Kimlik Doğrulama ve Erişim Kontrolü Teknikleri

Genel İnceleme

Hazırlayan: Harun BENLİ

Artificial Intelligence Security Lab (AISECLAB) aiseclab.org

Haziran / 2023

# Kullanıcı Kimliği Yönetimi

Kullanıcı adı ve kullanıcı şifresi olmak üzere kullanıcı kimliği temelinde iki öğeyi barındırır. Kullanıcı kimliği kadar önemli olan diğer konu ise kullanıcı kimlik yönetim sistemleridir.

## Dijital Kimlik Yönetim Sistemleri

NIST SP 800-63-3 (*Digital Authentication Guideline*, October 2016) rehberi kullanıcı kimlik yönetim sistemlerini elektronik ortamda tanıtır. Bir kullanıcı ilk olarak üye olabilmesi için belirli kriterler altında kullanıcı yetkilendirmesine dahil olmalıdır.

Temel Güvenlik Gereksinimleri: (Kimlik ve yetkilendirme güvenliği gereklilikleri **NIST SP 800-171 göre**)

1) Bilgi sistemi kullanıcılarını, kullanıcılar adına hareket eden süreçleri veya cihazları tanımlayın.

2) İzin vermenin bir ön koşulu olarak bu kullanıcıların, süreçlerin veya cihazların kimliklerini doğrulayın (veya doğrulayın) kurumsal bilgi sistemlerine erişim.

Türetilmiş Güvenlik Gereksinimleri:

3) Ayrıcalıklı hesaplara yerel ve ağ erişimi ve ağ erişimi için çok faktörlü kimlik doğrulama kullanın

ayrıcalıklı olmayan hesaplara.

4) Ayrıcalıklı ve ayrıcalıklı olmayan hesaplara ağ erişimi için tekrarlamaya dayanıklı kimlik doğrulama mekanizmaları kullanın.

5) Tanımlayıcıların tanımlı bir süre boyunca yeniden kullanılmasını önleyin.

6) Tanımlanmış bir hareketsizlik döneminden sonra tanımlayıcıları devre dışı bırakın.

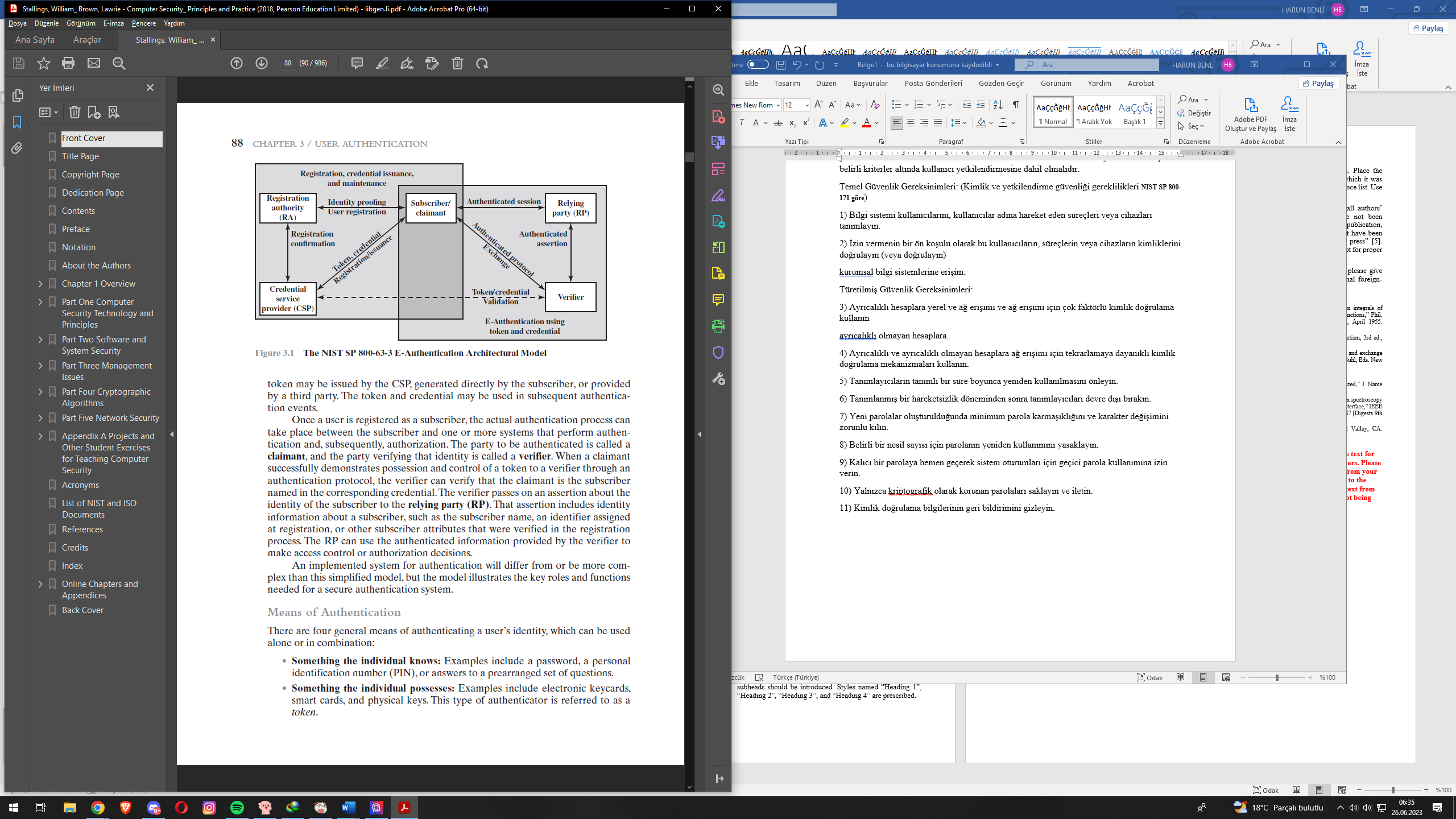
7) Yeni parolalar oluşturulduğunda minimum parola karmaşıklığını ve karakter değişimini zorunlu kılın.

8) Belirli bir nesil sayısı için parolanın yeniden kullanımını yasaklayın.

9) Kalıcı bir parolaya hemen geçerek sistem oturumları için geçici parola kullanımına izin verin.

10) Yalnızca kriptografik olarak korunan parolaları saklayın ve iletin.

11) Kimlik doğrulama bilgilerinin geri bildirimini gizleyin.

  
*Figure 3.1 Kimlik yönetimi mimarisi*

Burada tokenler aracılığıyla yönetim bileşenleri taşınır ve aktarılır.

Claimant : Kimliği doğrulanması gereken kişi.

Kimlik doğrulaması gereken kişinin kimliği token kontrol aracılığıyla doğrulanır.

Bazı kimlik yönetim sistemlerine örnek olarak; şifre, pin kodu, fiziksel kart, anahtar, akıllı kart, parmak izi, retina, yüz okuma, ses algılama, el yazısı tanıma.

Bu sistemlerden birden fazla doğrulamanın olması güvenliği artırmaktadır. Doğrulayıcının kontrol sistemlerinin farklı ve bağımsız olması önemlidir.

## Kullanıcı Kimlik Doğrulama için Risk Değerlendirmesi, üç ayrı konseptle ilgilidir; güven seviyesi, potansiyel etkisi, risk etki alanı. İlk olarak, güven seviyesi etki düzeyinin 4 ayrı seviye ile açıklayabiliriz.

Level 1 : Çok fazla doğrulamanın olmadığı sistemdir. Örnek olarak bir zoom üzerinden konferans paneline bağlanmak.

Level 2 : Güvenlik doğrulamaları arasından biri ya da birkaçı bu seviyede kullanılabilir.

Level 3 : Üst düzey koruma vardır. Yetkili alanlara erişimi olan kısıtlı kişiler vardır. Örnek olarak, patent dosyalarının yetkili kişiler tarafından yetkili olan başka kişilere sistem üzerinden gönderilmesi. Bu dosyalara kısıtlı erişimin bulunması.

Level 4 : Yüksek düzey koruma vardır.Kısıtlı erişim vardır ve uygun olmayan erişimlerin zararı oldukça fazladır. Örnek olarak avukat dava dosyaları ya da kriminal kayıtların veri tabanında saklanması. Çoklu doğrulama gerektirebilir.

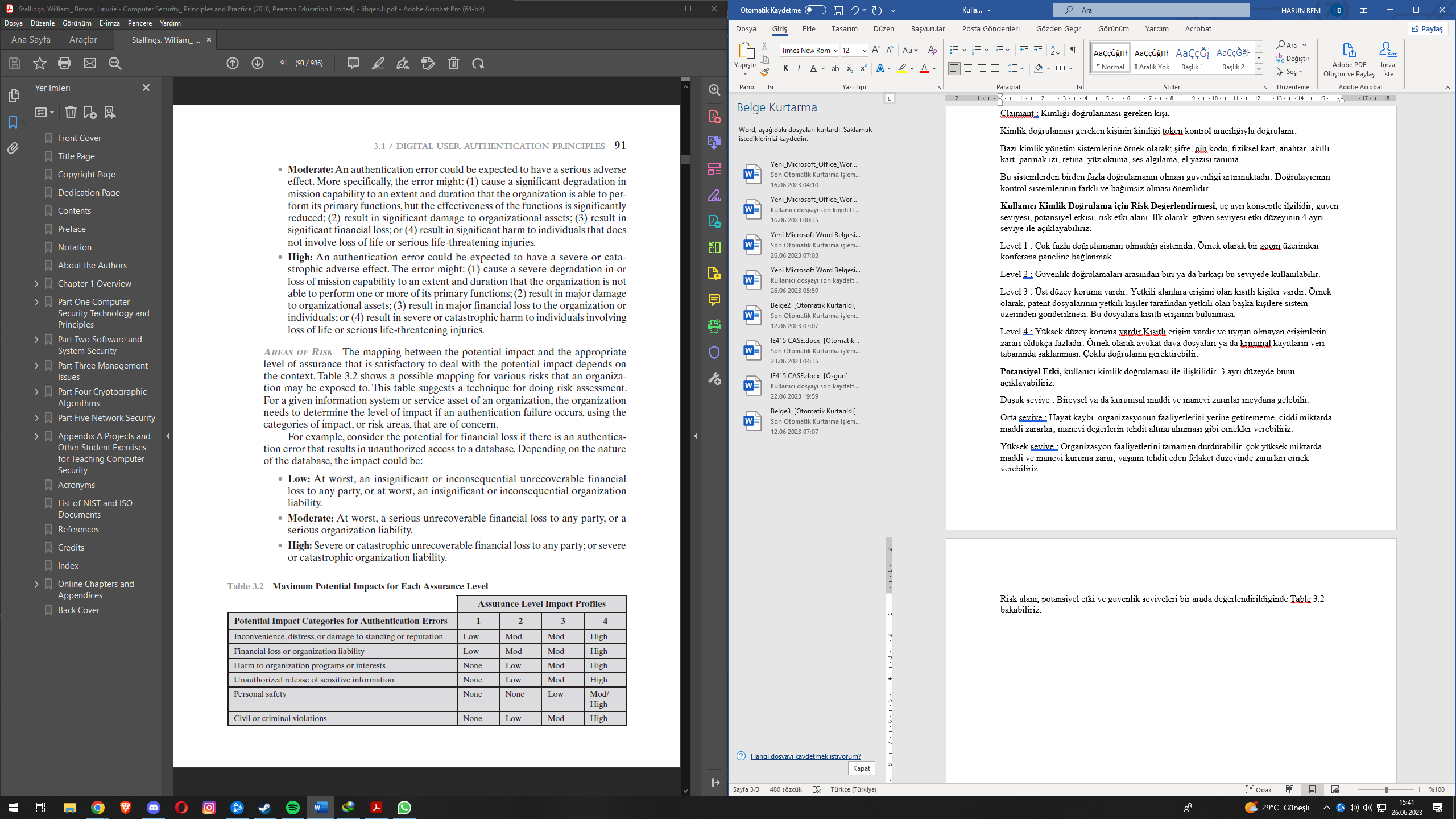
## Potansiyel Etki, kullanıcı kimlik doğrulaması ile ilişkilidir. 3 ayrı düzeyde bunu açıklayabiliriz.

Düşük seviye : Bireysel ya da kurumsal maddi ve manevi zararlar meydana gelebilir.

Orta seviye : Hayat kaybı, organizasyonun faaliyetlerini yerine getirememe, ciddi miktarda maddi zararlar, manevi değerlerin tehdit altına alınması gibi örnekler verebiliriz.

Yüksek seviye : Organizasyon faaliyetlerini tamamen durdurabilir, çok yüksek miktarda maddi ve manevi kuruma zarar, yaşamı tehdit eden felaket düzeyinde zararları örnek verebiliriz.

## Risk alanı, potansiyel etki ve güvenlik seviyeleri bir arada değerlendirildiğinde Table 3.2 bakabiliriz.



Üç seviyede değerlendirilir.

Düşük seviye : Kurum ya da kuruluş için gereksiz kurtarılamaz kayıplar olabilir.

Orta seviye : Kurum için maddi ve kurtarılamaz kayıp olabilir.

Yüksek seviye : Kurum için yüksek miktarda maddi ve kurtarılamayacak kayıplar olabilir. Bunlardan kurum sorumlu tutulabilir.

## Şifre Tabanlı Kimlik Doğrulama

Web servisleri ya da diğer uygulamalar üzerinde kayıtlı olan kullanıcıların yönetimi birkaç yönetici “superuser”, “Administrator” tarafından sağlanır. Bazı sistemlerde misafir ya da kimliksiz hesaplara izin verilebilir. Kullanıcıların kullanıcı kontrol tablosundan sadece okuma yetkisine sahiptir.

## Şifre Zafiyetleri :

Çevrimdışı sözlük saldırısı : Şifre ile korunan sistemin şifresi önceden hazırlanmış şifre kombinasyonlarıyla denenerek uygun şifre eşleşmesini elde eder. Sisteme yönetimsiz erişim hakkı elde eder.

Özel hesap saldırısı : Belli bir kullanıcı adı için şifre denemeleri yapılır fakat belli bir denemeden sonra sistem kilitlenir yaklaşık olarak 5 deneme diyebiliriz.

Popüler şifre saldırısı : Yaygın olarak kullanılan şifreler denenerek erişim hakkı elde edilir.

Bir kullanıcıya karşı şifre tahminleme : Bir kullanıcı hakkında elde edilen veriler ile veriyi eğiterek şifre tahminlemesi yapılmasıdır.

İş istasyonunu ele geçirme(Workstation hijacking) : Yöneticinin sistemi monitör etmediği zamanda sisteme gözetimsiz denemeler yapılması ve erişim elde edilmesidir.

Kullanıcı hatalarından yararlanma (Exploiting) : Sistemin default olarak atadığı parolaların zorluğundan dolayı kullanıcı sisteme parolasız yada parolayı bazı düşük seviye korumalı kanallar üzerinden paylaşarak erişmeye devam edebilir. Bu durumda sisteme kolay şekilde erişim elde edilebilir.

Benzer şifrelerden yararlanma : Kullanıcının başka platformlar üzerinde kullanmış olduğu şifreler sistemde denenerek erişim yetkisi elde edilir.

Elektronik monitörleme : Kullanıcın kullanmış olduğu ağ üzerinden dinleme yapılarak parola tahminlenebilir.

## Şifreli parolaların kullanımı:

Kullanılan parolaların tahminlenmesi ve çözülememesi için kullanılacak parolaların şifreleme algoritmaları kullanılarak şifrelerin belli algoritma ile karıştırılması saldıran taraf için daha fazla işlem yükü ve zamana neden olacaktır ya da şifreye tamamen erişememesine neden olacaktır. Günümüzde halen bazı zafiyetler olduğun dolayı şifrelerin tamamen erişememesinden bahsedemeyiz. Fakat güvenlik seviyelerini artırarak daha güvenli hale getirebiliriz.

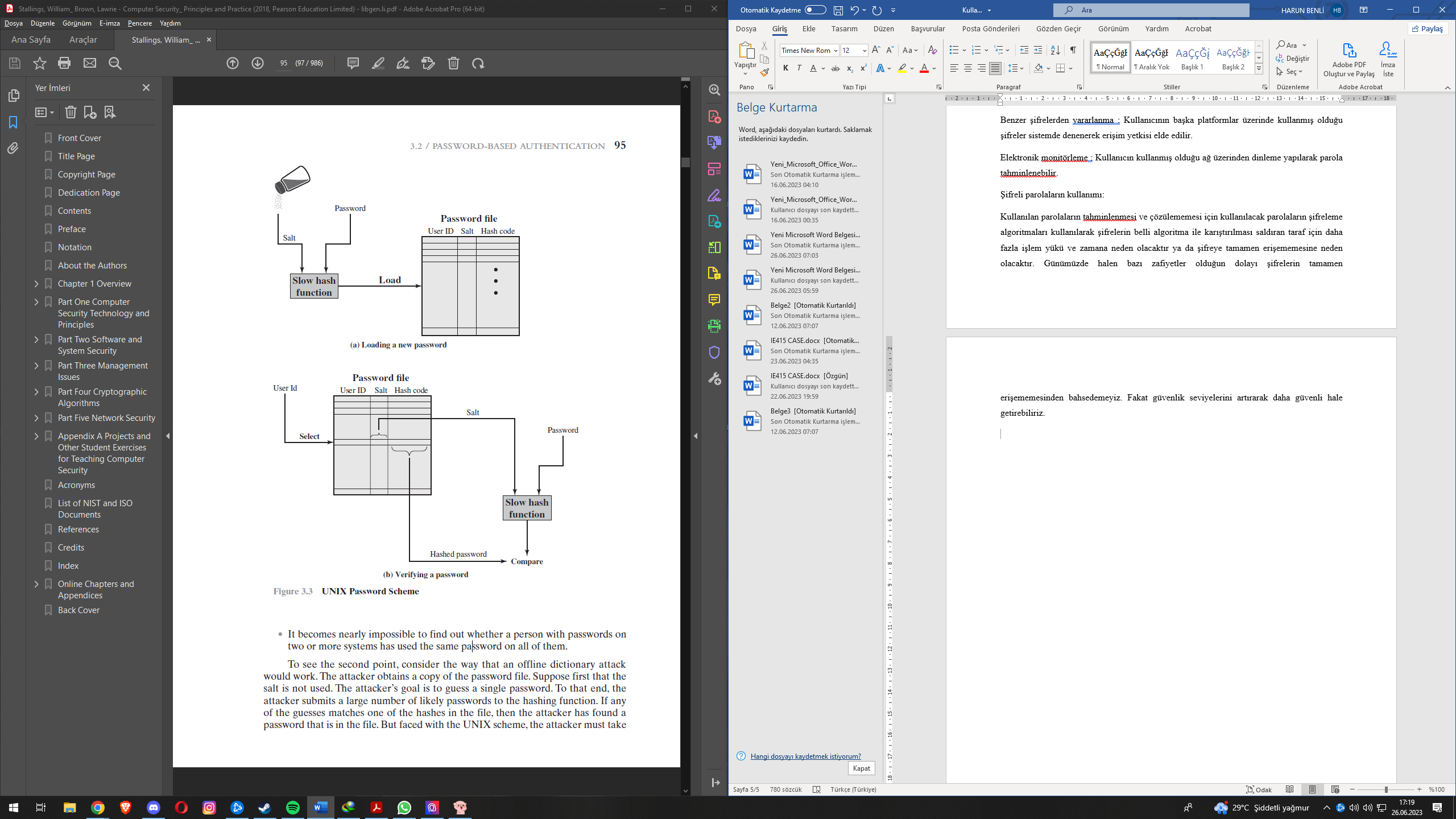


Figure 3.3 ‘de her parolanın(farklı yada benzersiz olmasına gerek yok) hash fonksiyonu ile şifrelenerek daha sonra şifrenin okunurken hash koduna göre çözülerek tekrardan okunur. Burada aynı şifre olmasına rağmen farklı hash kodları ile şifrelenir. Bu bize şifrenin çözülmesinde daha güvenli ortam sağlayacaktır.

UNIX şifreleme yöntemi, kullanıcının seçtiği parolayı 56 bitlik bir anahtar olarak kullanan DES (Veri Şifreleme Standardı) tabanlı bir şifreleme rutini ile çalışır. 12 bitlik bir tuz değeri kullanılır ve DES algoritması bir karma işlemi gerçekleştirmek için 25 kez tekrarlanır. Sonuç, 11 karakterlik bir dizeye dönüştürülen 64 bitlik bir çıktıdır. Bu yöntem DES algoritmasını tek yönlü bir hash işlevine dönüştürmeyi amaçlar.

Ancak bu UNIX şifreleme yönteminin güvenlik açısından yetersiz olduğu düşünülmektedir. Saldırı testlerinde, bir süper bilgisayar kullanılarak yapılan bir sözlük saldırısı, 80 dakika içinde 50 milyondan fazla parola tahmininin işlenmesiyle sonuçlanmıştır. Aynı sonucun tek işlemcili bir makine ile yaklaşık 10.000 dolar harcanarak birkaç ayda elde edilebileceği de gösterilmiştir. Bu nedenle UNIX için daha güçlü hash/salt yöntemleri mevcuttur. Örneğin Linux, Solaris ve FreeBSD gibi birçok UNIX sistemi için önerilen hash fonksiyonu MD5 güvenli hash algoritmasına dayanmaktadır. MD5 şifreleme rutini 48 bit'e kadar bir tuz değeri kullanır ve parola uzunluğunu sınırlamaz. 128 bitlik bir hash değeri üretir. MD5 crypt, crypt(3)'ten çok daha yavaş çalışır ve 1000 iterasyonluk bir iç döngü kullanır.

OpenBSD için geliştirilen en güvenli UNIX hash/salt yöntemi Blowfish simetrik blok şifre algoritmasına dayanır. Bu yöntem Bcrypt adında bir hash fonksiyonu kullanır ve çok yavaş çalışır. Bcrypt 55 karaktere kadar şifrelerin kullanılmasına izin verir ve rastgele 128 bit tuz değeri ile 192 bitlik bir hash değeri üretir. Bcrypt ayrıca bir maliyet değişkeni içerir; maliyet değişkenindeki bir artış, Bcrypt hash işlemini gerçekleştirmek için gereken sürede bir artışa neden olur. Yeni bir parola için atanan maliyet yapılandırılabilir, böylece yöneticiler ayrıcalıklı kullanıcılara daha yüksek bir maliyet atayabilir.

## UNIX Uygulamaları

Her kullanıcı 8 karakter uzunluğunda parolalar kullanacak. 7-bit ASCII kullanılarak 56-bit lik değere sahiptir. Hash rutini kriptosunda DES tabanlı olarak 12-bit tuz(salt) değeri kullanılır. 64-bit sıfır bloğu DES algoritmasında yer alır. Bu algoritmanın çıktısı ikinci aşamanın girdisidir. Proses toplamda 25 aşamalı kripto tekrarlanır. 64-bit’lik çıktı 11 karaktere dönüştürülür. Bu modifikasyon tek yollu hash algoritmasına dönüştürülür. Algoritmanın çalıştırıldığı donanıma göre her bir hash’in çözüldüğü zamanı 25 tekrar için 25 ile çarparak toplam süreyi elde ederiz.

Bir süper bilgisayar kullanılarak gerçekleştirilen bir sözlük saldırısının sonuçları, [PERR03] adlı kaynakta rapor edilmiştir. Bu saldırı, yaklaşık 80 dakika içinde 50 milyondan fazla parola tahminini işlemişti. Ayrıca, bu saldırının birkaç ay içinde tek işlemcili bir makine kullanılarak 10.000 dolara sonuçlanabileceğini gösterilmiştir. UNIX şifreleme şeması, bilinen zayıflıklarına rağmen, hala mevcut hesap yönetimi ile uyumluluk gerektiren yazılımlarda veya çok satıcılı ortamlarda sıkça kullanılmaktadır. Fakat günümüzde kullanılan güvenlik için yeterli bir yöntem değildir.

MD5 teknolojisi ile ktriptoloji 1000 iterasyonlu işleme sahiptir ve daha güvenli hale getirilmiştir ve daha yavaş işleyen bir prosestir.

Şifre kırmada geleneksel yaklaşımlar :

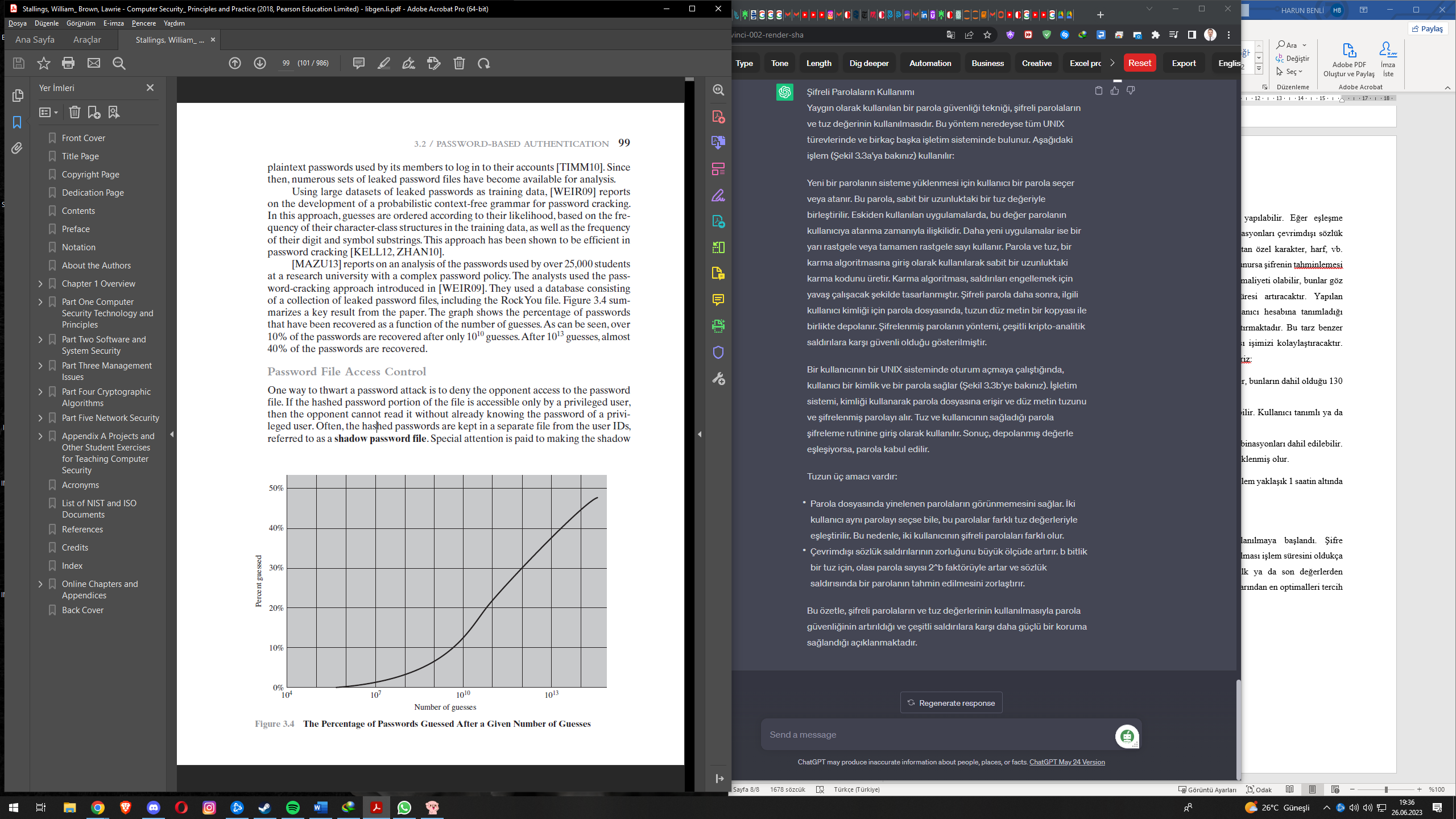
Şifre depolama dosyasındaki hashlerle şifreler karşılaştırma yapılabilir. Eğer eşleşme bulunamazsa şifre kırma programları ile hashlerin tüm şifre varyasyonları çevrimdışı sözlük kullanılarak tahminleme yapılabilir. Kombinasyonlara ek olaraktan özel karakter, harf, vb. eklemesi yapılabilir. Elimizde ne kadar büyük bir sözlük verisi bulunursa şifrenin tahminlemesi neredeyse %99.9 olacaktır. Fakat bu işlemin zamansal ve parasal maliyeti olabilir, bunlar göz önünde bulundurulabilir. Sözlük verisin büyümesi işlem süresi artıracaktır. Yapılan araştırmalar sonucunda çoğu kullanıcının benzer şifreleri kullanıcı hesabına tanımladığı saptanmıştır ve şifrenin kırılma süresini azaltmakta ve kolaylaştırmaktadır. Bu tarz benzer şifrelerin olduğu, yüksek olasılığa sahip sözlüklerin kullanılması işimizi kolaylaştıracaktır. %25 başarı oranıyla yapılabilecek yöntemleri şu şekilde sırayabiliriz:

1. Kullanıcının adı, hesap adı, kullanıcıyla ilgili kişisel bilgiler, bunların dahil olduğu 130 farklı permutasyon denenebilir.
2. 60.000 üzerinde kelimeye sahip farklı sözlükler kullanılabilir. Kullanıcı tanımlı ya da halihazırda olan hazır sözlükler kullanılabilir.
3. 2.aşamadaki sözlüklerin büyük-küçük harf, rakam vb. kombinasyonları dahil edilebilir.
4. 2. ve 3. aşamalar birleştirilerek yaklaşık 2 milyon kelime eklenmiş olur.

Böylece, 3 milyon kelime test edilmiş olur. Hızlı işlemciler ile bu işlem yaklaşık 1 saatin altında hesaplanabilir.

## Modern Yaklaşımlar :

Son 25 yılda şifre belirlemede daha iyi yöntemler kullanılmaya başlandı. Şifre tahminlenmesinde her geçen gün yeni algoritma tarzlarının kullanılması işlem süresini oldukça düşürmektedir. Bunlardan biri olan, Markov, tahminlemeye ilk ya da son değerlerden başlayarak tüme yaklaşım yapmaktadır. Karışık problemlerde aralarından en optimalleri tercih edilerek, iterasyon sayısını ciddi şekilde azaltmaktadır.



*Figure 3.4 : Belirli Bir Tahmin Sayısından Sonra Tahmin Edilen Şifrelerin Yüzdesi*

Şifre belirlemede, kullanıcının eğitimi, şifrenin uğramış olduğu değişiklikler, şifrenin tekrardan aktifliği, karışık şifre politikaları dikkatle değerlendirilebilir.

## Şifre Dosyası Erişim Kontrolü

Parola saldırılarına karşı bir savunma, rakibe parola dosyasına erişimi reddetmektir. Hashlenmiş parolalar gölge parola dosyasında saklanır. Gölge parola dosyasının korunması önemlidir. Halen bazı zayıf noktaları mevcuttur. Yetkişiz erişimlerle sisteme girişlerde bu dosya çalınabilir. Benzer makinelerde benzer parolarının kullanılması, sisteme sızıldıktan sonra diğer cihazlarında verilerinin ele geçirilmesine neden olur. Fiziksel şekilde de bu dosyaya erişim olabilir.

Bu nedenle, bir parola koruma politikası, erişim kontrol önlemlerini, kullanıcıların tahmin edilmesi zor parolalar seçmeye zorlayan tekniklerle tamamlamalıdır.

## Parola Seçim Stratejileri

Kullanıcılar kısıtlanmadığında, çoğu kişi kısa, benzer, basit parolalar kullanacaktır. Amacımız kullanıcının istediği bazı şartları sağlayan parolaların belirlenmesidir. Kullanıcının eğitimi, bilgisayarın oluşturduğu karmaşık parolalar, tepkisel parola ve karmaşık parola politikasıdır. Bazı kullanıcılar ise kendi düşünsel algoritmalarını kullanarak zor parola koyduklarını düşünerek hareket edecek ve aslında kolay parola belirlemiş olacak. Bilgisayar tarafından belirlenen parolaların da kullanıcılar tarafından ezberlenme zorluğu bulunmaktadır. Kullanılmasını istemediğimiz parolalar için büyük bir sözlük gerekebilir ve bu sözlük içinde paroları aramak zaman alabilir. Bloom filtresi, kullanılarak süreç hızlandırılır.

## Kimlik Doğrulamasında Kullanılan Token Türleri

Hafıza kartları, kimlik doğrulama için pin şifresi ile beraberinde kullanılabilir.

Akıllı kartlar, bir mikro işlemciyi içerirler. Bu kartlar banka kartlarına benzeyebilir. Kartlar hem temaslı hem temassız olabilir.

Akıllı tokenlerin amaçlarından biri kimlik doğrulamasını sağlamaktır. Kimlik doğrulama protokolleri statik, dinamik şifre üretici ve meydan okuma-yanıt olmak üzere üç kategoriye ayrılır. Bazı kartlarda şifre koymak yerine devreye entegreli özel işlem bulundurur.

## Elektronik Kimlik Kartları

Elektronik kimlik kartları, ulusal hükümet tarafından geçerli ve otantik olarak doğrulanmış olan bir akıllı karttır. Kart sahibinin dijital bilgilerini içinde saklar. Dijital imza, dijital pasaport bunlara örnek olabilir.

Temassız kartlarda RF çipine yönlendirilmiş herhangi bir işlem PACE ile kontrol edilir. Çevrimiçi uygulamalar için 6 haneli pin girmesi beklenir. Çevrimdışı uygulamalar için kartın önünde basılı olan 6 haneli erişim numarası kullanılır.

## Biyometik Kimlik Yönetimi

Biyometrik kimlik doğrulama, bir kişinin benzersiz fiziksel özelliklerini temel alır. Bunlar statik özellikler olan(parmak izi, el geometrisi, retina ve iris desenleri) ve dinamik özellikler (ses izi, imza) olarak ikiye ayrılabilir. Her kullanıcıyı temsil eden eşsiz şablonlar sayı setleriyle sistemde tutulur ve bunlar eşsizdir. Biyometrik sistemlerinin doğruluğu yanlış eşleşme oranı ve yanlış eşleşmeme oranıyla benzerdir ve önemlidir.

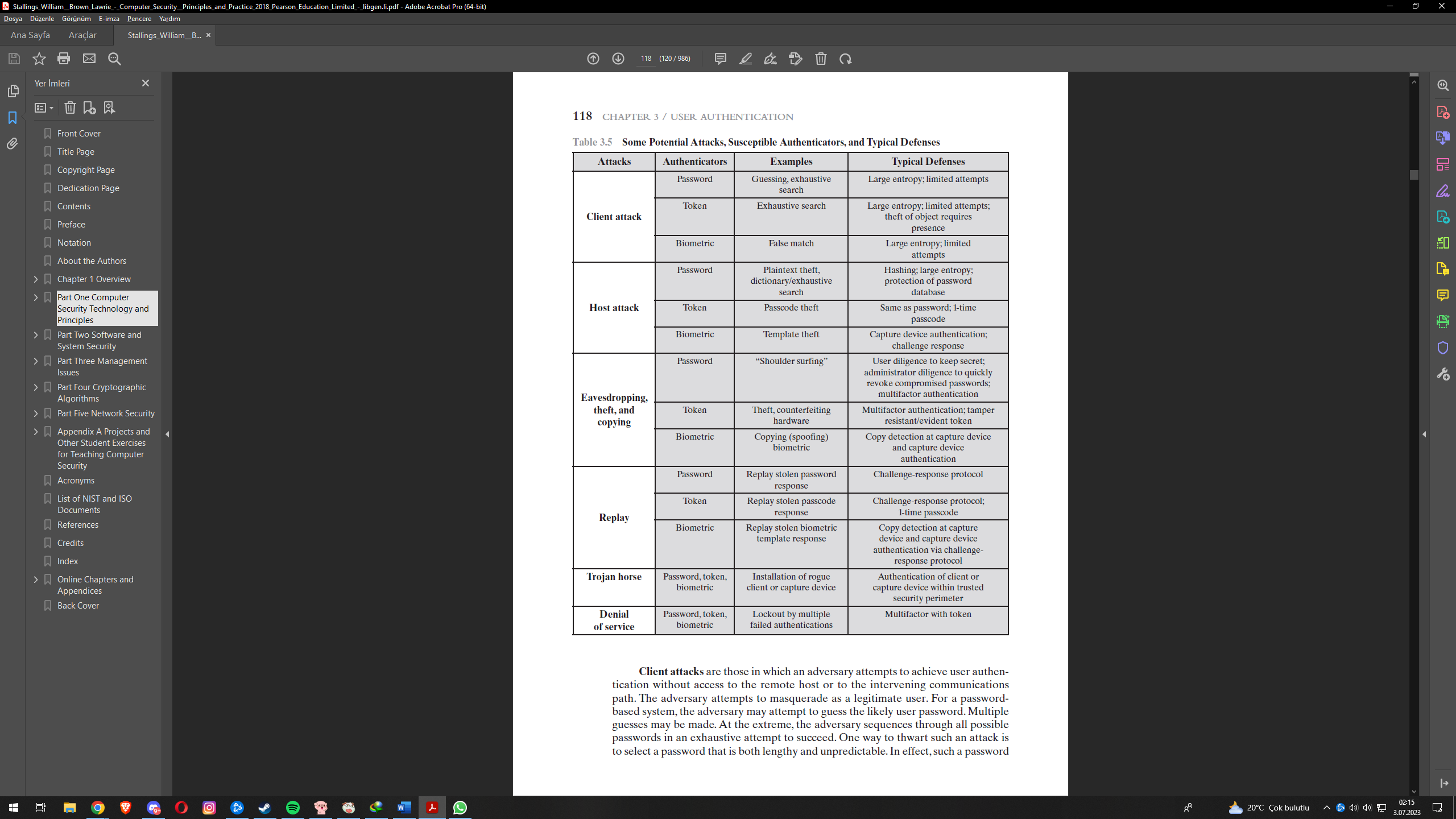
## Uzaktan Kimlik Yönetimi

Şifre prokolü, kullanıcı kimliği hosta iletilir ve bir sayı üretilir, kullanıcıya sayı gönderilir. Kullanıcının yanıtı, rastgele sayının ve kullanıcının şifresinin hash fonksiyonunu içerir. Host, her kullanıcının şifresinin hash'ini saklar ve gelen yanıtı bu hash ile karşılaştırır. Eşleşme durumunda kullanıcı doğrulanmış olur.

Token protokolü, kullanıcıya özel bir passcode sağlar. Kullanıcı, bu passcode'u kullanarak bir yanıt oluşturur ve hosta gönderir. Host, gelen yanıtı kontrol eder ve eşleşme durumunda kullanıcıyı doğrular.

Statik biyometrik protocol, host, bir rastgele sayı üretir ve bu sayıyı kullanıcıya gönderir. Kullanıcı, bir biyometrik cihaz aracılığıyla bir biyometrik şablon oluşturur ve bu şablonu hosta gönderir. Host, gelen bilgileri kontrol eder ve eşleşme durumunda kullanıcıyı doğrular.

Dinamik biyometrik protocol, statik biyometrik protokole benzer, fakat host, rastgele bir sayının yanı sıra rastgele bir dizi de gönderir. Kullanıcı, bu diziyi okuyarak, yazarak veya yazılım yoluyla giriş yapar. Host, gelen bilgileri kontrol eder ve eşleşme durumunda kullanıcıyı doğrular.



## Kullanıcı Kimlik Yönetiminde Güvenlik Sorunları

Host saldırıları, hostlarda saklanan şifre ve özel veriler için yapılır. Biyometrik verilerin korunması zor olabilir.

Client saldırıları, saldırgan erişim yetkesi olmadan sisteme girmek için kimlik doğrulaması için tahmin yapar. Deneme sayısını sınırlamak burada etkili olacaktır.

Dinleme (Eavesdropping), kullanıcı gözlemlenerek şifre bulunmaya çalışılır. Keylogger gibi yazılımlarla kullanıcı girmiş olduğum şifreler kayıt altına alınabilir.

Replay saldırıları, saldırgan daha önce yakaladığı yanıtları tekrardan dener.

Truva atı(Trojan) saldırıları, saldırgan kurbanın cihazına sızarak(uygulama yükleyerek, tıklayarak vb.) kullanıcı verilerine erişebilir.

Hizmet dışı bırakma (Denial-of-Service) saldırıları, sisteme aşırı kimlik denemesi yapılarak sistem devredışı bırakılır. Çok faktörlü kimlik doğrulaması bu yöntemde etkilidir.

## Hashing Nedir?

Hashing, belirli bir anahtarı daha kısa ve yönetilebilir bir kod haline dönüştürme işlemidir. Bu işlem, veri tabanında anahtar değerlere hızlıca erişim sağlarken, aynı zamanda bir veri tabanının güvenliğini artırabilir. Hashing, bir hash fonksiyonu aracılığıyla, orijinal veri dizelerini genellikle daha kısa bir hash değeriyle temsil eder.

Hashing'in iki temel uygulaması vardır: veri tabanı alımı ve şifreleme. Veri tabanı alımında, hashing, örneğin Dewey ondalık sistemine benzer şekilde, verinin hızlı ve verimli bir şekilde bulunabilmesi için bir tür indeksleme işlevi görür.

Şifreleme bağlamında, hashing, orijinal veriyi tanınmayan bir formata dönüştürerek güvenliği artırır. Bu, hashlenmiş verinin, özellikle bir yönlü bir hash algoritması kullanıldığında, çalınamayacağı anlamına gelir.

Ayrıca, hashing teknolojisi, dosyaların bütünlüğünü doğrulamak ve potansiyel değişiklikleri veya müdahaleleri belirlemek için de kullanılır. Bu, dosyanın hash değerini kontrol ederek ve dosyada herhangi bir değişiklik olup olmadığını belirleyerek gerçekleştirilir.

Sonuç olarak, hashing, veri erişimini hızlandıran, güvenliği artıran ve veri bütünlüğünü doğrulayan çok yönlü bir teknolojidir.

## Encoding-Decoding Nedir?

Encode, şifrelemek ya da kodlamak olarak bilinir. Verinin başka bir kullanıcıya iletirken veri içeriğinin okunmaması için şifreleme teknikleri kullanılarak formatının değiştirilmesine denir. Verinin tekrardan çözülmesi işlemine de decoding denir. Bazı encode teknikleri: BASE64, MD5, URL ENCODE, SHA-2 ENCODE, ROT13, MORSE, VİGENERE.

##### **KAYNAKÇA**

1. Stallings, W., & Brown, L. (2022). Computer Security: Principles and Practice (4th ed.). Pearson.
2. <https://www.techopedia.com/definition/14316/hashing-cybersecurity>
3. <https://www.siberegitmen.com/encode/#:~:text=Encode%20siber%20g%C3%BCvenlik%20alan%C4%B1nda%20bir,Yap%C4%B1lan%20bu%20i%C5%9Fleme%20encoding%20denir>.