AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY

19CSE337 Social Networking and Security

Lecture 26

Topics to Discuss

- Mitigating DDoS Attacks.
- Mitigating Malware Attacks.

Mitigating DDoS Attacks

- An attempt to monopolize a computer resource.
- Hubs in social networks are usually susceptible to DDoS attacks.
- The following solutions may be recommended.
  - Monitoring traffic flow via an AI based system.
  - Only close friends can share posts.
  - Only friends with high reputation score can post in hub’s profile.
  - Hosting services in a cloud based system where resources are shared across multiple servers.

Mitigating Malware Attacks

- Malicious software (Malware) is a program that is specifically designed to gain access, disrupt computer operation, gather sensitive information or damage a computer without the knowledge of computer owner.
- Maximum coverage algorithm is one of the proposed solution against malware attacks via OSN.
- The algorithm picks a subset of legitimate users and to which defense system attaches decoy friends to monitor entire social graph.
- When the decoy friends receive an evidence of malware propagation, the system performs local and network correlations to distinguish actual malware evidence.

Compromised Accounts

- Attacker gets access to an OSN account and behaves just like a legitimate user.
- ML based learning models are needed to compare the behaviour of user before and after attack.
- The possible features considered are text message format, type of posts shared, likes and dislikes, newly added friends, user login or activity hours, location of operation etc.

General Guidelines

- Use strong passwords.
- Limit location sharing.
- Selective with friend requests.
- Careful about sharing or retweeting.
- Aware of links and third party applications.
- Install and regularly update internet security software.
- Report users.
- Privacy settings: hide personal information.
- Multi-factor authentication.

Thanks……