

InCyT Eğitim Modülleri

Çalışanlar için Bilgi Güvenliği

Birim no: (3) 6. Hafta

Birim (Modül) adı: (Gizlilik ve Veri Koruma)

Öğrenme aktiviteleri	☐ Web semineri ☐ Egzersizler ☐ Atölye ☐ Sunum ☐ Diğer
Öğrenme Sorumlusu	- Miroslaw Mazurek - Pawel Dymora
Öğrenme Hedefleri	<i>Etkinliği</i> - Disklerin ve bölümlerin şifrelenmesi - VeraCrypt Aracı nasıl kullanılır
Kazanılacak Beceriler	- TS1 - SS1 - SS2
Öğrenme süresi	<i>faaliyetinin</i> 2 hafta
Öğrenme Gereksinimler	<i>İhtiyaç duyulan şey?</i> - internet girişi - İnternet tarayıcısı - VeraCrypt programı

Modül hakkında kısa bilgi



Tanım

Bu modülün amacı, özel veya kurumsal diskinizdeki verilerin korunması ve verilerin şifrelenmesi ile ilgili bilgi ve pratik beceriler kazanmaktır.

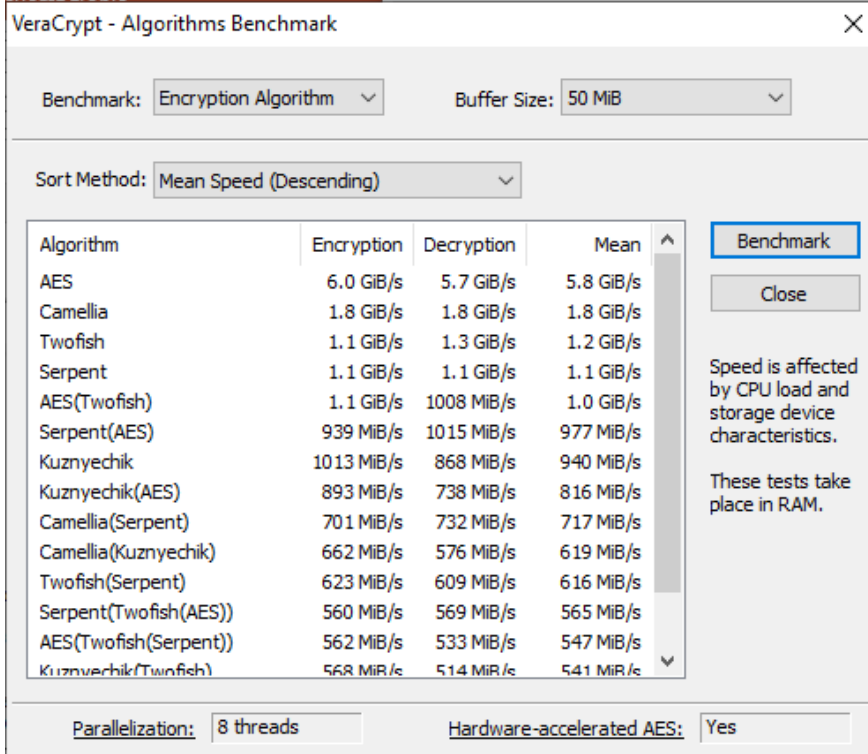
Öğrenme Materyalinin İçeriği

1. Disklerin ve bölümlerin şifrelenmesi. Teorik temeller: çalışma prensibi, şifreleme algoritmaları. Programın kurulması (konfigürasyon, diskin tanımlanması, parametrelerin seçilmesi, anahtarların oluşturulması).

Bilgisayar sistemlerinin güvenliği, yalnızca işletim sisteminin kendisi, uygulamalar gibi kaynakların değil, tüm verilerin çoğunun korunmasını gerektirir. Güvenlik duvarı gibi kaynaklara erişimi engelleyen bilinen güvenlik yöntemleri her zaman etkili değildir. Bu nedenle birden fazla güvenlik yöntemi birbiriyle birleştirilmelidir. Sunulan veri şifreleme yöntemi, bir davetsiz misafirin bilgisayarımıza erişiminden kaynaklanan birçok tehdidin ortadan kaldırılmasını sağlar.

En yaygın kullanılan çözümlerden biri ücretsiz VeraCrypt veri şifreleme yazılımıdır. Yalnızca tüm diskleri veya bölümleri değil, taşınabilir USB diskleri bile şifrelemenize ve belirli bir kapasiteye sahip sanal şifreli diskler oluşturmanıza olanak tanır. VeraCrypt, aşağıdaki algoritmaları kullanarak şifreleme sağlar: AES, Camellia, Kuznyechik , Serpent ve Twofish ; AES- Twofish , AES- Twofish - Serpent, Serpent-AES, Serpent- Twofish -AES, Twofish -Serpent ile çoklu şifrelemenin yanı sıra .

Bilgisayarın yapılandırmasına bağlı olarak, bu algoritmaların her biri için şifreleme ve şifre çözme hızı, Şekil 1'de gösterildiği gibi değişecektir.



VeraCrypt - Algorithms Benchmark

Benchmark: Encryption Algorithm Buffer Size: 50 MiB

Sort Method: Mean Speed (Descending)

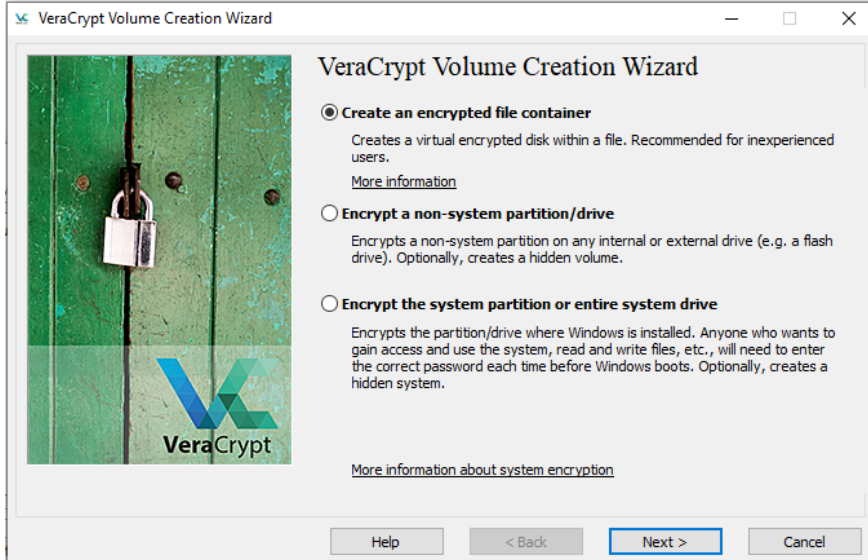
Algorithm	Encryption	Decryption	Mean
AES	6.0 GiB/s	5.7 GiB/s	5.8 GiB/s
Camellia	1.8 GiB/s	1.8 GiB/s	1.8 GiB/s
Twofish	1.1 GiB/s	1.3 GiB/s	1.2 GiB/s
Serpent	1.1 GiB/s	1.1 GiB/s	1.1 GiB/s
AES(Twofish)	1.1 GiB/s	1008 MiB/s	1.0 GiB/s
Serpent(AES)	939 MiB/s	1015 MiB/s	977 MiB/s
Kuznyechik	1013 MiB/s	868 MiB/s	940 MiB/s
Kuznyechik(AES)	893 MiB/s	738 MiB/s	816 MiB/s
Camellia(Serpent)	701 MiB/s	732 MiB/s	717 MiB/s
Camellia(Kuznyechik)	662 MiB/s	576 MiB/s	619 MiB/s
Twofish(Serpent)	623 MiB/s	609 MiB/s	616 MiB/s
Serpent(Twofish(AES))	560 MiB/s	569 MiB/s	565 MiB/s
AES(Twofish(Serpent))	562 MiB/s	533 MiB/s	547 MiB/s
Kuznyechik(Twofish)	568 MiB/s	514 MiB/s	541 MiB/s

Parallelization: 8 threads Hardware-accelerated AES: Yes

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

Şekil 1. Algoritmaların hızını test etme

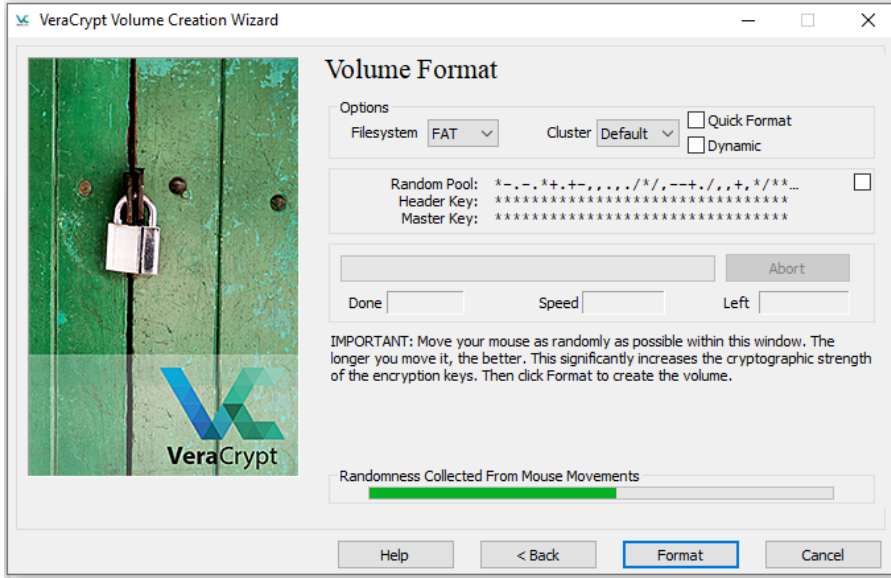
Şifreleme işlemi, birimin oluşturulmasıyla başlar. Tüm diski, bölümü veya herhangi bir birimi şifreleyebilirsiniz (Şekil 2).



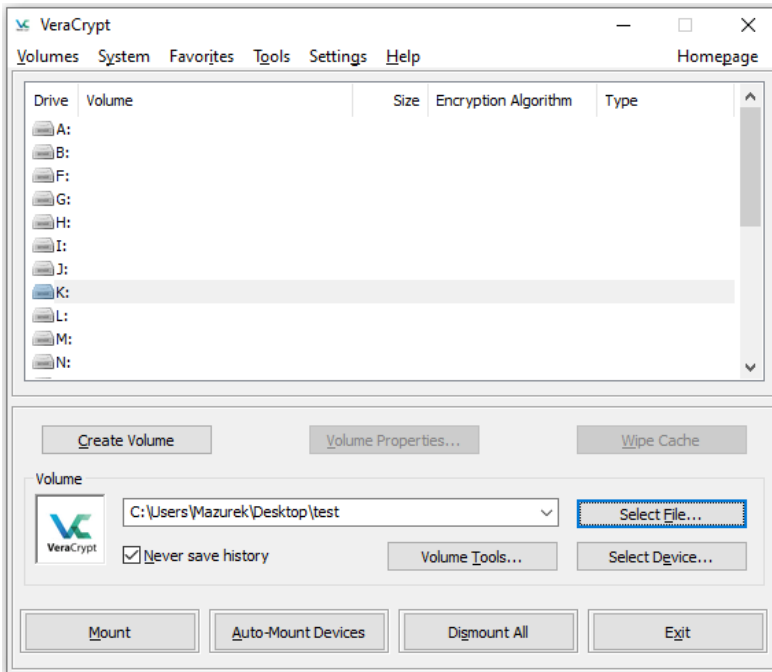
Şekil 2. VeraCrypt birim oluşturma sihirbazının penceresi

Birimin yerini seçtikten sonra ona bir isim vermelisiniz. VeraCrypt birimi, bir sabit diske veya USB sürücüsüne kaydedilebilecek bir dosyaya yerleştirilir. Birim normal bir dosya gibi davranır, yani onu kopyalayabilir, yeniden adlandırabiliriz, vb. Bir sonraki adım, uygun şifreleme algoritmasını,

örneğin AES'yi seçmek ve ilgili kalite kurallarına (uygun uzunluk, büyük ve küçük harfler, sayılar, özel karakterler). Ardından birim biçimlendirilir. Sihirbaz, güvenliğini artırmak için, oluşturulan anahtarların kriptografik kalitesini önemli ölçüde artıran rastgele fare hareketleri oluşturmanızı ister (Şekil 3). Biçimlendirmeden sonra, birim kullanıma hazırdır. Sadece şifre girilerek bağlanması gerekir (Şekil 4).



Şekil 3. VeraCrypt birimlerini biçimlendirme süreci



Şekil 4. VeraCrypt birimleri bağlantı penceresi

Yüksek seviyede koruma istediğimiz ve şifreleme süresini önemsemediğimiz durumlarda çoklu şifreleme seçilmelidir. Aynı anda farklı algoritmalar ile farklı kapasitelerdeki hacimler için şifreleme

sırasındaki performans test edildiğinde, şifreleme algoritması ne kadar güçlü olursa, dosyayı şifreleme ve şifre çözme hızının o kadar düşük olduğu fark edilebilir. Her algoritma, hacim boyutundaki bir değişikliğe eşit şekilde yanıt vermez. Yükleyiciden gelen net talimatlar sayesinde bir birim oluşturmak hızlı ve kolaydır.

Sorular :

Sorular Tartışma Forumu kısa bir açıklama ile cevaplanacak. Cevaplar, mentorluk oturumları sırasında mentor ile tartışılacaktır.

1. Bilgisayarınızın sabit diskindeki verilerinizi nasıl koruyabilirsiniz?
2. Verilerinizi korumak için ne tür bilgisayar programları kullanabilirsiniz?

Öz değerlendirme soruları. Cevap verdikten sonra, öğrenci sonuçları görebilir ve platformda kayıtlı olanlarla karşılaştırabilir.

1. Dosyalarınızı güvence altına almak için en güvenli şifreleme yöntemi nedir?

Ekler:

1. Sunum
2. Video

Referanslar:

1. <https://www.veracrypt.fr/en/Home.html>
2. <https://github.com/veracrypt/VeraCrypt>
3. <https://veracrypt.eu/en/Beginner%27s%20Tutorial.html>