Katholieke
Universiteit
Leuven

Faculteit
Wetenschappen

IPSEC EXTENSIONS

Franjo MAJSTOR

Thesis submitted for the degree of
Master of Science

2001–2002

Supervisors : Prof. Dr. ir. B. DE DECKER
Prof. ir. C. HUYGENS

Faculteit Wetenschappen

K.U. Leuven
Academic year 2001–2002

Name and first name student: Majstor Franjo

Title:

IPsec Extensions

Dutch translation:

Uitbreidingen voor het IPsec Protocol

ACM Classification: C.2.2
AMS Classification: 68M12

Abstract:

Security of the IP protocol, although already defined through the IPsec framework within IETF (Internet Engineering Task Force) RFC (Request For Comments) standards 2401 till 2412, is still an undergoing research subject. There are multiple communication protocols, which rely on further results of the IPsec protocol development, as well as several areas where the IPsec framework itself requires further research and development. The IKE (Internet Key Exchange) protocol, used by IPsec for peer authentication, secure session key distribution and security policy negotiations, though vital for its flexible deployment, is going through further development to reduce its complexity, while at the same time expected to give additional flexibility for its extensions. This thesis gives an overview of the current state of the IPsec protocol as well as directions in its future development. It focuses on the development of extensions that are needed for a large-scale remote access VPN (Virtual Private Network) and has a practical part in design review and demonstration of specific IKE extension implementations in IOS (Internetworking Operating System) based low-end router platforms from Cisco Systems.

Thesis submitted for the degree of
Master of Science (in Informatics)

Supervisors:	Prof. Dr. ir. B. De Decker Prof. ir. C. Huygens
Reader:	Prof. Dr. ir. F. Piessens
Counsellor:	Prof. Dr. ir. B. De Decker