Michael Guidry
June 8, 2017
Mass surveillance falling short on delivering its promises of security

The processes and information explained here are all theoretical regarding how these systems may work, and I do not condone manipulating the platforms realistically. It is to show how vulnerable the entire country is due to these systems. I take no responsibility for anyones actions if you proceed to try anything shown here as an example, or otherwise.

Mass Surveillance has been in the spotlight for a few years now. The most extensive information regarding it has been leaked by Edward Snowden. It has caused damage to United States interests, and technology corporations worldwide. The United States is not the only government using these technologies. It is publicly known to be used by Australia, China, France, Germany, India, Russia, Sweden, Switzerland, United Kingdom, and privately by several other regimes worldwide [1]. The information being gathered includes telephone records, e-mail, social media posts, banking transactions, search engine history, and various other sources of information. The information is vast enough to require specific data centers just to contain, and process the information.

Surveillance programs place equipment at telecommunication corporations, or Internet backbone companies which redirect data throughout other parts of the world. The protocols used on the Internet were not designed to have the information siphoned using these techniques. The result is a technology that will never be ultimately secure. The amount of information alone is too much to hire any amount of employees to help process. It requires software automating the billions of calculations for each record required to analyze, and prioritize before a human analysts ever sees the entries.

The Snowden leaks caused damage to government interests that goes well beyond technology exports from their territories. Indirect problems arise whenever a country decides to stop using Cisco products for the alternative Huawei products from China. The products may contain different features than the American counterparts. It is possible that they contain Chinese specific back doors. It gives a long term disadvantage to America’s geopolitical posture due to intellectual property theft losses in those regions. It also means that a different superpower will get involved in various events happening within those countries as well. It essentially can be figuratively thought of as America moving out, and China is on the way in. I doubt the United States military expected that creating surveillance programs would end up causing more problems than what they were attempting to resolve. Washington has publicly admitted its fear of Chinese technology [3].

The various sources of data processed by mass surveillance programs:

E-mail Sources from SMTP as Transmission, POP as Receiving, or IMAP as receiving

E-mail was the initial area the United States government began monitoring using the publicized Carnivore program. Electronic mail has many issues such as a vulnerability allowing falsification of source e-mail addresses address without requiring direct access to systems whatsoever. It just requires the e-mail addresses of both parties. It ensures that these programs may always pick up falsified information which is purely fabricated to manipulate their systems. It is possible to ensure that these e-mails would look like Spam to normal providers such as Google Mail. It would have the consequences of the user never receiving the e-mail, although the surveillance programs would have processed that as if actual intelligence was contained inside of it. Nothing can be done to fix this situation.

Telephone services such as land lines, cellular, or voice over IP

Caller Identification information is used to link two entities inside of intelligence databases. Voice over IP (VoIP) in the recent years brought ability for small businesses to falsify Caller ID information allowing them to place outgoing calls under the numbers that they had purchased. It was widely publicized whenever people would call 911 from a particular phone number and claim that they were doing various illegal activities [5]. The purpose was to push for Special Weapons and Tactics (SWAT) to raid the house in question. It had even resulted in someone being shot accidentally in a unfortunate case. It is extremely simple to falsify call records to allow particular thresholds of intelligence databases to recognize. The technique is called Automatic Number Identification (ANI) spoofing and it is regularly used during normal VoIP operations within Asterisk telephony software [11]. It is important to remember that this tactic works against land line, and cellular phone networks because only one side of the connection needs to be falsified as a different intended source of the call. It means that you can call a number falsifying the caller identification information of a suspected criminal, or terrorist to trigger investigations on that individual.

Web Traffic

Web browser traffic is being monitored by many Internet providers in a lot of regions of the world. It is of current concern since the Federal Communication Commission (FCC) is in the process of changing regulations which would allow Internet providers to sell the data that they are capturing from their customers. The funny part is that it will allow any private corporation worldwide to buy the same exact data from them that citizens had a problem with the surveillance capturing. It would also contain mobile application sessions as they contact servers for performing operations. It contains various different sources of information. The applications on iPhones, and Android would usually fall into this category. It is all traffic that is over the HTTP protocol but also covers massive amounts of protocols, and applications which fall back on HTTP.

Social Media (PRISM)

Social media specific web traffic has far surpassed regular web activities within the past decade. It is a major resource for probably all current intelligence research operations. The information usually flows through the PRISM program. It happens over HTTP although is considered different from other web traffic because it is covered by PRISM rather than secret surveillance taps on fiber backbones. The social media information is different technically because the companies themselves have already processed the information. The surveillance programs obtain the data without having to piece together each packet thus it wouldn’t have the same vulnerabilities. The resulting data is however processed using all of the same algorithms at later stages of these operations. The final product ends up in the X-Keyscore database as well. It is therefore still a major infliction point for attacking these programs. The vulnerabilities could be as simple as having similar names, spaces or other character variations in user names, or other tactics used for Phishing campaigns [10]. It would depend on how technologically proficient the analysts is with the various skills being used by attackers.

It is very significant to understand that the surveillance platforms are taking unproven identities from social media and cross linking this information with actual citizens. It is absurd

that defense contractors are charging the United States government the cost they have been for unverified identities tied to various misinformation on a real time basis.

PRISM relies on Section 702 of the Foreign Intelligence Surveillance Act (FISA) court to obtain information regarding targets through Internet technologies corporations. It is subject to the same vulnerabilities that any other type of software contains through engineering, or structural errors. The difference is that the government coerces a secret arrangement on corporations with automated technology regardless of repercussions. It is ridiculous that these corporations may lose business, and reputation due to a situation that isn't currently within their legal rights in America. It is improbable that using techniques to prove involvement wouldn't become an absolute winning argument for the next several years while ways of performing these tasks are designed.

Proof? Catching PRISM in action…

If you'd like to determine whether a company is actively involved with PRISM related surveillance mechanisms then you you can follow a few simple steps. Start by picking a random suspected terrorist from the watch list, or other resource on the Internet[12]. You will need to create a new identity "A" as a new social media identity under a name preferably without other social media presences attached to it. Identity "A" should be created on the social media company that you wish to verify is or isn't a provider in PRISM. Identity B is another identity that you will need to fictitiously create on a social media platform that you are already positive is within the PRISM program due to leaks.

You should post links on Identity "B" page, or time line containing ways of verifying automated tasks are performing checks, or analyzing the account. An example could be a web hosting script which logs geographical locations, and other factors regarding connections to the web server. Another possibility would be to log host names from Domain Name System (DNS) requests and use unique host names for each individual attack. The unique parameters should be posted to the social networking account of identity B. The purpose is to ensure only someone that looks for that profile, and attempts to visit would ever actually end up there. If this is a new social media account then it shouldn't have anyone that accidentally lands on the name which doesn't show up anywhere else, and has no friends.

Next you would post to identity A either by link, or by adding as a friend for identity B. The final step would be to distribute information for surveillance taps, or PRISM networks regarding relations to the terrorist suspect that you had picked, and identity A. It would mean that if anyone falls within the various links, websites, or other actions you prepared for on the social media page for Identity B then you have just turned PRISM into a scripting language essentially that you can manipulate.

Theses bugs relating to PRISM will continue to be a cat and mouse game like the other issues with surveillance taps. The same mechanism used to bypass the surveillance taps will end up being used for social media or PRISMS sources. Each particular platform will share the same security features which will be used for both applications as the game proceeds. How many information leaks will take place before people shutdown these systems? I bet nobody will actually know.. literally. How much faulty technology putting government, Americans, and subsequently the world at risk can defense contractors slab off to the United States government?

Financial Statements

Financial information is only recently being proven as a source of intelligence [6]. Credit card

purchases may give insight into habits of a target. It may help link separate entities in databases together by merchant, or location. It is unclear publicly how it is used in detail outside of wire transfers. It would be smart to assume that the details of credit card transactions could be used just as well to manipulate these systems. It wouldn't require much time to use Square, PayPal, or other services to help in an operation. The wire details may also be thrown directly into these databases.

Examples of exploiting these programs:

Adding someone to America's terrorist watch list

The most used public reason justifying removing citizens privacy rights relate to terrorism. It is important that all terrorists are found, and their organizations dismantled before they cause more damage to the US, foreign interests, or the world. It would mean that the processing of information for these purposes should be pretty fool proof.

If justification of FISA statues are taking place then what would it mean to be able to falsify a citizen as a terrorists? Does this mean that the systems do not work? Does this mean that maybe things have to be reconsidered? It definitely will bring up several other questions regarding processing of information, and the conclusions drawn from that information.

An example of a theory regarding how a possible person may be subjected to being forced onto a terrorist watch list is literally only requires a few steps of work to accomplish. You would need to identify a particular terrorist group of which you wish to portray a connection amongst [12]. You should study all information available. It requires you to have some concept of locations, or ability to fabricate information tying the terrorist group, and the target individual together. You would need to falsify social media accounts, and also possibly create virtual connections for surveillance taps to proceed manipulating these databases. Once you are fully prepared with the virtual session PCap files then you can use various tools to replay each side to manipulate the surveillance program. You should also falsify call records, e-mails from similar names, or possibly even going as far as manipulating credit card merchants to show connections between the two entities. This process may need to be repeated depending on how many connections, and how much information your messages contain. If you understand the publicly available information about these platforms then you will understand that is it a concrete yes that it will work. Documents have leaked in 2013 regarding homeland security's handbook for determining if someone is a terrorist or not, and this could be directly useful for this type of manipulation [13].

Financial gain from exploitation of surveillance platforms

Individuals, or corporations also have the ability to falsify information for financial gain while exploiting these programs. It is inconceivable to believe that false intelligence results on entities, or individuals is as far as the problem will extend. What if you wanted to hurt the reputation of a competitor? The most convincing way to hurt the reputation in my opinion would be to force investigations, or other publicly shown situations on the competitor that you wish to cause a negative impact. If it is a publicly traded company then it is possible to cause dives into stocks by leaking information simultaneously to news outlets. It is really tough to refute the amount of damage that will actually occur from planned actions such as these.

If you were to attempt to test this scenario then you could try to pick a corporation on a publicly traded list such as NASDAQ. You should fabricate a story for ensuring bad publicity over FBI, or other

intelligence agencies obtaining your falsified story. You should integrate concepts such as sensors to determine if, and when the information has been acted upon by government, or law enforcement alike. An example of this would be to include a third party which could be monitored on the Internet by web camera. It would allow a virtual untraceable mechanism to determine when the actions take place.

A simple example would be using Boeing and a security consultant company if you were also a security consulting provider. Boeing has various government contracts worldwide therefore must keep to a high standard. If you were to leak, and manipulate information for government databases to become populated with details of this security company selling exploitation technology to underground criminals then it would almost certainly damage their reputation beyond repair. Boeing would begin to consider other competitors, and the surveillance programs of governments just helped you succeed in developing business contracts by their vulnerabilities. The story would more than likely be believed worldwide as to the usual previous connection between hackers, and the criminal underground.

Triggering a nation's cyber warfare policies to attack an innocent third party nation

Einstein is a government program publicly presented on the Homeland Security website [8]. It claims sensors in government networks observe, and notify whenever hacking takes place. It is inconceivable that the analysis platform for Einstein is not also using the same technologies directly on all of the other web connections being found on these surveillance taps. Government classified networks operating on the Internet are classified, and usually not under government cover [9]. Any of these covert servers wouldn't be covered by Einstein therefore would fall under mass surveillance territory. It would give direct ability to manipulate the reporting of these networks to falsity reports of hacking from another intended source nation.

America has automated systems for hacking targets worldwide using mechanisms such as Quantum Insert to exploit their web browsing sessions. It should be expected that certain aspects of Cyber Warfare policies are tied directly into these surveillance systems as well. It would be ridiculous to assume that it is only for intelligence information regarding individuals, or corporations. It more than likely actively gathers all possible information regarding the majority of web connections happening. It would include hacking attacks being stored alongside the other intelligence information. Some information regarding X-Keyscore has surfaced which discloses searching for logins, and passwords for particular servers. If the databases are being populated with information such as this then it means that you could trigger results of these Cyber Warfare policies individually without ever having any nation state having anything to do with it. The problems arise whenever you are triggering it directly forcing their networks to believe it is another third party.

Future of mass surveillance

How many times would these circumstances have to take place before people begin to dismantle these programs? The sheer fact that there are an unknown number of vulnerabilities shows how ridiculous these programs really are in the long run. Could you start an actual war manipulating these programs?

Tools for examples of exploitation

An attack called "Fourth party" will allow you to manipulate these surveillance programs by using

virtual intelligence. The intelligence is virtual because it is fabricated, and placed strategically into the surveillance tap with means of manipulating it. You would need to pick a particular identity, or several such as terrorism as the example earlier. You have to have some concept of where surveillance taps exist in the world. You can find this information from documents obtained by Edward Snowden leaking classified United States intelligence. NSA, and GCHQ have a large amount of surveillance taps between America, and Europe respectively. I would personally target Europe although cloud providers such as Amazon data centers in America contain servers for a variety of companies, and social media platforms.

You need to find web servers which are known to be of interest to their surveillance programs. I am sure any social media, blogging, or communication platform is a good choice. You should find a server within the same data center, or IP ranges. It should be possible for their platforms to assume the IP address is an authentic server of the website your attempting to falsify messages within. An example would be starting an EC2 instance in the same AWS region as some social media platform. You would then use a server, or connection in the region of the end user that you are wishing to falsify information as. If you are attempting to falsify some terrorist to attempt to trigger some police response then you would want to use a dial up, server, or proxy in their city, state, or country.

You need to create a request using a real web browser towards the social media platform. You could try with a messaging feature as long as the information for triggering the surveillance platform is noticeable in the raw HTTP request. It would not be smart to target a platform which uses encrypted, or secure (SSL) connections because you wouldn't have access to their secret keys. You should copy the response from the authentic platform, and upload it to your server which is located near it. You should place it exactly how the real provider's files are handled. It should look exactly the same whenever you repeat the request. If it worked out, and seems identical with a debugging proxy then you can ensure that the information was queued into the surveillance platforms for analysis. If you were to have used some other name along with the terrorist identity then its probable that they would become known associates depending on the message. You just manipulated a multi-billion dollar a year platform created by intelligence agencies.. for intelligence, and abused by the "best hackers in the world." (NSA/GCHQ) Go you. ;)

Another way exists which could be used to perform mass injections which would be clever for attempting to game the system for financial benefit. You could merge specific profiles, and keywords together in crafty ways forcing various types of categorization which may result in information leaks. The possibilities is any e-mail of anyone world wide possibly being put through an analysis engine with some other profile, or trigger where you could attempt to determine whether particular words, keywords, or situations exist between two arbitrary entities in our world. Essentially you can gain insight into almost anything in the world that is captured by their systems. It would require some testing, crafting, and extensive work but it would be worth it in the end. I believe it could be used to determine if stocks may go up or down if you were able to manipulate it successfully in the correct ways. Every word in messages going to people will alter the state machine of their analysis engines. It would also branch off into other topics, or people's profiles. It is quite magnificent how much of a major issue these vulnerabilities really are. That is the creativity side required.

If you wished to perform the network side to get the information injected into the surveillance taps databases then you would want to setup various servers worldwide targeting different social media platforms, e-mail systems, etc. You would want to either use dial up, or obtain access to actual residential, and business IP addresses. It would be preferable to have raw socket access because it would be required for most of the circumstances with packets. You wouldn't need to be directly on the

same AWS region. You could spoof that server's IP address towards a profile, and I'll continue to use terrorist as an example because of the earlier information. You would then on the profile's side spoof packets back towards the server. The point is that you can use real IP addresses of these servers, and clients if you obtain the information. You just have to be on both sides of the surveillance tap. If you know a fiber tap exists between Paris, and London then you would want a computer on each side. If that tap is also gathering traffic for user's in London talking on Paris message boards then you can falsify any information whatsoever regarding those users directly into the surveillance databases. You would just need to send spoofed TCP packets of both sides of the connection. It means that it cannot be an actual web browser performing the connection. It would need to be separate Pcap format files. Each file would have to have the packets being sent. It would mean that to the surveillance tap it would look like a real connection. In the end, each part of the connection may send back some packets since the connection doesn't exist, and it may attempt to let the other side know by ICMP packets such as port unreachable. I highly doubt the surveillance taps are processing extensive details into every connection if you just continue to send the packets correctly in order waiting for the other to receive, and send back an acknowledgement. This entire system should be scripted, and contain several mechanisms and known triggers for their analysis engine to gather more information using URLs, etc. I am giving you an overall concept of what is possible. I have not developed the attack although if you understand how surveillance taps function then it is fundamentally possible.

The other way would be to use a social media network regularly and just use various modifications for the identities to link it with things such as a 'terrorist' for example. You should attempt to use two middle initial characters, small spelling changes, or other simple factors that will allow you to falsify the account in tune with a particular identity.

References:

1. https://en.wikipedia.org/wiki/Mass_surveillance
2. http://www.zdnet.com/article/snowden-prism-fallout-will-cost-u-s-tech-vendors-47-billion-less-than-expected/
3. http://world.time.com/2013/04/04/huawei-the-chinese-company-that-scares-washington/
4. https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2769645
5. https://www.911.gov/pdf/PublicSafetyInfo-Swatting-may2015.pdf
6. https://www.rt.com/news/384796-hackers-expose-nsa-financial-spying/
7. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
8. https://www.dhs.gov/einstein
9. https://arstechnica.com/security/2016/10/new-leak-may-show-if-you-were-hacked-by-the-nsa/
10. https://en.wikipedia.org/wiki/Phishing
11. http://www.hackerschronicle.com/2011/11/voip-hacks-how-to-spoof-your-caller-id.html
12. https://en.wikipedia.org/wiki/FBI_Most_Wanted_Terrorists
13. https://www.start.umd.edu/gtd/contact/