NSA Prism for E–Surveillance

Shubham Sharma[1], Sukhwinder Singh[2]
[1]Student, [2]Mentor
[12]Department of Electronics and Communication Engineering,
P.E.C. University of Technology, Chandigarh, India

Abstract: This paper examines the PRISM (Planning Tool For Resource Integration, Synchronization And Management), a top secret data mining "connect the dots" program by NSA aimed at terrorism detection and other pattern extraction authorized by federal judges working under the Foreign Intelligence Surveillance Act (FISA). The paper firstly looks into the purpose of the program, its origin & history and the positive and negative impacts of this initiative. An overview of the method of working of PRISM is provided. Also included is the impact of the same on the cloud computing firms especially the ones with U.S. background.

Keywords: PRISM; cloud firms; NSA; privacy; aggregate; surveillance.

I. INTRODUCTION

PRISM is unstructured big data aggregation framework — audio and video chats, phone call records, photographs, e-mails, documents, financial transactions and transfers, internet searches, Facebook Posts, smartphone logs and connection logs – and relevant analytics that enable analysts to extract patterns, save and analyze all of the digital breadcrumbs people don't even know they are creating. An interesting topic that comes out of this is "but who will watch the watchers". The Prism program collects stored Internet communications based on demands made to Internet companies such as Google Inc. and Apple Inc. under Section 702 of the FISA Amendments Act of 2008 to turn over any data that match court-approved search terms. The NSA can use these Prism requests to target communications that were encrypted when they traveled across the Internet backbone, to focus on stored data that telecommunication filtering systems discarded earlier, and to get data that is easier to handle, among other things
.

II. HISTORY

The origin of PRISM program can be traced back to the period when George Bush was the president of U.S. It began in 2007 with the passing of PROTECT AMERICA ACT. Its existence was leaked by NSA contractor Edward Snowden [8], who warned that the extent of mass data collection was far greater than the public knew and included what he characterized as "dangerous" and "criminal" activities. Documents published by various agencies and newspapers like THE GUARDIAN [6] and THE WASHINGTON POST indicate that PRISM is "the number one source of raw intelligence used for NSA analytic reports", and it accounts for 91% of the NSA's Internet traffic. The U.S. officials have defended the program by asserting that it cannot be used on domestic targets without a warrant and that it has helped in preventing terrorist threats many times.
According to The Register, the FISA Amendments Act of 2008 "specifically authorizes intelligence agencies to monitor the phone, email, and other communications of U.S. citizens for up to a week without obtaining a warrant" when one of the parties is outside the U.S. PRISM was publicly revealed when classified documents about the program were leaked to journalists of the The Washington Post and The Guardian [6] by Edward Snowden [8] – at the time an NSA contractor – during a visit to Hong Kong. The leaked documents included 41 PowerPoint slides, four of which were published in news articles. The documents identified several technology companies as participants in the PRISM program, including Microsoft in 2007, Yahoo! in 2008, Google in 2009, Facebook in 2009, Paltalk in 2009, YouTube in 2010, AOL in 2011, Skype in 2011 and Apple in 2012. The speaker's notes in the briefing document reviewed by The Washington Post indicated that "98 percent of PRISM production is based on Yahoo, Google and Microsoft".[3]During a House Judiciary hearing on domestic spying on July 17, 2013 John C Inglis, the deputy director of the surveillance agency, told a member of the House judiciary committee that NSA analysts can perform "a second or third hop query" through its collections of telephone data and internet records in order to find connections to terrorist organizations. "Hops" refers to a technical term indicating connections between people. A three-hop query means that the NSA can look at data not only from a suspected terrorist, but from everyone that suspect communicated with, and then from everyone those people communicated with, and then from everyone all of those people communicated with.

III. PRISM – WORKING

The program is called PRISM, after the prisms used to split light, which is used to carry information on fiber-optic cables. This is sort of a massive aggregate of aggregates. Each vendor Facebook, Google, LinkedIn etc.[6] collects an incredible amount of data across their portfolio of properties and applications. What the NSA has done is take this to the next level by creating a massive mashup of all the sources to look for end-to-end patterns and relationships. The challenge that NSA is tackling is look-forward real-time intelligence. Can you predict in almost real-time a potential threat … intercepting a mobile phone call while someone is on the move towards a target and being able to create a rapid response to avert the threat. PRISM puts all the information collected from various data collection agencies together, combs through all aggregated data and analysis the same for potential threats to the security of citizens. The program is using two types of data collection methods: Upstream from the switches themselves (raw feeds) and downstream from the various providers (contextual feeds). The data is extracted, transferred and loaded into servers at the Utah Data Center in Bluffdale. There is enough capacity to store a Yottabyte of data… large enough to store all the electronic communications of all of humanity for the next 100 years. The question arises that what is the need to store such a huge amount of data. Ira Hunt of Central Intelligence Agency, said in a speech at GigaOM Structure:Data conference that “The value of any piece of information is only known when you connect it with something else that arrives at a future point of time.” Here is a use case of how PRISM can be used to unearth patterns. This is taken from the article “NSA –The Mother of All Big Data Projects “by Ravi Kalakota also referenced below [4]. “In October, a foreign national named Joe Jackal does a Google Search and purchased a one-way plane ticket from Cairo to Miami, where he rented a condo. Over the previous few weeks, he’d made a number of large withdrawals from ATM machine linked to a Russian bank account and placed repeated calls to a few people in Syria. More recently, he rented a truck, drove to Orlando, and visited Walt Disney World by himself. As numerous security videos indicate, he spent his day taking pictures of crowded plazas and gate areas.

None of Jackal’s individual actions would raise suspicions. Lots of people rent trucks or have relations in Syria, and no doubt there are harmless eccentrics out in amusement parks taking pictures. Taken together, though, they suggested that Jackal was up to something. And yet, his pre-attack prep signature would have gone unnoticed. A CIA analyst might have flagged the plane ticket purchase; an FBI agent might have seen the bank transfers. But there was nothing to connect the two. The day Jackal drives to Orlando, he gets a speeding ticket, which triggers an alert in the PRISM system. An analyst types Jackal’s name into a search box and up pops a wealth of information pulled from every database at the government’s disposal. There’s fingerprint and DNA evidence for Jackal gathered by a CIA operative in Cairo; video of him going to an ATM in Miami; shots of his rental truck’s license plate at a tollbooth; phone records; and a map pinpointing his movements across the globe.As the CIA analyst starts poking around on Jackal’s file, a picture emerges. A mouse click shows that Jackal has wired money to the people he had been calling in Syria. Another click brings up CIA field reports on the Syrians and reveals they have been under investigation for suspicious behavior and meeting together every day over the past two weeks. Click: The Syrians bought plane tickets to Miami one day after receiving the money from Jackal. The software brings up a map that has a pulsing red light tracing the flow of money from Cairo and Syria to Jackal’s Miami condo. That provides local cops with the last piece of information they need to move in on their prey before he strikes.”

IV. IMPACT OF PRISM ON U.S. CLOUD FIRMS

Now since PRISM is no longer a secret , people have come to know that the National Security Agency (NSA) and other U.S. law enforcement and national security agencies have used provisions in the Foreign Intelligence Surveillance Act (FISA) to obtain electronic data from third-parties. This surely will have an immediate and long lasting impact on the U.S. based cloud computing firms if foreign customers realize the risks of storing data with a U.S. company will be passed on. The United States has been the leader in providing cloud computing services not just domestically, but also abroad where it dominates every segment of the market [2]. But other countries are trying to play catch-up to the United States’ early success [5]. Of the $13.5 billion in investments that cloud computing service providers made in 2011, $5.6 billion came from companies outside North America. So a significant amount of revenue is at stake. U.S. cloud computing providers might lose $35.0 billion by 2016. This assumes the U.S. eventually loses 20 percent of the foreign market to competitors and retains its current domestic market share. In June and July of 2013, the Cloud Security Alliance surveyed its members, who are industry practitioners, companies, and other cloud computing stakeholders, about their reactions to the NSA leaks. For non-U.S. residents, 10 percent of respondents indicated that they had cancelled a project with a U.S.-based cloud computing provider; 56 percent said that they would be less likely to use a U.S.-based cloud computing service. For U.S. residents, slightly more than a third (36 percent) indicated that the NSA leaks made it more difficult for them to do business outside of the United States.so it is quite evident that the U.S. cloud service providers stand to lose between 10 and 20 percent of their foreign market in next few years.

V. COMMERCIAL IMPACT OF PRISM

This includes predictive search industry which is growing at a fast rate. A range of start-ups - Cue, reQall, Donna, Tempo AI, MindMeld and Evernote - and big companies like Apple, Google are working on what is known as predictive search or augmented reality — new tools that act as personal valets, anticipating what you need before you ask for it. Google, for instance, is continuously changing the landscape of search with predictive analytics. Google launched the practice of predictive search back in 2004 with Google Suggest.In 2010, Google Instant came on the scene, generating search results instantly as users type. Google’s Knowledge Graph in 2013 further enhances predictive search by predicting what type of information a user is searching for when they search a celebrity name “Brad Pitt” and generates specific related content right alongside normal search results. Google is in a unique position to know what information people are most interested in seeing and when they want it based on the giant volume of Web searches processed by the search engine daily. The different cloud services that it enables creates a web of rich data that is unsurpassed by few other firms. Google provided some clarification on how it transmits FISA information: by hand (tapes), or over secure FTP. Google claims that they don’t participate in any government program involving a lockbox or other equipment installed at its facilities to transfer data to the government. It is hard to believe that peta-bytes of content can be effectively transferred and ingested by tapes or Secure FTP. The role of FACEBOOK and APPLE also can’t be ignored at this level.

VI. OFFLINE SPYING

Some researchers state that the National Security Agency has implanted software in about 100,000 computers around the world, allowing the United States to surveil those machines while creating a trail that can be used to launch cyber-attacks. Though most of the software is installed by gaining access to computer networks, the NSA can also employ technology that enters computers and alters data without needing internet access. The secret technology uses covert radio waves transmitted from small circuit boards and USB cards clandestinely inserted into targeted computers, The New York Times reported. The waves can then be sent to a briefcase-sized relay station intelligence agencies can set up just miles away, according to NSA documents, computer experts and US officials.

The radio frequency technology - which often needs to be physically inserted by a spy, manufacturer or unwitting user - has helped US spies access computers that global adversaries have gone to great lengths to protect from surveillance or cyber-attack. The NSA calls use of the infiltration software and radio technology - all part of a program known as Quantum - “active defense” against cyber-attacks, though it has condemned use of similar software by Chinese attackers against American companies or government agencies.“What’s new here is the scale and the sophistication of the intelligence agency’s ability to get into computers and networks to which no one has ever had access before,” James Andrew Lewis, cyber security expert at the Center for Strategic and International Studies in Washington, told The Times. “Some of these capabilities have been around for a while, but the combination of learning how to penetrate systems to insert software and learning how to do that using radio frequencies has given the U.S. a new window.”[7]

VII. CONCLUSION

So the question arises that are the governments justified in interfering with the privacy of citizens and come up with such mass data aggregation programs like PRISM? On one side is the threat to the privacy of citizens and on the other side is potential threat to the nation’s security. Also we need to take into account the risk of cloud firms losing their credibility. The United States has both the most to gain and the most to lose. Many of the economic benefits of cloud computing, such as job growth and revenue, are dependent on the United States being able to export cloud computing services. If U.S. firms are to maintain their lead in the market, they must be able to compete in the global market. It is clear that if the U.S. government continues to impede U.S. cloud computing providers, other nations are more than willing to step in to grow their own industries at the expense of U.S. businesses. The biggest argument against such data aggregation is the breach of peoples’ privacy. Afterall no one should have the right to interfere in other persons’ life. But then again such data collection helps curb terrorism and avoid potential threats to the nation’s security. So we can say that programs like PRISM are a necessary burden on the citizens. These are quite important for the nation but a burden to the common man [9].

REFERENCES

[1]. “How Much Will PRISM Cost the U.S. Cloud Computing Industry? “BY DANIEL CASTRO, AUGUST 2013 ,ITIF(Information Technology & Innovation Foundation.

[2]. NSA PRISM – The Mother of all Big Data Projects by Ravi Kalakota.

[3]. For PRISM technology, refer: http://en.wikipedia.org/wiki/PRISM_(surveillance _program)

[4]. U.S. Cloud Firms Suffer From NSA PRISM Program, by Kenneth corbin, july 25, 2013.

[5]. Rahn, “Europe Won’t Les U.S. Dominate Cloud.”

[6]. "NSA Taps in to Internet Giants' Systems to Mine User Data, Secret Files Reveal – Top-Secret Prism Program Claims Direct Access to Servers of Firms Including Google, Apple and Facebook – Companies Deny Any Knowledge of Program in Operation Since 2007 – Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks". The Guardian. Retrieved June 15, 2013.

[7]. "PRISM: Here's How the NSA Wiretapped the Internet". ZDNet. June 15, 2013.

[8]. "NSA Whistleblower Edward Snowden: Washington Snoopers Are Criminals". International Business Times. Retrieved June 30, 2013.

[9]. NSA able to target offline computers using radio-waves for surveillance, cyber-attacks, published – January 15 2014.