Issues Related to Web Security and Privacy

Manveen Kaur
Assistant Professor,
Department of Computer Applications
Chandigarh Group of Colleges, Landran
mahil.preet@gmail.com

Baljinder Singh
Assistant Professor,
Department of Computer Applications
Chandigarh Group of Colleges, Landran
cec.bca.baljinder@gmail.com

Abstract
Internet privacy is a subset of computer privacy. Internet privacy and web security is the major issue in these days. With the advancement in the technology and lots of participation of the peoples on the web has make it unsecure. Today web world is the main source of information, communication and the interaction of the peoples with each other through the social networking site. In these social networking site peoples share their personal information and intract with each other this make the call for using their information in wrong way. Not only this, web security has also some major threats such as worms, viruses, hacking etc. that make the web document and the user system unsecure. Viruses and Worms attack the user documents and systems and make their data unusable. Many security solutions are applied to remove these threats such as Antivirus, Firewall, and Spam-filters etc. All these security solutions remove the Viruses and Worms and provide the firewall that stop unauthorized access to the system. Not only this Governments are also making strict rules to stop the Hacking and make the users information private and confidential. Some Governments have also made the Cyber Security Cells that look after the unauthorized attack on government system or their personal data and information. They have also made the Cyber Crime Cells that look after complaints of peoples that are affected by cyber-attack. Thus web security and privacy is the major issue in today's world and should have the high level techniques to solve it.
Keywords: Computer and Internet privacy, Identity Issue, Hacking, Viruses and Worms, etc.

Introduction

World Wide Web is nothing but is the new electronic communication of the people's around the world. The Internet and the Web has changed the whole world and make it easier for every person to communicate and navigate any information on the web. Communicate to others needs some personal information and that information should be in the security and should not be shown to other people that are the main security and privacy issue of the web.

Protection of data has been an issue ever since the first two computers were connected to each other. With the commercialization of the Internet, security concerns expanded to cover personal privacy, financial transactions, and the threat of cyber theft. Later the universe of malware expanded and techniques for detecting them also expanded with the new protection software's.More recently, concerns over the authenticity of software and the protection of intellectual property gave rise to various software verification and attestation techniques often referred to as trusted or measured boot[1].

Web Security and Privacy Issues

The present threat to internet user is a combination of old(e.g. Trojans, Viruses) and the new (e.g. web bugs, confidential data being stored in plain – text cookies, unique identification numbers, ad- ware/ spyware and unauthorized transmission of the user's personal data). Most of the problem originates in the methods by which online advertising companies track and store data about net surfer in order tocompiles statistics for more effective advertising.

"Privacy on the Internet" means the level of protection that Web sites operate according to internet users' personal information. The basic issue revolves around giving Internet users notice about what personal information will be collected by government and commercial Web sites when they visit the site and how it will be used. Most Web sites collect and sell personal information through online registrations, mailing lists, surveys, user profiles, and order fulfillment requirements. Internet security refers to the extent to which Web sites are vulnerable to unauthorized intrusions or attacks by ill-motivated persons [2].

Ecommerce Issue

With the growth of Electronic Communication and sharing of personal information through Electronic Commerce has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic Commerce. Some of the regulatory mechanisms and legal infrastructures come within the domain of Cyber law that encompasses Cyber-crimes, Electronic and Digital Signatures, Data protection and privacy [3].

Steel of Identity Issue

Weak authentication and the existence of anonymous services, makes it easy to steal account details(With all resulting threats) to impersonate people and
Publish 'on behalf of (identity theft) them to harass, insult or disparage people. The impact of this is augmented by the complexity of deleting published information and weak terms of service.
Server authentication issues also play an important role in network security that is based on DNS-resolved host names but network access ultimately uses IP addresses. When the browser starts loading network content, the host name is first resolved by the DNS system and after this the request is sent to the IP address, which defines the final destination.But Users ignore SSL Certificate errors, enabling middle-man to attack on them not only this users do not notice domain types and other anomalies, enabling phishing attacks.

System Information Through Cookies

A cookie is a small amount of information sent from a web server to the user's computer when they use the web site. This information does not personally identify them. It simply gives information about the areas of interest or the sites user has visited. It also informs if the user has selected a product and put it in the shopping basket, it does not tell about the user's personal identity unless they are registered with them.

Security Solutions

Web is becoming more and more widely day by day and the protection & security solutions must also be needed to make secure browsing and keep information secure and keep the systems free from malware and virus free. So some of the security solutions are as follow:

Secure Booting to System

Secure booting can prevent the system from unauthorized access. Secure booting means authenticate user can only login the system. When power is first introduce to the device, the authenticity of the software on the device is verified using password protection or some digital signatures or by finger scanning devices. Asecurity softwareor scanning device attached to the system verifiesand ensures that only the authorized can logon to the system and run that device.

Access Control of System

Access control built into the operating system limit the privileges of device components and applications so they access only the resources they need to do their jobs. If any component is compromised, access control ensures that the intruder has as minimal access to other parts of the system as possible. Even if someone managed to steal corporate credentials to gain access to a network, compromised information would be limited to only those areas of the network authorized by those particular credentials. The principle of least privilege dictates that only the minimal access required to perform a function should be authorized in order to minimize the effectiveness of any breach of security.

Device Authentication

When the device is plugged into the network, it should authenticate itself prior to receiving or transmitting data. But they require an input to that network device. Just as user authentication allows a user to access a corporate network based on user name and password, machine authentication allows a device to access a network based on a similar set of credentials stored in a secure storage area.

Firewall

A firewall is software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set. The device also needs a firewall or deep packet inspection capability to control traffic that is destined to terminate at the device. Deeply embedded devices have unique protocols, distinct from enterprise IT protocols A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

Updates and Patches

Once the device is in operation, it will start receiving hot patches and software updates. Operators need to roll out patches, and devices need to authenticate them, in a way that does not consume bandwidth or impair the functional safety of the device. Microsoft sends updates to Windows users

and security patches. Software updates and security patches must be delivered in a way that conserves the limited bandwidth and intermittent connectivity of an embedded device and absolutely eliminates the possibility of compromising functional safety.

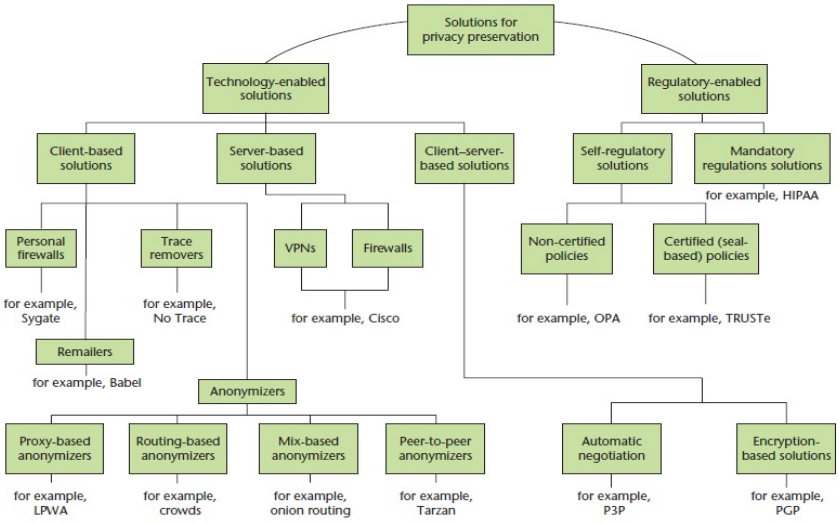

Figure 1: web Security and Privacy Solutions [16]

Removing Trace Route

Trace Route is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path) by removing or by using No Tracer the users identity can be secured not even this users data can also be made secure.

Encryption

Encryption is the process of encoding messages or information in such a way that only authorized user can read it. Encryption doesn't prevent hacking but it reduces the likelihood that the hacker will be able to read the data that is encrypted.In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key can access it [4].

Security Attack Statistics

- 21% of internet users have an email or social networking account compromised or takenover by someone else without permission.

- 13% of internet users have experienced because of something the user posted online about them.
- 12% of internet users have been stalked or harassed online.
- 11% of internet users have had important personal information stolen such as their SocialSecurity Number, credit card, or bank account information.
- 6% of internet users have been the victim of an online scam and lost money.
- 1% of internet users have lost a job opportunity or educational opportunity because of something they posted online or someone posted about them [5].

1.4. Personal Information Statics

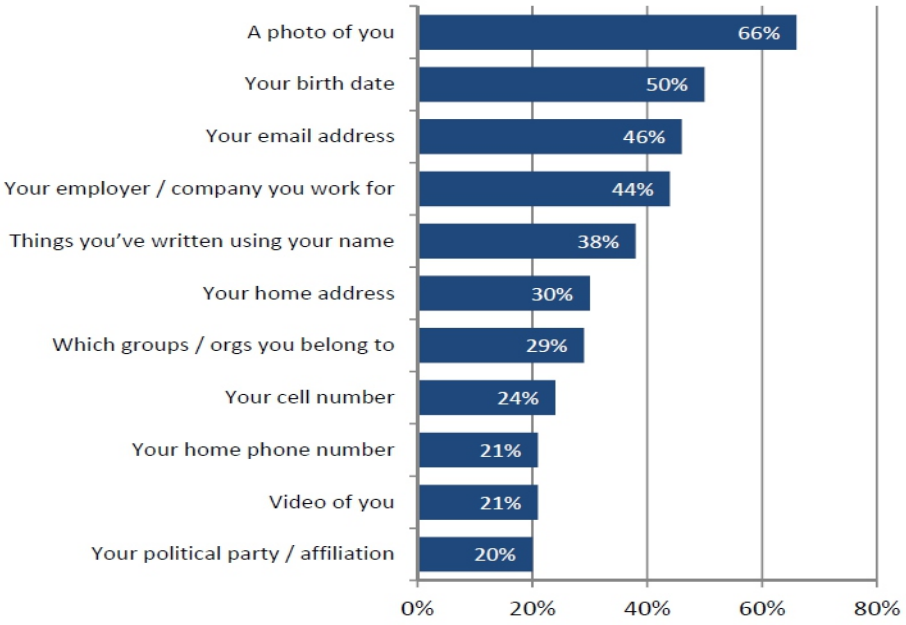

Figure 2: Personal Information of the people on the web [5]

Conclusion

Internet privace and security is the major issue in these days. All arround the world every day many of the hackers use to attack on the others system and personal information and enterprises data and try to use them in a wrong way, so to secure the data from unauthorized access secutity parameters and security sollutions should be made strong and the servers systems should be make more secure with updated softwares and security hardwares. Users should also make efforts to make their personal data and confidential data secure and not to enter them on any website on the web unless they don't know that there data is secure.

References

[1] AJ Shipley "Security in the internet of things".

[2] Orrin G. Hatch" Internet Security and Privacy" U.S Government Office, May 2000. http://en.wikipedia.org/wiki/E-commerce_security_2 http://en.wikipedia.org/wiki/Encryption.