Chapter 24
MCOQR (Misuse Case-Oriented Quality Requirements) Metrics Framework

Chitreshh Banerjee
Amity University, India

Arpita Banerjee
St. Xavier's College, India

Santosh K. Pandey
Ministry of Communications and IT, India

ABSTRACT

In today's information age, software is attacked deliberately resulting in breach of security & people's trust. These malicious attacks provide harm to individuals, organizations, and the world at large. The attacker targets vulnerabilities to exploit the software. The chapter highlights the importance of security metrics which is comprehensive in nature and easily implementable. It also emphasis on the early implementation of security metrics i.e., from the requirements elicitation phase of requirement engineering stage so that a comprehensive and complete set of security requirements could be defined with their countermeasure to develop a secured software. For development of security metrics a framework has been proposed using use case and misuse case tree modeling. The proposed work may help the Software Security Team to identify and analyse the potential vulnerabilities and associated threats which may be exploited by the attacker to harm the system well in advance in the requirements engineering phase thereby balancing the security using misuse cases modeling.

DOI: 10.4018/978-1-7998-3016-0.ch024

INTRODUCTION

In today's cyber age, the use of software is so important in today's human life that it has become an essential and integral part of it. In fact, the global economy is solely dependent on the synchronized and secured use of software. People's trust can only be gained if the software contains optimum level of security. When these software are targeted and attacked purposely to steal information of highly sensitive nature be it personal or official, the result is that people starts to lose trust. And, due to the breach of security, harm and damage is caused not only to individuals but the associations and organizations, nations are also affected.

Software contains vulnerabilities (security loop holes) and the attacker targets them to exploit the software. These threats endanger intellectual property and operation & services of any business organization. Since past few decades, serious financial damages were noticed and reported. Since 1977, security has been an issue and a major concern with incidents of security breach like intrusions, spam emails, virus attacks, denial of service, identity theft, hacking, racking, SQL injection, government-level top-security computer network's worm infiltration, debit & credit card related fraud and misuse, etc. according to Banerjee and Pandey (2009).

In the recent past, a newly detected ransomware variant pretends to be communication from US Department of Justice infected user's computer and exposure of Social Security numbers & other personal information were also reported. A summarized visuals below shows the various attacks, weaknesses and outcomes for the year 1999-2011 is shown below:-

As per statistics available in Banerjee and Pandey (2009), revenue loss due to piracy alone was estimated to have reached 51.4 billion dollars worldwide in 2009. In Asia-Pacific region the loss was estimated at 16.5 billion dollars as compared to 11.6 billion during 2006. Recently, in 2012, some phishing cases were reported with financial loss of approx. US $1 million in one case & US $1.3 million in another case.

In Information Technology area, security is said to exist in many form and types. Like, security can be classified into computer security, data security, software security, information security, network security, and web security. *Computer security* encompasses information & assets protection from security breach allowing them to remain accessible & productive to its intended users. *Data Security* encompasses protection of database(s) from unauthorised users. Information security encompasses information system protection from unauthorized access.

Software security encompasses areas like vulnerabilities, threats, attacks, etc. and implementation of security during the software development activities along with the measures of security aspect and if any security issue arises then to provide countermeasures which can minimize or prevent attacks & exploits. *Network security* encompasses monitoring & prevention of unauthorized access & misuse of the network along with its resources. *Web security's* aim is to define and draw protocols and measures which safeguards the system against attacks over the Internet.

As per available statistics, it has been estimated that around 90% of security incidents which are reported are due to the various defects and exploits left uncovered, undetected, and unnoticed during the various phases of the software development process. Implementing security in software provides assurance that the data in a system has a reasonable expectation of protection & privacy ensuring reliability, availability and integrity to the system as per Banerjee and Pandey (2009).