to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented.

There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well-developed process. There isn't a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design.

When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.

When developing a secure network, the following need to be considered [1]:

1. Access – authorized users are provided the means to communicate to and from a particular network
2. Confidentiality – Information in the network remains private
3. Authentication – Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refute that he used the network

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack [1]. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavor.

To lessen the vulnerability of the computer to the network there are many products available. These tools are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Businesses throughout the world are using a combination of some of these tools. "Intranets" are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the internet greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself.

The types of attacks through the internet need to also be studied to be able to detect and guard against them. Intrusion detection systems are established based on the types of attacks most commonly used. Network intrusions consist of packets that are introduced to cause problems for the following reasons:

- To consume resources uselessly
- To interfere with any system resource's intended function
- To gain system knowledge that can be exploited in later attacks

The last reason for a network intrusion is most commonly guarded against and considered by most as the only intrusion motive. The other reasons mentioned need to be thwarted as well.

1. Brief History of Internet

The birth of the interne takes place in 1969 when Advanced Research Projects Agency Network (ARPANet) is commissioned by the department of defense (DOD) for research in networking.

The ARPANET is a success from the very beginning. Although originally designed to allow scientists to share data and access remote computers, e-mail quickly becomes the most popular application. The ARPANET becomes a high-speed digital post office as people use it to collaborate on research projects and discuss topics of various interests. The InterNetworking Working Group becomes the first of several standards-setting entities to govern the growing network [10]. Vinton Cerf is elected the first chairman of the INWG, and later becomes known as a "Father of the Internet." [10]

In the 1980s, Bob Kahn and Vinton Cerf are key members of a team that create TCP/IP, the common language of all Internet computers. For the first time the loose collection of networks which made up the ARPANET is seen as an "Internet", and the Internet as we know it today is born. The mid-80s marks a boom in the personal computer and super-minicomputer industries. The combination of inexpensive desktop machines and powerful, network-ready servers allows many companies to join the Internet for the first time. Corporations begin to use the Internet to communicate with each other and with their customers.

In the 1990s, the internet began to become available to the public. The World Wide Web was born. Netscape and Microsoft were both competing on developing a browser for the internet. Internet continues to grow and surfing the internet has become equivalent to TV viewing for many users.

2. Security Timeline

Several key events contributed to the birth and evolution of computer and network security. The timeline can be started as far back as the 1930s.

Polish cryptographers created an enigma machine in 1918 that converted plain messages to encrypted text. In 1930, Alan Turing, a brilliant mathematician broke the code for the Enigma. Securing communications was essential in World War II.

In the 1960s, the term “hacker” is coined by a couple of Massachusetts Institute of Technology (MIT) students. The Department of Defense began the ARPANet, which gains popularity as a conduit for the electronic exchange of data and information [3]. This paves the way for the creation of the carrier network known today as the Internet. During the 1960s, the Telnet protocol was developed. This opened the door for public use of data networks that were originally restricted to government contractors and academic researchers [3].

During the 1980s, the hackers and crimes relating to computers were beginning to emerge. The 414 gang are raided by authorities after a nine-day cracking spree where they break into top-secret systems. The Computer Fraud and Abuse Act of 1986 was created because of Ian Murphy’s crime of stealing information from military computers. A graduate student, Robert Morris, was convicted for unleashing the Morris Worm to over 6,000 vulnerable computers connected to the Internet. Based on concerns that the Morris Worm ordeal could be replicated, the Computer Emergency Response Team (CERT) was created to alert computer users of network security issues.

In the 1990s, Internet became public and the security concerns increased tremendously. Approximately 950 million people use the internet today worldwide [3]. On any day, there are approximately 225 major incidences of a security