

Permasalahan Keamanan pada Sistem Instant Messaging Peer-to-Peer

PROPOSAL

Felix Kharis Yohendi
132 03 034
k_yohendi@students.ee.itb.ac.id
EC5010 - 2006

Instant Messaging (IM) adalah sistem komunikasi melalui internet yang memungkinkan penggunanya bertukar pesan dan *file* secara nyata-waktu. Berbeda dengan IRC, Instant Messaging dapat juga memantau status online seorang pengguna, karena semua user harus terdaftar pada penyedia layanan terlebih dahulu. Pengguna dapat mengirim pesan dan ketika pesan sampai, pesan akan membuka jendela baru yang akan menarik perhatian penerima. Metoda ini efektif untuk menyampaikan pesan kepada pengguna lain karena instan dan menarik perhatian.

Karena sifat-sifat tersebut IM merupakan alat komunikasi yang penting dan banyak digunakan pada pengguna yang memiliki koneksi internet tanpa batas (24-jam) termasuk pengguna tingkat korporat yang juga memerlukan metoda komunikasi yang cepat dan praktis.

IM dikembangkan tanpa mempermasalahkan aspek keamanan, karena pada awalnya IM ditujukan untuk penggunaan sehari-hari yang tidak memerlukan keamanan tinggi. Kini, dengan semakin beragamnya pengguna IM, dibutuhkan suatu solusi keamanan untuk menjamin Kerahasiaan, Keutuhan, dan Ketersediaan layanan ini. IM sudah memiliki sistem autentikasi pengguna dengan password ke server. Setelah pengguna terautentikasi, penyedia akan memberikan list alamat dan status pengguna lain yang terdapat pada daftar kolega (*buddy list*) pengguna tersebut. Pesan akan dapat dipertukarkan secara peer-to-peer (P2P) atau melalui server (*mediated messaging*). Secara P2P pesan dapat disampaikan lebih aman menggunakan protokol yang sudah ada seperti SSL.

Tulisan ini akan membahas permasalahan keamanan yang dihadapi sistem P2P, khususnya IM antara lain penyebaran *worm*, *trojan*, pembajakan identitas, penyadapan dan pencurian informasi dengan *trojan*. Untuk mengatasi masalah-masalah ini, beberapa metode telah diusulkan, salah satunya dengan metoda Key Exchange.

Bandung, 30 Mei 2006

Sumber:

- CipherTrust IronIM™: Secure Instant Messaging Gateway
- Dan S. Wallach. A Survey of Peer-to-Peer Security Issues
- Mannan, Mohammad & P.C. van Oorschot. Secure Public Instant Messaging: A Survey
- Mannan, Mohammad & P.C. van Oorschot. 2006 . A Protocol for Secure Public Instant Messaging
- Neal Hindocha, Threats to Instant Messaging. Symantec Security Response
- Neal Hindocha. 2003. Instant Insecurity: Security Issues of Instant Messaging
- Stefano Campadello . Peer-to-Peer Security in Mobile Devices: a User Perspective