Michael Guidry
April 7, 2017
Intelligence agencies blindly place backdoors into our economic systems

Government surveillance taps bring vulnerabilities into many different areas of government, and social mechanisms. The taps are placed at critical Internet backbones which allow monitoring of millions of Internet Protocol (IP) addresses simultaneously. It is critical for them to be placed at these backbones for various reasons including being invisible, having physical security, and obtaining information on as many networks as possible. It also brings new types of vulnerabilities into the world which are previously undocumented. Britain's Government Communications Headquarters (GCHQ) having 200 taps on various fiber backbones brought this type of vulnerability to my attention. It shows just how far reaching surveillance taps are, and that manipulating them is thousands of times easier than I've considered until now. GCHQ's taps are important because they monitor networks connecting USA, Europe, and the Middle East. It more than likely carries a large portion of Asia traffic through those links as well. It is impossible to analyze their amount of daily events without automated systems in place processing the data in a first stage scenario. These systems are where the vulnerabilities lie.

Financial markets are extremely important within our society. It helps companies raise capital to invest in further resources required to expand. It gives the investors buying shares the ability to generate revenue by betting on their future. Hedge funds invest peoples retirement, and the entire world is interconnected through these markets. The economy crunch of the last decade makes it simple for anyone to understand how important financials markets are within the banking system. Shares are traded constantly by humans, and machines alike. High frequency trading is used by the top banks on Wall Street, and more than likely in most markets worldwide. Russia is particular because it doesn't have laws against insider trading. All trades are based off of accumulations of dozens of data sources changing at an ever expanding pace. The Internet is the main mechanism of information sharing worldwide at the current moment. It is the most important resource of advancement for humanity.

Imagine being able to use information leaks in surveillance taps to determine whether stocks will rise or fall. It is something that I highly doubt anyone previously would have suspected possible. The surveillance programs are generally considered black boxes to all citizens. Intelligence agencies could read through mass surveillance events to find insider information on stocks. It is illegal which is why governments require security clearance to obtain access for investigative purposes. It is not currently public knowledge that information leak vulnerabilities in these systems can give equally important information to attackers. It doesn't even require direct access and could be completely silent to the government. It is horribly simple to perform, and there is no true way to protect against it. Injecting into their databases is required to perform these attacks. It will be a new area of cat and mouse until these programs are dismantled.

An example of why surveillance programs are currently thought of as extremely important relates to Islamic State in Iraq and Syria (ISIS). ISIS is using recruitment campaigns, and propaganda online in various countries. It is important for governments to monitor possible extremists constantly. Its a good reason for using surveillance taps for mass surveillance programs to find these needle in haystack situations. Governments spying on each other is nothing like what we face with these situations. Spying will always be of concern, and continue for the extent of life of earth while having multiple governments. I do not believe these

surveillance programs are necessary to deal with those types. Corporations spying on each other is even of less importance. The data captured is filtered in ways obtaining possible extremists related keywords, or many other factors. When found it would be escalated for human investigation from an analysts for possible further review. It requires a massive amount of processing to be performed on the data before it ever reaches an analyst. No other method exists to find these recruiting campaigns as they are also ever changing. If your solely looking at citizens obtaining new passports, and flights to the Middle East then it is too late for those individuals manipulated.

The processing of the information from surveillance taps has vulnerabilities like any other software application. Every type of known software attack needs to be reapplied, and tested against surveillance systems. Examples of possibilities may include timing attacks, Blind Structured Query Language (SQL) like scenarios, or numerous situations which are inevitable due to general computer science techniques used in all applications. It is not really a black box which has no connections to the outside world. It is a necessity that these databases have cross connections linking to similar events, or other areas of interest. I'm assuming a large portion of the information in this manner. This fact means that surveillance programs will forever be fundamentally flawed. My first suggestion would be to filter out publicly traded companies although then they would become a known method for bypassing these systems. It proves difficult to create filters that would allow these financial institutions, or companies to somehow bypass the analysis of these programs while keeping security intact.

Information leaks are used in application exploits to leak Central Processing Unit (CPU) memory addresses to ensure exploitation has a high rate of success over mass amounts of computers. Newer technologies regarding mitigations of exploits forced the security industry to spend thousands of months of accumulated time to bypass these mechanisms. Information leaks are rarely discussed outside of software exploitation. Social engineering is a similar mechanism but by exploiting humans working for corporations, or government. Blind SQL injection is a mechanism to use calculable differences in timers on a system to determine if the application encountered an vulnerability while your attempting to manipulate its database operations.

Injecting information into government databases through these surveillance taps allows a whole new area of security. This area brings all of the same problems from software exploitation into this new arena. The information leak crosses over into the social world. It is an example of how humans on a mass scale react just like software logic. Governments are especially vulnerable to these exploits crossing over since they uniform reactions regarding everything with training.

Database corruption, exhaustion, and other Denial Of Service (DoS) attacks are some of the problems I expressed in prior papers. Those were considered as a way to disrupt surveillance taps when necessary for numerous possible reasons. If you were to give the general public the knowledge of manipulating these databases then it is only a matter of time before people uncover all sorts of design flaws, and vulnerabilities within these systems. The intelligence applications which analyze these systems are no more secure than all other networks in the world. The applications are developed in the same languages as everything else in this world.

I am only imagining how the surveillance systems are designed, and function internally. It is not necessary to know the exact details since they are so widespread. Reverse engineering works just as well. I have worked on numerous projects involving scalability, and mass infrastructure techniques. I have considered other known designs, and realize that there is no safe way to

implement these systems which allow a totally secure surveillance system which uses information from hacks such as tapping Internet backbones.

The United States government have been discussing being hacked by various countries more lately than ever. If major parts of the United States government is being hacked on a regular basis then why would anyone believe that these surveillance programs are any more secure? Every surveillance tap is processing data which may trigger vulnerabilities within their systems. In the past some special rooms at telecoms were reported because they had private data links to government data centers. This is technically the most secure way for them to transmit information. It does not however mitigate these types of attacks because it relates to processing of the captured data from the Internet backbones.

Automation is usually the key to success and scalability. It is however the fundamental flaw with these surveillance programs because it is necessary to operate, and also creates their biggest vulnerability. The vulnerabilities exist because those programs must continuously verify, and process information regarding events found on these backbones. It cannot accurately prioritize the data otherwise, and this would leave infinite amounts of queues for people to process.

Social engineer is based on human vulnerabilities generally related to an attackers confidence and presentation. Facial reactions is also a way of gaining information disclosure against a target. The cues are similar for attempting to replicate these attacks on mass applications such as surveillance software. Marketing is an industry which relies heavily on human reactions, and uses target specific information disclosures to increase probability of a wanted reaction. Mass surveillance programs are a mixture of software, and social engineering vulnerabilities. It contains a finite amount of responses for a short amount of data type categories. Data is either relevant, not relevant, or unknown. The saved datasets are processed to determine whether to ignore, investigate, or process further. It may have a few other situations such as scoring, or linking to other entries. The system is pretty basic in reality. The difficult part is obtaining access to the data which is being gathered from the Internet backbones. It requires access, and specialized hardware but the specifics are not necessary for attacking them.

The other difficult portion of the surveillance programs are data storage, and processing of vast amounts of data being collected every second. It becomes relatively simple databases after processing is completed. XKeyscore outlines supposed Google like simplicity for accessing processed intelligence information. It creates a relational dataset which analysts may access using Google like search keyword modifiers. All of that complexity happens after the part of the system that is important for these specific information leaks. The XKeyscore search engine may contain further vulnerabilities as well. Its job includes presenting information from worldwide sources to computers used by government employees. Filtering algorithms exist for social media platforms to remove Hypertext Markup Language (HTML), and the Javascript language. These algorithms have their own vulnerabilities, and are an entire subset of web security. I wouldn't doubt that more vulnerabilities are possible on this side of the surveillance frameworks.

Injecting custom data into these databases is key for any of the attacks. You have to replay previously generated Transmission Control Protocol/Internet Protocol (TCP/IP) connections on both sides of the tap. The text, or events need to be crafted in specific ways to cause responses from the processing of the information after the taps have siphoned it. A secondary subset of calculated text needs to exist to force human analysts to react with the information.

Both are necessary to have as many sensors of responses as possible. Telecommunication metadata can even be manipulated by spoofing telephone calls using Voice Over IP (VoIP) Automatic Number Identification (ANI) manipulation. You can sit and pick ways to exploit many different sources of these intelligence capturing technologies. Complete distrust in these systems is an inevitable conclusion which will happen shortly. It is impossible to cause so much false information with human assets. Enough people are not employable to create as many events as possible digitally manipulating these taps.

The entire method of manipulation is the exact reason why these systems will need to be shutdown as soon as possible. All of the attacks relate to pairing custom information which are triggers that you wish to activate with information relating to high profile priorities for intelligence agencies. It means that you should use modules, or entries which relate directly to activate terrorists, or attacks. Terrorism is a widely known reason that intelligence analysts will trigger responses in a way that is identifiable externally by your software, or human assets. It also proves that these systems at their current implementations may be riddled with false information. In time you can analyze responses and justify using other keywords outside of terrorism. It is going to be required to gage ranges of responses for more complex analyses.

Marketing is a huge help in these areas. Examples would be custom web Uniform Resource Identifiers (URL) which are logging possible web connections by surveillance systems. Referrers themselves are informative in these cases because analysts may, or may not go through effort of spoofing a third party site before accessing URLs included in the false information campaigns. Asterisk, and VoIP are another set of tools which should be used to create custom phone numbers for each campaign. If you were to prepare with thousands of worldwide numbers then you can begin to create statistical information in these areas about random marketing calls. Anything after you launch campaigns can be deemed a response by these systems if they are included in messages. Domain Name System (DNS) servers will have information resolved if domains are used in messages depending on how the preprocessing of the initial data happens on these systems. Web servers may begin seeing traffic, and banners from other services on these systems may begin being initiated from IP addresses under control by systems, or analysts of them. Internet Corporation for Assigned Names and Numbers (ICANN) Whois servers for domains if you control the registrars would allowing recognizing whenever these surveillance systems query those databases. The more control you have over all of these footprints the better. It ensures that you are able to capture all responses from these systems.

Human analysts will follow through with the most critical information campaigns. If you relate your keywords with current terrorists activities than you may ensure intelligence agencies respond by delegating police forces for surveillance, or other actions. The actions may come as investigators, or even by police raids. It might closely resemble the old emergency (911) ANI spoofing which caused police raids on peoples targets homes. It is unfortunate, but these systems allow many more of these types of attacks on a variation of levels. I am not condoning using manipulation to this degree. I am however expressing how much of a vulnerability these systems are to the general public in whole. It is necessary to understand the possibilities.

Many hacked databases of citizens have leaked from websites which include names, e-mail addresses, passwords, and sometimes mailing addresses. Any of these names may be used for these tasks especially in areas where you can setup surveillance easily. Another possibility is to obtain access to cameras near the identities to gage whether or not government takes

action against the campaigns. Neural networks could be used to automate this process even further. It is a completely cyber way to determine responses by intelligence agencies, and could be used on a mass scale to automate all of these types of attacks. Information placing campaigns do not solely have to relate to individuals. Government responses can be conjured against corporations, countries, or other types of entities. It will prove why these systems are a really bad source of intelligence overall.

Stocks themselves are just an example of abusing these information leaks. It would require calculation, and understanding of the thresholds of each agency, and the category of information. All current news are good beginnings to determine possible keywords to use in these campaigns. Once you know each taps responses then you can begin to attempt pairing various types of keywords together for complex analysis. If you notice a major case, or rumors of stock market manipulation then you may wish to plant information relating to those companies, or individuals to recognize whether or not response will incur.

Once you begin to understand internals, and levels of responses then you can start to automate pairing them even further. If you pair two high priority keywords then it should ensure the responses are not only quicker, but it may be of higher caliber. It will require all of the prior information before recognizing this. It might take pairing several different keyword types together to recognize the different patterns. Timing of responses will be extremely important as well. If you include certain companies within this then it may start to tell you whether prior information has been processed between two companies. It literally will begin allowing you to use these systems to determine if a lot of information has been processed regarding two companies. It might not seem like a huge deal at first but if you can recognize if two people even know each other through the different responses, reactions, or timing of these systems then that alone is a huge information leak.

It can begin to develop into more advanced scenarios with your inquiries. It isn't a regular programming language such as requesting some data, and obtaining it immediately. It will require development and careful planning. Your injections themselves will begin to modify results if not carefully planned. The reaction time if using similar keywords with different associates may give information on whether or not particular people are under surveillance. Active surveillance would definitely happen quicker to important keywords than priorities processing slower.

I am not releasing this to entice manipulation of the system for financial gain. I am merely pointing out how much of a vulnerability it is. It literally allows leaking of incalculable amounts of information regarding almost any topic that passes through these surveillance taps. It is an issue we have been living with for a decade now. I cannot believe that there isn't someone else in the world manipulating them already.

If you are one to believe that the government agencies can mitigate these attacks you should reconsider. Fake news is an example. If these massive worldwide corporations cannot block fake news from being distributed across their websites and affecting everything from high frequency trading to national news then how can intelligence agencies? It is ridiculous to believe that governments have more "top secret" technology than the biggest private corporations of the world. The more that they apply ways of cross examining the data being injected is going to increase the amount of responses, or sensors detecting their processing of

the information. It is an actual directly correlated Catch-22 which proves just another reason why these surveillance programs are more of a burden than they are actual intelligence.

I believe the only fix to these vulnerabilities is for financial institutions to lobby against government intelligence agencies. Financial markets are at risk until these programs are completely disabled. Web intelligence gathering must be destroyed at all costs. The Federal Communications Commission (FCC) repeal on laws against selling web history is another similar problem. It will be a crucial factor in a lot of future stock trades, and this is just as bad. The only difference is that these leaks are going to come from private information which is e-mailed, or directly recorded from phone calls. All phone calls content which gets inserted into these intelligence agency data centers are going to continuously adjust responses.

These vulnerabilities can also be used to leak information on subjects being monitored which may have usefulness in court cases. If explained correctly it may help present facts to a jury about evidence origins. The amount of investigations happening at any point in time by police forces, or agencies is also another easy to determine fact using these methods. The entire framework is terrible at keeping any facts related to the data from being siphoned secretly from their surveillance programs.

I do not have a better solution at the moment for fighting terrorism, or categorizing humans possibly planning attacks. Its possible that removing e-mails, and phone calls could help mitigate most of these exploits. It would place more emphasis on other types of events such as wire transfers, credit card purchases, etc. It is possible that these events are so invasive that they may already be used in ways to fake, or direct intelligence communities towards decoys. It doesn't matter whether I release this document or not. It will be discovered by someone. It is a matter of time. Any true artificial intelligence when developed would easily understand logic around these systems. Online services, and social networking companies should work directly with intelligence agencies to process information. It would bypass the necessity of a surveillance tap, and would be a much more secure approach.

I'd hope United Nations members can come together to work out a generally acceptable approach for the future of law enforcement. Cyber crimes have far surpassed all other types worldwide. Engagement of these issues should take place head on rather than function behind the scenes with hacks such as surveillance taps. The entire world is vulnerable until better ways to battle cyber crimes are discovered. The world, and America literally doesn't need groups like the National Security Agency (NSA) to use offensive hacking to perform their jobs. It should be built into frameworks from the beginning. Being a super power, or a country with advanced capabilities does not mean that you are doing things correctly. Groups with resources should design secure ways of executing these tasks. Technology companies may be more inclined to accept protocols that have been developed in this manner. The current surveillance state is creating more vulnerabilities than the amount of actual intelligence being captured.