IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB10830

Chapter V

Peer-to-Peer Security Issues in Nomadic Networks

Ross Lee Graham
Mid-Sweden University, Sweden

Abstract

The security concerns for a peer-to-peer implementation of nomadic networks are described with special emphasis on taxonomy and on their identification. The underpinning reference question is how to provide a wide scope of secure networking functions in a completely decentralized and unmanaged network (an ad hoc mobile nomadic network). Though many of the identified security concerns apply to any overlay network, the complete selection of concerns is based on their possible importance in an implementation such as the AmIGo Project collaboration for a ubiquitous nomadic network.

Introduction

For personal devices and ubiquitous interfaces, the problem to solve is how to provide a wide scope of secure networking functions in a completely decentralized and unmanaged network (an ad hoc mobile nomadic network).

There are two available network technology modes that address this problem; wireless Internet access (WAP, Bluetooth, wireless data, etc.) and wireless broadband access (LMDS, MMDS) (Barkai, 2001).

Peer-to-peer implementations are based on having every node treated as an access point (AP). The Internet access mode is typically based on an IP network. The broadband access mode is based on mobile radio networks. Both systems have similar structures in their routing algorithms.

The routing architecture is a central module within the unmanaged networks. The routing algorithms find paths on a dynamic topology. These routing architectures open new vulnerabilities to security (see below).

Both networks show similarities in their routing principles. These algorithms adapt to the dynamic self-organization characteristics that these networks exhibit (Barkai, 2001).

The Motivation for Peered Networks

If we look at the design of the Internet, the essentials of its first form were anticipated for the U.S. Department of Defense (DOD) in 1964, by Paul Baran at Rand Corporation. This preparatory work identified the general specifications and proposed solutions for the main concerns of the DOD. Lawrence G. Roberts from MIT was the main architect for ARPANET (Advanced Research Projects Agency Network). However, he states directly that the Rand work (including Baran) had no significant impact on the ARPANET plans and Internet history. Even so, Roberts admits to reading Baran's work and meeting with him (in 1967) prior to designing the overall network, network economic analysis, line optimization, and the selection of computer sites to be connected. Furthermore, ARPANET was consistent with the DOD requirements identified in the Rand work (Baran, 1964; Roberts, 2003).

ARPANET was a DOD project and the DOD had three major concerns: