Chapter 65
Reviewing the Security Features in Contemporary Security Policies and Models for Multiple Platforms

Omkar Badve
National Institute of Technology Kurukshetra, India

B. B. Gupta
National Institute of Technology Kurukshetra, India

Shashank Gupta
National Institute of Technology Kurukshetra, India

ABSTRACT

Numerous vulnerabilities have a tendency to taint modern real-world web applications, allowing attackers in retrieving sensitive information and exploiting genuine web applications as a platform for malware activities. Moreover, computing techniques are evolved from the large desktop computer systems to the devices like smartphones, smart watches and goggles. This needs to be ensure that these devices improve their usability and will not be utilized for attacking the personal credentilas (such as credit card numbers, transaction passwords, etc.) of the users. Therefore, there is a need of security architecture over the user's credentials so that no unauthorized user can access it. This chapter summarizes various security models and techniques that are being discovered, studied and utilized extensively in order to ensure computer security. It also discusses numerous security principles and presents the models that ensure these security principles. Security models (such as access control models, information flow models, protection ring, etc.) form the basis of various higher level and complex models. Therefore, learning such security models is very much essential for ensuring the security of the computer and cyber world.

DOI: 10.4018/978-1-5225-3422-8.ch065

1. INTRODUCTION

In the contemporary era of World Wide Web (WWW), online Internet facilities are easily being accessible by every single human belonging to different community. A continued boom of social networking sites, online shopping sites, Internet banking and all other widespread modern web applications provide dynamic access of contents to the users and this has increased utilization of user generated HTML contents. Top vulnerabilities like Cross-Site Scripting (XSS) attacks (Gupta, 2015a; Gupta, 2015b; Gupta, 2015c; Gupta, 2015d) have turned out to be a plague for the modern web 2.0 applications. The exploitation of XSS attack is done by injecting the malicious JavaScript code (Gupta, 2016) on the injection points of vulnerable web applications (Gupta, 2012a; Gupta, 2012b; Gupta, 2014).

1. Need of Security

In initial computers, the need of security was limited to the data that is stored in the central computer servers. With the advancements in Internet and communication systems the need of security of messages has been becoming difficult and complicated. Today's computer systems must not be only preserve privacy of the data or messages but also the other factors like availability, integrity, non-repudiation etc. Basic security mechanism includes providing username and password to the authorized user; and using that information to authenticate the user. Another common method used is to encrypt the critical database and allow access to decrypt is only them who have the secret key. Organizations require more sophisticated and highly secure mechanisms that can successfully prevent the possible attacks.

Since the attackers are becoming more and more sophisticated, they do not need to go even outside to perform damage on their rivalry. In 1982 during the cold war, CIA injected the code into Siberian gas pipeline software system in Russia to allow it to malfunction which caused it to explode (French, 2004). In the world of Internet no one is secure, not even president of USA. In 2008 during presidency run, suspected hackers from China and Russia, attacked on computers used in campaigning of both Barack Obama and John McCain, which includes sensitive information such as emails and campaign data (Larson, 2013). Despite the fact that India is emerging as one of the biggest IT service providers, it hasn't escaped from cyber attacks. On July 12, 2012, emails of more than 10,000 people including government officials such as Prime minister's office, Defense ministers, external affairs, finance ministries and Intelligence agencies were hacked (Selvan, 2012). Big, famous companies are also not far away from these attacks. In 2014, eBay experienced very large attacks as attacker managed to steal personal records such as password, email address, physical address, phone numbers etc (McGregor, 2014). There are many incidents happening every day all over the world. According to the report generated by Kaspersky antivirus company (Funk, 2013), in the year of 2013 they managed to neutralize 5,188,740,554 number of cyber attacks on user computers and mobile devices. Therefore, it is stringent need of cyber security against these attacks.

2. Principles of Security

To understand the attacker and mode of attack we need to study the principles of security to tackle the problem of attack. Following are the major security principles that each organization has to consider before they make their data online. Table 1 summarizes all the principles of security.