**Ćwiczenia laboratoryjne z przedmiotu Kryptografia i Bezpieczeństwo Danych**

**Temat: Wybrane mechanizmy szyfrowania i ochrony danych w systemie Windows 10 PRO**

**Autor: Sławomir Samolej**

**Wprowadzenie**

1. Częstym sposobem dystrybucji plików jest zamieszczanie ich do pobrania z zastosowaniem przeglądarki, czy usługi ftp. Obok plików publikuje się również ciągi znaków oznaczające ich „skróty”. W prawidłowych rozwiązaniach treść skrótu powinna się znajdować w części serwisu „tylko do pobrania” aby zapobiec możliwości fałszowania pliku i skrótu. Skróty oblicza się przez „przepuszczenie” plików przez algorytm skrótu. Po pobraniu pliku można sprawdzić jego integralność przez ponowne obliczenie funkcji skrótu na lokalnym komputerze i porównania ich wartości z tymi opublikowanymi w Internecie [5].

W Windows 10 można dokonać sprawdzenia skrótu przez wywołanie odpowiednich komend konsoli PowerShell. Przykładowo, polecenie:
**Get-Filehash** ścieżka\_i\_nazwa\_pliku **–Algorithm SHA256**

Oblicza skrót wskazanego pliku z zastosowaniem algorytmu SH256.

Polecenie umożliwia sprawdzenie skrótów plików z zastosowaniem algorytmów: SHA1, SHA256, SHA384, SHA512, MACTripleDES, MD5, RIPEMD160.

Są problemy z wyświetleniem wyniku dla SHA512, jest on „ucinany” na ekranie konsoli.

Jest jeszcze inne polecenie konsoli pokazujące hash, przykładowo:
**CertUtil –hashfile** ścieżka\_i\_nazwa\_pliku **SHA512**
również wyświetla (ale teraz prawidłowo) skrót wskazanego pliku.

Na marginesie, polecenie CertUtil pozwala na znacznie więcej, niż wyświetlenie hash pliku. Jest to jeden z podstawowych programów do zarządzania certyfikatami w systemie

1. System **Windows 10 PRO** umożliwia szyfrowanie plików, czy folderów [3]. Mechanizm ma zabezpieczyć pliki przed kradzieżą na zewnętrzy nośnik. Takie pliki, bez skradzenia również certyfikatu z kluczem do odszyfrowania są trudne do odszyfrowania. Dla użytkownika zaszyfrowanie danego folderu sprowadza się do zmiany jego właściwości w programie Eksplorator Windows. Z punktu widzenia użytkownika pliki w dalszym ciągu można otwierać i modyfikować.

Szyfrowanie wybranego folderu można wykonać przez wybranie sekwencji: (Prawy przycisk na folderze/pliku)->Właściwości->(zakładka ogólne) przycisk Zaawansowane…->(pole wyboru) Szyfruj zawartość, aby zabezpieczyć dane. Jeśli szyfrowany jest folder, to pojawi się pytanie, czy zaszyfrować również wszystkie pliki i foldery zawarte w tym folderze.

Pliki zaszyfrowane można przekazać innej osobie, ale wraz z nimi należy przekazać osobno wygenerowany (i najlepiej osobno przekazany) certyfikat z kluczem umożliwiającym odszyfrowywanie tych plików. Ogólnie, odszyfrowywanie cudzych plików można przeprowadzić w taki sposób, że otrzymany certyfikat instaluje się w swoim systemie, co oznacza, że otrzymaliśmy uprawnienia do odszyfrowywania plików udzielone nam przez właściciela. Zainstalowanie takiego certyfikatu pozwala po prostu kopiowanie takich plików na swój komputer oraz ich otwieranie.

Tworzenie certyfikatu zaczyna się od uruchomienia Panelu sterowania Windows. Należy wybrać odnośnik „Konta użytkowników”, a następnie ponownie odnośnik „Konta użytkowników”. Wtedy po lewej stronie okna będzie widoczny odnośnik „Zarządzaj certyfikatami szyfrowania plików”. Wybranie tego odnośnika uruchamia kreatora certyfikatu, dla którego podaje się nazwę pliku, hasło do odblokowania. Najczęściej taki certyfikat pozwala na odszyfrowywanie wszystkich plików należących do właściciela konta Windows.

Jeśli mamy w komputerze zaszyfrowane w ten sposób pliki lub foldery należy wyeksportować i przechować w bezpiecznym miejscu certyfikat szyfrowania. W przypadku ponownej instalacji systemu tylko dzięki temu certyfikatowi będzie można odszyfrować zaszyfrowane uprzednio pliki.

1. Szyfrowanie całych dysków w systemie Windows 10 można przeprowadzić z zastosowaniem wbudowanego narzędzia BitLocker [2], [1]. Do szyfrowania Narzędzie służy do zabezpieczania danych, zwłaszcza w urządzeniach przenośnych. Zaszyfrowaniu ulega cały dysk, lub (szybciej) cześć dysku zwierająca dane, które chcemy ochronić. Próba odczytu dysku z takiego urządzenia w innym komputerze kończy się zapytaniem o hasło dostępu. Narzędzie może też służyć, np. do szyfrowania napędów przenośnych. Wtedy, odczyt danych na innym urządzeniu, niż macierzyste wymaga podania hasła dostępu.

Podobnie jak w przypadku szyfrowania folderów jest możliwość wyeksportowania kopii zapasowej klucza odzyskiwania dostępu do napędu. Może ona być zapisana w pliku, lub naszym koncie Microsoft. Nie ma ona postaci certyfikatu.

Program BitLocker można zastosować do zaszyfrowania wybranego fragmentu dysku. W przystawce diskmgmt.msc można utworzyć osobny dysk logiczny na bazie wskazanego pliku (Akcja->Utwórz Dysk VHD), w tak utworzonym dysku należy utworzyć nowy wolumin, który od tej pory będzie w systemie widoczny jako osobny dysk. Taki dysk można zaszyfrować. Wadą tego rozwiązania jest konieczność „ręcznego dołączania” takiego dysku za każdym razem do zestawu widocznych woluminów po uruchomieniu komputera.

Przykładowo, dysk przenośny można zaszyfrować w następujący sposób. Po włożeniu dysku do portu USB należy uruchomić „panel sterowania”, a następnie wybrać odnośnik „szyfrowanie dysków funkcją BitLocker”. Jeśli dysk przenośny jest widoczny, to można włączyć dla niego funkcję BitLocker i zaszyfrować albo zawarte na nim dane, albo cały dysk. Przed rozpoczęciem szyfrowania należy wskazać hasło odszyfrowywania lub urządzenie (np. karta chip) gdzie na się znaleźć klucz odblokowujący wolumin.

1. Jeśli w systemie Windows 10 PRO stosowany jest Windows Defender, jako oprogramowanie antywirusowe, to można w jego ustawieniach wskazać tak zwany „kontrolowany dostęp do folderów” [6], [7]. Taki kontrolowany dostęp do folderów pozwala wskazać, które aplikacje mają prawo korzystać z plików zawartych w danym folderze. System Windows chroni w taki sposób już foldery systemowe, ale pozwala na wprowadzenie ochrony na inne foldery.

Zainstalowanie programu od zewnętrznego dostawcy może blokować niektóre funkcje Windows Defender.

1. W celu zabezpieczenia komputera przed niepowołanym kopiowaniem danych na zewnętrzne nośniki danych (dyski przenośne) w systemie Windows 10 można posłużyć się przystawką do zarzadzania o nazwie gpedit.msc [8]. Otwierając drzewo konfiguracji: „Konfiguracja użytkownika-> Szablony administracyjne -> System -> Dostęp do magazynu wymiennego” uzyskujemy między innymi możliwość zablokowania odczytu/zapisu z urządzeń wymiennych. Ta sama przystawka może posłużyć do blokowania użytkownikom dostępu do wiersza poleceń oraz do możliwości uruchamiania wybranych aplikacji.

**Przebieg ćwiczenia**

Założenia: posługujemy się Windows 10 PRO (Dystrybucja Windows 10 Home może nie zawierać omawianych mechanizmów).

Uwaga: Zmieniamy tutaj ustawienia komputera. Warto rozważyć utworzenie jakiegoś ćwiczebnego konta na tymczasem do dokonywania modyfoikacji…

1. W wielu serwisach służących do pobierania plików razem z plikami publikowane są ich skróty. Proszę o pobranie kilku wybranych plików, dla których opublikowane są skróty i sprawdzić, czy po pobraniu ich skróty nie uległy modyfikacji.
2. Dla zachowania bezpieczeństwa Waszych danych ćwiczenie należy wykonać np. na tymczasowo założonym koncie w waszym systemie operacyjnym. Proszę zaszyfrować wybrany plik z danymi na swoim (tymczasowym) koncie oraz wygenerować certyfikat z kluczem szyfrowania do tego konta. Proszę przesłać plik i certyfikat na inne konto Windows 10 PRO i sprawdzić, czy plik można odczytać. Potem proszę zainstalować otrzymany certyfikat i ponownie sprawdzić, czy plik można odczytać. Ćwiczenie można wykonać przez przenoszenie danych pomiędzy różnymi komputerami.
3. Proszę zaszyfrować jedno ze swoich urządzeń przenośnych w taki sposób, żeby dostęp do niego był możliwy z zastosowaniem hasła.
4. Opcjonalnie: Proszę wybrać folder należący do jakiegoś innego konta na tym samym komputerze i zablokować możliwość uruchamiania w nim wybranego programu (np. blokada uruchamiania notatnika dla plików tekstowych w tym folderze)
5. Opcjonalnie: Proszę skonfigurować komputer, aby zwykli użytkownicy nie mogli w nim skorzystać z kopiowania danych na urządzenia przenośne.
6. Opcjonalnie: W pozycji literatury [4] jest zaproponowany gotowy skrypt Windows do zabezpieczania hasłem danego folderu. Proszę sprawdzić działanie skryptu.

**Literatura**

1. (Dokumentacja BitLocker Microsoft) <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview>
2. (Zabezpieczanie dysków z zastosowaniem bitLocker) <https://www.faqforge.com/windows/windows-10/how-to-protect-your-files-on-windows-10-with-bitlocker/>
3. (Windows 10 Pro + szyfrowanie) <https://www.youtube.com/watch?v=NIB3lvy04as&t=281s>
4. (Zabezpieczanie folderów hasłem – skrypt) <https://netbe.pl/blog/jak-zabezpieczyc-folder-haslem-w-windows-10/>
5. (Poradnik, jak sprawdzać skróty w różnych SO) <https://pl.if-koubou.com/articles/how-to/what-are-md5-sha-1-and-sha-256-hashes-and-how-do-i-check-them.html>
6. (Blokowanie dostępu do folderu dla danej aplikacji 1) [https://www.dobreprogramy.pl/Kontrolowany-dostep-do-folderu-wlacz-ochrone-przed-ransomware-w-Windows-10,News,83868.html](https://www.dobreprogramy.pl/Kontrolowany-dostep-do-folderu-wlacz-ochrone-przed-ransomware-w-Windows-10%2CNews%2C83868.html)
7. (Blokowanie dostępu do folderu dla danej aplikacji 1) <https://support.microsoft.com/pl-pl/help/4046851/windows-10-allow-blocked-app-windows-security>
8. (Blokowanie możliwości kopiowania danych na urządzenia zewnętrzne) <https://variatkowo.pl/poradniki/blokujemy-dostep-do-nosnikow-zewnetrznych-w-windows/>