Steganographic Encoded Communication in Social Media

Ashley Ferraro
ECE Department
University of Virginia
cbf6yd@virginia.edu

***Abstract*—This paper will present a proposed way of communicating encrypted data through social media. This proposed form of steganographic communication is one that focuses on disguising encrypted communications as typical social media traffic. This method accomplishes this by using a network of bots to communicate a message through public social media features such as liking, commenting, favoriting, etc.**

Keywords— Steganographic, transmitter account, receiver account, cyclical network

I. INTRODUCTION

The proposed system in this paper is a method that is designed to conceal the medium in which encrypted messages are passed through. This method is an example of steganography, which is the study of concealing message or data hidden within plain site to avoid detection. The premise of steganography has been studied for centuries, and digital steganography has been in use since as early as the 1990s [1]. This paper contains a proposed digital steganographic system that relies on hidden communication in social media platforms using a network of fake accounts.

This system is capable of transmitting data without directly sending a message to a particular user. Rather, this system hides communication by having a collection of fake accounts perform arbitrary actions such as liking, commenting, or favoriting in such a way that any account that can see these actions can derive an encoded message from it.

This means any account knowledgeable of the network and how it operates can decode an external message by looking at their social media dashboard. This data even when under review will only seem to be a normal browsing feed. This results in a system of communication that is hard to detect and one that even if discovered reduces the possibility of any malicious actors or criminals from being incriminated because of its discovery.

The conceptual system presented in this paper is limited in scope to around 128 bytes, 1024 bits, per message and has a high amount of complexity present behind it. Nonetheless, this system serves as conceptual example of how information can be transmitted discretely over social media in ways previously not conceived. It is possible more advanced variations of this fundamental concept could be implemented in a practical form that improves the amount of information transmitted.

II. FUNCTIONALITY

This system can function in variety of forms and be implemented in many social media sites. However, for the sake of clarity and to allow for easy comprehension, this paper will use Twitter as an occasional example and the only action that will be used to encode the information will be retweeting. While this system can use many actions at once such as liking or commenting to increase the amount of information encoded, this paper will only focus on one social media action.

A. Simplifed Model

This model is a simplified version meant to convey the basics of the system. In this system there is two accounts that are malicious. One account is the *transmitter account*, which is the account that uses its actions on social media, in this case retweeting, to encode data. The other account is the *receiving account*. The receiving account is able to view the actions of the transmitting account such that it can decode data based on the transmitting account's actions.

In this example the transmitting account encodes data by performing a social media action on certain accounts that it follows, such as retweeting. Let's assume the number of accounts the transmitter account follows is 8. This is shown in Figure 1.

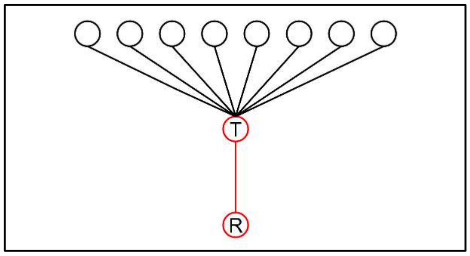

Figure 1: Simplified Model

The transmitting account assigns a number to each account it follows, which can be any unrelated legitimate account. This is shown in Figure 2.

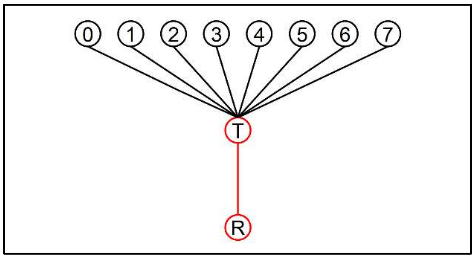

Figure 2: Simplified Model with Numerical Labels

The transmitter account performs a social media action, such as retweeting, on one of the eight accounts. Upon doing so this is observed by the receiving account as the receiving account is following the transmitter account. The receiving account can decode this social media action by looking up what numeral was associated with that account. So, by retweeting one account the receiving account can decode the number the transmitting account wished to communicate.

The amount of information that is encoded per action when converted to bits is equivalent to 3 bits. An example of the respective bits associated with each account is shown below in Table 1 to help in comprehension. It should be noted that assigning numbers to accounts is arbitrary and can be randomized.

TABLE I. EXAMPLE OF ENCODED BITS

Associated Encoded Bits with Social Media Action		
Account Retweeted	***Number***	***Bits***
Account 1 Retweeted	0	000
Account 2 Retweeted	1	001
Account 3 Retweeted	2	010
Account 4 Retweeted	3	011
Account 5 Retweeted	4	100
Account 6 Retweeted	5	101
Account 7 Retweeted	6	110
Account 8 Retweeted	7	111

To better convey the capabilities of this system, shown below is the equation that characterizes the relation between the information transmitted by transmitter accounts and the accounts a transmitter account follows.

$$A = 2^b \tag{1}$$

Where A represents the accounts followed by each transmitter accounts and b represents the amount of information in bits that each transmitter accounts transmits per social media action. Therefore 256 accounts followed could transmit 8 bits and 1024 accounts followed could transmit 10 bits in a single social media action. This relationship is exponential. This results in less information encoded as more accounts are followed. Therefore, with this simplified model there is a practical limit to encoding information in this system. To showcase this limitation and to visualize the relationship showcased in Equation 1, Figure 2 is shown below.

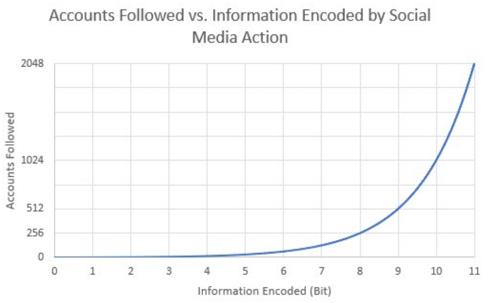

Figure 2: Accounts Followed vs. Information Transmitted

In order to transmit 1 more bit of information the amount of accounts followed must be doubled. This results in a practical limit of this system residing around 256-512 accounts followed by a single transmitter account. The amount of information transmitted is very low; 8-9 bits per social media action. However, this model can be expanded by increasing the amount of transmitter accounts within this network and cycling between each account to transmit parts of a message.

B. *Cylical Model*

One proposed alteration of this system is adapted by multiplying the amount of transmitter accounts within a network and establishing a cycle in which each transmitter account performs a social media action after another.

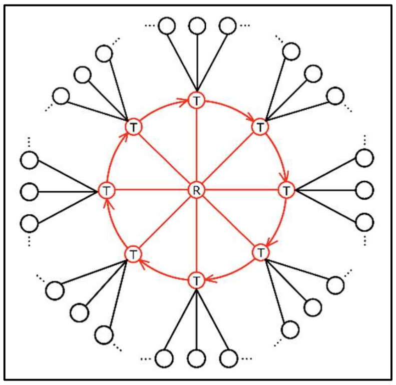

Figure 3: Cyclical Configuration

All transmitter accounts are controlled by the same actor, potentially through separate VPNs, and a message is encoded by one transmitter account after another performing a social media action on a legitimate account they are following. This continues in a cycle until each transmitter account interacts with enough posts from different accounts such that the data is sent. Using Twitter as an example each transmitter account in this system would retweet one after another in specific order until the receiving account following the transmitter accounts receives the data. To characterize this system Equation 2 is shown below.

$$\frac{s}{b} = IT \tag{2}$$

Where s represents the size of the message in bits and T represents the amount of transmitter accounts in the cyclical network. The variable b is the bits presented in Equation 1 that each transmitter account will transmit upon performing one social media action. The variable I represents the amount of social media actions needed to transmit the information by each transmitter account. In addition, the amount of social media actions performed by a single transmitter account in this cycle is shown in Equation 3 below.

$$\frac{I}{T} \tag{3}$$

As an example, a small network of 64 transmitter accounts each following 256 accounts is configured in a cyclical configuration in which one transmitter account performs one social media action after another. To transmit a message s with a size of 1024 bits the required amount of social media actions would be 128. This requires each transmitter account to perform two social media actions each; using Twitter as an example this would be two retweets for each transmitter account.

This level of activity for each transmitter account is very low, which is ideal for maintaining a low profile on social media websites. While the receiving account will have to view a total of 128 individual social media actions, this task becomes easy as all activity is shown on the receiving account's dashboard. Therefore, no direct messaging or direct interaction between the receiving account and transmitter account is performed.

III. Obscuring Methods

This system proposed in this paper, or the information transmitted by this system, can be further concealed from discovery by implementing a variety of methods. These methods aren't inclusive of all possible modifications that can be performed on the system, rather these methods presented are the more obvious or useful methods.

A. Pseudo Random Number Assignment

A method that makes it difficult to decode the information transmitted is randomly assigning which section of the message a transmitter account transmits per social media action. This random order would be determined by a Pseudo Random Number Generator (PRNG) in which the seed for the random number generator is shared between the transmitting account network and receiving account. A visualized example of this random assignment is shown in Table 2 below. For simplicity this example and section assumes only one social media action is performed per transmitter account. However, this simplification doesn't have any impact towards the results presented in this section.

TABLE II. Parts of Message Assignment

	Transmitter Account Assigned to Part of Message	
Parts of Message in Bits	***Bits Transmitted***	***Random Transmitter Account***
$b_0 \dots b_7$	8	T_4
$b_8 \dots b_{15}$	8	T_1
$b_{16} \dots b_{23}$	8	T_3
$b_{24} \dots b_{31}$	8	T_2

This random assignment of transmitter accounts to pieces of the data further obscures any message transmitted over this medium. In order to obtain the information transmitted any third-party observer would have to obtain the PRNG seed and algorithm. To characterize how much this obscures the original message Equation 4 is shown below. The number that is produced by Equation 4 is the number of possible combinations in which order does matter and there is no replacement.

$$T! \tag{4}$$

Therefore, for a network of 64 transmitter accounts the number of possible transmitter account to data combinations is approximately $1.29 \cdot 10^{89}$. While this amount may seem extreme, the calculations presented are like those performed to calculate the number of possible combinations for a deck of cards. This number approximately is $8.06 \cdot 10^{67}$ [6].

If each transmitter account can perform multiple social media actions, then the number of combinations relates to number of iterations in a cycle wherein the variable I was established in Equation 2. The probability of guessing the correct data assignment to each transmitter account is reproduced below in Equation 5.

$$P(E) = \frac{1}{I!} \tag{5}$$

B. Unused Followed Accounts

A method to further obscure the network is for the transmitting and receiving accounts to follow legitimate accounts. By following legitimate accounts any relationship between a transmitting account and a receiving account becomes less definite. In essence this will allow the network to blend in with the activity in the social media website. To visually showcase this principle this method is shown in Figure 5 below.

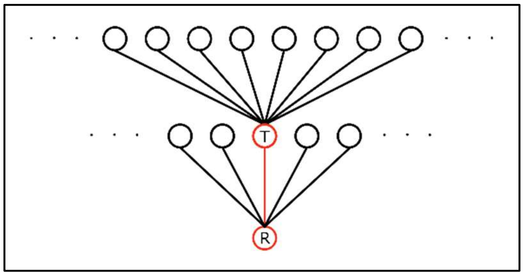

Figure 5: Generic Simplified Model with Unrelated Actors

If transmitting accounts especially follow accounts that aren't used in relaying data, then another layer of difficulty is added to decoding the transmitted data. If the assigning of bits for each followed account is random then the possible number of combinations are shown in Equation 6 below.

$$P(E) = \frac{1}{A!} \tag{6}$$

However, let's say that on top of randomizing which bits correspond to which followed account the transmitter accounts follow unused accounts. This means any social media action performed on these unused accounts does not contribute towards encoding data. The probability of successfully determining which accounts followed are unused or meant to be ignored is shown in Equation 7.

$$P(E) = \prod_{k=0}^{n} \frac{1}{A-k} \tag{7}$$

Wherein A is the accounts followed by each transmitter account and n is the amount of ignored accounts followed by each transmitting account. As an example, let's say 256 accounts are followed that are meant to be used while 64 accounts are to be ignored upon performing a social media action on it. This would give us the probability or determining which accounts are to be ignored by a third party is $1.583 \cdot 10^{-160}$.

C. Dummy Transmitter Accounts and Networks

If methods are implemented in order to detect the activity or existence of a transmitter network creating fake transmitter accounts or even entire networks could be an effective tactic in wasting third-party resources. In order to decrypt or identify a network it is anticipated until tools are created to autonomously detect networks that human resources must be utilized. Therefore, creating networks that are easier to discover could result in significant waste of resources. This could also provide a metric for malicious actors on what methods or activity is exposing transmitter networks. By having networks that don't contain any sensitive information becoming removed or monitored, malicious actors can update more subtle transmitter networks to protect against actual networks from being exposed.

IV. Uses

The system described in this paper presents a method of transmitting information disguised as social media activity indirectly between users. The limits of this system lie within the low amount of data transmitted per social media action. Therefore, the utility of this system lies within short discrete messages rather than long messages or file transferring.

It should be reaffirmed that this system can exist in other social media sites besides Twitter, which was used as an example in this paper. If a social media site has the ability to interact with other users in the form liking posts, favoriting, commenting, etc. and those actions are visible to other accounts then a similar system can be created and used to transmit information. Possible social media site that this system can be used in is Facebook, Instagram, and Reddit.

A. Encryption Keys

An example of a novel use of this system involves asymmetric cryptography. A small cyclical network is capable of transmitting anywhere between 512 to 1024 bits. This amount of data is enough to transmit private encryption keys. Encryption keys range from anywhere between 120, 192, 246, and 1024 bits in length [2]. In order to maintain secure communications between malicious actors, encryption keys should be occasionally exchanged in a set schedule. This is performed in order to reduce the chance of a compromised private key being used to decrypt past or future sensitive information.

While this encoded information is posted on an active social media website, it would be very difficult to differentiate encrypted traffic from normal social media traffic. The system is shrouded in a sea of user generated activity, which is an enormous amount of data to sift through. Twitter alone has approximately 322.4 million daily users worldwide in 2021, with each user consuming or producing data through their activity [3]. Even if a third party purposefully monitors activity for bots, they'll have a hard time differentiating between the bots already existing on social media platforms.

With an upwards estimate of 15% of all Twitter's active users being bots and with cases of influencers buying thousands of bot followers to inflate their online following, it would be difficult to characterize automated accounts between transmitter accounts [4]. Potential tools or advanced monitoring methods could be developed with help from western social media companies to characterize suspicious activity, but will require time and effort to create or use effectively.

B. Short Communication and Coordination

It is expected that due to the limited amount of data that can be transmitted during use, that this would only be used for basic and brief communication. This communication could possibly involve coordinating time/dates, location information, or brief updates. However, this isn't an inclusive list of all the potential applications. Depending on the creativity of the malicious actor this system can be used for any application that requires in-direct communication limited only by the size of the data transmitted.

To put into perspective the versatility of this limited system a comparison to frequently used medium of communication is provided. The data transmitted is comparable in size and use to a typical SMS text message. A SMS message utilizing GSM-encoded characters, 7 bits in length, is a maximum of 140 bytes (1120 bits) [5]. In comparison, in the previous example presented a cyclical network involving 64 transmitter accounts and 256 followed accounts can transmit 128 bytes.

V. Conclusion

Presented in this paper is a foundation that can be potentially improved upon through future implementations and research. If this system were to exist, it would be slightly different than the system proposed in this paper. More efficient methods of encoding information per social media action of other accounts could be performed to reduce the size and complexity of the transmitter network.

Rather, the proposed system is an example of one of the many potential ways a malicious actor or criminal can exchange information indirectly without being noticed. Every time a medium of illegal communication or coordination is cut off another one will be invented as a direct response. While it is unlikely a system like this may currently exist, the fact that it could exist is valuable in of itself. After all, in order to keep pace of the cat and mouse game that is cybersecurity, it's better if we invent a new system before any malicious actors do. Using our creativity and considering potential alternatives is one of the few ways we can ever hope to gain an advantage over people who wish to perform illegal activities or cause harm to others.

References

[1] Newman, L. H. (2017, June 26). What Is Steganography? Retrieved from https://www.wired.com/story/steganography-hacker-lexicon/

[2] Stubbs, R. (2021, November 19). *Classification of cryptographic keys*. Cryptomathic. Retrieved December 26, 2021, from https://www.cryptomathic.com/news-events/blog/classification-of-cryptographic-keys-functions-and-properties

[3] Published by Statista Research Department, &amp; 9, N. (2021, November 9). Twitter: Number of users worldwide 2020. Statista. Retrieved December 26, 2021, from https://www.statista.com/statistics/303681/twitter-users-worldwide/

[4] Confessore, N., & X, G. J. (2018, January 27). The Follower Factory. Retrieved from

https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html

[5] Support, N. (2020, April 17). How Long is a Single SMS body? Retrieved from https://help.nexmo.com/hc/en-us/articles/204076866-How-Long-is-a-Single-SMS-body-

[6] *There are more ways to arrange a deck of cards than there are atoms on Earth*. Office for Science and Society. (2019, July 16). Retrieved December 26, 2021, from https://www.mcgill.ca/oss/article/did-you-know-infographics/there-are-more-ways-arrange-deck-cards-there-are-atoms-earth