Internet technology has played an increasingly important role in how people interact with each other. People form various virtual communities based on conditions relevant to their personal activities and/or backgrounds, such as their interests, occupations, and locations. People in virtual communities can share information, perform group-oriented tasks, and communicate with each other quickly and efficiently. Community-based internet applications are very useful in many different application domains, especially in social networking. The situations become more complex as corporations began to recognize the importance and power of social computing, and permit their employees to leverage on this newly found “connectivity” as a novel "productivity" tool. Large social networking websites, such as Facebook, LinkedIn, and MySpace provide various software supports for users to interact and manage communities.

However, since users of such applications often reveal a lot of personal and corporate information and frequently exchange data with others who may not be trustworthy, security and privacy in using these community-based applications imposes major challenges for research. These challenges span across many areas, including digital identity management, social networking, privacy-preserving data sharing and integration, and software protection against malware.

This panel will address the critical and fast-emerging challenges for security and privacy in community-based internet applications, and discuss potential solutions and future research directions to tackle the identified challenges.