Michael Guidry
April 4, 2017
Fourth party attacks on third party TCP/IP “oracles”

Fourth party is a new ideology that there’s always the possibility of another layer of involvement with Transmission Control Protocol/Internet Protocol (TCP/IP) manipulation attacks. Other methods exist beyond hijacking a single occurrence of a web page which are not currently known. It may relate to long lasting data intelligence gathering manipulation. Web session hijacking which led to ability for National Security Agency’s (NSA) offensive Fox Acid (FA) programs have vulnerabilities of their own. It uses third party mass surveillance taps to modify web pages in transit for ability to infect targets computers through their web browsers. FA has a counterpart program called Quantum Insert (QI) which forces their targets to reach its servers. It includes taking advantage of undisclosed vulnerabilities (0-day) by using their exploits in cases where the end user is expected to be completely patched by assumption, or javascript verification.

Third party surveillance taps are a double edge sword. It is a great position at first glance, although could very well be a negative one. It happens at such a high level on Internet Service Provider (ISP) routers that it cannot accurately process every state within the TCP/IP protocol. It essentially means that the security is much less than that of a normal operating system which is performing the TCP/IP connection itself. It uses a high level overview to have ability to single out targets over hundreds of millions of connections. It is a double edged sword, and could lead to many new problems which have never been discussed publicly.

I’ve read online of people claiming, or insinuating the NSA are “hacking gods.” I’ll let you know that this is simple not true. Huge budgets, government contractors, and national security leeway allows them to perform the various offensive applications that have been leaked in the recent years to media. The NSA themselves purchase most of their hacking tools worldwide from tens of thousands of people. NSA led programs are themselves vulnerable to the same issues that the applications they exploit contain. It is quite a funny scenario to realize that the same system that they are exploiting will always be a vulnerability within their own programs. The same exploit used to modify web page contents can be used to plant information directed at the NSA aggregation servers for signal intelligence.

FA infection servers are a part of their targeted offensive hacking platform’s infrastructure. It is the first example of using third party surveillance taps in a fourth party manner. Routers give enough insider information regarding a connection to an application so that it can modify a web session in real time. The modification causes the web browser to interpret a web page from the FA server. Its server will use javascript, and other HyperText Markup Language (HTML) scenarios to verify application versions, and operating system information. The application versions matter to help determine the probability of whether or not certain bugs having been patched. The servers may decide to use 0-day exploits if the target is expected to have been completely patched for all publicly known bugs. This scenario is the most important.

NSA’s first stage infection malware is more than likely not too interesting compared to publicly released information on sophisticated malware used worldwide. The framework, and intelligence gathering as whole is why governments generally get most of their respect. Secondary malware may be installed later which allows highly capable plugins, or advanced

methods although it would be ridiculous to infect every target with them from the beginning. This concept is why I wouldn't solely focus on attempting this method for obtaining their advanced backdoors. If you wish to create an entire computer with complete profile of an NSA suspected target then you may possibly get access to the most advanced malware used for highly prioritized targets.

If you wanted to manipulate the NSA surveillance taps in hope of getting sent to these FA servers then you have to understand how they operate. Cyber surveillance taps sit on routers siphoning particular data from millions of connections simultaneously. It determines which connections are of relevance and processes these independently of regular routing mechanisms. How the taps determine whether your connections are of interest is beyond the scope of this document. It could be from web history, or prior intelligence from alternative databases. Once you are deemed a target then it will have the router direct the necessary information required to perform offensive TCP/IP hijacking via QI. This attack method will modify the web page being requested with an alternate data stream which will cause the browser to load secondary web page from the FA servers.

The surveillance taps are pretty much dumb nodes which rely on third party lists of these target IP addresses. I have no internal information regarding any of these programs. I am unsure how they update their internal list in real time although it is of no importance. I've traveled outside of USA, and have had a machine hit a blank webpage before. I am absolutely positive that this was a manipulation from a QI or similar framework. The whole point is that something I had browsed within that region of travel put me into a category that enforced manipulation of my web traffic. It will only happen once which is not shocking. It is important to keep it as hidden, and private and possible. I was unable to trigger the hijacking again while debugging my browser, or network packets.

If you were to find information such as Internet Protocol (IP) addresses, e-mail addresses, or other personal information on possible NSA targets then you have a chance to pretend to be them with intention of triggering this system. The vulnerability lies in where these taps physically exist on Internet backbones. The tap usually has several backbone routers between a web server, and a target on both sides of the TCP/IP connection. It is handling surveillance of millions of IP addresses. Each case may change briefly although generally you can easily find sides of the connection on both sides of the surveillance taps you may target. Spoofing TCP/IP packets is possible although hijacking other peoples connections like QI is not feasible due to the randomization of the Acknowledge, and Sequence numbers inside of the TCP/IP protocol. The surveillance taps are either physical hardware through legally forced national security directives, or by hacking routers. You could perform QI attacks if you were to obtain access to routers, or backbones in the same ways. However, if you are targeting these third party taps then you can play this new game of being a fourth party.

Fourth party manipulation methods for example can begin by choosing a social media site that you wish to have the NSA believe is being communicated with by the suspected target your assuming the identity of. You then need an IP address on the other side of the tap in the area of the target itself. If you replay each side of a TCP/IP connection's traffic logs on each side of the tap pretending to be the relevant sides then you have the ability to force this third party surveillance tap to believe that the connection is really taking place. In reality, the connection doesn't even have to exist. It could be completely false, and is just happening with intention of having the surveillance tap give that information for the NSA program to inject a FA redirection

into your fake session. You would need control over the IP address within the target's region so the geographical location is similar. You need to receive packets for an IP address within that region. You need to receive packets for an IP address within that region to notice whenever the QI injection occurs. You either need to sniff this information from a router which is difficult, or you can find some way to have an IP address there.

It might seem very difficult however you can take cloud providers as an example of how vulnerable these third party taps can be. Amazon AWS covers a large portion of web traffic these days. It hosts many social media companies as well as various blogging sites. It contains Content Delivery Networks (CDN) servers as well. It is a great starting point to have one side of the tap prepared. You can then find servers, residential IP addresses, or other means of executing code within the region of the person you wish to spoof. You could even dial up internet access within that country using long distance to obtain an IP address near the target region. The amount of ways to handle this is extensive, and I will not give information on tactics to get IP addresses of profiles you are wishing to assume.

Another possibility is that even if a social media site isn't directly on a cloud region you pick but you know of a tap, then you can falsify e-mails across the tap. The reasons would be to escalate your IP address on one side of the tap hoping that the NSA programs will then prioritize you as a target. It is entirely about how many connections these taps monitor which makes them vulnerable to countless issues. The other NSA program which leaked named XKeyscore entails various separate programs worldwide. Some programs include traffic which is beyond regular web traffic. It is up to you to create your own modules for manipulation of worldwide surveillance programs to attempt to become targeted online.

Lets call the web server side of the tap the intended server, and the NSA target or client side the intended client. If you are attempting to fake a session between a web server for some site within Amazon AWS IP ranges on a particular cloud region then you would purchase an AWS instance there. Your AWS would be the spoofed server, and the intended client should be some IP address within the region of the NSA target. You can consider this the spoofed client. It could be a dialup IP address, or some machine that you have code execution ability on.

Wireshark should be used while you connect to the intended server from the spoofed clients IP address. You can perform some tasks such as logging in, or other scenarios such as blogging posts. You save these packets with Wireshark to disk. You can modify the packets using various methods to falsify the profile, or other information to make it seem exactly like the intended clients computer. You should ensure their user agent, and other information is correctly correlated to the intended profile. Anything that the surveillance taps may verify would be necessary to be correct for this fourth party attack to function properly. It is amazing how much dynamic IP addresses leave for vulnerabilities in systems worldwide. The surveillance taps are more than likely going to assume the IP address is different due to Dynamic Host Configuration Protocol (DHCP) leases.

Once you have both sides of the intended server, and intended client's packets prepared you have to create a sort of replay timing mechanism between them. It needs to work sequentially, and structured perfectly like a real session on both sides o the tap. It should occur just like the Wireshark log files had dumped them, and in the correct order. I would personally create a system which can communicate on another channel to allow major file transfers within the same attack mechanisms. You would load these packets onto the spoofed server, and spoofed client.

The moment you begin replaying both sides of these packets then tap begins to analyze, and interpret it within its surveillance routines. It will be no different than any other connection going across the router. It will believe that these packets are a true connection happening between these servers. Your spoofed server does not even have to have the same IP address of the intended server. It can spoof that IP address using raw packets. It is within the same area of Internet backbone connections so the tap would see it as the intended server's IP address. You do not have to have access to the intended server to obtain any variables required for TCP hijacking. You are replaying a real session which has everything perfectly correct as if it was literally in real time being generated by their operating systems. It is a sort of blind TCP hijacking because to the tap it is so real that it will perform all the same duties. The actions should be performed as it would if the intended server was actually a part of the connection being injected.

The intended client's IP address had to be changed to your spoofed client's address so that you can actually recognize, and retrieve the QI modification of the web page when it occurs. It is an attack which requires you to have true access to at least one side of the connection. The tap is none the smarter because it is intended to handle millions of connections simultaneously at a different layer, and router. Most routers online do not contain anti spoof mechanism because they can break certain protocols which rely on things such as Domain Name System (DNS), Multicast, or Anycast. These User Datagram Protocol (UDP) based services would break if anti spoofing was enabled by default on every router. It is not something that will ever be fixed have a true fix. Fourth party manipulation of third party surveillance taps will exist until the day TCP/IP is relinquished for a more secure transmissions protocol for online communications.

Other attacks exist which do not require having either intended server, or intended client's IP addresses although they are also beyond the scope of this document. It is only intended to detect, and acquire NSA 0-day exploits worldwide using other information to determine which profiles to spoof.

I hope to have shed some light on the vulnerabilities that these mass surveillance programs introduce into worldwide privacy situations, national security programs, and the Internet as a whole. The methods will never be truly fixed for the foreseeable future. I highly doubt a surveillance platform will ever be installed on every computer worldwide legitimately. In other words, we will never have a secure surveillance platform. These platforms will always be third party, and never considered during engineering by designers. It is not intended to be used in these ways so any manipulation of protocols like this, or others will always end with the same results.

Happy hunting.