# AN APPROACH FOR DEFENSIVE INFORMATION WARFARE IN THE TURKISH LAND FORCES COMMAND

**A THESIS SUBMITTED TO**
**THE INFORMATICS INSTITUTE**
**OF**
**MIDDLE EAST TECHNICAL UNIVERSITY**

**BY**

**FUZULİ ÖZCAN**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE**
**IN**
**INFORMATION SYSTEMS PROGRAM**

**AUGUST 2002**

Approval of the Informatics Institute

_____

Prof. Dr. Neşe Yalabık

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Prof. Dr. Semih Bilgen

Head Of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Prof. Dr. Semih Bilgen

Supervisor

Examining Committee Members

Prof. Dr. Semih Bilgen _____

Assoc. Prof. Dr. Onur Demirörs _____

Assoc. Prof. Dr. A.Kadir Varoğlu _____

Assoc. Prof. Dr. Elif Demirörs _____

A. Nusret Güçlü _____

# ABSTRACT


**AN APPROACH FOR DEFENSIVE INFORMATION WARFARE IN THE TURKISH LAND FORCES COMMAND**

Özcan, Fuzuli

M.S., Information Systems Program
Supervisor: Prof. Dr. Semih Bilgen

August 2002, 71 pages

In this study, Information Warfare (IW) and Information System (IS) security concept in the Turkish Land Forces Command (TLFC) are investigated. An approach that will enhance the success for a secure Information System to alleviate experienced risks is proposed. Starting with the general overview of the literature about IW and IS security, the relation between the concepts, the future, advantages and disadvantages of security development approaches, and the requirements for security are reviewed. Then the specific problems, security risks and IW threats of the TLFC are considered. After reviewing the specific problems, a proposal for IS security in Defensive Information Warfare process in the TLFC is presented and partially applied. The proposal is evaluated within the framework of a case study. The stronger points of the proposal are reviewed by comparing the proposed approach with some other approaches actually applied.



Keywords: Information Warfare, IS Security, IS Security Engineering, TLFC

# ÖZ

## KARA KUVVETLERİ KOMUTANLIĞI'NDA SAVUNMA BİLGİ HARBİ İÇİN BİR YAKLAŞIM

Özcan, Fuzuli

Yüksek Lisans, Bilişim Sistemleri Programı
Tez Yöneticisi: Prof. Dr. Semih Bilgen

Ağustos 2002, 71 sayfa

Bu çalışmada Türk Kara Kuvvetleri Komutanlığı'nda bilgi harbi ve bilgi sistemleri güvenliği konuları incelenmiştir. Yaşanmış riskleri azaltmak için Bilgi Sistemleri güvenliğini arttıracak bir yaklaşım önerilmiştir. Bilgi harbi ve Bilişim sistemleri güvenliği literatürüne genel bir bakışla, kavramların ilişkisi, farklı sistem güvenliği geliştirme süreçlerinin iyi ve kötü yönleri, bilgi güvenliğin özellikleri ve geleceği tartışılmıştır. Daha sonra Kara Kuvvetleri'nin özel problemleri ve Bilgi Harbi ve Bilişim Sistemleri güvenliği tehditleri ele alınmıştır. Özel problemlerin ele alınmasını müteakip Kara Kuvvetleri savunma bilgi harbinde güvenlik sistemi geliştirilmesine ait bir süreç önerilmiş ve kısmen uygulanmıştır. Uygulamanın doğruluk ve güvenirliliği örnek çalışması ile değerlendirilmiş ve önerinin avantajları, önerilen yaklaşım ile gerçekte uygulanan gelişigüzel yaklaşımlar karşılaştırılarak incelenmiştir.

Anahtar sözcükler: Bilgi Harbi, Bilgi Sistemleri (BS) Güvenliği, BS Güvenlik Mühendisliği, KKK

# ACKNOWLEDGMENTS

I would like to thank all of the instructors in Informatics Institute of Middle East Technical University. I would like to give my great appreciation for Dr. Onur Demirörs, Dr. Elif Demirörs and A.Nusret Güçlü in giving fundamental knowledge about Information Systems.

I am grateful to Dr. Semih Bilgen who was so helpful and precious during my thesis and was generous in sharing his great knowledge with me.

Of course I dedicate this study to my son Yiğitalp and my wife Süheyla whom I somemites have not cared much during my studies.

# TABLE OF CONTENTS

# LIST OF FIGURES AND TABLES

## ACRONYMS AND ABBREVIATIONS

C2: Command and Control

CIIS: Common Integrated Intelligence System

DIW. Defensive Information Warfare

IS: Information Systems

ISD: Information Systems Department

ISP: Internet Service Provider

IT: Information Technology

IW: Information Warfare

IWS: Information Warfare Squadron

MLS: Multi Level Security

NSA: National Security Agency

SSECMM: System Security Engineering Capability Maturity Model

TLFC: Turkish Land Forces Command

TLFCISD: Turkish Land Forces Command Information Systems Department

TCSEC: Trusted Computer Security Evaluation Criteria

TCB: Trusted Computing Base

# CHAPTER 1

## 1 INTRODUCTION

Information Warfare (IW) is one of the direct results of the great changes in Information and Communication technology. While this technology has helped daily life in many areas, it also constraints and confuses life in many ways. Organizational boundaries are not strict after computer networks and it is concluded that those boundaries are violated on the side of users too. [Laudon1998] Those consequences have made the security concept in Information Systems a vital issue. Information Security (IS) has evolved and also has modified some other concepts like warfare in the Armies and developed new domains like IW [RAND1997].

IW can easily be summarized as using information and information system to gain information and to have superiority against the potential or current hostiles and enemies and at the same time to prevent any other side from doing the same to our systems. [Libicki1995] This definition proposes two concepts at the same time, offensive side of IW and inevitable defensive side of IW. During this study defense side of IW namely Defensive Information Warfare (DIW) will be reviewed. This does not necessarily mean that other form of IW is not possible for TLFC. Nonetheless the point is that regardless of the country, organization and technology DIW is a reality if anyone uses Information Technology in its business processes. To use information and communication technology means to accept its vulnerabilities and threats along with its advantages.

IW is a reality that enforces the governments and Armies to take extraordinary steps to prevent its threats and to use its advantages if possible. A new institution like National Information Security Organization is

under planning to regulate information security.[1] It is aimed that this organization will oversee public information, classify it and regulate access control to that information in the country.

IW is not the reality or the problem just for Armed Forces or Land Forces. It is the problem of any organization that uses IT in its business organization and also for individuals who are utilizing information and communication systems. [Denning2000] Keeping this fact in mind, the approach that will be developed in the thesis and the application will be based on TLFC. Namely the effects, future, threats and measures for IW in TLFC will be considered in this study. Since the domain of the study is focused especially on DIW, while reviewing IW in Turkish Land Forces Command and Units, a proposal for DIW and IS security will be developed.

In this study, Turkish Land Forces Command (TLFC) is chosen as a sample unit to be investigated in terms of Information Security and IW. Even though its one level upper organization Turkish General Staff has an information system department under J6 department, TLFC has also Information System Department (ISD) to execute the IS functions. With its changing vision this department is responsible from development, acquisition, regulating and coordinating IS functions of TLFC and its lower units and headquarters. From this perspective TLFCISD is also responsible from securing IS projects both the ones that are developed and the ones that are outsourced in some way. But all the departments are also responsible from using the information systems securely and coordinate the security issues of their Information System with TLFCISD. As for IW we must say that responsibility is both in ISD and both in Intelligence (J2) and Operation (J3) department of TLFC. In this approach it will be discussed mainly how an IS project that will be acquired could be secured for IW.

[1] http://www.milliyet.com.tr/

TLFC naturally has some problems in security of IS projects, like most of the other organizations in Turkey and in the world. Some of these problems are in the essence of software engineering and project development. These problems are usually due to unawareness and underestimation of security issue. Other part of the problems is usually due to deficiencies in the projects like unqualified human resources, unqualified suppliers, budget and planning problems.

***The objective of this thesis*** is to investigate specific IS security and IW problems in the TLFC and to propose a standard approach to alleviate experienced problems and risks. Increasing awareness for the concept especially for IW is one of the objectives of the thesis. If realized an application to practice multilevel security in a project will be the beginning for the design of secure information systems. Besides, this definition of an approach will help to describe the way for securing information systems in the context of DIW.

***The scope of this thesis*** is restricted to the analysis and design steps of the IS security engineering. Nonetheless the security and IW concepts will be handled in every aspect. The risk and threat management and assurance phase is left out of the scope of this thesis.

A general literature review of IW will be presented in Chapter 2. The definition, forms, reasons for the future of IW, the risks, advantages, and disadvantages of IW will be reviewed. The past incidents and examples regarding military and public sector organizations will be presented then. Those incidents reveal the threats, risks and consequences of them precisely. At the end of the chapter the reality and threats for TLFC will be considered.

In Chapter 3, beginning with the basic concepts of security, general risks threats on security of the TLFC will be reviewed according to RFC2828 [RFC2828]. In this chapter a general description of a secure system will be defined then the consequences that disrupt the security in the system will be stated. Security engineering process will be considered and the advantages

and disadvantages of different processes will be reviewed. At the end, a comparative table for different processes will be given.

An application of security requirements specification and design will be presented according to Waltz approach [Waltz1998] in Chapter 4. A security process for an intelligence system will be proposed. [KEISIAM][KEISMPL] Proposed security process will be applied partially for this system, since intelligence function is very important in conducting both offensive and defensive IW. A security policy, security policy requirements, access control and authorization models of the system will be specified according to Multi Level Security principles. [Sandhu1994]

A case study of the proposal will be considered in Chapter 5. Current projects of the TLFC are chosen for the case study. The names of the people and organizations will not be used for the sake of secrecy and protecting the privacy of the project's contributors. Instead of that, the roles and responsibilities are defined and renamed for the case study. First, the systems to be studied are identified. Then the answer to the question: " what would have been if some other security policy, model and mechanisms were dictated by the requirements for specific services" is reviewed by comparing and evaluating the process and the activities in the projects with the proposed approach. At the end, a comparison of the proposed process with the actually applied ad-hoc approach is presented.

Chapter 6 will present the conclusions of the thesis. The achievements and the deficiencies of this thesis will be reviewed. At the end, possible future works, that are not covered, will be presented [Pressman2000][SSE-CMM1999]. In future work, recommendations in or beyond the scope of this thesis will be given to reveal the possible optimum security architecture in the TLFC to be used in IS projects.

# CHAPTER 2

# 2 Information Warfare Concept

## 2.1 What Do We Mean by Information Warfare (IW)?

The term IW is certainly the combination of two words hence an analysis of the words, information and warfare, must be made at the beginning. The exact meanings of two words will reveal the media in which IW rests and it will be the starting point for understanding IW.

Information is “data that have been shaped into a form that is meaningful and useful to human beings.” [Loudon1998] Information is the processed data or processed raw facts that are ready and meaningful for the use of human beings. The perception and the aim of the person who gets information are crucial at that point. U.S Department of Defense Dictionary of Military Terms describes information as “facts, data, or instructions in any medium or form.” and as “the meaning that a human assigns to data by means of the known conventions used in their representation."[2] U.S. Army defines information as “in intelligence usage, unevaluated material of every description that may be used in the production of intelligence.”[FM34-1] Then from a military point of view information is firstly; *a message or data from the head to the neck or vice versa*, secondly; information is the *actions, material or resources to obtain intelligence*, thirdly; in complex rifle systems or in systems with embedded software, *information is also the medium and the coherent part of a system*. As for the warfare “the set of all lethal and non-lethal activities undertaken to subdue the hostile will of an adversary or

[2] http://www.enolagaia.com/IWGlossary.html

enemy." [3] It is obvious that warfare is distinct from war: “an event characterized by the open, total, and relatively unrestricted prosecution of warfare by lethal means.” [Waltz1998] Warfare does not require a declaration of war; therefore in warfare there is no need for the existence of a condition widely recognized as a state of war. “In warfare, the warring parties perceive each other’s objectives as mutually exclusive and apply force and other means to achieve their own victory. IW emphasizes the operations that apply the other means.” [Waltz1998] IW might be conducted outside the situational frame of war. IW operations have been applied intensively during wartimes; nevertheless they could be used in peacetime too. Since rivalry and competition is high in contemporary world policy, the governments and organizations begin their IW operations in peacetime in order to conduct them successfully on war. At that point the question “In what way wars and conflicts were changed and how will they be possibly conducted in the future? ” is a vital question must be answered explicitly to understand IW.

The concept of war has not changed; only the means and speed of acquiring and transmitting valuable information have changed. The principles of war that a commander must ask to himself during a war have not changed. All the developments and advancements in information technologies (IT) developments have helped the commander answer following questions easily and correctly for the use in the battlefield:

- “What is my mission?
- What is the enemy doing?
- How can I keep him from knowing what I am doing and lead him to believe I am doing something else?
- Where am I vulnerable and does the enemy know?
- Where is the enemy vulnerable and how can I exploit it and win at least cost to my soldiers.” [Franks1994]

---

[3] Richard Szafranski, *A Theory of Information Warfare*, Preparing for 2020, http://www.airpower.maxwell.af.mil/airchronicles

The above needs for information are clear for the battlefield in fact they were clear from the days of Sun Tzu "The way to avoid what is strong is to strike what is weak"[4] and it is concluded that a commander should strike at an important point the enemy has to defend. Hence to attack strategic and vulnerable targets like "information" was always rational. The world has faced the wars in small and medium scale and in high technology in the form of guerilla warfare mainly in 90's. "The concept of limited warfare crept in to the lexicon of military theorists." [Novlin1998]. Most netwars will probably be non-violent, but in the worst cases one could combine the possibilities into some mean (LIC) Low Intensity Conflicts.

It would be fruitful now to give the "blind men opinions about the elephant" [Libicki1995] in order to understand IW and it will help to understand how and why it was used and is being used:

"Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[5]

"IW is the offensive and defensive use of information and IS to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, IS, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries" [6]

" IW encompasses actions taken to achieve information superiority by affecting adversary information, information-based processes, IS and computer-based networks, while defending one's own information, information-based processes, IS, and computer-based networks. [DoD1997]

"It consists of the actions taken to preserve the integrity of one's own IS from exploitation, corruption or destruction while at the same time

---

[4] http://all.net/books/tzu/tzu.html

[5] http://www.dtic.mil/doctrine/jel/doddict/data/i/03097.html

[6] http://www.psycom.net/iwar.2.html

exploiting, corrupting or destroying an adversary's IS and, in the process of achieving information advantage in the application of force." [Aspin1994]

Although some researchers including U.S army think that there is a new concept as "information operations" that refers to IW activities that are conducted during peacetime till the beginning of a conflict, the term IW will be used to represent all activities at any time in this study to avoid unnecessary complexity of terminology.

### 2.1.1 Different Forms of IW

Arquilla and Ronfeldt classified IW into four different forms. [RAND1997]

**Netwars** is aimed to control the information for the reasons of perception management and to affect the social targets.

In **Politics War**, measures that will disrupt national political systems and the actions that will impair the strategy of governments are taken.

In **Economical War**, in order to influence the national political leaders measures are taken to affect the national economy by the production and distribution of the products.

In **Command and Control Warfare or Cyberwar** the command and control structure of the adversary is targeted in order to reach the military goals. Psychological War, Electronic War, Deception and Use of Information are classified under this form of warfare.

Libicki, despite the similarities with the classification of the above writers classified IW into seven forms as:

- **Command-and-Control-Warfare (C2W)**
- **Intelligence-Based Warfare (IBW)**
- **Electronic Warfare (EW)**
- **Psychological Warfare (PSYW)**
- **Hacker Warfare**
- **Economic Information Warfare (EIW)**

- **Cyberwarfare**. [Libicki1995]

Schwartau thinks that information must be classified according to the actors of the domain. [Schwartau1994] He assorted the forms as *national, corporate and personal IW*. The author thinks that **Network Warfare, Economic Warfare, Political Warfare and Command-and-Control Warfare** are under the classification of national IW.

These forms of IW can be thought as the ones that can be applied to military forces, the ones that can be waged only on the civilian forces of a society and the ones that can be applied through the society or every element of a society.[7]

## 2.0 How Could IW Affect Turkish Land Forces Command?

"Turkey, too, is dependent on information technology, more so than you might think. It is over a year now since studies have begun being conducted and high government officials have started making alarming statements." [Kazaz 1998] Turkey will be threatened by terrorist organizations, drug dealers, organized criminals and, adversary countries in terms of information systems too. The TLFC will have difficulty in searing its own information systems and in defending the information infrastructure with its newly assumed responsibility. The problems stated above are also valid for the TLFC. The TLFC is also vulnerable because it is using the software and hardware systems of the firms whose headquarters are in other countries. Hence TLFC is dependent on foreign companies in information and telecommunication sector. Even though approximately 95 percent of all communications in the U.S Army is done via commercial lines, the ratio is small for Turkey. According to unconfirmed and unauthorized information

[7] http://www.ndu.edu/inss/strforum/forum28.gif

from Turkish General Staff J6 department the figure is around %15-20 for the Turkish armed forces. Even though there are great endeavors to separate the communication lines of the TLFC form commercial lines thoroughly, it is still using the commercial lines even in some secret labeled communications. Nonetheless there is no guarantee that these secure lines would be totally secure indeed. CARNIVORE was always in the official help of FBI. In recently confirmed U.S led communication surveillance network Echelon, it is alleged that American intelligence agencies tap into satellite transmissions and undersea communications.[8] According to an Army resource 1000-1500 hacker activities are recorded for the Turkish General Staff web site daily most of which are from other countries like U.S.A and Canada. In a six-month period, a department of Turkish Armed Forces has received 3908 virus-injected files. The main difference of Turkish army is that it feels that computer networks on commercial lines are not so safe hence it does not rely heavily on it. Turkish Army generally uses its own ISP and uses satellites. The TLFC is vulnerable since it uses the weapon and defense systems that were produced in foreign countries with the chips in it that was produced in other countries too. Desktop computers that are used almost in every room in the Turkish Land Forces units are threats for security. From the maintenance to complex rifle systems, from personnel files to communication systems computers are being used.

We are living in an era, in which developed countries are talking about the arms control agreement on IW tools. They think that an IW agreement is essential. “Russia can act as the initiator of rational agreements based upon international law that minimize the threats of the employment of information weapons.” [Adams1998] The significance of the subject is clear: U.S is spending between $1.7 and $2.1 billion annually on IW and it is expected that until the year 2005 it will be budgeted at $18 billion. In a future war, where the systems like Appliqué and Land warrior, that possess

[8] http://www.newscientist.com/news/news.jsp?id=ns9999789

databases, digital maps and network communication, will be used extensively, the criticality for preparedness is clearer today. Turkish Land Forces should take necessary steps in IW to defend its Defense Information Structure. It should improve its current situation in DIW (Defensive Information Warfare). With the advancements in software and hardware, along with regulations and manuals it must be ready for an IW attack by developing detection and prevention tools and especially by securing its information systems. Otherwise it could watch its GPS (Global Positioning System) be blinded, its choppers hit themselves since they perceive each other as foe, or it could find itself in a standstill in which critical information system do not work or no commander could communicate with his troops, with his headquarter and get no intelligence about the battle space.

# CHAPTER 3

# 3 Information System Security Process In The Context Of DIW (Defensive Information Warfare)

In this chapter, first fundamental terminology of Information Systems Security will be presented; then the risks, threats in the environment and different processes for security engineering will be reviewed.

## 3.1 Keywords In A Security Process

It is generally accepted that DIW (Defensive Information Warfare) must implement a multi-layered information security process [RFC2828] [Waltz1998] [Pfleeger1997] [Anderson2001]. This security process must be installed with a system approach to the information system after a security analysis and design.

The concept of security encompasses many terms and concepts when it is examined with an IW (Information Warfare) vision. It entails network security, communication security and data security. Nonetheless, the focus is on data and information; i.e. data is prevented from unauthorized disclosure and unauthorized modification. Every system tries to reach its “system high” [RFC2828] in its current “security environment” [RFC2828] in terms of confidentiality, integrity and availability. Below, the fundamental concepts of information system security will be reviewed with the purpose of establishing the terminological framework for the rest of the thesis document.

***Confidentiality*** means that the “assets of a computing system are accessible only by authorized parties” [Pfleeger1997]. It ensures that “information is not disclosed or revealed to unauthorized persons” [Ford1994]. Privacy could be regarded within this objective. Confidentiality objective tries to prevent unauthorized disclosure of data in order to protect

the secrets of people and the organizations. It is the basic objective since if confidentiality is present then it is hard to disrupt integrity and availability objective.

***Integrity*** is the “property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner”. [RFC2828] It provides “consistency of data, preventing unauthorized creation, alteration, or destruction of data”[Ford1994]. Integrity objective tries to protect data from unauthorized modifications and changes either accidentally or maliciously and it ensures the legitimate use. With integrity transactions will be certified and unable to be subsequently repudiated”. [Waltz1995]

***Availability*** refers to the objective that legitimate users must access and use the system resources. It means “assets are accessible to authorized parties”. [Pfleeger1997] It ensures that “legitimate users are not unduly denied access to information and resources”. [Ford1994] Performance specifications, reliability and quality are usually associated with the availability requirements. That is performance requirements of the system must be met within availability objective and “system must exist at some defined level throughout an attack and restore to full service”. [Waltz1995] Information warfare comprises the activities against those security objectives. IW causes “increased availability to offensive player and decreased availability and integrity to the defensive player”. [Denning2000]

A ***threat*** is a “person, thing, event, or idea, which poses some danger to an asset in terms of that asset’s confidentiality, integrity, and availability”. [Ford1994] Threats are potential violators of security. They challenge the system with their potential capability; they prevent systems from reaching its objectives in security, and cause loss and harm to the system in case of occurrence.

***Vulnerabilities*** are weaknesses in a safeguard or the absence of a safeguard. They are the proofs of the presence of “a circumstance, event and capability that could breach and impair security and cause harm.” [RFC2828] Vulnerabilities are considered along with threats and those flaws

and weaknesses in the system that could lead to security failures with threats. ***Vulnerability analysis*** looks for those flaws and the holes in the system. Security deficiencies are identified by vulnerability analysis; and also effectiveness and confirmation of security safeguards are evaluated by vulnerability analysis. ***Safeguards*** are countermeasures and controls, consisting of actions taken to decrease the system's existing degree of vulnerability to a given threat probability.

***Risk*** is the natural result of vulnerability and threat. It is regarded as the "expectation and the possibility of loss, expressed as the probability that a particular threat to information will exploit a particular vulnerability with a particular harmful result". [RFC2828] It is the measure of the cost of a successful attack.

***Risk management*** provides the "identification, control elimination and minimization" [RFC2828] of uncertain events that will cause problems in the system resources. It may include "risk analysis, cost/benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and system review".[9] In ***risk assessment*** activity, the main objective is to allocate safeguards and countermeasures to system resources while remaining minimum exposure. To do this system resources; namely data, capabilities and services in the system; and threats to that resources, vulnerabilities in those resources are pinpointed in terms of criticality and cost with ***risk analysis***. As a result risk management is related with cost optimization, functionality in protection and ease of use.

[9] http://www.oft.state.ny.us/security/Glossary.htm

### 3.1.1 Threat Consequences

Confidentiality, integrity and availability declare the “ideal” for security. Obstacles to that ideal are expressed in terms of threat, vulnerability and risk. Threats are available and they become ***threat consequences*** after a successful attack, namely after a ***threat action*** that results in a security violation. Threat consequences in the domain of DIW can be classified as:

***Unauthorized disclosure:*** This form of threat consequence occurs after an unauthorized access to an information system, hence it is a violation of the confidentiality objective. Threat actions that cause this form of threat consequence are:

- ✓ **Exposure**, is the action in which sensitive data is directly released to unauthorized entity, embraces deliberate exposure and scavenging, “searching through a data collection to get access information” [RFC2828], in the context of DIW.
- ✓ **Interception** is possible in network environments, data that is “traveling between authorized sources and destinations are accessed by unauthorized entities”. [Stalling1997]. Theft, wiretapping, and emanation analysis are among such threat actions.
- ✓ **Inference** is the one in which sensitive data is accessed indirectly by controlling the communication environment; it includes traffic and signal analysis.
- ✓ **Intrusion** refers to threat action in which data is accessed after security measures have been circumvented. Intrusion includes trespass, penetrate, and reverse engineering and cryptanalysis.

***Deception***: An authorized entity gets false data and believes that it is true. Threat actions for this consequence are as follows:

- ✓ **Masquerade** refers to the actions in which an unauthorized entity gains access and performs actions, spoofing and malicious logic Trojan horses are the forms of masquerade.

***Spoofing*** is the "creation of TCP/IP packets by using somebody else's IP address".[10] ***Trojan horse*** is a special kind of malicious logic that looks like valid but performs harmful and unauthorized activity in the system

- ✓ In **falsification**, false data deceives an authorized entity; substitution and insertion are the forms of falsification. The message or a part of the message is changed by another one or a change is inserted to the message.
- ✓ **Repudiation** is the action "in which an entity deceives another one by denying the responsibility for an action that he has done"[Anderson2001]. False denial of receipt and origin are possible forms. This threat will influence the combats in which network communication will be used intensively.

***Disruption:*** Disruption is related with availability objective, it embraces the conditions in which the correct operation or one of the services of the system is interrupted or prevented. The forms of disruption are as

- ✓ **Incapacitation** is the threat action in which one of system component is disabled by a malicious logic or after a physical destruction. ***Malicious logic*** refers to hardware software and firmware that is inserted to the system in order to perform different harmful activities in the system. "Malicious logic is usually inserted into executable programs and run immediately or in a scheduled time".[11]
- ✓ In **corruption** a system function is modified and operation of the system is altered because of tamper and/or malicious logic.
- ✓ In **obstruction** system operation is hindered by interference or overload. Overload refers to the incidents in which a system entity gets more input than it can process.

---

[10] http:advice.networkice.com/Advice/Underground/Hacking/Methods/Technical.html

[11] http://home.netscape.com/security/basics/glossary.html?cp=sspmid - horse

***Usurpation:*** It is the threat consequence in which control of system operations and functions are gained by unauthorized entities.

- ✓ **Misappropriation** occurs when an unauthorized entity gets physical and logical control of the system by the help of theft of data, service or function.

### 3.1.2 Security Services

Potential dangers and their possible results in a security environment make implementation of security countermeasures to the system a necessity. To prevent those potentials from becoming realities, ***security services*** are integrated to the system as the main security guards. As part of a security system those processing and communication services "implement security policy and they are implemented by security mechanisms". [RFC2828] Security services in the context of DIW could be stated as:

- ✓ ***Access control service:*** This service protects against unauthorized use or manipulation of system resources. "Access control is concerned with limiting the activity of a legitimate user". [Sandhu1994] This service dictates for identification and authentication of entities that want to access to the resources.
- ✓ ***Authentication service:*** Authentication is the process of "determining whether someone or something is, in fact, who or what it is declared to be".[12] In that sense authentication service provides the identity of entities to other entities of the system.
- ✓ ***Audit service:*** In computer security context audit is "independent examination of records and activities to ensure compliance with established procedures and policies".[13]

[12] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html

[13] http://www.sans.org/newlook/resources/glossary.htm

Security service stores the information “to provide the accountability for system events and the actions that cause those events”. [RFC2828] Information gathering process could be “offline or online in real time, in the latter case, the process is usually called intrusion detection”. [Sandhu1996] Auditing is also useful in catching privilege misuse of legitimate users.

- ***Availability service:*** This service tries to ensure the availability of system. It ensures that system is accessible and usable by authorized entities. Availability is dependent on other security services. In availability service an emergency plan called contingency plan is crucial for planning. “Contingency plan is for emergency response, backup operations, and post-disaster recovery in a system as part of a security program to ensure availability of critical system resources and facilitate continuity of operations in a crisis”. [RFC2828]
- ***Data confidentiality service:*** This service tries to ensure confidentiality of data in the system.
- ***Data integrity service:*** This service tries to ensure integrity of data in the system. Changes to data must be detectable and must be reported to system entities for fulfilling this service. Elimination of errors that has been detected can be thought under this service.
- ***Non-repudiation service:*** Non-repudiation service protects against false denials of communication and exchange after those activities occurred.” While these services do not prevent a user from repudiating another user’s claim that something occurred, they ensure the availability of irrefutable evidence to support the speedy resolution of any such disagreement”. [Ford1994]
- ***System integrity service:*** In system integrity, integrity of the whole system, the property of being unmodified and being able

to perform its intended function is crucial. System integrity service protects the system from those modifications and changes that will impair its integrity.

### 3.1.3 The Multi-Layered Security Process

Ravi Sandhu [Sandhu1994] has established and developed the concept of security engineering process. He has proposed a four-layered information security process.[14] Each layer in the process has a different function and service. Those layers will determine the number and the names of services that will be present in the security system and their implementation. “The layers are from the top to the bottom as security policy, security model, security architecture and security mechanisms”. [RFC2828] Nonetheless, different views on the layers and security engineering are available. “A top down approach to security engineering is possible, it will typically take the form of threat model-security policy-security mechanisms”. [Anderson2001] Whatever the phases are called, security engineering process tries to determine what services will be provided in the system in the upper stages and tries to find the ways to implement those services at the bottom stages.

#### 3.1.3.1 Security Policy

***Security policy*** is described as “a set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources”. [RFC2828] Security policy defines “clearly and concisely what the protection mechanisms are to achieve”. [Anderson2001] The authorities impose “the set of rules that is called as security policy in order to use and allocate security services and security facilities”. [RFC2828] Security policies enumerate what the systems

[14] http://www-dse.doc.ic.ac.uk/events/policy-99/pdf/03-sandhu.pdf

will do, what services they will have to be secure. Security policy is applied to all security relevant issues in the security domain. There are two forms of security policy as:

- ✓ ***Rule-based security policy*** is "based on global rules imposed for all users." [RFC2828] These rules usually rely on comparison of the sensitivity of the resource being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.
- ✓ ***Identity-based security policy*** is a security policy "based on the identities and attributes of users, a group of users, or entities acting on behalf of the users and the resources and objects being accessed." [RFC2828] Identity–based security policy makes it necessary for officials to identify and define individuals, groups and roles.

The issues that must be regarded in a security policy were generalized by RFC1244 as follows:

**1. Who is allowed to use resources?**

**2. What is the proper use of the resources?**

**3. Who is authorized to grant access and approve usage?**

**4. Who may have system privileges?**

**5. What are the user's rights and responsibilities?**

**6. What are the rights and responsibilities of the system administrator versus those of the user?**

**7. What do you do with sensitive information?** [RFC1244] [Stephonson1995]

Beyond those issues ethical issues, concerns and ethical policy of the organization could be stated in the security policy.

#### 3.1.3.2 Security Model

***Security model*** is as a "schematic description of a set of entities and relationships by which a specified set of security services are provided by or within a system". [RFC2828] "Security models are an important concept in the design of any secure systems. They all have different security policies applying to the systems."[15] The "Biba model" "Lattice model" and "Bell-LaPadula model" are the security models that dictate multilevel security in a system.

- ✓ The ***Bell-LaPadula Model (BLM)***, which is also called as the multi-level model or multilevel security, was proposed by Bell and LaPadula [Anderson2001] for enforcing access control and information flow in government and military applications. The model tries to find allowable paths of communication in a system where secrecy is important. BLP is focused on confidentiality, and enforces two properties in essence: simple security property or no read up (NRU) says that no process may read data at a higher level. ****-Property*** or no write down (NWD) says that no process may write data to a lower level. [Anderson2001] The third property, tranquility property, says "classification of an object could not be changed during process of the object by the system". [RFC2828] This model of protection consists of a set of subjects, a set of objects, and an access control matrix, several ordered security levels. Each subject and object is assigned to its own security level. Security levels, unclassified < restricted < confidential < secret < top-secret are used in Bell-LaPadula model. The security levels are used to determine appropriate access rights. In the applications this model is intended for, subjects and objects that are often

[15] http://infoeng.ee.ic.ac.uk/~malikz/surprise/spc99e/article1/

partitioned into different security levels. The clearances of subjects are compared to the classification of objects. For instance, the following are two typical access specifications: “unclassified personnel cannot read data at confidential levels" and “Top-Secret data cannot be written into the files at unclassified levels”. [16]

- ✓ ***Lattice model*** is based on the “lattice that is formed by the finite security levels in a system and their partial ordering” [RFC2828]. Classification level and the category designation that the elements have, is called as security level and levels are important in the relation and ordering between elements. Lattice model in fact is same with BLP model, but Lattice model is focused on horizontal information flow rather than the vertical. Hence Lattice model is focused on access security and “a security model designed to implement lattice models of security can be used in a military environment”. [Pfleeger1997]
- ✓ ***Biba model*** has the similar characteristics with the Bell-LaPadula model. Biba defines integrity levels, which are analogous to security levels of the BLP. Namely objects have integrity levels and could access to subjects according to those integrity levels.

#### 3.1.3.3 Security Architecture

“The ***architecture*** is the physical, logical, and administrative embodiment of your policy.” [Stephonson1995]. ***Security architecture*** is, “a plan and set of principles that describe the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services, and the performance levels required in

[16] http://www.cs.unc.edu/~dewan/242/s00/notes/prot/node14.html

the elements to deal with the threat environment". [RFC2828] System architecture is the direct result of applying system-engineering process in security engineering. "A complete system security architecture includes administrative security, communication security, computer security, emanations security, personnel security, and physical security". [RFC2828] Understanding security architecture certainly depends on the term system engineering and the forms of security that constitute security architecture.

"The multidimensional and dynamic nature of today's problems makes the need for them to be solved by the help of different disciplines with a wide overview and make it a necessity to update them according to the reevaluations due to changes with the time. ***System engineering*** is the discipline that was developed to meet that need". [KHO1992] Before any engineering process the system in which the process resides must be pinpointed. The need for understanding the "whole", before understanding and producing the components that will comprise the "whole" is always crucial. Understanding the whole will make it easier to meet the requirements and to satisfy the acquirer. "The system engineering process usually begins with a world view. That is, the entire business or product domain is examined to ensure the proper business or technology context can be established. The worldview is refined to focus more fully on specific domain of interest. With specific domain the need for targeted system elements is analyzed. Finally analysis, design and construction of a targeted system element are initiated". [Pressman2000] At the top of the pyramid, a very broad context and models are established and at the bottom, detailed technical activities, performed by the relevant discipline are conducted. In security engineering, abstract explanations of system behavior are reached after security architecture has been established, even though specifications are general and interdisciplinary at the upper levels. "Specialty sub-disciplines" [SSE-CMM1999] in the security architecture that is reviewed below form those different views of the security architecture.

- ✓ ***Administrative security*** includes management procedures and constraints to prevent unauthorized access to a system. "The management constraints, operational procedures, accountability procedures, and supplementary controls established to provide an acceptable level of protection for sensitive data are also defined under administrative security". [RFC2828].
- ✓ ***Communication security (COMSEC)*** is "related to the communication of information between security domains". [SSE-CMM1999].
- ✓ ***Computer security (COMPUSEC)*** refers to the measures that implement security services and assure the availability and functions of security services in a computer system. COMPUSEC is usually used to include the functions and characteristics of hardware and software in the system. "Computer security may refer to anything involving the physical protection of the machine, the integrity of the operating systems or the confidentiality and integrity of the data on it" [Beckett1997]
- ✓ ***Personnel security*** involves the procedures to ensure that persons who access a system have proper clearance, authorization, and need-to-know as required by the system's security policy. It is related with awareness and trustworthiness of the user.
- ✓ ***Physical security*** is related with the physical measures and security to prevent unauthorized physical access to a system.

After proper implementation of those security procedures the help of security mechanisms could establish the security architecture in coordination with security policy and security model.

#### 3.1.3.4 Security Mechanisms

***Security mechanisms*** are “low-level hardware and software functions that can be configured to implement a security policy”. [Sandhu1994] Those functions in the form of a process or a device have processes that can be used in a system to implement a security service. Digital signatures, Access Control Lists (ACL), Tickets, S/Key, Secure Socket Layer (SSL), authentication exchange, checksum, hash functions, firewalls and encryption are some of the examples of security mechanisms. As the bottom layer, security mechanisms constitute implementation layer of security engineering process.

With the security policy the organizations or security officials decides on the security services that they would have in their security system. The point here is that a security service, especially access control service could be referred to as a stand-alone security system, e.g. [Sandhu1994] [Sandhu1996]. Officials require that an access control service must be provided in order to meet security policy by declaring explicitly “users should have information according to need-to-know principle” in the security policy. Then a security model must establish the relationship between objects and subjects in the security domain. A model like Bell-LaPadula will state the clearances of users and labels of objects and access modes for the objects. After the entity-relationship for this specified security service has been described, the architecture to implement security policy, security service and system elements that will be used to meet the security requirements must be stated within security architecture with the help of total system engineering approach. Administrative, personnel, operational and communications security issues; namely issues like how will physical utilities be protected, how clearances of users will be sustained, how will hardware in the system be utilized; are pinpointed within security architecture. Then the mechanisms will implement the security policy while complying with the model, i.e. considering security levels of objects, in the light of the security architecture.

An ACL (Access Control List) will regulate the access modes of users and at the same time security labels will reveal the security levels of the objects, on the other hand firewalls of the system could filter the unauthorized access endeavors from outside.

Mechanisms must be implemented as simply as possible, so that simplicity enables the security officers to verify that the security mechanisms meet the requirements in the security policy of that information system. That "economy of mechanism" principle along with "open design" [Saltzer1975] helps the system to protect itself against attacks. The totality of security mechanisms in a system including software, hardware and firmware that is responsible for enforcing security policy are called Trusted Computing Base (TCB). The term Network Trusted Computing Base (NTCB) is used in network systems.

***Cryptography*** could be regarded as the fundamental mechanism of information system security. In fact it is the basic element for many other security mechanisms. Digital signatures, hash functions, an interface like GSS-API (Generic Security Service-Application Interface), a protocol like Kerberos could use cryptography. With the help of cryptographic card or tokens, cryptography provides access control service. Cryptography deals with transforming data in order to hide its meaning, against alteration and unauthorized access, by using encryption. Encryption is a "process of encoding a message so that the meaning of message is not obvious and open, decryption is the reverse process that "transforms an encrypted message back into its normal form". [Stallings1995]

## 3.2 Security Engineering Process

Security engineering process could be thought as the one that helps a system under development or a security system development and integration to a working system. Then it is clear that classical system development

phases are applicable to develop a security intensive system. Nonetheless, the point is usually to insert the security to the systems during development.

In fact ***Sandhu's approach***, defines a security engineering development process. Beyond that it outlines security system layers. Sandhu's four-layered approach indicates the goal that other security engineering processes try to reach. Design and analysis of the system proceeds from policy to mechanisms and tries to provide security objectives by applying security services. Every process tries to develop and implement systems that are compliant with security policy and model.

***SSE-CMM (Systems Security Engineering-Capability Maturity Model)*** is a community-owned model description that has been developed by an ad-hoc working group. It aims to lead the organizations that try to ensure good security engineering and describes the essential characteristics of an organization's security engineering process. Developers, integrators, acquisition organizations, system administrator and end users could use it. Security engineering practices must be practiced during all life cycle phases including "pre-concept, concept exploration and definition, demonstration and validation, engineering, development, operations and support and disposal". [SSE-CMM1999] It offers reusable standards for Request for Proposal and evaluation, reduced risks, fewer protests due to uniform assessments on industry standards and predictable and repeatable service in product and service for software and system acquisition organizations. Even though SSE-CMM does not declare a process development method for security it guides the organizations on security engineering and it states a security engineering process overview. SSE-CMM divides security engineering into three basic areas as: ***risk, engineering and assurance.*** At the simplest level the ***risk*** process pinpoints the risks and make a prioritization for the dangers inherent to the developed product and the system. ***Engineering*** process with the help of other engineering disciplines strives to find, determine and implement solutions to the identified dangers in risk process. As the last area

***assurance*** establishes trust and confidence in those solutions and deploys that confidence to the acquirer.

***Abrams et al*** bring their authenticate classification to security systems development process by focusing on the concept of system integration and development that meet multilevel security and operational requirements. Stages of security system development process are as follows according to them:

> "Security Requirements, Security Model, Risk and Vulnerability Analysis, Security Architecture, DTLS (Descriptive Top Level Specification), Covert Channel Analysis, FTLS (Formal Top Level Specification), Covert Channel Analysis, Security Testing Document, Certification and Accreditation even though the stages are Project Start, System Requirements Analysis, Preliminary Design, Critical Design, Coding, Testing and Completion in a typical system development process". [IEEE1995] Covert channel is defined as " a intra-system channel that permits two cooperating entities, without exceeding their access authorizations, to transfer information in a way that violates the system's security policy" [RFC2828].

A concise phase classification, could be as requirements phase, design phase, integration phase and, certification and accreditation. In requirements phase an applicable security policy is determined. First step in determining a security policy is to identify the objective. Trust, along with mission and trust requirements are identified. Security official has to select the trustworthiness that provides sufficient countermeasures for the risk environment and at the same time sustains the operational requirements set. Security concept of operation must be on spot during that phase. "Security ConOps" [IEEE1995] emphasizes security over the other operational aspects. Design phase is in the second layer. Certification team participation is of great importance in design phase. In integration phase combining products securely and porting not so much trusted applications are important issues. MLS (Multi Level Security) integration policy must be established after that process.

Certification and accreditation is the last phase of security system development process where the evaluation of the security is made. [IEEE1995]

***Waltz*** proposes a security analysis, design and simulation model in the realm of DIW. In the model, the first step is the vulnerability and threat assessment phases in order to develop a threat matrix as a result of these phases. Vulnerability assessment is made according to system specifications and “functional architecture”. Threat assessment is made under the light of the information that comes from the processes of threat intelligence and threat model that has been reached before threat matrix is produced with vulnerability assessment. After threat matrix has been developed risk management phase starts. In this phase risk elements are evaluated in terms of occurrence possibility and loss in case of occurrence, alternative ways are developed in order to manage acceptable risks and risk evaluation and security criteria are defined. During this phase security services and threats are taken into account.

The next step is in Waltz’s model to establish defense program plan. In this plan all components of protection and elements of OPSEC, TCSEC and INFOSEC are defined. After that plan security design begins. During design phase countermeasures, TCSEC and INFOSEC are designed. An error analysis is made and OPSEC policy and procedures are developed. Physical security is also designed during that phase. A red team, after design phase, develops independent attack plans and implements those attacks as a tool of security verification test, namely they try to create security incidents. In the light of those attacks test plans and design feedbacks are developed. The attacks also help threat assessment. [Waltz1998]

Another IW based approach has been proposed by ***Denning***. She like the other authors thought that the first point in security against those IW attacks is measuring vulnerability. Then a secure security system must be developed to eliminate those flaws. Since DoD is usually an acquirer rather

than a developer, in the context of IW she reviews the **TCSEC (Trusted Computer Security Evaluation Criteria)**.

***TCSEC*** describes the security requirements firstly. It declares six requirements to make a system secure. Requirement 1 and 2 are interested in policy. Requirement 1 (policy) states that**: "**There must be an explicit and well-defined security policy enforced by the system. Given identified subjects and objects, there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object." [TCSEC] Requirement 2 (marking) is related with marking according to security policy: "Access control labels must be associated with objects." [TCSEC] Next two one of the requirements are related with accountability. Requirement 3 (identification) states, "individual subjects must be identified." [TCSEC] Requirement 4 (accountability) states that, "audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party." [TCSEC] Last two of requirements are related with assurance. Requirement 5 (assurance) states that, "The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements 1 through 4 above. In order to assure that the four requirements of Security Policy, Marking, Identification, and Accountability are enforced by a computer system, there must be some identified and unified collection of hardware and software controls that perform those functions." [TCSEC] Requirement 6 (continuous protection) declares, "No computer system can be considered truly secure if the basic hardware and software mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion." [TCSEC] Documentation is also a requirement not mentioned in this classification.

TCSEC later describes criteria and divisions. Trust levels from the lowest to the highest; they are D, C1, C2, B1, B2, B3, and A1. The four primary requirements of the C2 standard are security policy, accountability, assurance and documentation. These security requirements are valid for

every evaluation class but their degree of implementation changes from class to class and among divisions.

After covering different security engineering approaches, in the following page a comparison of different approaches that are used both in developing, integrating and assuring secured and trusted systems are given to enable brief description:

| **SECURITY APPROACH** | ***SSE-CMM Approach*** | ***Waltz Approach*** | ***Abrams et. al Approach*** |
|---|---|---|---|
| **GENERAL CHARACTERISTIC** | Helps the security eng. and user organizations define process and life cycle | A security analysis and simulation | Defines typical security engineering activities |
| **APPLICATION DOMAIN** | Could be applied by all stakeholders during all life cycle phases | Could be used mainly in DIW Operations | Defines all of the security engineering process |
| **RELATEDNESS WITH OTHER APPROACHES** | Accepts a risk identification step then generalizes the engineering step | Could meet the threat and vulnerability analysis requirements of other approaches | Integrates the process with Sandhu's approach and TCSEC requirements |
| **ADVANTAGES** | 1.Provides standardization 2.Same for organizations | 1.Could be applied with other approaches 2.Specific for IW | 1.Meets MLS requirements 2.Thorough for security engineering phases |
| **DISADVANTAGES** | 1.Implementation process is implicit. 2.Helps on defining process not defines one | Mainly a supplementary for other approaches | 1.Overestimates and does not explicitly define risk, threat and vulnerability |

Table 3.1. Comparison of Different Information Security Approaches

| **SECURITY APPROACH** | ***Denning's Approach*** | ***TCSEC*** |
|---|---|---|
| **GENERAL CHARACTERISTIC** | Focuses on vulnerability analysis and building the system securely | Rather than defining the development process evaluating the systems in terms of security and defining security needs is possible. |
| **APPLICATION DOMAIN** | Does not specify a process | System manufacturers, acquisition management teams could use it as a guidance and metrics, also it specifies a basis for specifying security requirements |
| **RELATEDNESS WITH OTHER APPROACHES** | Compliant with the security engineering phases of SSE-CMM | Establishes assurance evaluation part for SSE-CMM. |
| **ADVANTAGES** | 1. Special for Information Warfare Security needs | 1.Specify both security features that must be present and assurances that must be met.<br>2.Its division nature gives a kind of modularity to the criteria. |
| **DISADVANTAGES** | 1.Depends on other approaches, not authenticate | 1.Designed to support multilevel security not so suitable for commercial use.<br>2. To comply with the criteria are costly and time taking.<br>3.Does not support the need of producers for greater flexibility in picking security features and assurances. |

Table3.1.Continued

# CHAPTER 4

# 4 Application Of DIW In Acquisition Of CIIS (COMMON INTEGRATED INTELLIGENCE SYSTEM) of the TLFC

## 4.1 Introduction

In this chapter by considering the existent studies on Integrated Intelligence Information System (CIIS) like master plan, As-Is Model and general system requirements; Security Policy Requirements and Security Model for CIIS is developed compliant with higher-level regulations and directives in order to defend the system against IW threats.

## 4.2 Approaches For Identifying And Eliminating The Weaknesses Before They Occur

There are four general approaches for identification and elimination of weaknesses before an attack incident is realized or security is violated. The approach could be, **monitoring information system for vulnerabilities and weaknesses or the system could be developed free of vulnerabilities as possible**. “User training and awareness about the threats and risks and avoiding single points of failure” could be other approaches [Denning2000] Since the project is in the phase of contract and “operational need” and “concept exploration” phases are over and the system will be developed from the scratch, the issue is to specify system security requirements and to make the system be built according to security standards.

## 4.3 Security Policy Requirements For CIIS

Security policy will establish the baseline for the rest of the security system. It will outline the general characteristics of the system. The policy must comply with the regulations and directives of the TLFC and must comply with higher level IS security policy.

### 4.3.1 Introduction

4.3.1.1 CIIS software security system will be designed and developed as a subsystem, and the requirements that will be covered in the following pages must include the security subsystem.

4.3.1.2 In the preliminary phases CIIS, information security subject is covered under counter intelligence and security requirements topic along with Physical Security and Personnel Security.

4.3.1.3 For the purpose of providing information security, implementing security and drawing the realm of information, security requirements for information security are specified and this document is presented.

4.3.1.4 Topics in the document comprises system security policy requirements and must conform to the security policy of other systems that CIIS will work with and after the beginning of usage policy requirements beginning from battalion level must be prepared.

4.3.1.5 All the users and developers must apply system security policy and security requirements.

4.3.1.6 System security module must be conformed and interoperable with all other system modules, hardware and system elements

4.3.1.7 System security development process for CIIS will be regarded, planned and applied with other system (hardware-software) development phases. The Supplier must present all the related deliverables and documents to the Acquirer.

4.3.1.8 The security model in this document will be regarded as a beginning model and the supplier must develop and apply its own physical and logical design for security in the development phase.

### 4.3.2 General

4.3.2.1 It must not be allowed for unauthorized people to access any files and programs with neither internal nor external methods.

4.3.2.2 CIIS information security system must meet the standards and requirements in the contracts prepared for related systems, and must be interoperable with those requirements.

4.3.2.3 CIIS must be regarded as a national system in NATO standards.

4.3.2.4 Multilevel system security and multilevel access control must be applied on CIIS.

4.3.2.5 CIIS system and all modules in the system must be password protected. Users must access all the authorized modules after entering their passwords once.

4.3.2.6 System administrator and security manager must define and apply the conditions in which dual authentication is necessary.

4.3.2.7 Passwords and usernames must not be shared among users. For this purpose the previous login date for the user must be shown in the user interface in every login.

4.3.2.8 Maximum wrong entrances for passwords must be parameter driven, after wrong password entrances due to that parameter, terminal for the user must be locked. The administrator must change parameter. System administrator must be alerted automatically and system must begin operating only by the administrator.

4.3.2.9 If the password for a username has been entered wrong before, in the first login for that username faulty event must be alerted on a window to the user.

4.3.2.10 Passwords must be eight characters at least.

4.3.2.11 Passwords must be case sensitive.

4.3.2.12 Users must change their password periodically according to their clearances, system must warn the users prior to next change date, due to a parameter. Users with cosmic top-secret clearances one in three days, with secret one in a week, confidential and restricted users one in two weeks and unclassified clearances one in a month must change their passwords. The administrator must determine change periods.

4.3.2.13 Usernames that has not logged in to the system due to a parameter must be deleted.

4.3.2.14 System must detect wrong and unauthorized log in and intrusion attempts, record them and warn the system administrator on the event. The attempts outside the system must be detected too.

4.3.2.15 CIIS must enforce need-to-know principle.

4.3.2.16 Encryption must be used in satellite communication.

4.3.2.17 CIIS security architecture must allow the users to have different roles, definition of different groups and permissions according to those roles. Furthermore definition of security profiles and access control including hardware components must be possible according to roles. Permissions for system administrator must be definable.

4.3.2.18 Definition, deletion and updating of new roles and groups must be possible. System administrator must apply those definition and permissions.

4.3.2.19 All the elements in the system, like menus, interfaces, tables, modules, buttons, frames and fields must be associated with a security label.

4.3.2.20 CIIS must allow the security official to define the permissions for a user group in the interfaces and the data in those interfaces until the bottom level.

4.3.2.21 Usernames must only be changed and deleted by system administrator in CIIS.

4.3.2.22 Installations in which the system will be implemented must be protected against HRF (High Radio Frequency) and EMP (Electro Magnetic Pulse) according to manuals and TEMPEST AMSG 720 standard.

4.3.2.23 Encrypted and protected circuits must be used in CIIS.

4.3.2.24 All the messages rather than unclassified and restricted must be encrypted before sending. The supplier and the acquirer according to Acquirer standards must determine encryption algorithms and mechanisms. Detection for unencrypted messages in the category must be made by the system.

4.3.2.25 Messages must be encrypted including message address.

4.3.2.26 Digital signatures must protect internal user definitions, authorizations. All the messages must be sent with a digital key that will authenticate the originator in the received side with the help of a private key.

4.3.2.27 No hardware or network in CIIS system, must have direct Internet connection even though it has firewall protection.

4.3.2.28 A firewall mechanism must be used before central database management system.

4.3.2.29 Suppliers will conform to DoD 5200.28-STD (TCSEC) standards during development and evaluation.

### 4.3.3 Procedural Baseline

4.3.3.1 It must be possible in CIIS to detect how much and when a user used the system, data amount that has been processed and used, the reports and objects that have been used by the user must be taken when needed. For the synchronization of the subsystems there must be a timeserver that will scan the records in a time sequence.

4.3.3.2 Critical transactions must be proposed by users and must be defined by the administrator. There must be mechanisms for defining critical transactions.

4.3.3.3 Critical transactions must be recorded including time and the user.

4.3.3.4 Other users must not have write or update permission in the memory limits in which a user runs his programs.

4.3.3.5 A user in the upper level must not have the permission to write in the objects and data on lower levels.

4.3.3.6 A user can not read the objects and the data on the upper clearance levels.

4.3.3.7 There must be a mechanism in which the users on the same level can cancel access control restrictions on the users at the same level regarding the need-to-know principle.

4.3.3.8 According to a user defined time parameter; the screen for a user must be closed if the user has left a program open for that time. To log in again, the username and password must be given.

4.3.3.9 After an attack the system must return to its last position that is presented by nonfunctional requirements after a time interval. In that condition the system must meet encryption and security model requirements

4.3.3.10 The messages must have hardware system number, recorded user code, category-security degree, page number and a unique serial number according to “MST 386-8 (A) Automatic Data Processing Security” manual document security section.

4.3.3.11 All the data exchange that is conducted by distance terminal connection must be sent through Secure Shell mechanisms.

4.3.3.12 CIIS must have intrusion detection systems that will control the traffic on networks and detect the intruders.

### 4.3.4 Data Acceptance

4.3.4.1 System must provide discretionary or full return alternatives, system must present incremental or full backup. CIIS must provide online backup preventing user access. All the transactions must be programmable, remote accessible and must be recorded. Backup must be on periodical base.

4.3.4.2. On a crackdown, or a hardware-software bug system must keep its integrity and it must save its uncompleted transactions.

4.3.4.3 System must return all uncompleted transactions to last consistent state and it must be possible to complete those transactions after those returns.
4.3.4.4 It must be possible to create data on other medias and hardware then to insert those data to the System by the users and he administrator. System must work with true and trial data. It must be prevented from being inserted the same data twice for different tables.
4.3.4.5 Inconsistent data must not be accepted by the system.
4.3.4.6 If it is likely to make mistakes on processing data; lists; menus and buttons must be used on those interfaces.
4.3.4.7 User approval must be necessary for deletion of data.
4.3.4.8 There must be a mechanism to return the data that has been deleted to the system before making another deletion.
4.3.4.9 Checksums must be used to detect the changes and damage on the data.

### 4.3.5 Hardware security

4.3.5.1 There must be an identification number for each hardware on the system that is hung on the hardware. A mechanism like ID chip is preferable.
4.3.5.2 This identification number must be used as hardware system number.
4.3.5.3 Messaging hardware must be recognized by the system. During software implementation and configuration those numbers must be inserted to the system. The system must not allow the messaging or information exchange functions rather than those machines.
4.3.5.4 Installations in which hardware will be installed must be built as secure places.
4.3.5.5 System must not communicate through the hardware, telephone numbers, IP numbers or wireless equipment rather than the predefined ones.
4.3.5.6 IP numbers, identification numbers and other information of the systems in the Tactical Internet Network must be protected from external

entities by the help of applied software and mechanisms. No hardware from external media must access those data.

4.3.5.7 Rooms where CIIS system has been installed must be close to the middle of the installations as much as possible.

4.3.5.8 Power and signal filters must be used on the circuits where the system lines will pass.

4.3.5.9 Electrical lines must use one ground line.

4.3.5.10 Unnecessary electrical and water lines must be removed before system implementation if there is any.

4.3.5.11 All the metal lines, equipment must be isolated from entrance and exit pointes where there is a risk of radiation.

### 4.3.6 Personnel Security

4.3.6.1 Users must not use their old, according to a defined parameter, passwords in CIIS.

4.3.6.2 Security inspections of the users must be made according to “Armed Forces Protective Security and Coordination Directive” [114-1B].

4.3.6.3 Users must take “CEIS Security” certificate before being a user. [114-1B]

4.3.6.4 The users who will use the systems with encryption must be authorized with “National Encryption Security Certificate”. [114-1B]

4.3.6.5 The users who will work on encryption centers must be inspected as stated in Encryption Security Inspection and “Encryption Security Inspection Certificate” must be filled.

4.3.6.6 If there is a denunciation about a user or if there are suspicious actions of the users the user must be prevented from using the system, until the end of the positive inspection

4.3.6.7 If a user leaves the related system entity or installation for good due to any reason, user account for the user must be closed.

4.3.6.8 All the users that will use the system must take an education about security. Supplier will give the education to system security officials firstly. The officials must keep on teaching security to users.

4.3.6.9 Passwords, encryption keys and data about security must not be sent via e-mail.

4.3.6.10 Supplier must inform the Acquirer about its personnel that will work on the system development of CIIS to provide the inspections about the personnel. Personnel turnovers must be reported immediately to Acquirer.

4.3.6.11 Supplier personnel must conform to security requirements as long as they are the members of the development or any other CIIS project team member. Responsibility is on the Supplier.

4.3.6.12 Working conditions of the supplier (installation, personnel, hardware, firmware, communication) must meet the standards stated above. The Acquirer must inspect those conditions.

4.3.6.13 Supplier is responsible to study and develop the product on the installation which Acquirer requests.

4.3.6.14 The standards and the procedures that will be used during development must conform to Acquirer security policies.

4.3.6.15 Working conditions and standards of the developed system must conform to Acquirer security policies.

## 4.4 CIIS Security Model and Security Architecture

Bell-LaPadula and Military Security Model features must be used as the reference in the modeling of CIIS in compliant with Multi Level Security. Therefore all the objects and the subjects in the system, the relationships between those objects and the subjects must be identified and access control lists according to that classifications must be prepared [Anderson2001].

According to military information system, objects and subjects have security levels and clearances called as Unclassified, Restricted, Confidential, Secret and Top Secret. Access control requirements and specifications must express which objects can access to which subjects. Steps for security requirements could be detailed as follows. In this study bolded parts reveal the main activities in military information security concept.

**1. Access control methods of CIIS must be determined. Hence, according to [386-8A] "Automatic Information Processing Security Directive":**

a) Sensitivity, sensitivity level of the data in the system must be explicitly stated. Sensitivity level comprises "category" and " security level".
b) Clearances of objects in the system must be identified.
c) Security requirements for the transactions that will be conducted on the subjects must be identified.
d) Measurements to protect the category of the subjects must be specified.

**2. Software-hardware units and objects in the system must be stated**

**3.Required software-hardware must be determined.**

**4. Physical media in which the system will run must be defined.**

**5. Human resources requirement for the system must be defined.**

**6. Security must be tested.**

**7**. **The security must be in a continuous structure.**

### 4.4.1 CIIS Security Architecture

Establishing the ***architecture*** means to state physical, logical, and administrative form of CIIS security policy. Architecture will describe the security services that CIIS is required to provide to meet the needs of its users, the system elements required to implement the services needed.

#### 4.4.1.1 CIIS Object Structure

Software subsystems must be detailed in System software design phase. Supplier must design and develop database and application software objects regarding the objects and subjects given in the following tables, the requirements specified in terms of objects-subjects when designing security subsystem software. With the help of this software, the system security officer must be able to define, extend, add, delete, update and interrelate the objects and subjects in terms of security, according to the objects–subjects stated in but not limited to the tables. Due to security and confidentiality considerations Object Identifications Table, Subject Identification Table, Security Features of Objects Table and the Subjects Processing Objects Table are not given in this document. Those tables could be found in the technical contracts in the related department of the TLFC.

### 4.4.2 CIIS Access Control Model

Modeling of access control according to roles [ACM5] [ACM7], that is regarded as the prime service for security services could be stated simply as follows:

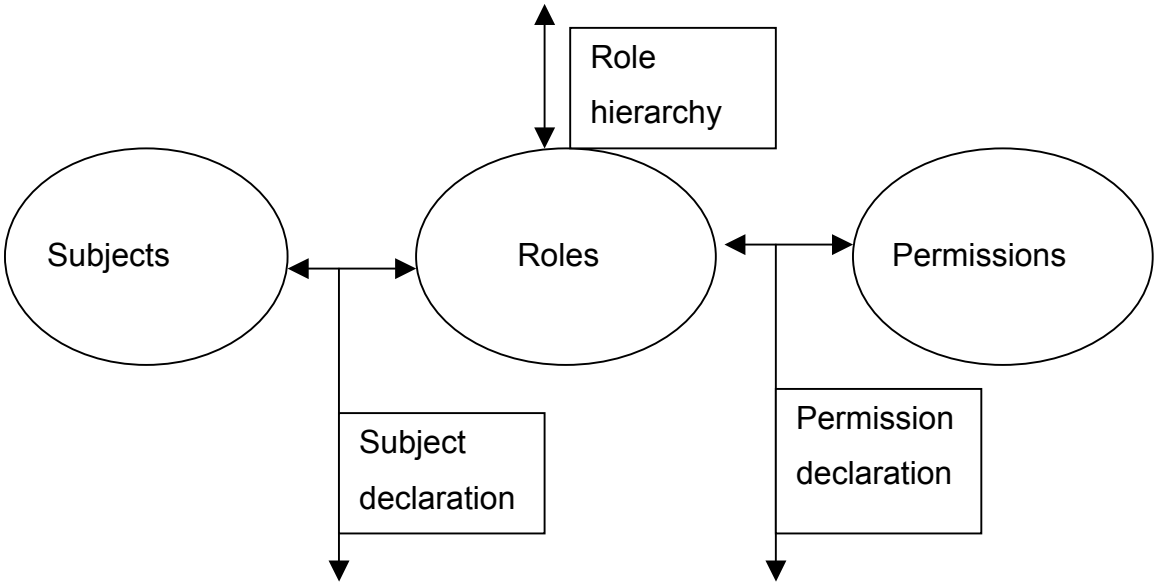


Figure 4.1 Role Based Access Control

When the main processes according to the model are considered, they can be stated as:

**Identification of Subjects - Identifications of objects.** While conducting those activities role hierarchies and groups must be considered. After the identification of Subjects the permissions, namely access rights that Subjects will have must be determined. Identification of roles could be regarded as the definition of Intelligence function in a hierarchical manner in Turkish Land Forces Command. Information exchanges among subjects are same as analyzed in business modeling of the Project. In order to express entity-relationship model of the subjects and objects that have been defined above security levels of the objects, intelligence category of the object,

clearance that is needed to access the subject, minimum level for the subject that can access the object, minimum level hardware that will transact the subject must be defined. This model will be the base for system access and authorization matrices.

Security degrees for the subjects must be defined according to Armed Forces Headquarter Services Directory (MY75-1A). According to the directory [75-1], security degrees for the formatted objects could be given default if possible, if it is not given or the information degree in the object is higher than the predefined degree a new degree for the object could be given by the creator of the object. Precedence could be defined according to Armed Forces Headquarter Services Directory (MY75-1A) and Armed Forces Report Directory. Creator could again change the Precedence of the object created.

Category is a factor that regulates the information flow and security level for the Objects. It provides the selection and transmission of the Objects according to importance degree. Categories are in three forms. Category-1 is called as Vital Reports and usually sent as Flash, Category-2 is called as needed Reports and usually sent as Operational Immediate. Category-3 is called as Useful Reports and sent as Priority. [227-1A]. In CIIS all the Objects that are defined in Armed Forces Report Directory are taking precedence over other Objects. When needed the communication of Category-1 and Category-2 Objects. [227-1A]

System administrator and other system officials will give security clearances of the Subjects. [386-8A]

After the security characteristics of objects are determined, entity relationships of those objects with the subjects must be defined. According to those relations authorizations of subjects over those objects and access modes must be stated. Hence, authorization-access control lists must be prepared. Authorization beginning level is taken as Platoon Commander. There must be four transactions over objects in CIIS.

**Creation (Definition)**: Authorization to create an object. Creators can only make deletion.

**Write**: Authorization to make changes on an object.

**Read**: Authorization to access an object without making any change.

**Process**: Authorization to make formal changes, analyze, assessment over an object and authorization to deliver the objects to neighbor, inferior and superior units.

Due to security considerations the preliminary model for security and the tables in the model for this project is not given in this study, but it could be found in the Technical Contracts for the related Project.

# CHAPTER 5

# 5 Case study

## 5.1 Introduction

In this chapter real current projects in TLFC, which are going through different software development stages for now, will be considered. The point to be investigated will be to find what are the weaker and stronger points in terms of secure system development process in the real projects. Since the evaluation of security of a specific project is not the purpose of this study the names of the people and organizations are not used. Instead, the roles are defined and renamed for the case study. Contracts will not be presented or analyzed in every aspect, only related security requirements of the contracts - draft contracts and if exists models that are suggested will be studied.

Even though contracts are not the only or full indicators of the information security of the systems, nor their readiness for the IW, it is assumed that for the development and acquisition of systems, contracts are trusted qualifiers for functional and nonfunctional requirements of a secure system; since a system is secure when it satisfies its security requirements as specified. It is also compatible with the basic rules of IW concept since it helps to ensure IW readiness in the first phase by providing the development of secure systems. Related with the issue security sections in the technical contracts of information systems projects are not the only parts for security, other properly examined sections, like well specified user requirements and functional and nonfunctional requirements help a lot in realizing security in the overall system.

What is suggested and applied partially in Chapter 4 is an approach that aims to design the most secure system that will provide readiness for future IW, namely the most secure system that meets the requirements of

DIW. In this case study, security requirements of different military IS projects will be analyzed and compared.

The comparison must be made among military information systems since the proposed security requirements and the model is for a military information system.

Reviewing different approaches will make it easier to understand " what would have been if some other security policy, model and mechanisms were dictated by the requirements for specific services." From a different perspective it will also reveal, "which security services are not considered" therefore " which threats are possible to occur in different contracts due to those vulnerabilities and risks"?

Rather than analyzing and synthesizing current projects on security and comparing them with the proposed approach one by one, it is preferred to analyze the projects individually and then to attempt a synthesis to compare the current practice with the proposed one.

The essence of case study will be the point in which it is stated that no information system is totally secure. But with the case study we will be able to understand how successful the current proposal is in providing an acceptable system in terms of IW and Security; it will also let us know what else could be done in the future and how could we enhance the security level of the proposed security approach. Beyond criticism the aim is to find the optimum approach for security in military information systems.

## 5.2 The Roles and Definitions To Be Used

PROJECT**:** Executed process to acquire the requested products and services.

USER**:** The user of the products and services.

SUPPLIER**:** The producer of the products and services in the project.

ACQUIRER**:** The organization, which tries to procure the system specified in the project.

## 5.3 The Case To Be Investigated

### 5.3.1 Purposes of the Projects

Project A is an information system project that is planned for the automation of procurement, maintenance, support and service functions of TLFC.

Project B is for acquisition of the system that will be used in the management and communication of TLF units.

Project C is about procurement of local area network and wide area network infrastructure of a TLF unit.

### 5.3.2 Information Security Approach in the Project Contracts

System specific security issues are not defined in the contracts. Security engineering process states that a four-layered process must be used in the development of secure systems. In the projects, those abstraction levels for security do not exist. ***For example it is not clear " what is the security policy of the organization, what is the policy for the project, which model and architecture will provide the requirements of this policy, which mechanisms will meet the needs of security services and the policy?"***

In general, the projects are not so much concentrated on security issues. ***There are no detailed specifications for information security***. The specifications are limited on general functions of the system. Beyond specification within acquisition of military information systems security must be regarded as a first priority issue. Since security in its general meaning is critical and the first mission of military units. Therefore not specifying security properly means, defeat for military units acquiring new information systems.

***Secondly, approaches for security are not integrated nor totally defined***. Inside the contracts quotations from different standards are observed but a specified process is not followed; different approaches from different standards could be found in the contracts. This reality creates neglected functions in security services.

Since there are security directives, manuals and orders published by TLFC, in the contracts those directives must be regarded as the guide, but in ***security analysis and specifications information security directives are not considered as a guide.***

***Finally the high level of dependence on supplier about security issues must be considered a weakness of security***. Without giving a preliminary design for security, acquirers have given only the names of services or the names of the concepts that they want. This probably will cause the system to be implemented without validation or with unsatisfied acquirer requirements, since it is subjective if they are real requirements or not.

### 5.3.3 Information Security in Project A

In the first specification for security it is stated that security model for Project A must be designed. Within this model it is stated that COMPUSEC and COMSEC for Project A must be designed. As reviewed before, ***security model and architecture based on this model needs to be composed of Administrative security, Personnel Security and Physical Security along with COMSEC and COMPUSEC.***

Even though MLS (Multi Level Security) is required for the system, it is not clear what is meant by MLS. After detailing the functions MLS specifications and the model must be constructed to meet those functions.

As a positive issue, acquirer wants the supplier to study the monetary side of the security issues and wants the supplier to assess the cost of the mechanisms in MLS approach and traditional ad-hoc approach. ***Besides, the***

***acquirer requires the supplier to submit Unit Security Model Design regarding cost.***

There are no detailed specifications for achieving the properties of a secure system. It must be explicitly specified how will ***Audit service, Availability service, Data confidentiality service, Data integrity service, Non-repudiation service and System Integrity service be provided in the system along with Access control service and Authentication service.***

### 5.3.4 Information Security in Project B

As in the first project general issues are present in the Project B too.

Project B is ***good in specifying security requirements regarding security services***. Specification for security in the technical contract encompasses authorization and authentication details.

Project B also ***handles security architecture regarding Personnel security and Physical security.***

As a proper method, ***security requirements are not limited in Security Properties section; issues that will enhance the security level of the system are specified in related sections.***

Even though role based access control is required; ***roles or groups are not defined in the specification.***

### 5.3.5 Information Security in Project C

Even though Project C is different from the other projects in functionality and size, it constitutes a good example for growing importance of network side of Information Security and IW.

General issues are valid for Project C too.

In the first specification Project C states that system must comply with C2 Security Level. This is surely a quotation from DoD 5200.28-STD. ***Rather than only requiring that level, defining the security requirements and giving relations among entities, as explicit requirements could be preferred.***

***There is no integration between security services and security requirements***. System security services are not well defined in the requirements. Hardware security requirements are explicitly specified. Since system is hardware intensive, security requirements for hardware are thoroughly and individually defined for any hardware.

As a result of not using a defined process, ***all the possible mechanisms for services are not defined in the system***. But mechanisms like firewalls are explicitly defined.

Technical contract describes the security mechanisms that will secure the main security mechanisms. ***To identify the security for security mechanisms is successful.***

## 5.4 Proposed Defensive IW Approach

### 5.4.1 Introduction

In chapter 4, security policy requirements and the architecture-model that will apply this policy and model were analyzed and designed.

In the application of the approach regulations, directives and the manuals in the domain and software engineering topic are considered as the guides that MUST be followed. Since the domain is military intelligence, TLFC and Turkish General Staff directives and manuals in the domain are followed. In Information Security topic MST 386-8 (A) is followed.

### 5.4.2 Process in the proposed approach

This approach considers security engineering ***as the support activity that must be conducted throughout the software engineering activities and software development and project life cycles***. It must be applied regardless of the development process and methodology. Hence all the modules, components, SW and HW of the system must be integrated and interoperable with the system security components.

While integrating security to military systems, cost, performance, technical risk and usefulness of the security mechanisms must be taken into consideration.

During security engineering process main areas in our approach are determined as:

- **Risk and threat management**
- **Development and engineering**
- **Security assurance**

Besides being applied in every phase of Software Engineering process, ***to apply security engineering efficiently, needs the steps and the activities of the SE must be conducted properly during engineering and development phase of security engineering.*** Those steps and the activities in the steps could be stated as:

- **Planning and organizing for security**, it must be coordinated with other project management activities and must have a management plan and risk management for security.
- **Requirement analysis, modeling and specification**
- **Design**

  - ✓ Logical Design

- ✓ Architectural Design
- ✓ Detailed Design

- **Implementation**
- **Testing and Certification**
- **Operation, Maintenance and Support**

This process approach certainly brings a layered process for security. In this layered process work products are successively as follows:

- **Security Policy**
- **Security Architecture**
- **Security Model**
- **Security Mechanisms**

In the approach it is considered that by applying software engineering activities for security, those levels must be followed and each following level must conform to the upper level. Security policy must comply with the security policy of upper units.

### 5.4.3 Application of the Proposed Approach

By considering the process and abstraction levels reviewed above, an approach to apply information security engineering for DIW is developed. First two activities of Development and engineering phase are applied in order to obtain Security Policy, Security Architecture and Security Model for the Intelligence System. The proposed approach stipulates that Eligible Security Mechanisms for the model be stated in the requirements along with the policy.

Application requires designing the model that will meet the requirements of Military Multi Level Security. It necessitates that,

- **Requirements must be elicited properly considering main Security Policy of the Organization.**

- **Entities and the related properties in the system, objects and the subjects, must be defined.**

- **Clearance and hardware for the subjects must be determined.**

- **Security level (Security degree (Security Classification) and category), Precedence minimum hardware that will process the object, clearance of the subjects that can process the subjects must be determined for the objects.**

- **To integrate all, transaction authorizations for the objects must be determined.**

Overall model comprises the authentication and authorization services that are so important for the security. Models for other security services could be developed as a future work.

## 5.5 Comparison and Evaluation of the Approaches

To compare and evaluate three contracts currently in the process of development with our system in terms of information security approach will reveal the differences concisely.

Following table will compare the approaches in this context.

| **THE ACTIVITIES OF SECURITY ENGINEERING** | ***AD-HOC APPROACH*** | ***PROPOSED APPROACH*** | ***EXPLANATION*** |
|---|---|---|---|
| Planning and organizing for security | Security planning is considered within project planning, a security team is not allocated. A project team member or central security department is responsible form security. | Even though security project management is thought as integrated with system project management time, resources and a plan is developed for security. | |
| Requirement analysis, modeling and specification | General requirements for security are analyzed. System functions and acquirer requirements are not considered. | System requirements are elicited considering system functions, acquirer requirements. | In Project A to require a cost planning for security is applicable for proposed approach. |
| Design | Design phase is left to the developers. | A preliminary model for access control and authorization is developed. | Preliminary model is not restrictive on Supplier. |

Table 5.1. Comparison of Contracts

Another comparison could be made among processes. Multi layered approach could be reviewed in different contracts could be compared as:

| **THE PROCESS OF SECURITY ENGINEERING** | ***AD-HOC APPROACH*** | ***PROPOSED APPROACH*** | ***Explanation*** |
|---|---|---|---|
| Security Policy | Security policy for the system is not specified, the requirements for policy after the deployment of the system is not explicit. | A security policy that complies with the basic policy of the organization is established. Requirements for security policy after deployment are explained. | A risk policy for security project management must be developed. |
| Security Architecture | Security architecture is not thorough, not including all the components of security architecture. | Security architecture is established regarding all components and security policy. | |
| Security Model | A model is not proposed | A preliminary model is designed. | |
| Security Mechanisms | Security mechanisms are specified. Nonetheless since there are problems in the process mechanisms are not proper. | Mechanisms are chosen following layered process and after acquirer requirements. Even though the problems in the essence of SWE exist, they are limited. | |

Table 5.2. Comparison of Project Security Process

### 5.5.1 Evaluation of Security Approaches.

A qualitative evaluation of the security approaches will be possible if the security process and security mechanisms could have been tested and certified after the System is fully developed and being deployed by the Supplier. In that case, quantitative evaluation of mechanisms could have been successful in giving us realistic figures by using defined test cases. But for now, the comparisons and analysis will be considered sufficient in evaluating the proposed approach.

- Proposed approach is different from ad-hoc approaches ***since it requires establishing a security team for security project management***. By establishing such a team resources, time and people could be assigned for security in the project. In another saying, specialists in security help to create an efficient and effective security system.

- Since there is a team for ***security, integration of system components with security components will be easy.***

- Proposed approach takes ***SSECMM (System Security Engineering Capability Maturity Model) and RFC2828 as a guide to enhance the degree of security in the system***. An ad-hoc process is not used to develop security in the system.

- Security requirements are specified taking user needs into account. Since ***users are involved in the analysis, requirements are specified more properly***. Since requirements are detailed, they will be probably more easily validated.

- An effective analysis ***of security requirements will help to specify other system requirements efficiently and effectively.***

- ***In order to apply multi level access control for compartmented data groups and roles are defined.*** Specification of objects help to define the relations and transactions between them effectively.

- In the proposed approach ***the policies, directives and manuals of TLFC are taken into consideration to establish a customized security for the needs of TLFC***. This reality will probably cause a system with high cost but also with a high assurance.

- While deciding on security mechanisms, rather than placing the probable mechanism to a SW or HW, ***the security mechanisms dictated by security policy and model are used to provide an optimum security level***.

- Since security services are in the Level 0 in the proposed process, ***while specifying the requirements all of the security services are considered to minimize possible threats.***

- To implement multilevel security in the system. ***Object and subject identifications are specified; a model that meets the requirements of compartmented information and Military Information Model is used.***

- As the last point, ***requirements in TCSEC, security evaluation standard that is accepted and applied in TLFC too, conform***

***to our application of proposed approach. Requirements about Security Policy, Marking, Identification Accountability and Assurance are provided in the proposed system.***

# CHAPTER 6

## 6 CONCLUSION

In this study a security engineering approach, which is based on Multi Level Security (Military Security Model) and which will help TLFC to prepare for DIW is proposed. In the limits of the approach security analysis and design phases are partially applied for a TLFC project.

In thesis studies a general literature review of IW is presented first, then the definition, forms, reasons for the future of IW, the risks, advantages of IW and the past incidents and examples regarding military and public sector organizations are reviewed. At the end of the chapter the requirements for DIW are specified generally.

Basic concepts of security, general risks threats on security of the TLFC are reviewed in Chapter 3. General description of a secure system is defined. Security engineering process is considered and the advantages and disadvantages of different processes are reviewed.

An application of security requirements specification and design for a TLFC information system project is presented in the succeeding chapter. A security policy, security policy requirements, access control and authorization models of the system are specified and a comparison of the proposed process with the actually applied ad-hoc approach is presented.

The proposed approach in broad terms seems to be applicable to any security engineering process. Nonetheless the approach is especially suitable to be applied on military security model and Multi Level Security. The applied part of the approach is a beginning towards implementing Multi Level Security in TLFC. The term was usually referred but beyond that was never applied in a real project before. This study also warns TLFC against

the possible threat in terms of IW. While digitalizing and automating its information systems, TLFC must keep in mind that by doing so, it is also creating some vulnerability along with its strengths.

Finally, the proposal is applied to a case study problem. After stating the current application and its results, the proposed and applied approaches for information system security development are compared and evaluated regarding current approaches reviewed.

The evaluation criteria of this case study are divided into two sub-titles: the activities of security engineering and security engineering process. The comparative evaluation of those subtitles is summarized in Table 5.1 and Table 5.2.

The security activities approach of the current applications is far less comprehensive than the proposed applied approach. It can easily be seen that the approach of the current application are not sufficient in securing the projects.

At last the project security processes are compared. Since there is no defined security process in current projects it creates security risks for current projects. It can be said that a procedure that is based on experiences are implemented during current process.

When the project security teams are compared, since there was no independent project security team in current approaches, the advantages of the proposed approach can also be easily seen.

The objective of this thesis was to investigate current IS security and IW problems in the TLFC and to propose a standard approach to alleviate experienced problems and risks. Even though there are great studies about IW and related topics, awareness for the undiscovered topics is one of the important objectives of the thesis. An application to practice multilevel security in a project is the beginning for the design of secure information systems. Besides this definition of an approach will help to describe the way for securing information systems in the context of DIW.

It is obvious that professional coordinated teamwork, a standard approach, and the most important one, the awareness of security in project management is necessary for the success of securing IS projects in TLFC.

It was seen that the fundamental problems are originating from the personnel who have insufficient skills and experience in such projects. Because of the lack of information, personnel avoid using definite statements in the specifications and the contracts. As we have concluded in case study, ***contracts are important in security requirements of IS, since large-scale IS projects are usually outsourced.***

Even though the case study of the proposal is based on an actual application, the results of the proposed approach could not be examined and evaluated via an application. Instead of it the probable results have been reviewed.

The proposal concentrated on the answer to the question: “What to apply?” but it can be observed that in chapter 4 the answer to the question: “How to apply?” is explained in a limited scale but explicitly.

Security could be considered as one of the quality elements in the system. The quality of security engineering process in that sense guarantees the quality of the products and services. Standard metrics could be very beneficial for DIW. Capability Maturity Model (CMM) gives the assessment models for software development and software acquisition. SSECMM (System Security Engineering) CMM and Software Acquisition CMM (SA-CMM) could be fruitful in the process of defining the system.

SSECMM covers the entire life cycle, the whole organization, and concurrent interactions with other disciplines and interactions with other organizations. With that feature it helps the organizations to improve their development process for security. Hence security teams and project teams in TLFC must take SSECMM along with other security evaluation criteria and standards in order to apply a defined process.

After completing this study even though a beginning is completed successfully, it can neither be assumed that information security for the TLFC

is fully provided nor an optimum security engineering process is applied. To fill the gaps in this study a future work is needed. Future work must be analyzed in two sections. Firstly IW activities must be investigated, then in this context DIW and IS security specific issues must be reviewed. Mainly ***other two areas of SSECMM, which were not covered in this study, risk and threat management and security assurance must be integrated to the approach and all the steps of engineering and development***, rather than analysis and preliminary logical design, phase must be applied to a project.

As the beginning **vulnerability and threat analysis for IS functions and IS projects in the TLFC or in the related department of the TLFC must be conducted**. This study will make the threats and vulnerabilities in Information Security realm clear. The same exercises like “Eligible Receiver” [RAND1997] and others must be conducted for the TLFC and the possible impact of IW activities on Defense Information Infrastructure must be pinpointed along with the vulnerabilities. There is no end for the needs for defensive digital warfare operation like it is in every economical fact for that reason realistic vulnerability assessment and vulnerability avoidance is important. Therefore the consequences of a possible IW activity must be assessed in multi-dimension and if possible **a threat matrix must be prepared**. In the matrix threats, possibilities of those threats and their consequences must be stated explicitly.

After that assessment risk management activities must be conducted for the systems. Realistic risk evaluation for security must be made. This study will reveal the most possible threats, possible loss and the consequences after those possible threat activities. Beyond that, before the beginning of every project risk plan for accomplishing security engineering process itself in that project must be done.

Security Policy Preparation and design phase must be gone through under the light of the information that comes from vulnerability assessment and risk management.

**There must be some changes in the organizational structure of the TLFC for conducting defensive IW**. New sections and headquarters must emerge for the IW and information systems like J6 departments. The number of these departments must certainly increase and beyond the headquarters the concept of "information warfare corps" must become a reality. These corps is now available in U.S.A. especially under the organizational structure of Air Force, like 609$^{th}$IW Squadron (IWS) based in South Carolina.

As for Information Security specific issues the beginning in **Multi Level Security (MLS) application must be developed and applied in IS projects** by taking TCSEC into account as:

1. Security policy for every project must be stated and the policy must be consistent with institutional policy and in itself.
2. Objects and the subjects in the system must be identified.
3. Labels for objects and clearances for subjects must be determined associated and marked according to the security policy.
4. Audit information must be kept in the system.
5. Evaluation of mechanisms must be done and security assurance must be provided.
6. Continuous protection for the mechanisms must be the aim.
7. Possible documentation must be submitted to users and officials.

Main current problem in MLS is the problem of processing Top Secret labeled objects according to manuals in the systems. **In order to overcome this issue, national system that will support B1 degree in TCSEC must be designed and developed**. Also decision for processing them manually or automatically must be made by the authorities.

If there is not an institutional policy it must be prepared immediately in order to implement regulations and directives.

Verification test for security in defensive IW could be accomplished by the help of a so-called red team. This team looks for the vulnerabilities in the

system and tries to create threat incidents in the system in order to prevent security flaws in the system.

Evaluation and accreditation of security must be made by independent expert groups in the TLFC. Security must not be violated during those studies.

Security is an underestimated issue in system engineering since it is regarded usually as a cost element. But in government organizations, especially in Armed Forces, cost must be regarded as a secondary issue especially in security realm.

While implementing security to an IS, getting the objectives or in other words efficiency of the system must be the primary issue during system development. Hence while taking cost and functional requirements into account the aim must be to build a not overestimated secure system.

Self-dependency is another concern in security engineering. Therefore TLFC must take necessary steps to establish its own Information Systems Security Structure in which training, project management and development could be done independently.

As the final conclusion to integrate and coordinate security of IS projects a centralized project office that will work with a decentralized nature will be successful. ***Domain experts for different projects will be necessary but a centralized office will specify the requirements better, will know much more about other TLFC projects and will not start the work from scratch for every project***. Besides security it will reduce the risks in other project management and outsourcing problems.

# REFERENCES

[ACM5], Proceedings of the 5th Conference on Computers and Communications, ACM Press.

[ACM7], Proceedings of the 7th Conference on Computers and Communications, ACM Press.

[Adams1998] Adams, James; The Next World War, Computers are the weapons and the frontline is everywhere, Simon&Schuster, 1998.

[Anderson2001] Anderson, Ross; Security Engineering, A Guide to Building Dependable Distributed Systems; John Wiley&Sons, Inc., New York; 2001.

[Arquilla1993] Arquilla, John and Ronfeldt, David; Cyberwar is Coming, Comparative Strategy, Spring 1993

[Aspin1994] Aspin, Les; U.S Secretary of Defense, Annual Report to the President and the Congress, 1994

[Beckett1997] Beckett, Brian; Introduction to Cryptology and PC Security; Mc Grew-Hill Companies; London; 1997.

[Denning2000] Denning, Dorothy E.; Information Warfare and Security, Addison&Wesley, 2000.

[DoD1997] DoD, Joint War Fighter and Technology Plan, 1997

[Ford1994] Ford, Warwick; Computer Communications Security, Principles, Standards, Protocols, and Techniques; Prentice-Hall Incorporation; New Jersey; 1994.

[FM34-1] Field Manual FM 34-1, Intelligence and Electronic Warfare Operations, Headquarters Department of Army.

[Franks1994] General Franks, Frederick M., Winning the Information War, A speech delivered to the Association of the U.S. Army Symposium, 1994.

[Friedman1998] Friedman, George; Friedman, Meredith; The Future of Warfare, St. Martin's Griffin, 1998.

[IEEE1995] Abrams et al; Information Security, An integrated collection of essays, IEEE Computer Society, 1995, p330-350.

[Kazaz1998] Kazaz, Harun; Cyber sabotage is not a farfetched reality for Turkey, Turkish Daily News, 11,07,1998.

[KEISIAM] KEİS İş Akış Modelleri; Odtü Enformatik Enstitisü, 2002

[KEISMPL] KEİS Master Planı (Not available for public release)

[KHO1992] Kara Harp Okulu Komutanlığı; Sistem Mühendisliği Tanıtım Broşürü, 1992.

[Laudon1998] Laudon, Kenneth C; Laudon, Jane P.; Management Information Systems, New Approaches to Organization and Technology, Prentice Hall, 1998.

[Libicki1995] Libicki, Martin; What is Information Warfare, National Defense University, 1995.

[386-8A], MST 386-8 (A), Otomatik Bilgi İşlem Güvenlik Standardı. (Not available for public release).

[Novlin1998] Novlin, David V. and J.Stupak, Ronald; War as an Instrument of Policy, Past, Present and Future; University Press of America.

[Pfleeger1997] Pfleeger, Charles P.; Security in Computing; Prentice-Hall; New Jersey; 1997.

[Pressman2000] Pressman, Roger S.; Software Engineering, A Practitioner Approach, McGraw Hill; 2000.

[RAND1997] Arquilla, John and Ronfeldt, David; In Athena's Camp, Preparing for Conflict in the information Age, National Defense Research Institute, 1997.

[RFC2828] The Internet Society; Request For Comment: 2828; 2000.

[Saltzer1975] Saltzer, Jerome and Schroeder, Micheal; The Protection of Information In Computer Systems; Proceedings of IEEE; Volume 63, No: 9, September 1995; p: 1278-1308.

[Sandhu1994] Sandhu, Ravi and Samarati, Pierangela; Access Control: Principles and Practice; IEEE Communications Magazine; September 1994; p: 40-48.

[Sandhu1996] Sandhu, Ravi and Samarati, Pierangela; Authentication, Access Control, and Audit; ACM computing Surveys; Vol. 28; March 1996; p: 241-243.

[Schwartau1994] Schwartau, Winn; Information Warfare, Chaos on the Information Superhighway, Thunder's Mouth Press, 1994.

[SSE-CMM1999] SSE-CMM; System Security Engineering - Capability Maturity Model; Model Description Document; Version 2.0; 1999.

[Stallings1995] Stallings, William; Network and Internetwork Security, Principles and Standards; Prentice-Hall; New York; 1995.

[TCSEC] NCSC (National Center for Computer Security); Trusted Computer Security Evaluation; Orange Book; DoD 5200.28.

[Waltz1998] Waltz, Edward; Information Warfare; Principles and Operations; Artech House; 1998

[114-1B], MY 114-1B, Silahlı Kuvvetler İstihbarat, İKK ve Koruyucu Güvenlik Yönergesi (Not available for public release).

[227-1A], MY227-1A, Silahlı Kuvvetler Rapor Yönergesi (Not available for public release).