Chapter 13
A Framework for Internet Security Assessment and Improvement Process

Muthu Ramachandran
Leeds Metropolitan University, UK

Zaigham Mahmood
University of Derby, UK

ABSTRACT

Internet security is paramount in today’s networked systems, especially when they provide wireless application access and enable personal and confidential data to be transmitted across the networks. Numerous tools and technologies are available to ensure system security, however, external threats to computer systems and applications are also becoming more and more sophisticated. This chapter presents a framework that consists of two components: (1) an assessment model to look at the existing security infrastructure of an organisation to determine its security maturity level; and (2) a process improvement maturity model to suggest an improvement mechanism for the organisation to progress from one maturity level to the next higher level. The intention is to provide a framework to improve the organisation’s Internet and network security so that it becomes more efficient and effective than before. The improvement process model is a 5-stage framework, which has the potential to be established as a standard maturity model for assessing and improving security levels in a manner similar to other software process improvement framework such as CMMI. Preliminary results, based on looking at the existing security measures of one particular organisation, reveal that there is indeed a need for an appropriate model such as the one being proposed in this chapter.

INTRODUCTION

In the information society of the 21st century, the information and communication technologies have revolutionised human lives. Wireless telephony, electronic commerce and online transactions are now common place and within easy reach of general public. All this has become possible through the proliferation of computing technologies and use of the Internet. There is no doubt that World Wide Web, or the Internet, is the binding and enabling force behind all this.
Since the use of the Internet is growing, the demand for the associated products, applications and services is also growing. As a bi-product, the concerns with respect to the security of information, confidentiality of data and reliability of services are also growing. Previously, when the computing systems were used as standalone devices, the security concerns amounted to only the physical security (i.e. fear of getting it damaged, getting it stolen, etc). Now, however, because of interconnectivity of computing equipment on a global basis, there are serious concerns with respect to security of networks (including the Internet), theft of data, cyber terrorism and so on. Although, network managers and security experts are doing their best to ensure that transactions are safe, networks are secure and malicious damage to data, services, applications and equipment is eliminated, hackers and cyber terrorists are also becoming more intelligent and finding new ways of breaking and getting into computing systems. The technologies that exist for the benefit of citizens are, ironically, the same technologies that hackers are using for their malicious acts. To ensure the security of internet applications and the use of internet, many approaches has been employed including systems such as the following:

- Intrusion detection mechanisms
- Intrusion prevention schemes
- Firewalls and Filters
- Virus detection and removal software

However, these mechanisms have limitations. In this context, the biggest challenge is to develop and apply appropriate internet security strategies consistently and uniformly across the entire network and ultimately to individual nodes of a network.

The aim of the current study is to suggest a framework for the Internet security and the security of an organisation’s use of Internet - along the lines similar to software process improvement frameworks such as CMMI (SEI, 2005).

The framework being proposed has two aspects to it:

- **Internet security assessment model:** Here, the intention is to understand the current security situation of an organisation to identify the strengths and weaknesses of the existing security practices in the organisation.

- **Internet security improvement model:** Here, the intention is to assess the security maturity level of the organisation and recommend ways for improving the security posture of the organisation and methods of implementing it.

In the rest of this chapter, we first discuss various aspects of internet security in “Internet Security.” Then, we present the internet security assessment process in some detail in “Security Assessment and Improvement Process” and “Proposed Framework for Security Improvement.” In “Preliminary Results”, we summarise results of a simple experiment. That follows the conclusions in “Conclusion.”

**INTERNET SECURITY**

**Types of Security Threats**

With the proliferation of computing, internet and wireless devices as well as their connection to the World Wide Web, security has become an issue of serious concern with respect to the following three core areas:

- **Confidentiality:** ensuring that data and information resident on computing systems and being transmitted over the networks are protected from access by unauthorised persons

- **Integrity:** ensuring that data and information resident on computing systems and