Roman Shaikh

Student number: 18300989

CS7NS5-Security and Privacy

Assignment 1: Security and Privacy Considerations.

Contents

1. Topic Abstract

The dissertation is being done under the guidance of Professor Glenn Strong. The topic is exploring the possibilities of recommender systems in education on a Technology Enhanced Learning (TEL) platform *Scratch [1]*. *Scratch* was developed at MIT media labs to help young people develop their critical thinking and reasoning skills. Scratch is also aiming at people who are new to programming to get them started with their creative thinking. With Scratch, the user can build interactive stories program games and animations. The collaborative features of scratch enable the users to share their code and build on others work (similar to git). Scratch is also finding its way into formal education, where teachers are using it to introduce concepts of programming to inexperienced users.

Overtime as the user gets more and more involved in online learning, we see a decreasing pattern in the interaction with the Scratch platform. The research aims at studying the improvements in the users learning experience by building a recommender system based on the public datasets available.

Such recommender systems which are publicly accessible presents a security problem, which could vary from an attacker modifying recommendations to leaking the privacy-sensitive information of the users. And since most of the users on the scratch learning platform are form the age group of under 16 that is most of the users are kids, it is vital to prevent the privacy of children.

As a recommender system grows and learns more and more data needs to be collected which brings great privacy concerns to public users as the survey shows in [8].

In this paper, we discuss the security and privacy considerations in developing such systems.

2. Threats

The user's going to pick dancing pigs over security every time. – Bruce Schneier

2.1.Security

Any online system may be subjected to an attack. A recommender system is a kind of adaptive system that learns based on users' interactions with the system over time. For any information system, the ability of an unknown user to change the behavior could be considered an attack.

Attackers who cannot be quickly distinguished from general users can introduce biased information and data in an effort make the system forcefully adapt to their advantage.

Detecting this kind of attacks, therefore, becomes a matter of importance while implementing the system. Effective detection of an attack may depend on the ability to

i. Detect patterns in user activity that are characteristic to an attack
ii. Detect changes in system behavior that suggests the presence of biased data

The first approach could be drawn from classic intrusion detection systems. In which we generally monitor the system for activity of a known pattern of an attack. If any suspecting user is found to be actively following the patters of a known attack, we could, for example, restrict the user from accessing the service.

The second attack can be a bit tricky to realize. Because a successful attack might not leave any trace behind of biased data. Although some analysis techniques could be applied like we could compare the data distribution of previously captured data to the new data set obtained and verify the subsets that seems like an anomaly in the data.

Another type of attack could be when a malicious user could give a chapter/item a high or low rating multiple time with various bogus profiles to manipulate the recommendations.

There have been various studies in the attack modeling in a recommender system, we would need to evaluate each and every type of attack to make it resistant to most if not all of them.

Perfect Knowledge attack: In this type of attack the bogus profiles which are injected by the attacker exactly matches the genuine profiles which show biased against a particular recommendation. [5] discusses the perfect knowledge attack in detail.

Random attack: In random attack only, a particular rating of the item is biased, and all other ratings are chosen at random. [6] uses this attack type craft profiles which has the same overall properties as the dataset but a different distribution of ratings across the items.

Consistency attack: in this kind of attack only the consistencies for different items are manipulated rather than the absolute value. [6] discusses this in detail.

Probing attack: In probing attack the attacker attempts to know the algorithm or parameters or both, of the recommender system. In security, it is a well-established principle that the fewer secrets a security system depends upon, the more secure the system is [7]. Thus, the security of a recommender system should not depend on the secrecy of its algorithm.

2.2. Privacy

2.2.1. Implicit considerations

Privacy is another serious concern in an online recommender system. While dealing with data to train/test various recommendation models, it should be of utmost priority to not violate the privacy of the users.

In the dissertation, we will be taking care of this by utilizing only the publicly available data given by Scratch itself. If at all any user sensitive data is present in the dataset it will be masked or discarded.

Also, if the research requires additional information from the Scratch platform, we may implement a crawler which will gather the dataset. It will be made sure to not capture any information which may disclose the identity of platform users.

All of this will, of course, be done post a formal approval from the college ethics committee.

2.2.2. Explicit considerations

In addition to implicit considerations, some explicit considerations for the recommender system to be privacy sensitive are as below.

The recommender system should not leak any information apart from what can be inferred from the recommendation. i.e. The output should not help an attacker to identify an individual or its other attributes.

An ideal recommender system that considers security should guaranty full privacy protection while giving the correct utility. Unfortunately, there is always a compromise between privacy and the usefulness of a system.

Some researchers have proposed operations on encrypted values using cryptographic solutions. But, often these solutions are quite computationally expensive. As suggested in [9], it can be up to six orders of magnitude difference in a cryptographic v/s plaintext arithmetic operation. This could again reduce the utility of the system.

Some of the privacy-preserving techniques that we could be exploring would include the following.

- Homomorphic encryption [2] in which the operations are done on ciphertexts and the results are then generated in encrypted form.
- Garble circuits [3,4] that allow two parties to evaluate any function without leaking information about their inputs apart from what can learn from the outputs.

A recent change in the privacy policy of Scratch [10], specify new data retention, protection, and data transfer rules in accordance with Europe's GDPR policy changes. This shows the impact stricter governing rules form governments could enforce companies for more stringent privacy policies.

Along with all this the general security practices like choosing a strong encryption standard for storing user information, securing the system and databases in which the information lives, etc., should ensure users private information is safely stored. All this would be considered while designing the recommender system.

Reference

[1] https://scratch.mit.edu/about

[2] Craig Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.

[3] Andrew Yao. How to generate and exchange secrets. In Foundations of Computer Science, 1986., 27th Annual Symposium on, pages 162–167. IEEE, 1986.

[4] Dahlia Malkhi, Noam Nisan, Benny Pinkas, Yaron Sella, et al. Fairplaysecure two-party computation system. In USENIX Security Symposium, volume 4. San Diego, CA, USA, 2004.

[5] O'Mahony, M., Silvestre, G. and Hurley, N. Collaborative Recommendation: A Robustness Analysis. ACM Transactions on Internet Technology. In press. Accessed at http://www.cs.ucd.ie/staff/nick/- home/research/download/omahony-acmtit2004.pdf.

[6] Lam, S. K. and Riedl, J. Shilling Recommender Systems for Fun and Profit. In WWW 2004, New York, May 2004.

[7] Schneier, B. Secrecy, Security and Obscurity. CryptoGram, May 15, 2002. Accessed at http://www.schneier.com/crypto-gram-0205.html.

[8] M. Beye, A. Jeckmans, Z. Erkin, Q. Tang, P. Hartel, and I. Lagendijk. Social Media Retrieval, chapter Privacy in Recommender systems, pages 263–281. Springer, 2013.

[9] NetEase Youdao. P4p: practical largescale privacy-preserving distributed computation robust against malicious users. 2010

[10] https://scratch.mit.edu/privacy_policy