Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 113 (2017) 267–272

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017)

Hidden Privacy Risks in Sharing Pictures on Social Media

Kambiz Ghazinour *, John Ponchak

Advanced Information Security and Privacy Lab, Department of Computer Science, Kent State University, Kent, Ohio, USA

Abstract

Shared pictures, videos and more constitute as shared media in today's world of social networks. Each piece of media shared has hidden privacy violations stored in their metadata. Over the past two decades, social media sites, and shared media on them, have grown exponentially. People are sharing more data, and with more people, such unknowing users easily become the victims of numerous types of privacy attacks. By creating a GUI based metadata reader and editor, much of this security risk can be alleviated for common users. By bringing the capability to view and change metadata to different platforms, the true risk, hidden in all shared media, can be brought outright and mitigated. Much of the important data that can be exposed deals with geotags for locations, as well as camera identification numbers, and time stamps. In this work, we discuss the importance of having control of this type of information and share a model application that can be used to help resolve privacy breaches of this type.

Keywords: Social Media; Privacy; Geotag; Pictures.

1. Introduction

Social media has quickly become an essential foundation for communication across multiple generations. Social media allows its users to share information about their lives knowingly and unknowingly [13]. Knowingly in when they sign up, they can input their information such as birthday, city, and other information and then choose their profile's privacy setting. While this has the potential to be the base for many severe privacy attacks, much more information is shared unknowingly. Given the number of photos and videos being shared on social media, it is clear that the

* Corresponding author. Tel.: +-330-672-9061.
E-mail address: kghazino@kent.edu

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.08.367

average person is more at risk to threats like identity theft, cyber stalking, and more. When users share pictures and videos of themselves and friends, usually taken with a smart phone, it also uploads the metadata for that picture. Metadata, to put it simply, is data about data. In this case, data about pictures and videos, shared to social media. Metadata includes such information as seemingly nominal as the camera's shutter speed, F-Stop, color spectrum, lens model, lens maker, camera model, and camera maker. It also includes more important information which can be used to track down a specific individual. This information includes, the cameras identifier number, the GPS Coordinates of where the photograph or video was taken and more. All this information is unknowingly entered into the metadata when the picture or video is created. This creates an issue for users who share media without knowledge of this occurring. The exploitation of a single shared photo can result in an adversary knowing the location the user posted from and more.

1.1. Contribution of this work

Through this work, we not only shed light on a topic that has become increasingly important over the past few years, but also offer a solution in the form of an extensible application, centered around key features, all of which will be discusses, such as portability between operating systems. This topic is the inadvertent sharing of privacy violating information in metadata. The resultant of such sharing through metadata has potential to be detrimental, and in certain cases incriminating. Deriving the need for such an application will be shown in Section 2. The application contribution will be discussed in Section 3 of this paper. In Section 4, we will discuss the application interface and demonstrate the functionality of the application. In the last section, Section 5, we conclude the paper and discuss the future work for this research.

2. Background and Related Work

Data privacy has increasing becoming an issue that researchers try to build models and methods to protect. In [8] Barker *et al.* introduce a data privacy taxonomy to introduce a guideline to assess privacy-awareness of different models. In [9, 10] the researchers propose a recommender system that helps the users to pick a better privacy setting in their social network. In [11, 12] the researchers facilitate understanding of ambiguous and long privacy policies to the users in an easy-to-understand format. There are even attempts to introduce access control models to dynamically reflect security policies [14].

As previously mentioned, metadata is a form of data that is included on all videos and pictures and is used to store information about that data, such as date photo was taken, photographic information and GPS coordinates. This information is often used by operating systems to save information such as the last date a document was edited. This information is occasionally very helpful to person sharing the photos. In a court case[1] in 2012, a freelance photographer was cleared of charges of interfering with the arrest of another citizen by "aggressively" blinding the police officer with flash from his camera. The free-lance photographer was cleared of this charge by viewing the metadata which show that his flash did not fire at all during the time he was taking pictures. The police officer was later charged with fabricating an arrest record[1].

Having exposed metadata in shared media is a threat to innocent citizens who would like to keep information like their home address, favorite locations, place of work, and more, private. Researchers have conducted polls to gather information about frequent posting locations and found that over 40% of all posts on social media are done at the user's home and 80% were taken at their 10 most visited places [2]. Using this information, a team of researchers could conduct a study of 30 participants who used various social media websites. For three weeks, their posts were monitored to see if, at the end, the researchers would be able to identify the participant's homes, and their 5 most visited locations. Three weeks later, the study concluded that it could deduce 85% of the participants' homes as well as their top five most visited locations. The study chose to keep the identities of the participants private, but strived to find very average social media users who posted frequently and fit into the role of a security pragmatist. This could be done using reading metadata of the shared media, and geospatial tags from posts, including check-ins on Twitter [15], Facebook, and Instagram [3]. This study addresses geospatial information found in posts themselves. When a user posts to social media, the website will capture your GPS coordinates and appends them to the post. Using the API an adversary, in this case researchers, could retrieve the exact coordinates the picture was taken at, via the metadata, and anyone seeing the post could get the city the post was made from via the geospatial tag in the post itself. This is included above or below the post, depending on the social media website. It is important to realize that the average post on social media reaches over 1,000 people, and that number is only growing [6]. Even users that are privacy aware and have their profiles set to the most rigorous settings, are still susceptible to privacy attacks because their profile picture is visible to public. Hence, even the most concerned social media users are still at risk of having their privacy violated by complete strangers. In the past, there have been research regarding the concerns of metadata in shared media on social media [4] which focuses on secure JPEG files only. The paper proposed a platform and for an iOS app to be created. A prototype was created, but no official app was ever created to present its functionality. The prototype is not available for download either. Most social media posts are done from smartphones. So, while the target audience was valid, their proposed model only covered secure JPEG files, and also was only supported on iOS. Since it is rare for a user to post to social media from only a single device, and to only post jpeg files the proposed work could not be widely utilized.

Other related work includes a powerful tool called Exiftool [5] which is a command line tool that allows metadata (XMP or Exif format) to be edited and read. This tool is open source and is supported on most operating systems. Because of its power and versatility, this tool was chosen to be the base of the Windows, Linux, Android, and Mac implementations discussed below. Exiftool also makes a freeware GUI. This GUI is only supported on Windows, and has experienced issues on newer operating systems. Because of these reasons, the GUI has never caught on and is not nearly as widely used as the command line tool. The command line tool is used, most notably, by Flickr to pull information about uploaded pictures. With that in mind, it also has notable drawbacks such as proprietary language that can be confusing to an inexperienced user, as well as the complex interface. Being a command line utility, this immediately disqualifies most of the users who need an easy-to-use tool. There have been other apps in the past for iOS that have viewed GPS Coordinates of photos, such as Photolocator. Photolocator only shows GPS Coordinates and struggled to do that. Other metadata, which is equally as important, is completely ignored in Photolocator. GPS Coordinates, which are addressed by Photolocator, only allow the user to view the coordinates, not edit them, which in a sense allows the user to see how exposed they would be if they uploaded that picture, but does not give the user any ability to reduce the privacy risk found in the metadata [7].

In contrast to previous works, the platform we have developed is *user friendly*, which runs on *mobile* devices, does *not include confusing language*, *edits* all *types* of metadata and *hides* geospatial locations in social media posts.

3. Our Proposal

To address the above issues, we identified the following requirements as essential for an application: a) Portability, b) Ability to read metadata, c) Ability to change metadata, d) Protect posting location, e) Easy user interface, f) No proprietary terminology.

To address point *a*, the program must be able to run on Windows, Mac, Linux, Android and iOS operating systems. Because of the functional requirements different programming languages would have to be used for a program to run on all of the mentioned operating systems. By writing one version in C#, the application would run on Windows, Linux, Mac, and Android. To have the application run on iOS, it would have to be written in Objective C. While the program could be written in Swift, the libraries are still under development and subject to change. Because of this instability, and iOS's continued support of Objective C, it makes the most sense for the application to be developed in latter.

To address requirements *b* and *c*, being able to read and change metadata, we have identified Exiftool as a good base for all platforms. This command line utility has its shortcomings but allows for the easy reading and manipulation of metadata of both Exif and XMP types. It also runs on each of the most popular platforms, with the exception of iOS. To use this on iOS, a client server relation could be set up between the app and a Linux server, which would be used to feed requests. By using Exiftool as a base for the application metadata can be read and changed from every file type and nearly each value specified in each data item.

By using the Windows Form Application, a GUI was able to be created which helps to satisfy one of the issues that Exiftool has faced which is a difficult user interface. By custom designing this user interface we were able to make it user-friendly, fitting to the operating system it is running on, and eliminate proprietary language. By eliminating the proprietary language of Exiftool and replacing it with simpler terminology, the user interface becomes much more clear and easy to use. Thus, we have successfully satisfied requirements *e* and *f*.

The last requirement that needs to be satisfied is *d,* which is hiding the geospatial posting location found in the posts themselves. This information is gathered from the IP address used to post on social media. There are several ways to hide this information such as spoofing an IP address. We chose to do so with the use of a proxy. This functionally allows the user to pick the spoof city they would like to pretend where the picture was taken. The social media website will look up where the posting IP address is located at, not where the originating IP address is, which effectively hides the true posting location.

4. Implementation

The application is written in C# which allows for easy extensibility and portability between operating systems. It is designed in Visual Studio using the Windows Form Application. We make calls to Exiftool to make the changes to the file itself. In the application, we identified three main sections that would need to exist to be a functionally application. One section to view metadata, second, to change metadata and third, to choose a proxy.

Fig. 1 shows the user interface that runs on Windows and Linux operating systems. With simple changes, the same code also works on android and Mac. The application can work on iOS in a client-server relationship where the client, iOS device, requests a Linux server to read and write metadata from the uploaded media.

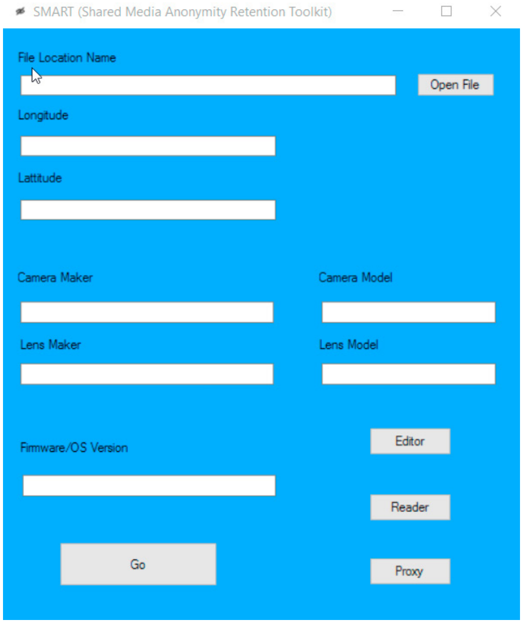
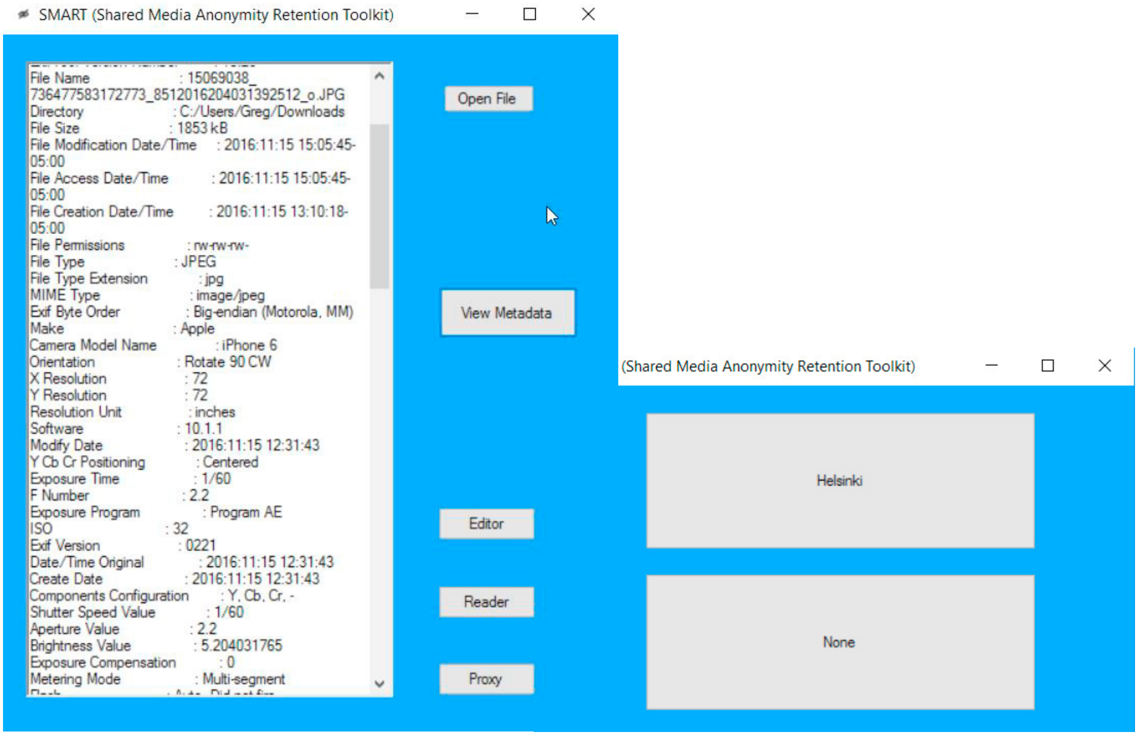


Fig. 1. The proposed UI

The application interface is simple and easy to manoeuvre. As shown in Fig. 1, the user first opens an image file and each text box is clearly labelled and accepts input. By filling out the values that the user wishes to change, they can click "Go" and it will change those metadata values of the file specified by the open file dialog.
On the lower right hand side of the application there are buttons that allow the user to navigate the aforementioned sections of the application. By clicking on reader, it brings the user to pane shown in Fig 2. The same open file dialog is seen here so the user has the option to select the file they would like to analyse.


SMART (Shared Media Anonymity Retention Toolkit)
Open File
View Metadata
Editor
Reader
Proxy
(Shared Media Anonymity Retention Toolkit)
Helsinki
None

```
File Name                  : 15069038_
736477583172773_851201620403139251_o.JPG
Directory                  : C:/Users/Greg/Downloads
File Size                  : 1853 kB
File Modification Date/Time    : 2016:11:15 15:05:45-
05:00
File Access Date/Time       : 2016:11:15 15:05:45-
05:00
File Creation Date/Time      : 2016:11:15 13:10:18-
05:00
File Permissions            : rw-rw-rw-
File Type                  : JPEG
File Type Extension          : jpg
MIME Type                  : image/jpeg
Exif Byte Order             : Big-endian (Motorola, MM)
Make                       : Apple
Camera Model Name            : iPhone 6
Orientation                 : Rotate 90 CW
X Resolution                : 72
Y Resolution                : 72
Resolution Unit             : inches
Software                    : 10.1.1
Modify Date                 : 2016:11:15 12:31:43
Y Cb Cr Positioning          : Centered
Exposure Time               : 1/60
F Number                   : 2.2
Exposure Program             : Program AE
ISO                        : 32
Exif Version                : 0221
Date/Time Original           : 2016:11:15 12:31:43
Create Date                 : 2016:11:15 12:31:43
Components Configuration       : Y, Cb, Cr, -
Shutter Speed Value           : 1/60
Aperture Value               : 2.2
Brightness Value             : 5.204031765
Exposure Compensation          : 0
Metering Mode                : Multi-segment
```

Fig. 2. Showing Metadata and Proxy Panel of the proposed software

The reader pane's function is to view the metadata of the file. Once a file is selected, clicking "View Metadata" will populate the text box with the metadata of the media selected. An example of the metadata is seen in Fig. 2. This is the resultant of a photo downloaded from Facebook. The picture was originally taken on an iPhone 6. The information can be viewed in the metadata, along with the modification date and creation date for the file. Further down in the file is where the GPS coordinates are shown. The last pane is the Proxy pane (shown in Fig. 2). It allows the user to select a proxy they would like to use to post. This allows the user to hide their posting location from being stored in the post itself. A proxy can be selected by simply clicking on a location. The "None" option clears the proxy information resulting in no proxy being used. The application is available for download on the Advanced Information Security and Privacy Lab at www.aisp.cs.kent.edu

5. Conclusion and Future Works

The growing usage of social media networks have opened a new world of privacy concerns. At the top of this list is the exploitation of metadata of uploaded media, such as photos and videos. To combat this growing issue, we have developed a model and an application to allow users to easily view their metadata, change their metadata, and hide their true posting location. The interface shown above is easy to navigate and fulfils all the identified requirements including voiding proprietary terminology, ability to change and view metadata for an image, portability, an easy to understand user interface and the ability to hide the posting location.

For future work, developers can use this model to create a similar platform for android devices and for iOS. The user interface is easy to use but could be developed more to be more appealing to users. Another area of improvement would be including a fourth pane for a secure file transfer utility. This would allow for an encrypted file transfer and for geospatial security. Such a secure file would only be able to be opened at a specified location. An example of this would be if the IRS is sending a tax return, it could be sent encrypted and use a custom metadata field to specify the opening location. An example of an opening location for this scenario would be the user's home. This would mean that the user would have to physically be at their house to open the file, making it more difficult for attackers to open tax returns, or any other secure files.

References

1. S. Kim. "Photographic Metadata Helps Convict Officer over Arrest of Journalist." *Photographic Metadata Helps Convict Officer over Arrest of Journalist | Reporters Committee for Freedom of the Press*. Web. 03 Dec. 2016.
2. T. Chen, A.R. Mohamen, and R. Boreli. "The Where and When of Finding New Friends: Analysis of a Location-based Social Discovery Network." *The Where and When of Finding New Friends: Analysis of a Location-based Social Discovery Network* (2013): 1-10. Web. 15 Oct. 2016.
3. S. Mascetti, L. Bertolaja and C. Bettini, "A Practical Location Privacy Attack in Proximity Services," *2013 IEEE 14th International Conference on Mobile Data Management*, Milan, 2013, pp. 87-96. doi: 10.1109/MDM.2013.19
4. L. Yuan, P. Korshunov and T. Ebrahimi, "Privacy-preserving photo sharing based on a secure JPEG," *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Hong Kong, 2015, pp. 185-190. doi: 10.1109/INFCOMW.2015.7179382
5. P. Harvey. "ExifToolGUI for Windows V5" *ExifToolGUI*. N.p., May 2012. Web. 16 Oct. 2016.
6. Haewoon Kwak, Changhyun Lee, Hosung Park, and Sue Moon. 2010. What is Twitter, a social network or a news media? In *Proceedings of the 19th international conference on World wide web* (WWW '10). ACM, New York, NY, USA, 591-600. DOI=http://dx.doi.org/10.1145/1772690.1772751
7. T. Mehrotra and B. M. Mehtre, "An automated forensic tool for image metadata and Windows 7 Recycle Bin," *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on*, Kanyakumari, 2014, pp. 419-425. doi: 10.1109/ICCICCT.2014.6992998
8. K. Barker, M. Askari, M. Banerjee, K. Ghazinour, B. Mackas, M. Majedi, S. Pun, and A. Williams. A data privacy taxonomy. In BNCOD 26: Proceedings of the 26th British National Conference on Databases, pages 42–54, Berlin, Heidelberg, July 2009. Springer Verlag.
9. K. Ghazinour, S. Matwin, and M. Sokolova, "YOURPRIVACYPROTECTOR, A recommender system for privacy settings in social networks," Int. J. Secur. Priv. Trust Manag, vol. 2, no. 4, 2016.
10. K. Ghazinour, S. Matwin, M. Sokolova: Monitoring and recommending privacy settings in social networks. EDBT/ICDT Workshops 2013: 164-168.
11. K. Ghazinour, M. Majedi and K. Barker, 'A Model for Privacy Policy Visualization', 2009. 33rd Annual IEEE International Computer Software and Applications Conference, 2009.
12. T. Albalawi, K. Ghazinour. (2016). A Usability Study on the Privacy Policy Visualization Model. In the proceedings of the 14th IEEE International Conference on Pervasive Intelligent and Computing (PICom 2016), New Zealand, 6 pages.
13. N. Memon and R. Alhajj. From sociology to computing in social networks: Theory, foundations and applications. Springer Vienna, Vienna, 2010. ISBN 9783709102930. doi: 10.1007/978-3-7091-0294-7.
14. K. Ghazinour, and M. Ghayoumi. Dynamic Modeling for Representing Access Control Policies Effect. In the Proceeding of the International Conference on Cyber Security (ICCS), 2015. California, USA.
15. K. Ghazinour, J. Ajayakumar. (2017). Spatial Privacy Concerns with Social Media Check-ins. In the Proceedings of the 4th International Symposium on Emerging Information, Communication and Networks (EICN), Lund, Sweden, September 2017. 6 pages.