Distributed Group Key Management

Gene Tsudik

University of California, Irvine

<gts@ics.uci.edu>

Abstract

With the growing popularity of collaborative applications, group communication has become increasingly important. Since most group communication takes place over the Internet, security is an issue of major concern. A fundamental security challenge is posed by group key management. Centralized key management methods are not well-suited for any-to-any collaborative and dynamic peer groups, such as MANETs and p2p systems. For this reason, this talk focuses on secure and efficient distributed group key management techniques. We will trace the history of group key management starting with the early 80-s and then go on to more recent research advances in this area.

In more detail, the talk will discuss the development of provably secure and efficient distributed key management techniques, their integration with reliable group communication platforms as well as experiments and experience with resulting systems. We will also address a number of various security models underlying existing group key management and outline some directions for future research on this topic.