УДК 004.056

Д. О. Каракута
А. В. Остапенко-Боженова

ПАРАМЕТРИ БЕЗПЕКИ ОС WINDOWS 10 MOBILE

Вінницький національний технічний університет;

Анотація

Досліджено безпеку мобільної операційної системи Windows 10 Mobile. Дана ОС забезпечує безпеку персональних і корпоративних пристроїв для захисту від несанкціонованого доступу, витоку даних і шкідливого програмного забезпечення.

Ключові слова: захист, безпека, мобільна ОС, витік даних, шифрування, автентифікація.

Abstract

The security of the Windows 10 Mobile mobile operating system has been studied. This OS provides security for personal and corporate devices to protect against unauthorized access, data leakage and malware

Keywords: protection, security, mobile OS, data leakage, encryption, authentication.

Вступ

Мобільні засоби, в умовах сьогодення, є основним робочим інструментом співробітників компаній. Тому, основною задачею сучасних мобільних операційних систем стає забезпечення захисту від шкідливого програмного забезпечення і крадіжки даних.

Метою роботи є дослідження технологій безпеки операційної системи Windows 10 Mobile [1], які забезпечують біометричну автентифікацію, захист корпоративних даних і конфіденційної інформації, шифрування пристрою на основі технології BitLocker, стійкість до шкідливого ПЗ за допомогою UEFI, Device Guard, AppContainer.

Результати дослідження

Windows Hello [1] – технологія біометричної автентифікації від компанії Microsoft. Перевірка біометричних даних дозволяє запобігти крадіжці облікових даних і спростити вхід користувачів в систему на їх пристроях. Схема автентифікації користувача зображена на рис. 1.

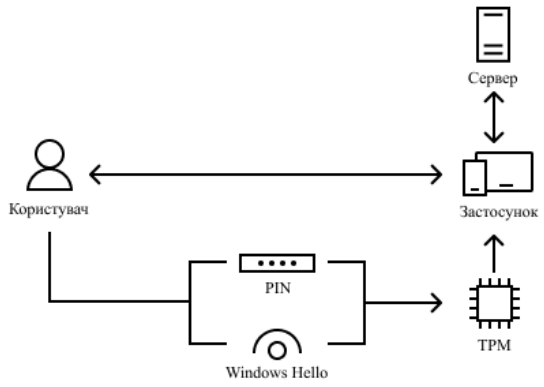

Рис. 1. Схема автентифікації користувача

Windows 10 Mobile включає в себе Windows Information Protection [2] для забезпечення безпеки корпоративних даних і конфіденційності особистої інформації. Модель безпеки Windows 10 Mobile заснована на принципі мінімальних привілеїв. Для цього використовується ізоляція. Кожна програма і навіть частини самої операційної системи запускаються всередині власної ізольованої «пісочниці» під назвою AppContainer. Це безпечний обмежений простір, в межах якого може запускатися додаток і його процеси.

У Windows 10 Mobile використовується система шифрування пристрою на основі технології BitLocker [2] для шифрування всієї внутрішньої пам'яті, включаючи розділи для операційної системи і зберігання даних. Користувач може активувати шифрування пристрою. Пристрій, на якому увімкнено шифрування, допомагає захистити конфіденційність даних, навіть у разі втрати або крадіжки пристрою.

UEFI [3] – це стандартизоване рішення, яке є сучасною заміною для BIOS. Ця технологія забезпечує ті ж функції, що і BIOS, додає деякі функції безпеки та інші розширені можливості. Як і BIOS, UEFI ініціалізує пристрій, а компоненти UEFI з функцією безпечного завантаження перевіряють, що тільки довірене вбудоване ПЗ може виконувати запуск на мобільному телефоні.

Device Guard [3] – це набір компонентів для захисту цілісності апаратного і програмного забезпечення. Застосування модель нульової довіри, виводять безпеку операційної системи Windows на новий рівень. Дана модель передбачає, що кожен користувач або пристрій повинні підтверджувати свої дані кожного разу, коли вони запитують доступ до будь-якого ресурсу всередині або за межами мережі.

10 грудня 2019 року вийшли останні оновлення безпеки для Windows 10 Mobile, оскільки Microsoft відмовилася від подальшої підтримки цієї операційної системи. Однією з причин, за якими Microsoft прийняла таке рішення, стала відсутність інтересу до Windows Phone з боку розробників програмних застосунків. А також компанія втратила значну частину довіри користувачів, коли відмовилася від підтримки Windows Phone 7 з досить розвиненою інфраструктурою. Замість цього Microsoft написала нову версію Windows Phone 8 без зворотної сумісності.

Висновки

Отже, всі розглянуті методи захисту гармонійно вбудовані в операційну систему Windows 10 Mobile. Біометрична автентифікація Windows Hello дозволяє запобігти крадіжці облікових даних і спростити вхід користувачів в систему на їх пристроях. Технологія BitLocker використовується для шифрування всієї внутрішньої пам'яті. Поєднання з технологією Windows Hello і шифрування BitLocker робить задачу отримання зловмиснику конфіденційних даних з пристрою неймовірно складною. Windows Information Protection визначає корпоративні дані і шифрує їх, дозволяючи використовувати їх тільки в межах організації. Поєднання Device Guard і AppContainer допомагає запобігти запуску неавторизованих застосунків. Якщо шкідлива програма проникне в систему, AppContainer дозволить обмежити його і потенційну шкоду.

Власний підхід до проектування ядра і самої системи, оптимізація ОС і прогрмного забезпечення під обмежений список підтримуваних чіпсетів, розміщують ОС Windows 10 Mobile посередині між повністю «закритою» операційною системою Apple iOS і повністю відкритою Google Android.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Функции безопасности в Windows 10 Mobile [Електронний ресурс] : [Веб-сайт]. – Режим доступу: URL : https://www.kv.by/blog/users/vladb/1048860-funkcii-bezopasnosti-v-windows-10-mobile, вільний – Назва з екрана.

2. How to enable device encryption on a phone with Windows 10 Mobile [Електронний ресурс] : [Веб-сайт]. – Режим доступу: URL : https://www.windowscentral.com/how-enable-device-encryption-windows-10-mobile, вільний – Назва з екрана.

3. Windows 10 Enterprise Security: Credential Guard и Device Guard [Електронний ресурс] : [Веб-сайт]. – Режим доступу: URL : https://www.dell.com/support/article/ru-ua/sln304974/windows-10-enterprise-security-credential-guard-%D0%B8-device-guard?lang=ru, вільний – Назва з екрана.

Каракута Денис Олегович — студент групи 1БС-17б, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: d.kyta@gmail.com

Остапенко-Боженова Аліна Василівна — асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: ostapenko-bozhenova_a_v@vntu.edu.ua

Karakuta Denys Olehovych - student of group 1BS-17b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: d.kyta@gmail.com

Ostapenko-Bozhenova Alina Vasylivna - Assistant of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: ostapenko-bozhenova_a_v@vntu.edu.ua