Effective Forest Fire Attack Prevention Using Social Authentication Security Model

SHANMUGAM P, Dr. D.SIVABALASELVAMANI

Web services present most commonly rely on passwords to authenticate users. Unfortunately, two serious issues in this paradigm are: users will inevitably forget their passwords, and their passwords could be compromised and changed by attackers, which result in the failures to access their own accounts. Therefore, web services often provide users with backup authentication mechanisms to help users regain access to their accounts. Unfortunately, current widely used backup authentication mechanisms such as security questions and alternate email addresses are insecure or unreliable or both Recently, authenticating users with the help of their friends has been shown to be a promising backup authentication mechanism. A user in this system is associated with a few trustees that were selected from the user's friends. This paper provides the first systematic study about the security of trustee-based social authentications. This paper introduces a novel framework of attacks, which is called as forest fire attacks. In these attacks, an attacker initially obtains a small number of compromised users, and then the attacker iteratively attacks the rest of users by exploiting trustee-based social authentications. Then, a probabilistic model is constructed to formalize the threats of forest fire attacks and their costs for attackers. The attacks will happen in the different phases that are the user registration phase or at the recovery phase the attacker try to enter in to the system in this phase this attack is done by the attacker to enter in to the network

I. INTRODUCTION

In a social context, trust has several connotations.[1] Definitions of trust[2][3] typically refer to a situation characterized by the following aspects: One party (trustor) is willing to rely on the actions of another party (trustee); the situation is directed to the future. In addition, the trustor (voluntarily or forcedly) abandons control over the actions performed by the trustee. As a consequence, the trustor is uncertain about the outcome of the other's actions; they can only develop and evaluate expectations. The uncertainty involves the risk of failure or harm to the trustor if the trustee will not behave as desired

Attacker entices computers to log into a computer which is set up as a soft AP (Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a "de-authentication attack". This attack forces AP-connected computers to drop their connections and reconnect with the hacker's soft AP (disconnects the user from the modem so they have to connect again using their password which one can extract from the recording of the event). Man-in-the-middle attacks are enhanced by software such as LANjack and AirJack which automate multiple steps of the process, meaning what once required some skill can now be done by are particularly vulnerable to any attack since there is little to no security on these networks..

- To novel framework of attacks, which we call forest fire attacks.
- To formalize Model the threats of forest fire attacks and their costs for attackers. More-over, we explore various attack scenarios and defense strategies.
- To extensively evaluate these attack scenarios, defense strategies, and the impact of system parameters using three real-world social network

The attacker could use a greedy strategy to select seed users. Specifically, the attacker selects seed users one by one. To select a seed user, the attacker iterates over each user that is not a seed user yet; for each such user u, the attacker pretends that u is a seed user and simulates our security model to predict the corresponding expected number of compromised users; and the user u which increases the expected number of compromised users by the most is added as a new seed user. However, it is not scalable to large social networks. It is a proposed research work to make the strategy scalable.

In paper design a trustee selection strategy based on some notion of community. Specifically could select trustees for users such that the trustee network consists of isolated communities, which could constrain the propagation of forest fire attacks. It is a proposed research work to explore these community-based trustee selection strategies.

A compromised user u might request a verification code from the service provider when the attacker performs an attack trial to a user who selects u as a trustee. Thus, a compromised user who is a trustee of many other users might request many verification codes each attack iterations. Therefore, limiting the number of verification codes that each user can request within a given period of time (e.g., one hour) can slow down forest fire attacks.
It is an interesting future work to explore the impact of such rate limiting on forest fire attacks and what strategies attackers can adopt to maximize the number of compromised users given a time constraint.

In proposed framework to extensively evaluate various concrete attack scenarios, defense strategies, and the impact of system parameters using three real-world social networks. First, find that forest fire attack is a potential big threat. In particular, when all the users with at least 10 friends in these social networks adopt trustee-based social authentications, an attacker can compromise tens of thousands of users in some cases even if the number of seed users is 0 using a small number users, the attacker can further compromise two to three orders of magnitude more users with low (or even no) costs of sending spoofing messages.

Second, our defense strategy, which guarantees that no users are selected as trustees by too many other users, can decrease the expected number of compromised users by one to two orders of magnitude and increase the costs for attackers by a few times in some cases. Third, find that, in contrast to existing work where the recover threshold is set to be three, it could be set to be four to better balance between security and usability.

Finally, improve authentication mechanisms such as security questions and alternate email addresses are insecure or unreliable or both. Previous works have shown that security questions are easily guessable and published, and those users might forget their answers to the security questions. A previously registered alternate email address might expire upon the user's change of school or job. For the above reasons, it is important to design a secure and reliable backup authentication mechanism.

The paper is organized as follows: The Chapter 1 describes the general background of the Social network security, objectives of the proposed methodology and definition of the problem. Chapter 2 describes the related work, background study and literature survey. Chapter 3 presents the fundamental system methodology of the proposed system and novel attack alert model is described in detail. Chapter 4 presents implementation software of the proposed model and setup, experimental results, and analysis. Chapter 5 contains the summary, conclusion of the proposed work and enhancement of proposed system as future research work. Chapter 6 consists of various journal references and website references.

II. RELATED WORKS

Joseph Bonneau et al they have report the results of the first large-scale empirical analysis of password implementations deployed on the Internet. Their study included 150 websites which offer free user accounts for a variety of purposes, including the most popular destinations on the web and a random sample of e-commerce, news, and communication websites. Although all sites evaluated relied on user-chosen textual passwords for authentication, they found many subtle but important technical variations in implementation with important security implications. Many poor practices were commonplace, such as a lack of encryption to protect transmitted passwords, storage of clear text passwords in server databases, and little protection of passwords from brute force attacks. While a spectrum of implementation quality exists with a general correlation between implementation choices within more-secure and less-secure websites, they find a surprising number of inconsistent choices within individual sites, suggesting that the lack of standards is harming security

Brainard, et al countless improvements have been proposed to improve password security or replace it altogether, but none has seen any significant adoption in the market for human authentication by Internet sites. The security economics community has begun to ask hard questions about why it is so difficult to deploy better techniques. It seems clear that security researchers have failed to fully understand the incentives in the market for password-based authentication. The demand side of the market is relatively well-known, with a large number of research studies documenting how users choose passwords and how they cope with the difficult requirement of maintaining passwords with many online accounts. Many users still choose easily-guessable passwords write them down, share them casually with friends, and rarely change yet frequently forget them. Most critically, users frequently re-use passwords, with the average password being shared by at least 5 sites.

J. Podd, J. et al practices cannot be written off as evidence of user ignorance or apathy. Consumer research shows that security remains the primary stated concern of e-commerce customers. Most users generally understand that there are risks of using easy-to-guess passwords or re-using passwords and recognize that they should separate high-security accounts from low-security ones. However, users simply have too many accounts to manage securely, with the average user holding over 25 separate password accounts. Users frequently state that they re-use passwords knowing it is risky because they simply feel unable to remember any more, and evidence suggests users are stretching their memory to its limits: traffic logs indicate that more than 1% of all Yahoo! users forget their passwords in any given month , and a laboratory study showed that users are unable to remember their own passwords for as many as a quarter of sites they have registered with .

H. Kim et al had presented a first of its kind study to measure and analyze attempts to spread malicious content on OSNs. Their work is based on a large dataset of "wall" messages from Facebook. Wall posts are the primary form of communication on Facebook, where a user can leave messages on the public profile of a friend. Wall messages remain on a user's profile unless explicitly removed by the owner. As such, wall messages are the intuitive place to look for attempts to spread malicious content on Facebook since the messages are persistent and public, i.e. likely to be viewed by the target user and potentially the target's friends. Through crawls of several Facebook regional networks conducted in 2009, they obtained a large anonymize dataset of Facebook users, their friendship relationships, and 1.5 year-long histories of wall posts for each user . In total, their dataset contains over 187 million wall posts received by 3.5 million users.

Hyoungshick Kim [4] describes a number of web service firms have started to authenticate users via their social knowledge, such as whether they can identify friends from photos. In this paper they have investigated attacks on such schemes. First, attackers often know a lot about their targets; most people seek to keep sensitive information private from others in their social circle. Against close enemies, social authentication is much less effective. They formally quantify the potential risk of these threats. Second, when photos are used, there is a growing vulnerability to face-recognition algorithms, which are improving all the time. Network analysis can identify hard challenge questions, or tell a social network operator which users could safely use social authentication; but it could make a big difference if photos weren't shared with friends of friends by default. This poses a dilemma for operators: will they tighten their privacy default settings, or will the improvement in security cost too much revenue.

I. Polakis et al face book recently launched a new user authentication method called “social authentication” which tests the user’s personal social knowledge. This idea is neither unique nor novel but Face book’s implementation is its first large scale deployment. A user is presented with a series of photos of their friends and asked to select their name of a highlighted face from a multiple-choice list. The current system is used to authenticate user login attempts from abroad.

Iasonas Polakis, et al [6] described the two-factor authentication is widely used by high-value services to prevent adversaries from compromising accounts using stolen credentials. Facebook has recently released a two-factor authentication mechanism, referred to as Social Authentication, which requires users to identify some of their friends in randomly selected photos. A recent study has provided a formal analysis of social authentication weaknesses against attackers inside the victim’s social circles. In this paper, they extend the threat model and study the attack surface of social authentication in practice, and show how any attacker can obtain the information needed to solve the challenges presented by Facebook

M. Zviran et al describe a recent study, provided a formal analysis of the social authentication weaknesses against attacker within the victim’s social circle. They expand the threat model and demonstrate in practice that any attacker, inside and outside the victim’s social circle, can carry out automated attacks against the SA mechanism in an efficient manner. Therefore they argue that Facebook should reconsider its threat model and re-evaluate this security mechanism.

III. METHODOLOGY

On the trustee-based social authentication includes two phases:

Registration Phase. The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password), and then a few (e.g., 5) friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice’s friend list and are appointed as Alice’s trustees.

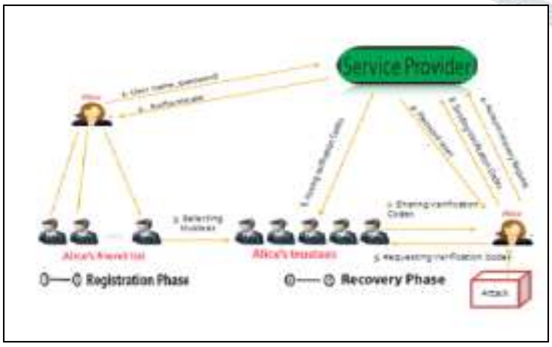

Fig 3.1 Two Phase Attacker

Recovery Phase. When Alice forgets her password or her password was compromised and changed by an attacker, she recovers her account with the help of her trustees in this phase. Specifically, Alice first sends an account recovery request with her username to the service provider which then shows Alice an URL. Alice is required to share this URL with her trustees.

Then, her trustees authenticate themselves into the system and retrieve verification codes using the given URL. Alice then obtains the verification codes from her trustees via emailing them, calling them, or meeting them in person. If Alice obtains a sufficient number (e.g., 3) of verification codes and presents them to the service provider, then Alice is authenticated and is directed to reset her password. Proposed Model call the number of verification codes required to be authenticated the recovery threshold.

FOREST FIRE ATTACKS

The existing methodology forest fire attacks consist of Ignition Phase and Propagation Phase.

- **Ignition Phase:**

In this phase, an attacker obtains a small number of compromised users which trustee call seed users. They could be obtained from phishing attacks, statistical guessing, and password database leaks, or they could be a coalition of users who collude each other. Indeed, a large number of social network accounts were reported to be compromised, 2 showing the feasibility of obtaining compromised seed users.

- **Propagation Phase**

Given the seed users, the attacker iteratively attacks other users. The attacker performs one attack trial to each of the uncompromised users according to some attack ordering of them. In an attack trial to a user u, the attacker sends an account recovery request with u’s username to the service provider, which issues different verification codes to u’s trustees. The goal of the attacker is to obtain verification codes from at least k trustees. If at least k trustees of u are already compromised, the attacker can easily c**m**promise u; other wise, the attacker can impersonate u and send a spoofing message to each uncompromised trustee of u to request the verification code.

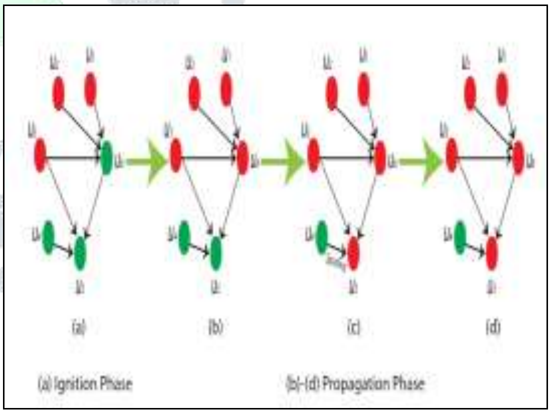

Fig 3.2 Forest Fire Attack

SOCIAL AUTHENTICATIONS

Depending on how friends are involved in the authentication process, social authentications a be classified into trustee based and knowledge-based social authentications. In trustee based social authentications the selected friends aid the user in the authentication process. Knowledge-based social authentication, however, asks the user questions about his or her selected friends, and thus friends are not directly involved.

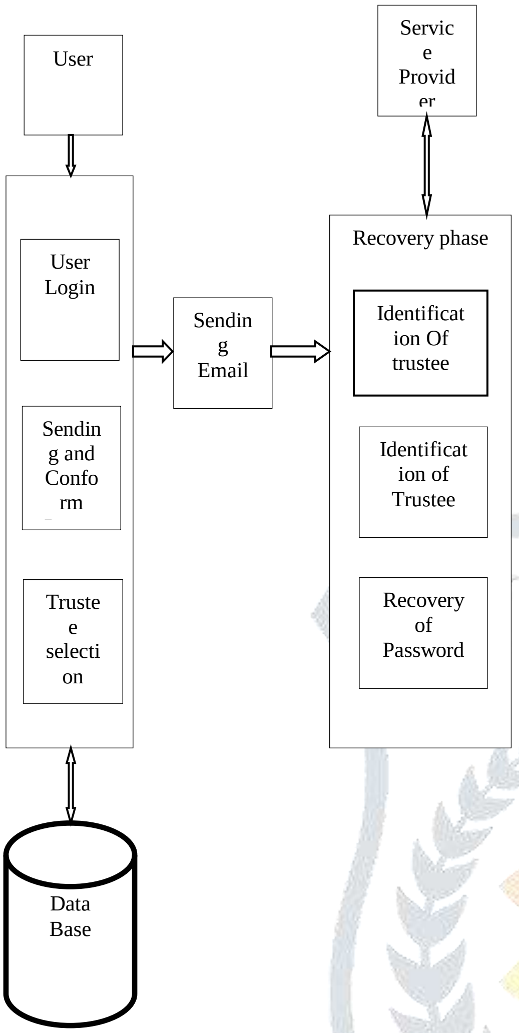

Fig 3.3 Existing Authentication

During the attack, in order to determine if the current flows fA are generating a service degradation, the Meter injects a flow fM of requests ’i overlapped to the attack flows fA, and estimates the service time tS to process each message ’i on the target system. In particular, if they assume that the flow fM is not limited by a network bottleneck, and the network latency is negligible, then, we can approximate tS with the response time of the target application.

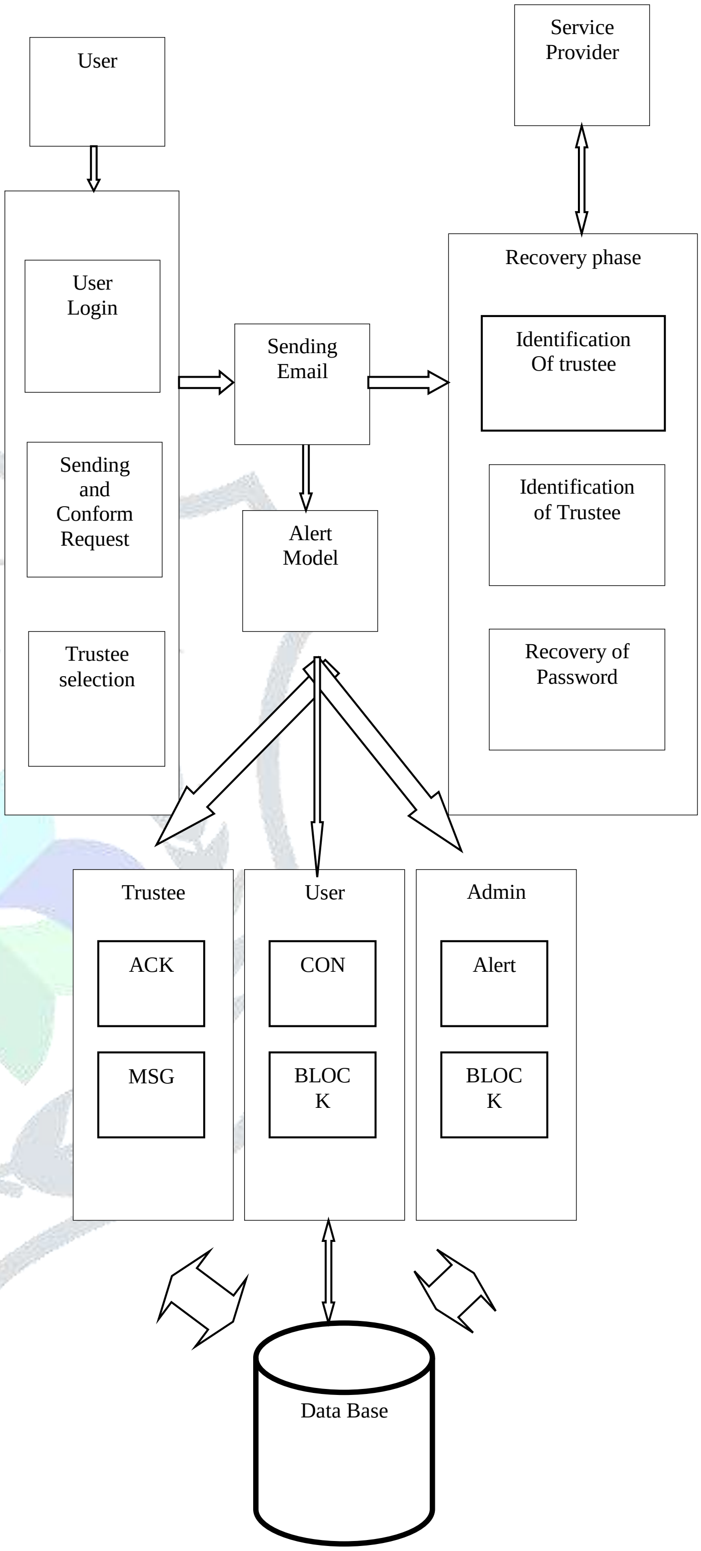

Fig 3.4 Proposed Methodology

Therefore, during a training phase, the attacker can estimate an approximation of the actual distribution of the response time tu, for each message of type #t u, and then, uses it to evaluate the service degradation achieved. Since the actual response time distribution may have a large variance during the attack, the estimation model has to be in charge of identifying message code deviations.

INPUT

The proposed system has the following as the input that is.

Step 1: Select the trustee network users in the service.

Step 2: Recovery threshold (that is the verification code is been obtained from the trusee)

Step 3: Probability of obtaining the verification code from the trustee).

Step 4: The number of seed user in the ignition and the propagation phase.

Step 5: The number of attacks in each iteration.

Step 6: Strategy to select users in the network.

Step 7: Ordering the construction strategy.

Step 8: The average cost of the spoofing attacks.

Step 9: Expected spoofing message.

Step 10: Finally the recovery probability of the recover phase.

OUT PUT

The average cost of the system.

Step1: To get the network trustee among the users.

Step2: Threshold for the recovery.

Step3: The total number of the compromised users.

Step4: The total number of the seed users and strategy.

Step5: The construction order strategy.

3.6. DEFENSE STRATEGIES

3.6.1. Hiding Trustee Networks

Preventing attackers from obtaining a trustee network is an essential step towards the defense of forest fire attacks. In the currently deployed social authentication systems, attackers can obtain a trustee network because users need to know their trustees to retrieve verification codes from them in the Recovery Phase. An alternative implementation of the Recovery Phase is that the service provider directly sends verification codes to the trustees of the user when receiving an account recovery request, and the trustees are required to actively share the verification codes to the user. This implementation does not require users to know their trustees, and thus it is hard for attackers to obtain the trustee network.

However, this implementation is unreliable and could annoy users and their trustees. Specifically, u‟s trustees might already forget they are trustees of u, and thus they might simply treat those verification codes as spams and not share them with u, which results in low reliability. Moreover, users do forget who their trustees are [24], and thus it is highly impossible for u to actively request verification codes from its trustees. If the trustees do actively share the codes with u, then attackers can frequently send account recovery requests to the service provider which immediately sends verification codes to the trustees, and the trustees will (possibly) frequently share the codes with u, which could be annoying to both u and its trustees. More seriously, after u‟s trustees realize that the verification codes are just spams, they might not actively share the verification codes with u even if she is really trying to recover her account, which again results in low reliability. Therefore, hiding trustee networks from attackers sacrifices reliability, which possibly explains why existing trustee-based social authentication systems didn‟t adopt this alternative implementation of the recovery Phase.

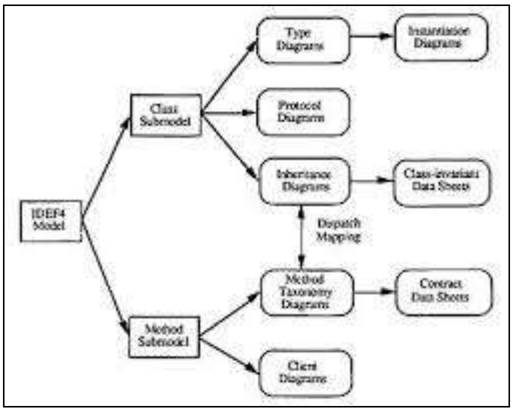

Fig 3.5 Hiding Trustee Networks

3.6.2 Mitigating spoofing Attacks

Another way to defend against forest fire attacks is to remind trustees of not sharing verification codes via messages. This strategy is not novel, and we include it for completeness. Indeed, existing social authentication systems already try to mitigate spoofing attacks. For instance, Microsoft‟s system asks a trustee why she is requesting the verification code and encourages her to share the code with the user via phone or meeting in person.

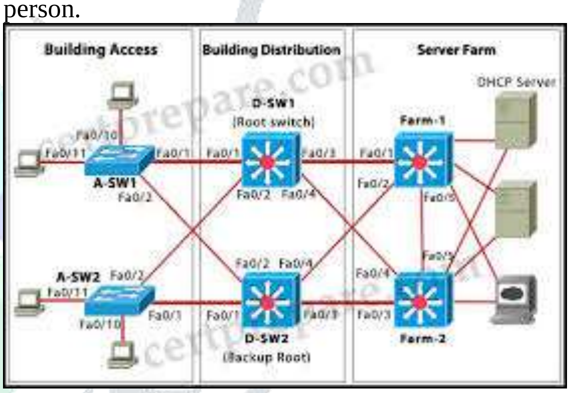

Fig 3.6 Mitigating spoofing Attacks

\3.6.3 Constraining Trustee Selections

Finally, introduce strategies to constrain trustee selections, which are easy to implement and effective at defending against forest fire attacks. We consider both local trustee selection strategies and global trustee selection strategies. A local trustee selection strategy is based on a user‟s local social network structure while a global one is based on the entire social network structure. A name these strategies with a prefix „T-‟ to indicate that they are used to select trustees. A note that how users select their trustees in a real trustee-based social authentication system such as Facebook‟s Trustee Contacts is not clear and thus might not be one of our strategies. However, our work focuses on a comparative study about different trustee selection strategies and can shed light on which strategy is more secure.

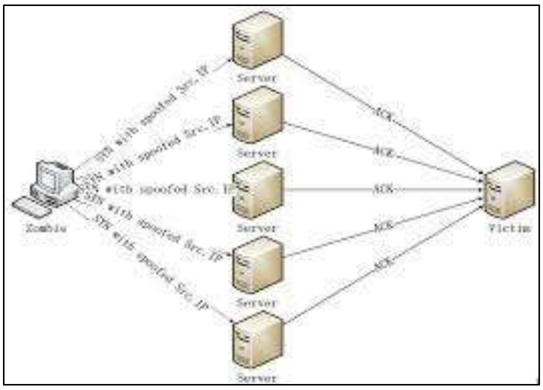

Fig 3.7 Constraining Trustee Selections

```
//*Algorithm 1 Existing Model*\\
//Selecting seed users in the Ignition Phase.
S ←− S(GT , ns )
//Calculating the compromise probabilities.
//Ignition Phase.
for u ∈ VT do
if u ∈ S then p(0)
c (u) ←− 1
else
p(0) c (u) ←− 0
end
p(0) a (u) ←− p(0)
c (u)
end
//Propagation Phase.
t ←− 1
C ←− 0
while t ≤ n do
//Constructing an attack ordering.
O(t ) ←− O(GT , p(t−1), a (VT ))
for i = 0 to O(t ) .size() − 1 do
u ←− O(t ) [i ]
Apply to u.
p (t ) a (u) ←− 1 − (1 − p(t−1) a (u))(1 − p(t ) c (u))
p(t )a (u) ←− (1 − p(t ) r (u))p(t ) a (u) c(t )
(u)←− Apply
C ←− C + c(t ) (u)
end
t ←− t + 1
end
//The expected number of compromised users.
nc(GT , k, ns , n, S,O) ←− u∈VT  p(n) a (u)
//The expected cost.
c(GT , k, ns , n, S,O) ←− cI + ceC
return nc(GT , k, ns , n, S,O), c(GT , k, ns , n, S,O)
            end
```

ATTACK STRATEGIES

The attacker could design the seed users selection strategy and the attack ordering construction strategy to maximize the expected number of compromised users. First, we show that finding the optimal set of seed users and the optimal ordering construction strategy is NP-Complete. Then, we explore various scenarios where seed users have different properties and introduce two ordering construction strategies

IV.PERFORMANCES ANALYSIS

The following Table 4.1 describes experimental result for comparison between existing and proposed system for in social networking using average attacker discovery. The table contains social network communication effectiveness, number of user communication, number of social Workers details, and average of attacker occur finding in existing system and average of attacker finding in proposed system details are shown.

$$\boxed{O(n) = \text{Average Case} = [(25*5)/5]/100}$$

$$\boxed{O(n) = \text{Average Case} = [(NSW*NC)/N]/100}$$

Table 4.1 Comparisons For Existing And Proposed System In Social Network Communication User

S.No	Number of User Communication [NC]	Number of Social Workers [NSW]	Average of attack finding in existing system (%)	Average of attack finding in Proposed system (%)
1	5	25	25.50	26.60
2	10	30	38.12	40.56
3	15	35	43.55	46.65
4	20	40	50.17	53.44
5	25	45	57.87	61.33
6	30	50	61.45	65.46
7	35	55	69.07	72.34
8	40	60	75.90	78.39
9	45	65	82.96	85.76
10	50	70	85.33	89.86

The above table shoes that the number of user communication happened between the number of user communication is occurred and the number of social workers and finding the attacker attacks in the existing system and the another field shows the number of attacks found in the proposed system that will be calculated in the above table numeric table calculation.

The following Fig 4.1 describes experimental result for comparison between existing and proposed system for in social networking using average attacker discovery. The figure contains social network communication effectiveness, number of user communication, number of social Workers details, and average of attacker occur finding in existing system and average of attacker finding in proposed system details are shown.

The above chart shows the average number of the attacker findings in the existing system and the average number of attackers in the proposed system the x axis shows the average attack time intervals. The y axis show the average attacks in the proposed system. That is been illustrated in the above chart.

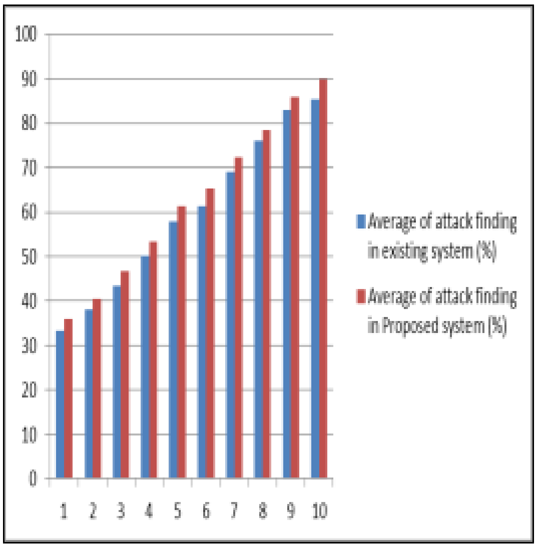

Fig 4.1 Comparison for existing and proposed system in scavenging effectiveness

The following Table 4.2 describes experimental result for comparison between existing and proposed system for in social network using average time taken finding attacker discovery. The table contains average attacker finding, number of user working details, number of social worker and average of attacker occur finding in existing system and average of attacker finding in proposed system details are shown.

O (n^2) = Best Case = [(NSW*NC)/N]/1000

O (n^2) = Best Case = [(25*5)/N]/1000

The above table 4.2 shows that the number of user communication happened in the particular time between the particular time that is number of user communication is occurred and the number of social workers and finding the attacker attacks in the existing system and the another field shows the number of attacks found in the proposed system that will be calculated in the above table numeric table calculation.

Table 4.2 Comparison for existing and proposed system in Finding Attacker effectiveness (Time)

S.No	Number Communication User (NC)	Number of Social Workers (NSW)	Average of attack Finding Time in Existing system (ms)	Average of attack Finding Time in Proposed system (ms)
1	5	25	25	26
2	10	30	35	31
3	15	35	42	39
4	20	40	54	48
5	25	45	63	57
6	30	50	72	68
7	35	55	81	75
8	40	60	95	84
9	45	65	99	87
10	50	70	103	95

The following Fig 4.2 describes experimental result for comparison between existing and proposed system for in social network using average time taken finding attacker discovery. The figure contains average attacker finding, number of user working details, number of social worker and average of attacker occur finding in existing system and average of attacker finding in proposed system details are shown.

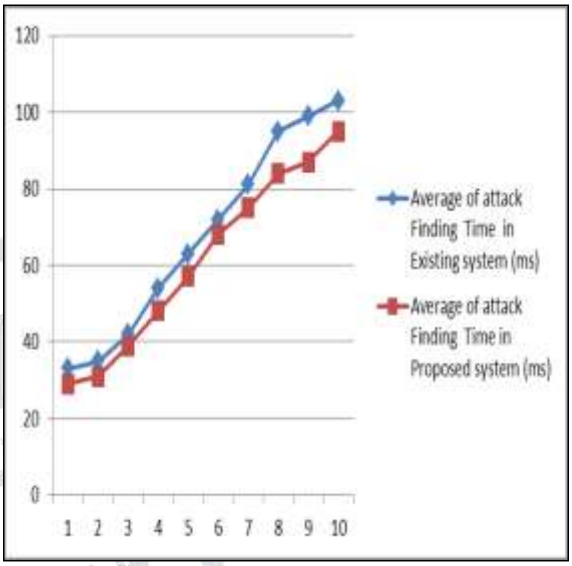

Fig 4.2 Comparison for existing and proposed system in Finding Attacker effectiveness (Time)

The above chart shows the average attacker finding time and the number of user working in the social network the comparison for the existing and the proposed findings attackers effectiveness in the particular time.

RESULTS

The performance of the project is concerned with the existing system and the suitable graphs are constructed and it is based on the parameter like average attacks in the Existing system. The average is been created for the existing system and the proposed system are continuously measured in this feature reduction.

In this experiment the table represents the average of the customer arrived in the network that is the total number of the users in the network and the total number of the users are in the communication that is which user can be communicate with the other user in the network during the communication the average attacks that is happened in the when the existing techniques are used in the system that average without mentioning the time interval of the system that is represented in the figure 5.1.

The graph demonstrate the detection ratio of the attacker when the communication is established between the users in the social networking it is not completely based on the time limits the user limit starts form 0 to 10 and the attack ratio starts form 0 to 100 the graph diagram raised consistently form 0 to 100.This graph shows that when the more number of user in the network is there the attack will be more comparatively this will be the major problem in the existing system.

The table 5.2 define the how the attack is been gradually reduced by proposing the new technique in the proposed system .Experimental result for comparison between existing and proposed system for in social network using average time taken finding attacker discovery. The figure contains average attacker finding, number of user working details, number of social worker and average of attacker occur finding in existing system and average of attacker finding in proposed system details are shown in figure 5.2.

The result when comparing the existing system and the proposed system the result is been gradually reduced form (20%) in the existing system this will be more useful in the proposed system.

The graph is been constructed to keep track of the attacks in the time limitation in the proposed system the time will be represented in milliseconds. It clearly explains the graph that is in the time limit the oscillation is been identified in this type of the attacks.The different types of the attacks is been identified in this attacks that the registration phase attacks that is happened in the registration of the users in the network. The one more attack is found that is recover stage of attack that is been caught out in this execution of the graph.

V. CONCLUSION

In this thesis new proposed system is introduce forest fire attacks. In these attacks, an attacker first obtains a small number of compromised seed users and then iteratively attacks the rest of users according to a priority ordering of them. Second, construct a probabilistic model to formalize the threats of forest fire attacks and their costs for attackers. Third, introduce a few strategies to select seed users and construct priority orderings, and we discuss various defense strategies. For instance, with a small number of users, an attacker can further compromise two to three orders of magnitude more users in some scenarios with low (or even no) costs of sending spoofing messages.

However, defense strategy, which guarantees that no users are trustees of too many other users, can decrease the number of compromised users by one to two orders of magnitude and increase the costs for attackers by a few times in some cases. Moreover, the recovery threshold should be set to better balance between security and usability. The recovery threshold is not set to better balance between security and usability. Time boundary is not set so that after verification code is retrieved from trusted user, the original user or attacker user can use the code at any time in future.

In thesis involves General Symmetric Encryption process which includes tag generation. Here Group based user management is not provided. Also Session based outsource data access is not provided. In future these options can be included so that Session based outsource data access can be provided to increase the security. User Revocation management can also implemented. Key Storage cost can be reduced when compared to existing system.

VI.SCOPE FOR FUTURE ENHANCEMENTS

In the future, how to utilize the inferred information and extend the framework for efficient and effective network monitoring and application design. The new system become useful if the below enhancements are made in future.

- The application can be web service oriented so that it can be further developed in any platform.
- The application if developed as web site can be used from anywhere.
- The algorithm can be further improved so that cost of the path can be further reduced
- The routing automatically reconfigured the path
- Retransmit the lost packets
- The failure can be overcome by further enhancing the technique
- Currently the scheme has a slightly less memory overhead, while in the more complex applications; the scheme may utilize more memory. The future study can be in the area of more significant memory savings.

The new system is designed such that those enhancements can be integrated with current modules easily with less integration work. The new system becomes useful if the above enhancements are made in future. The new system is designed such that those enhancements can be integrated with current modules easily with less integration work.

The social network tag is created to work in the social network tag the entire user are requested to work in that particular tag if any information in the group is been shared by any one of the group member that will be initiated to all the group members of that group that is been tagged by the all group members and the admin of the group. The key management is been done on this social networking that is the key for the communication can be maintained by the admin it leads to secure and the privacy for the key to the user in the group if any one try to work he must need the key to work.

REFERENCES:

1. J. Bonneau and S. Preibusch, “The password thicket: Technical and market failures in human authentication on the web,” in Proc. 9th Workshop Econ. Inform. Security (WEIS), 2010
2. Robert Morris and Ken Thompson. Password security: a case history. Commun. ACM, 22(11):594–597, 1979
3. Cormac Herley, Paul C. Oorschot, and Andrew S. Patrick. Passwords: If We’re So Smart, Why Are We Still Using Them? pages 230–237, 2009
4. Donald A. Norman. When Security Gets in the Way. Interactions, 16(6):60–63, 2009
5. Dinei Florêncio and Cormac Herley. A large-scale study of web password habits. In WWW ’07: Proceedings of the 16th international conference on World Wide Web, pages 657–666, New York, NY, USA, 2007. ACM
6. Nancy J. Lightner. What users want in e-commerce design: effects of age, education and income. Ergonomics, 46(1):153–168, 2003
7. Shirley Gaw and Edward W. Felten. Password Management Strategies for Online Accounts. In SOUPS ’06: Proceedings of the Second Symposium on Usable Privacy and Security, pages 44–55, New York, NY, USA, 2006. ACM

8. Gilbert Notoatmodjo and Clark Thomborson. Passwords and Perceptions. In Ljiljana Brankovic and Willy Susilo, editors, Seventh Australasian Information Security Conference (AISC 2009), volume 98 of CRPIT, pages 71–78, Wellington, New Zealand, 2009. ACS
9. Shirley Gaw and Edward W. Felten. Password Management Strategies for Online Accounts. In SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security, pages 44– 55, New York, NY, USA, 2006. ACM
10. Blake Ives, Kenneth R. Walsh, and Helmut Schneider. The Domino Effect of Password Reuse. Commun. ACM, 47(4):75–78, 2004
11. Ashlee Vance. If Your Password Is 123456, Just Make It HackMe . The New York Times, January 2010
12. Trusteer Inc. Reused Login Credentials. February 2010
13. Brian Prince. Twitter Details Phishing Attacks Behind Password Reset. eWeek, January 2010
14. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Zhao, "Detecting and characterizing social spam campaigns," in Proc. Internet Meas. Conf. (IMC), 2010
15. Facebook traffic tops google for the week. CNN Money.com, March 2010
16. Swamynathan, G., Wilson, C., Boe, B., Almeroth, K. C., and Zhao, B. Y. Do social networks improve e-commerce: a study on social marketplaces. In Proc. Of SIGCOMM Workshop on Online Social Networks (August 2008)
17. Users of social networking websites face malware and phishing attacks. Symantec.com Blog
18. Verisign: 1.5m facebook accounts for sale in web forum. PC Magazine, April 2010
19. Wilson, C., Boe, B., Sala, A., Puttaswamy, K. P., and Zhao, B. Y. User interactions in social networks and their implications. In Proceedings of the ACM European conference on Computer systems (2009)
20. H. Kim, J. Tang, and R. Anderson, "Social authentication: Harder than it looks," in Proc. Financial Cryptography (FC), 2012
21. Rice, A.: A Continued Commitment to Security. http://blog.facebook.com/ blog.php?post=486790652130 (January 2011)