Abstract

Topic: Research on the implementation of virtual cryptographic network interfaces in the Linux OS kernel.

Purpose: The purpose of the work is to study the mechanisms of the Linux operating system family kernel with the aim of the subsequent implementation of virtual network interfaces based on cryptographic protocols described in state standards (GOST).

Tasks:

- research of methods for implementing virtual network interfaces in the Linux kernel;
- analysis of the kernel cryptographic subsystem "`Crypto API`" regarding the possibility of embedding cryptographic protocols described in GOST;
- study of existing virtual network interfaces;
- selection of an optimal set of cryptographic protocols;
- development and testing of a virtual crypto-interface prototype.

Results: While carrying out the research the author decided to use `WireGuard` as a basis for embedding cryptographic protocols described in GOST. A set of basic cryptographic primitives was successfully developed in the form of Loadable Kernel Modules (`LKM`) using the `Crypto API`. Based on the `WireGuard` architecture, the `WireGost` module was developed using domestic cryptographic algorithms.

Testing showed that `WireGost` is capable of operating at speeds up to **900 Mbps**. This confirms the advantage of in-kernel implementation over user-space solutions; nevertheless, it yields to the original `WireGuard`. The slowest part of the system proved to be the "Kuznyechik" block cipher, which, compared to "`ChaCha20`" used in the original protocol, is much more expensive in terms of computational complexity.

Recommendations: To improve the performance of the developed solution and bring its metrics closer to the physical link speed, it is recommended to revise the implementation methods of the "Kuznyechik" block cipher in the form of loadable kernel modules, as well as to ensure more efficient support for basic mathematical operations used in GOST.