Kriptografik Modüllerin Güvenlik Gereksinimleri

Oğuz YAYLA

Özet*— Bu çalışmadaki amacımız açık anahtar altyapısında kullanılan kriptografik modüllerin FIPS PUB 140 standardı çerçevesinde sağlaması gereken minimum gereksinimlerin temel itibariyle neler olduğu ve bu gereksinimlerin standardın ilk sürümünden son sürümüne kadar nasıl değiştiğini göstermektir. Bunun yanında, hala FIPS PUB 140-1 standadına uyumlu kriptografik modül ile hizmet veren elektronik sertifika hizmet sağlayıcısının daha güncel ve üst seviyelere çıkışını kolaylaştıracak bilgileri vermektir. Ayrıca, kriptografik modül sağlayıcılarının ilgili modüllerinin yeni sürümlere onaylı hale nasıl geterebileceğine değineceğiz.

Anahtar sözcükler—**Kriptografik Modüller, Güvenlik Gereksinimleri, FIPS PUB 140**

I. GİRİŞ

Kriptografik algoritmalar ve anahtar üretme gibi önemli güvenlik işlemleri yapan donanım ve/veya yazılım bileşenlerine kriptografik modül denilmektedir. Modüller diğer bir çok güvenli kriptografik işlemler yapan bileşen gibi bir onay sürecinden geçmektedir. Bu ulusal[1] ve uluslararası[2] tebliğlerde de belirtilmiştir. Bir kriptografik modülün neden onaylanması gerektiği şu şekilde açıklanabilir:

- Onay, modülün, kabul gören güvenlik şartlarını sağladığının garantisidir.
- Onay programı ile modülün tasarım gereklerine göre en uygun güvenliği yerine getirmesi sağlanır.
- Güvenilir bir onay standardı tarafından onaylanmış kriptografik modül kullanıcılarına/müşterilerine gerekli olan güveni verecektir.

[1,2]'de belirtildiği üzere kriptografik modüller

> " *i. FIPS PUB 140–1 veya FIPS PUB 140-2'ye göre seviye 3 veya üzerinde veya*
> *ii. CWA 14167-2'de belirtilen kriteriere uygun veya*
> *iii. CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olmalıdır.* "

Oğuz Yayla Uygulamalı Matematik Enstitüsü, Orta Doğu Teknik Üniversitesi 06531 Ankara e-posta:yayla@metu.edu.tr
Bu çalışma TÜBİTAK 105G126 Nolu proje tarafından desteklenmiştir.

şartını sağlamalıdırlar. Bu çalışmada birinci maddedeki Federal Information Processing Standards Publication(FIPS PUB) 140 standartlarını[3,4,5] inceleyeceğiz. Açıkcası, [2] 'nin yeni sürümlerinde FIPS PUB 140-1'e uygun olabilme seçeneğini kaldırılmıştır. Ancak Türkiye'de hala FIPS PUB 140-1'e uyumlu kriptografik modüller kullanılabilmektedir.

FIPS PUB 140 standartları, ana başlıkları ile, modülün doğru çalışmasını, standartlara uygunluğunu, testlerini ve güvenliğini incelemektedir. İlk sürümü 1994 yılında yayınlanmıştır. Daha sonraki sürümü 2001 yılında yayınlanmış ve daha taslak halinde olan son sürümü kullanıma açılmış ve yakın zamanda son halinin verilmesi beklenmektedir. Bu çalışmanın ikinci bölümünde bu standartın ilk sürümünün genel özelliklerini açıklayacağız. Üçüncü bölümde standartın ikinci sürümünün ilk sürümünden farklarını belirteceğiz. Dördüncü bölümde de standartın son sürümünün gerektirdiği yeni gereksinimlere değineceğiz. Beşinci bölümde ise yeni sürümlere veya seviyelere uyum sağlamak isteyen elektornik setifika hizmet sağlayıcıların ve kriptografik modül sağlayıcıların önceki bölümlerde bahsedilen farklardan yola çıkarak neler yapabileceğini belirteceğiz.

II. FIPS PUB 140-1 1994

Bu standart, bilgisayar ve haberleşme sistemlerindeki (örneğin bilgi depolama, erişim denetleme ve kimliklendirme, radyo, video, faks gibi) kriptografik modüllerin (örneğin akıllı kartlar) sağlaması gereken güvenlik gereksinimlerini tanımlamaktadır. Kriptografik modül, sağladığı kriptografik hizmete (örneğin şifreleme, kimlik doğrulama, e-imza, anahtar yönetimi gibi), kullanıldığı alana ve bulunduğu ortama göre çeşitli güvenlik gerektirmektedir; bu yüzden standart artan güvenlik seviyeleri belirtip bu seviyelerin maliyetine uygun gereksinimleri açıklamaktadır.

Bu güvenlik gereksinimleri, temelde kriptografik modülün güvenli tasarım ve uygulamasını kapsamaktadır:

- temel tasarım ve belgelendirme,
- modül ara yüzleri,
- fiziksel güvenlik,
- yazılım güvenliği,
- işletim sistemi güvenliği,
- anahtar yönetimi,
- kriptografik algoritmalar,
- elektromanyetik güvenlik ve
- testler.

Kriptografik modüller, yalnızca donanım değil, aynı zamanda yazılım, sürücü ve bunların birleşimini içermektedir.

Etkili bir güvenlik sistemi tasarlamada temel amaç sisteme yapılacak atağın sistemin kaybedeceği bilgiden daha pahalı olmasıdır.

Standardın yedi temel amacı vardır:

1. Kriptografik modülünü istenmeyen işlemlerden ve kullanımdan korumak.
2. Kriptografik modülündeki gizli bilgilerin yetkisiz kişi veya programlar tarafından açığa çıkmasını engellemek.
3. Kriptografik modülündeki yetkisiz değişiklikleri engellemek.
4. Sınıflandırılmamış bilginin korunmasında onaylı güvenlik yöntemlerini uygulamak.
5. Kriptografik modülünün işlem durumunun bilgisini sağlamak.
6. Kriptografik modülünün düzgün çalıştığından emin olmak.
7. Kriptografik modülünün işlem hatalarını algılamak ve bu hatalar yüzünden, önemli güvenlik bilgilerinin açığa çıkmasını engellemek.

Güvenlik Seviyeleri

Bu alt bölümde FIPS PUB 140-1 standartının belirlediği güvenlik seviyelerinin gereksinimlerini kısaca belirteceğiz.

Seviye 1

Kripto modülünde, FIPS onaylı kriptografik algoritmaların kullanılmasını şart koşmak gibi donanımsal güvenlikten bağımsız kişisel bilgisayar üzerinde çalışan sistemler için temel güvenlik öngörmektedir.

Gizli anahtarların yetkisizce değiştirilmesi veya açığa çıkarılması; ayrıca, açık anahtarların değiştirilmesi engellenmelidir. Eğer bu anahtarların üretilmesi modül içerisinde yapılıyorsa, FIPS onaylı üretme algoritmaları kullanılmalıdır. Üretme algoritmasında rastgele sayı üreteci kullanılmalı, gerekli testlerden (rastgelelik testleri) geçmiş olmalı ve bu üreteçteki besleme değerleri ve ara durum değerleri gizli anahtar gibi korunmalıdır. Anahtar dağıtımı onaylı elden, otomatik veya birleşimi yöntemlerle yapılmalıdır. Elden dağıtılan anahtarların modüle girilmesi veya modülden çıkışı yine elden veya elektronik yöntemlerle yapılmalıdır. Elden girilen anahtarların doğru ve ilgili kişiye girildiğinden emin olunmalıdır. Gerekirse şifreli metinin açık halini göstermemek şartıyla kısa süreli gösterimi olabilir. Elden dağıtılan gizli anahtarlar açık veya şifreli yöntemlerle modüle girilmeli veya modülden çıkarılmalıdır. Ancak elektronik dağıtılan gizli anahtarlar şifreli yöntemlerle modüle girilmeli veya modülden çıkarılmalıdır. Anahtar arşivleme yapılıyorsa şifrelenmiş arşivler tutulmalıdır.

Sistem üzerinde çalışan yazılımların detayları raporla belirtilmelidir.

İşletim sistemi yürütülür kod formatında olmalı, onaylı kimlik doğrulama tekniğini kullanmalı, aynı anda sadece bir kullanıcının modülü kullanmasına izin vermeli ve modül birden fazla hizmeti aynı anda vermemelidir.

Modül kendi kendine düzgün çalıştığını test edebilmeli ve bu test seviyesine çalıştırılır çalıştırılmaz geçebilmeli ve hemen kriptografik algoritmaların herbirinin doğru çalıştığını örneğin önceden bilenen değerlerle, yazılım ve sürücü bileşenlerinin doğru çalışabildiğini örneğin e-imza algoritmasıyla ve diğer önemli fonksiyonları kendi içlerinde test edebilmelidir.

Ayrıca, eğer modül anahtar ikililerini üretiyorsa anahtar ikililerinin uyumluluğunu örneğin şifreleme veya e-imza algoritmalarıyla, dışardan yüklenen yazılım ve sürücülerinin güvenliği testini yine örneğin e-imza algoritmasıyla, elle girilen anahtarlarda hata belirleme kodlarıyla ve rastgele sayı üreteci koşan modüller ardaşık ürettikleri rastgele sayı bloklarının farklılıklarını test edebilmeli ve geçmelidir.

Seviye 2

Seviye 1'e ilave olarak,

1. Kriptografik modüldeki fiziksel zorlama ve işlemlerin olduğunu belli edecek fiziksel güvenliği artırmaktadır.
2. Modül üzerinde işlem yapanın rolüne özgü kimlik doğrulama yapılmalıdır.
3. İşletim sistemi erişim kontrolünü sağlamalı ve önemli güvenlik bilgilerine yetkisiz erişimi engelleyebilmelidir.

Seviye 3

Seviye 2'ye ilave olarak,

1. Kriptografik modüldeki önemli gizli bilgilerin, fiziksel zorlama ve işlemlerle ulaşılmasını engelleyecek fiziksel güvenliği sağlamalıdır. Gerekirse içindeki önemli bilgileri sıfırlayabilmelidir.
2. Sistem üzerinde çalışan yazılımlarda yüksek seviye diller kullanılmalıdır.
3. Modül üzerinde işlem yapanın gerçek kimliğine özgü kimlik doğrulama yapılmalıdır.
4. Veri kablo ve yuvaları fiziksel olarak diğer kablo ve yuvalardan ayrılmalıdır. Modüle bilgi girişi ve çıkışı şifreli yapılmalıdır.
5. İşletim sistemi kriptografi yazılımına ve önemli güvenlik bilgilere sistem üzerinde çalışan diğer güvenilmeyen yazılımlar tarafından erişilmesini engellemelidir. güvenilir haberleşme yolu sağlayabilmelidir.
6. Modül çalıştırıldığında rastgele sayı üretecinin düzgün çalıştığını test edebilmelidir. Ardaşık 20000 bit için monobit, poker, runs ve long runs testlerinden geçebilmelidir. Bu testlerin ayrıntıları [3]'de verilmiştir.

Seviye 4

Seviye 3'e ilave olarak,

1. Kriptografik modülünün herhangi içine sızmaya karşı içindeki önemli bilgileri yok ederek tepki vermesini sağlamalıdır ve gerekiyorsa modül çalışmamalıdır.
2. Modülü çalışmaz hale getiren en düşük ve en yüksek arası voltaj ve -100°C ile 200°C arası sıcaklık değişimlerinde modülün güvenliğinin tehlikeye girmesini engelleyebilmelidir.

3. Sistem üzerinde çalışan yazılımların matematiksel yapıları ilk ve son koşulları ile beraber raporla belirtilmelidir.
4. Sadece onaylı işletim sistemleri üzerinde çalışılmalı, kullanılan işletim sistemi doğru işleyebildiğinin güvenliğini sağlayabilmelidir.

III. FIPS PUB 140-2 2001

Kriptografik modül onay programı standarda eklenmiştir. Bu program modülün bu ve diğer kriptografik standartlara uygunluğunu onaylamaktadır.

Müşterek Ölçütler (Common Criteria) EAL 2/3/4, sırasıyla seviye 2/3/4'e eklenmiştir.

"*Önemli bilginin korunması için onaylı güvenlik işlemleri doğru bir şekilde uygulanmak ve çalıştırmak*" amacı standardın amaçları arasına eklenmiştir.

İşletim Sistemi Güvenliği (Operating System Security) başlığı İşlemsel Çevre Güvenliği (Operational Environment Security) ile, Yazılım başlığı Tasarım ile ve Çevresel Etkiler başlığı Fiziksel Etkiler ile değiştirilmiştir; ancak, içerdikleri güvenlik gereksinimleri benzer tutulmuştur.

Kriptografik algoritmalar, kriptografik modül özellikleri altında verilmiştir.

Belgelendirmeye daha fazla önem verilmiş ve her türlü ayrıntının belgesini onay almak için istenmektedir.

140-1'de modül üzerinde işlem yapmak için kimlik doğrulama ve bunun için de PIN, parola, biyometrik gibi mekanizmalar kullanılıyordu. Ayrıca, 140-2'de 10^{-6} olasılıkla rastgele kimlik doğrulayabilme olabileceğini belirtmiştir. Dakikadaki çoklu erişim için daha yüksek bir olasılık (10^{-5}) da belirtilmiş. Ayrıca, açık parola girilmemesi gibi kimlik doğrulama geri beslemesi de açık olmamalıdır.

Rastgele sayı üretecinin güvenlik seviyesi kriptografik algoritmalarla aynı seviyeye çıkarılmıştır.

Modül içerisindeki herhangi bir servisin durması halinde sistemin dışarıya istenmeyen bir bilgi verip vermeyeceğini test eden by-pass testi eklenmiştir.

Modülün hem kullanıcı hem de yönetici yardım belgelerinin olması gerektiği eklenmiştir.

IV. FIPS PUB 140-3 2008

140-3'de rastgele kimlik doğrulayabilme olasılığı 10^{-6}'dan 10^{-8}'e indirilmiştir. Dakikadaki çoklu erişim için ise 10^{-5}'den 10^{-7}'e indirilmiştir. Parola uzunluğu üzerinde kısıtlama olması ve basit parolaların kullanılmasının da engellemesi istenmiştir. Ayrıca, doğrulamada geri besleme yapılmaması önerilmiştir.

Her türlü geçici önemli güvenlik bilgisi, parolaların özeti ve test anahtarları da sıfırlanmalı ve geri dönüş olmamalıdır.

Ayrıca güvenlik seviyelerinde 140-2'ye ek olarak şunlar ilave edilmiştir:

1. Seviye 3'deki kriptografik modül
   a. Önemli kriptografik bilgilerini zaman ölçümü atağına karşı koruyabilmelidir.
   b. Üzerinde çalışılan işletim sistemi, kullanıcıları, kripto yazılımını ve güvenlik bilgilerini değiştirebilmesini engelleyebilmeli ve işlemlerini denetleyebilmelidir. Güvenlik verileriyle güvenilir bir kanal üzerinden haberleşmelidir ve bunları denetleyebilmelidir. Ayrıca, işletim sistemi uzaktan yönetime izin vermemelidir.
2. Seviye 4'deki kriptografik modül
   a. İki seviyeli kimlik doğrulamasıyla işlem yapanı denetleyebilmelidir: gizli parola, fiziksel anahtar/token veya biyolojik özellik(biyometrik).
   b. Önemli güvenlik bilgileri basit ve değişmeli güç ölçüm ataklarına karşı koruyabilmelidir. Ayrıca, modül kullanılmıyorken bile içerisindeki önemli güvenlik bilgilerinin dışa çıkmasını engellemek için bu bilgileri şifrelemeli ve erişim kontrolü sağlamalıdır.

140-3'de yeni bir güvenlik seviyesi tanımlanmıştır:

Seviye 5:

Bu seviyedeki bir modül, seviye 4'e ilave olarak modül kullanılmıyorken bile içerisindeki bütün güvenlik bilgilerinin dışa çıkmasını engellemek için bu bilgileri şifrelemeli ve erişim kontrolü sağlamalıdır.

Sıcaklık ve voltaj dalgalanmalarında hatalara karşı dayanıklı olmalıdır. Görünmez radyasyona karşı dayanıklı olmalıdır. Ayrıca, fiziksel mukavemet algılayıcı ve sıfırlama devrelerinin işlemez hale getirilmesine karşı korunaklı olmalıdır. Sıfırlama gerektiğinde, içindeki bütün güvenlik bilgilerini sıfırlamalıdır.

V. TAVSİYELER

Bölüm III ve IV'den anlaşılacağı üzere standartın güncel sürümlerinin bir önceki sürümünden çok fazla farklılıkları yoktur. Ancak, dikkat edilmesi gereken "FIPS Onaylı algoritmaların" sürekli değişim ve gelişim içinde olmasıdır. Simetrik kriptosistemlerinde DES[6]'ten AES[7] veya TDES[8]'e geçilmesi zorunlu hale gelmiştir. Yine simetrik kriptografide kullanılan şifreleme modları değiştirilmiştir[9]. Açık anahtarlı kriptosistemlerde ise RSA'nın Bleichenbacher'ın geliştirdiği ataklara açık olduğu anlaşılmış ve 2002 yılında RSA'nın uygulama yöntemi değiştirilmiştir[10]. Ayrıca, 2009 yılından itibaren en az 2048 bit açık anahtar uzunluğu kullanılacaktır[13]. Diğer e-imza sistemlerinden, DSA sisteminin kullandığı değerlerin nasıl üretileceği detaylandırılmıştır[11]. EDSA sisteminin ise nasıl uygulanacağı ilk kez detaylı halde açıklanmıştır[11]. Ayrıca, aynı standartın güncel sürümü[12] taslak halinde olmasına rağmen yaklaşık iki yıldır yorumlara ve tavsiyelere açıktır. Geliştirilecek RSA/DSA/EDSA e-imza sistemlerinin, bu taslak da göz önüne alınarak geliştirilmesinde gelecek uygulamalar için faydalı olacağı kaçınılmazdır. Özetleme algoritması MD5 kullanımdan tamamen kaldırılmış ve 2011 yılından itibaren en çok kullanılan SHA-1 özetleme algoritması da kullanımdan kaldırılacaktır[13]. Yerlerine SHA-256/SHA-384 veya yeni bir algoritma kullanılacaktır. Rastgele sayı üreteci için kararlı yöntemlerin önemli bilgilerin korunması işlemlerinde kullanılması önerilmiştir[14].

Dolayısıyla, elektronik sertifika hizmet sağlayıcı veya kriptografik modül sağlayıcı temel anlamda modül üzerinde işlem yapmak için kimlik doğrulama verisini (PIN vb.) en az sekiz basamaklı tanımlarsa, modül içerisinde kullanılan rastgele sayı üreteçlerini [15]'de belirtilen yöntemlere göre tanımlarsa ve güncel kriptografik algoritmalarını (AES, RSAPSS, SHA256 vb.) da tanımlarsa modülün güncel sürümlere; hatta üst seviyelere uygun olmasını sağlamış olur.

VI. SONUÇ

Bu çalışmada kriptografik modüllerin güvenlik gereksinimleri FIPS PUB 140 standardına göre verilmiştir. Yeni nesil kriptografik modüllerin daha fazla anahtar boyu ve daha dayanıklı kriptografik algoritmalar ile son kullanıcıya daha uygun güvenlik çözümleri sunacağı anlaşılmaktadır. Çalışmanın bütününü bozmamak için kriptografik algoritmalarda(DES, RSA, DSA, SHA-1, rasgele sayı üreteçleri vb) olan değişiklikler detaylı verilememiştir. Ancak, böyle bir çalışmanın bu çalışmanın devamı olabileceği görülmektedir.

VII. TEŞEKKÜR

Bu çalışmanın şekillenmesinde büyük katkıları olan TÜBİTAK 105G126 nolu projedeki yöneticilerime ve arkadaşlarıma teşekkür ederim.

KAYNAKLAR

[1] Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ T.C. Telekomünikasyon Kurumu 06.01.2005.
[2] ETSI TS 101 456 V1.4.1 Electronic Signatures and Infrastructures 2006
[3] Federal Information Processing Standards Publication Securıty Requırements For Cryptographıc Modules 1994
[4] Federal Information Processing Standards Publication Securıty Requırements For Cryptographıc Modules 2001
[5] Federal Information Processing Standards Publication Securıty Requırements For Cryptographıc Modules DRAFT 2008
[6] National Institute of Standards and Technology, Data Encryption Standard (DES), Federal Information Processing Standards Publication 46-3, October 25, 1999.
[7] National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001
[8] National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004.
[9] National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001.
[10] RSA Laboratories, PKCS#1 v2.1: RSA Cryptography Standard, June 14, 2002.
[11] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2 with Change Notice 1, October 05, 2001.
[12] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-3 DRAFT March, 2006.
[13] National Institute of Standards and Technology, Cryptographic Algorithms and Key Sizes for Personal Identity Special Publication 800 -78-1, August 2007.
[14] National Institute of Standards and Technology, Annex C: Approved Random Number Generators for FIPS 140-2, Security Requirements for Cryptographic Modules, March 17, 2003.
[15] National Institute of Standards and Technology, Special Publication 800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2006.