the system and as well as can hijack business critical credentials.
f. Unauthorized access: Yet another type of attack is made by someone with valid, authenticated credentials who somehow gains access to systems that they shouldn't have access to, by subverting the access control scheme.
g. Repudiation of message (request/response): In any form of communication a communication partner can deny having received a message (repudiation of receipt of response from the system) or it can also deny having sent a message (repudiation of sending a request to the system).

Internal Threats:

a. Abuse of administrative right: There are sets of people who will be responsible for administration of WISSDOM. If in any case, they abuse their access rights and perform some sensitive operation then that may cause loss of business in terms of financial social value and loss of customers' confidence.

b. Abuse of user rights: Besides the administrative people, a group of users are defined and assigned rights to perform some less sensitive or non-sensitive operations. If these people misuse their right and divulge some information to third parties, then that may open a backdoor of the system for the hackers.
c. Manipulation of management parameters: Management systems can also be used for an attack on a computer system by deliberately causing incorrect configuration. The incorrect configuration can be caused in various ways. In the process, it is possible to manipulate both the management platform and the equipment it controls. This may just lead to inconsistencies in the network management system, but could even be deliberately used to cause gaps in the security.
d. Unauthorized use and manipulation of crypto module [1]: If a third person succeeds in using a crypto module without authorization, this can lead to various types of damage such as a perpetrator may manage to read secret keys, alter the keys or even manipulate vital security parameters.
e. Unauthorized copying of data: When data media are replaced or moved, this can mean that the information to be transferred is transported from a secure environment via insecure channels to a possibly insecure environment at the receiving end. In such cases, unauthorized persons could copy this information more easily than in the original environment.

Communicational Threat:

a. IP Spoofing/Web Spoofing: IP spoofing is a method of infiltration in which incorrect IP numbers are used to act out a false identity to the IP system being attacked. It occurs when a malicious attacker behaves as the service itself, fooling a client into making requests to it directly. By doing this, important client credentials reach to the potential attacker. This type of attack violates integrity and confidentiality of the client credentials.
b. Man in the middle attack: Some non-trusted third person may be listening to a communication between the service provider and the service consumer. During this period this person may indulge in some malicious activities like going through the message (if not encrypted), modifying the message or enrooting the message to some other location (Routing Detour). In this way the confidentiality and integrity of the message for communication will definitely be violated.
c. Routing Detours [5]: The Web Services-Addressing specification provides a way to direct SOAP traffic through a series of intermediaries by using XML tags that assign routing instruction. If an attacker overtakes one of these intermediaries, they may insert bogus routing instruction to point a confidential document to an unauthorized location where critical information can be stolen. This technique may also be used to execute a DoS attack by routing the document to a non-existent destination. By characteristics it is a kind of Man in the Middle attack.
d. Malicious Morphing [5]: Malicious morphing is another form of Man in the Middle attack. Data or security information can be modified by an attacker during transmission of SOAP messages resulting in data integrity and operational problem.

3.2. Identification of different security tools and their features

a. Router: It provides some security support like On-board encryption, Support of VPN tunnels, Antivirus defense support through Network Admission Control (NAC), Intrusion Prevention, etc. So using this tool we can eliminate the threat like Routing Detours, IP Spoofing/Web Spoofing.
b. Firewall: By considering different features of the firewall it can block the threats like Computer Viruses and Worms, Cross-Site Scripting (XSS), SOAP attachments, IP Spoofing/Web Spoofing.
c. Layer3 (L3) Switch: It can provide dynamic IP lockdown, source port filtering, secure shell, etc. It can prevent the threats like Man in the middle attack, Malicious Morphing, IP Spoofing/Web Spoofing.
d. Layer2 (L2) Switch: It provides some security features like Dynamic Host Configuration Protocol (DHCP) snooping, dynamic Address Resolution Protocol (ARP) inspection, port security, etc. The threat like Abuse of user rights can be prevent by this tool.
e. Intrusion Detection System (IDS): It can detect the threats like Denial of Service (DoS), Coercive parsing, Session theft (Impersonation of sender/receiver).
f. Virtual Private Network (VPN): It can provides Internet Protocol Security, Transport Layer Security (Secure Sockets Layer (SSL)/Transport Layer Security (TLS)), Secure Socket Tunneling Protocol, Layer2 Tunneling Protocol, Multi Path Virtual Private Network, etc. Men in the middle attack, Malicious Morphing, IP Spoofing/Web Spoofing are the threats that can be avoid by this tool.
g. Encryption: By using this tool we can prevent the threats like Mistake or alteration of encrypted data, Failure of crypto module or insecure crypto-algorithm, Loss of data confidentiality, Man in the middle attack, Malicious Morphing.
h. Backup Software: Backup software is a computer program used to perform a complete backup of a file, data, database, system or server. This tool prevent the threats like Buffer overflow, Failure of a database, Loss of stored data, Loss of database integrity/consistency.
i. Digital Signature: This technique is being used for the purpose of authentication to sending a data from one host to another. It can detect the threats like WSDL Enumeration, Password Hacking, Unauthorized access, Repudiation of message (request/response), Unauthorized use and manipulation of crypto module, Unauthorized copying of data.
j. Hardware Tokens: It can avoid the threats like Manipulation of management parameters, Unauthorized access, Abuse of administrative right, Abuse of user rights, SQL injection, Parameter tampering, Schema Poisoning.
k. Anti Virus: This tool can prevent the threat like Computer Viruses and Worms.
l. Biometrics: It can detect the threats like Manipulation of management parameters, Unauthorized access, Abuse of administrative right, Abuse of user rights, SQL injection, Parameter tampering, Schema Poisoning.
m. Smart Card: It can detect the threats like Manipulation of management parameters, Unauthorized access, Abuse of administrative right, Abuse of user rights, SQL injection, Parameter tampering, Schema Poisoning.

3.3. Concepts of Location Based Advisory

Location Based advisory tells an individual/organization the exact location of security tools, to be placed to mitigate the security risks of the organization.

Using the knowledge of the tools, this phase will specify the locations and a number of alternatives will be generated using the risk value.

This advisory consists of a set of sequential activities.

- The input data is collected from the mapping between different threats and their corresponding countermeasure called security tools.
- This data is compared with the knowledge bases i.e. different features and compatibility of security tools.
- Finally a report is generated at where the tools and there location would be specify, which will be presented to the organization.
- The organization will select some tools from this advisory for installation so as to secure its assets.
- The selected tools will also be used as input to the testing phase.

Developing Location Based Advisory: We categories the above mention tools into two ways. Such tools which are placed at the top of the network architecture are called special category tools and others are called general category tools. The network architecture is the collection of some domain. Each domain contain may be same or different devices within the same environment. The tools like Router, H/W Firewall, L3 switch, H/W IDS, L2 Switch are considered as a special category tools and others tools are consider as General Category tools

3.4. Guideline to Place those Tools

To find out the exact location for the above tools the following step should be take care of.

Router: To avoid threats and vulnerabilities of different assets if router required with its corresponding features then at first organization will check whether this features can be upgrade into its existing router or not? If up gradation is possible then organization will upgrade the existing router with this required features otherwise organization will buy a new router with its required features and placed it at the gateway between public network and private network.

Hardware Firewall: If router is available in a network then checked H/W Firewall already exists or not.

If firewall does not exist then connect a minimal features firewall with router by comparing the other H/W firewall.

If firewall with less featured already exists and other advanced feature firewall is suggested then at first Check how much domain required this upgraded features firewall.

If number of domain is one then Connect this upgrade firewall with existing firewall by using L2 switch, Connect that domain(x) with this upgrade firewall and Check the inter domain connectivity of the above domain. Find out directly connected domain with the above domain(x) and connect them with L2 switch that is placed between existing firewall and required firewall because these domains are not required this upgrade features Firewall

If no. of domain is more than one then Connect those domains with this upgrade firewall by using L2 switch, Connect this upgrade firewall with existing firewall by using L2 switch, Check the inter domain connectivity of the above domain. Find out directly connected domain with the above domain which is not required such type of upgrade firewall and connect them with L2 switch that is placed between existing firewall and required firewall.

If upgraded features firewall is not required then Exit.

Hardware IDS: If upgraded features required in existing H/W IDS and if it is possible to upgrade then upgrade this existing H/W IDS with required features otherwise check for L3 Switch availability . If L3 switch is available then connect this H/W IDS with this L3 Switch otherwise check for H/W Firewall's availability, If H/W Firewall is available then Connect this H/W IDS with this H/W Firewall otherwise connect with Router

L3 Switch: If upgraded features required in existing L3 Switch and if it is possible to upgrade then upgrade existing L3 Switch otherwise check for H/W IDS's availability, If H/W IDS is available then connect L3 switch with H/W IDS otherwise check for H/W Firewall's availability. If H/W firewall is available then connect L3 switch with this H/W firewall otherwise connect with Router.

L2 Switch: Location of L2 switch will depend upon the availability of L2 switch, L3 switch, H/W IDS, H/W Firewall and Router. Due to their availability, last four out of five tools will be connect as per above mention logic and with respect to their connectivity L2 switch will be connect from bottom to top approach.

General category tools will be placed as per their requirement. For a particular asset if more than one tools are being suggest to eliminate same threat then organization will be decide any one.

Sequence Diagram for Special Category Tools are shown in Figure 1a and 1b. Sequence Diagram for General Category Tools are shown in Figure 2.

4. Conclusion and future scope

This project is a small attempt to propose certain tools and techniques to secure the resources of a web-based enterprise. The security needs of an enterprise are an ever-changing phenomenon. To keep pace with this rapid change manually is a tedious task. Most organizations cannot cope up with this pace, thus resulting in a lot of security loopholes in the systems of the organization. This project attempts to ease this task by developing an automated tool that generates the security specification of an organization given the security requirements and the security policy.

The system is firstly to develop a knowledge base as what are the available tools, what they do and how to locate the available tools to secure an organization and then develop a tool, which will automate the process of advisory generation, which will comply with ISO 17799 standard and will reduce the work of organization greatly.

The user of this tool should have knowledge about networks and about the security tools.

Use of this tool will make the securing process of any organization simpler than ever before. Those organizations, which use computers for their business operations are suitable users for this tool.

After getting the security infrastructure specification, a cost-benefit and detailed risk analysis is performed by the management of the organization concerned. Based on this, the organization decides on the particular infrastructure that it would like to implement. This is stated in the form of a security infrastructure selection. This selection will take into account all kinds of policies of the organization. Finally, the organization implements the security infrastructure as decided by it.

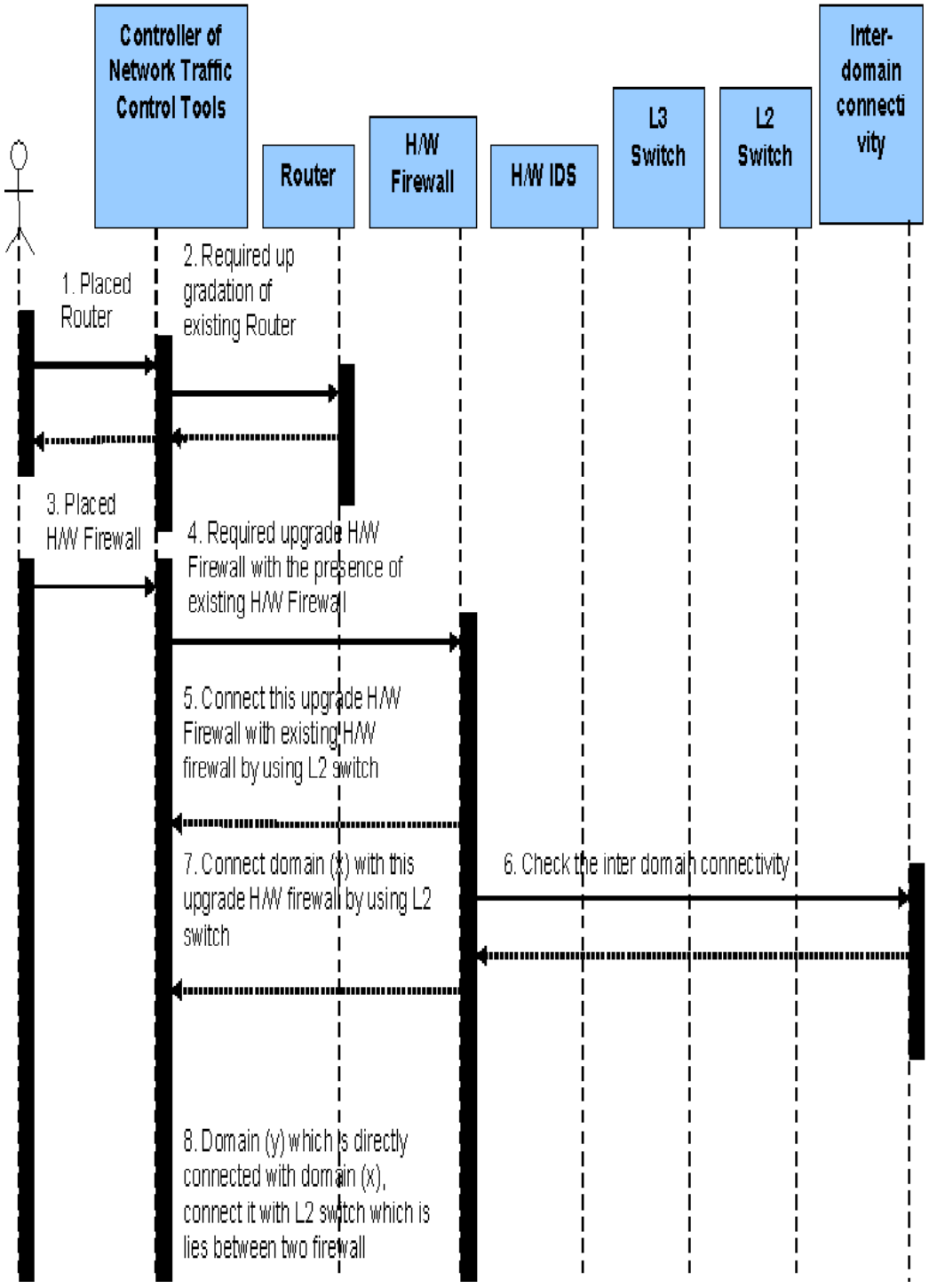

Figure 1a. Sequence Diagram for Special Category Tools.

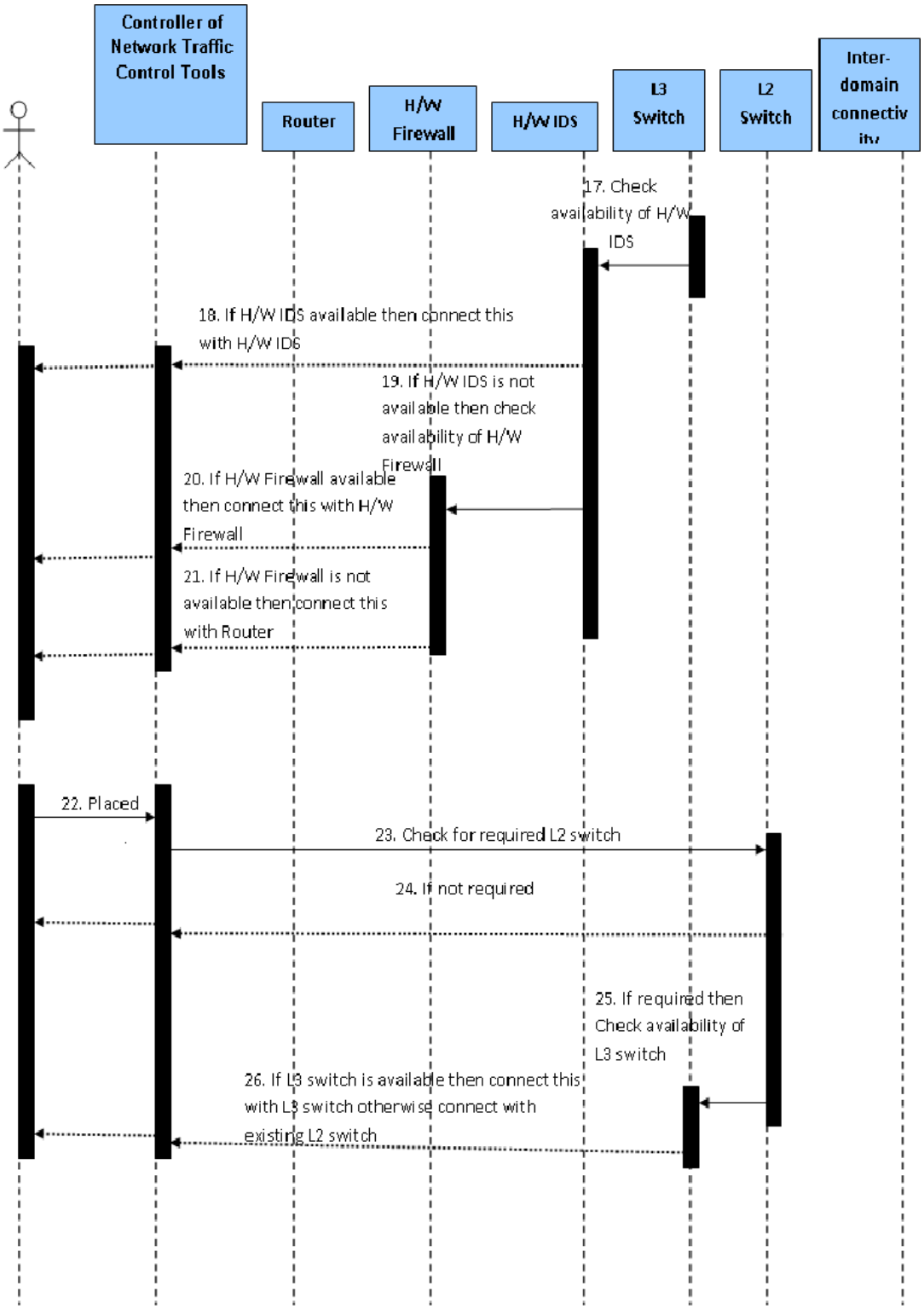
Controller of Network Traffic Control Tools
Router
H/W Firewall
H/W IDS
L3 Switch
L2 Switch
Inter-domain connectiv ity
17. Check availability of H/W IDS
18. If H/W IDS available then connect this with H/W IDS
19. If H/W IDS is not available then check availability of H/W Firewall
20. If H/W Firewall available then connect this with H/W Firewall
21. If H/W Firewall is not available then connect this with Router
22. Placed
23. Check for required L2 switch
24. If not required
25. If required then Check availability of L3 switch
26. If L3 switch is available then connect this with L3 switch otherwise connect with existing L2 switch

Figure 1b.

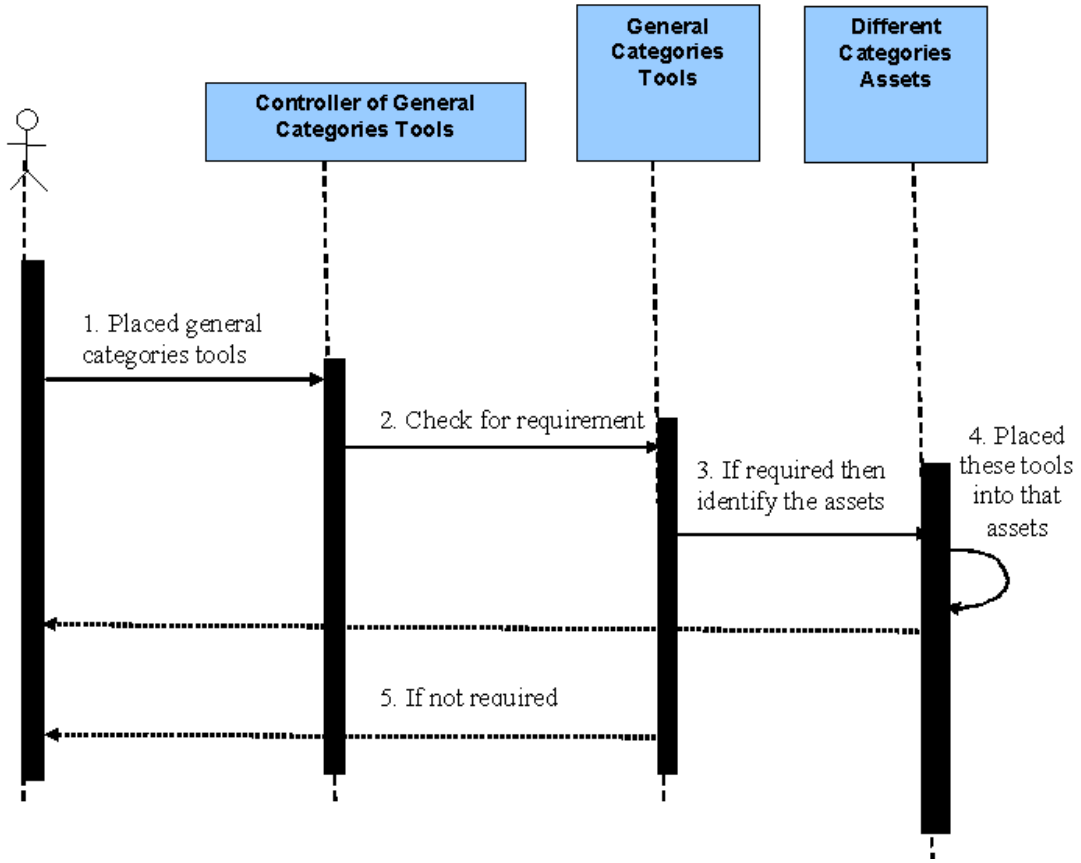

Figure 2. Sequence Diagram for General Category Tools.

There is scope for further enhancement of this work. First and foremost, need to consider load balancing factor of different tools to install at different location. Secondly, need to optimum the general category tools into their proper position.

References

[1] IT baseline Protection Manual – BSI. http://www.bsi.bund.de/fehler/index.htm

[2] Improving Web Application Security – threats and countermeasures. Practices and Patterns – Microsoft Corporation. http://www.cgisecurity.com/lib/Threats_Countermeasures.pdf

[3] Sarath Indrakanti and Vijay Vardharajan, "An Authorization Architecture of Web Services", INSS Research Group, Dept. of Computing, Macquarie University, NSW 2109, Australia.

[4] M Hondo, N Nagaratnam, and A Nadalin, "Securing Web Services", IBM research Lab.
http://www.research.ibm.com/journal/sj/412/hondo.html

[5] The Web Services Security Threats – the risk, the threats and what you can do about it.
http://www.actional.com/products/docs/white_paper_web_service_security_threat.pdf

[6] Web Service Security - Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0. Microsoft Corporation.
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpag2/html/wssp.asp

[7] Professional Web Services Security – Ben Galbraith, Whitney Hankison, Andre Hiotis, Murali Janakiraman, Prasad D.V. Ravi Trivedi, David Whitney. From WROX Publication.

[8] Web Server Security Guidelines. Indian Computer Emergency Response Team. Dept. Information Technology. Govt. of India. Issue Date: August 17, 2004.

[9] Tips and Tricks: Web Services Attacks and Defenses. By John Lilly, CTO, Reactivity, Inc.

[10] Anatomy of a web services Attack – A guide to threats and preventive countermeasures, ForumSystems. http://www.forumsystems.com

[11] Enterprise Information System Security, February 2005, Center for Distributed Computing, Jadavpur University, Kolkata.

Authors

Uttam Kumar Dash, M.Tech, Kolkata. He is working as a Lecturer with the Information Technology Department at Heritage Institute of Technology, Kolkata. He has 3 years of experience in Teaching. His research interest is Security Engineering. He has published 1 Research Paper in International Journal.

Debnath Bhattacharyya, M.Tech in Computer Science and Engineering from West Bengal University of Technology, Kolkata and currently Professor of Hannam University, Korea. He has 15 years of experience in Teaching and Administration. His research interests include Bio-Informatics, Image Processing and Pattern Recognition. He has published 66 Research Papers in International Journals and Conferences and 6 Text Books for Computer Science.

Prof. Tai-hoon Kim, M.S., Ph. D (Electricity, Electronics and Computer Engineering), currently, Professor of Hannam University, Korea. His research interests include Multimedia security, security for IT Products, systems, development processes, operational environments, etc. He has 14 Years of experience in Teaching & Research. He has already got distinctive Academic Records in international levels. He has published more than 100 Research papers in International & National Journals and Conferences.