УДК 004.056.5

Стебельський М. – ст. гр. СБс-33, Букатка С. – ст. гр. СБс-32
Тернопільський національний технічний університет імені Івана Пулюя

ЗАГАЛЬНОСИСТЕМНІ КРИПТОГРАФІЧНІ ПОЛІТИКИ ОС LINUX. ПОРІВНЯЛЬНИЙ АНАЛІЗ

Науковий керівник: Тимощук Д. І.

Stebelskyi M. Bukatka S.
Ternopil Ivan Puluj National Technical University

SYSTEM-WIDE CRYPTOGRAPHIC POLICIES OF LINUX OPERATING SYSTEMS. COMPARATIVE ANALYSIS

Supervisor: D. Tymoshchuk

Ключові слова: криптографічні політики, ядро, алгоритм, Linux.
Keywords: cryptographic policies, core, algorithm, Linux.

Загальносистемні криптографічні політики – важливий компонент системи, який налаштовує основні криптографічні підсистеми, що охоплюють протоколи TLS, IPsec, SSH, DNSsec, Kerberos та інші. Ці політики відносяться до системи захисту даних на ОС Linux, яка відома своїм високим рівнем захищеності, що в основному забезпечується за допомогою різних криптографічних методів. Адміністратор може обирати набір необхідних політик з певного пакету, а програми та сервіси змушені використовувати їх та відкидати будь-які інші протоколи, які не узгоджуються з встановленою політикою. Програми, які не відповідають вимогам встановленої політики можуть використовувати її лише тоді, коли їм це явно дозволено.

Однією з найважливіших складових загальносистемних криптографічних політик в ОС Linux є криптографічний модуль ядра Linux, який забезпечує реалізацію обраних політик та підтримку необхідних алгоритмів і протоколів на рівні ядра. Крім того, криптографічне ядро забезпечує інтеграцію із засобами керування ключами та сертифікатами, такими як OpenSSl, GnuTLS, NSS та інші.

В ОС Linux є ряд політик, які широко застосовуються для регулювання криптографічних алгоритмів з метою забезпечення безпеки даних. Це такі політики, як: Default, Legacy, Future та FIPS.

Стандартною загальносистемною криптографічною політикою є Default. Дана політика пропонує безпечні налаштування для багатьох загроз, використовуючи криптографічні алгоритми AES, RSA та SHA-2, а також протоколи TLS 1.2 і 1.3, IKEv2 та SSH2. Ключі RSA і параметри Diffie-Hellman також приймаються, якщо вони мають довжину не менше 2048 біт. Ця політика забезпечує хороший рівень безпеки та сумісність із старшими версіями ОС Linux.

У різних версіях ОС Linux можуть використовуватись різні криптографічні алгоритми, які потребують підтримки для збереження сумісності із старішими додатками або системами і для цього існує політика Legacy. Вона включає в себе застарілі криптографічні алгоритми, такі як MD5 чи SHA-1. Варто зазначити, що ця політика повинна використовуватись лише для сумісності із старими системами, які не можуть працювати з більш сучасними та безпечними криптографічними алгоритмами, адже використання застарілих алгоритмів створює вразливості в системі.

З метою забезпечення більш високого рівня безпеки і відповідності новим стандартам в найближчому майбутньому можна використовувати політику Future.

Однією із основних особливостей цієї політики є відмова від використання менш безпечних криптографічних алгоритмів, таких як TLS 1.0 та 1.1, а також RSA ключів з довжиною менше 2048 біт. В політиці Future використовуються нові криптографічні алгоритми, такі як Elliptic Curve Cryptography (ECC), EdDSA та підтримка SHA-3. Встановлюються суворіші параметри безпеки, наприклад, використання більш довгих ключів і сертифікатів, що забезпечує більшу стійкість до атак і зламів.

Політика FIPS (Federal Information Processing Standard) є стандартною для використання в урядових системах США. В ній використовуються такі алгоритми шифрування, як AES, Triple DES, RSA, DSA, SHA та інші. Метою цієї політики є забезпечення високого рівня безпеки даних в урядових системах, а використані криптографічні алгоритми проходять сертифікацію та валідацію для забезпечення їх відповідності вимогам безпеки, встановленим Національним інститутом стандартів та технологій США.

Основним практичним застосуванням загальносистемних криптографічних політик є забезпечення безпеки інформації, яка передається або зберігається на системах із використанням ОС Linux. Це дозволяє забезпечувати конфіденційність та цілісність інформації від несанкціонованого доступу, модифікації або втрати даних. Дані політики зазвичай використовуються в урядових установах, банках, великих корпораціях та інших організаціях, які працюють із конфіденційною інформацією.

Вибір певної загальносистемної криптографічної політики залежить від різних факторів, які включають в себе переваги та недоліки кожної із політик, конкретні потреби та обмеження в організації, використовуване апаратне та програмне забезпечення, а також рівень загроз. Політика Default підходить для забезпечення більшості вимог, які необхідні для захисту інформації, а такі політики, як Legacy, Future та FIPS мають більш спеціалізований напрямок, як наприклад сумісність із старішими системами, використання новітніх криптографічних алгоритмів чи застосування в сфері урядових організацій.