CERIAS

The Center for Education and Research in Information Assurance and Security

iSONG - Intrusion into Social Network Groups

Shagufta Mehnaz
Department of Computer Science
Purdue University

Elisa Bertino
Department of Computer Science
Purdue University

Introduction

Online Social Networks (OSNs) allow a set of multiple individuals to connect in a group. This groups:

- are sometimes open for all to join,
- and in some cases, have closed community with some special attention.

The second type of groups mentioned above may become the target of intruders.

1

Adversary Model

The primary goal of the intruders is:

- collecting confidential group information,
- or transferring these information to places that are vulnerable to the group's interest.

Also, a significant number of intruders may:

- affect critical discussions or decisions of the group,
- or deviate the group from its original intent.

2

Set-Cover Attack

We introduce a sophisticated intrusion mechanism, the ***'Set-Cover Attack'*** to intrude into a target group.

Motivation:

- The simplest approach for intrusion would be sending friend invitations to all members of the group and then sending group join request. But this untrained approach is too naive to accomplish group membership.
- Different infiltration models, e.g., 3-clique attack concentrates on strongly connected communities. In contrast, our *Set-Cover* approach considers real-life OSN groups where members may not always be connected strongly.

3

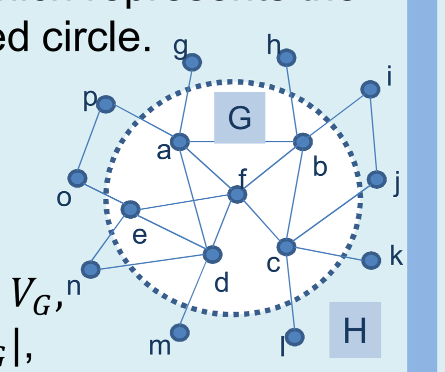
Background

Consider a social network depicted as a simple, undirected graph $H(V_H, E_H)$ where:

- vertices V_H represent the users and
- edges E_H denote friendship connections.

Also, let $G(V_G, E_G)$ be the sub-graph of H, i.e.,$V_G \subseteq V_H$ and $E_G \subseteq E_H$, which represents the target group within the dotted circle.

The number of members in the group = 6.



For each group member $v \in V_G$,

- $n(v) = |u \in V_G: (u, v) \in E_G|$, i.e., the number of v's friends within *G*.

4

Phases of Attack

Phase 1: the intruder targets $C \subseteq V_G$.

- the size of C is determined by threshold ratio p. If p = 0.5, C includes at least the half of the members of the group.
- members in C are strongly targeted.

Phase 2: the intruder targets $V_G - C$.

- members in $V_G - C$ are targeted weekly in comparison to the phase 1.

For the target members of phase 1, the intruder goes into depth two (or even three), i.e., invites the friends of friends of C. And for the targets of phase 2, the intruder only goes into one level of depth, i.e., tries to befriend only the friends of $V_G - C$.

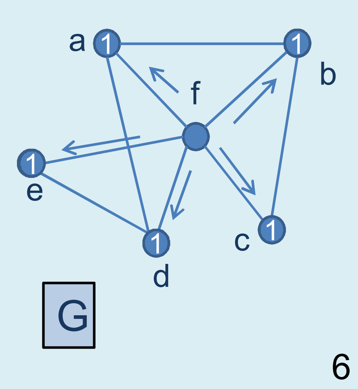
5

Phase 1

We set p = 0.5. So, in phase 1, the intruder will target at least three group members. Thus, $|C| = 3$.

In the first iteration, the attacker wants to ensure at least one mutual friend with each member of the group. So, the attacker calls $getCover(1, G)$ which returns $S = \{f\}$.

Befriending member f ensures that the intruder has one mutual friend with all the group members.



6

Phase 1

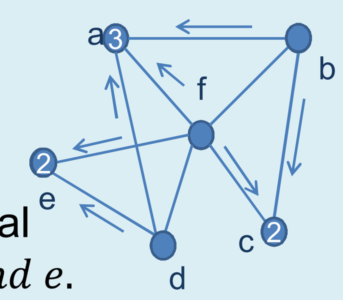
Befriending f:

- invite f's friends of friends
- invite f's friends
- invite f

Current $|C| = 1$, for which $\frac{|C|}{|V_G|}$ is less than p.

The intruder next calls $getCover(2, G)$ to ensure two mutual friends with each group member which returns $S = \{b, d\}$.

Befriending members b and d in the same way as mentioned above, the intruder has at least 2 mutual friends with each of $a, c,$ and e.



7

Phase 2

Current $|C| = 3$, for which $\frac{|C|}{|V_G|} \geq p$.

❖ Phase 1 ends, Phase 2 starts.

In phase 2, the intruder befriends members $a, c,$ and e. The technique of befriending each of them is more relaxed than that of phase 1. For example, to befriend a:

- invite a's friends
- invite a

And after trying to befriend as many group members as possible in phase 1 & 2, finally, the intruder sends the *'group join request'*.

8

Algorithm

Algorithm 1 Intrusion using Set-Cover Attack

- $G' \leftarrow G$, $C \leftarrow \emptyset$, $S \leftarrow \emptyset$, $i \leftarrow 1$ /* phase 1 starts */
- **while** $\frac{|C|}{|V_G|} < \mathrm{p}$
  - $S \leftarrow getCover(i, G')$
  - Sort$(v \in S, n(v))$
  - **foreach** vertex v in S
    - $Fv \leftarrow f(v)$
    - $FFv \leftarrow \bigcup_{j=1}^{|Fv|} f(j)$
    - Send friend invitation to FFv, Fv and v in order
  - **endfor**
  - $C \leftarrow C \bigcup S$
  - $G' \leftarrow G' - S$
  - $i \leftarrow i + 1$
- **endwhile** /* phase 1 ends */
- Sort$(v \in V_{G'}, n(v) \bigcap C)$ /* phase 2 starts */
- **foreach** vertex v in $V_{G'}$
  - $Fv \leftarrow f(v)$
  - Send friend invitation to Fv and v in order
- **endfor**
- sendGroupJoinRequest(G) /* phase 2 ends */

9

Defense

To mitigate such group intrusion attacks, we propose the following tentative solution:

Secret and random trust hierarchy:

- For each group join request, select verifiers from the group members.
- Verifiers highly vary in $n(v)$.
- Verifiers are chosen randomly, e.g., if there are five group members with a high $n(v)$, they are chosen equally likely as verifiers for different group join requests.

Advantages:

- verifiers vary in $n(v)$, so intruder cannot target precisely.
- random verifiers, even if the intruder knows about the hierarchy, he cannot predict.

10

Conclusion

Contributions:

- Proposed a *Set-Cover* based novel infiltration technique to intrude into a target OSN group. The attack works in two phases targeting two subsets of group members to maximize the chance of intrusion and also to minimize the cost of attacks.
- Presented a tentative solution to defend this type of intrusion attacks. Our proposed approach relies on the randomness and confidentiality of the verifiers.

11

References

1. R. Potharaju, B. Carbunar and C. N-Rotaru, "iFriendU: leveraging 3-cliques to enhance infiltration attacks in online social networks," ACM Conference on Computer and Communications Security, pages723-725, 2010.
2. O. Lesser, L. Tenenboim-Chekina, L. Rokach and Y. Elovici, "Intruder or Welcome Friend: Inferring Group Membership in Online Social Networks," SBP, pages 368-376, 2013.

Presenter information:
Shagufta Mehnaz
305 N University St,
West Lafayette, IN 47907
smehnaz@purdue.edu

12

CERIAS

PURDUE UNIVERSITY