International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Layers of Internet Privacy

Amit Dabas[1], Ashish Kumar Sharma[2]

[1, 2] Cyber Forensics & Information Security, Maharishi Dayanand University, Rohtak, India

Abstract: ***Privacy is said to be born right of an individual whatever or wherever he lives but going in digital world means loosing privacy with or without your consent. Research on privacy issues is going on for long now and the privacy problem is not only giant but diverse on its accountable characters. In this review paper we will discuss different layers of privacy for an online user and try to categorize the privacy needs of a user. Though privacy in digital world is as complicated subject as simply it is taken by most of the people.***

Keywords: Privacy attacks, Online Privacy, Privacy safety layers, Data breach attacks, Online Scams**.**

1. Introduction

There is no constant definition of privacy in digital world as it changes with every individual's needs, living style, age, work ethics etc.it was published in NBC news "INTERNET PRIVACY is a murky, complicated issue full of conflicting interests, misinformation, innuendo and technology snafus. On the face of it, e-commerce companies and privacy advocates are locked in stalemate. Web sites want to know all they can about you; consumers generally want to share as little as possible."[1] So in this paper we will divide a user's privacy in four different layers because it is very difficult for a user to value his privacy or information in digital world as digital world promises great deals which might only effect a user's privacy in future. Privacy is been categorized in many ways depending on many characteristics. One of the most looked clear approach about privacy is given by Daniel J Solove's taxonomy of privacy. In this paper we will define layers of privacy and there impacts on user's privacy.

2. Individual or personal Layer

First layer of users privacy is personal layer , In this layer a user gives up his privacy on his own terms means he chooses to use different services in return of losing some of his privacy. This layer doesn't contain highly dangerous impacts on a user's privacy but it is considered to be basic step of losing privacy. An online user can control or save his privacy if he/she is well known to the factors impacting a user's privacy in this layer. Here we will look after basic bargains a user do in his personal layer for keeping his/her presence in digital world and how a user loses key privacy information in these bargains.

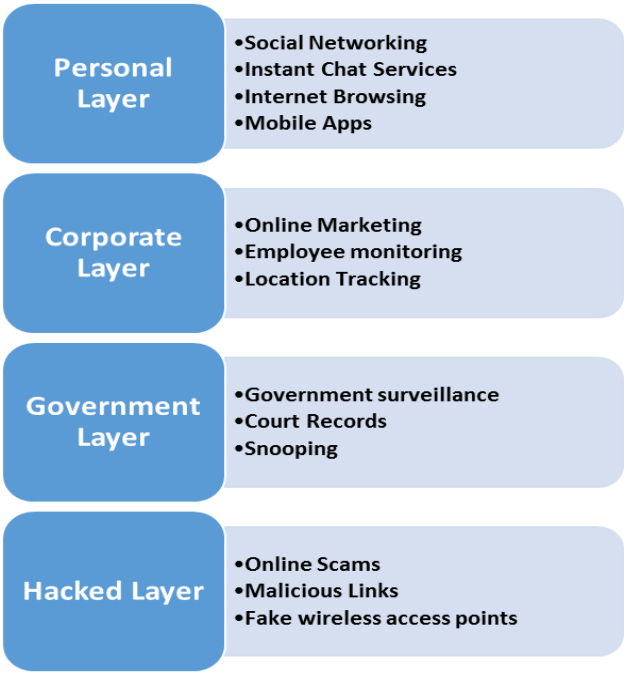

Figure 1.1: Layers of Internet Privacy

2.1 Social Networking

Social networking is about maintaining social relationships on websites that is being available in digital world with your identity. It is used to stay in touch with friends, make new contacts and find people with similar interests and ideas. Now this is the better side of social networking websites but there is another side which shows concern about a user privacy.

As it is very easy to post picture, social interests, comments, invite friends, refer friends on these social networking sites. Major problem here is use of information posted on these social networks because it is difficult to control reuse of that information by others. Most of the social sites provides privacy settings but not all the users are aware or use them to the highest level which leads to information leaks, identity thefts and social engineering attacks. As it is clearly mentioned in privacyrights.org that many people besides friends and acquaintances are interested in the information people post on social networks. Identity thieves, scam Artists, debt collectors, stalkers, and corporations looking for a market advantage are using social networks to gather

information about consumers.[2] Not only these but even social networking websites themselves using lots of user's information for monetization purpose.

2.2 Instant Chat Services

Online chat services made internet more popular in youngsters as it not only provided globalization i.e. east to chat to people whole over world but it was easy access in bonding new relationships. Though chat services can be archived, stored, and recorded on your computer as easily as emails. These instant chat services allow file transfers which can lead to serious cyber issues as sometimes these files could be malicious and attack user's computer.[2] Social Engineering attacks are also easy in such conditions as no one keep their guards high when they randomly chat to strangers on these Chat services. In pasts hacks of the archived chat history has taken place which leads to reputation loss to online users. Even spammers are found very active on these services. Advertisers also use such platforms with the help of malicious bots which act as human but then redirect users to other places. Privacy has been a great concern on these services but these are personally chosen services by users they can deny or choose safe options in such services like turn off the chat archives or don't give all information to stranger's policy or hide your identity.

2.3 Internet Browsing

First step of every internet user is browsing the internet so at this step not all the users are aware of privacy issues or attacks they are going to face in future for being online. So at first it may not seem like you are giving very much information, when you browse the Internet but you are relaying personal information to websites. Not only personal information but browser provides your IP address to the site operators this information is further user by web trackers. Internet browsing not only is about go and access internet but then comes the browsers features to allow pop up ads or let users personal information leak out by different methods. Most famous is Cookie proliferation when a hacker steals our cookies, and by virtue of doing so, becomes us -- an increasingly frequent occurrence these days. Rather, they become authenticated to our websites as if they were us and had supplied a valid log-on name and password. Then they can do lots of malicious activities through original accounts.
Now a days many browsers provide stealth modes or private modes but not all the users are aware of it. As we all know search engines have given the wings needed by internet. Google now processes over 40,000 search queries every second on average, which translates to over 3.5 billion searches per day and 1.2 trillion searches per year worldwide mentioned by Internet Live Stats on its website. [3] With this term we can guess how many data would be available online any basic online user can find IP addresses, names, other details with simple search criteria. Most of use navigate internet by search engines. So search engines leak a lot more information about us which we might have shared on blogs or our personal website or in comments.

2.4 Mobile Apps

Mentioned in Pew Internet Project's research related to mobile technology that 64% of American adults own a smartphone and it is just one country survey if we look at whole world smart phones and mobile apps they are growing with a pace to catch online websites in numbers.[4] But does they affect our privacy? A recent survey by semantic researchers have identified an alarming percentage of apps that collect and send valuable personal information to app developers. Earlier this year, Symantec began beta technology trials to experiment with scanning Android apps prior to download for vulnerabilities and privacy risks using a proprietary tool, Norton Mobile Insight(link is external). There technology found intimate personally identifiable information (PII) such as a device's phone number, usernames, passwords, calendar details, call log information, and even pictures and text messages, are regularly accessed by apps that may not have reason to do so. Shockingly, almost one-third of apps scanned by Norton Mobile Insight leak SIM card information such as address book details, mobile PIN numbers and call history. Additionally, roughly 13 percent (or nearly 2M apps) of Android apps scanned by Norton Mobile Insight send a user's phone number off the device [5].

After reading this research any user will be scared that how much a user data is leaked through mobile apps almost every second app collects data from mobile and send to developers including phone details or even contact numbers. Many of the mobile devices even don't have privacy policy and if they have users are not much aware of them. Today's smartphones can leak not only personal information but location and likes or dislikes of a user which could be used by advertisers or attacker.

3. Corporate Layer

In second layer we bring the issues which are not as much personal to the user but result of corporate activities on internet. As this layer comes out of personal issues of users and its more about tracking the interests or information of user. Not very much of attacks comes in this layer but most advertisers, online marketing, employee monitor systems comes though they all can lead to privacy leaks. Corporate layer privacy loss comes more of user's willful deals for lucrative offers online.

3.1 Online Marketing

The Internet can be useful to businesses for marketing purposes. Through the Internet, businesses can sell and communicate with Customers. The Internet also allows businesses to identify and learn about their customer base. Additionally, many customers expect that a company they interact with in the physical world will also have an online presence. What Consumers may not be aware of is how all of these purposes interact. When a business meets your need of having a website with store hours and directions, it may also meets its need of determining how many customers may want to go to a particular store branch.

3.2 Employee monitoring

Employee monitor and feedback systems in corporate world are quite famous as the employer or any corporate boss will always like to keep an secret or open eye on his employees even though if he gets regular reports from them. Such system are successful because of employers keep these clauses in their work letters so it's always beneficial to read privacy policy before joining any organization further it is also described in privacyrights.org that Individuals who access the Internet from work should know that employers are increasingly monitoring the Internet sites that employees visit. Be sure to inquire about your employer's online privacy policy. If there is none, recommend that such a policy be developed. If you are unsure of what the policy is or if there is no policy, assume everything you do on your work computer is being monitored. In most states there is no law requiring your employer to tell you if it monitors email or Internet usage. In Delaware and Connecticut, an employer must advise employees in a "conspicuous manner" that monitoring is occurring. In Connecticut there is a limited exception for investigations of illegal activity.[1]

3.3 Location Tracking

When it comes about location tracking first comes google as you may not know it but Google tracks your location history unless you disable it yourself. It gathers this data from your usage of Google Maps. You can disable this, and even manually delete certain places from your location history. Any website or app can determine the approximate location of your computer or device by using one of several technologies. If you are using a computer, your IP address can identify your approximate location. Most IP addresses can identify you by your city or metropolitan area. Some can identify a more specific location.

4. Government Layer

This is the layer which is not considered for attacks or any form of cyber issue but it is the layer leads to privacy leaks someway as we all are aware of that governments need to do surveys, surveillance, record keeping of the country person so we can see all this lead to information keeping which could be personal or more. When government does all this they do with authority so data accuracy increases and so increases its value in black markets where data is sold for malicious purposes. Not only record keeping but in recent times one more issue has been in limelight that is snooping which means governments keep an secret eye on personal conversations or call records or other movement though it is used for safety purpose but the big issue is loss of privacy with no intention or acceptance by any person.

4.1 Government surveillance

Government surveillance has been also discusses in in many review papers but here we are referring to the privacyrights.org as there article gives very clear view of government surveillance it is been discussed there as the government may want your personal information for law enforcement purposes as well as for foreign intelligence investigations. Law enforcement generally can access your electronic communications and records in two ways: through wiretapping or through subpoena.[1]

Law enforcement can also use a pen/trap tap to get the following information from your ISP, email, header information other than the subject line, your IP address, the IP address of computers you communicate with, and possibly a list of all sites you visit.

4.2 Government Records

Government keeps records of its countrymen these records could be census record of population which almost contain lots of personal detail. Though these records are kept safe and out of attackers but sometimes these records can get leaked by insider frauds or political moves in a country which mean people loose privacy without even being part of it. No one can deny to give information for such records or somehow they comes under government rules in many countries but when some malicious activity take place in cross country space means attacks to gain information from other country at that time these records leaks data in mass and keeps the privacy of lacs of people in danger. Only good policies by government can keep the privacy secure because these terms comes under government rules no people have in say in these matters as they are done by authentic firms. As published in idtheftcentre.org that "From 2007 to 2011, the Business sector, with a 10-year average of 34.3 percent, represented the largest percentage of breaches, often far surpassing the next highest category. The Medical/Healthcare sector, with a 10-year average of 26.4 percent, took over the top spot in 2012, attributed primarily to the mandatory reporting requirement for healthcare breaches being reported to the Department of Health and Human Services (HHS). In 2005, this category reported the least number of breaches" [6]. This story tell it's in increasing order day by day.

4.3 Snooping

Snooping, in a security context, is unauthorized access to another person's or company's data. The practice is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission.[8] Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device. The US National Security Agency's Prism program - a systematic collection of private user data - has affected people around the world. Protecting yourself from online surveillance is tedious and has other risks. A lawsuit filed by the operator of Wikipedia and other organizations challenges the US government's mass online surveillance programs, claiming that tapping into the Internet "backbone" is illegal. The lawsuit was filed in Maryland federal court by the Wikimedia Foundation, Amnesty International USA, Human Rights Watch and other organizations. It said the effort by the National Security Agency and other intelligence services "exceeds the scope of the authority that Congress provided" and violates US constitutional guarantees. The National

Security Agency is currently collecting the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers, under a top secret court order issued in April.

5. Hacked Layer

Well this is our fourth layer and most uncontrollable by a user as this layers includes all the attacks by hackers most probably due to negligence in previous layers. Hackers uses many mean of attacks and always have lots of purposes sometime there purpose or target might not be a user's privacy but in the end their attacks can lead to loss the privacy of many online users. Hackers could perform DDOS attacks, SQL Injections, Cross site scripting methods or many more of their attacking weapons they have to break a user's safety barrier and leak out their personal information. This layer is mostly uncontrollable by an internet user if he/she doesn't tighten the security policies at first layer that is their individual layer.

5.1 Online Scams

Scammers use email, online ads, pop ups, and search results to trick you into sending them money and personal information. As it was mentioned in an article published on thisismoney.co.uk that "The ten biggest online scams lost victims across the country £670million over 2014 – and this figure is likely to be far higher due to unreported cases, National Fraud Intelligence Bureau data reveals.[10]

The case of a victim known only as Chris, who had thousands stolen by fraudsters who simply rang his bank to gain details and also conned his Facebook friends into sending money too, is highlighted by Get Safe Online.

It comes as a study found half of those who have been a victim of cyber fraud – which includes ID theft, economic losses, hacking and viruses - said they felt either 'very' or 'extremely violated' by their ordeal. Online fraud and scams operate under many different disguises and go by many names, including consumer cybercrime, internet fraud, online crime, and e-crime. No matter what it's called, it causes considerable distress to everyone it affects, and it can even culminate in serious financial problems, as some victims have discovered.

5.2 Malicious Links

Attackers behind malicious spam campaigns have shifted their tactics in recent months and are increasingly attempting to infect victims by luring them into clicking on links rather than sending them malicious attachments.

Since late November, Symantec Security Response has seen a spike in the number of malicious emails using this tactic. Over the last six months, there were relatively few spam emails containing malicious links.[12] For example, in October, only seven percent of malicious spam emails contained links. That number jumped to 41 percent in November and has continued to climb in early December.

While many malicious emails come with an attachment, organizations can block and filter these types of messages. Symantec believes that the Cutwail botnet (Trojan.Pandex) is behind some of the recent spam messages, along with other botnets, and that attackers have resorted to using links in a bid to avoid email security products that scan for malicious attachments. [12]

5.3 Wireless Network Hack

Wireless attacks have increased with it popularity there are many type of sniffers available which cut loose the wireless security and let strangers sniff in personal details of wireless users though most of wireless users now a days uses WEP password encryption still there are many other ways to attack or sniff through an wireless network one of the famous wireless privacy attack is written in blog by Roger A. Grimes on infoworld.com which states that "No hack is easier to accomplish than a fake WAP (wireless access point). Anyone using a bit of software and a wireless network card can advertise their computer as an available WAP that is then connected to the real, legitimate WAP in a public location. No hack is easier to accomplish than a fake WAP (wireless access point). Anyone using a bit of software and a wireless network card can advertise their computer as an available WAP that is then connected to the real, legitimate WAP in a public location.[14]

Think of all the times you or your users have gone to the local coffee shop, airport, or public gathering place and connected to the "free wireless" network. Hackers at Starbucks who call their fake WAP "Starbucks Wireless Network" or at the Atlanta airport call it "Atlanta Airport Free Wireless" have all sorts of people connecting to their computer in minutes. The hackers can then sniff unprotected data from the data streams sent between the unwitting victims and their intended remote hosts. You'd be surprised how much data, even passwords, are still sent in clear text.[14]

The more nefarious hackers will ask their victims to create a new access account to use their WAP. These users will more than likely use a common log-on name or one of their email addresses, along with a password they use elsewhere. The WAP hacker can then try using the same log-on credentials on popular websites Facebook, Twitter, Amazon, iTunes, and so on and the victims will never know how it happened.[14]

6. Conclusion

This review paper defines four layers of internet privacy which defines the type of attacks in each layer there impact and control though most of these attacks are well defined in many research papers but here we divided these attacks in layers to study them in depth and provide an easy perspective for online users about their privacy and security. These four layers can tell where a user need to tighten his/her security policy and where his security relies on other factors then his own. Distribution of privacy attacks in layer can get us to solve the complicated privacy issues. These layers give clear view to users that what could lead to privacy loss and what they could control with very basic steps though no safety

steps mentioned in this paper but there are many research papers which defines security and steps of safety for all these attacks only user need to know the worth of his privacy.

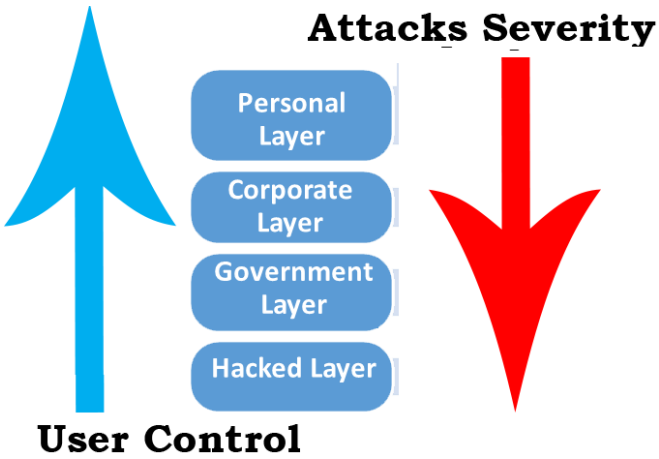

Figure 1.2: Privacy attacks severity & User control

We can see in Figure 1.2 that there are two factors which defines privacy attacks first is the severity of attacks and second is its controllability by user. Users can control the attacks in personal layer more easily then in hack layer. Similarly the attacks intensity in hack layer is always more than the personal or corporate layer. Privacy issue is more to be users understanding and learning about their privacy loss factors.

References

[1] http://www.nbcnews.com/id/3078835/t/online-privacy-fears-are-real/
[2] https://www.privacyrights.org/online-privacy-using-internet-safely https://www.privacyrights.org
[3] http://www.internetlivestats.com/google-search-statistics/
[4] http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/
[5] https://community.norton.com/en/blogs/norton-protection-blog/study-finds-mobile-privacy-concerns-often-traded-free-apps
[6] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html
[7] http://www.ndtv.com/world-news/lawsuit-challenges-legality-of-nsa-online-snooping-745605
[8] http://www.dw.de/what-can-you-do-against-online-snoops/a-16878421
[9] http://searchsecurity.techtarget.com/definition/snooping
[10] http://www.thisismoney.co.uk/money/news/article-2801328/top-ten-online-scams-fraudsters-stole-victim-s-money-conned-facebook-friends-too.html
[11] https://www.onguardonline.gov/articles/0002-common-online-scams
[12] http://www.symantec.com/connect/blogs/malicious-links-spammers-change-malware-delivery-tactics
[13] https://community.norton.com/en/blogs/norton-protection-blog/study-finds-mobile-privacy-concerns-often-traded-free-apps
[14] http://www.infoworld.com/article/2610239/malware/7-sneak-attacks-used-by-today-s-most-devious-hackers.html