Chapter 15
Instant Messaging Security

Zhijun Liu
The Ohio State University, USA

Guoqiang Shu
The Ohio State University, USA

David Lee
The Ohio State University, USA

ABSTRACT

Instant Messaging (IM), a popular communication system, is inevitably exposed to security attacks. With its commercial and government applications, its secure and reliable service becomes indispensable.

In this chapter, we introduce IM system and its security with an emphasis on the most damaging threats of IM spam and worm. Due to the real-time nature of IM services, the existing Internet and e-mail spam and worm defense techniques are not directly applicable to IM systems; new and effective methods are urgently needed for coping with IM network security problems.

After a review of the existing IM spam and worm defense approaches, we present our solutions for filtering IM spam and controlling IM worm, including smart worm. Based on the characteristics of IM system architecture and services, as well as worm spread patterns, we propose an analytical model with statistical branching process and provide a detailed analysis. As a result, we design new and effective defense procedures, including topology based tracing and quarantine and topology-aware throttling.

"Introduction" contains an introduction to IM system and its security threats along with a survey of various defense methods. "Instant Messaging Spam: SPIM" is on IM spam filtering. "Instant Messaging Worm" presents a mathematical model and analysis of IM worm along with its defense mechanisms.

DOI: 10.4018/978-1-60960-777-7.ch015

INTRODUCTION

Instant Messaging (IM) provides real-time communication services with presence information of the communicating parties – typically end-users (Debbabi & Rahman, 2004; Day et al., 2000; Day et al., 2002). Started as a simple chatting service, IM has become a popular communication mechanism that allows users to chat anywhere from desktop to cell phone and handheld device.

Due to its simplicity and convenience users are enjoying online chatting with different kinds of IM tools (Grinter & Palen, 2002). Popular IM systems, such as Internet Relay Chat (IRC), America Online Instant Messenger (AIM), Microsoft MSN Messenger (MSN), ICQ, Yahoo! Instant Messenger (YIM), Jabber, Google Talk, Skype and Tencent QQ, have changed the way we communicate with friends, acquaintances and business associates. Social networking providers, such as Facebook, Twitter and Myspace, often offer IM capabilities. IM service has been extended for commercial applications. Companies and government organizations are interested in using IM for communications at work places (Herbsleb et al. 2002; Scupelli et al., 2005). Many companies begin to deploy internal enterprise IM systems as a supplement of traditional E-mail communication systems to take advantage of the convenience and efficiency of IM services. Prevalent business IM systems include Google Talk, Enterprise AIM, Microsoft Office Communications Server, Yahoo Business Messenger, Jabber XCP, MSN, IBM Lotus Sametime (Jabber), and Cisco Webex Connect (Jabber).

However, as IM is gaining popularity, it is also exposed to severe security threats, which have become a major hurdle for IM to be offered as a secure and reliable communication service. Most prevalent IM systems are designed with scalability rather than security, and, consequently, IM systems are vulnerable to various security attacks, among which IM spam and IM worm are particularly damaging. With its real-time communications IM differs from other Internet applications and most existing security mechanisms, which are designed for other Internet applications such as E-mail, are inadequate for IM. For the public awareness of the threats to IM systems and for secure IM services, it is indispensible to explore existing IM attacks and investigate the corresponding defense techniques.

This chapter introduces the architectures and protocols of IM systems, describes existing threats to IM services, and discusses various defense methods with an emphasis on IM spam and worm. In more details, we discuss new defense procedures against IM spam and worm that we have developed in recent years. For effective filtering of IM spam, we design a new defense method that takes advantage of the unique infrastructure of IM systems and facilitates IM spam filtering at client and server side, as well at various IM gateways. A number of mature spam filtering techniques are also discussed and modified for IM applications. We introduce a statistical branching process for the modeling and analysis of IM worm. Stochastic variables are used for modeling user behaviors, social network knowledge, worm propagation patterns and its impact on defense mechanisms. Based on the analysis, two IM worm defense schemes are developed: 1) Topology based detection and quarantine mechanism that aims at multicast-based worms and that provides real-time worm detection and isolation by constructing the potential infection chaining graph from abnormal network events; and 2) Topology-aware throttling procedure that achieves better usability and worm containment by utilizing the clustering information of IM network topology and that effectively detects and filters worms, including smart worms.

Instant Messaging Systems

As a popular Internet communications service, IM systems enable individuals to exchange text messages and track presence information with each other in real-time. To use IM service, a user usually needs to register and login an IM server