Toward Worm Detection in Online Social Networks

Wei Xu, Fangfang Zhang and Sencun Zhu

Introduction & Motivation

- Online Social Networking (OSN) Websites
  - Popularity: Facebook (>400M users) MySpace (>70M)
  - Attractive targets for worm
- Characteristics of OSNs
  - Small average shortest path length
  - High clustering
  - Scale-free networks

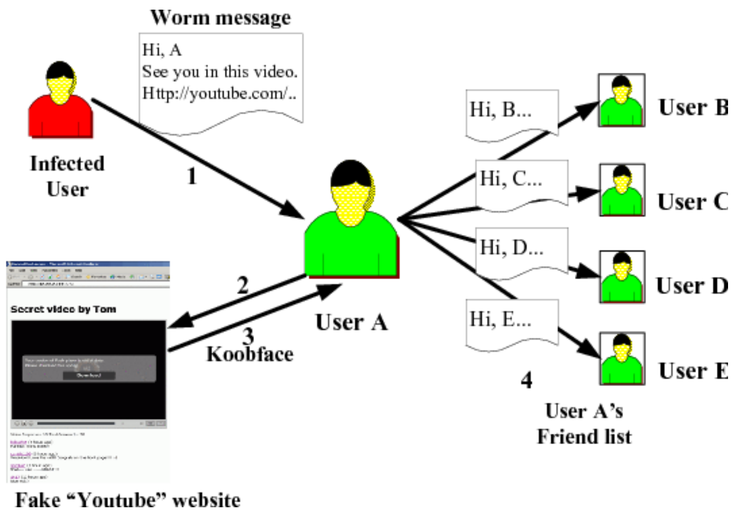

Fig. 1: Koobface Worm Infection Cycle

- OSN Worms
  - Fast-spreading
  - Exploiting features of OSN websites (e.g., messaging)
  - Follow social connections of infected users
- Goal
  - An early warning OSN worm detection system

System Design

- System Overview
  - A honeypot-like surveillance network in OSNs
  - A two-level correlation scheme to minimize detection error

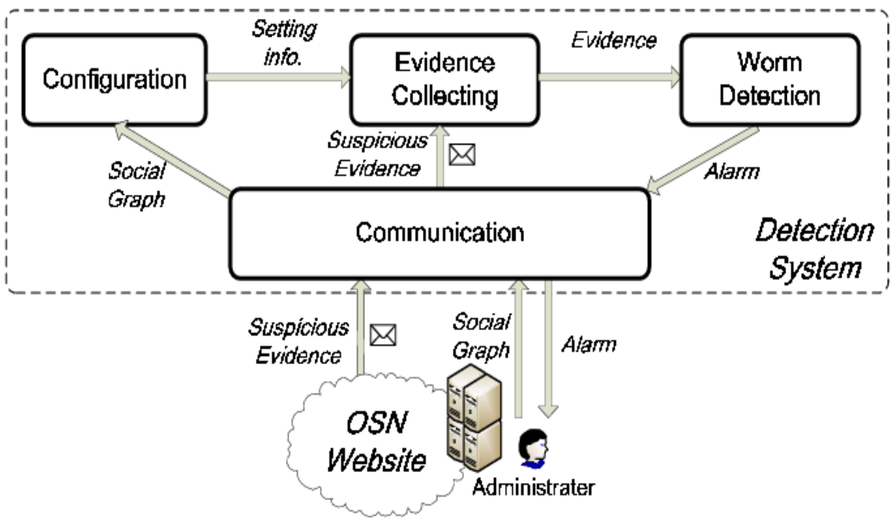

Fig. 2: Worm Detection System Overview

- Configuration Module
  - Select as few as possible normal user accounts to deploy decoy friends
  - Leverage topological properties of OSNs
- Evidence Collecting Module
  - Passively collect worm propagation evidence (E.g., worm messages, worm updates)
- Worm Detection Module
  - Two-level spatial-correlation detection
  - Local correlation
  - Network correlation
- Communication Module
  - Communicate with OSN administrators

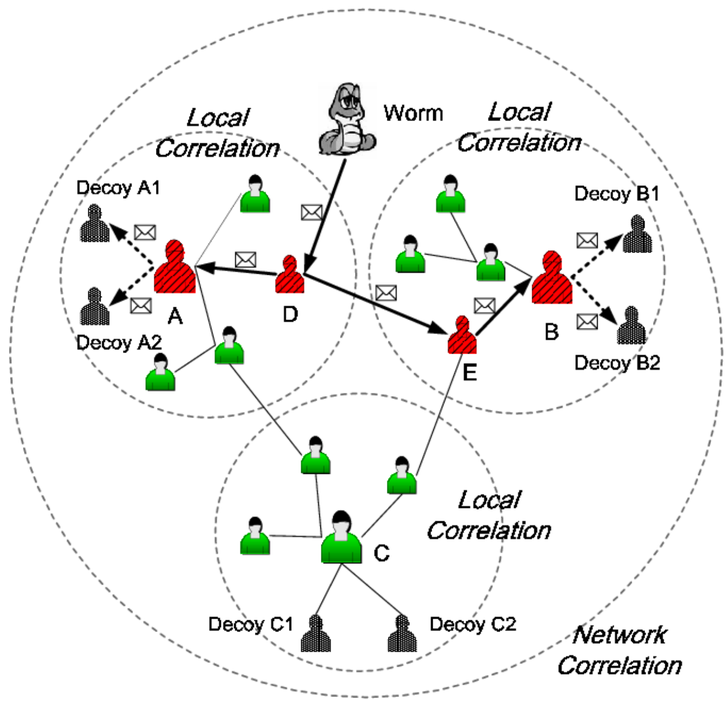

Fig. 3: An Example of Two Level Correlation

Evaluation on Flickr Dataset

- Early Warning Detection

Worm	Avg. Infection #	Max Infection #	Min Infection #
Koobface	700	1851	2.75
Mikeyy	1023	2420	2.8

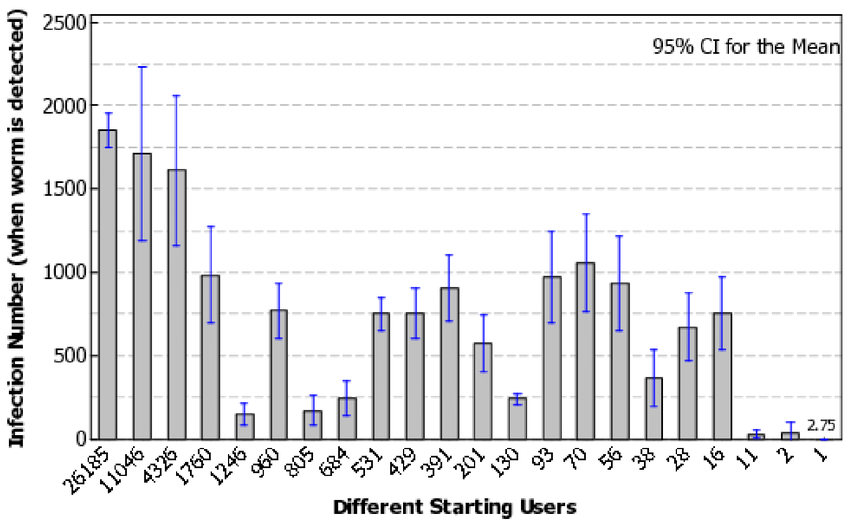

Fig. 4: Worm Infection Number versus Different Initial Infected User Accounts (Koobface worm case)

- Impact of Selected User Set Size

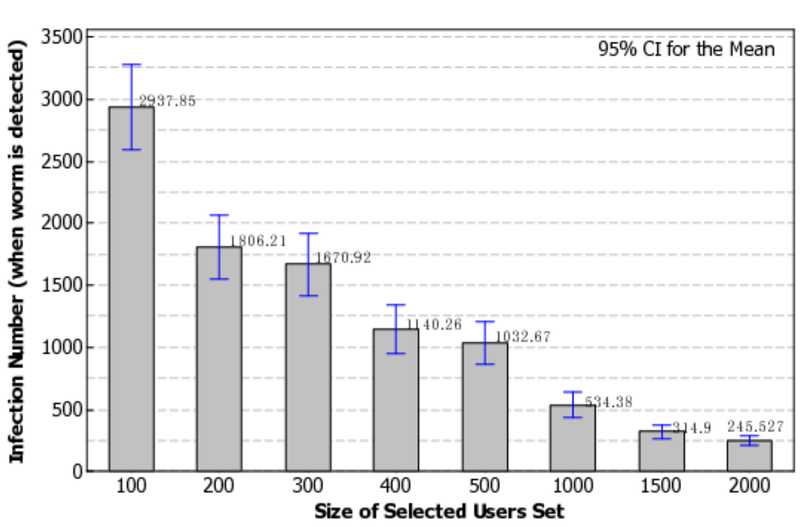

Fig. 5: Worm Infection Number versus the Size of Selected Users Set

- Containment Measures

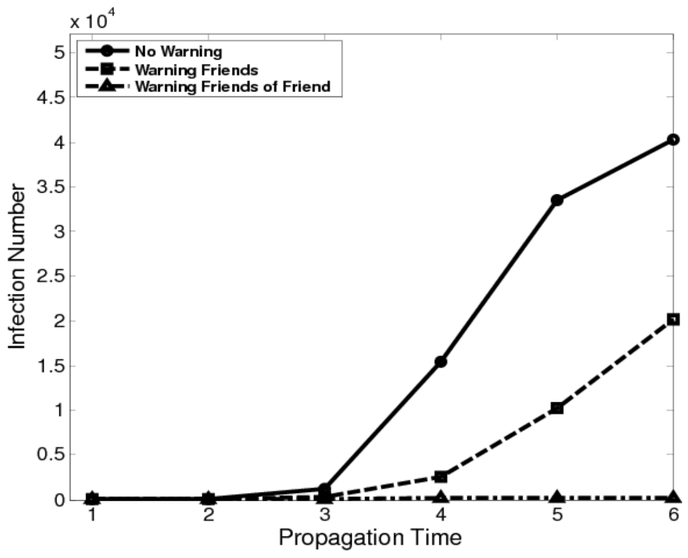

Fig. 6: Worm Infection versus Different Containment Measures

[1]. "Toward Worm Detection in Online Social Networks" To appear in Proceedings of 25th Annual Computer Security Applications Conference (ACSAC), 2010

More information is available: http://www.cse.psu.edu/~szhu/