Journal of Applied Mathematics & Bioinformatics, vol.3, no.4, 2013, 207-211
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2013

Communications and information security: Case study military systems

Peter Stavroulakis[1]

Abstract

In this paper we present in a tutorial the field of Communications and Information Security as it applies to the design of secure large scale communications systems as they are used in military systems.

1 Introduction

The Subject of information and communication security, the transfer of accurate and uncompromised information as well as the secure transfer of information has become an International issue ever since 31of December of 1999. The year 2000 scare which has been coded as the Y2K scare refers to what prominent scientists and business people feared that all computer networks and the systems that are controlled or operated by them could break down with the turn of the Millennium since their synchronizing clocks could lose synchronization by not recognizing a number (instruction) with three zeros. A positive

[1] Military School on leave from ECE, Technical University of Greece.
E-mail: pete_tsi@yahoo.gr

Article Info: *Received* : August 1, 2013. *Revised* : October 20, 2013.
Published online : December 10, 2013.

outcome of this scare was the creations of the various CERTS (Computer Emergency Response Teams) around the world which now work cooperatively to exchange expertise, information and be coordinated in case of major problems arise in the modern IT environment. On the military front in which the legality of actions taken is of secondary importance the entire field converged into a new philosophy coined as Information Warfare. After the second World War with the technology advancement on unprecedented heights it was considered that the a technological advantage it was simultaneously translated to a war advantage and thus the World power proceeded in a ever more expensive pace in employing technological innovations to Military Systems under the doctrine of Star War. Very soon it was proved that technology advantage is ephemeral, its implementation and deployment in military system design very easily copied and for the time limitation of real battle period, the most important element is the information advantage. Going back to the ancient Chinese (Sun Tzu) and Trojan War Doctrine which defines the Information Warfare.

<<……Knowing the enemy and knowing yourself in a hundred battles you will never know peril. When you are ignorant of the enemy but know yourself your chances of winning or losing are equal. If ignorant of both your enemy and yourself in every battle you will be in peril…..>>.

In this paper we present in a tutorial the field of Communications and Information Security as it applies to the design of secure large scale communications systems as they are used in military systems. Another example that this field finds applications is in the design of multimedia large scale security systems as is the security network of Olympic Games. The similarity of the applications of CIS to Olympic Games and military systems is based on the following characteristics. In both cases multimedia systems are used in every case, the time limitation for processing and the exactness of the information received is of paramount importance, the network uncompromisability and resiliency is

necessary in addition to the fact that in both cases the legality of actions taken is suspended.

Information transfer in a multimedia environment to satisfy the requirements of an integrated military system used in a battle uses the infrastructures of the modern information environment consisting of the interdependent network of information technology infrastructures (IT) including both private and public networks such as the internet, computer systems, integrated sensors, system control networks and embedded processors and controllers as explained in the following under the context of security. The now ambiguous term as Cyberspace and information warfare has become a conventional means to describe anything associated with computers, information technology and the internet which is coined as the cloud in modern computing. The OSI seven layer Model below is used to indicate main system vulnerabilities which include the multimedia network, the information transfer and security and the way that can be faced layer by layer with reference to security.

2 OSI Model

With modern analytical tools, information networking has been based on a seven layer model–the open systems interconnect (OSI) Seven Layer Network Model as shown in Figure , [3].

The above model concept will be used in this paper in the context of information security in a multimedia environment. It presents concisely what technological parameters are critical in communication and information security and that the layer by layer approach to security is the most appropriate in order to make sure that all possibilities for security compromise are covered. This approach also helps the technologists to offer a cure and face effectively a specific

threat instead of using a trial and error approach without any real results. This model also helps us determine whose responsibility is any specific action required.

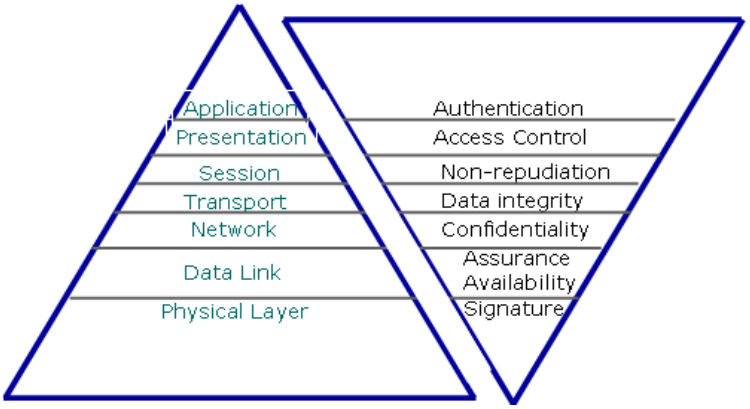

Figure 1: OSI Model

We thus have to analyze vulnerabilities of each layer related to security and develop specific controls to avoid security compromises. This model more or less presents the specific response of the technology to various security threats at each layer. In the paper we shall take each layer and examine it on the basis of its formal definition, its practical place in the network and present possible controls for possible relevant risks and threats and how technology and new theoretical developments can be applied to design a secure information and communication system that can be used even for a military environment.

References

[1] P. Stavroulakis, *Communication and Information Security*, Special Issue, China Communication, February 2007.

[2] P. Stavroulakis, *Terrestrial Trunked Radio-TETRA, A global Security Tool*, Springer, 2007.

[3] P. Stavroulakis and M. Stamp, *Communication and Information Security*, Springer, 2010.