УДК 004.451.9 **Технические науки**

Мешкова Елена Владимировна, *студентка 4 курса электротехнического факультета,*

Пермский национальный исследовательский политехнический университет

ФУНКЦИИ КОНТРОЛЯ УДОСТОВЕРЕНИЙ И ДОСТУПА КАК МЕХАНИЗМ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS 10

Аннотация. В данной статье рассматривается один из механизмов безопасности ОС Windows 10, а именно функции контроля удостоверений и доступа с новыми компонентами Microsoft Passport и Windows Hello.

Ключевые слова: операционная система, Windows, Microsoft Passport, Windows Hello, TMP, пользователь.

Abstract. In this article one of mechanisms of safety of Windows 10, namely function of control of certificates and access with new components of Microsoft Passport and Windows Hello.

Keywords: operation system (OS), Windows, Microsoft Passport, Windows Hello, TMP, user.

В июле 2015 года вышла новая версия операционной системы Windows. Windows 10 предоставляет новые функции и улучшения. Механизмы защиты от известных и возникающих угроз безопасности в данной версии ОС обеспечиваются по большому спектру атак, таких как фишинговые атаки, вирусы и различные виды вредоносного программного обеспечения, поэтому уровень безопасности Windows 10 гораздо выше, чем у ее предшественников.

Так, например, для повышения безопасности ОС был значительно расширен один из механизмов защиты – функции контроля удостоверений и доступа, в который входит идентификация пользователя, проверка подлинности и его авторизация. К ключевым нововведениям в данном механизме безопасности относятся Microsoft Passport, Windows Hello. Рассмотрим возможности работы каждого из них.

Microsoft Passport позволяет выполнять строгую двухфакторную проверку подлинности (2FA) [1]. Двухфакторная система безопасности основана на том, что пользователь, кроме того, что знает пароль доступа к определенному имени пользователя («логину»), – владеет и инструментом для получения соответствующего ему ключа доступа [2]. В качестве такого инструмента может выступать личный телефон пользователя, на который приходит СМС с кодом подтверждения, компьютер, на котором сохранен электронный сертификат безопасности, либо специальное электронное устройство для считывания отпечатка пальца. Технология 2FA заменяет пароли в Windows комбинацией из зарегистрированного устройства и ПИН-кода или Windows Hello. Проверка подлинности проводится с использованием пары ассиметричных ключей.

Microsoft Passport обладает высокой гибкостью. Он предоставляет администраторам и пользователям возможность управлять проверкой подлинности. Microsoft Passport работает с биометрическими датчиками и ПИН-кодами, дает возможность использовать телефон как фактор проверки подлинности на ПК. Учетные данные учетные данные пользователя могут поступать из вашей инфраструктуры открытых ключей [1]. Кроме того, Windows сама может создать учетные данные [1].

Windows Hello является биометрической технологией входа для Microsoft Passport и представляет собой приложение, позволяющее входить на устройства с ОС Windows 10 более персонализированным способом с помощью взгляда или быстрым проведением пальца. Биометрические данные пользователя не хранятся централизованно и не перемещаются между устройствами пользователя.

Приложении поддерживает следующие типы датчиков, установленные на устройстве:

– Специальный электронный датчик для сканирования и распознавания отпечатка пальца. В новой версии Windows усовершенствованы алгоритмы сканирования, распознавания и защиты от получения доступа обманным путем (спуфигнг).

– Инфракрасные камеры, которые используются для распознавания лиц. Такие камеры могут быть, как и внешними, так и внутренними, встроенными на само устройство.

Windows Hello дает возможность использовать более безопасный метод входа в систему на всех устройствах вместо того, чтобы запоминать длинные сложные пароли.

В заключении хочется уделить внимание безопасности учетных данных. Microsoft Passport исключает использование паролей для входа в систему, что снижает риск хищения и использования учетных данных пользователя злоумышленником. Использование пар асимметричных ключей повышает безопасность в том, что учетные данные пользователей не будут похищены в случае нарушения безопасности поставщика удостоверений или веб-сайтов, к которым пользователь осуществляет доступ [1].

Для повышения конфиденциальности в системе используется криптографический ключ TMP 2.0, который шифрует биометрические данные пользователя в недоступной для чтения форме.

С выходом новой версии Windows 10 и появлением в ней новых компонентов Microsoft Passport и Windows Hello злоумышленнику гораздо сложнее нарушить безопасность системы. Так, например, для нарушения безопасности учетных данных пользователя, защищаемых TMP, злоумышленнику необходимо получить доступ к физическому устройству, а также подделать биометрические данные пользователя, что является более сложной процедурой, чем похищение пароля, при условии, что все это необходимо сделать раньше, чем функциональный механизм защиты от взлома TPM заблокирует само устройство.

Библиографический список

1. Microsoft TechNet // Обзор системы безопасности в Windows 10 – [Электронный ресурс]. – URL: https://technet.microsoft.com/ru-ru/library/mt601297(v=vs.85).aspx (дата обращения 24.08.2016)

2. Microsoft TechNet // Основы TMP URL: https://technet.microsoft.com/ru-ru/library/mt601297(v=vs.85).aspx (дата обращения 24.08.2016)

3. Хабрахабр // Двухфакторная аутентификация – [Электронный ресурс]. – URL: https://habrahabr.ru/company/1cloud/blog/277901/ (дата обращения 24.08.2016)