T.C.
ONDOKUZ MAYIS ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

KRİPTOGRAFİK MODÜL İÇEREN CİHAZLARIN GÜVENLİK GEREKSİNİMLERİ

YÜKSEK LİSANS TEZİ

Halil KARAALAN

Tezin Savunma Tarihi : 21 Şubat 2014

Tez Danışmanı : Yrd. Doç. Dr. Sedat AKLEYLEK

Bu Yüksek Lisans Tez Çalışması Ondokuz Mayıs Üniversitesi OMÜ PYO.MUH.1904.12.014 no'lu Proje ile Desteklenmiştir.

Ondokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalında

Halil KARAALAN Tarafından Hazırlanan

KRİPTOGRAFİK MODÜL İÇEREN CİHAZLARIN GÜVENLİK GEREKSİNİMLERİ

-

başlıklı bu çalışma jürimiz tarafından 21/02/2014 tarihinde yapılan sınav ile YÜKSEK LİSANS tezi olarak kabul edilmiştir.

Başkan	**:**	**Prof. Dr. Bünyamin KARABULUT** Ondokuz Mayıs Üniversitesi	.....
Jüri Üyeleri	**:**	**Yrd. Doç. Dr. Tolga SAKALLI** Trakya Üniversitesi	.....
		Yrd. Doç. Dr. Sedat AKLEYLEK Ondokuz Mayıs Üniversitesi	.....

…./…./...2014

Prof. Dr. Recep TAPRAMAZ

Enstitü Müdürü

Eşime ve oğlumuz İlke'ye

ÖNSÖZ

Bu tez çalışmasını PYO.MUH.12.014 numaralı proje ile destekleyen Ondokuz Mayıs Üniversitesi'ne teşekkür ederim. Ayrıca tez çalışmalarım esnasında bana büyük destek veren ve bana güvenen, bilimsel çalışma yöntemini örnek aldığım danışman hocam Sayın Yrd.Doç.Dr. Sedat AKLEYLEK'e saygı ve şükranlarımı sunarım.

Şubat 2014 Halil Karaalan

İÇİNDEKİLER

Sayfa

ÇİZELGELER LİSTESİ

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

KISALTMALAR

AES	**:** Advanced Encryption Standard-Gelişmiş Şifreleme Standardı
ARP	**:** Address Resolution Protocol-Adres Çözümleme Protokolü
BİLGEM	**:** Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
CADES	**:** Cryptographic Message Syntax Advanced Electronic Signatures-Kriptografik Mesaj Sözdizimi Elektronik İmzalamaları
CBC	**:** Cipher Block Chaining-Şifre Blok Zinciri
CRT	**:** Chinese Remainder Theorem-Çinli Kalan Teoremi
DH	**:** Diffie–Hellman
ECB	**:** Electronic Code Book-Elektronik Kod Kitabı
EKG	**:** Elektrokardiyografi
DOS	**:** Denial of Service-Hizmet Engelleme
ECDSA	**:** Elliptic Curve Digital Signature Algorithm-Eliptik Eğri İmzalama Algoritması
ECDH	**:** Elliptic Curve Diffie–Hellman – Eliptik Eğri Diffie-Hellman
EEPROM	**:** Electronically Erasable Programmable Read-Only Memory-Elektronik Silinebilen Programlanabilen ROM
ETSI TS	**:** European Telecommunications Standard Institute Technical Specification-Avrupa Telekominikasyon Standart Enstitüsü Teknik Şartnamesi
FIPS	**:** Federal Information Processing Standard-Federal Bilgi İşleme Standardı
GPS	**:** Global Positioning System-Küresel Konumlama sistemi
GSM	**:** Global System for Mobile Communications-Küresel Mobil İletişim Sistemi
IPA	**:** Information-Technology Promotion Agency, Japan-Japonya Bilgi Teknolojileri Gelişim Ajansı
ISO-IEC 19790	**:** Uluslararası Standardizasyon Organizasyonu-Uluslararası Elektroteknik Komisyonu 19790
ISO/IEC 17799:2000	**:** International Organization for Standardization/ International Electrotechnical Commission
ISDFS	**:** International Symposium on Digital Forensics and Security-Uluslararası Adli Bilişim ve Güvenlik Sempozyumu
KBSA	**:** Küçük Bilgisayar Sistem Arayüzü
KCT	**:** Kriptolu Cep Telefonu
MİLCEP	**:** Milli Cep telefonu
NIST	**:** National Institute of Standards and Technology-Ulusal Standartlar ve Teknoloji Enstitüsü
NSM	**:** Norwegian National Security Authority, Norway-Norveç Ulusal Güvenlik Kurumu
PC	**:** Personal Computer-Kişisel Bilgisayar
PIN	**:** Personal Identification Number-Kişisel Kimlik Numarası
PKCS	**:** Public Key Cryptography Standards-Açık Anahtar Kriptografi Standartları

RAM	**:** Random Access Memory-Rastgele Erişimli Bellek
ROM	**:** Read Only Memory-Yalnızca Okunabilen Bellek
RSA	**:** Rivest Shamir Adleman
SCIP	**:** Secure Communications Interoperability Protocol-Güvenli İletişimler Karşılıklı Çalışma Protokolü
SHA	**:** Secure Hash Algorithm-Güvenilir Özetleme Algoritması
SMS/MMS	**:** Short Message Service/Multimedia Messaging Service-Kısa/Çoklu Mesaj Servisi
TAFICS	**:** Turkish Armed Forces Integrated Communication System-Türk Silahlı Kuvvetleri (TSK) Entegre Muhabere Sistemi
TASMUS	**:** Taktik Saha Muhabere Sistemi
TÜBİTAK	**:** Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
USBK	**:** Universal Serial Bus Kriptolayıcı-USB bellek Kriptolayıcı
XADES	**:** Extensible Markup Language (XML) Advanced Electronic Signatures-Genişletilebilir Biçimlendirme Dili Geliştirilmiş Elektronik İmzalamalar
Wi-Fi	**:** Wireless Fidelity-Kablosuz Bağlantı

KRİPTOGRAFİK MODÜL İÇEREN CİHAZLARIN GÜVENLİK GEREKSİNİMLERİ

ÖZET

Bu çalışmada kriptografik modüllerin farklı seviyelerdeki güvenlik gereksinimlerine ve kripto modülü içeren kriptolu cep telefonları (KCT) ile USB bellek kriptolayıcı (USBK) cihazlarına yönelik tehditler ve bu cihazların güvenlik gereksinimlerine değinilmiştir. Bu gereksinimler Federal Information Processing Standard (FIPS 140-3 ve FIPS 180-4)'te tanımlanan güvenlik ihtiyaçları ile halen kullanılmakta olan kriptolu cep telefonları ve USBK bellek kriptolayıcılarının güvenlik özelliklerinin analiz edilmesi suretiyle açıklanmıştır. FIPS 140-3 bilgisayar ve iletişim sistemlerindeki gizlilik dereceli bilgileri koruyan bir güvenlik sisteminde kullanılan kriptografik modül için farklı güvenlik seviyeleri belirler ve her seviyede modülün güvenlik gereksinimlerini tanımlar. Hedeflenen güvenlik modeli güvenlik seviyeleri, tehdit seviyeleri ve kriptografik olarak güvenli ve onaylı algoritma gereksinimlerinden oluşmaktadır. Yapılan araştırma ve analizlerde KCT'nin sıradan cep telefonlarına nazaran şifreli konuşma ve mesajlaşma gibi üstün niteliklere sahip olduğu ancak yine de yetkisiz erişim, akıllı kartın kurcalanması, yapısal (fiziksel) bozulma, saldırılar (DoS,vb.), kötü yazılımlar ve kriptanaliz gibi pek çok tehdide açık olduğu görülmektedir. USBK cihazı, kullanıcılarına verilerini bir harici bellek ve/veya USB belleğe gönderdikten sonra koruma imkanı veren entegre bir sistemdir. Kullanıcı veri aktarma sırasında bu veriyi şifreler. Ancak USBK cihazlarının da yetkisiz erişim, entegre devrenin kurcalanarak anahtarların ele geçirilmesi, yapısal bozulma gibi tehditlerle karşı karşıya olduğu görülmüş; bu tehditlere karşı cihazda biyometrik kimlik denetimi, kurcalama delili, tespiti ve tepki devresi, sıcaklık ve gerilim değişimlerine karşı fiziksel direnç, uzaktan erişim ve acil anahtar silme güvenlik özelliklerinin bulunması gerektiği anlaşılmıştır.

Anahtar Kelimeler: Kriptografik Modüller; Güvenlik Gereksinimleri; FIPS 140-3, Kriptolu Cep Telefonu, Kriptolu Bellek.

ON THE SECURITY REQUIREMENTS OF THE DEVICES WITH CRYPTOGRAPHIC MODULES

ABSTRACT

In this study, security requirements are given for different levels of cryptographic modules and threats to mobile phones and USBs with crypto module and security requirements of these devices. The security requirements given in Federal Information Processing Standard (FIPS 140-3 and 180-4) are analyzed. New security requirements and features of the mobile phones with crypto module and USBK crypto devices are proposed. The FIPS 140-3 specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems and provides different security levels. The proposed security model consists of security levels, threat levels, cryptographically secure and approved algorithm requirements. Mobile phones with crypto module have outstanding security features according to the other cell phones, such as encrypted voice and data communication. In this thesis, it's concluded that they have threats as unauthorised access, tampering smart card, corruption, attacks, malwares and cryptanalysis. USBK is an integrated system which provides users to protect their data after the transmission to a back disk. The user can transfer data by encrypting it. It's concluded that there are several threats like unauthorised access, revealing keys by probing the integrated circuit and corruption and the device should have security features such as biometric authentication, tampering detection, evidence and response, physical robustness to temperature and voltage exchanges, remote access and immediate key zerozation.

Key Words: Cryptographic modules; security requirements; FIPS 140-3, mobile phone with crypto module (crypto phone), USB with crypto module (crypto stick).

1. GİRİŞ

Bilgi teknolojilerindeki yenilikler ve gelişmeler sonucunda veriler kolayca başka bir platforma aktarılmaktadır. Bu transfer şeklinde ortaya çıkan sorun istenen güvenliğin nasıl sağlanacağıdır. Askeri, siyasi, sağlık, adli, finans vb. alanlarda gizli bilgilerin korunması ve güvenli biçimde aktarılması önem arz etmektedir. Bu sahalardan birinde yaşanabilecek gizli bilgi kayıpları kurum ve devletleri büyük zarara uğratabilecektir. Kriptografik protokolleri kullanarak bilgi güvenlik hedeflerinin sağlanmasına ihtiyaç vardır. Bu hedefler gizlilik, bütünlük, kimlik doğrulama ve inkar edilemezliktir. Bilgi güvenliği hedeflerini standart kullandığımız cihazlar ile her zaman sağlamamız mümkün olamamaktadır. Bunları başarmak için cihaz, kripto modülü adı verilen kısmı içinde bulundurur. Güvenli kripto modülü uygulamaları gereksinimleri FIPS 140-3'de [6] ve Uluslararası Standardizasyon Organizasyonu-Uluslararası Elektroteknik Komisyonu 19790 (ISO-IEC 19790)'de [45] ayrıntılı biçimde açıklanmıştır. Kriptografik modül içeren kripto cihaz ve sistemlerin pek çok güvenlik özelliği bulunmakla birlikte, geliştirilmesi gereken ihtiyaçlarının olduğu açıktır. Bu nedenle pek çok ülke kripto güvenliğini artıracak araştırmaları sürdürmekte ve kriptografik modül içeren cihazların güvenlik gereksinimleri üzerine milli politikalar üreten kurum ve kuruluşlar (Information-Technology Promotion Agency, Japan (IPA), Norwegian National Security Authority, Norway (NSM) vb.) teşkil etmekte [46,47], kripto modüllerinin güvenlik ihtiyaçlarını belirlemeye yönelik çalışmalar yürütmektedir.

Cep telefonları günümüzde haberleşme, alışveriş, sosyal medya başta olmak üzere pek çok işleviyle artık bir ihtiyaç haline gelmiştir. Haziran 2010'da dünyada toplam 219 ülkedeki tahmini GSM cep telefonu kullanıcı sayısı 4,4 milyar civarındadır [14]. Bununla birlikte cep telefonıu görüşmelerinin ve bu telefonlar üzerinden yazılı/görüntülü veri transferinin güvenli biçimde yapılabilmesi önemli bir sorun haline gelmiştir. 2011 yılında ABD'de yayımlanan bir rapora göre ülkede akıllı cep telefonları o yıl ilk kez kişisel bilgisayarlardan (PC) daha fazla satılmış ve saldırganlar eski tekniklerle akıllı telefonlara pek çok saldırı düzenlemiştir [2]. Cep

telefonu haberleşmesini güvenli hale getirmek için öncelikle cep telefonlarının maruz kalabileceği tehditleri ortaya koymak ve bu tehditlere karşı alınacak önlemleri araştırmak gereklidir. Özellikle akıllı telefonların son zamanlardaki popülerliği ve zayıf güvenlik özellikleri, saldırganlar için bu cep telefonlarını cazip hedef haline getirmiştir. Akıllı cep telefonlarındaki güvenlik duvarı, antivirüs yazılımı ve kriptolama gibi güvenlik önlemleriyle işletim sistemleri, kişisel bilgisayarlarınki kadar güncel değildir [3]. Bu nedenle şifreli telefon görüşmesi, SMS, e-posta gönderimi ile yine şifreli görüntülü görüşme güvenlik özelliklerini sağlayan kriptolu cep telefonlarının (KCT) tasarlanması son yıllarda önem kazanmıştır. Şu ana kadar üretilen kriptolu cep telefonları üstün güvenlik özelliklerine sahip olmakla birlikte, bu cep telefonlarının geliştirilmesi gereken güvenlik ihtiyaçları bulunmaktadır.

Dünyada ve ülkemizde bilgi güvenliği kapsamında araştırma ve geliştirme faaliyetleri sürdürülen kripto cihazlarından birisi de kriptolu USB bellekler ya da USB bellek kriptolayıcılardır. Verilerin bilgisayar sistemlerinden başka bilgisayarlara ya da ortamlara şifrelenerek güvenli şekilde taşınması, USB belleklerde ya da harici belleklerde şifreli saklanması; ihtiyaç duyulduğunda da bu verilerin şifresi çözülerek sadece yetkili kullanıcılar tarafından okunabilmesi büyük önem kazanmıştır. Bu cihazlar küçük yapıda olması nedeniyle kolaylıkla kaybolmakta, çalınabilmekte ve dolayısıyla içindeki veriler yetkisiz kişilerin eline geçebilmektedir. USBK, USB bellek ya da harici belleklere şifreli biçimde veri transferine yarayan ve bu verilerin istenen zamanda şifresinin çözülerek USB/harici belleklerde yalnızca yetkili kullanıcısı tarafından açılabilmesine yarayan bir cihazdır.

Bu tez kapsamında kripto cihazlarının güvenlik gereksinimleri, kripto modüllerinin tasarım ve analizi için FIPS 140-3'de tanımlanan güvenlik seviyeleri 2. Bölümde genel bilgiler başlığı altında kısaca özetlenmiştir. Seviye yükseldikçe modül daha fazla özelliğe sahip olmakta, daha da önemlisi bunlar daha güvenli sistemler sağlamaktadır. Ayrıca fiziksel güvenlik, işletim sistemi güvenliği, anahtar yönetimi ve diğer güvenlik gereksinimleri kapsamında öneriler incelenmektedir. 3. Bölümde kriptolu cep telefonu (KCT) ve USBK adı verilen USB kriptolayıcıya yönelik tehditler ve bu cihazlara yönelik güvenlik önerilerini kapsayan materyaller ve yöntemler, 4. Bölümde ise tez kapsamında yapılan çalışmalar sonucunda elde edilen bulgular vurgulanmıştır. 5. Bölümde sonuç ve öneriler açıklanmıştır.

2. GENEL BİLGİLER

Bu bölümde kriptografik modüllerin standartlarla belirlenen güvenlik seviyeleriyle sağlaması gereken güvenlik gereksinimleri [6] ve önerilen ilave güvenlik gereksinimleri açıklanmıştır. Bu gereksinimler işletim sistemi güvenliği, işletim ortamı ve erişim kontrolü, fiziki güvenlik ve personel güvenliği, anahtarlar, girişimsel olmayan saldırılar, yapılandırma yönetimi, otomatik kontrol testleri ve diğer saldırılara karşı güvenlik gereksinimleridir. Bu bölümde yer alan öneriler [25,26] nolu çalışmaların bir bölümünü oluşturmaktadır. Kriptografik modül, onaylı ya da izin verilmiş güvenlik fonksiyonlarını (kriptografik algoritmalar ve anahtar kurulumu) uygulayan ve kriptografik sınırı kapsayan bir donanım, yazılım ve/veya gömülü yazılım grubudur [6].

2.1 Güvenlik Seviyeleri

Bu kısımda kriptografik modül içeren cihazların güvenlik seviyeleri özetlenmektedir. Cihazların farklı kullanımları için verilen 4 seviye vardır [6,47].

Seviye 1 en az güvenlik gereksinimlerine sahip güvenlik seviyesidir. Kriptografik modül üretilen ya da kullanılan anahtarları korumaz. Seviye 1 üretim aşaması bileşenleri için temel gereksinimlere sahiptir. Başka özel fiziksel güvenlik mekanizmalarına ihtiyaç duymaz [6,47].

Seviye 2'de ise kriptografik modülde kurcalama izi tespiti sayesinde kriptografik modülde fiziki güvenlik gereksinimi artar. Ayrıca operatör özel bir rolü üstlendiğinde kriptografik modülün kimlik doğruladığı ve yetki onayladığı rol tabanlı kimlik doğrulamayı gerektirir [6,47].

Seviye 3 kriptografik modülün kapakları ya da kapıları açıldığında tüm kritik bilgileri (anahtar vb.) sıfırlayan tepki devrelerini ve kurcalama tespitini gerektirir. Anahtarların modüle giriş ve çıkışı kriptolu olarak ya da bölünmüş bilgi yöntemi ile yapılabilir. "Güvenli devre" uygulaması açık anahtarlar ve modül yazılımını güvensiz yazılım ve uzaktan yönetime karşı korur [6,47].

Seviye 4, Seviye 3'e ilave olarak operatör kimlik denetiminde şifre, anahtar, biyometrik gibi çok faktörlü kimlik doğrulamayı getirir. Ayrıca modülün sıcaklık ve gerilim dalgalanmalarından olumsuz etkilenmesine karşı koruma sağlar. Bunların dışında Seviye 4 kritik bilgileri girişimsel olmayan saldırılara karşı korur. Kritik bilgilerin girişimsel olmayan saldırılara karşı korunmasını sağlar [6,47].

2.2 Güvenlik Gereksinimleri

Bu kısımda güvenlik gereksinimleri incelenmekte ve yeni gereksinimler tanımlanmaktadır. İşletim sistemi güvenlik gereksinimleri, işletim ortamı ve erişim kontrolü, fiziksel güvenlik ve personel güvenliği, girişimsel olmayan saldırılar, anahtarlar, yapılandırma yönetimi, otomatik kontrol testleri ve diğer saldırıların azaltılması alanlarındaki güvenlik gereksinimleri ile güvenlik hedeflerine sırasıyla değinilecektir.

2.2.1 İşletim sistemi güvenlik gereksinimleri

Operatör, modülü onaylı bir işletim modunda işletmelidir. Onaylı bir işletim modu onaylı bir güvenlik fonksiyonu ya da anahtar kurulum mekanizması hizmeti sağlamalıdır. Modülün güvenlik politikasında operatörün modülü onaylı bir işletim modunda nasıl işletebildiği açıklanmalıdır.

İşletim sistemi tarafından bir kriptografik modüldeki yazılım ve gömülü yazılımına, onaylı imzalama algoritmalı elektronik imza ya da anahtarlı mesaj kimlik kodu uygulanmalıdır. Her bir kriptografik modül örneği, anahtarlarını kontrol altında tutabilmelidir. İşletim ortamı anahtarlara kontrolsüz erişimi engellemek üzere ayarlanmalıdır. Tüm kriptografik yazılım, anahtarlar, kontrol ve durum bilgisi dağıtık erişim kontrolü uygulayan işletim sistemi kontrolünde olmalıdır.

2.2.2 İşletim ortamı ve erişim kontrolü

Bir kriptografik modülün işletim ortamı modülün doğru şekilde işletilmesi için gerekli olan tüm yazılım, gömülü yazılım ya da donanımdan meydana gelir. İşletim ortamı Değiştirilemeyen, Sınırlı ve Değiştirilebilir işletim ortamı olmak üzere üç türde olabilir [6]. Bu ortamlar;

(1) Değiştirilemeyen işletim ortamı sadece yazılım ya da donanımı içerecek şekilde tasarlanmıştır. Bu ortam, programlanamayan hesaplama platformu ya

da gömülü yazılım modülü ile değiştirilemeyen hesaplama platformunda işletilen bir gömülü yazılımdan oluşur.

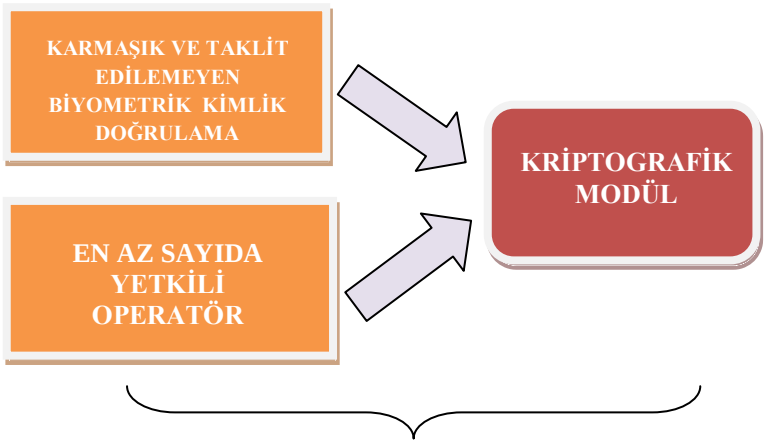
(2) Sınırlı işletim ortamı sadece yazılım ve donanımı içerecek şekilde tasarlanmıştır fakat kontrollü değişikliklere izin verir.

(3) Değiştirilebilir işletim ortamı işlevsellik ekleme, çıkarma, değiştirme için yeniden yapılandırılabilen ve/veya genel maksat işletim sistemi yeteneklerini (örneğin programlanabilir yazılım) içerebilen bir işletim ortamını ifade eder.

Bir sunucu bilgisayara eş zamanlı ve mümkün olduğunca çok sayıda istek gönderilmesi, sunucunun kapasitesinin aşılması sonucunda da hizmet veremez hale getirilmesi ilkesine dayanan hizmet engelleme saldırıları (Denial of Service-DoS) karşısında bir kripto modülü düzgün çalışmaya devam edebilmeli ve sahip olduğu önemli güvenlik bilgilerinin bu saldırılar sonucunda ele geçirilmesine izin vermemelidir.

2.2.3 Fiziksel güvenlik ve personel güvenliği

Fiziki güvenlik mekanizmaları bir kriptografik modüle izinsiz fiziksel girişleri ve modülün izinsiz kullanımını engellemelidir. Fiziki güvenlik gereksinimleri bir kriptografik modülün belirli üç somut örneği için tanımlanır [6]:



Şekil 2.1. İlave fiziksel güvenlik ve personel güvenliği gereksinimleri

(1) Tek yongalı kriptografik modüller bir tek entegre devre yongasının bağımsız modül olarak kullanılabildiği veya fiziksel olarak korunamayan bir koruncak

ya da ürünün bünyesine yerleştirilebildiği fiziki örneklerdir (örneğin tek bütünleşik devre yongalı akıllı kartlar).

(2) Çoklu yonga yerleştirilmiş kriptografik modüller iki veya daha fazla entegre devre yongasının birbirine bağlı olduğu ve fiziki olarak korunamayan bir ürün veya koruncağın bünyesine yerleştirilmiş fiziksel örneklerdir (örneğin genişleme kartı, adaptör).

(3) Çoklu yongalı bağımsız kriptografik modüller iki ya da daha fazla entegre devre yongasının birbirine bağlı olduğu ve tüm bileşenlerin fiziksel olarak korunduğu fiziksel örneklerdir.

Modüle fiziksel giriş denemesindeki kurcalamanın delili ve sıfırlama devresiyle anahtarlar, PIN, şifre vb. kritik bilgilerin sıfırlanması sağlanmalıdır.

Bakım esnasında modüldeki tüm anahtarlar sıfırlanmalıdır. Sıfırlama operatör tarafından ya da otomatik olarak modül tarafından uygulanmalıdır.

Kripto güvenliğinde modülün güvenlik özellikleri ile birlikte operatörün de eğitim ve dikkati önemlidir. Şekil 2.1. modülün ilave fiziksel güvenlik ve personel güvenliği gereksinimlerini ifade etmektedir. Güvenlik risk olasılığını en düşük seviyede tutmak için erişim yetkisi verilen operatör sayısı kısıtlanmalı, mümkün olan en az sayıda kripto operatörü modülü işletmeye yetkilendirilmelidir.

Modüle erişim denetimi iki seviyeli kimlik doğrulaması (gizli parola, fiziksel anahtar/token ve biyometrik özellik) ile sağlanmalıdır. Ayrıca modül erişim için operatörden parmak izi, iris, ses tanıma vb. biyometrik özellikler ile kısa süreli hareketli yüz videosu ya da sabit görüntüyü tanıma özelliği vb. geliştirilmiş güvenlik özellikleri istemelidir. Şekil 2.1.'de gösterildiği gibi modül, erişim için operatörden daha karmaşık ve taklit edilemez/çalınamaz biyometrik özellikler istemelidir.

ISO/IEC 17799:2000 bilgi güvenliğine yönelik tehditleri kaynaklarına göre doğal, teknik, bilinçsiz ve kasıtlı personel kaynaklı olmak üzere dörde ayırmıştır [48]. Doğal kayaklı tehditler deprem, yangın, sel, şiddetli fırtına, kaza ve çevre kirliliğidir. Bu amaçla kriptografik modüller;

(1) Sağlam bir koruncak içerisine monte edilerek depremde gerçekleşen şiddetli sarsıntı sonrası ya da bina enkazı altında kalma durumunda zarar görmeyecek ve düzgün çalışmaya devam edecek şekilde tasarlanmalıdır.
(2) Yangına karşı dayanıklı yanmaz bir koruncak içerisinde yapılanmalı ve yangından zarar görmeyerek düzgün çalışmaya devam edecek şekilde tasarlanmalıdır.
(3) Modül yetkisiz kimselerin eline geçme tehlikesi anında kolay ve hızlı şekilde koruncaktan sökülüp; yakma ya da darbe ile kırıp parçalara ayrılarak imha edilebilecek şekil ve fiziki yapıda olmalıdır.

2.2.4 Girişimsel olmayan saldırılar

Girişimsel olmayan saldırılar bir kriptografik modülü fiziksel olarak değiştirmeden ya da içine sızmadan, içindeki kritik güvenlik parametrelerinin bilgisini ele geçirerek modülü tehlikeye sokmaya çalışır.

Bu kısmın gereksinimleri tek yongalı kriptografik modüllere ve hibrit modüllerin tek yongalı bileşenlerine uygulanabilir olmalıdır [6].

Bir kriptografik modül kritik güvenlik parametrelerini, uygulanabilen tüm girişimsel olmayan saldırılara karşı korumalıdır. Ayrıca azaltma tekniklerinin verimliliği belirlenmelidir.

Kriptografik modül tüm girişimsel olmayan saldırılar ve bu saldırılarla ilgili yetkili ya da onaylı güvenlik fonksiyonları için testten geçmeli ve geçerlilik otoritesince belirlenen gereksinimleri karşılamalıdır.

2.2.5 Anahtarlar

Anahtarlar yetkisiz giriş, kullanım, ifşa, değişiklik ve yer değişikliğine karşı korunmalıdır. Modüldeki açık anahtarlar yetkisiz değişiklik ve yer değişikliklerine karşı korunmalıdır. Ayrıca modüldeki kritik bilgiler (anahtarlar, PIN vb. diğer kritik veriler) operatör tarafından güvenli bir kanal vasıtasıyla modüle girilmelidir. Bu "güvenli devre" anahtarları değiştirme ve çalınmalara karşı korumalıdır.

Elle taşınan anahtarlar hem kriptolanmış hem de gruplandırılmış olmalıdır. Elektronik taşınan anahtarlar ise güvenli kriptografik algoritmalar kullanılarak şifrelenmelidir.

Elle taşınan anahtarlar tek bir anahtar üretim merkezinden kripto birimlerine götürüp teslim etme yöntemiyle, yolda çalınma, kaybolma ve yetkisiz kişilerce imha

girişimlerine karşı fiziksel önlemler alınacak şekilde transfer edilmelidir. Bu yöntem anahtarların söz konusu kayıp, çalınma ve imhalara karşı toplam taşınma süresini azaltmayı ve daha iyi fiziksel korumayı amaçlamalıdır.

2.2.6 Yapılandırma yönetimi

Yapılandırma yönetim sistemi modüldeki kazaen ve yetkisiz değişikliklerle değişiklik (modifikasyon) izlenebilirliğini sağlayan bir sistemdir [6]. Bu sistem bir kripto cihaz/sistemindeki modülün ve bileşenlerinin geliştirilmesi için kullanılmalıdır. Modülü kapsayan her bir konfigürasyon adedinin (kripto modülü, donanım parçaları, modül yazılım bileşenleri, güvenlik politikası vb.) her bir sürümü belirlenmeli ve tek bir kimlik numarasıyla etiketlenmelidir. Sistem kripto modülünü kullanım ömrü süresince her bir konfigürasyon adedinin kimlik ve sürüm ya da revizyonundaki farklılıkları takip etmeli ve muhafaza etmelidir. Ayrıca yapılandırma öğeleri otomatik bir yapılandırma yönetim sistemi kullanılarak yönetilmelidir.

2.2.7 Otomatik kontrol testleri

Bir kriptografik modülün düzgün çalışmasını sağlamak için işletim öncesi otomatik kontrol testleri ve koşullu otomatik kontrol testleri uygulanmalıdır. Tüm testler uygulanmalı ve testten geçme-kalma durumu, harici kontrol ve yöntemler ya da operatör müdahalesi olmadan, modül tarafından saptanmalıdır [6].

İşletim öncesi otomatik kontrol testleri, öncelikle tüm veri çıktılarını veri çıktı arayüzü vasıtasıyla temin eden modüle uygulanmalı ve modül başarılı biçimde testten geçirilmelidir.

Koşullu otomatik kontrol testleri, uygulanabilir (uygun) güvenlik fonksiyon ya da işlemi çalıştırılırken uygulanmalıdır.

Modül düşük işlem modunda işletilirken durum göstergesi sağlamalıdır. Modülün başarısız olan koşullu otomatik kontrol testlerini göstermesi, arzu edilen bir durumdur.

2.2.8 Diğer saldırıların azaltılması

Bu standartta (FIPS 140-3) başka kısımlarda belirtilmeyen saldırılara karşı kriptografik modülün hassasiyeti modül tipine, uygulamaya ve uygulama ortamına

bağlıdır. Bu saldırılar genelde modülün dışındaki kaynaklardan elde edilen bilginin analizine dayanır. Her durumda saldırılar modül bünyesindeki bazı kritik güvenlik parametre bilgilerini saptamayı dener.

Bir kripto modülü standartta tanımlanmayan bir ya da daha fazla özel saldırıyı azaltmak için tasarlanmışsa, modülün destekleyici dokümanları, azaltmaya yönelik tasarlandığı saldırıları numaralandırmalı/sıralamalıdır.

Yukarıdaki gereksinimlere ilave olarak, kripto modüllerinde FIPS 140-3'te tanımlanmayan özel saldırıların azaltılması amaçlandığında dokümantasyon, saldırıları azaltmak ve azaltma tekniklerinin verimliliğini test etmek için kullanılan yöntemleri tanımlamalıdır.

2.3 Güvenlik Hedefleri

Güvenlik gereksinimleri bir kriptografik modülün güvenlik tasarımı ve güvenlik uygulamalarıyla ilgilidir [6]. Bu güvenlik gereksinimleri:

- Onaylı ve izin verilen güvenlik fonksiyonlarını çalıştırmak,
- Kriptografik modüllleri yetkisiz erişimden korumak,
- Kriptografik modüllerin içeriğinin yetkisiz olarak ifşa edilmesini engellemek,
- Kriptografik modüllerin işlem durum bilgisini sağlamak,
- Anahtarların yetkisiz modifikasyonu, değişikliği, eklenti ve silinmesini kapsayan; kriptografik modülün ve algoritmanın yetkisiz ve tespit edilemeyen modifikasyonunu engellemek,
- Onaylı işlem modunda kriptografik modülün doğru çalışmasını sağlamak,
- Kriptografik modülün işlem hatalarını algılamak ve bu hatalar nedeniyle önemli güvenlik bilgilerinin ifşa olmasını engellemek,
- Operatör kaynaklı işletim ve güvenlik hatalarını engellemek [48],
- Her türlü çevre koşullarında modülün düzgün çalışmasını sağlamaktır [48].

3. MATERYALLER VE YÖNTEMLER

Bu bölümde kriptolu cep telefonu (KCT) ve USB kriptolayıcı (USBK), 2. Bölümde anlatılan güvenlik seviyeleri ve mevcut cihazların analizi kapsamında incelenmektedir.

3.1 Kriptolu Cep Telefonu (KCT)

KCT'nin güvenliğine yönelik tehditler ve bu tehditlere karşı güvenlik önerileri bu kısımda açıklanmıştır.

3.1.1 Tehditler

Bu kısımda KCT'te yönelik muhtemel tehdit türleri özetlenmiştir. Bu tehdit türleri yetkisiz erişim, yapısal (fiziksel) bozulma, akıllı kartın kurcalanması, hizmet engelleme (DoS) saldırıları, kötü amaçlı yazılımlar ve kriptanalizdir.

3.1.1.1 Yetkisiz erişim

KCT'ye yetkisiz kişilerin erişmesi halinde içindeki tüm kullanıcı bilgilerine erişim mümkündür. Cep telefonlarında erişim güvenliği PIN kodu ile sağlanırken, şifre ile birlikte taklit edilmesi zor biyometrik özellikler olan parmak izi, yüz ve ses tanıma gibi güvenlik sistemleri sayesinde KCT'ye yetkisiz erişim riski en aza indirilebilecektir. Ancak bunların da taklit edilmesi ya da KCT'nin çalınması ve kaybolması halinde yetkisiz kişilerin KCT'ye erişerek kullanıcı bilgilerini elde etmesi cihaz için bir tehdittir.

Kötü niyetli kimse KCT'yi doğru şifreyle ya da kullanıcı biyometrik özelliklerini taklit ederek çalıştırabilir ve telefondaki verilere erişim sağlayabilir, kötü yazılım yükleyebilir, donanımda değişiklik yapabilir. Ayrıca KCT'nin çalınması ya da kaybolması halinde de yetkisiz erişim mümkündür.

3.1.1.2 Yapısal (Fiziksel) bozulma

Kullanıcı güvenlik özellikleri ve donanımı doğal nedenlerle yapısal (fiziksel) bozulmaya uğrayabilir. Çok soğuk-sıcak havalarda ya da gerilim dalgalanmalarında KCT düzgün çalışmayabilir. Bu olumsuz koşullarda KCT düzgün çalışmadığı gibi güvenlik bilgilerini ya da kullanıcı verilerini kontrolsüz biçimde rastgele yetkisiz cihazlara gönderebilir ve ifşa edebilir.

Türkiye'nin Doğu Anadolu Bölgesinde kış aylarında hava sıcaklığı gündüz -20 C, gece -40 C'ye kadar düşebilmektedir. Aşırı soğuk hava, normal cep telefonlarının donanımına ve ekranına zarar vermekte, tuşların fonksiyonlarını yavaşlatmakta ve telefonların düzgün çalışmasını olumsuz etkilemektedir.

KCT genellikle güvenlik güçleri ve Türk Silahlı Kuvvetleri tarafından kullanılacaktır. Bu nedenle çalışma sıcaklığı -40 C ile +60 C arasında olmalıdır. Ayrıca havaların yağmur ve kar yağışlı olduğu zamanlarda kolay kullanım için KCT dokunmatik değil, Şekil 3.1.'deki gibi klavyeli kullanılacak biçimde tasarlanmalıdır. Ayrıca klavyedeki tuşlar askeri operasyonlarda kullanım esnasında sessizliği sağlamak amacıyla yumuşak ve plastik maddeden yapılmalıdır.

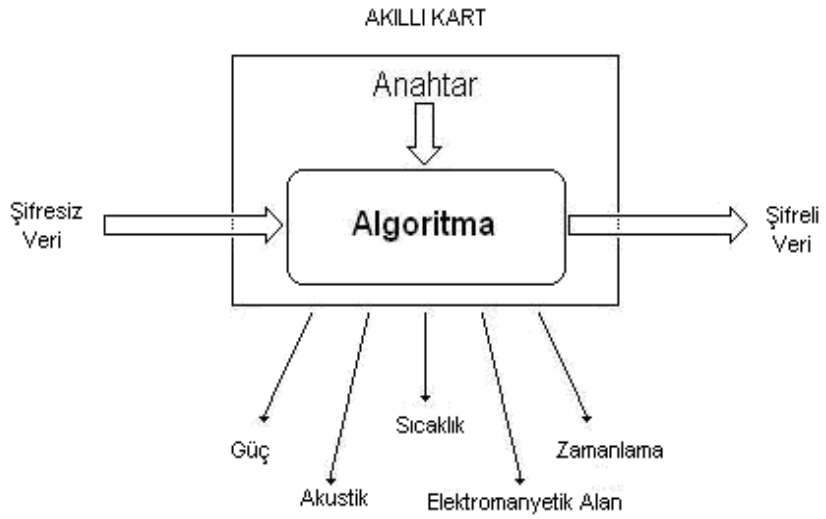
Şekil 3.1. Kriptolu cep telefonu (KCT)

3.1.1.3 Akıllı kartın kurcalanması

Kullanıcı bilgileri ve şifre sadece okunabilir olan bellek (read only memory-ROM) kurcalanarak ifşa edilebilir. ROM'un kurcalanarak içinde saklanan kullanıcı bilgilerinin donanım analisti yetkisiz kişiler tarafından elde edilmesi işlemi diğer bir

tehdit biçimi olarak algılanmalıdır. Burada vurgulamak istediğimiz nokta, şifreleme işlemi için cihaza gömülü bir şekilde gelen algoritma ve bu algoritmanın kullanımı için oluşturulan anahtarın ele geçirilmemesi gerektiğidir.

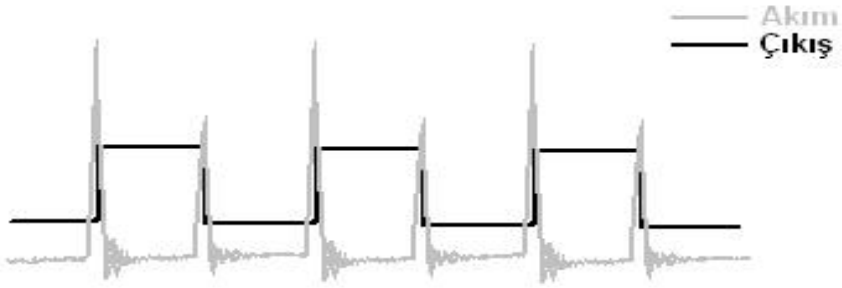
Kriptografik algoritmaların üzerinde koştuğu akıllı kart, beklenen şifreleme ve şifre çözme işlemlerini yaparken, yaptığı işlemle veya işlenen veri ile ilişkili Şekil 3.2.'de belirtilen birtakım çıkışları yan kanal bilgisi [33] olarak ortama vermektedir. Bu çıkışlar kripto anahtarı veya algoritma işlemi ile ilişkilendirilerek anahtar veya algoritma saldırgan tarafından elde edilebilir.



Şekil 3.2. Yan kanal bilgileri

Akıllı kartın çalışması sırasında ortaya çıkardığı güç, elektromanyetik alan, saat darbe sayısı (zamanlama), akustik, ısı gibi çıktılar kullanılarak, algoritmanın işleyişi ile veya işlediği veri ile ilişkilendirilebilir. Böylelikle kriptografik algoritmanın gizli anahtarı elde edilmeye çalışılır.

Akıllı kart üzerinde kriptografik işlemler gerçekleşirken, yapılan işleme ait Şekil 3.3.'teki güç eğrisi ölçümü ile o anda işlenen "1" lerin sayısına ya da "1-0" geçiş sayısına dair bilgi sahibi olunabilir ve KCT'de çalışan kriptografik algoritma elde edilebilir.



Şekil 3.3. Akım değişikliği

Akıllı kart RSA kripto algoritmasında toplama ve çarpma gibi farklı mikroişlemci komutları gerçekleştirilirken entegre devreler farklı miktarda güç tüketirler. Kriptografik algoritma çalışırken güç tüketimi ölçülerek yürütülen işlemlerle güç tüketimi arasında ilişki kurulması ve ölçüm sonuçlarının incelenmesiyle gizli anahtar bitleri elde edilebilir.

Algoritma içerisindeki aşamalarda yürütülen toplama ve çarpma gibi işlem süreleri ile kullanılmakta olan gizli anahtar saldırgan tarafından ilişkilendirilebilir ve böylece gizli anahtar tahmin edilebilir.

Transistörler durum geçişlerinde (0-1, 1-0), yüksek akım çekerler. Akım değişimi bir elektromanyetik alan oluşturur. Dolayısıyla bu yan kanal bilgisi kullanılarak işlenen veri ve işlenen kriptografik anahtar hakkında bilgi sahibi olunabilmektedir. Uygun bir anten düzeneği ile fiziksel bağlantı kurulmadan ve belirli bir mesafeden elektromanyetik alan yan kanal bilgisi akıllı kartın çalışması sırasında toplanabilir. Ayrıca hazırlanan anten düzeneği, akıllı kart üzerinde gezdirilerek belirli noktalara odaklanılabilir.

Akıllı kart üzerinde bulunan belirli noktalara direkt müdahele edilebilir. Çalışma koşulunun ani değişimiyle karttaki bir ya da birkaç flip-flop'un değeri saldırgan tarafından değiştirilerek sistemde hatalı çalışma sağlanabilir. Akıllı kart hataya zorlanarak yanlış bir çıkış değeri vermesi ve elde edilen yanlış çıkış ile doğru çıkış arasında ve algoritma işleyişi arasında bağlantı kurularak anahtar ve algoritma elde edilebilir. Lazer kaynağı kullanımı, gerilim değişikliği yapılması, frekans değişikliği yapılması, sıcaklık ve radyasyon değişikliği gibi işlemlerle akıllı kart hataya zorlanabilir. Saldırgan tarafından içeriği bilinen veri parçası KCT'nin akıllı kart sisteminde hatalı ve hatasız sonuçlar elde etmek üzere işleme sokularak hatalı ve hatasız işlem sonuçları kıyaslanarak anahtarlar elde edilebilir. Örneğin Chinese

Remainder Theorem (CRT) ile gerçeklenmiş RSA algoritması için bilinen Bellcore saldırısı, RSA özel anahtarının elde edilmesini sağlamaktadır [34].

Matematiksel açıdan çok güçlü kriptografik algoritmalar içeren fakat yan kanal analizi'ne karşı yeterli önlem içermeyen akıllı kartların, tasarımdan kaynaklanan zayıflıklarından dolayı koruduğu algoritma ve anahtar bilgilerini ifşa etmesi mümkündür.

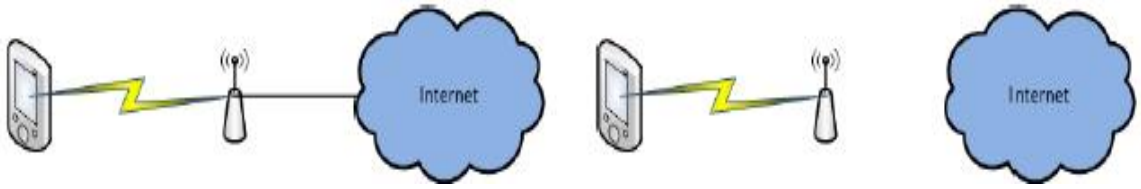
Öneri: Akıllı kartların yan kanal analizi kapsamında test edildiğini ve sertifikalandırıldığını gösteren ve uluslararası alanda geçerliliği olan sertifikasyon, ISO 15408 Ortak Kriterler (Common Criteria) sertifikasyonudur. KCT akıllı kartının tasarımsal zayıflıklardan kaynaklanan yan kanal bilgilerini sızdırmadığı yönünde analiz edilmesi ve yeterli karşı önlemleri içerdiği yönünde sertifikalandırılması gerekmektedir.

3.1.1.4 Hizmet engelleme saldırıları (Denial of service-dos)

KCT internet üzerinden hizmet engelleme saldırılarına (Denial of Service-DoS) maruz kalabilir ve düzgün çalışamaz hale gelebilir.

Günümüzde özellikle kurumların ağa bağlı bilgisayarlarının sıkça karşılaştığı saldırılardan biri de hizmet engelleyici saldırılardır. DoS saldırıları, kullanıcıların belirli bir web sitesi, web servisi, bilgisayar sistemi veya herhangi bir ağa bağlı elektronik cihazı istenilen şekilde kullanmalarını engelleyen saldırılardır [5]. Sisteme düzenli ve sürekli olarak saldırılması sonucu sistem hizmet veremez hale gelir ve sunucular hizmet dışı kalabilir. Hedef seçilen bir akıllı telefonla ağ erişim noktası arasındaki trafik, sahte adres çözümleme protokolü (ARP) yanıt paketleri kullanarak kesilebilir. SYN paketleri gönderilen akıllı telefon çok yavaşlayarak ağ erişim noktasıyla erişimi kesilebilir ve yeniden başlatma ihtiyacı duyabilir [30,31]. Bu saldırıların bir örneği de Temmuz 2009'da Güney Kore ve ABD'de şebeke yavaşlatma biçiminde gerçekleşmiştir. Saldırganlar kablolu ve kablosuz binlerce cihaza komut vererek defalarca bir siteyle bağlantı kurmak, erişimi yavaşlatmak, daha da kötüsü siteyi çökertmek için telefon sinyalleri ve cihazlarını planlarının bir parçası olarak kullanmışlardır. Masum kullanıcıların telefonlarına yükleyecekleri bir uygulama geliştirilmiş ve bu uygulama önceden planlanan saldırı komutunu başlatmıştır [32].

KCT, aslında kriptografik modüle sahip bir cep telefonu olduğundan söz konusu saldırılara açık bir cihazdır. Böyle bir saldırı durumunda KCT düzgün çalışamayabilir ya da hiç çalışmayabilir. Burada çalışmama ile anlatılmak istenen nokta, şifreli haberleşmenin gerçekleşememesidir. Saldırganlar bu saldırıyı farklı şekillerde uygulayabilir. Örneğin internet ağı olmayan otel, hava alanı, kafe gibi bir yerde her hangi bir bilgisayarla Şekil 3.4.'teki gibi sahte kablosuz erişim noktası tesis edilebilir ve ortamda bulunan akıllı telefonların internet ağı bulunmayan bu sahte kablosuz internet ağına otomatik bağlanmaya çalışması sonucunda kurbanlar internet hizmetinden mahrum kalabilir [15].



(a) Gerçek Erişim Noktası (b) Sahte Erişim Noktası

Şekil 3.4. Sahte kablosuz erişim noktası ile hizmet engelleme (DoS) saldırısı.

Saldırganların akıllı telefonların kontrolünü ele geçirerek bu telefonlarla internet üzerinden veri paketlerini şebekelere göndermesi ve bu aşırı yüklenme sonucunda şebekeyi çalışmaz hale getirmeleri [16], solucan adı verilen kötü yazılımların SMS'lerle telefon şebekesine gönderilerek hizmet engelleme şartlarının oluşturulması [17], çok sayıda akıllı telefona eş zamanlı olarak kötü yazılım gönderilmesi, Şekil 3.5.'teki gibi hedef akıllı telefona sürekli istek göndererek bataryasını hızlı biçimde bitirmeyi amaçlayan [10,30] saldırılar yaygın DoS saldırılarıdır.

Şekil 3.5. Batarya tüketme amaçlı DoS saldırısı

3.1.1.5 Kötü amaçlı yazılımlar ve kriptanaliz

Kötü yazılım olarak bilinen ve aşağıdaki örnekleri kapsayan 3'üncü parti uygulamaları bilgisayar sistemlerine zarar verme amacı güdecek biçimde tasarlanmışlardır [19]:

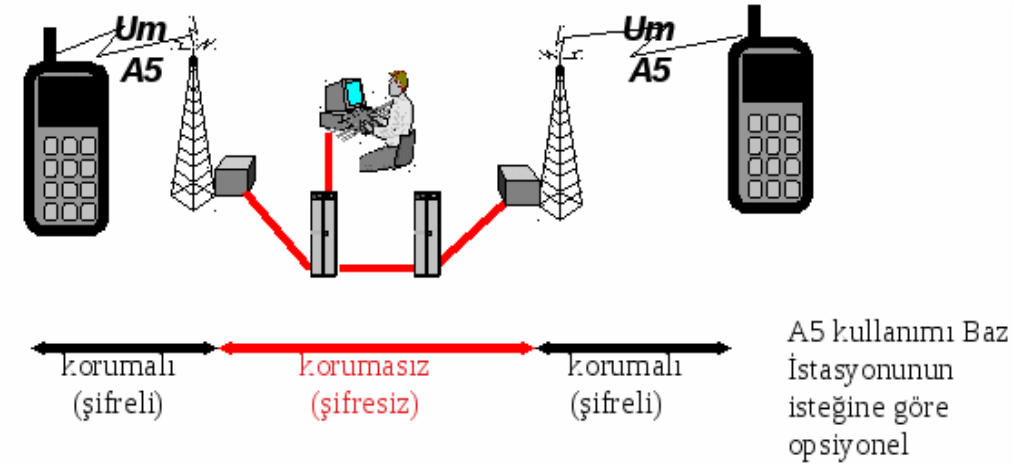
- **Virüs**: kendi kendini bilgisayardaki uygulamalara kopyalayarak sisteme zarar veren ve sistemi kullanılmaz hale getiren kötü yazılımlardır.
- **Truva atı:** faydalı gibi görünen (ekran koruyucu vb.) ancak içerisinde zararlı kodlar içeren ve işletim sistemine zarar veren uygulamalardır.
- **Solucan:** ağlarda kendi kendini kopyalayarak yayılan potansiyel olarak bilgisayar sistemlerine zarar veren program ya da uygulamalardır.
- **Casus yazılım (Spyware):** kullanıcı izni olmadan kullanıcı hareketlerini ve kişisel bilgilerini kaydeden ve saldırgana gönderen yazılımlardır [20].

Kötü amaçlı yazılımlar çoğunlukla kullanıcılara ait kimlik bilgileri, kredi kartı ve banka hesap numarası gibi kolaylıkla paraya dönüştürülebilen bilgilerle bilgisayar yazılımı, finansal algoritmalar ve ticari sırlar gibi fikri hakları çalma gibi amaçlarla kullanılır [9]. Kullanıcıdan izin almadan kötü niyetli kişilerce internet üzerinden KCT'ye kötü amaçlı yazılımlar yüklenerek cihaz bozulabilir, işlevsel özellikleri durdurulabilir, içindeki bilgi ve verilere saldırgan tarafından erişilebilir [18].

Yıllardır bir çok saldırgan dinleme, yazılım çökertme ya da başka saldırılar amacıyla cep telefonlarının yazılımlarını sömürmektedir [3]. Bir kullanıcı web listeleyicideki zayıflığı kullanan ve kötü niyetle tasarlanan bir linke tıklayarak saldırı başlatabilir. Ayrıca arka planda çalışan zayıf bir uygulama ya da ağ hizmeti olan cihazı kullanarak pasif olarak saldırıya maruz kalabilir [4]. Cabir adlı solucan yazılım sürekli olarak bluetooth taraması yapar ve bataryanın tükenmesine neden olur. CommWarrior ise bluetooth üzerinden kendini kopyalayıp rehberdeki numaralara rastgele MMS olarak gider ve otomatik olarak SMS/MMS'lere yanıt verir. Ayrıca kendini hafıza kartına kopyalar ve telefondaki diğer dosyalara girer. WinCE.Infomeiti solucanı kendini hafıza kartına kopyalarak yayılır. Ayrıca gizli bilgileri uzaktaki bir siteye gönderir ve güvenlik ayarlarını azaltır [18].

KCT'ye kötü yazılımlar internet ağından ulaşabileceği gibi kötü niyetli kişilerce bluetooth ve Wi-Fi ağları yayımlanarak KCT'nin bu ağlara otomatik bağlanması veya KCT kullanıcısını kandırarak bu ağlara manuel bağlanması ve bunlar üzerinden de kötü amaçlı yazılım içeren dosyaların cihaza gönderilmesi şeklinde gerçekleşebilir. Yine bluetooth ayarları doğru yapılmadığında adres defteri, çağrı detayları ve daha fazlası hedeflenen telefondan çalınabilmektedir [50].

1988 yılından bugüne kadar kullanılan, 64-bitlik şifreleme temeline dayanan cep telefonu ağı şifreleme algoritması A5/1 gizlilik algoritması, 5 aylık bir çalışma sonrasında Alman bilgisayar mühendisi Karsten Nohl liderliğindeki ekipte görevli 24 kişi tarafından kırılmıştır [50]. Şekil 3.6.'da görüldüğü gibi cep telefonu ağı şifreleme algoritması A5/1, cep telefonu cihazı ile baz istasyonu arasında şifreleme gerçekleştirmekte, aradaki haberleşme safhası ise şifresiz gerçekleşmektedir. Anlaşılacağı üzere cep telefonunda gizlilik dereceli haberleşme için A5/1 güvenli değildir. 3. nesil cep telefonlarında kullanılan yöntem A5/3 olarak isimlendirilmiştir. Ancak bu sistemin de güvenlik problemleri olduğu bilinmektedir.



Şekil 3.6. GSM ağında A5/1 ile şifreleme

3.1.2 Güvenlik önerileri

Bu bölümde KCT'nin güvenlik gereksinimleri incelenmekte ve cihaza yönelik güvenlik önerileri yer almaktadır.

3.1.2.1 Kimlik doğrulama ve deneme sayısı

Kimlik doğrulama, kriptografik modül içeren cihaza erişmek isteyen kullanıcının yetkili kullanıcı olup olmadığını denetleyen mekanizmadır [6]. Kimlik denetimi sayesinde KCT'ye erişmeye ve cihaz üzerinde bazı işlemleri gerçekleştirmeye yetkili kullanıcıdan başka yetkisiz şahısların cihazı açma ve işlem yapması engellenir.

KCT açılırken kullanıcıdan her defasında kimlik doğrulama maksadıyla şifre ve buna ilave karmaşık ve taklit edilemeyen biyometrik özellik (parmak izi, yüz/ses, kısa süreli yüz videosu tanıma vb.) istediği takdirde iki seviyeli kimlik doğrulaması [13] sağlanmış olacaktır. KCT SMS, MMS ve e-posta gönderimleri gibi işlemlerde ise rol tabanlı kimlik doğrulama mekanizmasını devreye sokmalıdır [6]. Bu hallerde KCT, kullanıcısından kimlik bilgileri ve biyometrik özelliklerini istemeli, aksi takdirde veri haberleşmesi yapmamalıdır.

Öneri: KCT, kullanıcının üç defa başarısız kimlik doğrulama denemesinde kullanıcı şifre ve anahtarlarını silmelidir.

3.1.2.2 Kriptografik algoritmalar

Gelişmiş şifreleme algoritması (Advanced Encryption Standard-AES) elektronik verileri korumak amacıyla kullanılabilen Federal Information Processing Standard (FIPS) onaylı bir şifreleme algoritmasıdır [7]. Amerikan hükümeti tarafından kabul edilen AES, uluslararası alanda da şifreleme standardı olarak kullanılmakta ve Şekil 3.7.'deki TÜBİTAK tarafından üretilen MİLCEP kriptolu cep telefonu, ses ve veri haberleşmesini bu onaylı algoritma ile şifrelemektedir. AES algoritması şifreleme ve çözümleme yapabilen simetrik bir blok şifreleyicidir. 128, 192 ve 256 bitlik anahtarlarla şifreleme ve şifre çözme yapabilir. Uluslararası standartlar ve TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) Kamu Sertifikasyon Merkezi tarafından önerilen algoritmalar ve en düşük anahtar boyları Çizelge 3.8.'de gösterilmiştir [36].

Şekil 3.7. TÜBİTAK üretimi MİLCEP kriptolu cep telefonu

Çizelge 3.8. Önerilen Algoritma Listesi [36]

Algoritma Tipi	**Algoritma**	**Anahtar Boyu (En az)**	**Önerilen Son Kullanım Tarihi**	**İlgili Standart**
Elektronik İmza	Rivest, Shamir, Adleman (RSA)	2048 bit	31.12.2030	PKCS#1 sürüm 2.1, ETSI TS 101733 (CADES), ETSI TS 101903 (XADES)
Elektronik İmza	Eliptik Eğri Elektronik İmzalama Algoritması (ECDSA)	256 bit	31.12.2030	FIPS 186-3, ETSI TS 101733 (CADES), ETSI TS 101903 (XADES)
Asimetrik Şifreleme	RSA	2048 bit	31.12.2030	PKCS#1 sürüm 2.1
Anahtar Paylaşımı	DH	2048 bit		
Anahtar Paylaşımı	Eliptik Eğri Diffie-Hellman Anahtar Paylaşımı (ECDH)	256 bit	31.12.2030	NIST SP 800-56A
Simetrik Şifreleme	Gelişmiş Şifreleme Standardı (AES)	128 bit	31.12.2030	FIPS 197, Çalışma tipi : NIST SP-800-38A, CBC Mode
Özet Alma	Güvenli Özet Fonksiyonu (SHA-512)	-	31.12.2030	FIPS 180-3

KCT'de telefon görüşmesi, e-posta ve SMS/MMS gönderimi, görüntülü görüşme, bluetooth ile dosya gönderimi, hafızada ses/veri/görüntü/video saklama işlemleri şifrelenebilmelidir. Haberleşme, gizlilik derecesine [51] göre farklı anahtar boylarıyla şifrelenerek gerçekleştirilmelidir. İfşa olması durumunda mili güvenlik ve çıkarlarımıza yaşamsal zarar verecek, yabancı bir devlete fayda sağlayabilecek ve güvenlik bakımından olağanüstü sonuçlar doğurabilecek bilgi ve belgeleri kapsayan

“çok gizli” gizlilik dereceli haberleşme 256 bitlik anahtarla şifrelenirken; ifşa olması durumunda mili güvenliğe, ülkenin saygınlık ve çıkarlarına büyük zararlar verebilecek, diğer taraftan yabancı bir devlet için fayda temin edebilecek özellik taşıyan bilgi ve belgeleri kapsayan “gizli” haberleşme ve ifşa olması halinde milletimizin saygınlık ve çıkarlarına zarar verebilecek veya bir şahsın zarar görmesine neden olabilecek nitelikteki “özel” gizlilik dereceli haberleşme KCT tarafından 192 bitlik anahtarla şifrelenmelidir. Çok gizli, gizli ve özel gizlilik derecesine sahip olmayan, ancak bilmesi gerekenler dışındaki kişilerin bilmesinin istenmediği bilgi ve belgeleri kapsayan “hizmete özel” gizlilik dereceli haberleşme ise 128 bitlik anahtarla şifrelenmelidir. Ayrıca KCT tarafından haberleşme öncesi kullanıcıya hangi gizlilik derecesine göre şifreleme yapılacağı sorulmalıdır.

KCT Kriptolu görüntülü görüşmeyi Skype, Tango vb. görüntülü görüşme uygulamalarıyla gerçekleştirmek yerine, KCT’nin kullanıldığı kurum personelinin birbiriyle güvenli olarak görüntülü görüştüğü ortak bir video konferans uygulaması üzerinden gerçekleştirmeli, bahsi geçen internet uygulamalarının güvenlik riski oluşturacağı göz önünde bulundurularak cihaz bu uygulamalara uyumlu olmamalıdır.

KCT ile SMS gönderme işlemi sadece şifreli yapılabilmeli, KCT kullanıcısı şifresiz SMS göndermek istediğinde başka bir cep telefonu kullanmalıdır. Bu şifreli SMS uygulamasından maksat KCT kullanıcısının yanlışlıkla gizli verileri yetkisiz kişilere mesajla göndermesini engellemektir. Ayrıca daha önce gönderilen şifreli bir metin aynen şifresiz şekilde gönderildiği takdirde, bu iki veri yetkisiz kişilerce elde edilip her iki verinin (şifreli ve şifresiz metin) ilişkilendirilerek anahtar ve algoritmanın elde edilmesi sağlanabilir.

KCT içerisinde bir akıllı kart bulunur ve şifreleme/şifre çözme işleminde milli algoritma veya AES, imzalama işleminde ECDSA e-imza algoritması ve özetleme için SHA serisi kullanılır. SHA serisi özetleme algoritmalarının belli koşullar altında güvensiz olduğu akademik camia tarafından gösterildiğinden, yeni özetleme algoritması standardı olan SHA-3 (Keccak) kullanılması önemlidir. Her oturum için ECDH (Elliptic Curve) ve TRNG (Gerçek Rasgele Sayı Üreteci) kullanılarak yeni bir anahtar oluşturulur ve oturum sonunda silinir. Simetrik şifreleme için 128, 192 ya da 256 bit uzunluğunda anahtar boyuna sahip AES kullanılmalıdır [8]. Donanımsal şifreleme sağlayan OMAP5912 tabanlı işlemci, C++ tabanlı yazılım (Embedded Linux), SCIP (Secure Communications Interoperability Protocol) ve buna uygun cihazlarla çalışabilme özelliklerine sahip olmalıdır.

Unutulmamalıdır ki FIPS [6] onaylı algoritmalar sürekli değişim ve gelişim içindedir. Bu nedenle KCT'de kullanılmasını istediğimiz AES ve SHA-3 algoritmaları, gelecek dönemde kripto sistemlerindeki gelişmeler sonucunda yerini daha dayanıklı ve farklı anahtar boylarındaki algoritmalara bırakacağından, KCT bu değişime uyumlanabilmeli, cihaz değişikliğine gitmeden yeni algoritmaları kullanabilmeli ve ayrıca milli algoritmaları içinde barındırabilecek bellek ve işlemci özelliklerine sahip olmalıdır.

3.1.2.3 Kötü yazılımlar ve dos saldırılarından korunum, işletim sistemi güvenliği

KCT mobil işletim sistemine sahiptir. İşletim sistemi, donanımı kontrol eden ve bazı fonksiyonları uygulayan yazılım birimidir. Mobil işletim sistemleri akıllı telefon, tablet PC, cep telefonu ve mobil medya player gibi mobil cihazlarda kullanılır. Akıllı telefonlar kişisel bilgisayarlar ve dizüstü bilgisayarlardaki birçok işlevi yerine getirebilse de, mobil işletim sistemleri enerji ve özel donanım gereksinimleri gibi nedenlerden dolayı kişisel bilgisayarlardaki işletim sistemlerinden farklılıklar gösterir [10,11].

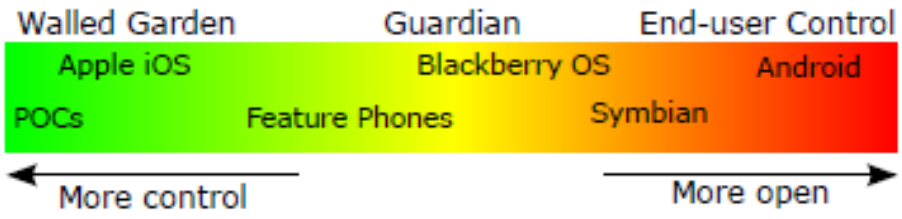
Ağa bağlı cihazlara yapılan saldırılar karşısında karşı yazılım/programlar ile güvenlik duvarı uygulamasının yetersiz kalmaya başlamasıyla, kod ile işlevselliğin ve yazılım güvenliğinin artırılması ihtiyacı doğmuştur [23].

İnternet kaynaklı yazılım uygulamaları, yayılım hızı ve karmaşıklığı ile doğru orantılı olarak, karşılaşılan en yaygın güvenlik riskleridir [21]. Cep telefonları da mutlaka bir ağa bağlı olan cihazlardır. Bu ağ normal olarak cep telefonu ağı, fakat çoğunlukla da kablosuz internet erişim noktası ya da cep telefonu ağı üzerinden internet ağı veya bluetooth ağı olabilir. Farklı türlerdeki bu ağlar saldırı yüzey alanını da bir hayli artırır [22]. Bu risklere karşı KCT virüs tarayıcısına, kötü yazılımları tespit eden yazılımlara ve güvenlik duvarına sahip olmalıdır. KCT şehirlerarası otobüs, hava limanı, terminal, kafe gibi toplu bulunan yerlerde kötü niyetli kişilerce tesis edilecek Wi-Fi ya da buralarda bir cihazın açacağı bluetooth ağına otomatik bağlanmamalı, KCT ortamda böyle bir ağ tespit ettiğinde mutlaka kullanıcısını uyarmalıdır.

KCT bir akıllı telefon olarak tasarlandığından mobil işletim sistemi de kötü yazılımların saldırılarına sıkça maruz kalabilecek, faydalı ve yasal görünen yükleme istekleri ile karşı karşıya kalacaktır. Bu kötü yazılımlara karşı KCT koruma

sağlamalı, kullanıcısına yazılım yükleme isteklerini ekranında göstermeli, kullanıcının izni olmadan telefona yazılım yüklenmesine izin vermemelidir.

Akıllı telefonların mobil işletim sisteminin ya da yazılım yükleme ve yönetiminde üretici firmanın sahip olduğu kontrol seviyesine göre 3 farklı yazılım yükleme modeli vardır [24]. Şekil 3.9.'da belirtildiği üzere, üretici firmaya en fazla kontrol yetkisi veren model The Walled Garden modelidir. Bu telefonlarda kullanıcı sadece onay verilen yazılımları yükleme yetkisine sahiptir. Akıllı olmayan eski tip cep telefonları, Apple IOS işletim sistemine sahip telefonların dahil olduğu bu modeller kötü yazılımlara karşı daha güvenlidir. End-user kontrol modelinde ise üretici firmanın yazılım üzerinde hiçbir kontrolü olmayıp yükleme işleminde tüm kontrol kullanıcıdadır. Android işletim sistemine sahip telefonları örnek gösterebileceğimiz bu modelde kötü yazılımlara karşı cihazı koruma sorumluluğu kullanıcıdadır. Blackberry ve Symbian işletim sistemleri ise yazılım yükleme yetkisinde Guardian modeli adı verilen orta seviye grupta yer almaktadır.



Şekil 3.9. Mobil işletim sistemlerinde yazılım yükleme yetkileri [24]

Anti-virüs ve bilgisayar güvenliği şirketi F-Secure, 2013 yılının ilk çeyreğinde (Ocak, Şubat, Mart) mobil işletim sistemlerinin aldığı tehditleri bir raporla sunmuştur [12]. Çizelge 3.10.'daki rapora göre 2013 yılının ilk çeyreğinde mobil işletim sistemleri için toplam 149 tehdit tespit edilmiştir. Android 136 tehdit, Symbian ise 13 tehdit almıştır. Blacberry, IOS ve Windows Mobile işletim sistemlerine ise tehdit tespit edilmemiştir.

Çizelge 3.10. Mobil işletim sistemleri tehdit raporu (F-Secure, 2013 Ocak-Şubat-Mart)

F-Secure Mobil İşletim Sistemleri Tehdit Raporu (2013 Yılı İlk Çeyreği)	
Mobil İşletim Sistemi	**Tehdit Sayısı**
Android	136
Symbian	13
Diğerleri (iOS, Blackberry, Windows Mobile)	0

Bu araştırmadan Android'in, Apple iOS, Blacberry ve Windows Mobile işletim sistemlerine göre tehditlere daha açık olduğu, ayrıca yazılım güvenliği açısından da kullanıcısına fazla yetki vermiş olması nedeniyle sakıncalarının bulunduğu anlaşılabilir. Ayrıca Apple, virüslü akıllı telefona uzaktan erişip zararlı uygulamaları silme yetkisine sahiptir [35]. Şu anki araştırmalara göre KCT'de Android yerine başka bir işletim sisteminin kullanılması daha güvenlidir [12,24].

Mobil işletim sistemini veya telefonu hizmet veremez hale getirmeyi amaçlayan tehdit türlerinden biri olan DoS saldırılarına [5] karşı KCT dirençli olmalıdır. DoS saldırıları uzun zamandır var olan ve sadece mobil cihazlara yönelik olmayan bir saldırı türüdür. Bu saldırılar bir servisi ya da cihazı kullanıcısı için kullanılamaz hale getirmeyi amaçlar. Çok miktarda yığın trafiğini ağ üzerinden host sisteme gönderme ve böylece sistemi hizmet dışı bırakma şeklinde yapılan bir saldırıdır. Normal bir bilgisayara ya da sunucuya saldırı düzenlemek için pek çok kaynağa ihtiyaç duyulurken bir akıllı telefona, kısıtlı donanımından dolayı, sadece bir saldırganın DoS saldırısı onu kullanım dışı bırakmak için yeterlidir.

Baskın (flood) ve DoS saldırıları KCT'yi tahrip amaçlı en tehlikeli yöntemlerdir. Bu saldırılar ayrı ayrı ya da organize halinde uygulanabilir. Bu nedenle KCT'nin bu saldırılardan korunması için anti-virüs yazılımı kullanılmalı ve söz

konusu güvenlik yazılımı tehlikeli ağ bağlantılarını engelleyen güvenlik duvarı içermeli [38], arama ve SMS filtreleme/engelleme [37] uygulaması ile KCT'yi DoS vb. saldırılardan ve kötü amaçlı yazılımlardan koruyabilecek özellikte olmalıdır.

3.1.2.4 Kurcalama koruması

Kurcalama algılaması, kriptografik modülün fiziksel güvenliğini tehlikeye sokacak bir girişimin KCT tarafından otomatik olarak belirlenmesidir. Kurcalama delili ise kriptografik modülün fiziksel güvenliğini tehlikeye sokacak bir girişim yapıldığını gösteren harici bir göstergedir. Bu kurcalama delili, kurcalamayı KCT'nin ekranında gösterge şeklinde kullanıcıyı uyarmalıdır. Kriptografik modüle yukarıda belirtilen girişimlerin yapıldığı modül tarafından tespit edildiğinde otomatik olarak verilen tepkiye (kullanıcı bilgilerinin silinmesi, cihazın kendini kapatması vb.) kurcalama tepkisi adı verilir [6,26].

KCT'ye fiziksel giriş denemesindeki kurcalamanın delili ve sıfırlama devresiyle PIN, şifre, kullanıcı bilgileri vb. kritik bilgilerin (milli şifreleme algoritması, gizli anahtar, milli anahtar oluşturma algoritması, vb.) sıfırlanması sağlanmalıdır. KCT'nin donanım parçaları ya da kapağı söküldüğünde KCT aynı şekilde bu bilgileri silmelidir.

3.1.2.5 Çalınma ve kaybolmaya karşı uzaktan erişim, alarm ve GPS

Kayıp/çalınma durumunda uzaktan erişimle KCT'deki veriler silinebilmelidir. Yer tespiti amacıyla uzaktan etkinleştirilen yüksek sesli alarmı bulunmalıdır. Ancak ülkemiz tamamen milli bir uydu teknolojisine sahip olmadığından halen küresel konum bilgisi için ABD'nin uydularından yararlanılmaktadır. KCT'ye verilecek Global Positioning System (GPS) özelliği ile sadece istenen şahıslar değil, yetkisiz şahıslar da cihazın konumunu bilebilecektir. Bu nedenle KCT'de GPS özelliği kesinlikle bulunmamalıdır. İleriki yıllarda ülkemizin % 100 milli imkanlarla üreteceği bir uyduya sahip olması durumunda, KCT'ye kazandırılacak bir GPS sayesinde düzgün şekilde çalışabileceği coğrafi koordinatlar kullanıcı tarafından tanımlanabilmeli, cihaza önceden kullanıcı tarafından tanımlanan coğrafi koordinatlar dışında KCT düzgün çalışmamalı, böyle bir durumda KCT'nin yetkisiz kişilerin elinde olabileceği ihtimaline karşı cihaz kullanıcı verilerini silmeli ve kendini kilitleyerek içindeki verilere erişimi engellemelidir.

3.1.3 Diğer hedefler

3.1.3.1 Diğer haberleşme ağları

KCT'nin özellikle Türk Silahlı Kuvvetleri (TSK) tarafından gizlilik dereceli haberleşme amacıyla kullanılacağı değerlendirilmektedir. TSK'nın Taktik Saha Muhabere Sistemi (TASMUS) [27] ve entegre muhabere sistemi (TAFICS) altyapısı sayesinde halen TSK birlikleri gizlilik dereceli haberleşmesini telli ve telsiz haberleşme sistemlerinden kriptolu olarak yapabilme yeteneğine sahiptir. KCT bu altyapıya entegre olabilmeli, bahsi geçen altyapılara güvenli askeri bölgelerde kablosuz ve kablolu bağlanarak bu altyapı üzerinden emniyetli ses/veri haberleşmesi yapabilmelidir. Ayrıca KCT, kriptolu görüntülü haberleşme sağlayan emniyetli terminallerle [28] kriptolu olarak haberleşebilmelidir.

3.1.3.2 KCT-PC bağlantısı

TÜBİTAK tarafından üretilmesi planlanan MİLCEP K2 [39] kriptolu cep telefonu, PC bağlantılı olarak da kullanılabilmektedir. Bu bağlantı bir kablo ile gerçekleştirilmektedir. PC'lerdeki klavye sayesinde kriptolu mesaj alışverişinin daha kolay yapılabilmesi amacıyla KCT, PC'ye kablolu ve/veya kablosuz bağlanabilmelidir. Bu bağlantı üzerinden KCT kriptolu mesaj alışverişi ve PC monitöründe kriptolu görüntülü görüşme yapabilmelidir. PC'ye kablosuz bağlanma özelliği, ilave bağlantı kablosu ihtiyacını ortadan kaldırarak KCT'nin askeri alanda kullanımını kolaylaştıracaktır.

3.1.3.3 Sosyal ağlar

İnternet ortamında farklı amaçlarla kullanılan facebook, twitter vb. sosyal paylaşım siteleri bulunmaktadır. Bu siteler anlık ileti, video ve fotoğraf paylaşımı,fotoğraf albümü oluşturma, kişisel bilgileri içeren profil oluşturma, iş, eş ve arkadaş bulma, iş bulma, reklam gibi hizmetler sunmaktadır.

İnternet kullanıcılarının kişisel bilgileri Amerika Birleşik Devletleri'nde bulunan şirketlerin fiziksel ve yazılımsal güvenlikle koruduklarını teyit ettikleri sunucularda saklanmaktadır. Bu bilgilerin yasadışı olarak 3. kişilere satılması hususu Amerika Birleşik Devletleri mahkemelerinin kapsamına girmektedir [29].

Örnek olarak Facebook sosyal paylaşım sitesinde yer alan yer bildirimi özelliği sayesinde mobil cihazın yeri kullanıcı tarafından bildirilmektedir. Bu siteler faydalı yönlerinin yanında kişisel bilgilere kötü niyetli kişilerin erişmesine yol açabileceği gibi, yer tespiti ve daha birçok tehlikeyi beraberinde getirebilecektir.

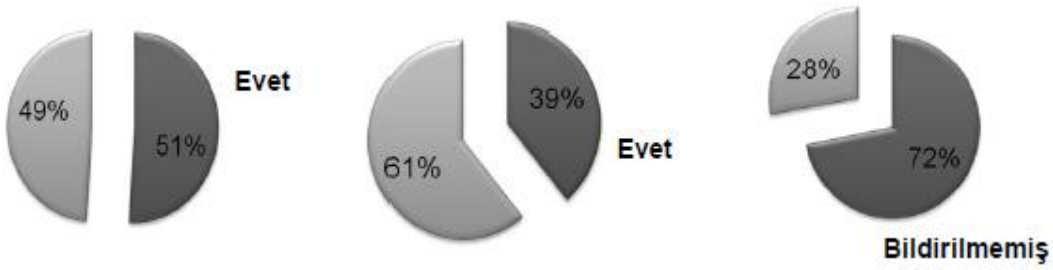
KCT'nin kritik ve yüksek mevkilerde bulunan şahıslarca gizlilik dereceli haberleşme maksadıyla kullanılması planlanmaktadır. Sosyal ağlara erişim ve bu ağların kullanım sorumluluğunun tamamen kullanıcıya bırakılması halinde kötü niyetli kişilerce KCT ve dolayısıyla kullanıcısı hem bilgi güvenliği, hem de can güvenliği açısından tehlikeye düşebilecektir. Bu nedenle KCT'nin facebook, twitter vb. sitelere erişimi bir güvenlik yazılımı ile engellenmeli, seçim kullanıcıya bırakılmamalıdır.

3.2 USB Kriptolayıcı (USBK)

USBK Şekil 3.11.'deki gibi, bir harici disk ya da USB belleğe veri gönderdikten sonra kullanıcısına bu veriyi koruma imkanı sağlayan entegre bir sistemdir [40]. USBK'nin bileşenleri veri transferi esnasında şifreleme ve şifre çözme işlemlerini sağlayan özel bir donanımla entegredir. USBK aktifleştirildiğinde ve başlatıldığında yetkili kullanıcı, veriyi 128 ya da 256 bitlik anahtar ile AES algoritmasını kullanarak formatlanmış bir diske şifrelenmiş bir şekilde transfer eder. Yetkili kullanıcı aynı zamanda diskteki şifreli verinin şifre çözme işlemini de yapabilir.

Şekil 3.11. USBK cihazı

2008 yılında 155 milyon USB bellek satılmış ve 2009 yılında bu rakam 222 milyona ulaşmıştır [41]. Ponemon Institute 2009 araştırma raporuna göre USB belleklerde gizli bilgi kullanımı ve bilgi kayıpları Şekil 3.12.'de verilmektedir.



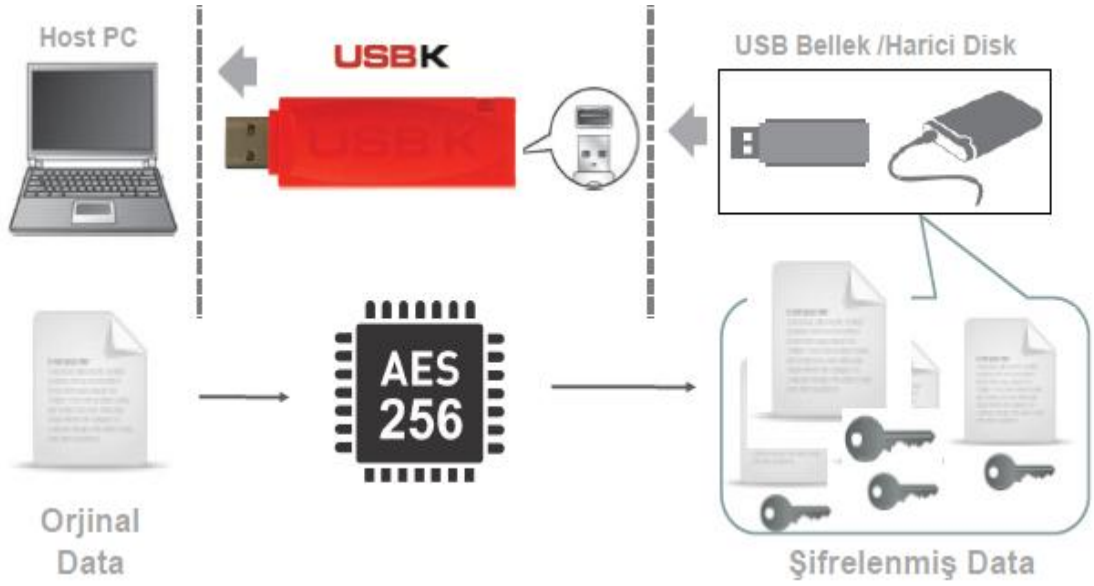
USB belleklere gizli bilgilerin aktarılması | Data ile birlikte kaybedilmesi | Kaybedilen belleklerin hemen bildirilmesi

Şekil 3.12. USB belleklerde gizli bilgi kullanımı ve bilgi kayıpları

USBK'nin temel özelliği, üzerinden transfer edilen verileri şifrelemek ve şifre çözmek olduğundan dolayı, USBK kullanıcıları sınırlı bir disk hacmiyle kısıtlanmamış, aksine kullanıcılar USBK'yi kendisine takılabilen herhangi bir USB bellek ve harici bellekle de kullanabilmektedir. Ayrıca USBK şifrelenmiş verinin transfer edilmek üzere alındığı host sistemin işletim sistemine bağımlı değildir. USBK host sistemle Küçük Bilgisayar Sistem Arayüzü (KBSA) ile iletişim sağlar. Host sistemdeki bir uygulama, kullanıcı ile KBSA arasında arayüz görevi yapar. Host sistemle USBK arasındaki bu tür iletişim, işletim sistemine olan bağımlılığı ortadan kaldırır.

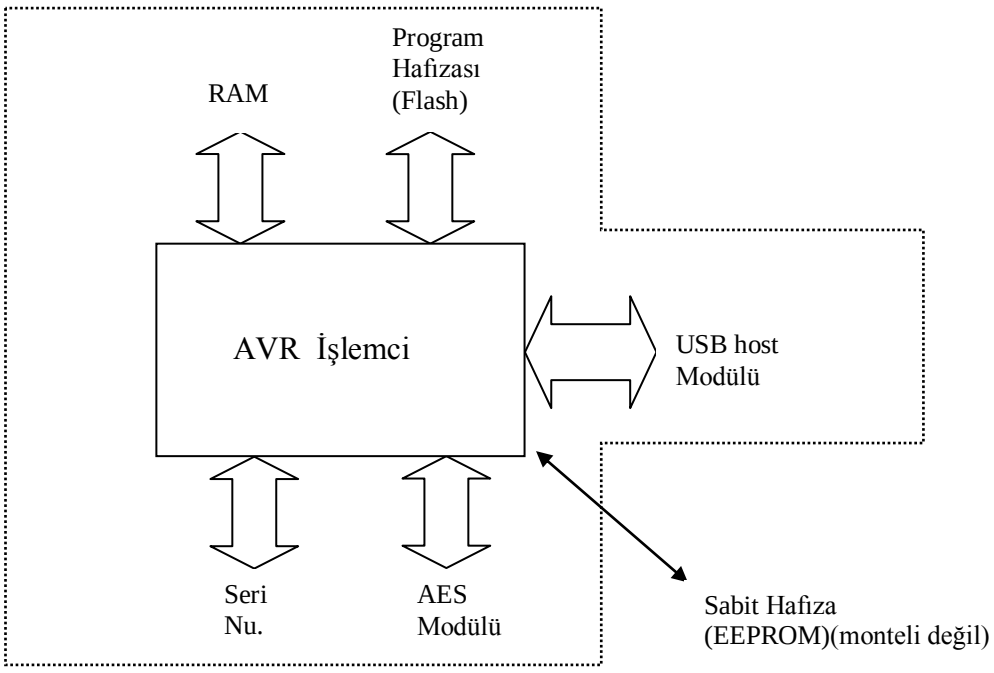
USBK'nin başlangıç ayarları (ilklendirme) ve aktivasyon işlemleri esnasında yetkili kullanıcı, veriyi 128 ya da 256 bitlik AES transfer anahtarıyla şifreleyerek, tercihen, formatlanmış bir diske transfer edebilmektedir. Ayrıca yetkili kullanıcı, diskteki şifreli dosyaların şife çözme işlemini de yapabilmektedir.

Kullanıcı, USBK'nin güvenlik fonksiyonlarını ve kullanıcı güvenlik özelliklerini sadece USBK işlem dışı bırakıldığında yapılandırabilir. Gerekli kullanıcı kimlik doğrulaması yapılandırma esnasında uygulanır. USBK'nin kullanım şekli Şekil 3.13.'te gösterilmiştir.



Şekil 3.13. USBK'nin kullanım şekli

USBK içerisinde bir entegre üzerinde 32 bitlik bir mikrodenetleyici olan AT32UC3A3256S, ve onun içerisinde de 32 bit AVR işlemci, 128 KB RAM (geçici bellek) ve anahtarların saklandığı EEPROM işlevini gören 256 KB program hafızası (flash) bulunmaktadır. Mikrodenetleyici Şekil 3.14.'te gösterilmektedir. USBK işletim sisteminden bağımsızdır ve geniş bir yelpazedeki ana sistem (host) ile uyumludur. Ana sisteme herhangi bir sürücü veya yazılım kurulumu gerektirmez.



Şekil 3.14. USBK içerisindeki mikrodenetleyici

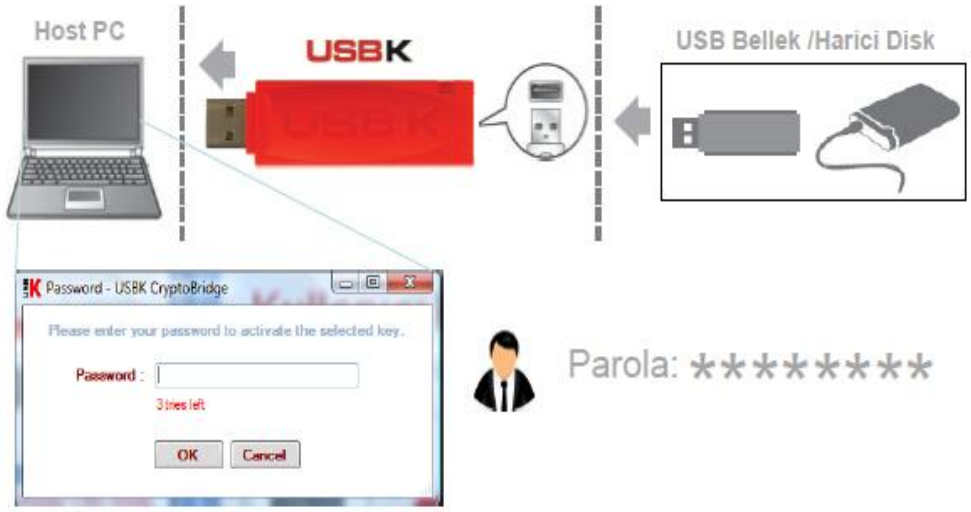
Bu bölümde USB kriptolayıcı (USBK), 2. Bölümde anlatılan güvenlik seviyeleri ve mevcut cihazların analizi kapsamında incelenmektedir.

3.2.1 Tehditler

Bu kısımda USBK cihazının güvenliğine yönelik muhtemel tehditler açıklanacaktır. Bu tehditler USBK'ye yetkisiz şahısların erişimi, entegre devrenin kurcalanması, program belleğinin kurcalanması ve yapısal bozulma olarak sıralanmıştır.

3.2.1.1 Yetkisiz erişim

Kötü niyetli kimse USBK'yi doğru kullanıcı şifresiyle aktifleştirerek arka diskteki verilere erişim sağlayabilir. USBK kullanıcı ile kötü niyetli kişinin her ikisinin de doğru şifreye sahip olması durumunda hangisinin yetkili kullanıcı, hangisinin yetkisiz kişi olduğunu ayırt edemez.



Şekil 3.15. USBK'de kullanıcı şifresiyle kimlik doğrulama

USBK Şekil 3.15.'teki gibi açılışta kullanıcı şifresi isteyerek kimlik doğrulama sağlamaktadır. Ayrıca USBK'nin EKG, osiloskop gibi test/ölçüm cihazlarında da kullanımı mümkün olabilmektedir. Ancak bu cihazlara USBK'nin takılması halinde USBK kullanıcı şifresi istemeden direkt olarak açılmaktadır. Bu kullanım kolaylığı, USBK'nin yetkisiz kişilerce ele geçirilmesi durumunda cihaz önce bir EKG ile, sonra da hemen bir USB veya harici disk ile kullanılabilir. Aynı verinin şifreli ve

şifresiz hali elde edilip, şifreli ve şifresiz veriler karşılaştırılarak şifreleme anahtarı tahmin edilebilir.

3.2.1.2 Entegre devrenin kurcalanması

Kullanıcı şifresi ve transfer anahtarı güvenlik özellikleri 256-bitlik AES hafıza anahtarıyla sabit hafızanın içine şifrelenir ve daha sonra şifresi çözülür. Bu hafıza anahtarı ilk çalıştırılma esnasında rastgele üretilir ve yaşam çevrimi süresince kullanılır.

Donanım analisti entegreyi kurcalayarak anahtarları ve kullanıcı şifresini elde edebilir. Aynı zamanda transfer anahtarlarıyla kullanıcı şifresini de şifreleyen hafıza anahtarının bulunduğu program hafızasını kurcalayarak hafıza anahtarını elde edebilir.

3.2.1.3 Yapısal bozulma

Kullanıcı güvenlik özellikleri ve donanımı doğal nedenlerle yapısal (fiziksel) bozulmaya uğrayabilir. Yüksek veya düşük sıcaklık ya da gerilim değişimi nedeniyle USBK içindeki entegre devreler zarar görebilir, dolayısıyla cihaz şifreleme işlevini düzgün yerine getiremeyebilir.

Ülkemizin coğrafi ve iklim şartları göz önüne alındığında hava sıcaklığı yazları 50 C'ye varabilen, kışları da -40 C'ye kadar düşebilen illerimiz mevcut olup, buralarda pek çok askeri birlik konuşludur. Türk Silahlı Kuvvetleri (TSK) USBK'yi bilgi güvenliği amacıyla arazide açık havada eğitim, tatbikat ya da savaş durumlarında kullanacaktır. USBK'ye benzer bir ürün olan Kingston marka kriptolu USB bellek cihazının çalışma sıcaklık aralığı 0 C ile +60 C derecedir [52]. TSK, arazide bu sıcaklık aralığının dışında aşırı soğuk ve sıcak hava şartlarında görev yapabilmektedir. USBK'nin çalışma sıcaklığı aralığı genişletilmediği sürece, TSK tarafından kullanılan cihaz zaman zaman arazi şartlarında soğuk havalarda işlevini yerine getiremeyecektir.

3.2.2 Güvenlik önerileri

USBK'nın güvenlik standartları [6] doğrultusunda sahip olması hedeflenen güvenlik özellikleri bu bölümde açıklanacaktır. Bu güvenlik önerileri kimlik doğrulama,

kriptografi, kurcalama koruması, otomatik test, acil anahtar silme ve imha, uzaktan erişim ve fiziksel direnç başlıkları altında müteakip maddelerde açıklanacaktır.

3.2.2.1 Kimlik doğrulama

USBK kullanıcıdan kimlik doğrulama için şifre ve ilave olarak da karmaşık ve taklit edilemeyen biyometrik özellikler (parmak izi, yüz/ses tanıma vb.) istemelidir.
Biyometrik sistemler şifre yaklaşımının aksine kişinin bildiği bir bilgi veya taşıdığı bir objeyle değil kişinin kendisinde var olan ve kişiye fiziksel olarak sıkı sıkıya bağlı olan bir özellikle kimliklendirilmesine olanak sağlar. Diğer yaklaşımlarda olan kaybedilme, unutulma, çalınma, tahmin veya taklit edilebilme, diğer kullanıcılarla ortak kullanılma, paylaşılma riskini neredeyse ortadan kaldıran bir teknolojidir [42].

USBK 3 defa başarısız kimlik doğrulama denemesinden sonra kullanıcı şifre ve transfer anahtarlarını silmelidir.

3.2.2.2 Kriptografik algoritmalar

USBK, ana sistemden harici bellek ya da USB belleğe veri transferi esnasında taşınan bu verileri şifrelemeli ve aynı şekilde şifresini çözmelidir. Şifreleme ve şifre çözme işlemleri USBK'nin aktivasyonunda seçilen transfer anahtarları ve AES algoritması tarafından donanım tabanlı şifreleme olarak yapılmalıdır. Donanım tabanlı şifrelemede şifreleme anahtarı donanım üzerindeki entegrede tutulduğu için bilgisayar ile asla paylaşılmaz. Anahtar boyu 128, 192 ya da 256 bit uzunluğunda olmalıdır. Transfer anahtarının belirlenmesi esnasında kullanıcı tarafından, gizlilik derecesine göre 128, 192 ya da 256 bitlik AES transfer anahtarı kullanılarak host ile disk arasında transfer edilen veri şifrelenip çözümlenmelidir. Başlangıçta USBK transfer anahtarlarını rastgele üretilen 256 bitliklerle yükler ve kullanıcı onları USBK'nin kurulumu esnasında değiştirebilir. Kullanıcı daha güçlü bir anahtar elde etmek için 128, 192 ya da 256 bitlik AES anahtarı ürettirebilir.

USBK veri korunumu ve kullanıcı verisinin gizliliğini, veriyi AES algoritmasıyla şifreleyerek sağlar. USBK aynı zamanda kullanıcı güvenlik özelliklerini de AES algoritmasıyla şifrelenmiş şekilde korur. USBK, kullanıcı ve güvenlik özelliklerini içeren program hafızasının okunmasına izin vermez. Yalnızca program hafızası silindikten sonra bu erişim geçerli olur.

Mevcut kripto cihazlarının çoğu AES'in ECB (Electronic Code Book) modu ile şifreleme yapmaktadır. USBK ise transfer ettiği verilerin şifreleme işlemini NSA (National Securtiy Agency-USA) tarafından çok gizli bilgiler için kullanımı onaylanmış en güvenli AES modu olan CBC (Cipher Block Chaining) modu ile gerçekleştirmelidir [43].

USBK transfer anahtarlarını ve şifreyi güvenli bir yöntemle saklamalıdır. Bu anahtarlar USBK'nin ilk kullanımında rastgele üretilen 256 bit uzunluğundaki hafıza anahtarı tarafından şifrelenerek saklanmalıdır.

FIPS onaylı algoritmalar sürekli değişim ve gelişim halindedir. Bu nedenle USBK'de kullanılmasını istediğimiz AES algoritması, gelecek dönemde kripto sistemlerindeki gelişmeler sonucunda yerini daha dayanıklı ve farklı anahtar boylarındaki algoritmalara bırakacağından, USBK bu değişime uyumlanabilmeli, cihaz değişikliğine gitmeden yeni algoritmaları kullanabilmeli ve ayrıca milli algoritmaları içinde barındırabilecek bellek ve işlemci özelliklerine sahip olmalıdır.

3.2.2.3 Kurcalama koruması

USBK, anahtarlara yetkisiz erişimi azaltma (hafifletme) gereksinimi sağlamalıdır. Fiziksel güvenlik mekanizmaları USBK'nin kapakları ya da kapıları açıldığında tüm kritik güvenlik parametrelerini sıfırlayan tepki devreleri ve kurcalama tespiti ile güçlü koruncak özelliklerini içermelidir.

USBK içindeki entegre devrelerin kurcalanması, kapaklarının açılması ve anahtarların elde edilmeye çalışılması durumunda USBK bu yetkisiz ve kötü niyetli kurcalama işlemini tespit edebilmeli, kullanıcısına sesli ya da yazılı olarak uyarı vermelidir. Bu kurcalama ve kapakların açılması esnasında cihaz derhal anahtarları ve şifreyi silmelidir.

3.2.2.4 Otomatik test

USBK açılıştan önce otomatik test gerçekleştirmelidir. Testler modüllerin işlevselliği ile, kullanıcı ve USBK'nin güvenlik özelliklerini ve gömülü yazılımını kapsayan veri hafızalarının bütünlüğünü kapsamalıdır. Bu testler Program hafızası ve kullanıcı güvenlik özellikleri Döngüsel Fazlalık Denetimi [44] (Cycling Redundancy Check-CRC) kontrolü, AES şifreleme/şifre çözme işlemlerinin kontrolü ve USBK'deki

iletişim trafiği kontrolü testleridir. CRC kontrol sonucuna göre kullanıcı güvenlik özelliklerinin yedek kopyası, yapısı bozulanın üzerine tekrar yazılır.

3.2.2.5 Acil anahtar silme ve imha

USBK'nin düşmanca saldırı, terör, sabotaj, gasp gibi yetkisiz kişilerin eline geçme riskinin muhtemel olması durumlarında, içinde bulunan şifre ve anahtarlar ile algoritma yetkisiz kişilerin eline geçebilir. Böyle bir tehlike hâlinde gizli verilerin ve haberleşmenin, dolayısıyla devletin/kurumun sırlarının ifşa olması mümkündür. USBK'yi düşmandan koruma imkan ve zamanı kalmadığında kullanıcı tarafından son çare olarak cihazın üzerinde bulunacak bir acil silme butonuna basarak şifre ve anahtarlar silinebilmelidir. Ayrıca cihaz kolaylıkla sökülüp parçalara ayrılabilecek şekilde üretilmeli, bu sayede yetkisiz kişlerin eline geçme tehlikesi anında süratle sökülüp imha edilebilmelidir.

3.2.2.6 Uzaktan erişim ve alarm

USBK'nin çalınması ya da kaybolması halinde kullanıcı tarafından bulunabilmesi için cihaz üzerinde kullanıcı tarafından uzaktan erişimle etkinleştirilen bir sesli alarm sistemi bulunmalıdır. Bu sesli alarm ile yakın çevrede cihazın kaybolması halinde daha kolay aranması ve bulunması sağlanabilecektir.

USBK'nin tüm aramalara rağmen bulunamaması veya çalınması halinde, şifre ve anahtarların yetkisiz kişilerin eline geçmesini önlemek amacıyla kullanıcı tarafından uzaktan erişimle USBK'deki şifre ve anahtarlar silinebilmelidir.

3.2.2.7 Fiziksel direnç

USBK çok düşük ve yüksek sıcaklıklarda, gerilim değişimlerinde donanımı zarar görmeyecek şekilde üretilmeli, şifreleme ve anahtarları koruma işlevlerini düzgün şekilde yerine getirebilmelidir. USBK'nin Türk Silahlı Kuvvetleri tarafından barış, ve savaş durumunda arazi şartlarında güvenli veri transferi amacıyla kullanılması tasarlanmaktadır.

Ülkemizin özellikle doğu ve güneydoğu bölgelerindeki hava sıcaklık değerlerine baktığımızda kış mevsiminde sıcaklık -40 C'lere kadar düşebilmektedir. Bu şartlarda elektronik devreler işlevini düzgün yerine getirememekte, iletim

yavaşlamaktadır. TSK'nın USBK'yi etkin kullanımı amacıyla cihaz -40 C ile +60 C arasında düzgün çalışabilmelidir.

4. BULGULAR

Bu bölümde kriptografik modüllerin ilave güvenlik gereksinimleri ve ayrıca hali hazırda kullanımda olan KCT ve USBK cihazlarının güvenlik özelliklerinin iyileştirilmesine yönelik öneriler sunulmaktadır.

4.1 Kriptografik Modüllerin Güvenlik Gereksinimlerinin Artırılması Üzerine Öneriler

Uluslararası bilgi güvenliği standartlarında belirtilen kriptografik modüllerin güvenlik gereksinimlerine ilave olarak sunulan güvenlik önerileri Çizelge 4.1.'de gösterilmiştir.

Çizelge 4.1. Kriptografik modüllerin güvenlik gereksinimlerinin artırılması üzerine öneriler

	Kriptografik Modüllerin Güvenlik Gereksinimlerinin Artırılması Üzerine Öneriler
1	Güvenlik riskini azaltmak için kripto modülüne erişim ve kullanım yetkisine sahip operatör sayısı en aza indirilmelidir.
2	İki seviyeli kimlik doğrulamasına (gizli parola, fiziksel anahtar/token ve biometrik özellik) ilave olarak kripto modülü operatörden daha karmaşık ve taklit edilemeyen biometrik özellikler (görüntü, yüz videosu, avuç içi, iris taraması gibi) istemeli ve erişim kontrolü için biometrik özellikler üzerine çalışmalar artırılmalıdır.
3	Hizmet engelleme saldırıları (DoS) karşısında kriptografik modül düzgün çalışmaya devam edebilmeli ve sahip olduğu önemli güvenlik bilgilerini (şifre, anahtar vb.) koruyabilmelidir.
4	Kurum-kuruluşlar tarafından bilgi güvenliği politikaları üretilmeli, Kripto operatörleri ve bilgi sistem kullanıcılarına bilgi güvenliğine yönelik eğitim verilmelidir.

4.2 Kriptolu Cep Telefonu (KCT) Güvenlik Özelliklerinin İyileştirilmesi Üzerine Öneriler

Bilgi teknolojilerinde Dünyanın önde gelen ülkeleri tarafından kriptolu cep telefonları üretilmektedir. Ülkemizde ise TÜBİTAK tarafından üretilen MİLCEP kriptolu cep telefonu kamu kurumları ve özel kuruluşlar tarafından gizlilik dereceli haberleşme için kullanılmaktadır. Bahse konu telefonda bulunan güvenlik özellikleri

ile bu güvenlik özelliklerinin iyileştirilmesi üzerine öneriler Çizelge 4.2.'de belirtilmiştir.

Çizelge 4.2. KCT'nin mevcut güvenlik özellikleri ve iyileştirme önerileri

	Kullanılan KCT'nin Güvenlik Özellikleri	**Güvenlik Özelliklerinin İyileştirilmesi Üzerine Öneriler**
1	Standartlar değiştikçe kriptografik algoritmalar ve anahtar boyları değiştirilememektedir.	Kriptografik modül üzerinde yetkili kişiler algoritma, anahtar boyları ve üretim yöntemlerinde güncelleme yapabilmelidir.
2	Özetleme algoritması olarak SHA-512 (SHA-2) algoritması kullanılmaktadır.	FIPS 180-4 (Mart 2012) güvenlik standardı doğrultusunda güncel SHA-3 (Keccak) algoritması kullanılmaldır.
3	PIN ve akıllı kart ile iki seviyeli kimlik doğrulaması yapabilir.	Açılışta kullanıcıdan PIN ve biyometrik özellik (ses, görüntü, parmak izi vb.) istemelidir.
4	Çalışma sıcaklığı 0 C ile 50 C arasındadır.	Çalışma sıcaklığı Türkiye kış şartlarına uyumlu olmalı, -40 C ile 50 C arasında çalışabilmelidir.
5	Hem kapalı (şifreli), hem de açık (şifresiz) SMS gönderebilmektedir.	SMS gönderimi sadece kapalı (şifrelenmiş) yapılabilmeli, açık SMS gönderememelidir.
6	Çalınma ve kaybolmaya karşı uzaktan erişimle anahtar silme ve sesli uyarı alarmı özelliği yoktur.	Uzaktan erişimle kullanıcı bilgilerini ve anahtarları silebilmeli, sesli alarm özelliği ile yer tespit kolaylığı sağlamalıdır.
7	KCT'nin kurcalandığında yaptığı işlemler hakkında bilgi bulunmamaktadır.	Yetkisiz kurcalamada ve kapaklar açıldığında tepki devresiyle anahtar ve kullanıcı bilgilerini silmelidir. Ayrıca daha sonra kullanıcısına cihazın kurcalandığını ekranda uyarı şeklinde göstermelidir.
8	Mobil işletim sistemi ve internete bağlanma özelliği ile kamera bulunmamaktadır.	Mobil işletim sistemiyle internete bağlanabilmekte, şifreli görüntülü görüşme yapabilmektedir. Sosyal ağlara (facebook, twitter vb.) erişim ise bir güvenlik yazılımı ile engellenmelidir.

4.3 USBK Güvenlik Özelliklerinin İyileştirilmesi Üzerine Öneriler

USBK'nin sahip olduğu mevcut güvenlik özellikleri ile güvenlik standartları çerçevesinde iyileştirilmesini önerdiğimiz güvenlik özellikleri Çizelge 4.3.'te gösterilmiştir.

Çizelge 4.3. USBK'nin mevcut güvenlik özellikleri ve iyileştirme önerileri

	Kullanılan Kriptolu USBK Güvenlik Özellikleri	**USBK Güvenlik Özelliklerinin İyileştirilmesi Üzerine Öneriler**
1	Standartlar değiştikçe kriptografik algoritmalar ve anahtar boyları değiştirilememektedir.	Kriptografik modül üzerinde yetkili kişiler algoritma, anahtar boyları ve üretim yöntemlerinde güncelleme yapabilmelidir.
2	Acil anahtar silme ve kolay imha özelliği bulunmamaktadır.	Acil anahtar silme özelliği bulunmalıdır. Kolay imha amaçlı, parçaları kolay sökülebilir fiziki yapıda olmalıdır
3	EKG cihazı ile kullanıldığında şifre istemeden çalışarak erişim güvenliği zayıflığına yol açar. Ayrıca aynı verinin şifreli ve şifresiz haline yetkisiz erişim nedeniyle anahtarlar tahmin edilebilir.	EKG cihazı ile kullanımda da kullanıcı şifresi ya da farklı biyometrik kullanıcı bilgileri istenerek erişim güvenliği sağlanmalı, cihaz sadece bu tür EKG'lerle çalışmalıdır.
4	Kimlik doğrulaması şifreyle sağlanmaktadır. (Kriptolu USB bellekte ayrıca akıllı kartla kimlik denetimi).	Açılışta şifreye ilave olarak biyometrik özellik istemiyle (ses, görüntü, parmak izi vb.) kimlik doğrulama yapılmalıdır.
5	Kurcalandığında ve kapaklar açıldığında tepki vermemekte, anahtarları silmemektedir.	Yetkisiz kurcalamada ve kapaklar açıldığında tepki devresiyle anahtar ve kullanıcı bilgilerini silmelidir. Ayrıca daha sonra kullanıcısına cihazın kurcalandığını sesli uyarı ya da görsel olarak bildirmelidir.
6	USBK'nin çalışma sıcaklığı hakkında bilgi bulunmamakta, Kingston marka kriptolu USB belleğin çalışma sıcaklığı 0 C ile +60 C arasındadır.	Çalışma sıcaklığı -40 C ile +60 C arasında olmalıdır.

5. SONUÇ VE ÖNERİLER

ISO/IEC 15408 Bilgi Güvenliği Sistemleri için Ortak Kriterler Standardı, ISO/IEC 17799 standardı ve FIPS 140-3 gibi başlıca geçerli bilgi güvenlik standartlarında açıkça belirtilen güvenlik özellikleriyle birlikte halen bilgi teknolojisi ve kriptografide pek çok açıkların bulunduğu ve bu zayıflıklıkların gerek kamu gerek özel kuruluşların bilgi güvenliğini tehdit edebilecek saldırı ve girişimlere karşı hazırlıksız olduğu, yakın zamanlarda gerçekleşen siber saldırılarda ve haberleşme trafiğinin gizlice takip edilmesi gibi olaylarda açıkça görülmüştür. Tüm bu tehditlere karşı özellikle Silahlı Kuvvetlerimiz ve emniyet güçlerimizin haberleşme gizliliği son derece önemlidir.

Bu tezde cep telefonundan ses ve veri haberleşmesi ile görüntülü haberleşmenin şifreli yapılmasına olanak veren kriptolu cep telefonları ile bilgisayar, EKG cihazı gibi sistemlerden USB/harici belleklere şifreli veri transferi yapan USBK cihazlarının güvenlik gereksinimlerinin neler olabileceği, ne tür tehditlere açık olabileceği araştırılmıştır. Günümüz koşullarında kullanılmakta olan KCT ve USBK cihazlarına yönelik tehditler, standartlar doğrultusunda sahip oldukları güvenlik gereksinimleri ve ilave ihtiyaç duyulan güvenlik gereksinimleri üzerine araştırma yapılmştır.

Kriptografik modüllerin fonksiyonel güvenlik özellikleri geliştirilse de insan faktörü göz önünde bulundurulmalıdır. Kripto güvenliği riskini azaltmak için modüle erişim ve kullanım yetkisine sahip operatör sayısı minimum düzeyde tutulmalıdır. Güvenlik standartlarıyla istenen güvenlik gereksinimlerine ilave olarak, iki seviyeli kimlik doğrulaması (gizli parola, fiziksel anahtar/token ve biometrik özellik) ve taklit edilemeyen biometrik özelliklerle (ses, görüntü, yüz videosu, avuç içi, iris taraması gibi) erişim kontrolü sağlayan kripto modül ve cihazları üzerine çalışmalar arttırılmalıdır. Hizmet engelleme saldırıları (DoS) karşısında kriptografik modül içeren cihazlar düzgün çalışmaya devam edebilmeli ve sahip olduğu önemli güvenlik bilgilerini koruyabilmelidir. FIPS onaylı algoritmalar sürekli değişim ve gelişim içindedir. Bu nedenle kriptografik modüllerle KCT ve USBK'de kullanılmasını

istediğimiz AES algoritması, gelecek dönemde kripto sistemlerindeki gelişmeler sonucunda yerini daha dayanıklı ve farklı anahtar boylarındaki algoritmalara bırakacağından, kripto cihazları bu değişime uyumlanabilmeli, cihaz değişikliğine gitmeden yeni algoritmaları kullanabilmeli ve ayrıca milli algoritmaları içinde barındırabilecek bellek ve işlemci özelliklerine sahip olmalıdır. MİLCEP tarafından kullanılmakta olan SHA-2 özetleme algoritması güncelliğini yitirdiğinden, yerine FIPS 180-4 (Mart 2012) güvenlik standardı doğrultusunda güncel SHA-3 (Keccak) algoritması kullanılmalıdır. KCT kullanıcı hatası sonucu gizli mesajları şifresiz olarak yetkisiz kişilere gönderme, ya da aynı mesajı şifreli ve şifresiz ayrı ayrı göndererek anahtarların tahmin edilmesine karşı mesaj (SMS) gönderimini sadece şifreli yapmalı, cihaz şifresiz SMS göndermemelidir. KCT'de kayıp ve çalınmalara karşı uzaktan erişimle kullanıcı bilgileri ve anahtarları silme, sesli alarm gibi özellikler bulunmalıdır. Yetkisiz kurcalamada ve kapaklar açıldığında tepki devresiyle anahtar ve kullanıcı bilgileri silinmeli, sonrasında KCT kullanıcısına cihazın kurcalandığını ekranda uyarı şeklinde göstermelidir. Sosyal ağlara (facebook, twitter vb.) erişim bir güvenlik yazılımı ile engellenmelidir.

USBK cihazında da tıpkı KCT'de olduğu gibi şifreye ilave biyometrik kimlik denetimi, algoritma ve anahtar boyu değişikliklerine uyum, kurcalamaya karşı anahtar sıfırlama devresi ve daha geniş sıcaklık aralığında çalışma yeteneği sayesinde aşırı soğuklardan olumsuz etkilenmeme güvenlik gereksinimleri bulunmalıdır. USBK'nin osiloskop, EKG cihazı gibi ölçüm cihazlarıyla kullanıcı şifresi istemeden direkt çalışası bir kimlik doğrulama zayıflığıdır. Bu özellik, yetkisiz erişim tehdidini artırdığından, EKG vb. cihazlarla kullanımın da güvenli hale getirilmesi üzerine araştırmalar yapılmalıdır. USBK donanım tabanlı yapısı ve işletim sisteminden bağımsız özelliği sayesinde DoS vb. saldırılar ve kötü yazılımlardan etkilenmemektedir. İşletim sistemi ve yazılım tabanlı olan KCT ise bu saldırılara ve kötü yazılımlara karşı anti virüs yazılımı, güvenlik duvarı, arama/SMS filtreleme güvenlik özellikleriyle koruma sağlamalıdır. USBK anahtar ve kullanıcı şifresini yakın düşman tehlikesi, terör, gasp vb. durumlara karşı koruma amaçlı acil anahtar silme tuşu ile koruma sağlamalıdır. USBK ayrıca tehlike anında kolay sökülebilir ve imha edilebilir fiziki yapıda olmalıdır. KCT TSK haberleşme altapıları olan TASMUS ve TAFICS'e entegre olabilmeli, bu altyapıdan bağımsız olmamalıdır.

KAYNAKLAR

[1] Ruggiero P. and Foote J., 2011. Cyber Threats to Mobile Phones, *United States Computer Emergency Readiness Team (US-CERT).*

[2] Panda Labs, 2011. Quarterly Report PandaLabs, http:// press.pandasecurity.com/wp-content/uploads/2011/04/PandaLabs-Report-Q1-2011.pdf, (Ziyaret tarihi: 16 Aralık 2013).

[3] National Institute of Standards and Technology, Guidelines on Cell Phone and PDA Security (SP 800-124), http://csrc.nist.gov/publications/nistpubs/800-124/SP800 124. pdf, (Ziyaret tarihi: 18 Aralık 2013).

[4] Cox J., iPhone on Wi-Fi Vulnerable to Security Attack, http://www.macworld. co.uk/ipod-itunes/news/index.cfm?rss&newsid=27777, (Ziyaret tarihi: 20 aralık 2013).

[5] Karig D. and Lee R., 2001. Remote Denial of Service Attacks and Countermeasures, *Princeton University Department of Electrical Engineering Technical Report*, CE-L2001-002.

[6] Gallagher P.D., FIPS PUB 140-3 Security Requirements for Cryptographic Modules, 2009.

[7] Federal Information Processing Standards Publication 197, November 26, 2001.

[8] Gallagher P.D., FIPS PUB 180-4 Secure Hash Standard (SHS), National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, March 2012.

[9] BITS Malware Risks And Mitigation Report, 2011. http://www.nist.gov/itl/upload/BITS-Malware-Report-Jun2011.pdf, (Ziyaret tarihi: 12 Kasım 2013).

[10] Mulliner C.R., 2006. Security of Smart Phones, Master's Thesis, University of California, Santa Barbara.

[11] Habib S.M., Zubair S., 2009. Security Evaluation of the Windows Mobile Operating System, Master of Science Thesis, Chalmers University of Technology Division of Networks and Systems and Department of Computer Science and Engineering Göteborg, Sweden.

[12] Mobil Threat Report Q1 2013 January-March, F-Secure, http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2013. pdf., (Ziyaret tarihi: 02 Ocak 2014).

[13] Yayla O., 2008. Kriptografik Modüllerin Güvenlik Gereksinimleri , *ISC Turkey*, Ankara, 25-26-27 Aralık.

[14] GSM Association. GSM World - Home of the GSM Association, http://www. gsmworld.com, (Ziyaret tarihi: 11 Haziran, 2010).

[15] Dondyk E., Zou C., 2012. Denial Of Convenience Attack to Smartphones Using A Fake Wi-Fi Access Point, Master thesis, Engineering and Computer Science, University of Central Florida, Orlando, Florida.

[16] CIAC Report, 2010. *Colorado Information Analysis Center Intelligence Bulletin*, pp 10-400.

[17] Hackers Targeting Advanced Cellular Phones, 2010. Department of Homeland Security (USA).

[18] Waheed A., Zareen M., Vapen A., Attacks Against Smartphones, Project Report for Information Security Course, Linköpings Universitet, Sweden.

[19] Protecting the BlackBerry device platform against malware, http://www. blackberry.com, (Ziyaret tarihi: 11 Ocak 2013).

[20] http://www.kaspersky.com/tr/threats_faq#spyware, (Ziyaret tarihi: 03 Kasım 2013).

[21] Gary M.G., Mar-Apr 2004. Building Security In Software Security, IEEE Security& Privacy, Vol.2, Issue.2, pp. 80 – 83.

[22] Philippaerts P., 2010. Security of Software on Mobile Devices, Dissertation for the degree of Doctor in Engineering, Katholieke Universiteit Leuven, Faculty of Engineering, Belgium.

[23] Yılmaz S., Sağıroğlu Ş., 2013. Yazılım Güvenliği Üzerine Bir İnceleme, *6th International Information Security & Cryptology Conference*, METU, Ankara, 20-21 Eylül.

[24] Barrera D., Oorschot P.C.V., 2010. Secure Software Installation on Smartphones, Carleton University.

[25] Karaalan H., Akleylek S., 2013. Kriptografik Modüllerin Güvenlik Gereksinimleri, *1st International Symposium on Digital Forensics and Security (ISDFS'13)*, Elazığ, Turkey, 20-21 Mayıs.

[26] Karaalan H., Akleylek S., 2013. On the Security Requirements of Cryptographic Modules, *3rd World Conference on Innovation and Computer Sciences*, Antalya, 26-28 Nisan.

[27] http://www.aselsan.com.tr/content.aspx?mid=375&oid=451, (Ziyaret tarihi: 03 Temmuz 2013).

[28] http://bilgem.tubitak.gov.tr/tr/icerik/milsec-4-emniyetli-ip-terminal, (Ziyaret tarihi: 14 Haziran 2013).

[29] Yavanoğlu U., Sağıroğlu Ş., 2013. Sosyal Ağlar ve Bilgi Güvenliği, *6th International Information Security & Cryptology Conference*.

[30] Khadem S., Security Issues in Smartphones and their effects on the Telecom Networks, Master of Science Thesis, Department of Computer Science and Engineering, University of Gothenburg, Göteborg, Sweden, August 2010.

[31] http://en.wikipedia.org/wiki/SYN_flood, (Ziyaret tarihi: 15 Ekim 2013).

[32] http://phonereport.info/blackberry-maker-concerned-about-denial-of-service-attack-through-smartphones, (Ziyaret tarihi:16 Temmuz 2013).

[33] Beydağlı E., http://www.bilgiguvenligi.gov.tr/donanim-guvenligi/akilli-kartlarda-yan-kanal-analizi-3.html, TÜBİTAK BİLGEM, (Ziyaret tarihi: 03 Ocak 2014).

[34] Aumüller C., Bier P., Fischer W., Hofreiter P., Seifert J.P., Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures, Infineon Technologies, Security and Chipcard ICs, Munich, Germany.

[35] http://www.chip.com.tr/chipdergi/arsiv/2011-11.html?download=true&accept=true, sayfa 61-62, (Ziyaret tarihi: 01 Ağustos 2013).

[36] Elektronik Belgeleri Açık Anahtar Altyapısı Kullanarak Güvenli İşleme Rehberi, REHB-003- 014, 2011. TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi, Gebze, Kocaeli, http://www.kamusm. gov.tr/ dosyalar/rehberler/güvenli_belge.rehberi.pdf, (Ziyaret tarihi: 19 Mart 2013).

[37] http://www.avast.com.tr/tr-tr/free-mobile-security#tab2, (Ziyaret tarihi: 04 Kasım 2013).

[38] http://www.kaspersky.com/mobile_downloads, (Ziyaret tarihi: Ocak 2013).

[39] http://www.bilgem.tubitak.gov.tr/tr/icerik/milcep-k2-milli-kriptolu-cep-telefonu, (Ziyaret tarihi: Eylül 2013).

[40] Certification Report, 12.10.2011, Turkish Standards Institution Common Criteria Certification Scheme, USBK Cryptobridge v2.0 For Model A101 and Model A103, http://www.commoncriteriaportal.org/files/epfiles/USBK%20Cryptobridge%20v2.0%20For%20Model%20101%20and%20Model%20103%20CERTIFICATION%20REPORT.pdf, (Ziyaret tarihi: 10 Kasım 2013).

[41] Gartner Inc. 2009 yılı araştırma raporu, https://www.gartner.com/doc/1222213. (Ziyaret tarihi: 23 Ekim 2013).

[42] ÖZKAYA N. ve SAĞIROĞLU Ş., 2006, Açık Anahtar Altyapısı ve Biyometrik Teknikler, *Ulusal Elektronik İmza Sempozyumu*, Ankara, 7-8 Aralık.

[43] http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation, (Ziyaret tarihi: 10 Ekim 2013).

[44] http://tr.wikipedia.org/wiki/D%C3%B6ng%C3%BCsel_art%C4%B1kl%C4%B1k_denetimi, (Ziyaret tarihi: 12 Kasım 2013).

[45] Information technology, Security techniques, Security requirements for cryptographic modules (ISO-IEC 19790), 2012.

[46] Norwegian National Security Authority, NSM Cryptographic Requirements, 2008.

[47] Japan Cryptographic Module Validation Program, JCMVP Cryptographic Module Security Requirements, November 2, 2008.

[48] Genic S., Information System Security Threats Classifications, Journal of Information and Organizational Sciences, vol.31, no.1, pp.51-61.

[49] Şentürk H., Cyber Security Analysis of Turkey, Internatıonal Journal Of Information Security Science, Vol.1, No. 4.

[50] TÜBİTAK BİLGEM Ulusal Bilgi Güvenliği Kapısı, http://www.bilgiguvenligi.gov.tr/son-kullanici-kategorisi/tehlike-cepte.html, (Ziyaret tarihi: 11 Ocak 2013).

[51] http.//www.ssm.gov.tr/anasayfa/kurumsal/Documents/GizlilikDerecelendirmeKilavuzu.pdf, (Ziyaret tarihi: 23 Ocak 2014).

[52] http://www.kingston.com/tr/company/press/article/6940, (Ziyaret tarihi: 02 Aralık 2013).

ÖZGEÇMİŞ

Adı Soyadı	: Halil KARAALAN
Doğum Yeri ve Tarihi	: Lüleburgaz /07 Kasım 1983
E-posta	: halil.karaalan@bil.omu.edu.tr
Lisans	: Sistem Mühendisliği (Kara Harp Okulu/Elektrik-Elektronik Alt Dal)

Mesleki Deneyim ve Ödüller:

2007 yılından bu yana Türk Silahlı Kuvvetlerinde bilgi güvenliği alanında görev yapmaktadır.

Yayın ve Patent Listesi:

[1] Karaalan H., Akleylek S., 2013. On the Security Requirements of Cryptographic Modules, *Global Journal on Technology, (Vol 4,* pp. 1017-1021, *2013)* ISSN: 2147-5369.

[2] Karaalan H., Akleylek S., 2014. Security Requirements of Cryptographic Modules with Case Studies on Crypto Phone and Crypto Stick, *Journal of Military and Information Science*. (Dergiye gönderilmek üzere hazırlanmaktadır).

TEZDEN TÜRETİLEN YAYINLAR/SUNUMLAR:

[1] Karaalan H., Akleylek S., Kriptografik Modüllerin Güvenlik Gereksinimleri, *Proceedings of International Symposium on Digital Forensics and Security,* pp. 151-154, May 20-21, Elazığ, 2013.

[2] Karaalan H., Akleylek S., 2013. On the Security Requirements of Cryptographic Modules, *3rd World Conference on Innovation and Computer Sciences (INSODE 2013),* AWERProcedia Information Technology & Computer Science, Antalya.