Web Security: A Survey of Latest Trends in Security Attacks

Pranesh V. Kallapur and V. Geetha

Department of Information Technology, NITK, Surathkal, Karnataka, India
geethav.nitk@gmail.com, praneshvkallapur@yahoo.co.in

Abstract. Every system used in real time will be having some security threats. Internet has not been exception for it. From as early as 1980s there has been occurrence of several different types of security attacks with Internet being their major target. Internet happens to be main target due to type and amount of information it stores and advancements in computer networks which makes it very easy for accessing the same. Also, at the same time limitations/design flaws in Internet design, programming languages etc. make attack techniques to evolve from day to day. Due to such evolution of new attack mechanisms, at present, we have a big list of different attacks. Further, motivations for making such attacks range from just having fun to sabotaging critical & specific infrastructures at national level. Hence, in this context, it is very necessary and useful to know about latest trends in security attacks. In this connection this paper provides a brief survey of latest security attacks on web. This paper also provides a summarized comparison of discussed attacks against chosen important parameters. In addition, an observational data about attacks via Emails over a period of time is also presented. The paper concludes by mentioning the need of such surveys and research opportunities in this area.

Keywords: Network, Security, Security Attacks, Web Security.

1 Introduction

Security is a very important aspect, be it with respect to a living or non-living entity. Security gains high importance as the nature of system or information handled by system becomes sensitive. Both individual computer system and Internet as a whole has constantly been the target of cyber-attacks. Intentions of attacks vary widely while ranging from disruption of service to stealing confidential information for abuse, bringing down entire communication infrastructure, sabotaging important national infrastructures etc. The cyber-attacks range, in terms of skill level required, from very simple [6] to very skilled works [13]. From the point of view of infrastructure involved these attacks may need nothing beyond a computer system with network access [6], [7], [8], [11], [12] to very large dedicated setup like in case of Stuxnets [13].

In the rest of this paper, section 2 gives related work, section 3 gives brief details about important cyber-attack techniques; section 4 gives comparison of discussed cyber-attack techniques against some useful parameters and observational data about attacks via Emails. Paper is concluded by mentioning the need and importance of research in this area.

Y. Wu (Ed.): Advances in Computer, Communication, Control & Automation, LNEE 121, pp. 405–415.
springerlink.com

2 Related Work

There has been a lot of work with respect to each type of cyber-attack in terms of studying its realization, detection and prevention plans etc.

Control hijacking has been one of the oldest and yet simplest way of realizing a cyber-attack. Latest study in this regard being [25] with clear explanation of how buffer overflows can be realized and used for attacking. DoS/DDoS has also been under enough investigation, especially for Low Rate DoS as in [26]. Rootkits, from the point view their attack style, extent of damage that can be caused and countermeasures, has been discussed in detail in [22]. Malware and Spams have also been surveyed already by analyzing their way of working, infection etc, with respect to social engineering sites like Facebook as detailed in [27]. Other two latest trends in cyber-attacks, namely Botnet and Stuxnets, have also been studied elaborately in [23], [24] respectively.

A point to be noticed from all these existing works is that they discuss, to the possible extent, about a particular type of attack along with any of its variants. In this connection, motivation of our paper has been to provide a survey on different types of cyber-attacks, covering as many aspects as possible for each type of attack.

3 Trends in Cyber Attacks

In this section major types of security attacks are discussed with respect to major features like its brief history, mechanism of developing attack, infection mode, targets, damage caused along with suitable examples wherever applicable.

3.1 Control Hijacking

The major goal of such attacks is to take over the target machine. This kind of take over is achieved by executing arbitrary code by hijacking application control flow. But, there must be some means for enabling attacker to execute arbitrary code on target machine in order to do this kind of controlhijack. Execution of arbitrary code in such cases is achieved by using language shortcomings or some other sorts of programming mistakes [1, 25].

General technique for attack involves following steps:

1. Understand stack frame structure and contents
2. Choose a convenient buffer, normally lying adjacent to return addresses or virtual table pointers
3. If no such buffer exists, try placing malicious buffer surrounded by objects/stack contents of interest by using sequences of memory allocation and free calls.
4. Provide contents for chosen buffer to cause overflow causing corruption of stack frame, return address, virtual table pointer, function pointers, or spraying shell codes arbitrarily in heap area[1], [2], [3], [5].

Above mentioned steps 1, 2 and 4 are common to buffer overflow, heap spray, and integer overflow based techniques. Optionally, attacker may also, in case of heap spray and vtable pointer corruptions, place malicious pointer to open shell, instead of