

**INFORMATION SECURITY MANAGEMENT  
IN WEB-BASED PRODUCT DESIGN & REALIZATION**

By

Pamela Nnenna Ajoku

B. Eng. in Computer Engineering, Enugu State University, Nigeria 1997

Submitted to the Graduate Faculty of  
the School of Engineering in partial fulfillment  
of the requirements for the degree of  
Master of Science

University of Pittsburgh

2002

UNIVERSITY OF PITTSBURGH  
SCHOOL OF ENGINEERING

This thesis was presented

By

Pamela Nnenna Ajoku

It was defended on

April 12, 2002

and approved by

Bartholomew O. Nnaji, Professor, Industrial Engineering

Raymond Hoare, Assistant Professor, Computer Engineering

Ming-En Wang, Assistant Professor, Industrial Engineering

Thesis Advisor: Bartholomew O. Nnaji, Professor, Industrial Engineering

## **ACKNOWLEDGEMENTS**

First and foremost, I thank my academic advisor, Prof. Bartholomew O. Nnaji, who has been a source of inspiration to me. His numerous suggestions, comments, and advice have made this entire thesis possible. My deep gratitude goes to the entire faculty and staff of the Department of Industrial Engineering at the University of Pittsburgh.

I thank my thesis committee members who, by giving their valuable time, aided the completion of this work. My sincere gratitude goes to Dr Raymond Hoare, who guided me through necessary systematic procedures and ensured the originality of this research. I also thank Dr Ming-En Wang whose invaluable feedback and advice also contributed to the successful completion of this thesis.

I appreciate efforts of the numerous people who have contributed in one way or the other to numerous journals, articles and books from which useful pools of information were drawn and integrated into ideas and concepts. My heartfelt thanks go to all the members of the Automation and Robotics Laboratory. They graciously provided expert opinions and responses, which embody the very essence of this thesis.

Finally, I extend my sincere thanks and gratitude to my wonderful family and friends, who have encouraged me to be the best I can be in all things and work hard for my liberty. Special thanks to my best friend, Buchi, for helping me fulfill my dreams and goals. Indeed, hard work has its rewards.

## **ABSTRACT**

# **INFORMATION SECURITY MANAGEMENT IN WEB-BASED PRODUCT DESIGN & REALIZATION**

Pamela N. Ajoku, M.Sc.

UNIVERSITY OF PITTSBURGH, 2002

There is an increasing interest in research and development in the area of information security. Areas of computer misuse include the theft of computational resources, disruption of computational services, unauthorized disclosure of computer information and unauthorized modification of computer information. In the recent past decades, there have been myriads of computer security implementations. Nevertheless, there have also been numerous computer break-ins and security breaches.

This is a thesis on *Information Security Management in Web-Based Product Design and Realization*, which is a sub-cluster of a broader currently on-going research project called *Pegasus*, at the Automation and Robotics Laboratory, University of Pittsburgh. Pegasus is a proposed scalable, flexible, and efficient collaborative web-based (or Internet-oriented) product design system, which will involve continuous transfer of sensitive information across seamless and possibly, international boundaries. The thesis commences with a statement of the problem of information security and presents a comprehensive summary of previous and current related research along with applicable results and application areas.

With the dawn of the 21st century upon us and use of the Internet growing exponentially, secrecy in the realm of technology has become an important issue. A managerial approach for alleviating the problem of information security or reducing it to the barest minimum is proposed in this thesis through the design and development of an *Information Security Management Model (ISM Model)* to monitor, enforce and manage information security. The design of the ISM Model incorporates a methodology for referencing activities in *Pegasus* with information security technologies.

## **DESCRIPTORS**

Access Control

Authentication

Confidentiality

Cryptography

Distributed Systems

Information Security

Information Management

Product Design

# TABLE OF CONTENTS

	Page
ACKNOWLEDGEMENTS .....	iv
ABSTRACT .....	v
LIST OF FIGURES .....	ix
1.0 INTRODUCTION.....	1
1.1 Distributed Networks, Product Design & Information .....	1
1.2 What is Security? .....	3
1.3 Computer Security in Distributed Networks.....	3
1.4 Research Background: <i>The Pegasus Project</i> .....	4
1.5 Statement of the Problem .....	7
1.6 Significance of the Problem .....	8
1.7 Research Focus, Objectives and Challenges .....	10
1.8 Approach to the Problem.....	12
1.9 Research Organization .....	13
2.0 LITERATURE REVIEW .....	14
2.1 Review of Current Information Threats and Security Issues .....	16
2.1.1 Threats.....	16
2.1.2 Computer Information Security .....	20

2.1.3	Hackers .....	21
2.1.4	Search Engines .....	24
2.1.5	Viruses, Trojan Horses & Worms .....	25
2.1.6	Confidentiality, Integrity & Availability.....	28
2.2	Review of Information Security Methodologies. ....	29
2.2.1	Firewalls.....	30
2.2.2	Cryptographic Security .....	31
2.2.3	Digital Signatures.....	32
2.2.4	Intrusion Detection Systems .....	35
2.2.5	Virtual Private Networks .....	38
2.3	The Quest for Information Security .....	39
2.4	Information Security Management .....	40
3.0	THEORY OF COMPUTER INFORMATION SECURITY .....	44
3.1	Principles for Information Security Management .....	44
3.2	Important Fundamental Concepts.....	46
3.3	The Information Security Policy .....	49
3.4	The Functionality of Internal Security Mechanisms.....	51
3.5	The Information Infrastructure.....	51
3.6	The OSI Seven-layer Model.....	54
3.7	Security in CORBA .... ..	55
3.8	The File Transfer Protocol .....	57
3.9	Public Key Infrastructure .....	58



3.10 The Secure Sockets Layer Protocol .....	59
3.11 IP Security Protocol .....	61
3.12 Building on Solid Foundations .....	63
 4.0 METHODOLOGY .....	 65
4.1 Methodology Approach .....	65
4.2 Required Features of the Security Layout .....	66
4.3 The proposed Information Security Management Model .....	67
4.3.1 The Information Security Policy .....	70
4.3.2 The Security Matrix .....	75
4.3.3 The XML Knowledge Base .....	77
4.3.4 Third Party Software Interface .....	78
4.3.5 The ISM Model Security Services .....	80
4.3.6 The Alarm/Alert Mechanism .....	87
4.3.7 The Communication Protocols .....	90
4.3.8 The Pragmatic, Ethical & Technical Principles' Hive .....	91
4.3.9 The User Manager .....	92
 5.0 MODEL ANALYSIS, VALIDATION AND APPLICATIONS.....	 94
5.1 General Feasibility of the ISM Model .....	94
5.2 Qualitative Risk Analysis .....	95
5.3 Limitations of the Model .....	97

5.4 Validation of the ISM Model .....	98
5.5 Benefits and Applications of the ISM Model .....	98
 6.0 CONCLUSION AND FUTURE WORK .....	 100
6.1 Conclusion .....	100
6.2 Future Research Extensions .....	102
 APPENDIX	
Appendix A .....	103
Appendix B .....	107
Appendix C .....	111
 BIBLIOGRAPHY .....	 120

## LIST OF FIGURES

Figure No.	Page
Figure 1 The Pegasus Project .....	6
Figure 2-1 Threats .....	17
Figure 2-2 A Search Routine using Google Search Engine .....	22
Figure 2-3 A Search Routine using Altavista Search Engine .....	23
Figure 2-4 Anonymous Proxies.....	24
Figure 2-5 Program infected with a virus .....	25
Figure 2-6 Building Blocks .....	41
Figure 3-1 Types of Information .....	52
Figure 3-2 Cluster of Servers .....	53
Figure 3-3 OSI Systems Management Overview .....	54
Figure 3-4 Main components of the ORB architecture and their Interconnections .....	55
Figure 4-1 General Overview of the Information Security Management Model .....	68
Figure 4-2 Detailed Overview of the ISM Model .....	69
Figure 4-3 A Security Matrix .....	76
Figure 4-4 A Simple Authentication Framework .....	81
Figure 4-5 A Symmetric Cryptosystem .....	83
Figure 4-6 A Public Key Cryptosystem: Encryption Mode.....	83
Figure 4-7 A Public Key Cryptosystem: Authentication Mode.....	84
Figure 4-8 Power Key Encryption and Decryption.....	84
Figure 4-9 Security Levels .....	89
Figure 4-10 General Overview of Security Levels .....	90

Figure 4-11 Hive Overview.....	91
Figure 4-12 User Permissions .....	92
Figure 4-13 User Permissions for Design Activities .....	93
Figure 4-14 User Permissions for Financial Activities .....	93

## ACRONYMS

AH	-	Authentication Header
CA	-	Certificate Authority
CAD	-	Computer-Aided Design
CAM	-	Computer-Aided Manufacture
CERT	-	Computer Emergency Response Team
CORBA	-	Common Object Request Broker Architecture
DARPA	-	Defense Advanced Research Projects Agency
DCE	-	Distributed Computing Environment
DES	-	Data Encryption Standard
DHCP	-	Dynamic Host Configuration Protocol
DNS	-	Domain Name service
DoS	-	Denial of Service
DSA	-	Digital Signature Algorithm
DSS	-	Digital Signature Standard
ESP	-	Encapsulating Security Payload
FTP	-	File Transfer Protocol
IDS	-	Intrusion Detection System
IIS	-	Internet Information Server
IKE	-	Internet Key Exchange
IP	-	Internet Protocol
IPComp	-	IP Payload Compression
IPSec	-	Internet Security Protocol
LAN	-	Local Area Network
NIST	-	National Institute of Standards and Technology
OA	-	Object Adapter
OMG	-	Object Management Group
ORB	-	Object Request broker
PKI	-	Public Key Infrastructure
RFC	-	Requests For Comments

RFI	-	Requests For Information
RFP	-	Requests For Proposals
SHA	-	Secure Hashing Algorithm
SL	-	Security Level
SLV	-	Security Level Value
SNMP	-	Simple Network Management Protocol
SSL	-	Secure Socket Layer
TCP	-	Transmission Control Protocol
URL	-	Uniform Resource Locator
VPN	-	Virtual Private Network
WAN	-	Wide Area Network

## **1.0 INTRODUCTION**

The aim of this preliminary research is to develop a framework for managing information security in web-based product design and realization. Web-based product designs take place in distributed networks and this chapter begins with clear-cut definitions of these key concepts. It also provides basic information regarding the background of the research, statement and significance of the problem and the proposed methodology.

### **1.1 Distributed Networks, Product Design & Information**

A Distributed Network is a system of two or more computers, terminals and communication devices linked by wires, cables or a telecommunications system in order to exchange information. Groups of such distributed networks are able to function separately and operate independently of similar networks. The network may be limited to a group of users in a local area (Local Area Network - LAN), or be global in scope e.g. the Internet.

Why build distributed systems? According to Mullender, people are distributed and as a result information is also distributed<sup>[1]\*</sup>. Distributed systems often evolve from networks of workstations. The owners of the workstations connect their systems together because

---

\* Parenthetical references placed superior to the line of text refer to the bibliography.

of the desire to communicate and share information and resources. Also, information generated in one place is often needed in another. Information and communication technologies have improved the way business is done and companies are becoming increasingly location independent. Other reasons for distributed systems include, but are not limited to the following:

- Performance/Cost - Distributed systems are economic or profitable
- Modularity - In contrast with centralized systems
- Expandability - Capable of incremental growth
- Availability - Data replication, built-in redundancy

Product design is a vital part of the entire product development process. It involves the recognition and imposition of constraints, preferences, ergonomic issues and economies of manufacture. Constraints in product design arise from business, technical, aesthetic issues etc. Thus, adequate product design improves performance, resolves conflicts and reduces the overall cost of manufacturing the product.

Information is the lifeblood of any business and any corruption or loss of such information could mean loss of significant profits and valuable business. So, information must be protected for business intelligence. In product design, information may flow from the customer to the designer or manufacturer and vice versa. The designers, engineers and/or manufacturers use such information in an organized, timely manner to design, develop and produce the product. In major businesses, which employ the use of



distributed networks, such information may move across many insecure boundaries. Hence, there is the need to ensure information security.

## **1.2 What is Security?**

According to Webster's New World College Dictionary, *security* is the state of being or feeling secure <sup>[2]</sup>. It is freedom from fear, anxiety, danger, doubt etc. From a technological point of view, security implies a condition of protection pertaining to information or infrastructure. It is protection or defense against attack or interference.

## **1.3 Computer Security in Distributed Networks**

Computer Security is a vast field and distributed network security can range from physical threats such as theft and fire, to infrastructure security where authorization, authentication etc., come into play. There are alternative formal definitions of computer security, but a practical definition is given below:

*Computer Security is a means of preventing intruders, attackers or other unauthorized persons, from achieving illegal objectives through unauthorized use or unauthorized access of computers, peripherals and networks.*

In this documentation, computer information security will concentrate on the following three categories:

- Confidentiality
- Integrity
- Availability

These categories arise as a result of three major disruptions that could occur on a computer system. These are:

- i) Information and/or services can become available to unauthorized use or access
- ii) Information and/or services can be deleted, altered, destroyed or corrupted
- iii) Information and/or services can become unnecessarily unavailable

#### **1.4 Research Background: The *Pegasus* Project**

Customers have changed the way discrete product manufacturers operate. There is a gradual deviation from the traditional *make-to-stock* production model to a *build-to-demand* model. Many customers are no longer satisfied with mass-produced goods. They are demanding customization and rapid delivery of innovative products. The current method of designing a *mechanically engineered* product is for a designer with knowledge

of design rules, product specifications and manufacturing preferences to evolve a design. However, today's Computer Aided Design (CAD) systems do not allow direct imposition of multi-disciplinary preferences regarding functionality, manufacturability, assemblability, safety, reliability, ergonomics, material, and other issues against which such products should naturally be tested.

Also, while *view* and *edit* functions on a product can be accomplished at remote locations in some advanced CAD systems, there is no platform which allows a customer at a remote location to participate in the design of the product through the imposition of design preferences.

This is particularly hindered by the fact that there is no mechanism for creating form from preference specifications. From an immediate point of view, it may seem unnecessary to investigate security issues all over again. This may arise from the fact that the word '*security*' has been a buzzword since the advent of information technology. However, this thesis is based upon the research done within the *Pegasus* Project. A general overview of the project is shown in Figure 1.

The goal of this project is to research and develop a scalable, flexible, and efficient collaborative *web-based* product design & realization platform. This platform will allow customers, designers and manufacturers work on a product concurrently, and to provide the customer, in virtual space, the capability to specify preferences, which will then

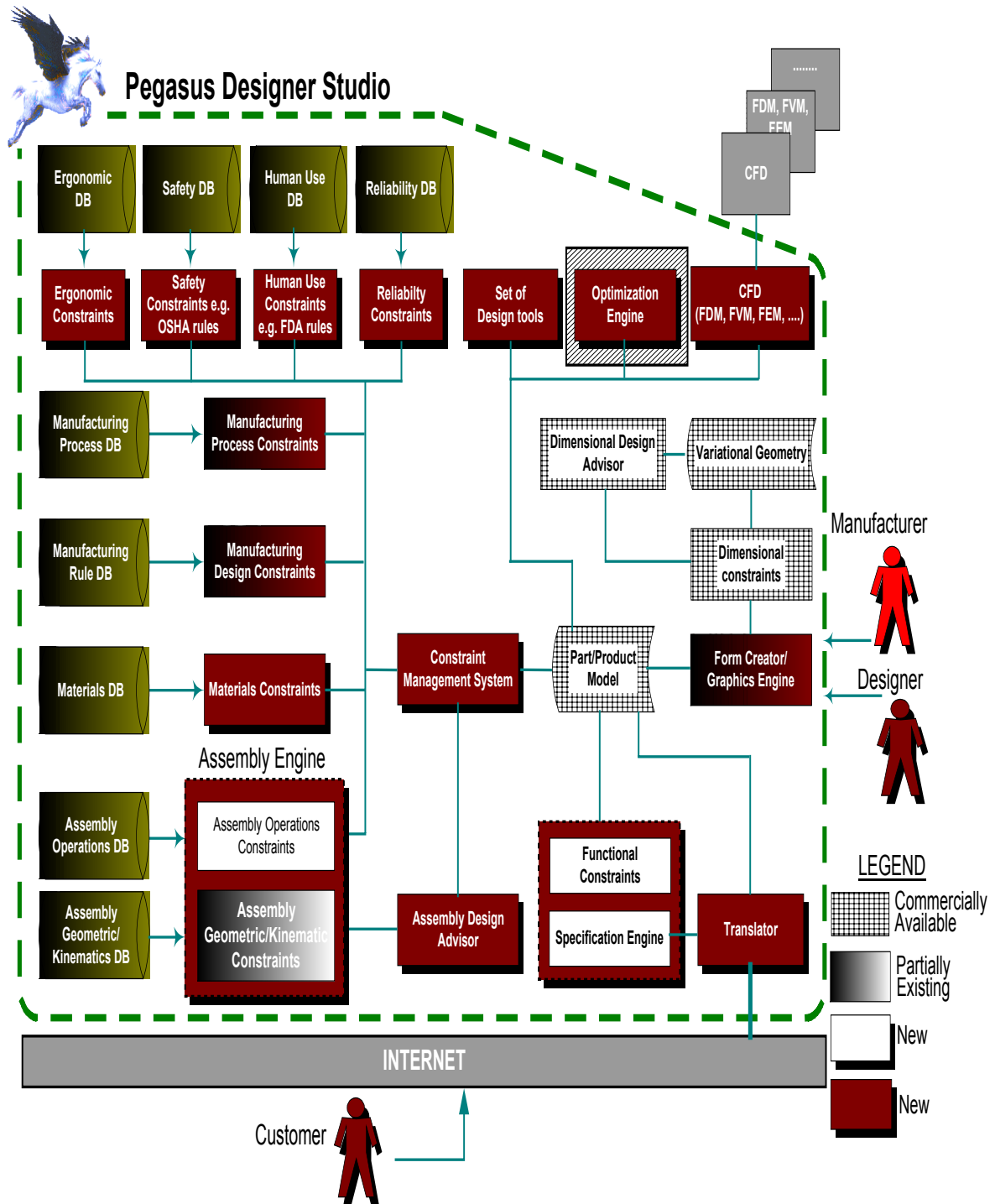


Figure 1 The *Pegasus* Project  
 Copyright: Prof. B. O. Nnaji, Director, The Automation and Robotics Laboratory,  
 University of Pittsburgh

impose domain specification constraints on the product and the product's components. It will allow for multi-disciplinary product design evolution. The entire design process contains proprietary information and examples of product representations (graphics, CAD) are included in Appendix A.

### **1.5 Statement of the Problem**

Distributed computing infrastructure developed with the advent of the Internet. Secure data transmission largely depends on the security of network controls and management protocols. However, the Internet, a viable means of communicating, has brought along its own share of woes. At the top of the list is security <sup>[3]</sup>. Technologically advanced intruders and hackers have become very rich overnight by taking advantage of the ubiquity of the Internet.

As useful as it may be, the Internet was not designed for privacy. In 1973, the U.S. Defense Advanced Research Projects Agency (DARPA) initiated a research program to investigate techniques and technologies for interlinking packet networks of various kinds.

The objective was to develop communication protocols, which would allow networked computers to communicate transparently across multiple, linked packet networks.

Today, there is no centralized security mechanism, which can address security issues across the Internet. There is a need to specifically address the security issues directly affecting the information infrastructure of an electronic product design system.

Dhillon states that, in recent years organizations have fallen short of developing adequate policies to deal with information security problems <sup>[4]</sup>. This is evidenced not only by increases in incidents of system penetration (such as hacking), but also in inability of authorities to establish adequate basis to deal with such computer crimes.

The proposed *Pegasus Designer Studio* requires a platform, which will enable secure information exchange and storage. The virtual and distributed nature of the systems further complicates the security issues. Two or more parties may wish to share proprietary information and such information may need to move across seamless boundaries.

## **1.6 Significance of the Problem**

A survey of computer crime conducted in 1999, to which 521 firms responded reported losses of up to \$124,000,000 <sup>[5]</sup>. Two-thirds of the loss was accounted for by theft of proprietary information and financial fraud. Viruses constitute another hazard, and are a measure of the malevolence of the community of Internet users. In 1989, 250 viruses had

been identified, but the number has been growing exponentially and through the third quarter of 1999, 44,600 viruses were known to exist <sup>[5]</sup>.

The Social Security Administration (SSA) reports that cases of misuse of social security numbers have increased from 7868 in 1997 to 30,115 in 1999. Also, during the last decade reports of network-based attacks and exploitation of bugs and design limitations have grown dramatically <sup>[6]</sup>.

At the time of this research and according to the Wall Street Journal, businesses and consumers spent \$4 billion in 1999 on security products to ward off intruders and the market is expected to grow by \$11 billion by the year 2004 <sup>[7]</sup>. In summary, some of the main reasons for protecting information include the following:

- Theft of proprietary information (such as business secrets, credit card numbers)
- Financial fraud; unauthorized use and access
- Viruses and other damaging self-replicating codes
- Denial of Service (DoS) attacks, service unavailability or untimely system shut-down
- Identity theft (access to personal information)
- Information corruption and invalidation
- Others

This information reinforces the need for improved methods for protecting information in order to limit the rapid growth of Internet crime.

### **1.7 Research Focus, Objectives and Challenges**

This research focuses on the management of information security issues during web-based design of products using distributed systems, infrastructure and software from the onset of the concept of the product to its realization. The design environment should be scalable, flexible, efficiently collaborative and secure. It should allow for the efficient interaction of customers, designers, manufacturers and supply chain personnel during the design and manufacture of a product. The customer, in virtual space, should be able to specify preferences, which impose domain specification constraints on the product and the product's components. The main objectives of this research are as follows:

- i) Investigate information security with respect to the impact of the Internet on corporate, distributed, enterprise-wide e-Business networks.
- ii) Identify the critical security issues concerning electronic information retrieval, transfer and storage.
- iii) Design the *Information Security Management (ISM) Model* and develop the preliminary framework for information management in electronic- (web-based) product design and realization.



- iv) Directly address the basic information security research issues, which would help to develop products efficiently with better quality, lower costs and faster time to deliver or market.

The challenges of this research include:

- i) Analyzing an issue (security), which is still an undying information technology buzzword in the new millennium.
- ii) Proposing a different approach to the problem of information security and establishing an adequate model for managing information security beyond the existence of complex individual technologies.
- iii) Establishing proper management policies and practices in geographically dispersed environments but maintaining the ability to control local organizational processes.
- iv) Reviewing the extensive research done in the area of information security and building upon standard foundations that have been laid.
- v) Perhaps the most challenging factor is the overwhelming concern business executives, investors, manufacturers and the general public have regarding information security as a whole.

## 1.8 Approach to the Problem

Dhillon states that solutions to the problem of managing information security in the new millennium hark back at shifting emphasis from technology to business and social processes <sup>[4]</sup>. However, the business and social processes must operate within a logical framework in order to succeed. This thesis establishes an integrated and robust management framework for information security within a scalable distributed platform for electronic product design. The main resources to be protected are:

- a) The processes
- b) The files (the data/information)
- c) The data in transit

A process is basically a program in execution which consists of the executable program, the program's data and stack, its program counter, stack pointer, registers and all other information needed to run the program.

A file, on the other hand is a collection of records or data designated by name or considered as a unit by the user. These are stored on memory or disks. Data in transit are packets of data being transmitted across a network.

## 1.9 Research Organization

In this documentation, Chapter 2 provides a literature review of relevant research areas and important aspects of this research. It investigates how these issues can be applied to *web-based product design and realization*. Chapter 3 explores the theory of computer information security. It analyses three concepts, which are the information security policy, the functionality of the internal security mechanisms and the assurance that these mechanisms adequately enforce the security policy.

Chapter 4 builds upon the concept of assurance and discusses the design and framework for the Information Security Management Model (ISM Model). Chapter 5 analyzes the ISM Model and discusses possible validation techniques, benefits and application of the model. Chapter 6 presents preliminary research conclusions and extensions for future research work.

## 2.0 LITERATURE REVIEW

The greatest asset of the Internet is its ubiquity and openness. Unfortunately, this is also its Achilles' heel. The flow of information and the use of the Internet as a medium for information transfer give rise to questions about security. According to Solms, Information Security can only be "managed" properly if an internationally accepted reference framework is used<sup>[8]</sup>.

Stark also states, quite bluntly, that networks connected to the Internet are at risk of intrusion. The most common methods of deliberate intrusion identified by the Computer Emergency Response Team (CERT) are *Internet Protocol (IP) spoofing* and *packet sniffing*. Part of the reason the Internet is riddled with security holes is the lack of any effective native security in the current version of IP, which binds the Internet's heterogeneous systems together<sup>[9]</sup>.

As businesses compete globally, using networks and other advanced means of communication, shorter product life cycles are desired. Networks have become indispensable for conducting businesses and transactions in industry, academic organizations and government. A networked system will provide quick access to product information and enhance design collaboration at a fraction of the *traditional* costs. Most organizations have adopted client-server architectures with the Internet providing opportunities for connecting to seamless boundaries at record speed.

However, trends highlighted in recent surveys conducted by the Computer Security Institute and Federal Bureau of Investigation (CSI/FBI) are disturbing<sup>[3]</sup>. Organizations are attacked from both inside and outside of their electronic perimeters. A wide range of cyber attacks have been detected and these can result in serious financial losses.

The CSI/FBI report also notes that defending against such attacks requires more than just the use of information security technologies. Clearly, more must be done in terms of adherence to sound practices, deployment of sophisticated technologies and adequate training of users of the system.

The annual Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) Computer Crime and Security Survey is conducted as a public service by the CSI. This effort aims to help raise the level of security awareness as well as to assist in determining the scope of computer crime in the United States. In its fifth year in 2000, the CSI/FBI collaboration showed in its study that ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches in that year, while 273 organizations reported \$265,589,940 (the average annual total from the year 1997 to the year 2000 was \$120,240,180) in financial losses<sup>[10]</sup>.

## 2.1 Review of Information Security Issues

### 2.1.1 Threats

*Threats*, *attacks* and *safeguards* are all terminologies used in connection with security. Within the context of this research, a *threat* is a person, thing, or event that poses danger to an asset's confidentiality, integrity, availability, or legitimate use. An *attack* is defined as the realization of a threat, and a *safeguard* is the protection against a threat. Thus, a complete understanding of threats provides the best route in dictating an approach to concept of information management.

Threats are categorized, in this research, as *Basic or Fundamental Threats*, *Enabling Threats* and *Underlying Threats*. Fundamental threats are major threats and these include:

- Threats against system penetration, confidentiality or *information leakage*.
- Threats of *integrity violation* where data is compromised through unauthorized deletion, creation, alteration, or destruction of the data.
- Threats of *illegitimate unavailability or denial of service* where authorized or legitimate users are denied the service of a resource.

- Threats of *illegitimate use* where resources and/or services are used without legitimate authorization. This threat worsens when security breaches occur from within the organization.

Hazards of hooking up to the Internet include legitimate users sending out proprietary information, legitimate users bringing in harmful information, packet sniffing, human error, lack of strong user identification, users running servers of which they are unaware, blind faith in firewall packages and bugs in commercial software <sup>[11]</sup>. Figure 2-1 depicts a typical threat scenario.

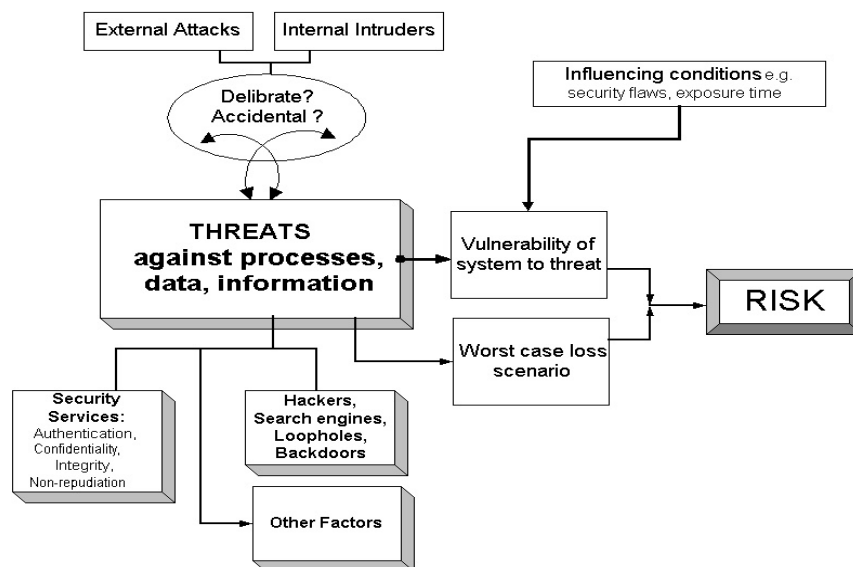


Figure 2-1 Threats

Fundamental threats acquire support from and are realized through the use of *enabling threats*. Enabling threats include:

- *Loop Holes and Back doors:* Most security technology comes with in-built flaws and loopholes are used to bypass security mechanisms thereby allowing unauthorized access to resources and services. Another source of “back doors” or “side-entrances” is the software designer/developer, who purposefully create hidden doorway, which they alone supposedly know about.
- *Masquerades:* This occurs when someone or something pretends to be someone or something else. For example, an individual trying to gain access to a resource or service by using a legitimate user’s identity to obtain privileges in the network. These are also known as "false appearances".
- *Insider threat:* This is worse than a false appearance or masquerade and occurs when an authorized user of the system misuses resources and/or service. This individual may decide to alter, leak, delete or suppress information.



- *Viruses and Trojan Horses:* A virus is malicious software and Trojan horses are a category of such malicious software <sup>[12]</sup>. A Trojan horse compromises security by destroying or stealing information, disguised as an innocent application, such as a computer game. It can copy information being used by an authorized user when the user is using an application. It performs its chores without the legitimate user knowing and copies the information to a different location where an attacker can access the information. Hackers and malicious computer users develop new viruses and variants of existing viruses every year.

The last category of threats is the *underlying threat*, which further support and enable more fundamental threats. Examples of underlying threats include:

- *Spoofing or Eavesdropping:* This involves the monitoring of a network with the intention of reading the information that passes through it. Unauthorized persons obtain information by gathering it when authorized users access it via the network.
- *Traffic analysis:* In the new millennium, advanced technology and equipment exists which gather useful information through the observation of traffic communication patterns in a network.

For example, traffic (information flow) between Company A and Company B may have increased over the past few days. This may lead a hacker or eavesdropper to infer the possibility of a proprietary information transfer, especially when the communication traffic is between two major organizations.

### **2.1.2 Computer Information Security**

There can be no doubt that information security, which may be described, as the discipline to ensure the confidentiality, integrity and availability of electronic assets, is today an extremely important aspect in the strategic management of any company. In support for the managerial approach to information security, Solms also states that information security has long ago moved being only a technical issue<sup>[13]</sup>. In the context of this research, computer information misuse has been categorized into four broad areas:

- (i) Theft of computational information resources
- (ii) Disruption of computational information services
- (iii) Unauthorized disclosure of information
- (iv) Unauthorized modification of information

Major techniques, which initiate breaches in computer information security, include:

- (i) Human error

- (ii) User abuse of authority
- (iii) Direct probing
- (iv) Probing with malicious software e.g. *Trojan horses, worms, bombs*
- (v) Direct penetration
- (vi) Subversion of security mechanisms

### 2.1.3 Hackers

Standard hacking procedures include finding vulnerable machines (*the discovery phase*) and gathering information (*the foot printing stage*) <sup>[14]</sup>. Hackers find weak systems by searching specifically for recently created Web Servers, knowing that they are often good targets. These systems are vulnerable because they have not been properly configured with the latest updates. Installing server software on some versions of Linux or Windows places certain administrative help files or HTML-based configuration files in the standard directory for web serving.

Since search engines constantly spider Internet Protocol (IP) address ranges and domains, the server will pop up as a site, listing this default content when a search engine indexes these files. The hacker then homes in on this information.

Internet Information Server (IIS) is just one among many that hackers can easily attack if they suspect that a particular machine is weakly protected or left wide open with a default

installation. For example, to find vulnerable Windows NT machines with default installations of IIS, a hacker can use a search engine such as [www.Google.com](http://www.Google.com) and conduct a search for "*publish with Microsoft Internet Information Server*".

There is a high probability that the search will contain links to several out-of-the-box IIS installations. Figure 2-2 shows a search routine using the string: "*Try the hyperlinks*

*above to see some examples of the content you can publish with Microsoft Internet Information serve*". This search produced eighty-one (81) pages of results, which includes a huge number of potentially vulnerable websites.

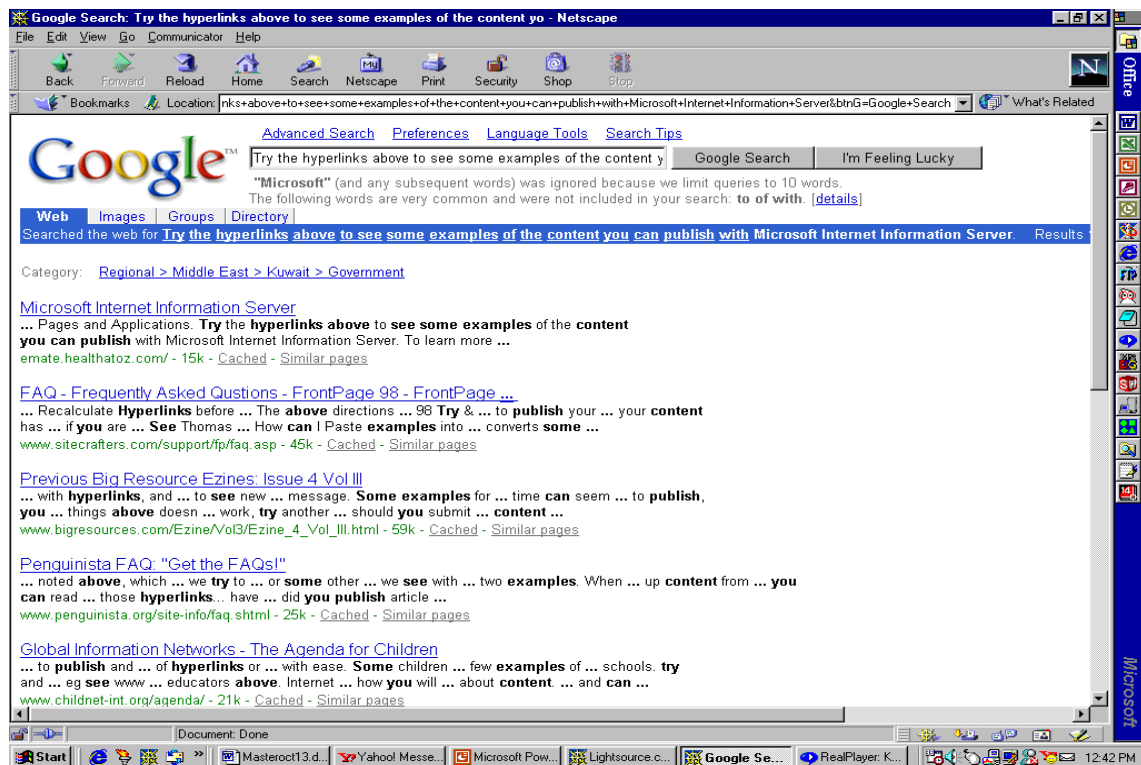


Figure 2-2 A Search routine using Google search engine

Analogously, another example using the Altavista search engine at [www.Altavista.com](http://www.Altavista.com) is shown in Figure 2-3. This example uses the string: *"This page is used to test the proper operation of the Apache Web server after it has been installed"*. The search produces 782,605,427 results. Inclusive in this number are websites with great potential for hacking activities.

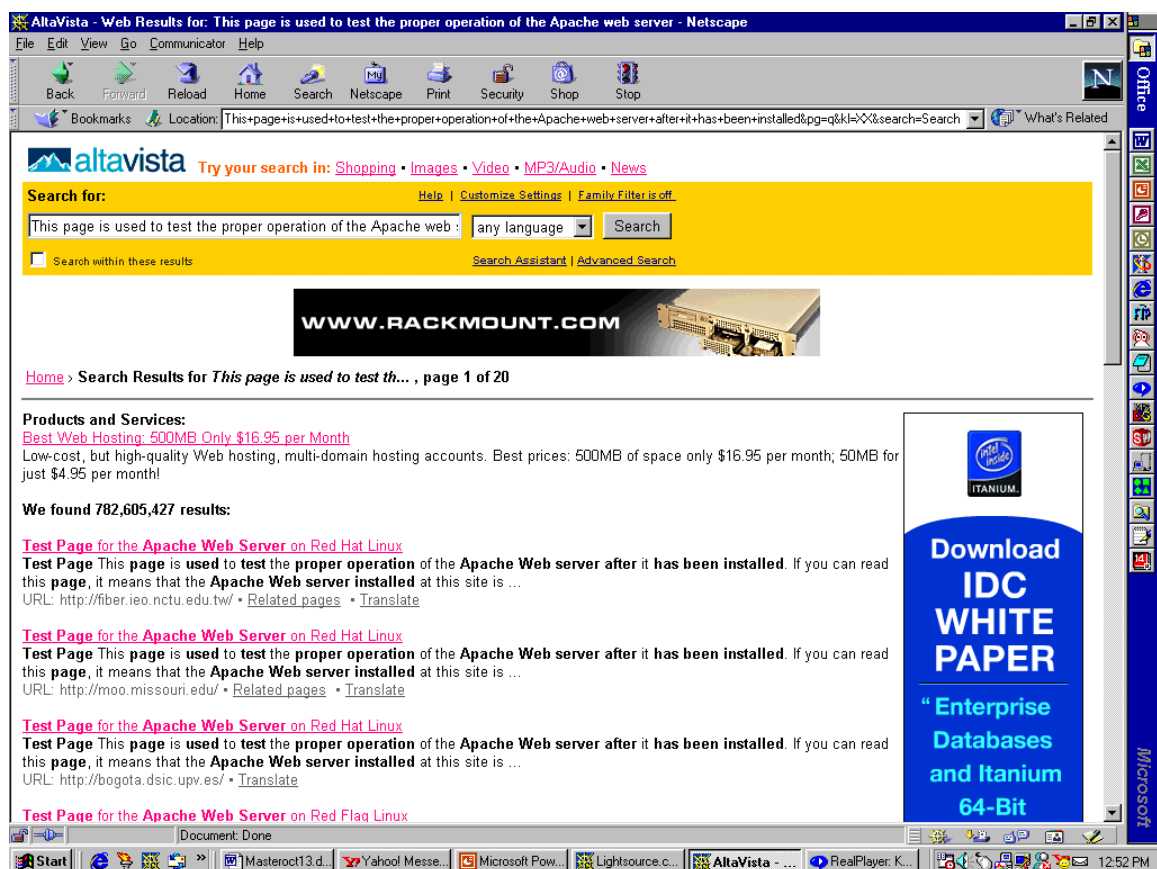


Figure 2-3 A Search routine using Altavista search engine

### 2.1.4 Search Engines

Search engines implement vulnerable security policies, which help hackers attack machines anonymously and gather confidential data <sup>[14]</sup>. Search engines index a huge number of web pages and other resources that sometimes inadvertently expose security weaknesses. Furthermore, search engines help hackers avoid identification.

Several search engines, such as Altavista, Google and HotBot, offer automatic web translation to their users. Users request a uniform resource location (URL) from a search engine; the resource is then downloaded, translated and sent back to the user. This sequence of anonymous proxies is depicted in Figure 2-4.

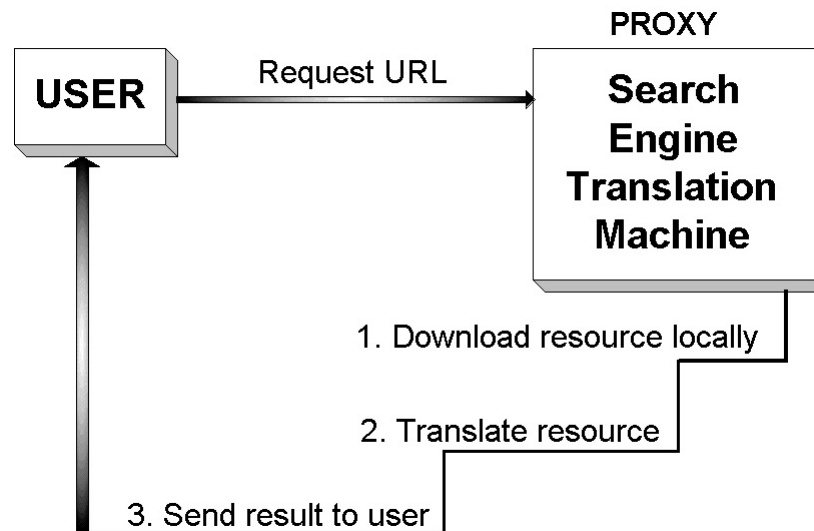


Figure 2-4 Anonymous proxies

### 2.1.5 Viruses, Trojan Horses and Worms

A computer virus is a program designed to spread itself by first infecting executable files or the system areas of hard and floppy disks. It then makes copies of itself and operates without the knowledge of the computer user. Some viruses are deliberately designed to damage computer files while others just interfere with computer operations.

Purposefully written malicious computer programs consist of two parts: the self-replicating code and the 'payload', which produces the side effects. Figure 2-5 shows a graphical representation of both infected and uninfected programs.

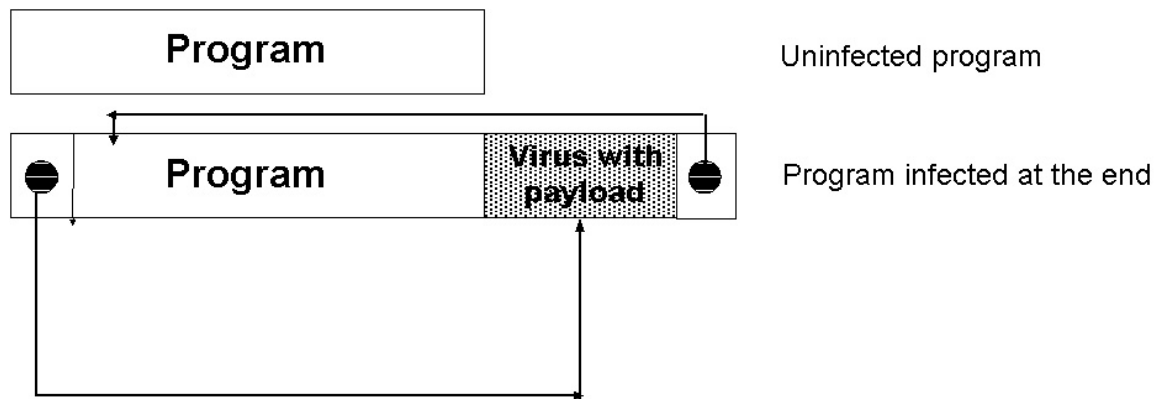


Figure 2-5 Program infected with a virus

*Trojan horses* are often confused with viruses. A Trojan horse is not a virus but is simply a program that pretends to be something else. It is a piece of code embedded in a program that performs unwanted actions <sup>[15]</sup>. For example, a sample program may be a login program that not only performs the login function but also makes unauthorized

copies of the usernames and passwords. A worm, on the other hand is a program that propagates itself from computer to computer. Worms may be classified as being either benign or malicious. A beneficial worm might be a migration of computing workload to unused computers and an example of a malicious worm is the November 1988 DARPA Internet intrusion in which a program rapidly replicated itself into many computers connected by a network <sup>[15]</sup>.

Viruses or Trojan horse programs are often activated when the computer, which hosts them, executes some type of executable code. This could be something from a floppy diskette, an attachment in an email, or a downloaded file via the Internet.

General remedies or protection against viruses include:

- Installation of anti-virus software from reputable companies. Such software packages need to be updated regularly because new viruses and variants of old viruses (which are designed to survive recent anti-virus "deactivation") come out every day. Good anti-virus packages have built-in features, which include the automatic scanning of any executable document.
- Disabling features such as JavaScript or Word macros which news and email software often activate automatically.
- Performing regular backups, which will ensure that important files are duplicated, incase a virus does attack.



According to Bontchev, the process of virus creation is not going to stop or even to slow down significantly in the foreseeable future <sup>[16]</sup>. After a few years of activity, the virus writers usually grow up and switch to other activities - but many new "wannabe" virus writers (usually adolescent kids) pop up in their place. What can be done?

Bontchev insists that the governments of the countries where most viruses are created should be pressed to pass the appropriate legislative measures <sup>[16]</sup>. Unfortunately, in many cases this is very difficult - Russia and some countries from the former Eastern Block have a notorious history of disregard of the concept of intellectual property. Other countries - the USA - consider virus writing as form of free speech and thus protected by the constitution. In general, the legislature is notoriously slow and backwards in dealing with computer-related problems. From the technical point of view, the users must be educated to rely more on other anti-virus measures, not only on scanning. Anti-virus software is certainly the most popular defense against viruses and may be classified as a good defense against viruses, but it is not the only defense. Gordon states that workable, effective policies and procedures set in place will improve the defense against viruses, and are necessary to ensure damage control <sup>[17]</sup>.

Indeed, the field of computer virus research is somewhat complicated. People have alleged that some of the academic virus *researchers* are actually creating the strains they claim to study. A few people have also accused the anti-virus software developers of creating a market for themselves in the first place, since it would be absolutely in their own best interests to keep the viruses flowing. Anti-virus companies worry about staying

profitable with the emergence of certain operating systems that cannot be infected with boot viruses<sup>[18]</sup>. Hence, implying the possible catastrophic loss of business.

#### **2.1.6 Confidentiality, Integrity & Availability**

Confidentiality, integrity and availability are seen as the generic properties of security<sup>[19]</sup>. Secure information is kept confidential. It remains private between communicating parties. The main method of enforcing confidentiality is through some form of encryption. Clipsham agrees that maintaining integrity of data during information processing is a problem throughout industry<sup>[20]</sup>.

The current emphasis and research for information integrity is based on the technical aspects of systems development. These include looking at the occurrence of errors in programming, hardware and software security, encryption and hashing algorithms. All of these are considered to be essential in ensuring safe and accurate information.

Clipsham also states that the problem of information and data integrity lies with the end user and the type of systems used. The systems developer needs to be made aware of the information integrity pitfalls and dangers in the development of end user systems<sup>[20]</sup>.

The confidentiality and integrity of systems and data are compromised by unauthorized access. Passwords remain the primary means of user authentication in most organizations. However, passwords as an effective access control mechanism have shown notoriously weakness in recent time. Close friends and colleagues can observe passwords easily. In other cases, two or more people have to share the same password to a common resource and thus it is no longer a secret for just one individual. This aids leakage, promotes unaccountability and increase security breaches.

With short, easy-to-crack passwords as the norm, the intruder's challenge of determining a correct password is neither difficult nor time-consuming. Armed with the wireless device and the user's password, an intruder can successfully impersonate the authorized user. Most hackers consider this a hobby and a form of entertainment.

## **2.2 Review of Information Security Methodologies**

Wave after wave of new technologies has deluged the information security marketplace. Information assurance problems have become more important as the world uses more information systems, since the security and survivability of information systems directly or indirectly affect organizations <sup>[21]</sup>. Current information security methodologies include firewalls, encryption, virtual private networks, and intrusion detection. A comprehensive list of these technologies and their limitations is given in Appendix B.

With each technological wave, the job of information security practitioners should get a little bit easier, but serious and systemic problems still exist. It is important to take advantage of the latest breakthroughs, but it is also vital to understand the limitations of these new technologies.

### **2.2.1 Firewalls**

A firewall is a term traditionally applied to one or more specialized routers used in optional coordination with hosts supporting proxy applications. A firewall's purpose is implementing part or all of a security policy by examining layer protocol headers and providing selective access to some or all of a network.

Firewalls are one of the newest pieces of information security improving equipment <sup>[22]</sup>. However, and according to Hancock, firewalls are not perfectly secure and their installation may hinder the speed of communication <sup>[23]</sup>. In order to get the best out of firewalls, these devices must be installed correctly.

These devices set up an invisible boundary between a network and the "outside world" (e.g. the Internet). It prevents unauthorized users from gaining access to organizational files and data. A firewall cannot control anything that happens after a user has passed authentication and access checks. A firewall cannot control people who go around or

circumvent it. If the network perimeter security integrity is not maintained then the system is still insecure.

Access through firewalls is controlled by source and/or destination IP addresses, layer protocols (UDP or TCP), the application and direction of stream establishment.

### **2.2.2 Cryptographic Security**

Cryptography helps provide accountability accuracy, and confidentiality. Fortunately, the good news is that algorithms and protocols are already available to secure systems. Molva states that most organizations, for fear of security breaches on the Internet, are forced to resort to radical solutions, which include physical separation between protected private networks (intranets) and the public Internet <sup>[24]</sup>.

However, the resulting segmentation is a major impediment to the accomplishment of the concept of a global Internet. Cryptographic security offers a viable alternative to segmentation by preserving a strongly connected global network. However, implementing the protocols successfully requires considerable expertise.

Several researchers have commented on the failure of cryptographic systems. Anderson states that designers of cryptographic systems suffer from a lack of feedback about how

their products fail in practice, as opposed to how they might fail in theory <sup>[25]</sup>. This is leading to a false threat model being accepted. Almost all security failures are in fact due to erroneous management and implementation. Interestingly, the bulk of computer security research and development is expended on marginally relevant activities rather than on real needs. The real problem lies in the search for the best scheme to build robust security systems. Recent research also shows that the fundamental organizing principle for security robustness properties appears to be explicitness. Robustness has been shown to be central in the design of cryptographic algorithms, authentication protocols, and securing operating systems, as well as in the application level.

### **2.2.3 Digital Signatures**

A digital signature scheme is a method by which the signer can sign an electronic document for the receiver (or the verifier) to keep as evidence that the document was indeed sent originally from the signer.

Digital certificates are used to prove the origin and authenticity of software programs and the data on the Internet, a key requirement for users who are downloading patches or software updates. Verisign and other certificate issuers generate and digitally sign such certificates after first verifying the identity of the individual or organization that submitted the request <sup>[26]</sup>.

The National Institute of Standards and Technology (NIST) proposed the Digital Signature Algorithm (DSA) as the public standard for digital signature. DSA is for signatures only and is not an encryption algorithm. The Digital Signature Standard (DSS) specifies the DSA.

DSA is a public key algorithm. Its secret key operates on the message hash generated by Secure Hashing Algorithm (SHA-1). SHA operates on any input length less than  $2^{64}$  bits to produce a 160-bit output, a message digest. It is input to DSA, which computes the signature of the digest (as opposed to of the message itself). To verify a signature, one re-computes the hash of the message, uses the public key to decrypt the signature and then compare the results. The key size is variable from 512 to 1024 bits, which is adequate for current computing capabilities.

The DSA authenticates the integrity of the signed data and the identity of the signatory. The DSA may also be used in proving to a third party that data was actually signed by the generator of the signature. The DSA is intended for use in electronic data interchange, software distribution, data storage, and other applications, which require data integrity assurance and data origin authentication. Other uses include electronic mail and electronic funds transfer.

Currently, the security of a digital signature system is dependent on maintaining the secrecy of users' private keys. For adequate performance, private keys must be protected

from unauthorized acquisition. While it is the intent of the DSS to specify general security requirements for generating digital signatures, conformance to this standard does not assure that a particular implementation is secure.

The responsible authority in each agency or department still needs to assure that an overall implementation provides an acceptable level of security. NIST proposes to review this standard every five years in order to assess its adequacy. The DSA can be implemented in software, firmware, and hardware or a combination of these.

The DSA makes use of the following parameters:

System parameters:

$p$  = a prime modulus, where  $2^{L-1} < p < 2^L$  for  $512 \leq L \leq 1024$  and  $L$  a multiple of 64

$q$  = a prime divisor of  $p - 1$ , where  $2^{159} < q < 2^{160}$

$g = h^{(p-1)/q} \bmod p$ , where  $h$  is any integer with  $1 < h < p - 1$  such that  $h^{(p-1)/q} \bmod p > 1$

( $g$  has order  $q \bmod p$ )

The integers  $p$ ,  $q$ , and  $g$  can be public and can be common to a group of users.

Public key and secret key of users:

$x$  = a randomly or pseudorandom generated integer with  $0 < x < q$  (secret key)

$y = g^x \bmod p$ , where  $1 < y < p$  (public key)

The public and private keys are fixed for a period of time. Parameter  $x$  is used for signature generation only.



Signature generation for message,  $m$

$k$  = a randomly or pseudorandom generated integer with  $0 < k < q$

$$r = (g^k \pmod{p}) \pmod{q}$$

$s = (k^{-1} \times (H(m) + x(r)) \pmod{q})$  where  $H(\cdot)$  is a one-way hash function.

The pair of numbers  $(r,s)$  make up the signature of the message,  $m$ , signed by the user with public key,  $y$ , and private key,  $x$ .

Signature verification:

$$w = s^{-1} \pmod{q}; u_1 = w(H(m) \pmod{q}) \text{ and } u_2 = w(r \pmod{q})$$

The recipient computes  $w$  and then verifies the validity of the following equation:

$$r = (g^{u_1} \text{ multiplied by } y^{u_2} \pmod{p}) \pmod{q}$$

#### 2.2.4 Intrusion Detection Systems

In the last several years, researchers have deeply investigated *intrusion detection systems* [27]. Intrusion Detection Systems (IDSs) both identify intrusions and trigger corresponding recovery procedures that lead the system from a faulty to a correct state. While current IDSs automatically handle intrusion detection, the system administrator usually manages the intrusion recovery.

According to the CSI, the market for intrusion detection systems (IDS) is growing. Just as in the early stages of the firewall market, there is a lot of hype, a lot of misconceptions, a lot of unrealistic expectations, and a lot of money being thrown around. The Aberdeen Group, estimates the IDS market at \$100 million in 1998 alone <sup>[3]</sup>.

Intrusion Detection is the art of detecting inappropriate, incorrect, or anomalous activity. Intrusion detection systems that operate on a host to detect malicious activity on that host are called host-based intrusion detection systems, and intrusion detection systems that operate on network data flows are called network-based intrusion detection systems.

An intrusion usually implies an attack from outside, while misuse describes an attack, which originates from the internal network. This is however somewhat subjective.

Three primary ways in which an intruder gets into a system are:

- Physical Intrusion, where the intruder actually makes physical contact with the source of entry i.e. the computer used to gain entry into the system
- System Intrusion, where the intruder already has some privileges on the system but goes beyond his/her authorized point
- Remote Intrusion, where the hacker intrudes from a remote location, possibly via the Internet.

Firewalls may not always recognize attacks and block them. For example, a typical corporate firewall allowing access to the Internet would stop all UDP and ICMP datagram traffic, stops incoming TCP connections, but *allows* outgoing TCP connections. This stops all incoming connections from Internet hackers, but still allows internal users to connect in the outgoing direction. Thus, the firewall acts as a fence. A fence has no capability of detecting somebody trying to break in (such as digging a hole underneath it), nor does a fence know if somebody coming through the gate is allowed in. It simply restricts access to the designated points.

As a result, intrusion detection systems are usually used to compliment firewall services. Intrusion detection systems are much more dynamic in their defense. An IDS will recognize attacks against the network that firewalls are unable to see. Intrusion detection systems are an important component of defensive measures protecting computer systems and networks from abuse <sup>[28]</sup>. In summary, IDSs are added to networks for the following reasons:

- It checks poorly configured firewalls
- It detects attacks that firewalls would legitimately allow
- It works within the perimeter as well

The most common approaches to intrusion detection are statistical anomaly detection and pattern-matching detection.

### **2.2.5 Virtual Private Networks (VPNs)**

Connection to the Internet inevitably increases exposure and vulnerability to unwanted attacks. A Virtual Private Network (VPN) is an IP-based network that uses encryption and tunneling to achieve security between connected networks (Local Area Networks – LANs and Wide Area Networks – WANs). A VPN can also extend the existing network security to include third party players such as partners, suppliers and customers. In its broadest interpretation, a VPN is a private logical network that uses a shared physical medium. Steinke et al. acknowledge that the dynamic nature of a virtual enterprise, as well as the increased use of information technology, creates additional concerns for security<sup>[29]</sup>.

The envisaged product design system will involve continuous or interrupted connection to third parties to enable all the key players have adequate participation in the design of any given product. In effect, trust relationships between domains are extended to include participating parties.

An important issue regarding the efficiency of VPNs is *performance*. Majority of VPN solutions exist on client machines and gateway servers at the extreme ends of the

communications path. Hence the elements and customers in the middle of this chain are not adequately serviced. The Internet is in the middle of the link and is ultimately affected by the negative issues surrounding the VPN. New VPN technologies are being developed today to improve its efficiency and eliminate most of its current loopholes.

### **2.3 The Quest for Information Security**

The total security in an organization has many forms and variations. Thomas Finne, describes an *Information Security Chain*, which links key factors in a company's information security<sup>[22]</sup>. Security links in this chain such as Back-up, Off-site Storage, Biometric Methods, Card Access, Computer (Server) Locks, Data Encryption, Passwords, Viruses, Firewalls etc., all emphasize the need to protect information.

Other researchers maintain that information should be consistently protected and this principle should apply in all instances<sup>[30]</sup>. This approach supports the goals of *Pegasus*. Forcht et al. acknowledge that many prospective business users are wary of the Internet because of existing and potential security loopholes and conclude that doing business online involves some risks, like any other business transaction, but if attention is devoted to installing secure procedures, it is no riskier than other business practices<sup>[31]</sup>.

## **2.4 Information Security Management**

With the advent of public key security and certification, the transition from current business delivery methods to future Internet-based systems is now possible. However, electronic commerce (or business) won't take off without a security infrastructure to protect users <sup>[32]</sup>. In looking for a solution to the information security problem, Kyamakya et al. noted that society is growing increasingly dependent upon large-scale, highly distributed systems that operate in unbounded network environments, which like the Internet have no central administrative control and no unified security policy <sup>[33]</sup>.

Kyamakya et al. made the proposal that the discipline of network survivability and security can help assure that such systems can deliver essential services and maintain essential properties such as integrity, confidentiality and performance, despite the presence of intrusion <sup>[33]</sup>. In other words, security breaches are somewhat unimportant.

The important thing was being able to perform effectively despite the break-in as a result of having a solid foundation of building blocks out of which the information infrastructure is formed. Figure 2-6 depicts the building blocks, which identify the presence of critical functions in a networked information infrastructure.

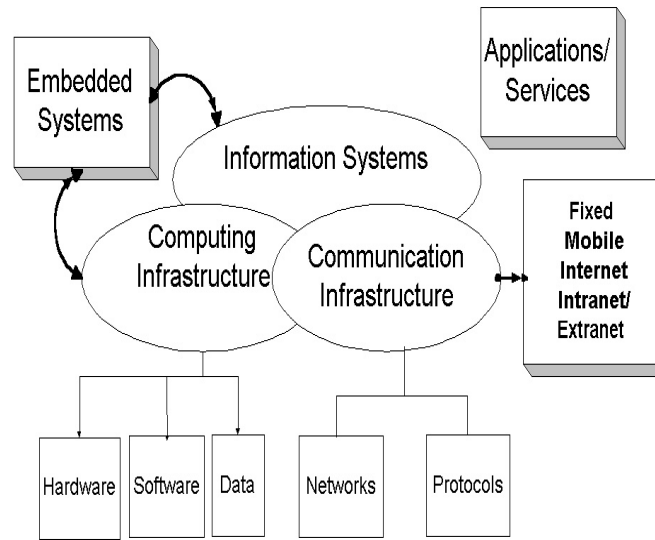


Figure 2-6 Building blocks

In contrast, the proposed model in this research does not intend to totally ignore intrusions and security breaches, but learn from such break-in, reduce them to the barest minimum, maintain and manage an effective level of security. However, Kyamakya et al. do support the need for management in information security by stating that as the information society expands, it may be the case that issues of *information management* take an increasingly dominant role <sup>[33]</sup>.

Duan et al. state that security management is one of five management functions defined by International Standards Organization/Open Systems Interconnection (ISO/OSI), which covers two aspects: security of management and management of security <sup>[34]</sup>. ISO/OSI recommends five groups of security services: authentication, access control, data integrity, availability and non-repudiation. Duan et al. also proposed a high-level security policy and collaborative *management* of firewalls. However, this approach does

not address all the problems of information security. Nevertheless, the need for security management is adequately recognized.

Berker also supports the management approach by stating that the use of security methodologies, such as cryptography, to secure business transactions will become more and more necessary and new mechanisms will be required to provide control between trading partners<sup>[35]</sup>.

Other researchers of information security management and certification also exist. The Information Security Institute of South Africa (ISIZA) developed a security certification model consisting of BS 7799 controls<sup>[36]</sup>. The BS 7799 Code of Practice for Information Security Management, now known as ISO 17799, is an internationally accepted scheme against which formal information security certification can be done precisely. They serve as guidelines and explicit instructions for protecting resources<sup>[37]</sup>.

However, although most companies were anxious to get some form of information security certification, the official BS 7799 route can be very difficult because of its 'all or nothing' design. A company must conform to all 10 sections of BS 7799, containing a total of 150 different high-level controls, before a certificate will be granted. Another set of guidelines known as the ISO 9000 incorporates the philosophy that a risks assessment must be performed if an information system is going to be both efficient and effective. ISO 9000 provides an important framework that management already understands for the



establishment, maintenance, enforcement and improvement of information security related infrastructure.

According to Stark, solutions to information security issues will involve three factors: the method by which the connection (to the internet) is made, the degree of security required and the Internet services the connect will support <sup>[9]</sup>. The proposed ISM Model will serve an information security control mechanism in the Pegasus project, securing an Internet-based WAN/LAN and securing Internet-based commerce.

### **3.0 THEORY OF COMPUTER INFORMATION SECURITY**

The full comprehension of certain principles (guidelines) and concepts is essential in addressing information security. These principles and concepts will be used as the foundation for establishing information security strategies, developing information security policies and formulating the framework necessary to manage information security issues effectively.

#### **3.1 Principles for Information Security Management**

This research categorizes the principles of information security management into three main classes. These are analyzed below.

##### **1. Pragmatic Principles:**

Education, training and awareness, although important are not sufficient conditions for managing information security <sup>[4]</sup>. Establishing a security culture will go a long way in developing and sustaining a consistently secure environment. Pragmatic principles tend to divert major attention from the technical issues of information security. For example, in the simplest form of domestic security e.g. securing a house - if the occupants of the house are not ready to lock the doors or set an alarm (if one exists) every single night of their occupancy in that house, they are more likely to have poor security results,

despite any ‘state-of-the-art’ security equipment that may have been previously installed in the house. Thus, pragmatic principles play a major role in the methodology used in this work.

## 2. Ethical Principles:

Ethics is an important facet of comprehensive information security. However, ethics from the point of view of security personnel and ethics from the point of view of hackers are defined differently. Leiwo et al. conducted an analysis of ethics as a foundation of information security and agreed that security of distributed systems requires both technical and administrative foundations<sup>[38]</sup>.

Their major argument is that hacking ethics is indeed significantly different from information security ethics and therefore major difficulties must be solved to establish widely accepted standards for ethical usage on information systems and communication networks.

However, further research questions exist regarding the feasibility of ethics-based foundations in information security. Ethics principles also include responsibility, trust and integrity.

## 3. Technical Principles:

Technology has a big role to play in any information security setting and cannot be ignored. It presents major constraints, which must be met in order to achieve

some form or semblance of security. Several principles also guide these technological constraints. For example, the use of firewalls to secure a network's perimeter

According to Dhillon, formal models for maintaining confidentiality, integrity and availability of information cannot be applied to commercial organizations on a grand scale because any formal model is an abstraction of reality <sup>[4]</sup>.

This would imply that technical principles present a domain approach to information security. This is called micro-management. Smaller pieces of the network information security are managed, until a cohesive enterprise-wide security is achieved.

The methodology for information security management in this research is a management framework, which will work with an *outward-perimeter* rule. This rule and other concepts are discussed in the next section.

### **3.2 Important Fundamental Concepts**

The *outward-perimeter* rule enables the proposed information security management model to begin its management process from the inside core of the host network and then

extend outwards in a virtual perimeter-wise fashion. This ensures total coverage of data in transit, stored files and other resources section by section depending on the information security policies in place.

Information security policies act as a foundation/support for the security and well being of information resources. These policies are the bottom line of information security within an organization.

Security policies can be developed or bought. The actual work involved with security policies is its implementation. The mere existence of security policy documents is not sufficient. The contents have to be deployed and implemented effectively; otherwise the document is more or less useless. Security policies should be comprehensive in their coverage of security issues and should directly reflect the needs of the organization. This indeed is a non-trivial issue.

From a pragmatic point of view, the model in this research postulates the need for information security policies, which start with an assessment of the current scenario and then take into consideration necessary changes according to other pragmatic, ethical and technological principles. The information security policy is one of the basic building blocks of the proposed Information Security Management Model (ISM Model).

A security model is a representation of the security policy. However, the security policy for one organization is bound to be different from that of another. Hence, there is also the issue of a language or communication protocol, which would serve as the common ground between diverse security policies.

In summary, this research established its methodology through the use of certain concepts, which include:

- a). An information security policy, stating the rules, laws and practices that regulate how sensitive information is distributed, managed and protected
- b). The use of an outward-perimeter rule to ensure the functionality of internal mechanisms that will enforce the information security policy
- c). Assurance that the mechanisms actually enforce the security policy

Elaboration is on the assurance that the security mechanisms in place actually enforce the information security policy. This incorporates the managerial approach to information security. However, the significance of the information security policy and the functionality of internal security mechanisms along with other principles and rules must not be ignored.

### 3.3 The Information Security Policy

Policies regarding the protection of business information and the processes for using and handling them are either non-existent or poorly specified <sup>[39]</sup>. Where these policies do exist, enthusiasm for the written word can run riot resulting in a many-paged document, rather than two (2) to four (4) pages which are more likely to be read and more easily digested.

Walker defined a security policy as “the set of laws, rules and practices regulating how an organization manages, protects and distributes sensitive information” <sup>[40]</sup>. The policy is needed to support security objectives and a range of security measures must be put in place to ensure that the goals of the security policy are met <sup>[41]</sup>. Nosworthy emphasizes the need enhance security through endorsements at all levels <sup>[42]</sup>.

There is *communications security*, which involves the security of information while it is being transferred or communicated from one system to another. Also, there is the *computer security*, which is the protection of information within a computer system. In this documentation, the word *information* is added between *computer* and *security* to denote special emphasis on information security. Hence in this context, computer security and computer information security virtually have the same meaning.

Kessler states that the main hurdle to adequate computer and network security is not the security technology, tools and products, but under-educated network administrators,

corporate managers and users <sup>[43]</sup>. Such conclusions also validate the significance of this research.

While attackers are constantly coming up with new ways to defeat improved security protection, the truth is that sophisticated attacks are usually unnecessary because a large percentage of sites only have the most rudimentary security measures in place. Security risks and the importance of secure systems need to be understood. Also, for security policies to be effective, they need to be implemented and enforced from the top management level, downwards.

Kessler also states some important issues, which seemingly dilute the effectiveness of any security policy <sup>[43]</sup>. These issues are listed below:

1. Distributed computing makes it harder to implement central policies
2. Some users do not take the information security issue seriously
3. Management does not support any infringement on user activities
4. Strong security runs counter to the organization's culture
5. Everyone believes that current and emerging security mechanisms are adequate
6. It is difficult to make the business case for strong security
7. Security is 'inconsistent' with the main line of business
8. Management does not punish security violations
9. Bottom line: There are no secure sites on the Internet, only vigilant ones



### **3.4 The Functionality of Internal Security Mechanisms**

The proposed web-based (electronic) product design system will enable users access data from various locations. Thus, the security system will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. Security perimeters can no longer work with static rules that associate a person with one or two IP addresses. Modern security technologies are needed to tune to the activities of IP infrastructures in order to apply meaningful restrictions and exceptions.

The Internal Security Mechanisms are the security services and software tools, which implement the required security functions. Depending on the specific activity undertaken in *Pegasus*, configured security mechanisms should be in place to ensure secure information transfer or storage.

### **3.5 The Information Infrastructure**

Any reasonable security layout for the web-based product design system will depend largely on the information infrastructure upon which it is built. Critical infrastructure is a test of whether a comprehensive strategy for trustworthiness is possible <sup>[44]</sup>. Infrastructure is the organization of a system at the most basic level. The structure of such a system, its design, behavior and characteristics of individual components and how they

interact make up the system's architecture. Information within the web-based platform is categorized as shown in Figure 3-1.

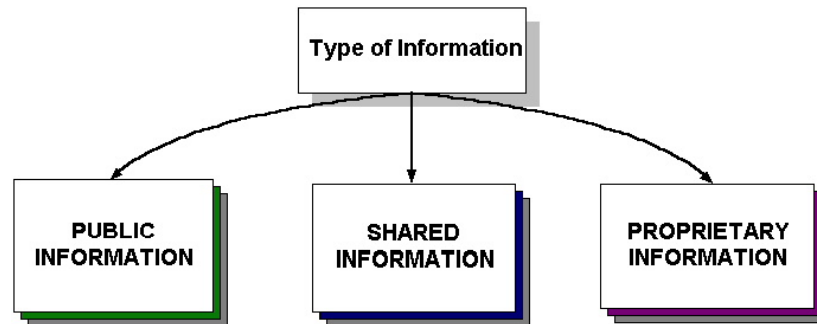


Figure 3-1 Types of Information

- *Public Information* (possibly open to the general public; not a security threat)
- *Shared Information* (between two or more affiliated organizations etc.)
- *Proprietary Information* (strictly between the customer and the designer)

The expected security model layout should be compatible with the infrastructure of the web-based design platform. The web-based design platform should exhibit:

- *Flexibility*: Ensuring that complete imposition of constraints and design objectives is impossible
- *Extensibility*: Ensuring that new constraint types can be incorporated as the system matures
- *Interoperable*: Allowing various constraints and designs to be retrieved and manipulated in a suitable format

- *Object-Oriented*: Design/Constraint Data and its interfaces can be stored together as a single interface

Generally speaking, information security is a composite and systematic problem <sup>[45]</sup>. Gollmann describes *e-commerce* security as protecting the parties involved in business transactions and not the messages transmitted during these transactions <sup>[46]</sup>. Indeed, information-based services raise profound nomenclature and security issues. Hence, the previous infrastructure requirements are defined within the context of this research and the broader project, *Pegasus*.

There are several security architectures for the distributed environment <sup>[47]</sup>. The Distributed Computing Environment (DCE) has its own security mechanisms. The Common Object Request Broker (CORBA) security model also defines security services such as authentication, access control, auditing and non-repudiation. As businesses head towards a unified connected planet, small global villages with global markets, are being satisfied with global goods and services. Clusters servers could be used in providing dedicated services via the Internet. A graphical example is given in Figure 3-2.

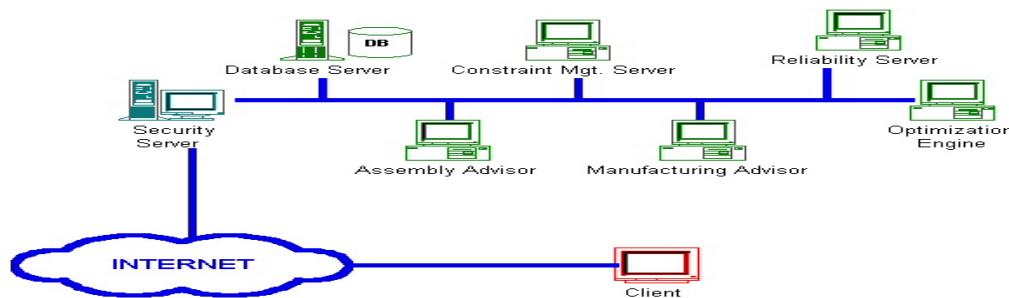


Figure 3-2 Sample cluster of servers

### 3.6 The OSI seven-layer model

The aim of the Open Systems Interconnection (OSI) is to provide a standardized means of communications between diverse computer systems. As a basis for the development of OSI standards, the International Standards Organization (ISO) have developed a Reference Model to partition the problem into discrete layers and to provide a conceptual framework for understanding the complexities involved.

OSI network management functions are grouped into five areas<sup>[48]</sup>. These functions are: configuration, fault, performance, security and accounting. Here, the security component is in two parts: *the management of security* and *the security of management*. Management of information within the OSI model is achieved through the definition of the security threats and services required to overcome such threats. Figure 3-3 shows an overview of OSI system management.

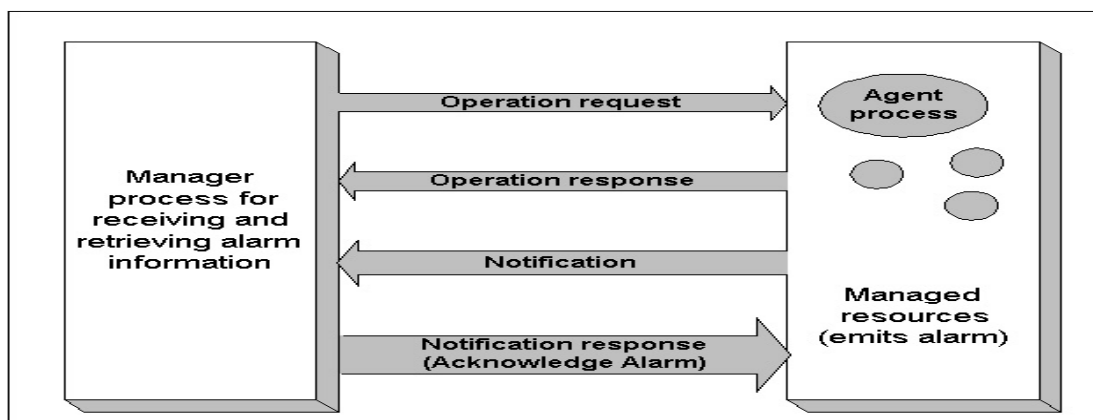


Figure 3-3 Overview of OSI Systems Management

### 3.7 Security in COBRA

Common Object Request Broker Architecture, CORBA, is an emerging open distributed object-computing infrastructure being standardized by the Object Management Group (OMG). The Object Management Group (OMG) realizes its goals through creating standards, which allow interoperability and portability of distributed object oriented applications. They do not produce software or implementation guidelines but specifications, which are, put together using ideas of OMG members who respond to Requests for Information (RFI) and Requests for Proposals (RFP). The strength of this approach comes from the fact that most of the major software companies interested in distributed object oriented development are among OMG members. Figure 3-4 shows the main components of the ORB (Object Request Broker) architecture and their interconnections.

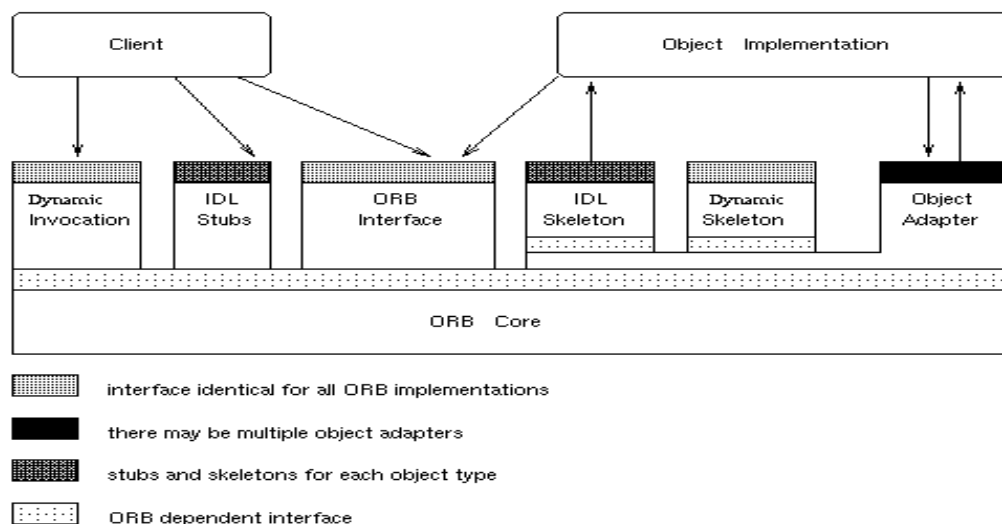


Figure 3-4 Main components of the ORB architecture and their interconnections

The Object Adapter (OA) handles communication between the object implementation and the ORB core. It handles services such as:

- Generation and interpretation of object references
- Method invocation
- Security of interactions
- Object and implementation activation and deactivation
- Mapping references corresponding to object implementations
- Registration of implementations

CORBA specifies a system, which provides interoperability between objects in a heterogeneous, distributed environment and in a way transparent to the programmer. Its design is based on OMG Object Model.

The Object Management Group (OMG) specifies four (4) policies that may handle object implementation activation:

- *Shared Server Policy*, in which multiple objects may be implemented in the same program
- *Unshared Server Policy*, *Server-per-Method Policy*, in which a new server is started each time a request is received, and
- *Persistent Server Policy*, in which the object's implementation is supposed to be constantly active (if it is not, a system exception results). If a request is invoked under

any other policy, the Object Adapter (OA) will activate the object in the policy specific way. In order to be able to do that, the OA needs to have access to information about the object's location and operating environment.

Currently, CORBA applications are run in an Intranet system protected by firewalls. However, the *Pegasus* Project incorporates links to the Internet.

### **3.8 The File Transfer Protocol**

A widely used way to send information across the Internet is using File Transfer Protocol (FTP). FTP appears to have some safeguards through the use of user ID's and passwords. However, these are weak safeguards at best because the user ID and passwords are transmitted in clear text. Adding some sort of pre-processing and post-processing to encrypt files before exposing them to FTP and then decrypting them afterwards incorporates security. However, cumbersome, slow and batch-oriented processes result. This is certainly not the kind of foundation on which high-flying e-commerce applications are built.

Then there is also the issue of the completeness of the data. With FTP, the user needs to know that all the data has been received during transmission. Files for transfer at the end of the day also need to be scheduled. This requires more customized development. The reality is that FTP is poorly suited for high volume business applications.

### 3.9 Public Key Infrastructure

This is a wonderful and clever technology to control authenticity, non-repudiation, and security of information. Basically, each entity is assigned a security certificate that contains a private key and a public key. Information encrypted with the public key can only be decrypted with the private key, and information encrypted with the private key can only be decrypted with the public key.

So if Company A wants to send data to Company B, they first send an “*introduction*” encrypted with their private key. When Company B decrypts this information successfully with Company A’s public key, they establish that they are indeed talking to Company A. Thereafter, Company A sends the actual information encrypted with Company B’s public key. Company B is the only entity that can decrypt this data, using their private key. So this clever *two-step process* ensures the integrity and safety of the information.

Where did these certificates come from? There are companies, which presently issue Public Key Infrastructure (PKI) certificates that work with their encryption software. However, the certificate issued by one company may not be compatible with certificates from another company. Also, the management of the issuance, expiration, and revocation of certificates is a critical component to ensure the certificates themselves are valid and not compromised.



At the time of this research, industry standards for controlling all of these administrative issues are not yet fully in place. As a result, PKI is not quite “ready for prime time” as of yet for most e-commerce applications, especially those that involve multiple companies.

### **3.10 The Secure Sockets Layer Protocol**

The Secure Sockets Layer (SSL) protocol is a security protocol that provides communications privacy over the Internet. It is an industry-standard security protocol that allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. SSL provides data privacy and authentication. By convention, web pages that require an SSL connection begin with "*https:*" instead of the usual "*http:*".

A secure server is a special server used for processing private or sensitive information submitted by users. It uses the Secure Socket Layer encryption to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g., Transmission Control Protocol), is the SSL Record Protocol.

The Secure Sockets Layer Record Protocol is used for the encapsulation of various higher-level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption

algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of the SSL is that it is application protocol independent.

A higher-level protocol can layer on top of the SSL Protocol transparently. The SSL protocol provides connection security that has two basic properties:

- *The connection is private:*

Encryption is used after an initial handshake to define a secret key. Symmetric cryptography may be used for data encryption (e.g., Data Encryption Standard (DES), RC4 Encryption Algorithm etc.). The peer's identity may be authenticated using asymmetric, or public key, cryptography (e.g., RSA Encryption, Digital Signature Standard (DSS) etc.).

- *The connection is reliable:*

Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g., SHA, MD5, etc.) are used for MAC computations.

The goals of the SSL protocol include:

1. *Cryptographic security:* SSL should be used to establish a secure private connection between two parties.

2. *Interoperability*: Independent programmers should be able to develop applications utilizing SSL that will successfully exchange cryptographic parameters without knowledge of each other's code.

3. *Extensibility*: SSL seeks to provide a framework into which new public key and bulk encryption methods can be incorporated as necessary.

4. *Relative efficiency*: Cryptographic operations tend to be highly CPU (Computer Processing Unit) intensive, particularly public key operations. For this reason, the SSL protocol incorporates an optional session caching scheme to reduce the number of connections that need to be established from scratch.

### **3.11 Internet Security Protocol**

The IP Security Protocol (IPSec) provides per-packet authenticity/confidentiality guarantees between communicating peers. IPSec consists of separate protocols:

$$\text{IPsec} = \text{AH} + \text{ESP} + \text{IPcomp} + \text{IKE}$$

(i) *The Authentication Header (AH)*:

The Authentication Header provides an authenticity guarantee for packets by attaching crypto checksum to packets. If a packet is received with an authentication header and the checksum operation is successful then the parties involved may possess a secret key that

is private between both parties. The authentication header covers the entire packet (from the IP header to the end of the packet).

*(ii) Encapsulating Security Payload (ESP):*

The Encapsulating Payload provides a confidentiality guarantee for packets by encrypting packets with encryption algorithms. ESPs received and decrypted successfully imply the absence of wiretaps in the packet. Also all secret keys shared between parties are kept secret between the parties in question.

*(iii) IP payload compression (IPcomp):* Encryption from the Encapsulating Security Payload places a negative impact on compression. IPcomp tackles this problem by finding a way to compress a packet before encrypting.

*(iv) Internet Key Exchange (IKE):* The Internet Key allows for communication between distant locations by providing key negotiation in secret.

IKE is implemented as a daemon process while AH, ESP and IPcomp are implemented in the kernel code. IKE is also optional since secret keys can be configured manually for AH/ESP. However, the security of the IPSec protocols depends on the absolute secrecy of the secret keys. The Transport Mode and the Tunnel Mode are the two modes in which the AH, ESP and IPcomp protocols operate. The Transport Mode provides

encryption of normal communication between peers. The Tunnel Mode encapsulates packets into the new IPv4/v6 header.

Policies are also used to configure and specify which packets require security. The selected policy determines which IPsec protocols (AH, ESP or IPcomp) will be used with each packet. Such policies can be configured in a *per-socket* or *per-packet* manner:

- *Per-packet:* Packets, which require security, are configured into the kernel just like packet filters e.g. "All packets going to address 111.23.33.255"
- *Per-socket:* Packets, which require security, are configured with respect to certain sockets e.g. "All outgoing packets from socket X".

### **3.12 Building On Solid Foundations**

The topic of distributed objects is complicated enough when considered on its own and it certainly doesn't get any simpler with the addition of security. As a result of this complexity, there are many issues that are under specified and open to interpretation at this time, which provides an increased scope and avenue for research and development in this area.

The different aspects of the theory of computer information security listed in this chapter serve as the backbone of the Information Security Management Model proposed in the next chapter. Once again, it is emphasized that this management model addresses issues strictly within the Pegasus project and all research was done with this project as its background.

As seen in the past sections, managerial models were also used for OSI network management. Many security issues overlap no matter the scenario. Thus, the basic questions which the proposed ISM Model addresses are:

- i) What security threats does the Pegasus Designer Studio environment face?
- ii) How can these security threats be addressed through security services or mechanisms?
- iii) How is the functionality of these services/mechanisms implemented through locations/within protocol stacks?
- iv) How is the entire Pegasus Designer Studio system managed to produce an environment that is *optimally* secure?

## 4.0 METHODOLOGY

The literature review in Chapter Two summarized numerous computer information threats and vulnerabilities along with various technologies, which exist today to provide security for a computer network. However, the failures recorded and the increasing number of security breaches, preempt the need for a different approach in tackling information security issues.

This chapter incorporated an administrative/managerial perspective into the technical overview. The new question is: Would there be better results if a management framework were involved in information security issues? This question is the basis of the methodology employed in the *Information Security Management Model (ISM Model)*.

### 4.1 Methodology Approach

As noted by Wood & Snow, one of the big problems haunting many information security efforts involves inadequate infrastructure <sup>[49]</sup>. As mentioned earlier, *Pegasus* will deal with three main types of information: the shared information, the proprietary (strictly private) information and the public information. The infrastructure is composed of the policies, procedures, responsibility statements etc. necessary to conduct secure business

transactions. Also mentioned in the literature review are certain principles, which serve as guidelines in creating a management framework for information security.

The methodology employed in developing the ISM Model framework takes note of the fact that even the best security systems can be compromised if they are not managed properly. The proposed Information Security Management Model aims at providing three basic facets of security: access control, integrity and availability.

## **4.2 Required Features of the Security Layout**

In line with the proposed web-based product design and realization system, the following requirements are essential to the design and development of the resulting security management model:

- ❑ *Flexibility:* The security management model should allow for complete imposition of design objectives.
- ❑ *Extensibility:* The security management model should allow for expansion in the future.
- ❑ *Interoperability:* The security management model should allow for fast manipulation of various designs. Issues such as patents and cross licensing come into play.
- ❑ *Object-oriented:* The security management model should comply with simultaneous design and constraint data storage as a single interface.



### **4.3 The Proposed Information Security Management Model (ISM Model)**

The proposed Information Security Management Model (ISM Model) presents a managerial approach to information security issues. It consist of eight (9) main components, namely:

- The User Manager
- The Information Security Policy
- The Security Matrix
- The XML Knowledge Base
- The Third Party Software Interface
- The ISM Model Security Services
- The Alert/Alarm Mechanism
- The Communication Protocols
- The Pragmatic, Ethical & Technical Principles' Hive

These components are all inter-related and each component serves as input or output to some other component. A general overview of the Information Security Management Model (ISM Model) is shown in Figure 4-1.

A more detailed graphical description of the model with subunits of the components is shown in Figure 4-2.

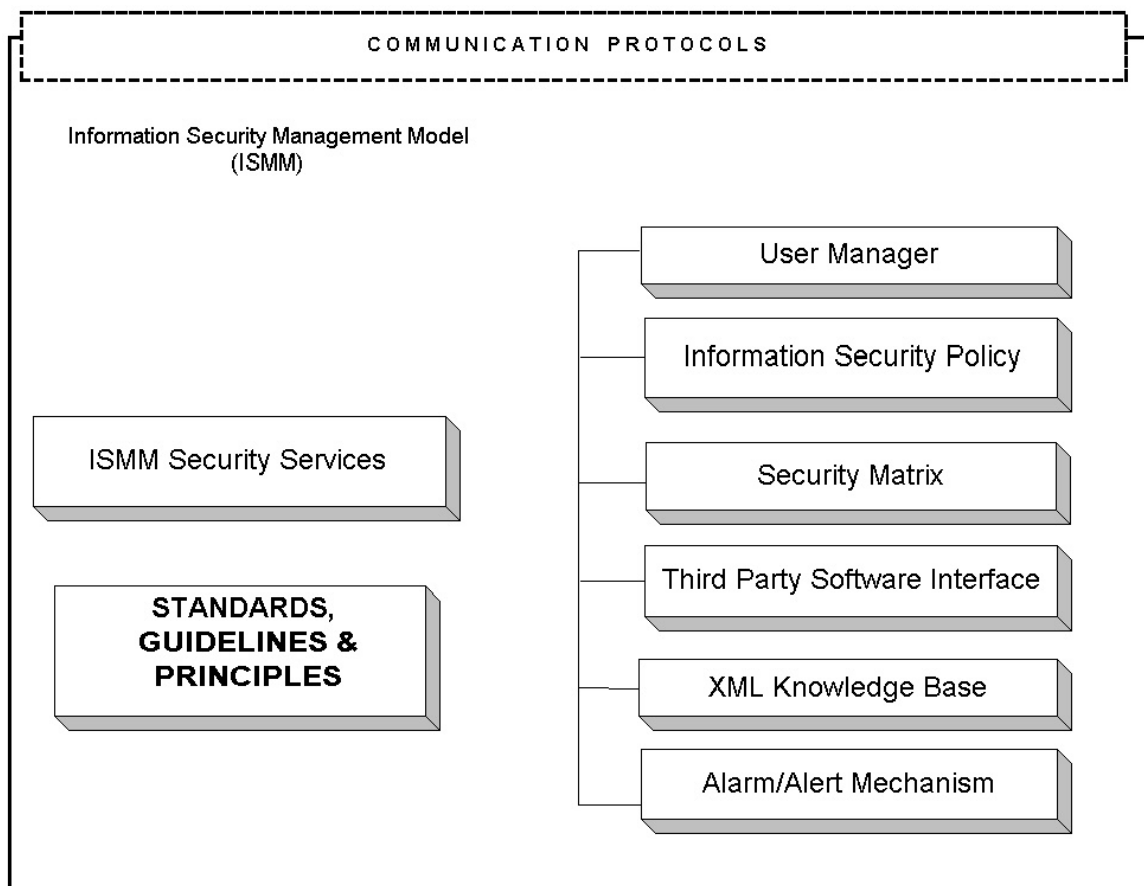


Figure 4-1 General Overview of the Information Security Management Model

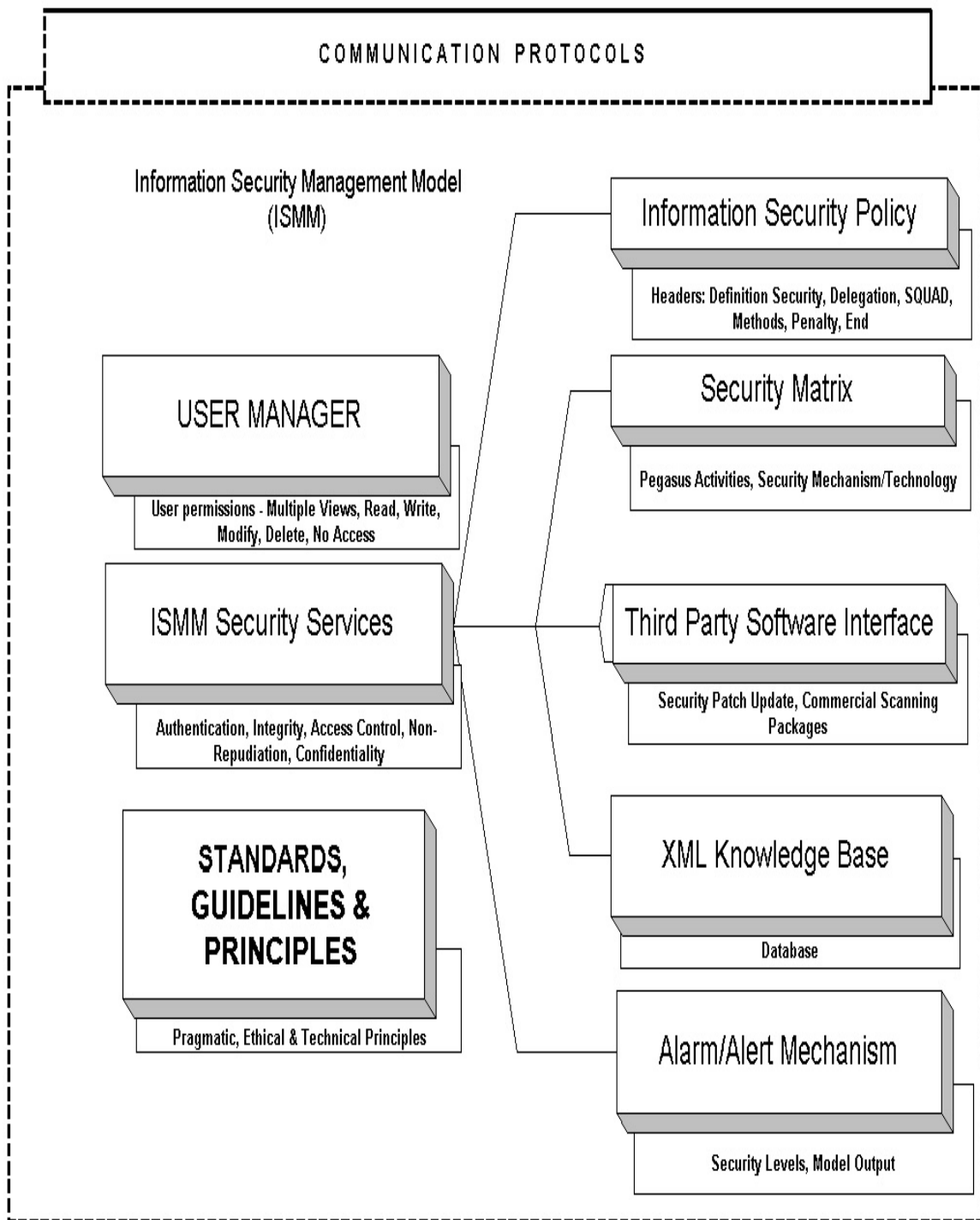


Figure 4-2 Detailed Overview of the Information Security Management Model

#### **4.3.1 The Information Security Policy**

Information security policies act as the foundation for the overall security and protection of information resources. The proposed web-based designer system encompasses information systems. This information is in the form of CAD diagrams, text files etc.

Suitable security measures usually entail investments, both financial and otherwise, at a considerable cost. Most researchers agree that such costs are only justifiable when they are adequately measured against investments, which can be judged in the context of an information security policy.

Resources and information assets need to be adequately appraised in order to acquire a working estimate of their value and quality, both to the organization and to potential hackers.

An information security policy provides a framework within which roles are defined and responsibilities are established with respect to information and data resources. Everyday activities in various organizations are becoming more and more dependent on network communications. Likewise, information security is becoming a shared responsibility of clusters of networks.

The Information Security Policy component of the ISM Model defines permissible behavior for each resource and/or service, by whom and in what circumstances. From a

pragmatic point of view, the security policy should provide the foundational context for a supporting set of guidelines and procedures, which will establish, at a detailed level, how security is implemented for all the information systems concerned. As an overview, the policy simply defines the role information security plays in supporting organizational mission, objectives and goals.

Technical personnel and middle managers usually handle the development of the information security policy. However, the pragmatic hive of the ISM Model also suggests that senior management of the organization need to take on deeper roles and involvement in information security policy development.

The Information Security Policy component of the model has varying levels of detail. However, it is designed to implement the barest minimum detail possible. The information security policy is also reviewed at specified intervals and the framework for this infrastructure provides periodic update alerts as it keeps track of the date and time of the most recent policy update. Nevertheless the policy should be relatively technology-independent, ensuring that once an information security policy has been established, it is implemented for an adequate length of time.

Headers are used in the policy component to segment the framework into definable regions. The Information Security Policy component comprises of the seven (7) headers.

These are *the Definition Header, the Security Header, the Delegation Header, the Methods Header, the SQUAD Header, the Penalty Header and the End Header.*

*(i) The Definition Header:*

This is the reference point of the policy and defines the mission, objectives and goals of the entire information security policy. It also presents a general overview of the most important security issues and other reasons for implementing the policy.

*(ii) The Security Header:*

This header addresses the main security issues of the policy and the organization. It contains the rules, laws and customized algorithms, which must be enforced and implemented. It may be subdivided into subunits for a more definitive impact. For example, subunits could include:

- Policy on Remote Access to Graphical Data
- Policy on User Passwords and User Names
- Policy on Internal Resources
- Policy on Internet Usage
- Policy on Privacy
- Etc.

Policies may also have options, which users may select based on preference. For example:

POLICY 1.

*Option A:* All remote corporate network users must use smart cards, digital signatures and IPsec ESP for authenticated, confidential entry

*Option B:* Users must have a reasonable password and use IPsec

*(iii) The Delegation Header:*

This section of the information security policy contains a statement of the infrastructure and information systems to which the policy applies. It also specifies the stakeholders of the policy. These include all users of the system or more precisely, those who benefit from the security of the information systems.

The Delegation Header also contains a statement of the individual and shared responsibilities of implementing the information security issues, rules and laws stated in the security policy. The personnel involved include head of security departments, heads of information technology departments etc. The individual(s) who directly configure or update the security policy are also specified explicitly.

*(iv) The Methods Header:*

The Methods Header contains step-by-step instructions for carrying out operations involving information security. This is the vehicle through which the policy is implemented. Adequate documentation of procedures and steps provide a good reference point for the staff and security personnel of the organization.

For example, the Methods Header should contain information on acceptable information resource backup procedures. Other procedures include the deletion or deactivation of unused user accounts, defragmentation of hard disks etc.

*(v) The SQUAD Header:*

The SQUAD header provides a contact list of individuals or groups of people who should be contacted incase of security breaches. It also specifies how such people should be contacted.

If need be, different pairs of individuals may be contacted for different kinds of security breaches. This technique will enforce a neutral coverage of all security breaches in the organization.

*(vi) The Penalty Header:*

The Penalty Header contains a statement of actions, which should be taken by the organization as a whole in the event of a breach of security.



When the breach is from inside the organization or is attributed to one or more of the organization's partners, the organization may determine a penalty and enforce it. Breaches from third parties may invoke a different kind of penalty.

Penalties (for security breaches from inside the organization) include suspension, legal prosecution and dismissal. The bluntness and clarity of the information security policy in stating such penalties must not be diluted.

*(vii) The End Header:*

The End Header contains a brief statement signifying the conclusion of the information security policy document. It also contains any other piece of information, which may be vital to information security in the organization.

References may be made in the End Header section of the information security policy, to any other document necessary for the implementation of security. It is essential that the information security policy be practical and realistic.

#### **4.3.2 The Security Matrix**

An adequate information security policy is only the first step to a full security plan. The realization of such policies usually requires a detailed implementation plan. The Security

Matrix provides a referencing mechanism for the security model. Activities within the Pegasus platform are assigned to required security features or levels. Such referencing schemes may be user-configured. This allows for flexibility in the determination of user security preferences. Figure 4-3 depicts an example a security matrix for a select set of activities.















SECURITY MATRIX						
Required Security Features	Source Authentication	Data Encryption	Resource Availability	Non-Repudiation	Access Control	Data Integrity
ACTIVITIES						
Browse Web Site						
Create Project						
Virtual Assembly						
Financial Transactions						

Figure 4-3 A Security Matrix

### 4.3.3 The XML Knowledge Base

XML stands for *Extensible Markup Language*. Its benefits include the following:

- XML supports a wide range of applications
- It is relatively easy to write programs which process XML documents
- XML documents are 'human-legible' and clear
- Searching for data is easy and efficient
- XML extract a Graphics User Interface (GUI) with relative ease
- Complex relationships like tress and inheritance can be communicated
- The code is much more legible: XML is self describing

The XML Knowledge Base is an updateable knowledge database containing security information and history. It analyses various information scenarios and provides, as an output, the best solution to a given query. Its functional design is analogous to that of an expert system, teaching itself by learning from mistakes of the past while incorporating the needs of the future.

The XML database is a *native database* specially designed to store XML documents. It offers support features such as multi-user access and application program interfaces (APIs). The native database defines a (logical) model for an XML document -- as

opposed to the data in that document -- and stores and retrieves documents according to that model.

Native XML databases preserve the document order, processing instructions and comments. This is in contrast to XML-enabled databases. XML-Enabled Databases contain extensions for transferring data between XML documents and themselves. Thus, document-centric documents may be stored using native XML databases. Also, native XML databases support XML query languages, which enable the ISM Model query the knowledgebase for information.

Document-centric documents, in this context, are defined as documents, which a human can read or access and interpret. For example, document-centric documents include newspapers, books, magazines, letters etc

#### **4.3.4 Third Party Software Interface**

Certain third part software is necessary to properly manage information security in the ISM Model. These include:

##### **(a) Security Patch Update Software**

A particularly important aspect of operating a secure system is staying up to date on security patches <sup>[14]</sup>. It is critical to know which patches have been applied to the system

and, more importantly, which have not. For Windows server, Microsoft has a command-line tool called *HFNetChk*, which significantly aids administrators in task of updating security patches.

*HFNetChk* is downloadable from <http://www.microsoft.com/technet> and checks the patch status of all the machines in a network from a central location. The tool does this by referring to an XML database that Microsoft constantly updates.

The XML file contains information such as security bulletin name and title; detailed data about product-specific hot fixes, including files in each hot-fix package, their file versions and their checksums; registry keys that the hot-fix installation package applied; information about which patches supercede other patches; and related Microsoft Knowledge Base article numbers. Tools similar to Microsoft's *HFNetChk* are available for other operating systems.

#### (b) Commercial Scanning Packages

Numerous public domain and commercial scanning packages can check systems and network elements for a large set of known configuration errors and vulnerabilities. They typically scan an IP address or range of IP addresses and then attempt multiple known attacks against the different services available on each device that responds to a probe.

Such scanning software will check for default user accounts and passwords, as well as vulnerability to various IP-based attacks such as teardrop or odd packet fragmentation. However, negative side effects of security assessments include possible host system crashes or odd dysfunctional states in response to determined attacks. Thus, security assessment endeavors should be planned and scheduled properly. Backup data should also be current and readily available. The third party software mentioned above support the Alarm/Alert Mechanism, which is discussed later in this chapter.

Kaufmann et al mention the use of *scans* and *Security Posture Assessments (SPA)* as two ways of assessing the current vulnerability of a network element or infrastructure <sup>[50]</sup>. Security Posture Assessment is also called *Tiger Teaming*. A scan is an automated mechanism to probe network entities for known exploitable services. An SPA is a consultative service that includes a scan as well as other analysis. Some very advanced and expensive SPAs analyze potential human factor operational vulnerabilities, in addition to the normal technical poking and prodding.

#### **4.3.5 ISM Model Security Services**

A *security service* is a software mechanism that implements a certain security function offered by a system. A security service safeguards against one or more threats against security in the system. Most enterprises require an information security solution that provides privacy, integrity and authentication.

The ISM Model security services aim at achieving high management levels of these requirements and these services are: *the Authentication Service, the Access Control Service, the Confidentiality Service, the Integrity Service, the Availability Service, the Non-Repudiation Service and the Trust Service*. The technological hive has a direct impact on these services.

2). *The Authentication Service:*

Authentication is a fundamental building block for security services. This service allows the user prove the authenticity of a stated identity. In a non-electronic world it could be a photo-identification card that is used to authenticate a person. A major loophole for the authentication process is that the network can be eavesdropped allowing an unauthorized person to gain access to private passwords.

The ISM Models determines whether an identified entity has the right or authority to execute a specific service or access a specific piece of information. Its responsibilities include the granting of rights and enforcement the security policy. Figure 4-4 shows a simplified authentication framework.

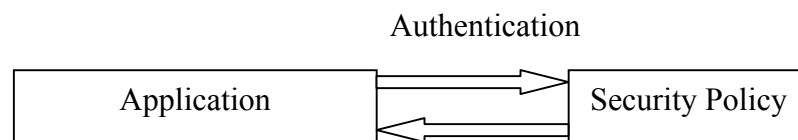


Figure 4-4 A Simple Authentication Framework

Goals of the Authentication Framework include: Ease of design and administration; Enable multi-tiered administration; Build on existing authorization systems; Application independence.

The authentication service uses cryptography to authenticate individual identities and establishes the integrity, origin and recipient of a message or transaction. Cryptographic platforms designed exclusively to support authentication do perform some type of data encryption, but only for information that is essential to the encryption process. In this case, Public Key Cryptography is used in the form of a *Certification Authority (CA)* or *Smart Card*.

A cryptosystem is used in the Authentication Service to define a pair of data transformations. The ordinary data item is referred to as plaintext and the corresponding unintelligible data generated is known as *ciphertext*. The two transformations are called encryption and decryption. An encryption transformation uses the plaintext data as input, along with a random data value known as an encryption key. Similarly, a decryption transformation uses a random decryption key. The Authentication Service may employ either of two types of cryptographic techniques:

a). Symmetric Cryptosystems:

These are characterized by the fact that the same key is used in the encryption and decryption transformations (shown in Figure 4-5). Both parties wishing to communicate



obtain knowledge of the data value to be used as the encryption key. This key is kept secret from all other parties other than the original two parties involved. The U.S. Data Encryption Standard (DES) is the only cryptosystem of this kind, which has, had its full specification published as a public standard.

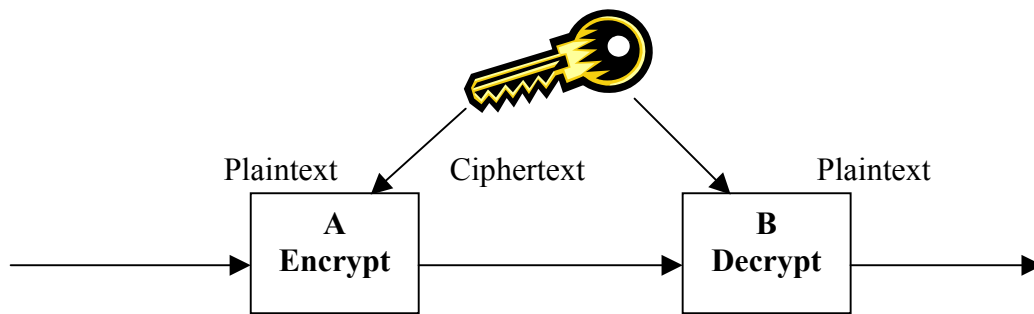


Figure 4-5 A Symmetric Cryptosystem

b). Public Key Cryptosystems: In contrast to symmetric cryptosystems, public key cryptosystems use complementary pairs of keys to separate the functions of encryption and decryption (shown in Figure 4-6, Figure 4-7 and Figure 4-8). Like the key in the symmetric cryptosystem, a private key is also kept secret in the public key cryptosystem. However, the second key is a public key (hence the name, *Public Key Cryptosystem*). The system also has the property that, given knowledge of the public key, the private key cannot be determined.

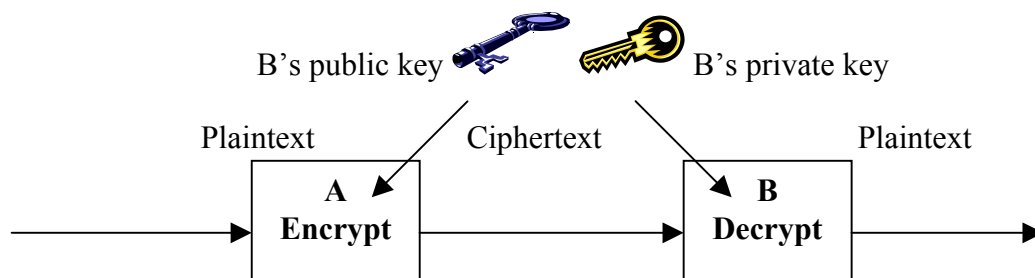


Figure 4-6 A Public-Key Cryptosystem: Encryption Mode

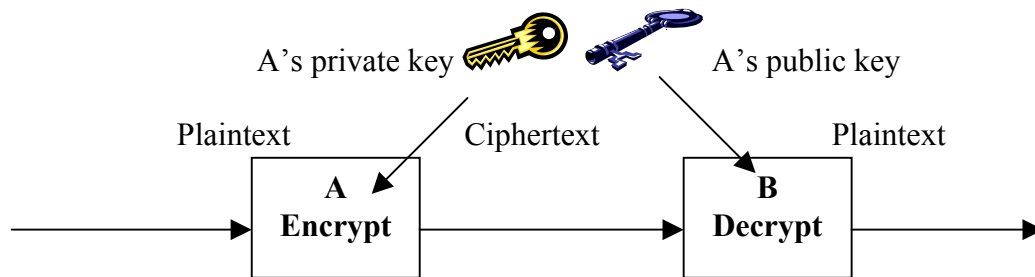


Figure 4-7 Public-Key Cryptosystem: Authentication Mode

Two systems A and B decide that they want to communicate securely.

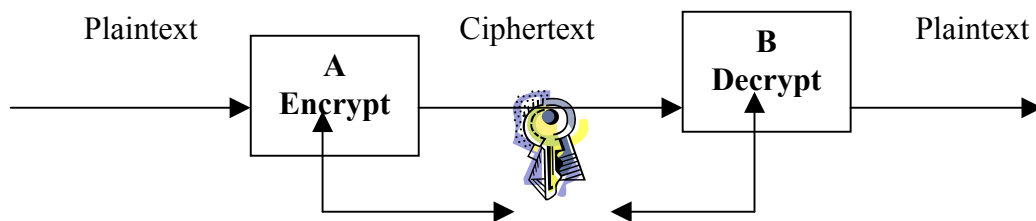


Figure 4-8 Power Key Encryption and Decryption

Ciphertext = Encrypt (Message, Key1)

Message=Decrypt (Ciphertext, Key2)

2). *The Access Control Service:*

This service provides protection against unauthorized access of resources. Locks and keys are access control items in a non-electronic environment. The term *authorization* can be used for this kind of service.

The Access Control Service contributes directly to achieving the goals of confidentiality, integrity, availability and legitimate use. Access control is a means by which authorization is enforced.

Product design documents, as a result of the huge graphics and CAD files, tend to be somewhat large. Hence, there is the need to handle bulk data properly. IPsec ESP handles bulk data encryption. Access rules may be linked directly to the information security policy. For example,

```
IF
Access_Rule(search, directory name, policy_line#)
THEN
SELECT CASE
CASE 1: Do Implementation_1
        CASE 2: Do Implementation_2
        CASE ELSE: Do Implementation_3
END SELECT
ELSEIF
        Access_Rule = New_Access_Rule
        Do Implementation_4
END IF
```

*3). The Confidentiality Service:*

The Confidentiality Service manages the prevention of unauthorized disclosure of information. It aims at protecting information from being exposed or revealed to unauthorized persons. For example, the everyday ordinary envelope is non-electronic way of protecting private information enclosed in it.

*4). The Integrity Service:*

This service acts as a safeguard against the unauthorized creation, alteration or modification of data. A service to protect data from being changed or deleted by unauthorized persons. A watermark in a bank note is a type of data integrity protection.

*5). The Availability Service:*

The Availability Service handles the management of unauthorized information denial prevention. Certain resources and/or services should be available to legitimate users at the right time.

*6). The Non-repudiation Service:*

The Non-repudiation service confirms that an exchange has taken place. With this service one party cannot falsely deny that an exchange has occurred. A non-electronic example is a notarized signature.

The ISM Model manages threats from legitimate users to other legitimate users rather than from unknown persons or hackers. This is done through the non-repudiation management and it provides the availability of irrefutable evidence to support the speedy resolution of disagreements, which may arise from one communicating party's claim that something occurred. The motivation for non-repudiation services arise from the fact that:

*7). The Trust Service:*

Trust is a major problem in worldwide-interconnected computer networks. There is always the question of who to trust. To design a security system there must be some analysis of which environment and what purpose the system has. Is there a third party that can be trusted? Is the system for an organization, a company or is it for interconnected networks with many organizations?

#### **4.3.6 The Alarm/Alert Mechanism**

The ISM Model manages information security and triggers an alert system if the security is breached in any way. The intensity of the alert depends on the level at which security is breached. Although it is necessary to avoid being overly melodramatic, it is important to ascertain the state of the management model at all times. The Alert/Alarm Mechanism

component of the ISM Model is the only formal means of output that the model provides to its the external environment.

As an example, four (4) Security Levels (SL) have been assigned as shown in Figure 4-9. Level 4 implies excellent security conditions, where all security principles, practices, concepts and technologies have been taken into consideration and all activities and recommended information technologies have a perfect match.

The main goal of the management model is to get the Security Level Value (SLV) as close to 100% as possible, without sacrificing performance and efficiency.

Several components of the model determine the SLV. Depending on the setup of the organization, the security personal or management staff will configure the model and apply the corresponding weights to each facet of security that the model manages.

For example, if new third party security patch updates are of optimal importance, then the third party software interface section of the Alarm/Alert Mechanism should carry more weight.

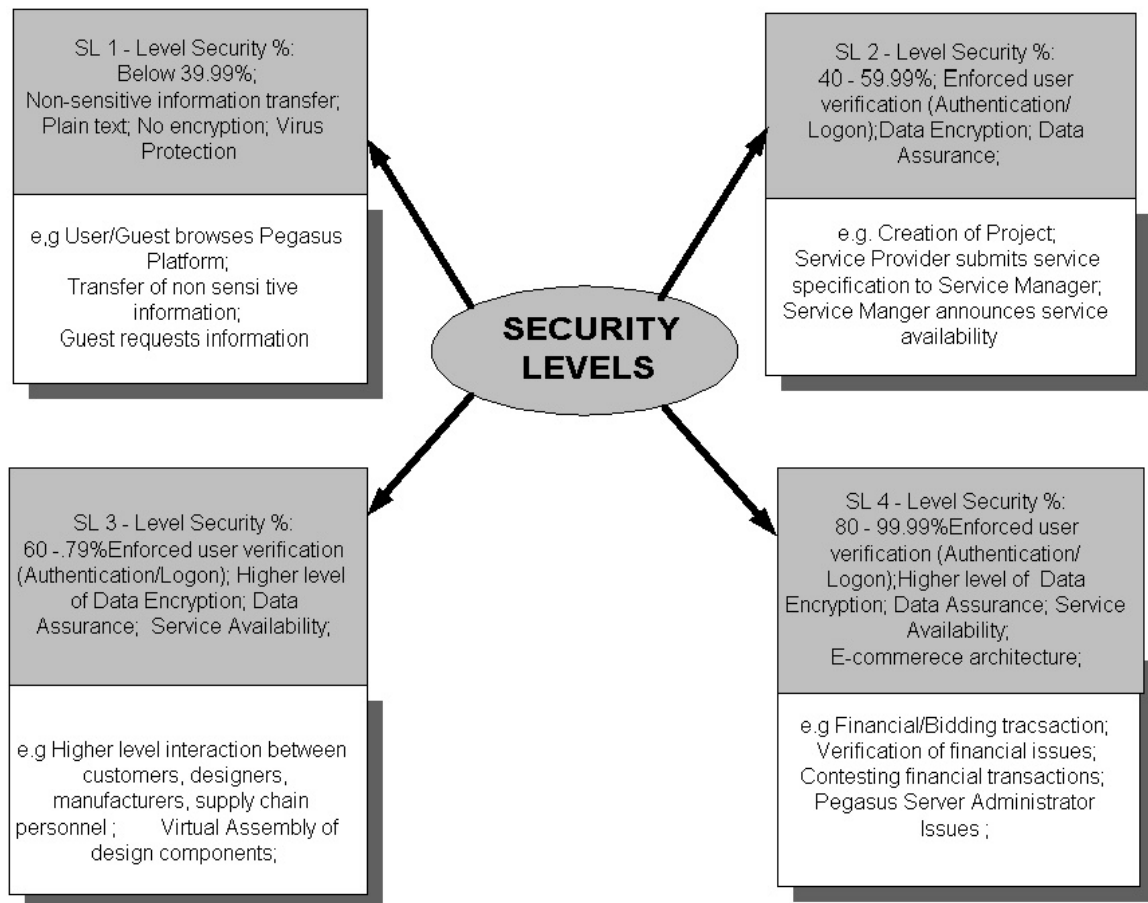


Figure 4-9 Security Levels

**\*\* Percentages were used as an example only.**

Thus, if any delay surfaces during the download of new security patches, the Alarm/Alert SLV will drop drastically, indicating a potential loophole in the security system. Figure 4-10 shows a general overview of the security levels.

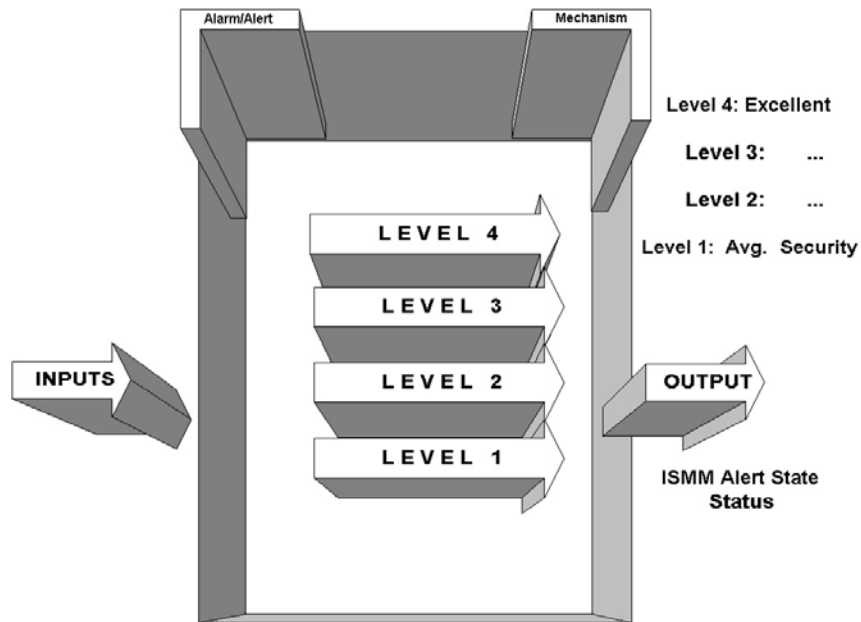


Figure 4-10 General Overview of Security Levels

#### 4.3.7 The Communication Protocols

This component analyzes cryptography, key distribution, and protocol design. So many standards exist in terms of cryptographic algorithms, certificate formats, and protocols. Nevertheless, adequate protocols must be chosen which scale the system to the Internet and allow organizations, which exhibit mutual distrust, to communicate with each other.

The IP Security Protocol (IPSec) provides cryptographic security services and is one of the main protocols employed in the ISM Model. Such cryptographic security services allow for authentication, integrity, access control, and confidentiality.



The Communication Protocols component of the model specifies the mode of connection: Host-to-Host; Host-to-Network (Router); Network (Router)-to-Network (Router);

#### **4.3.8 The Pragmatic, Ethical & Technical Principles' Hives**

The Pragmatic, ethical & Technical principles Hive are the most difficult part to represent in the model. The Pragmatic Principles' Hive entails the use of common sense and laws of reason. The Ethical Principles' hive includes the controversial topic of ethics, which was discussed in Chapter 2. The Technical Principles' Hive includes technological constraints, which play a major role in the Information Security Management Model Security Services.

Extensions of this research will involve an adequate representation language, which will interpret the simplest principle from each hive. Needless to say, the ISM Model may function adequately for a while without the hive component, but these principles are the very foundations upon which the idea of security was first built. Figure 4-11 depicts the hive overview.

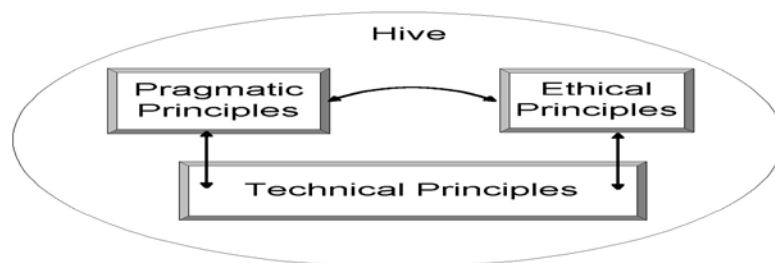


Figure 4-11 Hive Overview

### 4.3.9 The User Manager

The User Manager component of the Model handles user permission and privileges. Permissions are classified into the following categories: Full Control, Read/View, Modify, Write/Add, Download (Service Download) and No Access. These categories are shown in Figure 4-12.

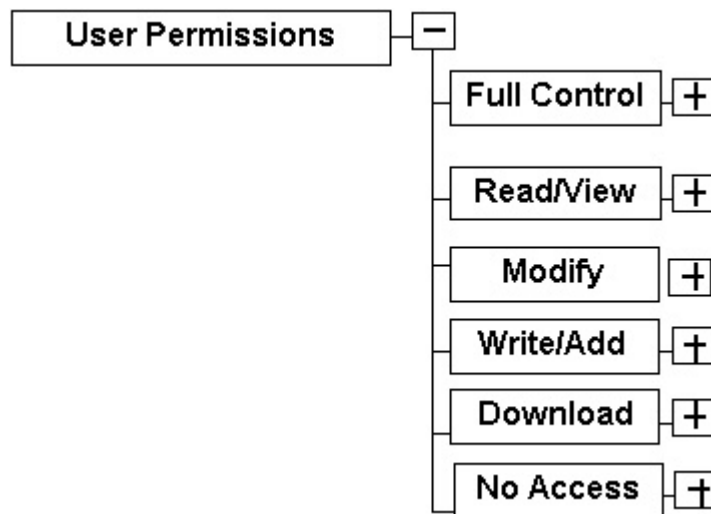


Figure 4-12 User Permissions

Each product design commences with the creation of a *Project*. A *Project* is initiation of a request for product design(s), which results in bidding transaction(s), submission of a detailed design and the eventual manufacture/realization of the product. The User Manager classifies parties or people involved (or to be involved) in a Project as *partners*. In Figure 4-13 and Figure 4-14, user permissions are shown for design and financial transaction activities.

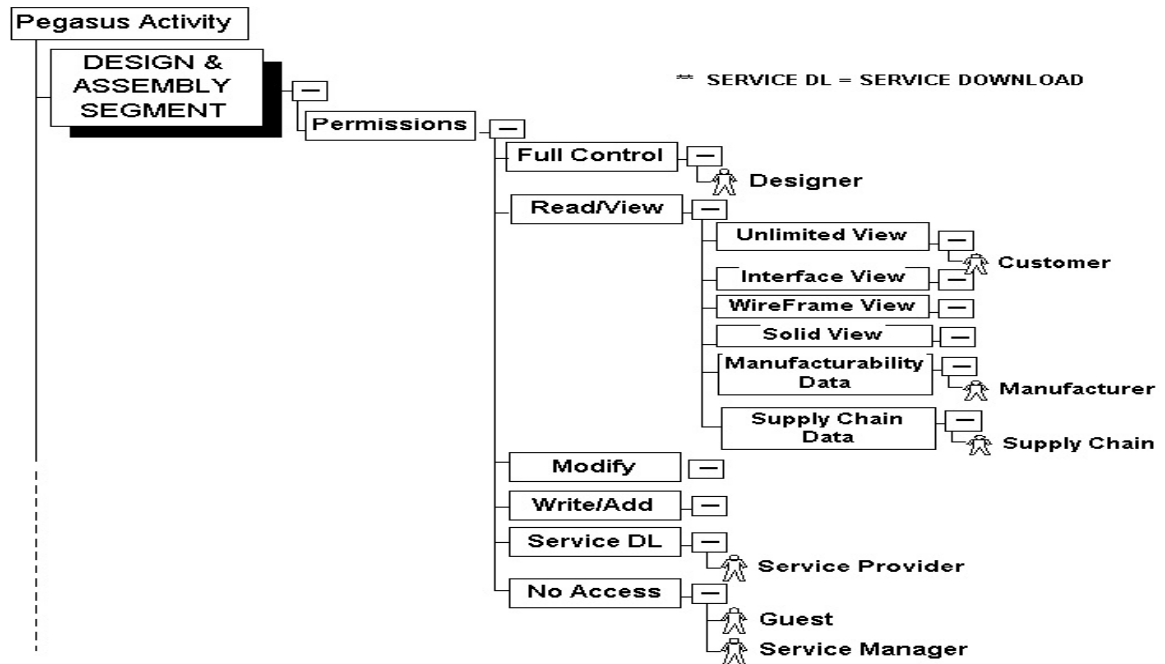


Figure 4-13 User Permissions for Design Activity

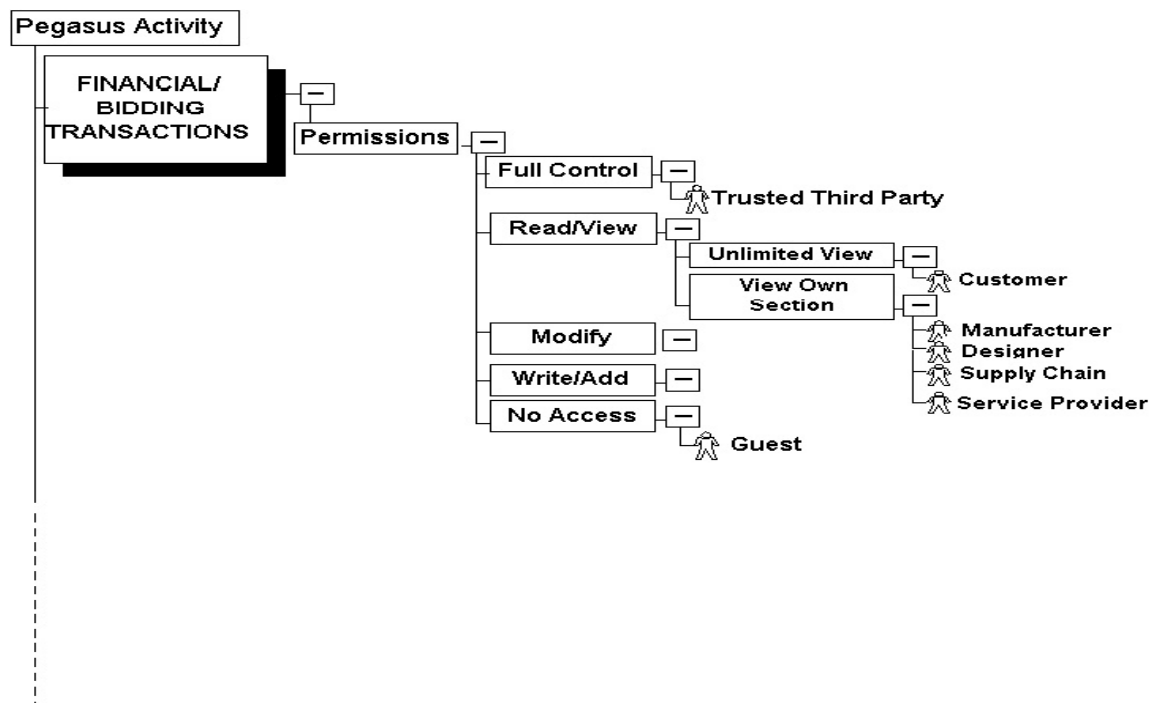


Figure 4-14 Use Permissions for Financial Transaction Activity

## **5.0 MODEL ANALYSIS, VALIDATION AND APPLICATIONS**

The ISM Model aims at establishing/implementing security policies and providing the assurance of successful implementation of such security issues within the Pegasus platform. Specified (required) security parameters are configured into the model via the Security Matrix component. Activities within Pegasus are then referenced by these security parameters. For example, a service customer may specify that security parameters involving source authentication and data encryption are requirements for all activities involving financial/bidding transactions.

### **5.1 General Feasibility of the ISM Model**

The ISM Model is somewhat heuristic in nature. It provides a modular framework consisting of components which will enable the system arrive at a solution for information security issues in e-Product design and realization, whereby flexibility is incorporated into the system in such a way that services customers have a say in security as it relates to their networks and data.

The general feasibility of the ISM Model is enhanced by the modular nature of its components. Each component may be individually developed and tested by different vendors.

A security service or protocol called *Kerberos* is designed to be a trusted third-party authentication service. With such a service, servers handle the authentication of computers in the network. As another example, the Security European System for Applications in Multivendor Environments (SESAME) was a project in the European Commission's RACE (Research and development in Advanced Communication technologies in Europe) programme. *SESAME* is a security architecture that starts from the *Kerberos* protocol and adds to it public-key based authentication, role based access control, delegation of rights and an extensive auditing facility<sup>[51]</sup>.

Sesame builds a system that can have many mechanisms for authentication. Authentication can use both Kerberos authentication and a SESAME specific authentication mechanism that builds on asymmetric cryptography. The SESAME mechanism builds on a role-based view, the user gets a ticket that is based of the kind of work that the user does. The ticket/certificate gives the user those rights that a member of that role group has. Thus, components of the model such as the User Manager or Authentication Service may be developed in a modular fashion and interfaced within the model.

## **5.2 Qualitative Risk Analysis**

Estimated potential loss is used to qualify the risk involved in transactions, which require security. This is by far the most widely used approach in risk analysis. Probability data

may not be required and most qualitative risk analysis methodologies make use of a number of interrelated elements. These elements involved in risk analysis are:

### 1. Threats

These are things that can go wrong or that can 'attack' the system. Examples might include fire or fraud. Threats are usually present for most systems. The most probable threat the security manager will address is the threat of missing or stolen information during data exchange.

### 2. Vulnerabilities

These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire vulnerability would be the presence of inflammable materials (e.g. paper).

For the designer system, vulnerability would be bugs or design limitations in the software, enabling intruders find easy loopholes to create havoc.

### 3. Controls

These are the countermeasures for vulnerabilities. The main control considered in this research include:

- Deterrent controls reduce the likelihood of a deliberate attack

- Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact
- Corrective controls reduce the effect of an attack
- Detective controls discover attacks and trigger preventative or corrective controls.

### **5.3 Limitations of the Model**

This model is only as good as its configuration. In essence, garbage in, garbage out. Also, the Technological, Ethical and Pragmatic Principles' Hive, plays a major role in the foundation of the ISM Model. If this information cannot be adequately represented using some form of representation language, this limits the optimal performance of the model. There is also the question of model compliance with widely accepted standards and guidelines.

Also, XML has certain drawbacks, which have hindered it from gaining widespread use since its inception. The main drawback is the lack of adequate processing applications. At the time of this research and in the current technological market, there are no XML browsers. However, Internet Explorer incorporates XML documents provided HTML (HyperText Markup Language) is the output. So, XML documents need to be converted to HTML before distribution.

## **5.4 Validation of the ISM Model**

Bearing in mind that network security is a marathon, not a sprint, validation of the ISM Model will involve planning in terms of months and years, where focus will be on incremental improvements in security. The proper and complete validation of this framework will be achieved through tests and implementation of the modular components.

However, the model's solid foundation on reality and management principles go a long way in validating its preliminary framework and infrastructure. Extensions to this research aim at confirming this initial research paradigms and building upon this basic framework for information security management in web-based product design and realization.

## **5.5 Benefits & Applications of the ISM Model**

Major information security stakeholders include:

- i) Industry
- ii) Academia
- iii) Government



Users who install web servers for the first time often are not aware that relatively easy help is available for updating a server to protect it against the most common security threats. According to Hernandez et al, hackers can always find a way into a system no matter how secure it is <sup>[11]</sup>. However, users do not need to give hackers or similar individuals, the keys to the front door, by connecting a server to the Internet and not providing appropriate security management mechanisms.

As stated in a previous chapter, Kessler states that the main hurdle to adequate computer and network security is not the security technology, tools and products, but undereducated network administrators, corporate managers and users <sup>[30]</sup>. The ISM Model provides a *security management paradigm*, which shifts major focus from the technical aspects to the administrative aspects of information security.

The ISM Model would alleviate this problem by providing a reference point from which administrators, managers and other users can adequately assess security policy enforcement. Applications of the ISM Model are vast and widespread. Virtually any system in need of adequate computer security management can incorporate the ISM Model in the form of an *Information Security Management Server* or *Information Security Management Module*.

## **6.0 CONCLUSION AND FUTURE WORK**

Security is an important requirement in modern information networks. However, all too often, system security is not considered until the operational requirements have been defined and the system is well into the implementation stage. This chapter presents the conclusion of this research and recommends areas of future work and extensions in the area of information security management in web-based product design and realization.

### **6.1 Conclusion**

An adequate security infrastructure and management scheme is necessary to protect sensitive and proprietary information in any network. Some of the major information security issues presented in this research include: Theft of proprietary information, financial fraud and monetary losses, external system intrusion, unauthorized access by insiders, denial of service attacks, data/network sabotage and virus attacks.

Many computer security breaches occur because internal employees of an organization subvert existing controls. Kessler also reaffirms this fact<sup>[30]</sup>. Security through obscurity is no security. Hence, this research argues that the core root of the information security problem may be more administrative than technical.

An Information Security Management Model (ISM Model) framework was proposed. This model will re-examine, establish and fortify the technical capabilities of the system and manage security from a supervisory point of view. The ISM Model consists of nine (9) components:

- The User Manger, which handle user rights and permissions
- The Information Security Policy, which supports the overall security infrastructure
- The Security Matrix, which references activities with required or specified security services
- The Third Party Interface, which serves as an interface to third party software
- The XML Knowledgebase, which is the ISM Model's database
- The ISM Model Security Services, which support authentication, integrity, access control etc. in the system
- The Communication Protocols, which promote secure communication over media like the Internet
- The Alert/Alarm Mechanism, which serves as the output component to the model

- The Pragmatic, Ethics and Technical Principles' Hive, which serves as the underlying foundation and support for the model.

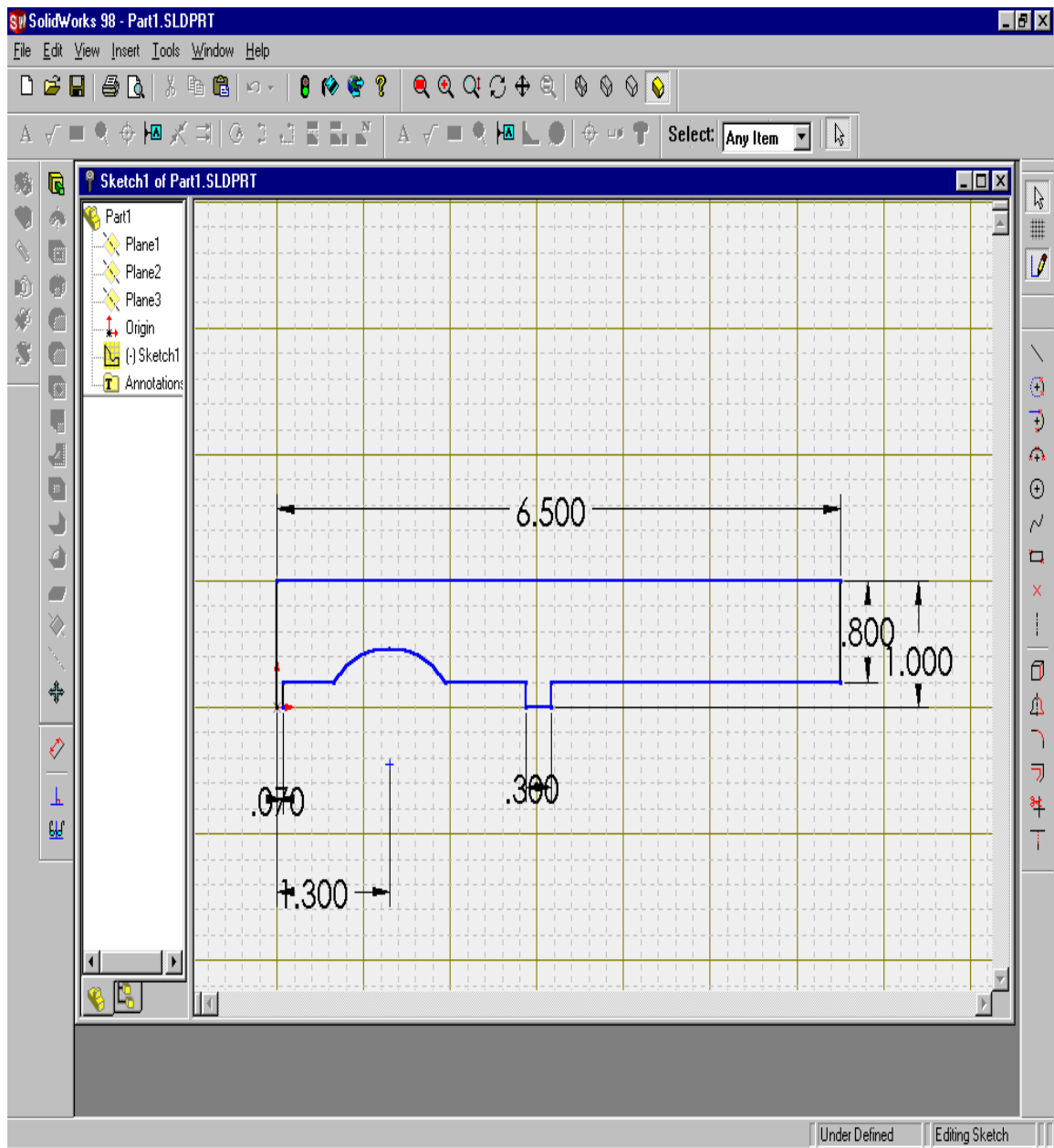
## **6.2 Future Research Extensions**

The challenges of managing information security can be seen in various aspects of personal and business life. For businesses, protection of information is absolutely critical to survival and profitability.

This documentation presented preliminary research issues regarding information management in web-based product design and realization. Evolving technologies give rise to not only new services, but also to new threats. Hence, the framework of the proposed security management model was presented. The main extension of this research is the development and interfacing of the various components within the model with detailed specifications of their complexities and interaction. The interface between the model and the web-based design system also presents an avenue for more research.

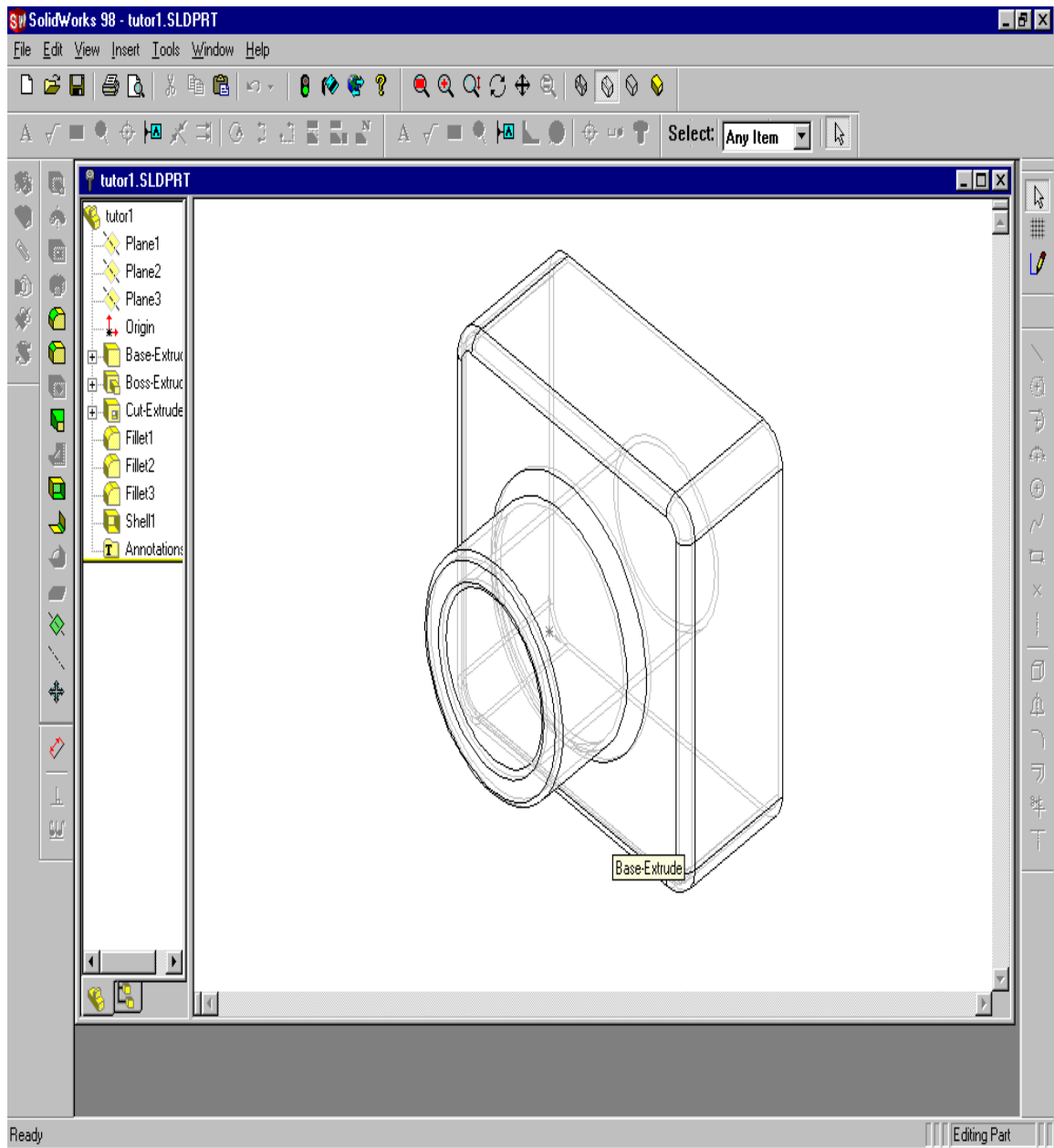
## APPENDIX A

A component represented in a CAD package with specifications



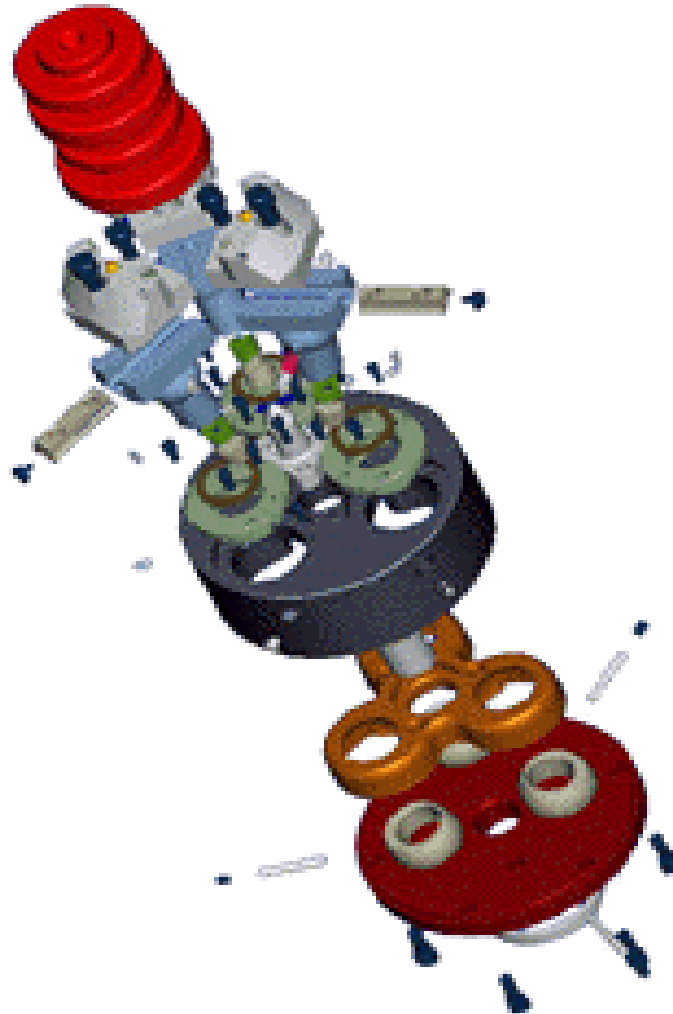
## APPENDIX A

### A component represented as a wire frame



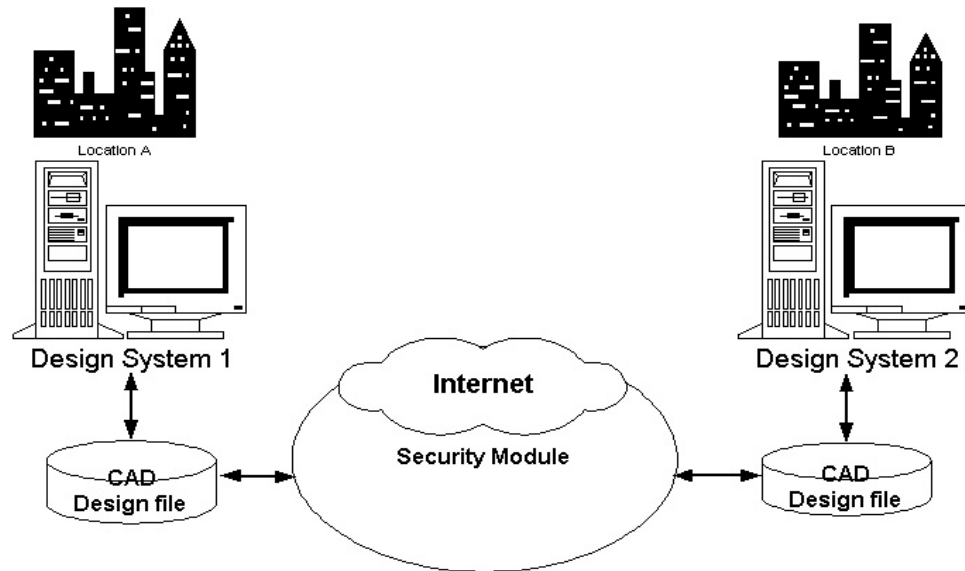
## APPENDIX A

Graphical data: Component assembly.

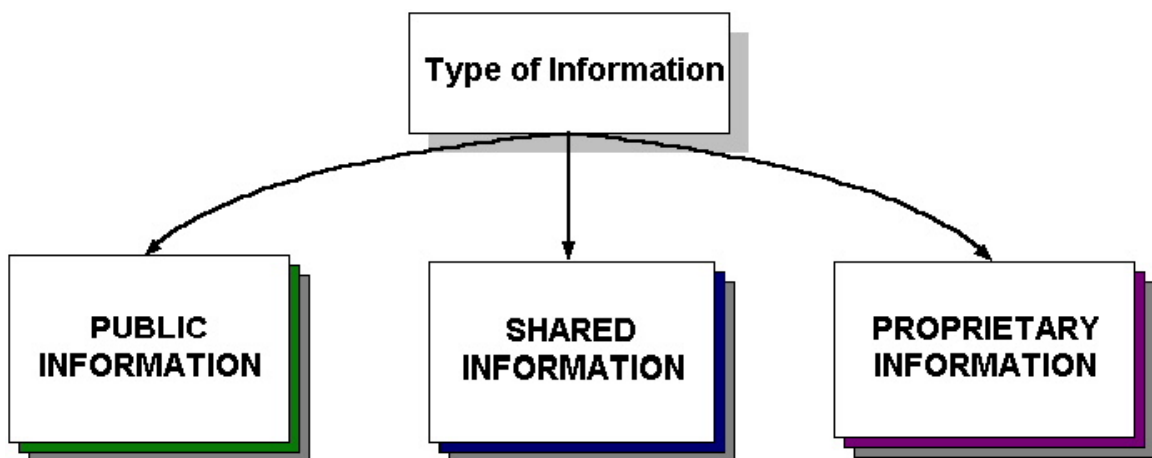


## APPENDIX A

### A Simple Network



### Types of Information





## APPENDIX B

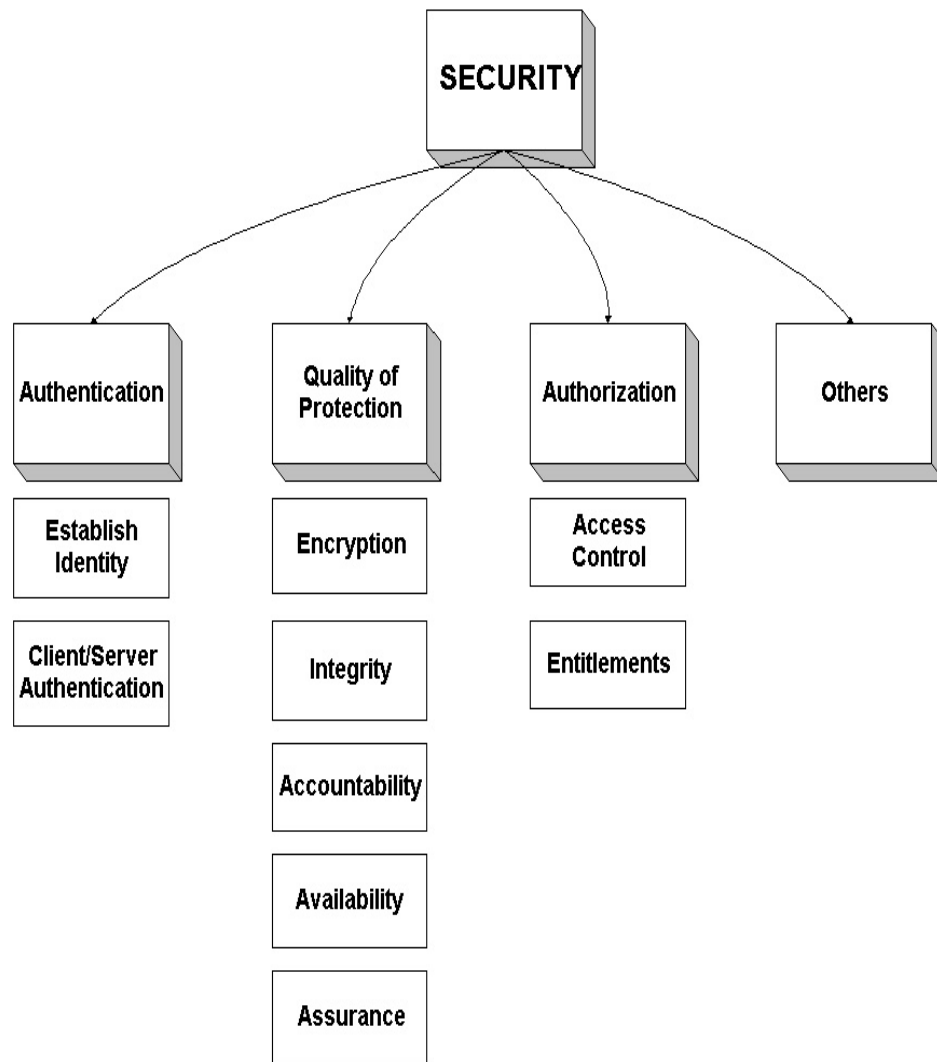
### Summary of some current security technologies

Component	Unique Features	Limitations
Firewall	Hides the corporate intranet from the Internet; Acts as a gatekeeper to give access to valid requests, blocking out all other requests or transmissions; Can be implemented between departments to provide certain users access to secured data; Records all intrusion attempts for future review and identification	Software-only encryption may curtail firewall performance; Presents a single point of failure; No guarantee to protect a network from harm; Must be installed and configured correctly to work properly
User Authentication	Enforces user verification; Can be incorporated within a firewall, application, document or a network OS	Password could be intercepted during transmission; User password could be related to their lifestyle making password identification easier for hackers if they know the habits of the user
Data Encryption	Scrambles the data before transit, making interception attempts futile	Cryptology community believes that point to point tunneling protocol (PPTP) technology may be flawed and unfixable
Key Management	Acts as an electronic key to open encrypted data	User may lose key or have it fall into the wrong hands
Digital Certificate	Verifies the authenticity of the email sender; Alerts the email recipient if the message has been altered	Not very useful if companies do not act as their own certificate authorities or get them from third-party service providers
Intrusion Detection System	Uses static and dynamic methods to spot attacks to the network in progress or over time, respectively	No IDS product can detect all of the attacks on a network when it is heavily loaded; IDS products work only on shared-access segments and not on switched networks
Virus Detection	Protects computers and servers from virus attacks	Useless if virus definitions are not updated on a regular basis
Virtual Private Network	An inexpensive way to connect remote users to an enterprise network; Cheaper than using a dial-	Some VPN products permit use of private addresses, while others require public

	up connection	IP addresses; Flexibility may come at a price; VPN product prices vary according to through-put and number of tunnels supported
Extranet	Provides fast data exchange between a company and its suppliers	Requires security and privacy systems to protect data during transmission

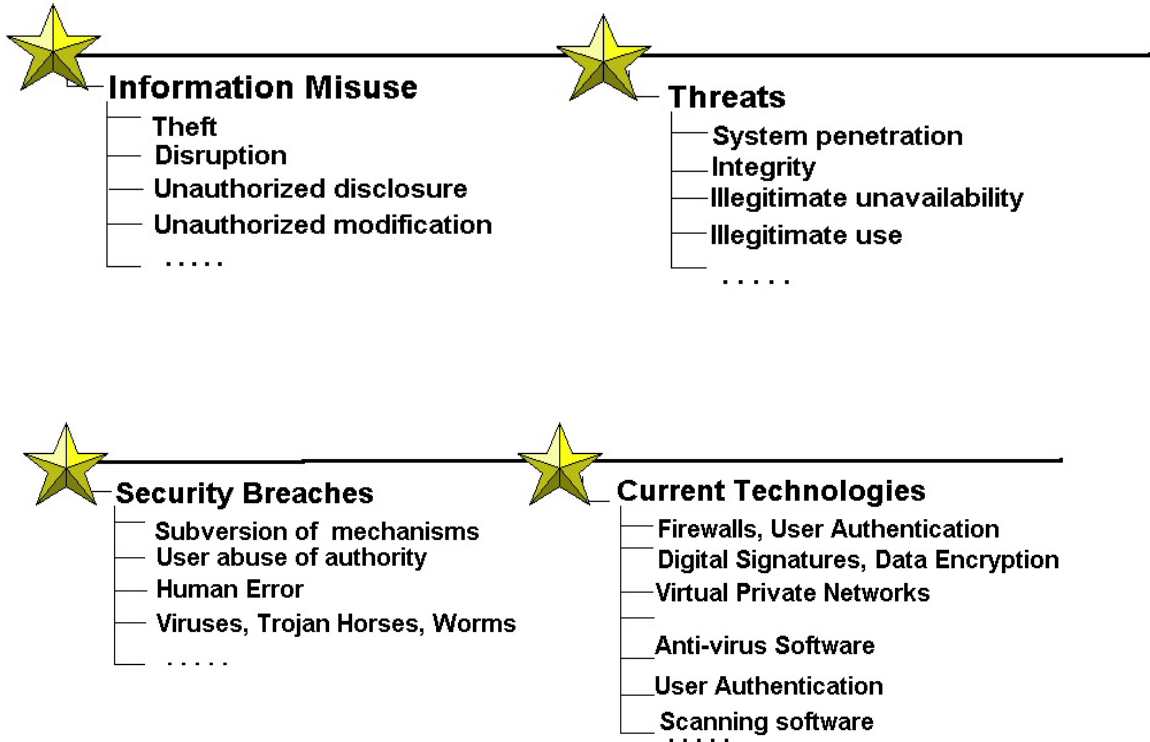
## APPENDIX B

### Facets of Security



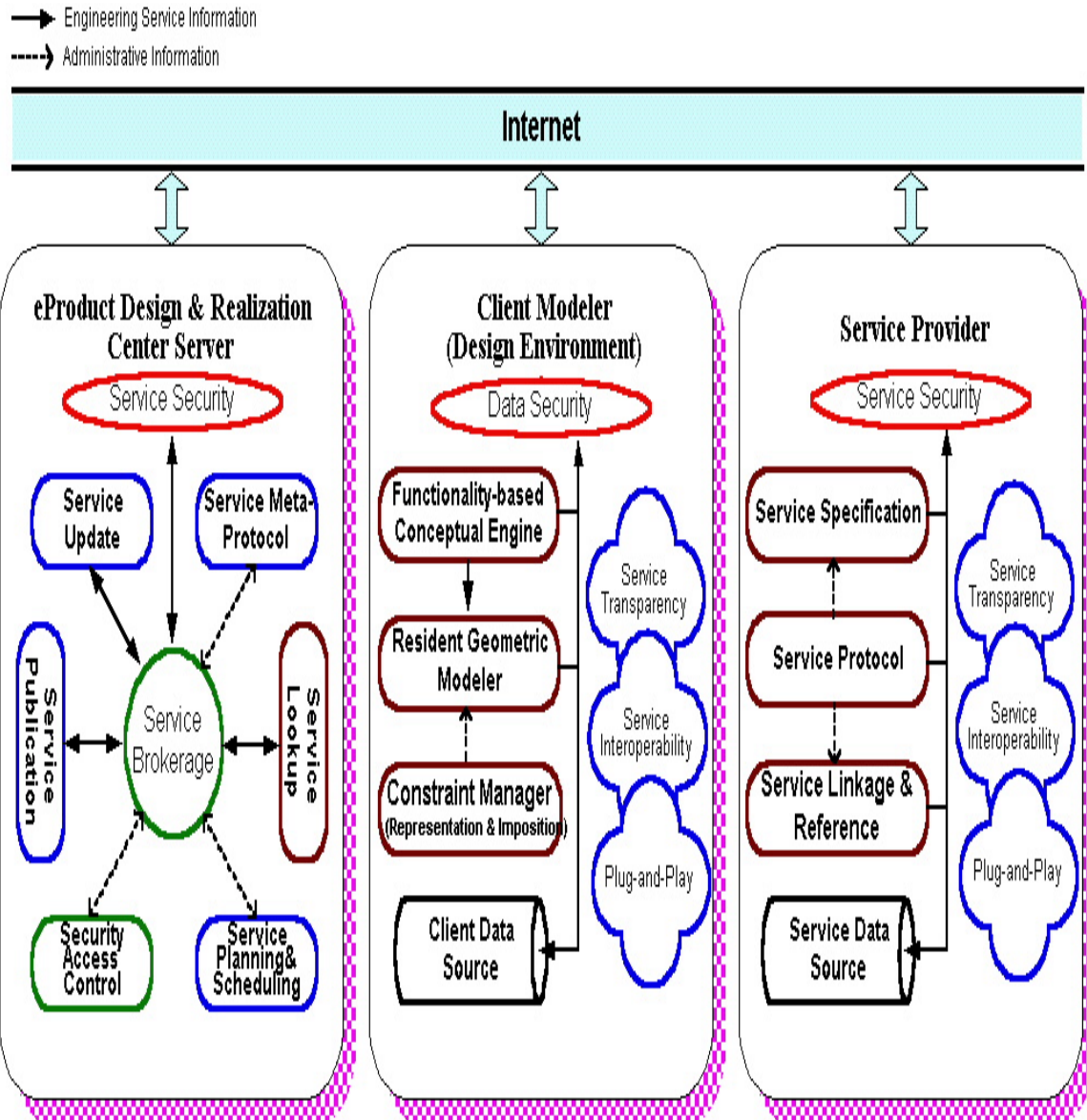
## APPENDIX B

### Short Summary of Security Review



## APPENDIX C

### MODULAR DESCRIPTION OF PEGASUS



## APPENDIX C

### SAMPLE SCENARIOS

\* *Project* - The request for product design(s), which results in bidding transaction(s), submission of a detailed design and the manufacture/realization of the product.

\*\* *Partners* - These are the parties/people involved or to be involved in a Project.

\*\*\* *Partner Status* - This denotes the security level at which customers, designers and manufacturers all agree to communicate with each other.

#### **SCENARIO A:**

##### **Summary:**

Customer starts Project and submits input regarding function/specification of a product comprising of multiple components; various designers design different components; various manufacturers manufacture the different components; Supply Chain team interact with design studio during design.

<b>Pegasus Feature/Activity</b>	<b>System/Security Requirements</b>
Customer initiates Project	User Interface; User Authentication/Logon;
Customer provides function and specifications	Data Entry;
Customer selects designers and manufacturers;  ISM Model determines security status levels of 'partners'  Communication between customer and designers/manufacturers;	Service/Resource Availability; User Authentication/Logon;  Assurance of information security; Determination of "Partner Status" **
Designers generate conceptual design; Manufacturers generate input (as necessary); Supply chain team generate input (as necessary); Customer views project-in-progress; Imposition of constraints &	CAD/3-D Modeler; Data Integrity; Non-repudiation/Data Assurance; Confidentiality/Data Encryption;  Multiple views;

preferences; Ergonomic factors; Design Rules etc.	Access levels;
Bidding/Financial Transactions	E-Commerce Architecture; Third-Party Verification Service; Digital Trust Services e.g. <i>Verisign</i> Data Integrity; Non-repudiation/Data Assurance; Confidentiality/Data Encryption;
Designers produces detailed design; Manufacturers generates input (as necessary); Customer views project-in-progress;	CAD/3-D Modeler; Data Integrity; Non-repudiation/Data Assurance; Confidentiality/Data Encryption; Multiple Views; Access levels/Limited Views
Designers conduct virtual assembly/tests of components viewing only interfaces of assembly;  Customer views assembly results;	CAD/3-D Modeler; Data Integrity; Non-repudiation/Data Assurance; Confidentiality/Data Encryption; Multiple Views; Access levels/Limited Views
Submission of Final Design to Customer/Manufacturers	CAD/3-D Modeler; Data Integrity; Non-repudiation/Data Assurance; Confidentiality/Data Encryption;
Manufacturers commence manufacture of components; Supply chain provide materials; Progress reports;	Non sensitive/Sensitive information transfer; Data Integrity;
Manufacturers register delivery of components to customer; Customer registers acceptance;  End of project;	Sign off on data leaving internal servers; Non-repudiation/Data Assurance; Data Integrity;

### **SCENARIO B:**

#### **Summary:**

Service Customer verifies all financial transactions with Designer and Manufacturer.

<b>Pegasus Feature/Activity</b>	<b>System/Security Requirements</b>
Customer initiates financial transaction verification request;	Data Entry; User Interface; User Authentication/Logon;
Neutral third party verifiers sends financial transaction information to customer;	E-Commerce Architecture; Third-Party Verification Service; Digital Trust Services e.g. <i>Verisign</i> Data Integrity; Non-repudiation/Data Assurance; Confidentiality/Data Encryption;
Customer accepts report/contests report?	Data Entry;
Customer accepts: End of financial verification session;	
Customer contests report; Third Party notifies all parties involved;	Data Entry; Confidentiality/Data Encryption; Non-repudiation/Data Assurance;
Third party resolves conflict;	Data Entry; Confidentiality/Data Encryption; Non-repudiation/Data Assurance;

### **SCENARIO C:**

#### **Summary:**

Designer requests service (Finite Element Analysis Service) from Service Provider (*FEA\_ServiceProvider*) through lookup service from Service Manager.

<b>Pegasus Feature/Activity</b>	<b>System/Security Requirements</b>
FEA* Service Provider sends FEA service publication to Service Manager (Pegasus Center);	Data Entry; User Interface; User Authentication/Logon;
Service Customer performs 'service lookup' via Service Manager;	Data Entry; User Interface;



Service Customer requests FEA Service;	User Authentication/Logon;
Financial Transactions (As necessary)	E-Commerce Architecture; Third-Party Verification Service; Digital Trust Services e.g. <i>Verisign</i> Data Integrity; Non-repudiation/Data Assurance; Confidentiality/Data Encryption;
FEA Service Provider provides Service Customer with FEA service;	Service/Resource Availability; User Authentication/Logon;

\* *FEA* - Finite Element Analysis

#### **SCENARIO D:**

##### **Summary:**

Designer\_A & Designer\_B perform virtual, collaborative product assembly for two components (Component\_A & Component\_B).

<b>Pegasus Feature/Activity</b>	<b>System/Security Requirements</b>
Designer_A requests product assembly session with Designer_B;	User Interface; User Authentication/Logon;
Designer_A specifies allowable 'view' privileges for Designer_B; Designer_B can only view interface of 'assembly interface' area of Component_A;  Designer_B specifies allowable 'view' privileges for Designer_A; Designer_A can only view interface of 'assembly interface' area of Component_B;  Customer has unlimited 'view' access; Customer has limited 'edit' privileges;	User Authentication/Logon;  Privileges/Access Rights (User Manager) categories with ISM Model of Pegasus;
Designer_A & Designer_B perform product assembly;  Customer views project-in-progress;	CAD/3-D Modeler; Data Integrity; Non-repudiation/Data Assurance; Confidentiality/Data Encryption;  Multiple views; Access levels;

### **SCENARIO E:**

#### **Summary:**

Designer requests service (Software License) from Service Provider (Software Vendor) through lookup service from Service Manager.

<b>Pegasus Feature/Activity</b>	<b>System/Security Requirements</b>
Software Service Provider sends license service publication to Service Manager (Pegasus Center);	Data Entry; User Interface; User Authentication/Logon;
Service Customer performs 'service lookup' via Service Manager;  Service Customer requests Software Licensing Service;	Data Entry; User Interface; User Authentication/Logon;
Financial transactions (As necessary)	E-Commerce Architecture; Third-Party Verification Service; Digital Trust Services e.g. <i>Verisign</i> Data Integrity; Non-repudiation/Data Assurance; Confidentiality/Data Encryption;
Software Provider provides Service Customer with software license service;	Service/Resource Availability; User Authentication/Logon;

### **SCENARIO F:**

#### **Summary:**

Designer creates design, specifies customer's choice of material and receives feedback.

<b>Pegasus Feature/Activity</b>	<b>System/Security Requirements</b>
Designer creates design from customers specifications; Submits customer's choice of material specification;	User Authentication/Logon; CAD/3-D Modeler; Data Integrity; Non-repudiation/Data Assurance; Confidentiality/Data Encryption;  Multiple views; Access levels;

Service Manager sends feedback to designer regarding infeasibility of material selection type with product design and specifications;	User Interface; Information transfer;
Designer formally reports status of material choice feedback to customer and provides acceptable alternative material choices;	User Interface; Information transfer;
Customer accepts new material selection choice and provides feedback to designer;	User Interface; Information transfer;

### **SCENARIO G:**

#### **Summary**

Service Provider provides service specification to Service Manager;

<b>Pegasus Feature/Activity</b>	<b>System/Security Requirements</b>
Service Provider sends service publication and availability to Service Manager (Pegasus Center);	User Authentication/Logon; User Interface; Data Entry;
Service Manager performs service update and sends out service publication to clients (customers);	Data Entry; Information transfer;

### **SCENARIO H:**

#### **Summary:**

Service Provider provides service to Service Customer;

<b>Pegasus Feature/Activity</b>	<b>System/Security Requirements</b>
Service Customer looks up a specific service from Service Manager's Internal Lookup Mechanism;	User Authentication/Logon; User Interface;

Service Provider provides customer with service after service lookup;	User Authentication/Logon; User Interface; Internal server auditing regarding customer's privileges, access rights and usage of service;
---	--

### **SCENARIO I:**

#### **Summary:**

Service Manager registers an available service;

<b>Pegasus Feature/Activity</b>	<b>System/Security Requirements</b>
Service Manager receives publication from Service Provider regarding available service;	User Authentication/Logon; Data Entry; User Interface;
Service Manager verifies Service authentication, necessity and availability;	
If in order, Service Manager negotiates financial transactions with Service Provider;	E-Commerce Architecture; Third-Party Verification Service; Digital Trust Services e.g. <i>Verisign</i> Data Integrity; Non-repudiation/Data Assurance; Confidentiality/Data Encryption;
Upon agreement/receipt of financial document(s), Service Manager registers the new service and sends out service publications or announcements to customers (clients);	Data Entry; Information transfer;

## **SCENARIO J:**

### **Summary:**

Service Manager enables material properties availability in databases for design;

<b>Pegasus Feature/Activity</b>	<b>System/Security Requirements</b>
Service Manager receives and verifies new material properties information from some group of designers;	User Authentication/Logon; User Interface; Information transfer;
Service Manager updates materials database;	User Authentication/Logon; User Interface; Data Entry;
Service Manager sends out materials database update/change to clients;	User Interface; Data Entry; Information transfer;

## BIBLIOGRAPHY

- [1] Mullender, Sape; Distributed Systems, 1989, ISBN 0-201-41660-3
- [2] Webster's New College Dictionary; Fourth Edition 1999
- [3] Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) Report 2000
- [4] Dhillon, Gurpreet; Information Security Management: Global Changes in the New Millennium; Idea Group Publishing ISBN 1-878289-78-0; 2001
- [5] Lukasik, Stephen J., "Protecting the Global Information Commons," Telecommunications Policy, Vol. 24 Issues 6-7 (August, 2000), Pg(s) 519-531
- [6] Oppliger, R.; Security at the Internet Layer; Computer Journal, Vol. 1, Issue 9; Sept. 1998; Pg(s). 43 - 47
- [7] The Wall Street Journal, (November 27, 2000), pg. 25
- [8] Solms, Basie Von, "Information Security - The Third Wave?" Computers & Security, Vol. 19 Issue 7 (November, 2000), Pg(s). 615-620
- [9] Stark, Thom; "Protecting your link to the Internet"; LAN Times, June 17, 1996; Pages 36-37
- [10] Power, Richard; 2000 CSI/FBI Computer Crime and Security Survey; Computer Security Journal Volume 16, Issue 2; 2000 Pg(s). 33-49
- [11] Berg, Al; "Hazards of hooking up"; LAN Times, June 17, 1996; Page 35
- [12] Pelaez, C. E.; Bowles, J.; Computer Viruses; Proceedings of the Twenty-Third Southeastern Symposium on System Theory 1991; pg(s) 513-517
- [13] Solms, Basie Von; Corporate Governance and Information Security; Computers & Security; Volume 20, Issue 3; 1 May 2001; Pg(s) 215-218
- [14] Hernandez, J.C.; Sierra, J.M.; Ribagorda, A. and Ramos, B.; "Search engines as a security threat ", Computer Journal, Volume: 34 Issue: 10, Oct 2001 Pg(s): 25-30
- [15] Casavant, T.L.; McWilliam, B. M.; Safe Computing; IEEE Potentials; Vol. 8, Issue 3; Oct. 1989; Pg(s) 29-31

- [16] Bontchev, Vesselin. Future Trends in Virus Writing. Proceedings, 6th Annual Virus Bulletin Conference. Jersey. 1994
- [17] Gordon 1995 Gordon, Sarah; Internet 101; Computers & Security Journal, Vol 14 Issue 7 1995; Pg(s) 599-604
- [18] Subramanya, S.R.; Lakshminarasimhan, N.; Computer viruses; IEEE Potentials, Volume: 20 Issue: 4 , Oct.-Nov. 2001 Pg(s): 16 -19
- [19] Heisel, M.; Pfitzmann, A.; Santen, T.; Confidentiality-preserving Refinement; Computer Security Foundations Workshop, 2001. Proceedings. 14th IEEE , 2001 Pg(s): 295 -305
- [20] Clipsham, Phil; Teaching Information Integrity - An Ethical Approach; ETHICOMP 1998
- [21] Montrose Bruce and Froscher, Judith N.; Tools for Information Security Assurance Arguments; Center for High Assurance Computer Systems; IEEE 2001; pg 287
- [22] Finne, Thomas; "The Information Security Chain in a Company"; Computers & Security Journal; Vol. 15 (1996); Pages 297-316
- [23] Hancock, William; "Network Security"; Computers & Security; June 1994
- [24] Molva, Refik; Internet Security Architecture; Journal of Computer Networks Vol. 31 (1999) Pg(s) 787-804
- [25] Anderson, Ross J.; "Why cryptosystems fail", Communications of the ACM, Volume 37, Issue 11, November 1994, Pg(s) 32-40
- [26] Hancock, Bill; "Security Views"; Computers & Security Journal; Vol. 20, 2001; Pages 188-201
- [27] Barruffi, R.; Milano, M. and Montanari, R., "Planning for security management", IEEE Intelligent Systems [see also IEEE Expert] , Volume: 16 Issue: 1 , Jan.-Feb. 2001 Pg(s): 74 -80
- [28] McHugh, John; Christie, Alan; Allen, Julia; Defending yourself: The role of intrusion detection systems, IEEE Software, Volume 17, Issue 5, September 2000, Pg(s) 42-51
- [29] Steinke, Gerhard and Leamon, Ronald; Information Security Issues facing Virtual Enterprises; IEEE 1996 pg. 641

- [30] Wood, Charles Cresson; "A policy for sending secret information over communications networks; Information Management & Computer Security; Vol. 4, No. 3, 1996, Pages 18-19
- [31] Forcht, Karen and Wex, Rolf-Ascan; "Doing business on the Internet: Marketing and Security Aspects"; Information Management and Computer Security; Vol.4, No. 4, 1996 Pages 3-9
- [32] Anthes, Gary; "In the 'Net We Trust"; Computerworld, July 29, Pages 59-61
- [33] Kyamakya, K.; Jobman, K. and Meincke, M., "Security and survivability of distributed systems: An Overview", MILCOM 2000. 21st Century Military Communications Conference Proceedings, Volume: 1, 2000 Pg(s): 449 -454
- [34] Duan, Haixin and Wu, Jianping; Security Management for Large Computer Networks; Network Research Center of Tsinghua University 2000
- [35] Beker, Henry; "The New Information Security Age – Electronic Commerce & Trusted Third Parties"; Computers & Security; Vol.15, No. 5, 1996
- [36] Solms, Basie Von and Solms, Von Rossouw; "Incremental Information Security Certification"; Computers & Security Journal; Vol. 20, 2001; Pages 308-310
- [37] Eloff, M.M. and S. H. Von Solms; "Information Security Mnagement: A Hierarchical Framework for Various Approaches"; Computers & Security Journal; Vol. 19, 2000; Pages 243-256
- [38] Leiwo, J. and Heikkuri, S.; An analysis of ethics as foundation of information security in distributed systems System Sciences, 1998., Proceedings of the Thirty-First Hawaii International Conference on , Volume: 6 , 1998 Pg(s): 213 -222
- [39] Lindsay, D., An overview of leading security issues - 1993
- [40] Walker, S.T.; "Network Security Overview"; Proceedings of the IEEE Symposium 1999 pg(s). 62-76
- [41] Ford, Warwick; Computer Communications Security: Principles, Standard Protocols and Techniques 1994; ISBN 0-13-799453-2
- [42] Nosworthy, Julie; "Implementing Information Security in the 21<sup>st</sup> Century – Do You Have the Balancing Factors?"; Computers & Security Journal; Vol. 19 , 2000; Pages 337-347
- [43] Kessler, G. C; Nontechnical hurdles to implementing effective security policies; IT Professional, Volume: 3 Issue: 2 , March-April 2001 Pg(s): 49-52



- [44] Blumental, Marjory S., "Reliable and Trustworthy: The Challenge of Cyber-Infrastructure Protection at the Edge of the Millennium"
- [45] Zhang, Yufang and Xiong, Zhongyang; Proceedings of the Fourth International Conference/Exhibition, May, 2000, "An MIS security strategy based on client/server architecture: High Performance Computing in the Asia-Pacific Region" pg(s). 676 - 677
- [46] Gollmann, D., "E-Commerce Security," Computing & Control Engineering Journal, Vol. 11 Issue: 3 (June, 2000)
- [47] Kim, Kyeongbeom, Kim, Youngkyun; Youngkee Song; Soran Ine, "A software platform for secure applications based on CORBA", Distributed Computing Systems, 1997., Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends ; 1997 Page(s): 22 -27
- [48] Raman, L.; OSI Systems and Network Management; IEEE Communications Magazine, Vol. 36 Issue: 3 , March 1998 Page(s): 46 -53
- [49] Wood, Charles Cresson and Karen Snow; "ISO 9000 and Information Security"; Computers & Security Journal; Vol. 14 (1995); Pages 287-288
- [50] Kaufman, Elizabeth and Newman, Andrew; Implementing Ipsec: Making Security Work on VPNs, Intranet and Extranets; 1999 ISBN 0-471-344672
- [51] Ashely, Paul; Rutherford, Mark; Vandenwauver, Mark; Boving-Sebastian; "Using SESAME's GSS-API to add security to Unix applications"; Proceedings-of-the-Workshop-on-Enabling-Technologies:-Infrastructure-for-Collaborative-Enterprises,-WET-ICE. 1998, IEEE Comp Soc, Los Alamitos, CA, Pages(s) 359-364