CRIMSON PUBLISHERS
Wings to the Research

Research in
Medical & Engineering Sciences

ISSN: 2576-8816

Review Article

Security and Privacy in Data Networks

Christos Beretas*

Member of Alpha Beta Kappa Honor Society, USA

***Corresponding author:** Christos Beretas, Information Technology Specialist, Member of Alpha Beta Kappa Honor Society, Alpha of Ohio, USA, Email: c_beretas@yahoo.com

Submission: June 01, 2018; **Published:** June 14, 2018

Abstract

This article has as a purpose to deal with security and privacy of the data handled daily worldwide. It describes and analyzes the ways of violating private communications that make in various ways such as (Internet activities, smart phones, viruses, hacking, social media, cloud computing, bots, mobile applications, internet of things, metadata, and tracking/surveillance). It analyzes the above mentioned and also trying to find countermeasures to protect the confidentiality and integrity of data. The collection and analysis of information nowadays is becoming more easily in different ways and from different sources to join all of them the information to create a virtual human profile becoming very easy. The freedoms of individuals have been reduced significantly in this contributed automated system in most cases without the consent of the users that record, store and process personal data including files unknowingly. This article aims to highlight the major problem of violation of the electronic data and privacy, to present countermeasures enriching knowledge from simple user until the advanced professional for the going on around and how it can defend itself.

Keywords: Internet activities; Smart phones; Viruses; Hacking; Social media; Cloud computing; Bots; Mobile applications; Internet of things; Metadata; Tracking; Surveillance; Privacy; Cyber security

Introduction

The security and privacy in any form of electronic communication is a matter of concern to humans from the early days of the internet existence. The loss, modification, alteration and non-consent intelligence is the most crucial risk in our days, the ways many, large interests, governments that want to control their citizens (see IRS in the U.S), government agencies in the name of security want to control the global digital data (see NSA and the PRISM program), government agencies monitor the digital data of their citizens (see Carnivore of FBI) Other nongovernmental organizations or either participate in various privacy breaches programs whether acting individually for the purpose of advertising or other actions. According to what we know, the present article is deemed resigned and crucial for the internet users because it needs to know to be able to defend itself, do not forget that knowledge is power [1]. In the article will be presented in detail the ways of violation of information security and human privacy considering the following technologies: "Internet activities, smart phones, viruses, hacking, social media, cloud computing, bots, mobile applications, internet of things, metadata, and tracking / surveillance".

Rationale of analysis

Using smart phones, Cloud computing, Internet of things, viruses, hacking, etc, but also the humans has created a new digital world with new data on the user service and the security and protection of personal data. Various devices and systems work in harmony with each other or independently offering to the user's smart choices, such as "smart homes", which allow people to interact via the command remotely or locally using the internet and the mobile phone. All these smart environments require transmission and processing of personal data, of course, there are issues regarding data protection, the risk of transmission of personal data grow if we consider that we live in one world where people and computers have continuous connection with the web. This research is necessary not only because it comes to bring up security and privacy problems that exist but do not appear on the surface for various reasons, but it comes to proposing new solutions that truly improve people security and privacy. This research will sensitize users and organizations to realize the need to protect their data and protect their privacy. This in turn will create new jobs, existing staff training, purchase of software, etc. This research is to enhance the global demand for integrity of the information at the same time moving to ensure as much as possible less exposure of personal data which must be strengthened and improved globally in all areas managed mainly sensitive information such as financial and governmental organizations, telecommunication companies, military, and emergency services [2]. Security and privacy is a multidimensional issue with many aspects. The main objective of the research is that people can have knowledge of data security and privacy, to learn to recognize the dangers and defend the creation of original knowledge that will lead later to subsequent further

research. The modern web technologies allow the collection, storage and processing of personal data without informing the requisite consent of the user. The data are revealing, as the Internet grows and expands as the likelihood that the personal data. Through electronic transactions is collected and saved a significant amount of data, the processing and analysis of the data shows a clear picture of the preferences and habits of each user and can be used for various purposes such as taxation, government, commercial or other purposes that cannot be described. Each online visit means disclosure of information but which is not capable by them to identify the users and his/her habits but is an online identity that follows the user and leaves traces of any online activity, of course, referring to the IP address and the MAC address. At first sight these public data are not able to reveal the true identity of the user, but when in those involved governments and security services related to the government then it is very easy to uncover the real person after they are recorded and remain permanently stored in the internet provider, as well as all digital footprints. Web services are either governmental or commercial use techniques that can easily discover the true identity of use, employ techniques such as:

1) Cookies
2) Server side scripts
3) Java script
4) Java
5) Log files
6) Exploits

Then the information is stored in data warehouses analyzed by automated tools, are sorted and then data mining tools become their extraction either to third people or on behalf of some people. The internet is known as a global network of connected computers and devices undertake to store and distribute personal data through every kind of services and various countries [3]. On the side of the user become impossible to monitor the integrity of information and unknown the security infrastructure of each country, or the opposite the information systems, infrastructure, and surveillance systems. The increasingly growing trend in the security of data in conjunction with the revision for the security and privacy levels in existing systems is a challenge and cannot be sure of that systems and security technologies that work today but developed in past years to support data and security are able to meet the new and growing challenges. Social media can be characterized as an open source of mining personal data for two reasons:

1. The data transferred by the user to the server and from server to server are subject to some storage and processing format from the same social networks, however, and by the third network (see state security services).

2. The user alone gives his/her personal data to create a genuine digital profile to be reliable for the visitors but also to show to other people's achievements.

The data that stored on social media are:

a) Name
b) Occupation
c) Marital status
d) Economic situation
e) Features such as height, weight, eye color, etc.
f) Age
g) Hobby
h) Habits
i) Religion
j) Music
k) Movies
l) Photos
m) Video

Other various activities of other various applications that collect data.

In conjunction with the publications and the activity of social media such as:

a) Posts
b) Group membership
c) Applications
d) Locations that someone frequently visit
e) Post photos and videos related to daily life
f) Opinions on specific issues

All the above lead to the creation of a full human profile that everybody that is involved is able to know for each user the following:

a) Political beliefs
b) Religion
c) Focus and passion for certain things
d) The psychological state of the user
e) Daily location
f) What likes to do
g) Who is
h) They have held their full facial features

It is worth noting that at times appeared various social media which to encourage users to register by offer financial compensation, these social media have not mentioned on their websites their headquarters or address, just had a contact form [4], as naturally quickly they became too many users because of their financial gain but to reach the desired results raised the social

media website to pay was very difficult, for example, made friends over a certain number, the specific social media networks they just wanted to collect the users' personal data where then does not know who managing that data, may be a government agency or to be sold for advertising in third people.

The personal information published by a user on the internet including the personal data of the profile as well as publications and other activities in social networking platform in conjunction with the data collected from various services (see NSA below) combine the perfect source for creating a fully electronic human profile. As mentioned above, personal data can be used by anyone since personal data located on third hand (the social networking platform). These data can be used in various ways such as:

a) Personal threaten

b) Financial loss

c) Physical damage

d) Blackmail

e) Advertising

f) Commercial purposes

g) State security services

Social media are a very typical example of violation of privacy, a classic example may be the person impersonate with the consequences for the real user that unknowingly other people's forge personal data fraudulently mainly purpose. Personal data published on the Internet as well as any kind of posts remain stored and always, even if the user accedes to the permanent deletion. Each social media networking platform as mentioned above can be used as a storage platform and promotional information where several ways mentioned in this article to collect personal information using methods that may even cause damage to the security of the system to visit these social media networking can be simple visitors rather users.

Automated attacks systems used (Bots) for violating services that have played an important role in privacy violation, such systems are used to access and infect with Malware viruses other remote systems that people behind these attacks to cover their tracks and to collect personal user data such as bank accounts, phone numbers, addresses. Many security systems nowadays to trace the Bots and to neutralize either using DDOS attacks back to the source of origin or blocking specific IP addresses, either based on the User Agent which is often "Spoofed", all have failed. I believe all operating systems have a back door that is used by the security services, as the door "compulsory installation" which means that the mobile phone or the computer placed under the control of third parties. This code is embedded in the operating system kernel and is structured so that it cannot be understood by analyzing the code. Also, applications distributed by specific companies participating in the "user tracking program" embedded a code that enables the remote management of the device.

A simple SMS is enough to activate the back door service or by using the GPS, the feeling of violation of privacy enhanced if we think when lost a smart mobile device enables the user to lock, block and locate the device on an electronic map which confirming the existence of the back door. Notably study by "Snoop Wall, 2014" revealed that there are several popular mobile phone applications that collect and send personal data of the users on servers located in Russia, India and China.

These applications spy on their users and use their personal data for the government or advertising purposes [2]. A virus is not necessarily be malware also a trojan horse virus can be installed on systems and perform in "Stealth" mode for years without being able to ever detected. During that period of a Malware or Trojan Horse virus remains installed on a system is stealing personal data, save Screen Shots, infect other systems on the Internet, opens cameras and then record all this data and sends it back to hackers exposing not only the security of information systems but also affecting the users because it sent personal data to third people's hands. A typical example of the ease to do this is the virus Carberp.

The cloud computing has been previously target of personal data collection and of course is a major threat for users who use it, below mentioning the physical threats for the following reasons:

a) No physical access to the Server, so anyone who has physical access to the Server as Server administrator has access to personal data.

b) We do not know where the data is stored and if encrypted and how.

c) Share Server with other users or competing companies.

d) We do not know the actual level of security they provide against attacks from viruses and external attacks and the security of the files that remain there.

e) We do not know the actual privacy policies that implemented.

f) The legislation on security and personal data differs from country to country.

g) If the Cloud provider gets back up files regularly, do not know if these files are forwarded to competitors.

h) How secure is the connection between a computer and the Cloud provider.

i) When the user delete data, if these data will be fully deleted and not stored in Data Warehouses.

j) Security services may request any file without user approval.

k) The Cloud Computing service providers can participate in the information exchange program.

In Cloud systems many metadata and information transferred to synchronize between server and user. The user in most cases cannot enhance the security level of a connection to the remote

server because the way and the security level set by the remote Cloud service provider. The internet service providers collect and analyze metadata, metadata is data that describes other data and for example an image can have accompanying information expressing the display some information associated with the image. Metadata are considered to describe a situation, therefore considered safe. Processing of metadata can lead to the creation of an electronic profiling revealing user behavior so leads to a complete picture of the user. Search engines are a good metadata example as they track and store forever about what the user seeking, when, and how, In the above include the fact that the security services have many more options than ordinary analysts, the quality and quantity of information that can be gained from the metadata is huge that we can say that metadata is much riskier than the data itself. For example, metadata can reveal information such as:

a) Geographic location

b) Hardware/Device Information

c) Names

d) Text

e) Software used

f) Date and time

g) Who participated

h) The content of the material transferred

The Bots are responsible for the greatest attacks worldwide leading not only to steal personal data but also to financial loss. They are responsible for sending bulk e-mail that impersonates a legitimate service like bank to lure the user to enter personal information and the credit card information to "Smart Flux" websites.

Today's security and privacy measures show very weak to cope with the vast internet cyberspace. The web browsers show unable to face Zero Day attacks as well as the users are unable to cope with deliberately tweaked browsers (see clone of Chrome) these browsers target to collect personal data of its users (and not only) on behalf of people that we do not know.

Java is a programming language that is widely known throughout the world because it runs on multiple platforms and operating systems, the software has been written to it can be considered safe and this because the security manager oversees the security sector with regard to system calls. If a Java program violates the security policy of the applet, the security manager terminates the applet. Floating the byte code verifier examines a Java program whether it is trusted. That all sounds well and good, but in practice is? There are many attacks that used as the basis of Java or breach computer systems or infect virus to users or to turn into a zombie computers.

The Internet of Things that are in vogue and we all love, few know that it's a backdoor entry by third parties to personal information or opposite an exit door. Specifically mention the following:

a) Network devices that share and use data to third parties such as service providers, services, government.

b) These devices are connected between them or autonomously with unique identifiers.

c) Apply everywhere.

d) It is in our lives everywhere, every kind of device can even be worn.

e) The data throughput has a direct connection to who we are, where we are, and our desires.

Suspicion created and is to be considered a violation of privacy:

a) Video recording without notice.

b) Save and analyze information without authorization.

c) Face recognition and biometric characteristics where then stored or use by other services or for analysis and processing.

d) The zero-personal data collection and management control.

e) Creating a user profile.

f) Monitoring.

g) Decisions that may not reflect the user opinion.

The biggest threat regarding data security and privacy in the digital world is that the majority of data transferred on the Internet is not encrypted, the existing security infrastructure in an environment of unencrypted information must be considered totally inadequate. Unencrypted communication means anyone with access to the internet to intercept any information. Government agencies and organizations knowing the SSL weaknesses, information intercepted by users from offensive websites, the non-encrypted information, anonymous proxy servers that offer keep alive anonymity that is essentially Honey Pot systems with recent example the NSA regularly collect information from this servers.

US security agencies have access in data of any internet user in the world. This practice on American ground is legal and is based on the FISA amendments act treaty and the patriot act that was applied after 11.09.2001 it is worth noting that the agreement was renewed in 2012. This treaty gives the freedom to federal agencies to store and to process huge amounts of data without exception if these people are criminalized or not. In accordance with the documents published by Snowden, the PRISM project became quite popular and reinforced worries of the world on the violation of privacy and data. The Project PRISM named after the word outlet means mirror - reflection and this is because the data pass through an internet node continue their route but the items are copied (reflection) from the PRISM project without harming their quality neither have been some form of alteration to worry the user that something is wrong. As shown in the Figure 1 below, to make a data breach between nodes the data must be copied without the user's knowledge. Usually this makes it coherent with telecoms operators and other services that there are active users (Figure 1).

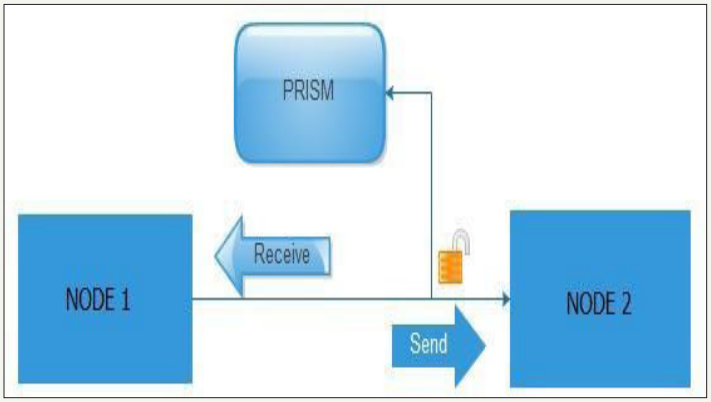

Figure 1: simple example of project PRISM.

All of the above would be useless if there was not the necessary data mining tool and statistical tests, called XKEYSCORE by pressing a few keys are able to know everything related to a human, such as telephones, e-mails, habits, searches has done in search engines, behaviors, internet of Things activities (IOT) and of course building electronic profile "e-profile". According to an article in "Der Spiegel", the security services have advanced already on potential networking devices controls and firewalls of known companies manufacturing such devices. According to slides published by snowmen the xkeyscore, used in conjunction with another program called turbulence, the turbulence are two subsystems the Turmoil and Turbine. Briefly mention that Turmoil is an information collection system of satellite and cable communications, while Turbine unleashes attacks on serial systems. From the above could not be missing collection of information from social media, Cookies, Internet services, Internet of Things, etc. Once the target is locked: the next step is the quantum theory attacks and quantum nation which will give full control of the remote device, even is a mobile phone, Internet of Things, computer, or anything else. All the above are important existent data security problems and privacy that must be analyzed, to be detailed in-depth research and to present suggestions and ideas on how all these breaches of data privacy and security may improve the quality and integrity of information handled within the global internet.

Indicating the program "US-984XN (Prism)" which has access to servers worldwide, in collaboration with other programs have the ability to clone security certificates and copies data during transfer. Intermediary fake servers are installed around the world to meet the demands of users to copy their requests then forward the request to the actual Server then returned the request with the content to the fake server and then forward the content to the user without the user understand anything. Looks how the US-984XN system (PRISM) (Figure 1).

The internet service providers collect and analyze data on the activities of their users. Interception of data involved by private firms financed by government agencies or third party organizations to collect personal data from different data sources that can be through cookies, scripting. Internet of things, mobile phone applications that have back doors, metadata from call centers which allow remote installation and data processing, fake security protocols, fooled by SSL. Automated bot trying to make access to the telephone centers or to attack specific facilities to gain access based on viruses (Figure 2).

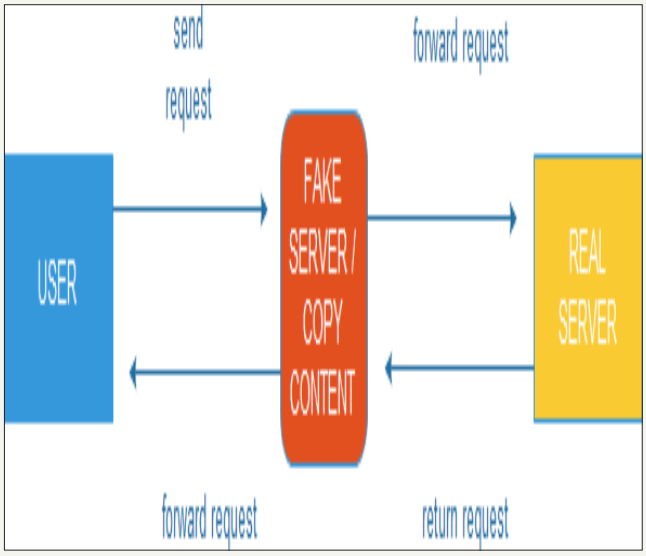

Figure 2: How is working the intermediary-fake-Server.

How to cite this article: Christos B. Security and Privacy in Data Networksl. Res Med Eng Sci. 5(4). RMES.000617.2018. DOI: 10.31031/RMES.2018.05.000617

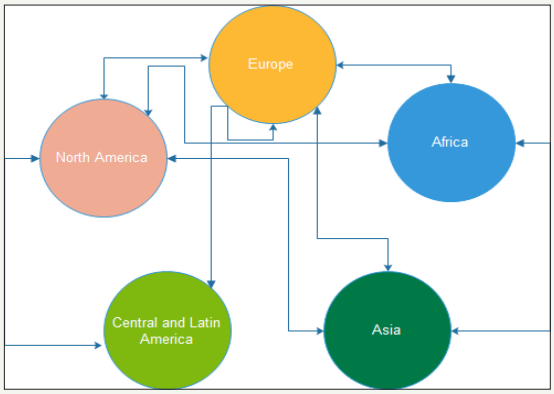

Figure 3: The data are not transferred in direct way but from the cheapest way.

Cloud Providers they have in their hands important personal data and user files, the mobile phones can reveal the identity of the user very easily from the location until the interlocutors and personal data. All of the above are based on the theory that the data are not transferred in direct way but from the cheapest way, as shown in Figure 3.

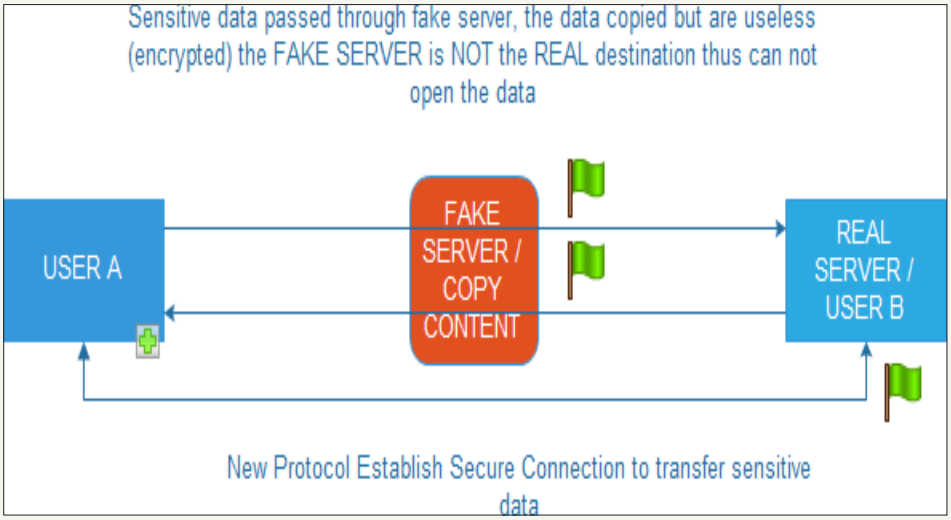

Figure 4:

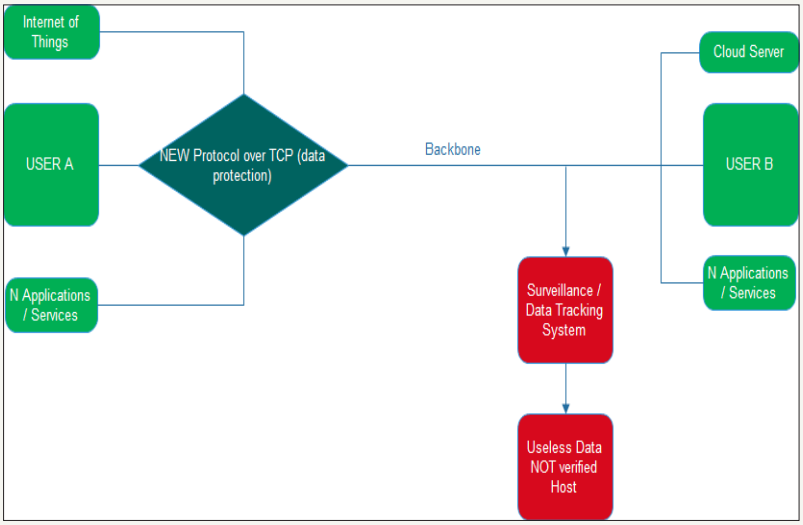

Figure 5:

From the first day of users connecting to the internet, the internet service providers wanted to know who doing what and where, later led to the identification of malicious attacks but later became abused to collect and store information. Organizations and governments want to know the routine of their users to have a society in an organized scheme know the character of each person.

The data collection and processing is performed by each device connected to the Internet, the Internet of things collect personal data transferred to Servers of their manufacturers, telecommunications providers know all about digital life and human conversations, applications for mobile phones collect personal data and data about user behavior. Imagine a smart TV which will send personal data to the manufacturer or other organizations and then those organizations to have remote access to smart TV and opened the camera and watched the place around. Many automated bot trying to break different kinds of access codes to gain access. In the social media or which is require the entry of personal data from the human is clear that the human responsible for their record and this can be restricted. As stated above, the present research will focus on the creation of a secure protocol that will protect the transferred sensitive data and it will stepped up on the existing data transfer protocols for the purpose of non-copy data/content third party people, so will greatly reduce the interception of data as shown in Figure 4 & 5.

Many problems are based on the data security and privacy over the years has been multiplied and this attributed to rapid technological developments and new ways of privacy violations are discovered daily. The research is based on the following entities: "Internet activities, smart phones, viruses, hacking, social media, cloud computing, bots, mobile applications, internet of things, metadata, and tracking/ surveillance". Analyze the countermeasures currently available against data breach and privacy for each of the above entities. All privacy protection techniques applied up today have as a basic feature, the users to restrict the use of their personal data either such personal data provided by users themselves with their own cohesion, whether the data collected by third-party bodies stored in digital files, but often are not collected by the user agreement. Below analyzed existing protection techniques applied up to date as well as the disadvantages and advantages:

1. Any website that invites the user to enter sensitive personal information must have a valid security certificate that means the data are transmitted securely, the page must support SSL/TLS. The SSL was created several years ago and offered extremely high protection for data communication but years ago. Of course continues to provide important safety but as time passes the architecture becomes more and more vulnerable, a malicious hacker to reach the target, it can easily steal a certificate to forge even find a new free from many currently available on the internet. So when someone visit a web page on the internet with active security certificate is not sure that the data entered will be stored in Servers of the organization where the data transaction took place, there are many stolen and misleading security certificates through clone's websites (Smart flux) trying to lure users to obtain their sensitive personal data. Whenever the integrity of the information cannot be based only on the SSL certificate. TLS, on the other hand requires continuous control of the certificates, there is NOT complete encryption of the message from the sender to the recipient, there is no confirmation of the authenticity of the sender, and problematic communication between sender and recipient when between them exist a firewall.

2. Disable Cookies, there are ways that can intercept user's personal data without his/her will. As we know the cookies can reveal important information about the human personality. Disabling cookies reduce the likelihood of personal data collection but only in the process of information gathering through Cookies. A website also includes various Scripts such as Java script, Java, PHP, ASPX, these programming languages have unlimited possibilities for the collection and storage of information are high level languages and are more close to the human understanding. Scripts written in these programming languages have the ability to download files in Stealth Mode on the local hard disk of the user's computer to execute the code and to collect the results.

3. Turn off Java script as it is responsible for broadcasts virus type zero day and also there are ways of obtaining information from users without undertaken. The java script off is an immediate protection - response to viruses that use Java script as the basis. The Java script off creates a very big problem, websites not play at all or not working properly. The security experts proposed as a solution to install the latest version of java on each computer and uninstall all the previous versions and this because the last version contains several bug fixed and extra protection. This measure is considered insufficient because no one can predict how an attacker will use a code written in java where based on a new addition - the possibility that there will be in the new version in order to exploit to violate a system.

4. The web browser and any other programs often used must be updated to avoid scripting type attacks and hijacking. Generally this is good to keep updated the programs because improves their performance, new features added, and corrected problems that identified. Unfortunately cannot be predicted future attacks to protect themselves in the appropriate manner so that there is no possibility of contamination. An updated web browser is considered safe but not 100% and this is because in modern web browsers used many add-ons and the cause of evil starts from there, for example a security hole in a flash add-on will infect the web browser because add- on and web browser are interconnected, so add-ons are a back door of a data violation.

5. In social media must not listed personal information such as marital status, place of residence, work, location, thus making difficult to third parties to create an online profiling for each user. It is a practice that is generally correct, but it is only right, for the common people and not for everyone for the following reasons:

a) Social media know the exact location based on IP addresses.

b) The MAC address is also recorded.

c) They use scripts that collect information about the visitor.

d) Third, companies and organizations collect information from other sources that their source connection will determine the characteristics of the user.

6. To browse the internet by using anonymous proxy servers and VPN ensuring the anonymity and overcome the internet service

provider that collect personal data and then transfer this data to governmental or non-governmental agencies. Anonymous proxy servers and VPN is completely safe only when the user know the infrastructure. The internet service providers when users use VPN they know the origin and destination of the data but do not know the contents because they are encrypted. They know the origin and destination of the data types reveals some information about the user. VPN networks and anonymous proxy servers are not always safe, in most cases it is a honey pot systems operating on behalf of government agencies [1] to store and process information. Several of these with a simple "Ping" to their IP address reveal their name that is "Honey pot". In Honey pot systems includes the TOR.

7. The smart phones are safe and not at risk of the back door threats and viruses if someone turned off the data. Experts in security suggest to smart phone users to disable the Internet data on their mobile phones when they are not needed them, when closing them to remove also the battery to be sure, but they forget something important, an attack breaches of privacy may start by a simple SMS which when opened will occur the following:

a) The mobile phone settings will change either to collect data either by the connectivity of services.

b) It will connect to a remote server for downloading spying software without the user's approval.

c) It will connect to a remote server to download virus without the user's approval.

Also security experts forget that an SMS can stay up to a week in mobile Server provider to be destroyed if not received by the recipient.

8. Several security experts argue that the antivirus and antispyware with continuous updates for personal users are ideal, but for companies propose sandboxes and web content filtering thus argue that the chances of falling victim to hacking and phishing are minimal. The breach of data security and privacy does not only emanate from attacks by viruses that will be installed through an infected website. Violation of personal data can take place in various ways, including:

a) Human factor

b) E-mail

c) IRC

d) Bot

e) Back doors

f) Various other ways

The Antispyware, Antivirus, Sandboxes, Web Filtering, protect only certain types of attacks and they are not in any way comprehensive solution to issues of violation of privacy and data.

9. The applications where they are online in cloud software distribution platforms such as the Google play, apple store, etc are usually but not always safe generally they do not contain back doors because programs are hosted on these platforms are usually tested for viruses. The programs are hosted on such platforms are tested for viruses; these programs are either from private developers, or software companies. When a virus infects a file does inject malicious code into the already existing file that wants to infect increasing the geometry of PE header and the general geometry of the file. When an antivirus check if a file is infected or not infected checks for the injected code into the file. An uninfected program can cause more damage than an infected, the code of a normal program can be so mixed that can collect everything in data and antivirus to see all this normal and this is because is a normal operation and part of the program, for example a program opens a TCP port to communicate with a server is not necessarily a virus, but is not necessarily secure. The back doors are part of the code which is not visible when examining the code and is activated when a particular incident takes action, so an antivirus cannot detect backdoors in software.

10. The metadata is something that concerns the service provider, and subject to the laws on personal data protection in each country. Users are protected by Privacy laws that applied in each country, this is not enough, no senior official is present at the time that personal information are collected to verify whether the law obey or not, so users should be turn to other solutions that will be analyzed in my research, just to mention one example here, Case 1: unnecessary communications exposure reduction, for example user A communicates by telephone with the user B that is a health agency to ask anonymously where can make examination for HIV. User A called from home phone of which the number is private and did not gave his/her name, so user A considers that remained anonymous, which is not the truth since the procedures behind the scenes to connect the user A with user B reveal the true identity of the user A. So it creates an entity for the user A because is called the user B that associated with HIV examinations, user A is possibly a disease vector, infected, or possibly he/she is related to a person that may be a disease vector or is sick.

11. The connection to the cloud is secure by using SSL/TLS or specific application that encrypts the data connection and user identity, while the provider of the Cloud service provides high security, protection, integrity and anonymity of information. The SSL/TLS as described above have several weaknesses but remain a reliable solution for safe connections. In cloud the problem is not only the connection but the storage and integrity of the information, how a user can be sure that the cloud provider does not provide data to government agencies? How the user is sure that after a hacking attack the data will not be intercepted? How the user is sure that his/her personal data will not leak to third parties for advertising purposes?

12. Hiding the real IP address of the computer is offer anonymous online browsing and security agencies of foreign countries they cannot discover real user identity scientists said. Most anonymous proxy servers and anonymous services either cooperate with government agencies either created by government agencies to monitor and control the data throughput, as mentioned

above many anonymous proxy servers with a simple "ping" return their name that is "honey pot". The websites offering anonymity expressly notice that if requested by an official security authority will release the true data of the user, and the question is, for what anonymity talking about? When we visit the web except the IP address exist the MAC address which is permanent and represents the network card, these two items are recorded by the internet service provider, these easy data can be compared even with different internet service providers so easily a computer can be tracked worldwide. An IP address reveals the ISP region, country, and even GPS coordinates so it is very easy to find the real user identity globally.

13. Both are targeted large companies and not simple users, the problem addressed by blocking specific IP addresses either on the Firewall or Router. The Bot creators targeting large enterprises because from there they will gain personal data and financial rewards, but attacks based on simple clueless users that their computers converted into zombie from the creators of Bot that the actual creator of Bot is hiding from tracking, as is indicated above, Bot creators using single clueless users for their attacks so IP addresses each time are different, so the existing solution that is applied is not effective.

14. Visiting a search engine through anonymous proxy server or VPN may not know the identity of the user. The violation of privacy through anonymous proxy server or VPN has been described above and as is expected when involved also and search engines then the problem swells for two reasons:

a) Users unfold their imagination and searching that their really interested and want to learn about.

b) Search engines work with government agencies and send the data of the visitors, including metadata.

15. Connecting a computer or a smart device to a free internet access point cannot identify the actual user identity, anybody can be connected, leave the impression that the level of protection of personal data is very high because the access is open and free and there are not surveillance cameras in the area but completely ignored the sense MAC address which is the identity of the computer's network card and it will accompany the device always, also escapes the mind of users that in most places with free internet access the packets are tracked (sniffing), and a large part of the computer hardware is also logged.

16. The mobile networks are safe because the communication is encrypted so no one can hear and intercept data but is a good practice sensitive data to not discussed by phone. The GSM is the most widespread type of wireless network world wide but containing security of previous years, the data were transferred in GSM is not encrypted everywhere for this reason should not be considered safe.

17. The Internet of things collect personal data processed by authorized people who examine them and process them without the ability to pass them to third people, the authorized people it can be a group of people or an organization. Is not permitted to collected personal data concerning racial discrimination, origin, politics, religion and sexual orientation. Protecting privacy and data through the use of the Internet of Things is based on:

a) Use of open source software

b) Use of alternative passwords

c) Two stage user identification

d) Avoid storing information on such devices

The above are not sufficient to protect the privacy of data as the Internet of things operate in different environments and situations, for example an automatic parking system in a car that collects information about the car and the driver and is synchronized with a satellite for positioning of the vehicle to park, the four above-mentioned solutions are not applicable.

Conclusion

The violation of privacy through the collection and processing of data without the approval is a reality. Private enterprises and government agencies cooperate for the continuous and unrestricted data collection. When there is electricity for data transmission there is the possibility of data interception. The development speed of internet services in conjunction with automated devices using the Internet to automate human life dramatically increase the interception of personal data and made new outbreak way of electronic spying. In today's lifestyle, the human is practically impossible to defend for the privacy, sacrificing privacy and their personal freedoms to enjoy a new lifestyle where information from various sources accumulate to create a virtual platform for the life and human behaviour. Governments rejoice because they know the profile of all citizens and businesses speculate because it is very big source of ready information used for marketing. As the problem leave the fate, it will swell so quickly come to saturation which means that soon the human will threatened from its own data but by the hands of third people. Require new research and proposals that will protect and improve the levels of people's privacy.

References

1. Stewart JM (2014) Network security, firewalls and VPNs. Jones & Bartlett Publishers, Burlington, USA.
2. Cole E (2009) Network security bible. John Wiley & Sons, New Jersey, USA.
3. Kizza JM (2005) Computer network security. Springer Science & Business Media, Berlin, Germany.
4. Jakobsson M, Ramzan Z (2008) Crimeware: Understanding new attacks and defenses. Addison-Wesley Professional, Boston, USA.