УДК 681.322

М. В. Васильківський[1]
О. В. Стальченко[1]
В. В. Чуба[1]

ПІДВИЩЕННЯ ФУНКЦІОНАЛЬНОСТІ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

[1] Вінницький національний технічний університет;

Анотація

Розглянута структура об'єкта дослідження - мобільної операційної системи. Розглянуті особливості реалізації мобільних операційних систем на прикладі операційних систем для смарт-карт. У кожній з представлених операційних систем були виділені особливості реалізації. На основі отриманих даних про архітектуру існуючих мобільних систем була побудована модель загроз операційної системи для мобільних систем.

Ключові слова: мобільний пристрій, захист інформації, операційна система, смарт-картка.

Abstract

The structure of the object of study - mobile operating system is considered. Features of implementation of mobile operating systems on the example of smart card operating systems are considered. Implementation features were highlighted in each operating system presented. Based on the data obtained on the architecture of existing mobile systems, a model of operating system threats for mobile systems was constructed.

Keywords: mobile device, protection of information, Operating System, smart card.

Вступ

Більшість практичних завдань забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем вирішується на програмно-апаратному рівні з використанням різнотипних операційних систем (ОС), хоча вбудовані механізми їх функціонування є досить схожими. Вбудовування в ОС механізмів аутентифікації і захисту інформації скорочує терміни і витрати на розробку прикладного програмного забезпечення для мобільних пристроїв різного типу і призначення. Засоби алгоритмічного захисту інформації широко застосовуються на практиці, однак їх вразливою частиною є узгодження параметрів захисного перетворення взаємодіючими в ході інформаційного обміну користувачами. Для перехоплення цих параметрів зловмисник може застосовувати примусові атаки, тобто засоби підкупу і спеціальні засоби впливу на користувача. Для захисту користувачів від примусових атак запропоновано застосування псевдовипадкового захисного перетворення. Інтеграція псевдовипадкового захисного перетворення в підсистему захисту інформації універсальної ОС забезпечить користувачеві системи більш високий рівень захисту від примусових атак [1, 2].

Дана робота присвячена вирішенню актуальних наукових і практичних проблем: розширення функціональності засобів захисту інформації, забезпечення переносимості програмних засобів захисту інформації на різні типи мобільних пристроїв (на різні типи технічних платформ) і вбудовування механізмів захисту від атак з примусом.

Мета даної роботи полягає в скороченні термінів і зменшення витрат по розробці захищених мобільних інформаційних технологій за рахунок розширення функціональності та забезпечення переносимості програмних засобів захисту інформації на різні типи мобільних пристроїв (на різні типи технічних платформ) і вбудовування механізмів захисту від атак з примусом.

Результати дослідження

Велика кількість елементів, які взаємодіють один з одним, в процесі роботи операційної системи (частини ядра, системні служби, драйвера апаратних пристроїв і прикладні процеси), роблять операційну систему ідеальним об'єктом для дослідження методів захисту інформації. Основне завдання – виділити найбільш актуальні для мобільної операційної системи загрози інформаційній безпеці. Були розглянуті особливості реалізації мобільних операційних систем на прикладі операційних систем для смарт-карт. Кожна з представлених операційних систем має в собі особливості

реалізації. Основною функцією операційної системи для смарт-карт є забезпечення функціонування протоколів роботи з картою, які описані в стандарті ISO / IEC 7816. Дані протоколи взаємодіють з криптографічними контейнерами, які можуть зберігатися як у внутрішній (захищеній) пам'яті мікроконтролера, так і на зовнішньому сховищі даних. Для реалізації захищеного сховища криптографічних контейнерів виробники смарт-карт застосовують два основних підходи: реалізація смарт-карти на основі спеціалізованого мікроконтролера; використання універсального мікроконтролера спільно з додатковими заходами захисту. Обидва вищевказаних підходи мають свої позитивні і негативні якості. У першому випадку виробник застосовує спеціалізовані мікроконтролери, які мають у своїй архітектурі захищене сховище даних. Негативною стороною використання спеціалізованих контролерів є прив'язка операційної системи до однієї конкретної апаратної платформи, що виконує функції пристрою залежними від апаратної платформи [1].

Для реалізації захищеного сховища на базі універсального контролера необхідно застосовувати додаткові методи захисту даних. Це обумовлено тим, що універсальні контролери націлені на велике коло пристроїв і мають в своєму складі засоби діагностики і налагодження. Нерідко універсальні мікроконтролери мають у своєму складі і блоки захисту даних. Але, на жаль, такі засоби захисту зазвичай мають обмежений функціонал. Зазвичай вони мають тільки механізми дискреційного розмежування доступу в обмеженому виконанні. Для даних в універсальних контролерів застосовують захищені віртуальні файлові системи. Дані в пам'яті зберігаються в зашифрованому вигляді. Механізми доступу до пам'яті також мають важливе значення [2].

В ході роботи над моделлю загроз мобільної операційної системи були виділені актуальні загрози мобільній операційній системі. Загрози згруповані в класи. Відповідно до даних класів загроз буде проводитися подальша розробка структури системи захисту мобільної операційної системи.

Операційні системи успішно застосовуються в засобах захисту інформації. Багато класів засобів захисту на апаратному рівні мають досить схожу будову. Застосування універсальної операційної системи в системах захисту інформації дозволить уніфікувати підходи до забезпечення безпеки при розробці таких систем. Це значно знизить витрати при розробці засобів захисту інформації і відповідно зробить такі продукти більш конкурентоздатною.

Висновки

Виконано дослідження особливостей скорочення термінів і зменшення витрат по розробці мобільних інформаційних технологій. Для досягнення цієї мети вирішується загальна науково-технічна задача розширення функціональності засобів захисту інформації, забезпечення переносимості програмних засобів захисту інформації на різні типи мобільних пристроїв (на різні типи технічних платформ) і вбудовування механізмів захисту від атак з примусом.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Березин А.Н., Молдовян А.А., Молдовян Н.А. Потоковое отрицаемое шифрование, вычислительно неотличимое от вероятностного шифрования // Международная конференция по мягким вычислениям и измерениям. 2015. С. 95-97.

2. Ли И.В., Балса А.Р. Современные подходы к разработке операционных систем для масштабируемых многоядерных систем // Информационные технологии и системы: управление, экономика, транспорт, право, No. 1, 2014. С. 6-14.

Васильківський Микола Володимирович — канд. техн. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет

Стальченко Олександр Володимирович — канд. техн. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет

Чуба Валерій Валерійович — студент групи ТТК-18м, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, Вінниця.

Vasylkivskiy Mykola V. — Cand. Sc. (Eng), Assistant Professor of Telecommunication systems and television, Vinnytsia National Technical University, Vinnytsia

Stalchenko Oleksandr V. — Cand. Sc. (Eng), Assistant Professor of Telecommunication systems and television, Vinnytsia National Technical University, Vinnytsia

Chuba Valeriy V. — Department of Infocommunications, radio electronics and nanosystems, Vinnytsia National Technical University, Vinnytsia