International Journal of Computational Research and Development (IJCRD)
Impact Factor: 4.775, ISSN (Online): 2456 - 3137
(www.dvpublication.com) Volume 1, Issue 2, 2016

DEDUCTION ATTACK ON BROWSING HISTORY IN TWITTER USING PUBLIC CLICK ANALYTIC AND METADATA

K. Dharani*, M. Rajesh & Dr. T. Senthil Prakash*****

* PG Scholar, Department of Computer Science and Engineering, Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamilnadu

** Assistant Professor, Department of Computer Science and Engineering, Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamilnadu

*** Head, Department of Computer Science and Engineering, Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamilnadu

Cite This Article: K. Dharani, M. Rajesh & Dr. T. Senthil Prakash, "Deduction Attack on Browsing History in Twitter Using Public Click Analytic and Metadata", International Journal of Computational Research and Development, Volume 1, Issue 2, Page Number 107-110, 2016.

Abstract:

Our attacks rely on the combination of publicly available information: click analytics from URL shortening services and metadata from Twitter. The goal of the attacks is to know which URLs are clicked on by target users. We introduce two different attack methods: (i) an attack to know who click on the URLs updated by target users and (ii) an attack to know which URLs are clicked on by target users. To perform the first attack, we find a number of Twitter users who frequently distribute shortened URLs, and investigate the click analytics of the distributed shortened URLs and the metadata of the followers of the Twitter users. To perform the second attack, we create monitoring accounts that monitor messages. This work represents inference attack on browsing information in public click analytic in twitter metadata from all followings of target users to collect all shortened URLs that the target users may click on. We then monitor the click analytics of those shortened URLs and compare them with the metadata of the target user.

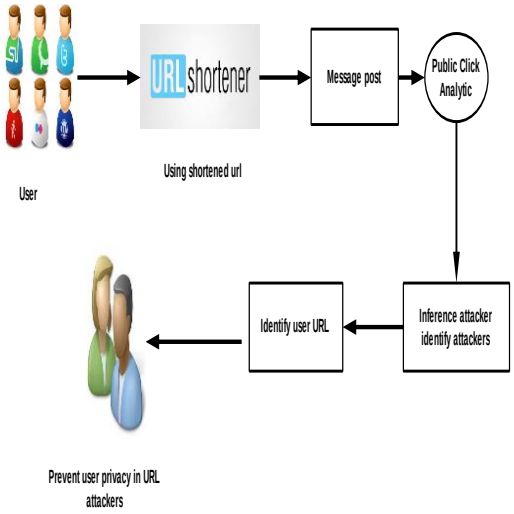
Key Words: URL Shortening Services, Twitter, Public Click Analytic & Metadata

Introduction:

Overall Description:

We proposed system attack methods for inferring whether a specific user clicked on certain shortened URLs on Twitter. Our attacks rely on the combination of publicly available information: click analytics from URL shortening services and metadata from Twitter. Two different attack methods: (i) an attack to know who click on the URLs updated by target users and (ii) an attack to know which URLs are clicked on by target users. To perform the first attack, we find a number of Twitter users who frequently distribute shortened URLs, and investigate the click analytics of the distributed shortened URLs and the metadata of the followers of the Twitter users. To perform the second attack, we create monitoring accounts that monitor messages from all followings of target users to collect all shortened URLs that the target users may click on. Then monitor the click analytics of those shortened URLs and compare them with the metadata of the target user.

System Architecture:



Problem Definition:

There are several types of history stealing attacks. First, attackers exploit cascading style sheet visited styles. They use the fact that browsers display visited links differently from unvisited links. They analyze behaviors of each browser related to CSS visited styles and build a system to detect browsing history of users efficiently. Second, attackers exploit browser and DNS cache to conduct history stealing attacks. Felton and Schneider describe attack methods using browser and DNS cache. Third, some researchers propose attack methods to steal browsing history using user interactions and side-channels. They also use a webcam to detect

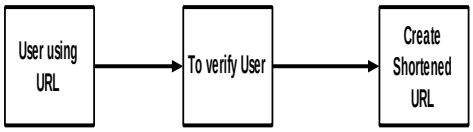
the light of the screen reflected at the user's face, which can be used to distinguish the colors of visited from those of unvisited links. The conventional history stealing attacks usually assume that victims visit a malicious web page or victims are infected by malware.

Module List:

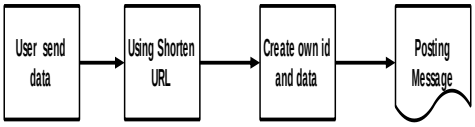
- ✓ URL Shortening Services.
- ✓ User Posting Message using shorter URL.
- ✓ Browsing history of public click analytic
- ✓ Inference attack to identify URL user
- ✓ To prevent the user privacy.

Module Description:

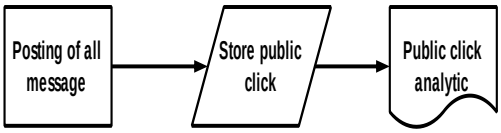
URL Shortening Services: The twitter user create own identification based on URL through web server. This web server verify to formation of shortened URL i.e., google-goo.com etc. Our attacks rely on the combination of publicly available information: click analytics from URL shortening services and metadata from Twitter. Two different attack methods



User Posting Message using shorter URL: User posting message through using shorten URL based on public click analytic. Some URL shortening services also provide click analytics about each shortened URL. Whenever a user clicks on a shortened URL, information about the user is recorded in the corresponding click analytics. The click analytics is usually made public and anyone can access it



Browsing History of Public Click Analytic: To perform the first attack, we find a number of Twitter users who frequently distribute shortened URLs, and investigate the click analytics of the distributed shortened URLs and the metadata of the followers of the Twitter users.



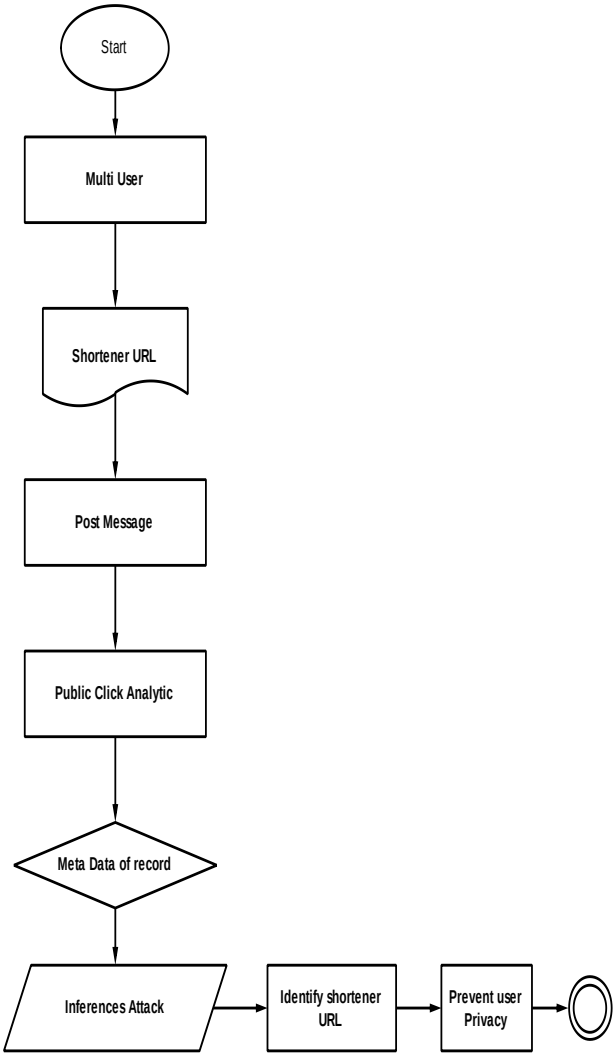
Proposed System:

- ✓ We proposed system attack methods for inferring whether a specific user clicked on certain shortened URLs on Twitter. Our attacks rely on the combination of publicly available information: click analytics from URL shortening services and metadata from Twitter.
- ✓ Two different attack methods: (i) an attack to know who click on the URLs updated by target users and (ii) an attack to know which URLs are clicked on by target users.
- ✓ To perform the first attack, we find a number of Twitter users who frequently distribute shortened URLs, and investigate the click analytics of the distributed shortened URLs and the metadata of the followers of the Twitter users.
- ✓ To perform the second attack, we create monitoring accounts that monitor messages from all followings of target users to collect all shortened URLs that the target users may click on. Then monitor the click analytics of those shortened URLs and compare them with the metadata of the target user.
- ✓ Some URL shortening services also provide click analytics about each shortened URL. Whenever a user clicks on a shortened URL, information about the user is recorded in the corresponding click analytics. The click analytics is usually made public and anyone can access it.
- ✓ The attack system chooses a target Twitter user and extracts his or her information from Twitter. The system monitors the click analytics of all shortened URLs posted by the followings of the target user.
- ✓ The system compares the information about the visitor with the known information the target user. If both pieces of information match, it infers that the target user clicks on the shortened URL.

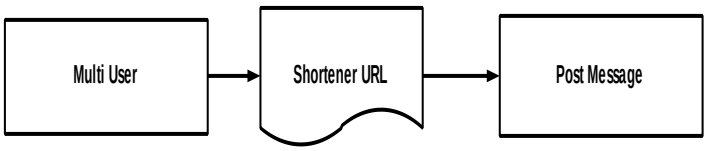
Advantages:

- ✓ Efficient for specific user click on curtained shortened URL.
- ✓ Easily to prevent user privacy accuracy. Information matching process is more accuracy.

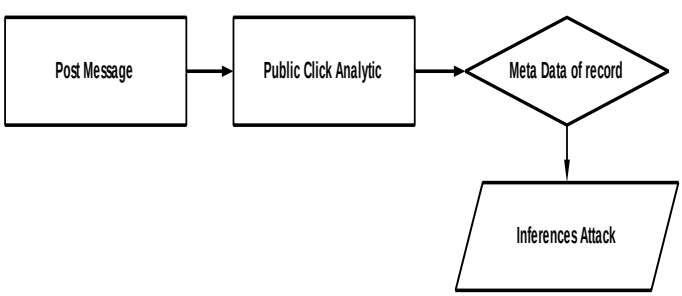
Dataflow Diagram:



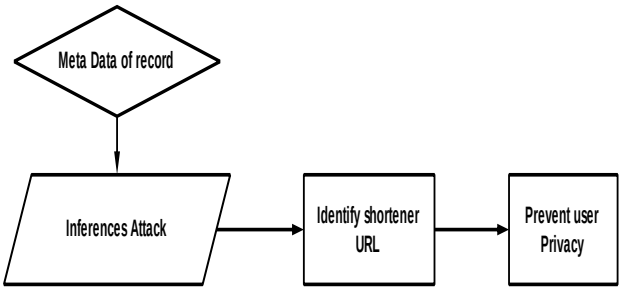
Level-0:



Level-1:



Level-2:



Implementation:

- ✓ We proposed system attack methods for inferring whether a specific user clicked on certain shortened URLs on Twitter. Our attacks rely on the combination of publicly available information: click analytics from URL shortening services and metadata from Twitter. Two different attack methods: (i) an attack to know who click on the URLs updated by target users and (ii) an attack to know which URLs are clicked on by target users.
- ✓ To perform the first attack, we find a number of Twitter users who frequently distribute shortened URLs, and investigate the click analytics of the distributed shortened URLs and the metadata of the followers of the Twitter users.
- ✓ To perform the second attack, we create monitoring accounts that monitor messages from all followings of target users to collect all shortened URLs that the target users may click on. Then monitor the click analytics of those shortened URLs and compare them with the metadata of the target user.
- ✓ Some URL shortening services also provide click analytics about each shortened URL. Whenever a user clicks on a shortened URL, information about the user is recorded in the corresponding click analytics. The click analytics is usually made public and anyone can access it.

Future Enhancement:

The future is to validate the correctness of our inference. To clarify, suppose that our system infers that a Twitter user A visits a shortened URL U. We collect the timeline and the favorites of the user A and check whether a tweet containing the shortened URL is exists. Twitter users include URLs in their tweets and favorite tweets with URLs only when they previously visit the URLs.

Conclusion:

Proposed inference attacks to infer which shortened URLs clicked on by a target user. All the information needed in our attacks is public information: the click analytics of URL shortening services and Twitter Meta data. To evaluate our attacks, we crawled and monitored the click analytics of URL shortening services and Twitter data. check whether a target user includes the URL inferred as visited in his (re)tweets or favorites it in the near.

References:

1. K. Dharani, M. Rajesh, Dr. T. Senthil Prakash and E. Anitha "Twitter user deduction attack on browsing record using public click analytic and metadata" Volume 8, July - December 2016 (e) 0976-9859 (p) 0976-985x
2. E. W. Felten and M. A. Schneider, "Timing attacks on web privacy," in Proc. 7th ACM Conf. Comput. Comm. Secur. (CCS), 2000, pp. 25–32.
3. M. Jakobsson and S. Stamm, "Invasive browser sniffing and countermeasures," in Proc. 15th Int. World Wide Web Conf., 2006, pp. 523–532.
4. S. Krishnan and F. Monrose, "Dns prefetching and its privacy implications: When good things go bad," in Proc. 3rd USENIX Workshop Large-scale Exploits Emergent Threats, 2010, pp. 10–10.
5. J. A. Calandrino, A. Kilzer, A. Narayanan, E. W. Felten, and V. Shmatikov, ""You might also like:" Privacy risks of collaborative filtering," in Proc. IEEE Symp. Secur. Privacy, 2011, pp. 231–246.
6. Z. Cheng, J. Caverlee, and K. Lee, "You are where you tweet: A content-based approach to geo-locating twitter users," in Proc. 19th ACM Int. Conf. Inform. Knowl. Manage, 2010, pp. 759–768.