WORM 2005, Fairfax, Virginia - Nov 11, 2005

On Instant Messaging Worms, Analysis and Countermeasures

Mohammad Mannan and Paul C. van Oorschot

Digital Security Group

Carleton University, Canada

Overview

- Review Instant Messaging (IM) worms
- Analyze known countermeasures for IM worms
  - Present two simple variations of current techniques
- **Raise awareness of IM worms**

Definition of IM worms

- **Worm**: Malicious code that propagates over a network, with or *without* human assistance [Kienzle & Elder, 2003]
- **IM worms**: Worms that spread in IM networks, by exploiting features or vulnerabilities of IM clients and protocols

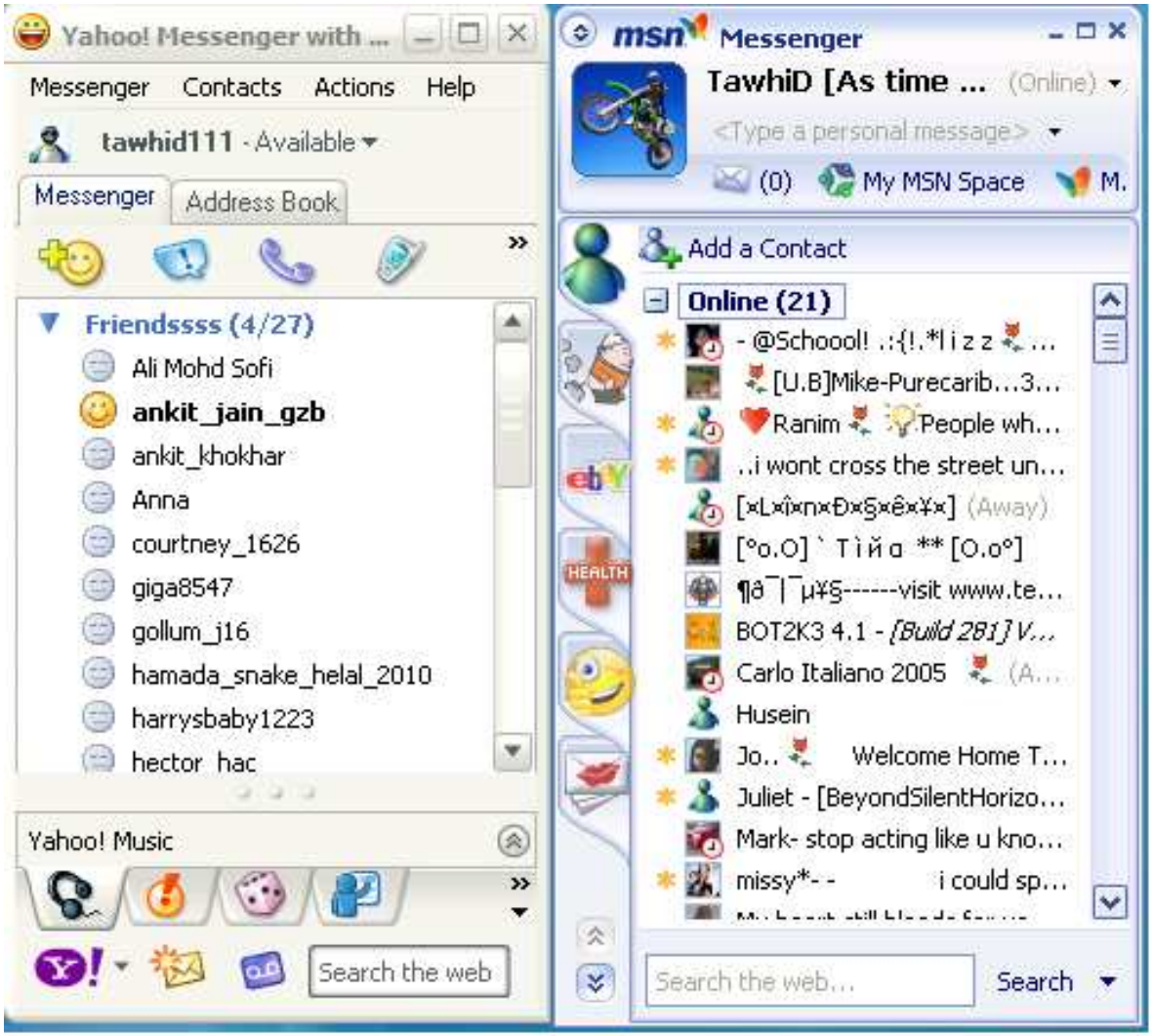
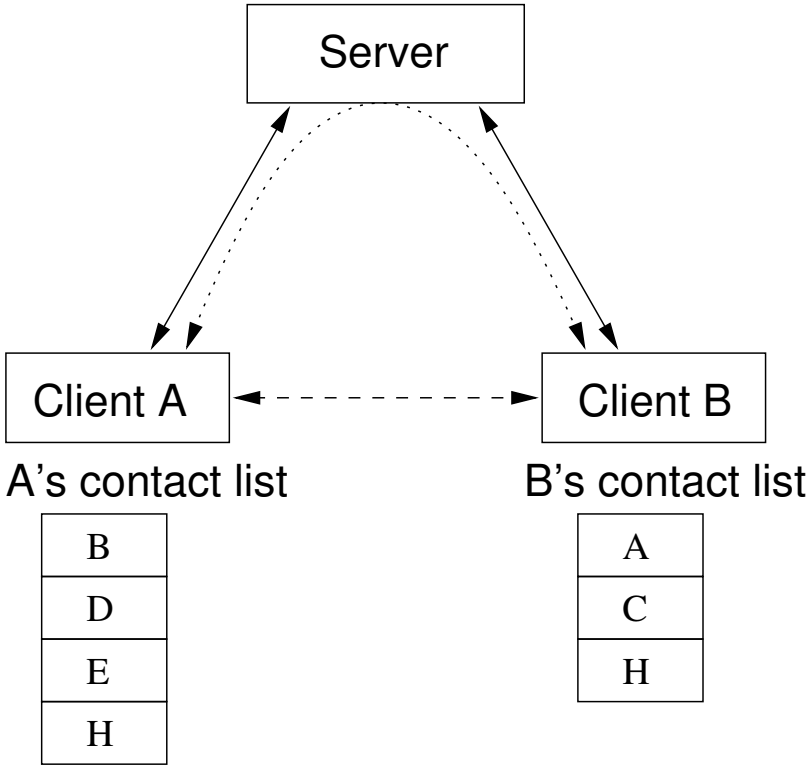


Figure 1: IM in action

IM communication model



Client–Server Communications (e.g. login, profile)

Client–Client Direct Communications (e.g. file data transfer)

Client–Client Server–mediated Communications (e.g. text message)

IM worms: why do we need to worry?

- IM is a popular application
  - instant **communication** (home users)
  - instant **collaboration** (enterprise users)
- Number of users (in millions): **MSN 185, Yahoo! 82, AOL 61**[a]
- Number of IM worms
  - 2004: 1 new IM worm per month
  - 2005: **28** new IM worms per month
- **13 of Fortune 50** companies were affected by IM-related security incidents in the last 6 months[b]

[a] Source: ComScore Media Metrix, Aug. 2005

[b] Source: IMlogic, Nov. 2005

“I don’t use IM. Why should I care?”

- The user base is **big enough** to impact the whole network
- You may use it **without knowing!** (integrated IM in popular applications)
  - Microsoft Outlook Express
  - Microsoft Live Communication Server

What makes IM networks different?

- IM and scanning worms

  1. Scanning worm's connection attempt to a target may fail
     - IM worms have **free** hit-list (contact list)
  2. Spread of IM worms may be latency-limited
     - Some scanning worms are **bandwidth-limited**

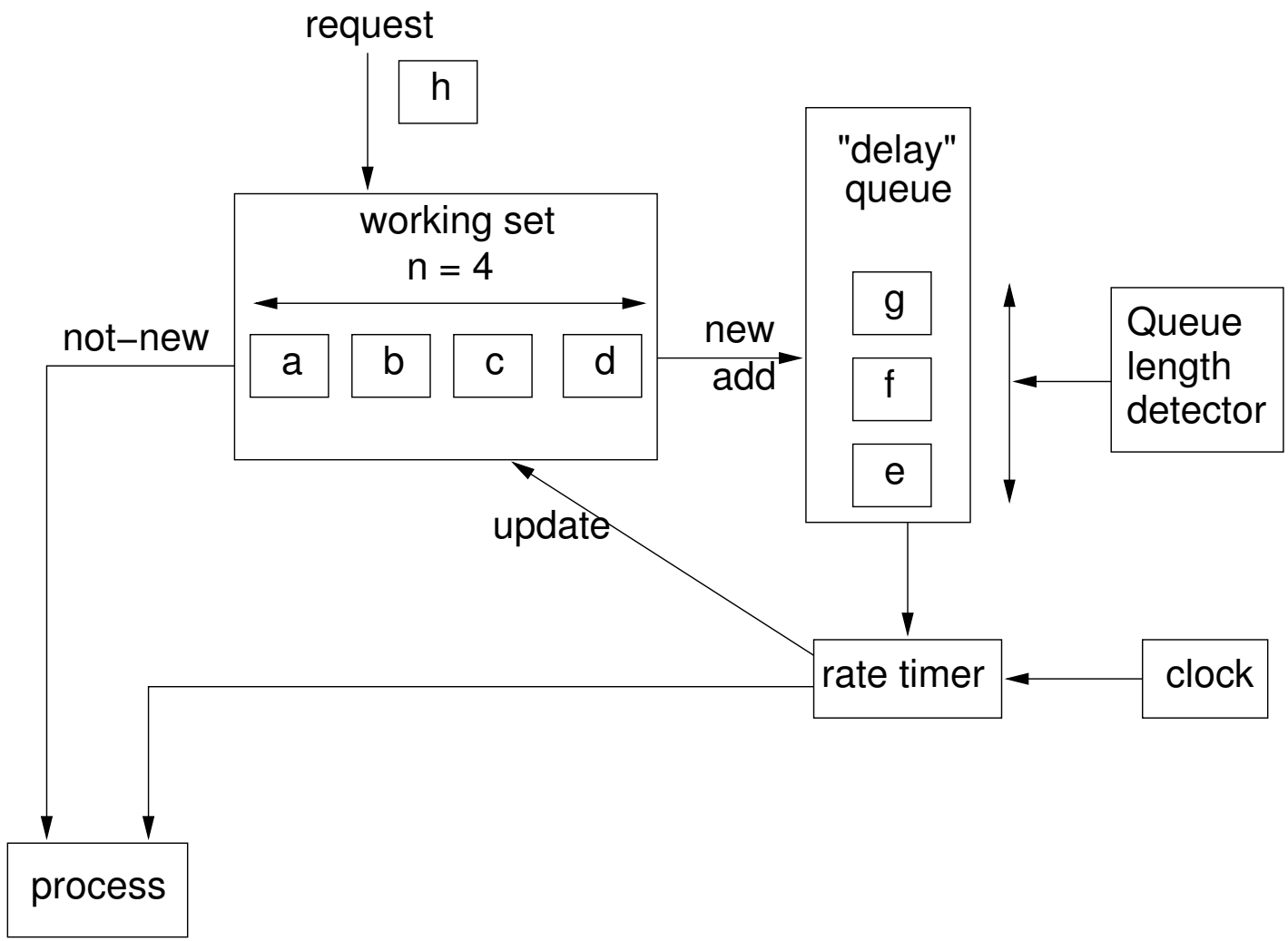
- IM and Email worms

  1. IM worms have access to an **online** hit-list
  2. IM worms can expect instant **user-action**

Existing techniques to restrict IM worms

1. Temporary server shutdown [Hindocha & Chien, 2003]
   – Unrealistic?
2. Temporarily disabling the most-connected users [Smith, 2002]
   – Disabling the top 10% connected users still would leave 90% of the remaining network connected
3. Virus throttling for IM [Williamson & Parry, 2004]
   – See the next slide

Virus throttling for IM – the mechanism



Virus throttling for IM – shortcomings

1. One new contact/day may be **too restrictive**
2. Instant messages may get delayed
3. Test data set is small – only 710 users and 2.5 messages/user/day
4. Group chat is not handled
5. Worm may **‘learn’** a user’s working set

Two simple proposals – motivation

- File transfer and URL messages are the most common propagation mechanisms
  - Neither is expected to be instant (but quick nonetheless)
- File transfer and URL messages are much less frequently used than normal text messages[a]
  - File transfer/user/day: 1.84
  - Text message/user/day: 334.03
- Idea: restrict file transfer and URL messages

[a] Data collected from Eyeball Networks, 2001 - 2005, on avg. 7459 online users

Two simple proposals – mechanisms

➠ Use these independently or in combination:

1. **Throttle** file transfer requests and URL messages
2. **Challenge** senders of a file transfer request or URL message with a CAPTCHA
   - Some users send more files than others – use secure cookies [cf. Pinkas & Sander, 2002]
   - Challenges may come from the server or recipient client

Comparing virus throttling to new proposals

- Throttling minimizes the number of IM worm connections – a worm can establish a **certain number of connections unchecked**
- New proposals restrict only file transfers and URL messages, not IM connections (e.g. for text messages) – intention is better **usability**

Concluding remarks

- IM security proposals must consider usability
  - IM users are mostly **‘casual’**
  - IM messages are expected to be **‘instant’**
- Early CAPTCHAs have been broken [Mori & Malik, 2003]
  - Arms race
- New proposals presented are **preliminary** (not implemented)