A Study of Cyber Security in Web Environment

Leena Chopra*
Tripti Lamba**

Abstract

Over the last few years, threats in cyberspace have risen dramatically. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow the smooth working of infrastructures in any organization. Since cyberspace is widely adopted and used worldwide, there is need of healthy functioning of cyberspace in terms of economical and national security. There are number of policies, strategies, actions that are taking place to reduce the threat of cybercrime in Today's world. This paper focuses on the "Need of Cyber security" and various areas of emerging technologies where Cyber Threats exist in different forms. Some of the crimes in various areas that occurred are also studied.

Keywords: Cyber world, Cyber security, Cyber Threats, Cyber attacks

Introduction

Cyber in "Cyber Security" prefix is a word that means Computer, Computer networks, and Security means safety, protection, freedom from risk, danger, crime etc. Cyber Security can be defined as a process of protecting the Cyber Space i.e. computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals. The need and importance of cyber security is discussed and then focus is given in the emerging technologies like Social computing/networking tools , Mobile platforms ,Cloud computing, Virtualization, Service-oriented architecture (SOA) where cyber threats are involved and most risky emerging technologies was discussed.

Need of Cyber Security

With the advent of latest technologies (Virtualization, Cloud Computing, Mobile Computing etc.) in the areas of Computer, there is growing need to secure, protect the cyber world from the threats, risks. This need of Cyber security arises due to following main areas of considerations:

Leena Chopra*
IITM, GGSIPU
Tripti Lamba**
IITM, GGSIPU

Growing number of users

First, there are a growing number of individuals who use the Internet, and many of these new users are unfamiliar with risks in cyberspace. To illustrate, the number of Internet users around the world in 2000 was approximately 361 million; at the end of 2013, the figure had grown to 2.8 billion. As the number of users on this cyber space is increasing day by day there is greater possibility of vulnerability which can be related to hardware, software, network, organizational etc.

Increased number of cyber applications

The number of cyber-related applications has increased steadily over the past two decades. When the Internet was first developed by the Defense Advanced Research Projects Agency (DARPA) in the late 1960s, its developers could not have comprehended the number of video, voice, and e-service applications that would be laid in the future. As more individuals rely on services such as e-commerce and e-banking, the greater is the risks to society. A greater dependence on Internet-based services also attracts criminal groups which seek new avenues to make money. Criminal groups are continually sightseeing new ways to hack into technologies such as credit cards, automated teller machines (ATMs), and Radio Frequency Identification Devices (RFID).

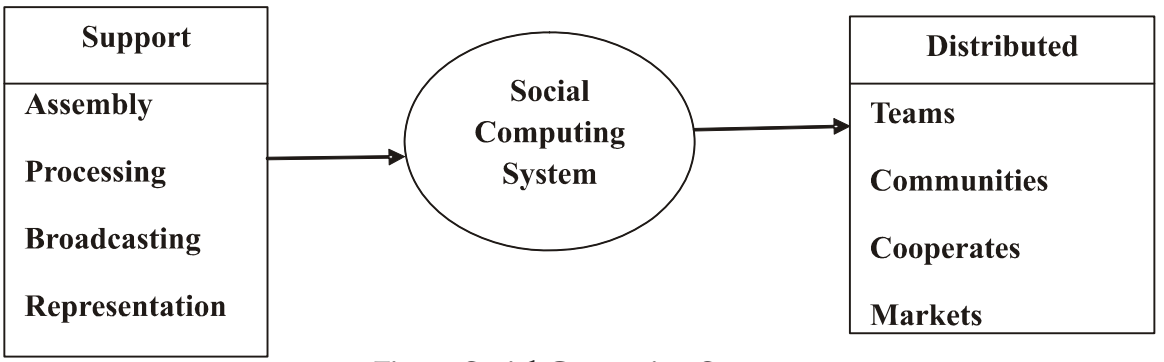

Fig. 1: Social Computing System

Use of Critical Infrastructures and Technologies

Massive growth of the Internet aided by emergence of cloud computing and mobile devices has imposes new requirements and challenges related to cyber security. From network related threats such as bots and denial of service attacks to privacy related concerns such as side channel attacks, cyber security enforces requirements of diligence and effectiveness on Internet-based systems.

Malicious Cyber Activities are Easier to Execute

Malicious cyber activities are becoming more sophisticated and easier to execute. Individuals interested in mounting a cyber attack do not need to have any advanced knowledge of computer programming, as they can purchase off the-shelf crime kit tool ware. An example of such program is the Zeus crime kit whose malicious code can be customized.

Individuals Threatening Cyber Space

There is a wide range of individuals and groups who may be interested in using cyber space for questionable objectives. While there is a tendency to focus on specific groups such as organized crime seeking financial gain and terrorists who might utilize the web to communicate and spread their ideologies, there are other profiles of individuals who could threaten cyber security. These include organizations and groups interested in accessing sensitive information from government sources or international organizations. There are numerous categories of individuals and groups who could threaten cyber space. These include script kiddies, hacktivists, and botnet operators. Complicating the threat picture are the groups' different motivations and methodologies to reach their ends. The above study is as per the reports cited in links in section [1, 2, 5].

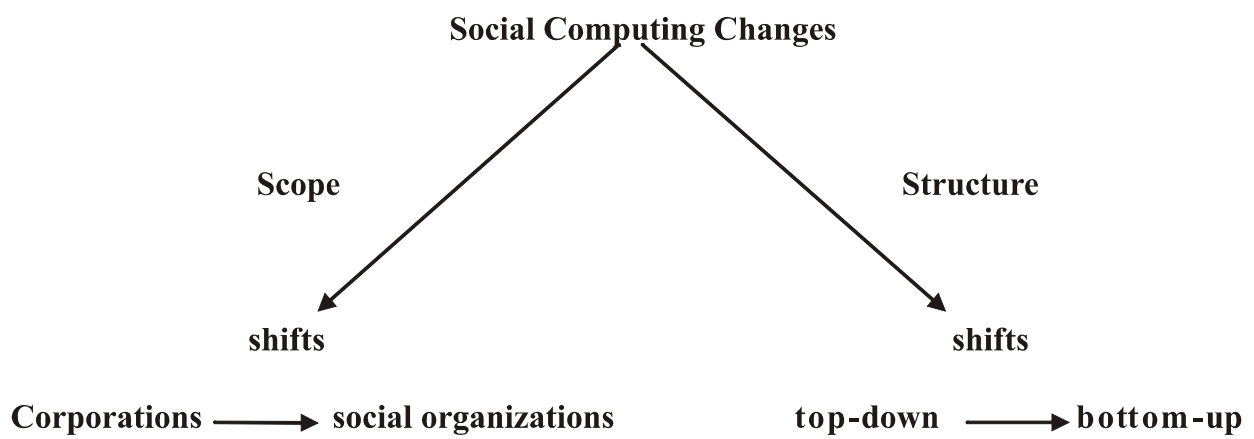

Fig. 2: Social Computing Trend

Emerging Technologies where Cyber Threats are involved

Social Computing/Networking Tools

Social computing refers to the use of "Social software" and enables people to connect or collaborate through computer-mediated communication and to form online communities. Social Computing System is shown in Fig. 1.

The 21st Century has seen dramatic shifts in business computing as shown in Fig. 2.

History of Social Networking

- **Social Networks 1.0**
  - Social Networks 1.0 were built during the late 1990s
  - Services like eGroups/OneList, ICQ, Evite
- **Social Networks 2.0**
  - Social Networks 2.0 began in the early 2000s was to enable the creation, growth and management of an explicit social network
  - Services like Friendster, Tribe, Facebook, LinkedIn
- **Social Networks 2.5**
  - Services like Bebo, MySpace, YouTube
- **Social Networks 3.0**
  - Allow members to link up to each other at different sites
  - Connect to any site using an Open Identity standard (OpenID) and get access to forum, blogs, wiki etc

Object Centred Sociality

- Users connected via a common object e.g. Job, University, Hobby
- Simulates real-life social interaction

Network Integration

- The Problem with the network integration is that users may have identities on different Social Networks and each identity has to create from scratch.
- The Solution with the network integration is that allow user to import existing identity and use single global identity with different views

Mobile Platforms

Mobile phones have become an indispensable and easiest way of communication today for everyone. **Mobile security** is important in mobile computing as it contained sensitive information to which access must be controlled to protect the user and the company data.

These technologies are causing weighty changes in the organization and have become the source of new risks. The risk/target can come from the means of communication like SMS, MMS, Wi-fi networks, and GSM. These attacks exploit software vulnerabilities from both the web browser and operating system.

Cloud Computing

Cloud Computing is a general term that provides hosted services over internet. Broadly speaking, these services are divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). IaaS provides physical resources such as CPU, network and storage etc. PaaS provides a platform for execution of application. SaaS provides different type of application and web services to the end users. The concept at the basis of Cloud Computing is the idea of moving from an "IT as Architecture" approach to an "IT as Service" approach. More generally, under this name can be grouped anything that involves delivering hosted services over the Internet.

One of the advantages of Cloud is, in fact, the possibility of enhancing the IT level of a company, while at the same time taking under control the costs of the investment (no internal infrastructure to be maintained, reduced need of IT personnel, reduced need for security personnel etc. Cloud Computing

is emerging approach because of high availability, efficient cost and performance. In Cloud Computing, service providers will provide the storage for data along with services. But due to lack of proper security policies, many business companies are reluctant to adopt the Cloud Computing technology. Findings gathered from link [6].

From a technical point of view, the main security challenges are due to the fully distributed nature of the cloud [6]. Some of the security issues that exist in Cloud Environment may be:

- Authentication and Identity Management (IDM)
- Threat of Data Breach of Loss
- Vendor Lock-in
- Multi-tenancy / Software Isolation
- Data Protection
- Availability
- Unauthorized Secondary Usage
- Legal Uncertain

Virtualization

Nowadays virtualization is being widely implemented in enterprises however, it is questionable whether there's been adequate consideration for possible security threats. While carrying out virtualization; security, risk and privileged access and activity on the virtual environments is a major area of concern. The fact that an administrator can provision a new virtual machine in no time and restart or dynamically move a virtual machine to another physical host in seconds, can lead to serious violations of enterprise security policies and enterprises are much more prone to human errors.

There are various possible security threats in virtualized environments that are emerging such as Blue Pill, SubVirt, Denial-of-Service, Trojan etc.

To minimize or overcome the threats that can occur both virtualization vendors and security professionals need to work hand in hand to address security in this ubiquitous environment. There should be Continuous monitoring and protection of virtual environments for better visibility. Moreover there is need of tighter security with privileged single sign on to ESX/guest machines that does not expose privileged credentials.

Service-Oriented Architecture (SOA)

SOA security is a type of security that focus on the security of entire IT system rather than focusing on one software program or one platform. The emergence of service-oriented architecture (SOA) as an approach for integrating applications that expose services presents many new challenges to organizations resulting in significant risks to their business. Important risks among them are failures to effectively address quality attribute requirements such as performance, availability, security, and modifiability.

Possible Attacks

Through Browser Context

A person buying goods online enters credit card number and other information into a web form. HTML 5 allows buttons, such as a submit button, to exist outside a web form. With the design flaw, an attacker could trick the buyer into sending the financial information to an unintended destination using a malicious button.

Browser Security Feature

Another possible attack outlined by Enisa[10] turns a browser security feature — a sandbox into a method of subverting HTML 5 securities. Putting websites into a sandbox prevents them from accessing the system via the browser. However, the attack described by Enisa uses the sandbox to disable protection against clickjacking[7]. In clickjacking, a user is fooled into clicking on a seemingly innocuous web object such as a button, which then reveals confidential information. This is cited in the study under link [7].

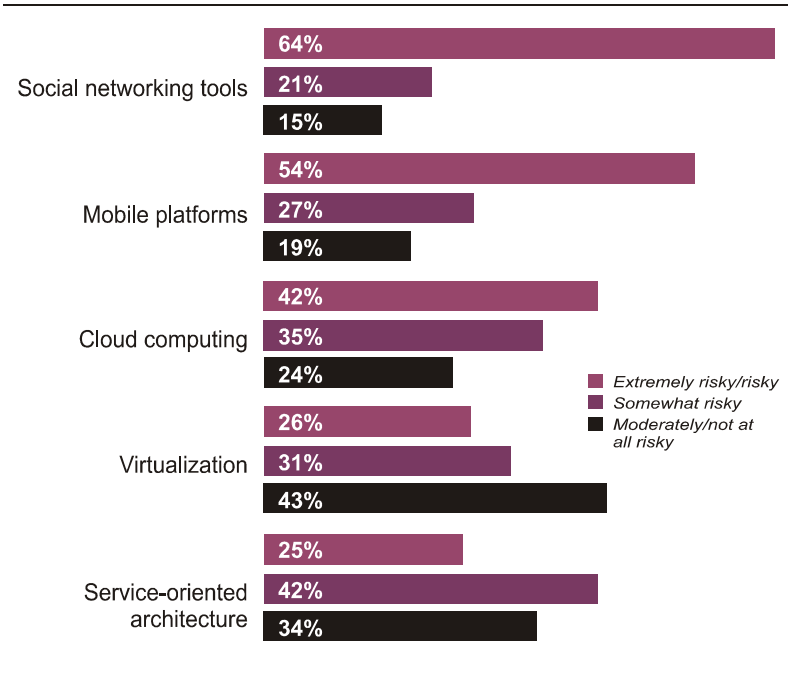

Fig. 3: Risk Emerging Technologies

The HTML 5 specification allows a hacker to put a malicious page inside a sandboxed iframe, disabling top-level navigation, and leaving the user open to clickjacking.

API Specification

Another flaw highlighted by Enisa, in the Geoloc-Secure-3 cache API specification, lets a hacker retrieve information about the user's location from the cache. In addition, the specification fails to set an upper limit to how long geolocation data is stored in the cache, leaving people open to attacks that give away their movements.

Finding Gathered from the Literature Review

Cyber-attacks are becoming increasingly complex and successful, especially over the past year which has seen a number of attacks against high profile targets.

Global Risk study was made by IBM and the findings confirm that IT leaders are concerned about IT security and business resiliency. IBM surveyed 560 IT managers and CIOs from all types of companies located all over the world to talk in order to understand issues surrounding IT risks from the perspective of IT leaders. Of these five technologies, social networking, mobile platforms and cloud computing were rated the most risky emerging technologies. Social networking tools (64% respondents) came out on top as the technology that posed the greatest risk. Second was mobile platforms (54%) followed by cloud computing (43%). The Fig 3 show the graph of the survey depicts as per reports cited in [3].

The survey was conducted in Jan 2013 to check the motivation behinds the attacks. The Fig. 4 depict the motivation behind the attacks and as per reports cited in [8].

The reports cited in [9] is shown in figure 2.

Conclusion

This paper discuss about the Cyber security vulnerability and how it allows an attacker to compromise the integrity, availability, or

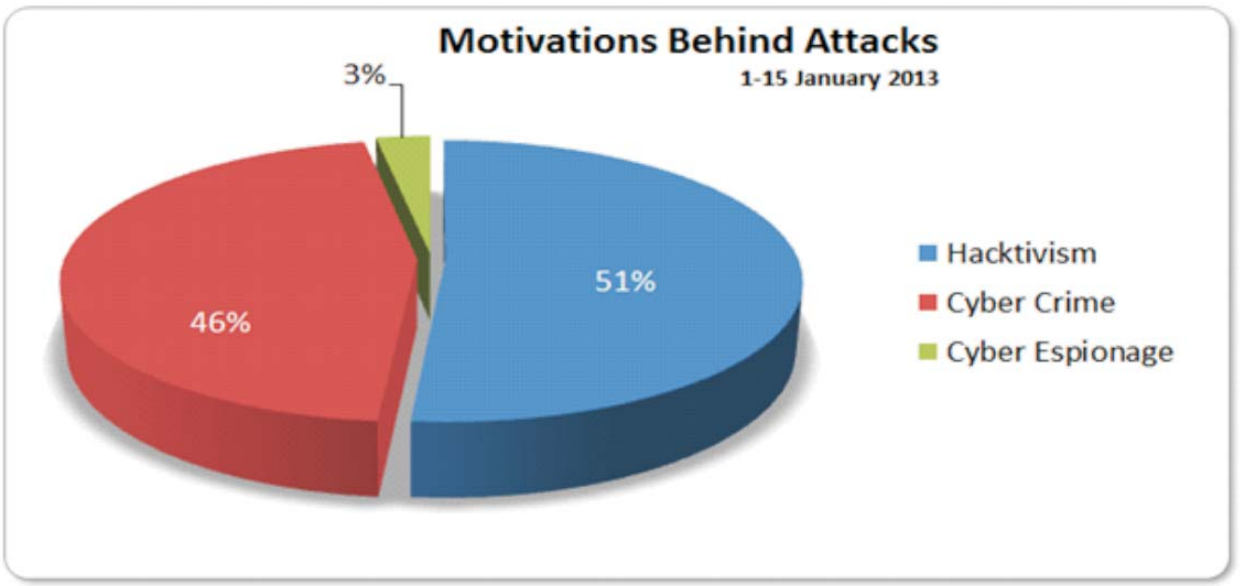

Fig. 4: Motivation behind the attacks

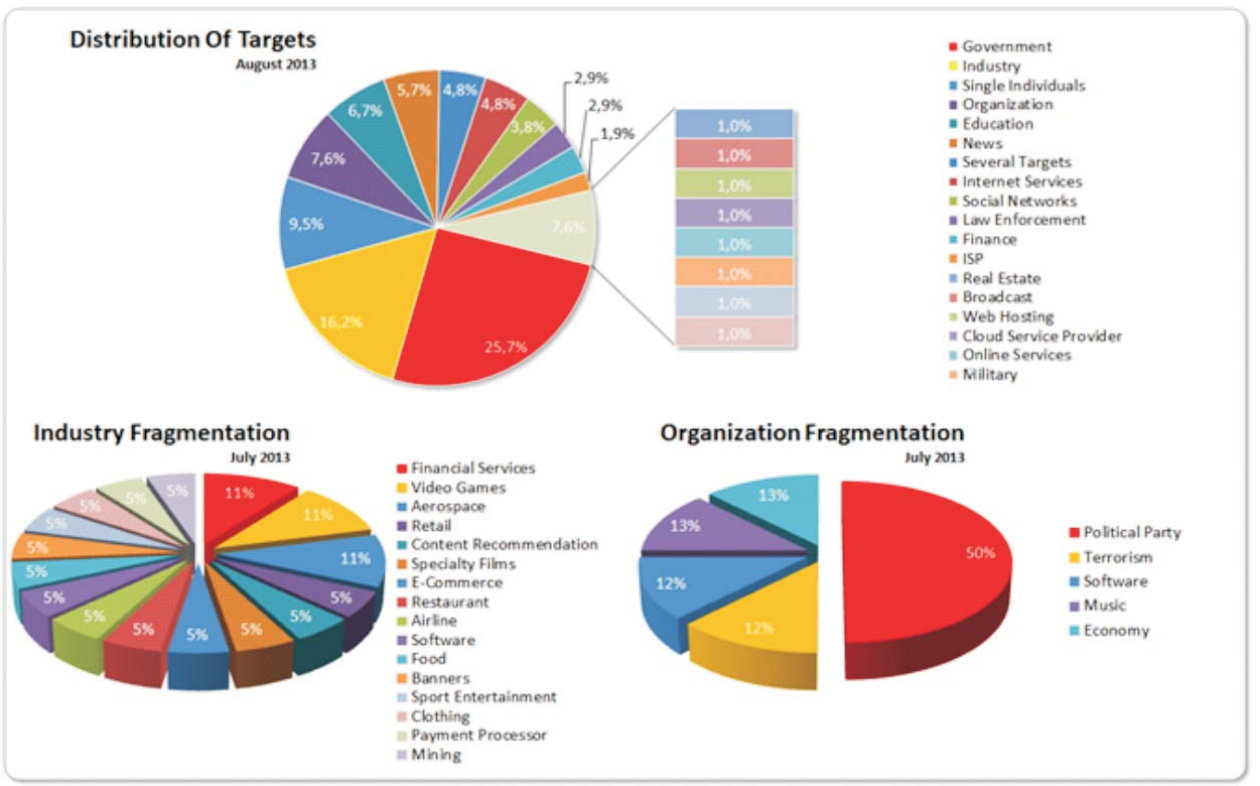

Fig. 5: Fragmentation: Industry and Organization

confidentiality of the information**.** We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable and cause the least damage possible.

References

1. Allan Friedman, "Cybersecurity and Trade: National Policies, Global and Local Consequences" Brookings Institution, 2013.
2. Allan Friedman, "Economic and Policy Frameworks for Cybersecurity Risks" Issues in Technology Innovation, 2011.
3. cios-social-computing-is-the-most-risky-emerging-technology.html dated 22/2/2014
4. CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats. Report
5. *Cybersecurity and CyberWar: What Everyone Needs to Know*, New York Times best-selling author P. W. Singer and Allan Friedman, 2013
6. D. L. Ponemon, "Security of Cloud Computing Users," 2010.
7. http://www.zdnet.com/enisa-w3c-web-standards-pose-51-security-threats-3040093582/
8. http://paulsparrows.files.wordpress.com/2013/01/1-15-jan-2013-motivations.png
9. http://paulsparrows.files.wordpress.com/2013/09/august-2013-targets1.png
10. eb-security-eu-cyber-security-agency-enisa-flags-security-fixes-for-new-web-standards.htm