Lappeenranta University of Technology
Faculty of Technology Management
Degree Program in Information Technology

Master's Thesis

Evgeni Kappinen

Internet Security and GOST Algorithms

Examiners: Professor Heikki Kälviäinen
Instructors: M.S.C. Jorma Levomäki
Professor Heikki Kälviäinen

TIIVISTELMÄ

Lappeenrannan teknillinen yliopisto
Teknistaloudellinen tiedekunta
Tietotekniikan koulutusohjelma

Evgeni Kappinen

Internet Turvallisuus ja GOST Algoritmit

Diplomityö

54 sivua, 5 taulukkoa

Työn tarkastajat: Professori Heikki Kälviäinen
M.S.C. Jorma Levomäki

Hakusanat: Internet Key Exchange, Transport Layer Security, virtuaalinen yksityisverkko, Cryptographic Service Provider, Government Standard
Keywords: Internet Key Exchange, Transport Layer Security, Virtual Private Network Cryptographic Service Provider, Government Standard

Tämä tutkimus keskittyy Venäjän kryptografian standardeihin ja niiden toteutukseen sertifioiduissa tuotteissa. Tässä työssä myös pohditaan menetelmiä, jotka parantavat suorituskykyä. Tutkimus jatkuu turvallisuuspalveluiden toimittajien vertailulla niitten saadun sertifikaattimäärän perusteella. Tämä auttaa arvioimaan Venäjän nykyistä markkinatilannetta. Sen lisäksi työssä kuvataan venäläisten algoritmien integraatiota TLS-, PKI- ja IKEv1-protokolleihin. Tavoitteena on protokollien yhteensopivuus erilaisiin tuotteisiin. Diplomityötä jatketaan tutkimalla IKEv2-protokolan integroinnin vaatimuksia. Lopuksi diplomityössä todetaan, että venäläiset algoritmit ovat turvallisia ja standardisointi auttaa ulkomaisia yrityksiä saamaan tarvittavat sertifikaatit.

ABSTRACT

Lappeenranta University of Technology
Faculty of Technology Management
Degree Program in Information Technology

Evgeni Kappinen

Internet Security and GOST Algorithms

Master's Thesis

54 pages, 5 tables

Examiners: Professor Heikki Kälviäinen
M.S.C. Jorma Levomäki

Keywords: Internet Key Exchange, Transport Layer Security, Virtual Private Network
Cryptographic Service Provider, Government Standard

This study focuses on the Russian cryptographic standards and their implementation by the certified cryptographic products. In addition, this work describes the techniques for improving performance. The research continues with the comparison of security vendors on the amount of received certificates. It will inevitably help to evaluate the current market situation in Russia. The paper also describes integration work of integration Russian algorithms with the TLS, PKI and IKEv1 protocols. The goal is to achieve compatibility with other products. The thesis continues by investigating some of the requirements for integrating of the Russian algorithms to the IKEv2 protocol. Finally, the thesis concludes by claiming that Russian algorithms are secure to use and that the standardisation will help foreign companies pass the required certifications.