Mass Surveillance and Cyber Security

Sohaib Noman Ahmed

October 20, 2018

Contents

1 Introduction

We are living in a age, where the possibility's of technology seems limit less, there are continuously coming new device, new smart phone, with new features and better specs, but is this improvement in technologies a good thing or a bad thing? Of course there a lot of benefits using smart technology, they make life easier, we can use them for almost anything. write documents, take notes, pictures, video, record sound, read the news, talk to each other as part of many other things. Moreover at the same time, we need to look into how this heavily use of technological devices might backfire. One issue is that these device record a lot of information which can be used in the wrong hand for surveillance, also just the idea that these devices exist; like phones, TVs, and cars as increasingly more devises are integrating more and more technology. Back doors or exploits to these systems, can create huge amount of problems that needs to be resolved, for this we need examine cyber security threats.

2 Mass Surveillance Strategies

Mass surveillance have become a hot topic after the headlines made by Edward Snowden on surveillance by the government on their own public. Its hard to believe that the technologies we love can be used this way against us, taking away our right for privacy and starting the conversation about what information, should a app or device be able to store.

2.1 What applications can store

We know that out phones have a lot of capabilities, they can register our locations, store personal information, from names, date of birth to credit card numbers and passwords. This data has a god functionality, which is that it makes life easier for us, since we don not need to type in all out information every time and, with location services we can easily figure out directions from one location to another and the time spent on the travel. All these features can be preformed by the small device in our hand. but we are losing something too, we are giving away our personal information. This might look harmless, since this information is needed for the applications to provide their services to the user, but the problem occurs when they can access information, that is not intended for them. "According to Felix Krause "when a user grants an app access to their camera and microphone, the app could do the following:

1. Access both the front and the back camera.
2. Record you at any time the app is in the foreground.
3. Take pictures and videos without telling you.
4. Upload the pictures and videos without telling you.

5. Upload the pictures/videos it takes immediately.
6. Run real-time face recognition to detect facial features or expressions.
7. Livestream the camera on to the internet.
8. Detect if the user is on their phone alone, or watching together with a second person.
9. Upload random frames of the video stream to your web service and run a proper face recognition software which can find existing photos of you on the internet and create a 3D model based on your face.” [1]

This is clearly more personal data, then most people would except the app they are installing have access to. I wanted to figure out for my self, how easy it can be to store information about people from a website, so a made my own using HTML, CSS and some logic from PHP. from the surface it look like any other website, but do we really know what kind of information a website is storing? Well my friends didn’t know, I made them take a look into the website and with some simple code a could store the IP address of the user and also what device they used to enter the site. The information gather is listed below.

```
193.157.162.50:Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36 -
besokte den - 2018.10.31

193.157.175.146:Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36 -
besokte den - 2018.10.31

193.157.173.182:Mozilla/5.0 (iPhone; CPU iPhone OS 12_0 like Mac OS X)
AppleWebKit/605.1.15
(KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1
- besokte den - 2018.10.31

2a02:2121:307:caf1:c1e9:3d7c:6073:eae0:Mozilla/5.0
(Linux; Android 8.1.0; ONEPLUS A5010) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/70.0.3538.80 Mobile Safari/537.36 -
besokte den - 2018.10.31

81.191.172.126:Mozilla/5.0 (iPhone; CPU iPhone OS 12_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148
Safari/604.1 - besokte den - 2018.10.31

81.191.172.126:Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
```

[1] https://www.theguardian.com/commentisfree/2018/apr/06/phone-camera-microphone-spying

```
(KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36 -
besokte den - 2018.10.31
```

The ip address could tell me where the person entering the site is and the device could tell me who was entering the site, since I know what device my Friends use. Now none of this information is that harm-full, but even-less no one of my Friend knew what I was storing, and I could easily monitor when they where entering my site. The information we know giant firms like Facebook, Google etc.. are storing are a lot more sensitive then what I was doing, what about the information we do not know they are storing.

2.2 PRISM

With all these information in our phone, it makes us vulnerable if someone who can gain access to it. According to the revelations from the Guardian the NSA does have access to this information. Under the undisclosed program named PRISM, NSA could access directly into the servers of giant firms like Apple, Facebook, Google, Yahoo, Microsoft including many others. The information they where able to obtain includes email, video, audio, photos, search history, file transfers. While this is happening the firm owning the data claims, that they do not give away personal information of there users to the government. [2] When the big firms are going to deny the fact that they are giving the information stored on there servers to the government, the question of trust comes to mind, who can we trust? and if we cannot trust the government what solution do we have to this problem? We will discuss this in the section making good applications later.

2.3 NSA "Hacking unit"

Tailored Access Operations is the names of the division of NSA, also called the NSA hacking unit. it consist of a elite team of hackers, who try's to figure out methods to hack into devices steal the data and insert spying devises into the computers, so they can have undetected access to their targets. The security wholes discovered by this team, are used for their own exploitation. [3]. So even if we are able to find a solution to big firms giving away their information to the government we can still not be completely protected, since the government are working to get that data them self, we will look deeper into cyber security later.

2.4 Backdoors in encryption

While making their own backdoors, NSA has not just made other firm build in back doors to their information, but even if the information is encrypted their still is a way for the NSA to get hold of that info. This strategy, consist

[2] https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[3] https://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao

making weak encryption algorithm to build in back doors into encryption, they reportedly paid of RSA 10 million to use their weaker algorithm instead of a more superior. [4], which arguably goes against the whole idea of encryption, since these backdoor can be exploited by hackers to, and put people in risk even if their data is encrypted.

These are only some few methods, there are several methods used to gather information about people, but by only looking into these, the point comes across, which is the importance for trustful security on our devises and re-evaluating the need and harm access to our personal information can have, this is what we will look into now.

3 The need and harm of mass surveillance

3.1 Criminal activities

One of the possibilities with having this much information about individuals, is also one of the common excuses used for the tracking techniques used to store sensitive information about people, and that's is fighting terrorism. Its true that with all of the information that is stored by the NSA they do have the information about people who ends up with doing criminal acts, and they can access this information to look at signs of a potential attacker in the future. One other benefits is that with having information about people stores, people get less motivated do do criminal activities as they know that there identity can be trace backed to them, and you might be able to find out where people who may have stolen cars are hiding, information make is easier to solve these cases and this does not only include hurting someone physically, but also in field of economy and politics as forgery and corruption.

Meanwhile the problem occurs of miss classification if a person with out any intent of a criminal activity starts getting looked over as if he is, that raises concerns even if you mean that a state should be able to track the information of their people. That is a issue we face when storing to much information, its hard to really use that information, all the latest terror attack may have been inside the record of the NSA, but its hard to make any use of that when their is to much data. This might be the reason that those attack did not get stopped, if you ask me, the best way to counter these attacked is by getting information from the inside, from the people around or the community that might have individual capable of performing such attack. That's a much better source, then by only looking at features you decide might have a relations with terrorism, which makes it a lot easier to miss-classify innocent individuals.

[4] https://www.theverge.com/2013/12/20/5231006/nsa-paid-10-million-for-a-back-door-into-rsa-encryption-according-to

3.2 War front

Where mass surveillance pays a huge tribute is in the war front, having information about your enemies and there strengths and weaknesses can be very beneficial when preparing for a war against someone. the well know quote from Sun Tzu comes in mind "If you know the enemy and know yourself, you need not fear the result of a hundred battles." [5]. So when this becomes a race, then its almost impossible to stop a countries from participating and you cannot longer blame the leading force for its activities as this can be justified by the name of protecting them self against treat from overseas. Then again we are facing the same problems as with the cold war and the arms race that was present, therefor we need some kind of regulation, some agreements to stop this before it escalates to far.

3.3 Making good application

The other part of the problem lies from the information stored by the popular app like Facebook, twitter , Google etc. but we cannot deny that this information is making our life easier to live day by day. Even in the research field the contribution this has to big data, machine learning that are creating unbelievable product like IBM Watson, is something to miss out if we regulate these companies to not be able to store the information they self seem necessary to give out the best product they can. so it almost feels necessary to let huge companies to get the information they, and even the public cant think of the idea to live without Google or Facebook.

One solution for storing personal information is to store it on your own device and not a remote server, so that no one can access the information unless your self and the people you share the information to, one popular app using this technique is Signal along side having end to end encryption. [6] This might still pose some problems, as there still are backdoors to the Phone itself, and when you want to make innovation in fields like medicine and psychology where most part of the information is personal and very sensitive, then this information needs to be sent again to everyone wanting or needing access to it.

3.4 Privacy and control

While we are talking about watching the action of other people, we also coming into another issue that of privacy, how much should someone be able to know about other people. Most would agree that tracking someone who might do an illegal activity should be allowed, as it can stop a greater tragedy, but every one should also be able to have the right of a private life. So when

[5] https://www.goodreads.com/quotes/17976-if-you-know-the-enemy-and-know-yourself-you-need

[6] https://www.wired.com/story/ditch-all-those-other-messaging-apps-heres-why-you-should-use-signal/

tracking go from tracking people who might do some criminal act to tracking almost everyone of that persons family, to their family ect. This is a breach of privacy. People have right for a private life, someone might be belong to certain religion, certain sexuality and need some kind of protection from the outside society, or some one might just do unmoral act that do not directly harm the society, all these thing can be caught up when tracing so much data. This information can then be used against people who might fear for their health and well being, to make them act in the way some one want, as the government want. Blackmailing can occur to make people spy or do more illegal or even criminal act so their privacy may not be public.

The potential of undermining the puplic becomes larger after noticing that this can be used to record protester and people posing a opinion on the government or the state. after it was revealed that the government was really monitoring the black lives matter movement in the united state. [7]. You start wondering can the government control what is expressed in the public? can they control your action or in someway dictate what you can or can not do in a society. Some alarming thoughts come to mind, isn't this the same kind of techniques used by oppressing states ta remain their control over their people.

Furthermore we need to ask our self, what kind of society we want to live in. Of course we do want security, but shouldn't people be able to make mistakes, and not being worried about every single move they make? A lot of creative, successful people has have rough past like Frank Abegnale who used to forge check and later after being caught worked for the FBI to stop the actions he self was doing in the past [8]. Dont we want people to have a second chance, do we want to live in a society where you need to be concerned about very move you make? these are the question we need to ask our self before agreeing to the methods used by the government. I could believe if those surveillance programs where something that has in the public eye, the NSA would have difficulties to start them from the beginning.

[7] https://www.aljazeera.com/news/2017/11/documents-show-monitoring-black-lives-matter-171128110538134.html

[8] https://en.wikipedia.org/wiki/Frank_Abagnale

4 Types of Cyber Security threats

After looking into state surveillance we know know about the possibilities and harm that can be done by being able to get the information of someone. But in the age we are living with technology every where in hour house, the light, microwave, cars, factories, power plants. cyber security is defined as "Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks." [9], to have a protecting we need to make sure that people who are not authorized to use a system cant use it, or who are not authorized to see or have control over data cant have it.

4.1 Malware

Malware or malicious software can be found in download able program, and are used to attacked some one computer. They can come in many shapes like viruses, worms, trojan horses, spyware, adware. Viruses are software that can hide inside the computer and make copies of itself to then attack, or destroy files. Unlike viruses trojan horse do not try to reproduce it self into files and directories, they usually masquerades as a normal program, ant then can be used as backdoor to get information from the computer. To be protected against malwares there are several anti virus programs, and security tools out there. [10]

4.2 Ransomware

Ransomware is a type of malicious software that is used to attack a person computer, so that usually the person can not access his files or data, the files and data can be encrypted and the attacker may want some ransom to have the files decrypted. It is difficult to track the attacker, and this type of method have become a lot more popular over the years. [11] There are lots of problems facing this kind of method first will be what if hospitals, banks is attack along side private persons, they almost have to give the ransom, since the information is so important. One way to counter attack ransomware is to just get better at backing up your information, so that if you might get attacked by a ransom ware, you do not need to pay the ransom, as you can just download your files back to the computer.

4.3 Social engineering

Is a method to trick a person to give away information that should be stored or protected, this can happen in many way, but the baseline is to figure out how people think about security so that they do not understand that they are getting tricked, but feel safeguarded. [12] There is difficult to figure out how you

[9] https://searchsecurity.techtarget.com/definition/cybersecurity

[10] https://en.wikipedia.org/wiki/Malware

[11] https://en.wikipedia.org/wiki/Ransomware

[12] https://en.wikipedia.org/wiki/Social_engineering_(security)

can stop this method, since we are almost reading every day about new tricks, and new people who have been tricked. There are two ways to attack this issue, one to make the our information more secure, so that the methods, used to lure sensitive information, get more difficult, the other is to just make people more educated of security in general. To look deeper into this problem we will look at one common social engineering attack called phishing.

4.4 Phishing

Is a form of social engineering, to get a persons log in information, password etc. this comes from emails that may look like its from a bank or a service you trust, so that you may type in your personal information. Common uses of this email is to scare you to take action, therefor its important to read the mail carefully for signs, also they want you to click a link so you get to their site, where they need you to type in the user name and password and may include misspelling, the generall rule is to never give away sensitive information to an email. [13] This can extends beyond that, just some watching you type in your password, or you can see some employee type in their pin code. Therefor we need protocols, to make sure that if you see a employee type in his pin code, and you get hold of his card, you should not be able to access all the information for the place he is working, and depending on the employee most should not have access to information that is sensible for the place.

4.5 DDos Attacks

DDos attack is a attack, preformed by several distrubuted sources, which try's to enter a website, so that the website can not achieve its regular service. This may affect the website to not be able to provide its service, for some time. These kind off attack usually targets high profile web servers, like banks, payment gateways, revenge, blackmail and activism. [14]

5 Problems facing cyber security

5.1 New technology

The reason for cyber security comes from improvements in technology, and the more new technology we make the more cyber security we need, and the treat of attacked increases. Since cyber security in itself is a consequences of innovation in technology. How can we protect our self completely from attack? well you cant, trough social engineering hacker exploit human fault, and these there is hard to get rid off, for now we need to make a computer securer and not "bulletproof", first thing to consider is to updating the operating software these update usually comes for a reason, and that is to fix security whole discovered in

[13] https://www.youtube.com/watch?v=9TRR6lHviQc

[14] https://en.wikipedia.org/wiki/Denial-of-service_attack

old version, beside just improving the OS in itself. you should also run anti virus programs to check if there already is harm full software on the computer. [15] It still might require you to just be more aware of the security threats, because none of this procedures can guaranty security, as hacker probably also know about them and are also working to counter this protection strategies.

5.2 Unauthorized control over other equipment

If you can hack into another persons, phone, pc or car. and perform actions you are not supposed to be authorized for, this can be used for a large amount if difficult situation, as taking control over a persons car while being authenticated as the driver, you can make en crash look like an accident, the possibilities for performing action that can make it seem like the hacker are the ones with the control over the society. this only increases the reasons for secure system. Therefor firm creating this technology need to be certain of the product they are releasing or at go through some qualification. Now days we can buy thing overseas like mobile phone and computer with no certainty that they are not bugged. Sooner or later some regulation need to take place.

5.3 Cyber warfare

While these attacks are happening, countries also stat using them for cyber warfare, the first example that comes in mind is the attack from Israel on Iran, where the created a malware by the name stuxnet, that was used to destroy Iran nuclear centrifuges. [16]. this almost create a arms-race, and the future warfare could be fought through the cyber world. the country that are in front in the cyber security as well as attack es, are the countries holding the power, and it becomes incumbent for other to built there own, even thou the systems created can make more harm then good.

[15] https://www.theguardian.com/technology/askjack/2015/jan/15/how-can-i-make-my-pc-completely-secure

[16] https://en.wikipedia.org/wiki/Stuxnet

6 Conclusion

6.1 Mass surveillance

Both for cyber security and mass surveillance there is no clear solution to these problems, every solution has its give and take. There is a good start to make application store the data they require in the device of the owner like the app Signal. This can not be done for every information, and takes away a lot of possibilities of storing information everywhere, since if a message is stored in the phone application it is not reachable on the computer application. On other option to have some regulation on what firm can store of personal information when they can not provide the security to protect that information from the state and more options to the user to choose what is stored and not, of course the backlash with this is that firm that have created really good product now cannot function in the same way as there are limitation to what they are able to get from the user, but this scarifies might be needed for better protection.

6.2 Cyber security

For cyber attack, wee need protocols to prevent key to get in the hand of attacker as well as if they do the key do not expose the whole firm, but only limited access the key holder had. also we need to involve out self for the protection against treat, we self even you and e can participate with having better password we lower the risk of cyber attack. a 4 digit number can be brute forced with 2^4 possibilities, which is easy for a computer, the more common thing, what also a group teacher at university of Oslo told me was to use a sentence, since you need to multiply the number of word in the alphabet, with the count of word in the password to brute force through it, and this is even difficult for a computer as it takes huge amount of computing power. The threats will be there as, new technologies will be created, so we need always try to be a step a head, of the attackers.

7 References

1. https://www.theguardian.com/commentisfree/2018/apr/06/phone-camera-microphone-spying

2. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

3. https://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao

4. https://www.theverge.com/2013/12/20/5231006/nsa-paid-10-million-for-a-back-door-into-rsa-encryption-according-to

5. https://www.goodreads.com/quotes/17976-if-you-know-the-enemy-and-know-yourself-you-need

6. https://www.wired.com/story/ditch-all-those-other-messaging-apps-heres-why-you-should-use-signal/

7. https://en.wikipedia.org/wiki/FrankAbagnale

8. https://www.aljazeera.com/news/2017/11/documents-show-monitoring-black-lives-matter-171128110538134.html

9. https://searchsecurity.techtarget.com/definition/cybersecurity

10. https://en.wikipedia.org/wiki/Malware

11. https://en.wikipedia.org/wiki/Ransomware

12. https://en.wikipedia.org/wiki/Socialengineering(security)

13. https://www.youtube.com/watch?v=9TRR6lHviQc

14. https://en.wikipedia.org/wiki/Denial-of-serviceattack

15. https://www.theguardian.com/technology/askjack/2015/jan/15/how-can-i-make-my-pc-completely-secure

16. https://en.wikipedia.org/wiki/Stuxnet