Detecting Covert Links in Instant Messaging Networks Using Flow Level Log Data

The purpose of this project was to develop a capability to identify the remote party to an Instant messaging (IM) chat session. Online IM networks – such as AIM, MSN messenger, Yahoo! messenger, Skype, IRC, and ICQ – are convenient and popular tools to communicate with other people over the Internet. However, they are also increasingly used by terrorists to communicate over the Internet. Terrorists prefer IM services to traditional communication services such as telephone, fax, and postal mail because of anonymity and non-surveillance.

Following are the project objectives which were achieved;

- Identified with a high degree of certainty a small set of potential collaborators of a suspect. This can give law enforcement agencies a new capability for identifying parties at both ends of an IM session.
- Developed a method that uses the limited information contained in Internet traffic logs (NetFlow logs) maintained by ISPs to reconstruct the social network of IM users.
- Produce a publication in a tier 1 IEEE and ACM conference.
- Developed local expertise of working with large, real-world data sets.
- Collaboration with other universities in Pakistan under the outreach program to mutually enhance and share the expertise and promote the culture of research.
- Developed a prototype application that can be used to demonstrate to potential customers the workability of such a system. Pakistan Internet Exchange (PIE), the FIA's Cybercrime wing, the GHQ, and the ISI have been identified as potential customers for such a system.
- Developed a long term working relationship with Yahoo! Labs that will allow us access to hard-to-get real-world data sets.
- Developed local expertise of working with large, real-world data sets.

As a national impact, the prototype of IM link detector will operate at the national level and will be able to identify pairs/groups of IP addresses on any subnet that are communicating via an IM service. The prototype system will operate out-of-line, as a passive probe on live traffic. Since a certain amount of data will be necessary to make reliable link predictions, this system will be operating and providing information in a near real-time mode.

Technology transfer will be accomplished through two channels, the ministry of defense production has announced its implementation of policy for R&D projects/funds, this policy provides multiple entry points for engagement in the production of defense sector systems. The prototype developed by the funded project will be presented to the DGMP for consideration under this program for pilot production of defense systems. The techniques developed were published as part of this research in tier-1 IEEE/ ACM security and/or networking conferences.