Network Security Project Proposal

An Exhaustive Study of Threats and Vulnerabilities in Geo-Tagging

Gaurang Khanwalkar, Niranjan Agnihotri, Japjeet Singh, Ajit Rajurkar

Advisor: Amir Rahmati

State University of New York Stony Brook, NY

1 Problem

Humans are clicking pictures on a daily basis and some of them every hour or even every minute. Users upload these photos on various social media platforms using their smart phones, laptops and other devices. These pictures contain a variety of information with them such as format of image, size, resolution and most importantly geo-tags.

GeoTagging, is the process of adding geographical identification metadata to various media such as a geotagged photograph or video, websites, SMS messages, QR Codes[1] or RSS feeds and is a form of geospatial metadata.

These geo-tags are used by major social media platforms and several cloud storage apps for providing a better user experience and feature enhancements. But these geo-tags can also be used by attackers to carry out unethical activities. Most of the people are not even aware of the fact that the images they are uploading have geotag in them.

Geotags are widely used, but there is no consolidated knowledge about how it is used, by whom and it can cause harm. Through this study, we want to conduct an exhaustive study of public geo tagged images on various parameters like the source, possible threats and attacks using this data, different social media platform's policies regarding geotags, formats used for storing this data. To make the user aware about the geotag being uploaded on the internet, we would make an extension in Firefox/chrome which will alert the user about it and give an option to remove that metadata before uploading the media.

2 Context

There are various publicly available tools which can read the geo tag data and present it in a visually appealing way like pic2map, metrics and exifviewer. Also some tools

which can help the user to delete the geo metadata. But all such tools are helpful if user is willingly using such tools before sending out images. There is no intuitive way through which user will be informed about this only while uploading the image and given an option to opt out.

MapExif: an image scanning and mapping tool for investigators talks about how the exif metadata can be used in law and enforcement to prove the evidences in the court. GeoTag-X research discusses how geographical metadata can be used to assist disaster relief efforts. 'Statistic Analysis of Millions of Digital Photos' a study conducted by Image Engineering Dietmar Wueller, digs deep into the exif data. But it was published before 2009, when use of geo tags was not prevalent and thus not analyzed in this paper. Our study will do similar analysis but will be more focused on location metadata. Also we will discuss in details about the possible attacks originating from such data.

3 Approach

A lot of research work has been done on extraction of geo-tag data from tweets, unstructured data and various other means. A very little work is available on the attacks carried out using geo-tag information. We will study the EXIF format, the standards followed by it, the tags present and security problems associated with it. There are various image sharing services like instagram, flickr, pint rest, facebook, which has different policies related to the geo metadata. We will study about all the platforms and analyze what happens to image the metadata after uploading and downloading the image.

According to an NYTimes article - Adam Savage host of the popular program "MythBusters", had his home robbed after he uploaded his photo online which allowed the thieves to extract the location of his house. In this study we will discuss about such similar attacks which are possible due to availability of geotag data and also any past attacks.

There are some social media platforms which don't strip off the geotagging from the image after upload, but it is unclear if that data is stored with them. They might be keeping this info and using it to profile the users. If the data collecting platform gets compromised, then this whole information can be available to an adversary. (consider Cambridge Analytica Scandal). Users may be also unaware that they would need separate tools to strip the Geo tags.

4 Evaluation

This being the analytical study, the evaluation measurement would the insights which we will gather from it. We will collect large datasets from images from various websites

and analyze them. Also the data gathered will be evaluated to see what type of attacks and harm can be conducted using this data and its impact.

We will develop one browser plugin which will make the user aware about the image's metadata and geotagging. The plugin - 'GStrip' will be either developed for Chrome or Firefox. Whenever user tries to upload any image on any type of social media using the explorer/finder on the operating system, GStrip will popup and check the image for geo tagging information. If there is no such metadata attached with the file then it will be uploaded otherwise one pop up will appear which will show the location data to the user. User will be given a choice to either keep the metadata intact or remove it. If user chooses the later option then all the geotag information will be stripped off and then the file will be uploaded on its intended website.

5 Scope

For the literature review deadline, we plan to finish all the background study of existing and related works done on this topic. We will do the extensive analysis of large amount of images and present our insights and finding in the progress report, which will also have the current status of the project, any obstacles which we might encounter and the workaround for that.

By the end of semester, we will have a comprehensive study on the threats and vulnerabilities involved with geo-tags in "EXIF" backed by data generated through our experiments and potential misuse of geo-tag data by attackers. We will also create a plugin 'GStrip' which can alert the user about the data stored in images before sharing the them on social media platforms and websites.