BEYKENT ÜNİVERSİTESİ FEN VE MÜHENDİSLİK BİLİMLERİ DERGİSİ
Cilt 6(2) 2013, 121 – 152

VERİ GÜVENLİĞİNDE TEMPEST SALDIRI TÜRLERİ ÜZERİNE TARİHSEL BİR İNCELEME

Hamdi ALTINER (*hamdialtiner@gmail.com*)
Beykent Üniversitesi, Fen Bilimleri Enstitüsü,
Bilgisayar Mühendisliği Tezli Yüksek Lisans Öğrencisi,

Ediz ŞAYKOL (*ediz.saykol@beykent.edu.tr*)
BeykentÜniversitesi, Bilgisayar Mühendisliği Bölümü,

ÖZET

Hayatımızın bir vazgeçilmezi haline gelen bilgisayarlar, günümüzde bazen farkında olmadan kendimiz bazen de kötü niyetli kişiler tarafından çok etkin bir ateşsiz silah olarak kullanılabilmektedir. Gayri yasal yollarla elde edilen bilgilerin ifşa edilmesi ile dünya çapında kaoslar oluşturulmakta, ülke güvenlikleri tehlikeye atılmakta, sağlık, elektrik, haberleşme hizmetleri gibi hayati faaliyetler durdurulmakta, şirketler zarara uğratılmakta ve özel hayatın gizliliği ihlal edilerek, hızla büyüyen bir ağ gibi tüm insanlık bu tehditlere karşı savunmasız hale gelmektedir.

Bu tehditler artan hız ve karmaşıklıkta devam etmekte olup bilişim hayatımızın içerisinde yer aldığı sürece de devam edecektir. Bilişim güvenliğinin sağlanmasına yönelik çabalar bitmeyen ve devamlı iyileştirmeler ile güncel tutulması gereken bir faaliyet olmalıdır. Bu nedenle bilişim güvenliği bir son durum değil, hiç bitmeyen, yaşayan bir süreç olarak algılanmalıdır.

Kişisel bilişim güvenliğine kıyasla kurumsal bilişim güvenliği daha çok bileşenli, önemli ve yönetimi zor bir süreçtir. Bu nedenle daha yüksek bir maliyet ve iş gücü gerektirir. Bilişim güvenliği pek çok ana ve alt konulardan meydana gelmektedir ancak özellikle gizli bilgilerin işlendiği kurumlarda uyulması gereken güvenlik önlemlerinin başında TEMPEST gelmektedir. Bilgi güvenliğinin değerini artırdığı günümüzde TEMPEST konusunun önemi daha da belirginleşmiştir.

Anahtar kelimeler. *TEMPEST, Bilişim Güvenliği, Elektromanyetik Girişim, Elektromanyetik Güvenlik, Elektromanyetik Uyum, Elektronik İstihbarat, Uzaysal Işıma, Ekranlama, Yan Kanal Saldırıları, Elektromanyetik Analiz.*

BEYKENT UNIVERSITY JOURNAL OF SCIENCE AND ENGINEERING
Volume 6(2) 2013, 121 – 152

A CHRONOLOGICAL REVIEW ON TEMPEST ATTACKS IN DATA SECURITY

Hamdi ALTINER (*hamdialtiner@gmail.com*)
Beykent University, Graduate School of Sciences and Engineering, MSc Student in Computer Engineering Department,

Ediz ŞAYKOL (*ediz.saykol@beykent.edu.tr*)
Beykent University, Department of Computer Engineering,

ABSTRACT

As an inevitable part of our life, computers sometimes can be used like a non-firearm unconsciously by ourselves or by malicious people. By disclosing illegally obtained information, worldwide chaoses can be created, security of countries can be endangered, vital services like health, electricity, communication can be interrupted, companies can be undermined and violating privacy of prive life and like a growing network all humanity becomes vulnerable against this threats.

These threats continue in increasing speed and complexity, and will last as long as information technology takes place in our life. The efforts for securing information security must be up to date activity with long lasting and continuous improvements. Therefore Information Security must be considered as a never ending process.

In comparison with personnel information security, institutional information security is much more complex and hard to manage process. Therefore it requires higher costs and manpower. IT Security consist of many main and sub topics but especially in security related institutions TEMPEST comes at the head of main precautions. Nowadays on which Information Security's value increased, importance of TEMPEST issue became more evident.

Keywords: *TEMPEST, Bilişim Güvenliği, Elektromanyetik Girişim, Elektromanyetik Güvenlik, Elektromanyetik Uyum, Elektronik İstihbarat, Uzaysal Işıma, Ekranlama, Yan Kanal Saldırıları, Elektromanyetik Analiz.*

1. GİRİŞ

Geçmişte sadece insanlar kullanılarak bilgi toplama çalışmaları yapılırken teknolojinin gelişmesiyle artık elektronik tabanlı bilgi toplama da yaygınlaşmıştır. Bir ajan, düşman arasına girerek bilgi ve belge toplar ancak yakalanması durumunda hem kendisi hem de ülkesi risk altına girer. Ancak elektronik tabanlı bilgi toplama çalışmalarında genellikle hiçbir iz bırakmadan bu riskler en düşük seviyelere inmektedir. TEMPEST saldırıları da pek çok kurum ve insanın farkında dahi olmadan maruz kaldıkları bu tarz saldırılardandır.

Bu saldırı yöntemleri çok basit teknikler olabildiği gibi gizli şifre ve anahtarların dahi çözümlenmesini sağlayabilen karmaşık yapılar da olabilir. Devlet sırlarının yanı sıra banka şifreleri, kişisel tercihlerimiz gibi özel hayatımıza dair bilgiler saldırganların eline geçebilir.

Karşı tedbirlerin alınmasını engellemek maksadıyla bilinen diğer saldırı yöntemlerinin aksine TEMPEST saldırı yöntemleri gizli tutulmaktadır. Bu nedenle pek çok insan ya bu tarz saldırıların birer efsane olduğunu düşünmekte ya da kullanılan saldırı yöntemlerinden habersiz yaşamaktadır.

Bu çalışmada kurumlar ve insanlar üzerinde bir TEMPEST farkındalığı yaratılarak muhtemel saldırı ve tehditlere karşı ön alınması hedeflenmiş ve bu maksatla tarihte yaşanan TEMPEST saldırılarından günümüzdeki TEMPEST saldırılarına kadar bilinen saldırı türleri geniş bir yelpazede incelenmiştir.

2. TEMPEST'İN TARİHİ GELİŞİMİ

19'uncu yüzyılda telli telefon kablolarının ilk kez kullanıldığı sistemlerde hatların karışması konusu sıkça karşılaşılan bir problemdi. 1914 yılında 1. Dünya Savaşı esnasında sahra telefon kabloları askerler ile karargâhları arasında irtibat sağlamak üzere düşman hatlarına sadece birkaç yüz metre uzaklıkta, paralel olarak kilometrelerce uzanmaktaydı. Ayrıca telefon kablolarında fazla ağırlık yapmaması için toprak dönüşü kullanan, tek telli izole kablolar kullanılmaktaydı. Kısa bir zaman sonra toprak hattı kaçağı nedeniyle düşmanın görüşmeleri de dahil olmak üzere tüm görüşmelerin dinlenebildiği fark edildi. Bunun üzerine hemen dinleme postaları kuruldu ve toprak hattı kaçaklarını engellemek maksadıyla iki telli kablolar

kullanılmaya başlandı. 1915'e kadar geliştirilen dinleme amplifikatörleri sayesinde, dinleme mesafesi yaklaşık olarak telefonlar için 100, Mors alfabesi makineleri için 300 metreye kadar ulaştı. 1916'ya gelindiğinde düşman hattına 3000 yarda (2.743 metre) mesafeye kadar toprak dönüşlü devrelerin kullanılması yasaklandı [1,2].

2.Dünya Savaşında ise kara ve deniz gizli haberleşme sistemlerinin omurgasını tek kullanımlık şeritler ve basit kripto cihazları oluşturmaktaydı. Bu sistemler kripto işlemini 131-B2 olarak adlandırılan Bell telefon karıştırıcısını kullanarak gerçekleştirmekteydi. 1943 yılında bu karıştırıcılardan biri Bell laboratuarında test edilirken bir araştırmacı tarafından laboratuar içerisindeki uzak bir noktada bulunan osilaskopun ekranında salt rastlantısal olarak, her işlem adımında bir darbe işareti oluştuğu fark edilmiş ve bu darbe işaretleri dikkatlice incelediğinde, açık bilginin elde edilebildiği anlaşılmıştır. Böylece bilinen ilk resmi TEMPEST kaçağı belirlenmiştir.

Bu cihazlar askerlere güvenlik garantisi ile satılmışlardı. Bu konuyla ilgili yetkili mercilere uyarılar yapıldı. Fakat bu cihaza sahip olmayanlar tarafından da açık mesajların elde edilebileceğine askerler tarafından ilk başta şüphe ile bakıldı. Bunun üzerine Bell araştırmacıları, askeri birlik kripto merkezinin 25 metre uzağındaki bir binaya konuşlandılar. Bir saat süreyle kripto merkezinde kullanılan cihazlardan yayılan elektromanyetik dalgaların kaydını yaptılar. Dört saatlik inceleme sonunda açık bilginin %75'ini elde ettiler [3]. Askeri birimler olan bitenden oldukça etkilendiler. Bu durumun daha ayrıntılı araştırılmasını ve 131-B2 karıştırıcılarındaki bu kaçakların giderilmesini istediler. Altı aylık bir çalışma sonucunda yayılımı önleyici üç temel yöntem önerildi.

- Işıma yoluyla oluşacak kaçaklara yönelik ekranlama (Shielding),
- Güç ve işaret hatlarındaki kaçaklara yönelik filtreleme (Filtering),
- Hem ışıma hem de iletken hatlara yönelik maskeleme (Masking).

Alınan bu önlemler de tam olarak etkili olmadı ve yeni sorunlar ortaya çıktı. Denetlemeler esnasında alınan tüm ilave tedbirlere rağmen 400 metre uzaklıktaki bir hattan açık bilginin elde edildiği tespit edildi. Bazı işaret hattı ve güç filtreleri ile işaret ve güç hattı kaçaklarının temizlenmesi sağlandıysa da ışıma kaçaklarına yine engel olunamadı ve güvenlik bölgeleri koruma alanlarının 60 metreye çıkarılması gibi pek çok ilave tedbir alındı [4].

1960'lı yıllarda kamu yayını hizmetlerinin desteklenmesi maksadıyla yıllık lisans ücreti ödenmesinin zorunlu olduğu İngiltere'de TV detektör

araçları üzerinde bulunan ve televizyonlardan yayılan sinyalleri tespit eden cihazlar ile denetimler yapılmaktaydı. Bu dönemde de bilgisayar güvenliği konusuyla ilgilenen insanlar, cihazlarda ve bağlantı kablolarında meydana gelen bu kontrol dışı emisyon kaçaklarının farkındaydılar [5].

1956 Süveyş krizi esnasında istihbaratçılar yan kanal saldırı tekniklerini kullanmaya başlamışlardır. İngilizler bir telefon böceği sayesinde Mısır Büyük Elçiliğinde kullanılan Hagelin şifre makinesine ait bilgileri elde etmişlerdir.

1960 yılında Fransız Büyük Elçiliğinde yapılan denetimlerde Avrupa Ekonomik Topluluğuna (AET) katılım sürecinde yapılan kriptolu görüşmelerin ikincil bir yan sinyal ile taşındığı ve açık mesajın elde edilmesi için başka bir düzenek kurulduğu tespit edilmiştir. Böylece şifre makinesinden bir şekilde sızan bilgiler açık metine dönüşmüştür [6].

1970'lerde Yayılım Güvenliği yüksek gizlilik dereceli bir konu haline geldi ve literatürden yavaşça silindi. Hollandalı araştırmacı Wim Van ECK'in 1985 yılında bir VDU (Visual Display Unit) üzerindeki görüntüyü belirli bir mesafeden nasıl elde ettiğini açıkladığı makalesi ile konu tekrar gündemdeki yerini aldı. Böylece TEMPEST saldırılarının ev yapımı basit bir cihazla bile yapılabileceği kanıtlanmış oldu ve bu bilişim güvenliği endüstrisinde büyük bir tedirginliğe yol açtı [7].

1990'ların ikinci yarısından itibaren yayılım güvenliği ile ilgili önemli makaleler yayınlandı. 1996'da Markus Kuhn ve RJ Anderson pek çok akıllı kartın içerisine yerleştirilecek ikincil bir frekansla veya güç ve saat sinyalleri üzerinde yapılacak bir müdahale ile kırılabileceğini göstermiştir [8]. Paul Kocher yaptığı çalışmalarda kripto sistemlerinde yaygın olarak kullanılan pek çok uygulamanın, veri işlem zamanları ile ilgili olarak yapılan hassas ölçümlerle kırılabileceğini göstermiştir [9].

1998 yılında kişisel bilgisayarlardaki kaçak emisyonun çeşitli yazılımlar kullanılarak azaltılabileceği veya artırılabileceği Markus Kuhn'un ve RJ Anderson tarafından yapılan laboratuar çalışmalarında gösterilmiştir [10]. Paul Kocher 1998-1999 yılları arasında yaptığı çalışmalarında akıllı kartlarda kullanılan kripto anahtarlarının işlem sırasında kart tarafından çekilen akımın hassas bir şekilde ölçülmesi ile elde edilebileceğini göstermiştir [11].

Son yıllarda da gelişmeler artarak devam etmektedir. 2002 yılından itibaren optik yansımalar sonucu ortaya çıkan kaçaklar üzerinde de çalışmalar yapılmaya başlanmıştır. Markus Kuhn çalışmalarında bir ekrandaki görüntünün odanın duvarlarındaki yansımasından veya ekran

karşısında oturan kullanıcının yüzündeki yansımadan tekrar elde edilebileceğini göstermiştir [12]. 2004 yılında Dimitri Asonov ve Rakesh Agrawal bilgisayar klavye tuşlarının her birinin ayırt edilebilir nitelikte farklı seslere sahip olmasından yola çıkılarak, yazılan metinlerin akustik yayılımlar sayesinde ele geçirilebileceğini göstermiştir [13]. 2005 yılında Li Zhuang, Feng Zhou ve Doug Tygar klavye tuş takımı karakteristikleri ve metin istatistiklerini kullanarak bu metodu daha da geliştirmiştir [14].

2006 yılında Steven Murdoch pek çok bilgisayarın CPU yükünün termal kaçaklar ile açığa çıktığını gösterdi. Tezinde işlemci saat sinyallerinin ortam ısısı ile etkileşim içerisinde olduğunu ve uzaktan ölçülebileceğini hatta hedef makinenin koordinatlarının dahi elde edilebileceğini ortaya koymuştur [15]. Daha pek çok araştırma sonucunun da önümüzdeki yıllarda açıklanması beklenmektedir

2007 yılında Amerikan Ulusal Güvenlik Dairesi (NSA) tarafından gizliliği kaldırılan makalede, Amerika'da TEMPEST'in ortaya çıkışı ve tarihi hakkında çok net bilgiler verilmektedir. Birinci Dünya Savaşında diğer ülkeler tarafından yürütülen, yukarıda bahsedilen dinleme faaliyetlerinin tam olarak TEMPEST kapsamında olduğunun söylenmesi mantıklı değildir. Ayrıca bu çalışmalar resmi bir kurum tarafından açıklanmadığı için yalnızca söylenti boyutunda kalmaktadır. Dolayısıyla TEMPEST'in keşfinin, yukarıda açıklandığı biçimiyle, Amerikalılar tarafından 1943 yılında yapıldığı düşüncesine varılmaktadır [4].

Günümüzde kullanılan, deşifre olmuş sıra dışı TEMPEST saldırı yöntemlerinden bazıları aşağıda sunulmuştur [16].

- Hedef bölgede gizli bir noktaya yerleştirilmiş basit telsiz mikrofon düzenekleri. Bu tarz cihazlarda en büyük problem pil ömrüdür. Birkaç yüz metre menzile ve birkaç haftaya kadar pil ömrüne sahiptirler.
- İhtiyacı olan gücü bağlandığı sistemden alan cihazlar; bir telefon kablosu veya harici güç kaynağı ile beslenen bu cihazlar bir kez yerleştirildikten sonra süresiz olarak aktif kalırlar. Bazıları kablo kanallarına kolayca yerleştirilebilen basit mikrofonlar olabildiği gibi yan binalardan açılacak deliklerle hedef bölge duvarlarına, zemin veya tavanına yerleştirilecek sinyal göndermeci veya kameralar olabilir. Aynı şekilde özel olarak tasarlanmış, yazılan metni saldırganlara da aktaran trojan yazılımlı bir bilgisayar klavyesi ile hedef bölgede işlenen bilgiler elde edilebilir.
- Pek çok modern dinleme yazılımı mobil telefon teknolojisini kullanır. Saldırgana çok geniş bir menzilde hedefine erişim imkânı veren bu

teknoloji ile hedef telefonunun bataryası dolu olduğu sürece saldırılara maruz kalır.

- Fort Meade NSA Müzesinde sergilenen bir diğer ilginç cihaz ise ABD büyük elçisine 1946 yılında Moskova'yı ziyareti esnasında verilen ahşap "Great Seal of United States" duvar süsüdür. Büyükelçi bu hediyeyi evindeki çalışma odasına asmış ve daha sonra 1952 yılında bu duvar süsünde dışarıdan gönderilen mikrodalgalarla bir mikrofon gibi görev yapan ve konuşmaları dışarı aktaran bir yankılama çukuru olduğu tespit edilmiştir. Soğuk savaş döneminin sonuna kadar ülkeler arasında benzer pek çok teknik kullanılmıştır.
- Hedef konuşmaların yer aldığı odada bulunan bir pencere gibi tam yansıtıcı veya yarım yansıtıcı bir yüzeye dışarıdan gönderilen lazer ışını, lazer mikrofonu görevi görür. Ses dalgaları, yansıyan lazer ışığında çeşitli modülasyonlar meydana getirir. Bunlar uzaktan alınarak deşifre edilir.
- Hükümetler tarafından kullanılan yüksek maliyetli frekans atlamalı ve demet gönderme tekniklerini kullanan cihazlar. Bunların yakalanma ihtimali çok düşük olup uzaktan açılıp kapatılabilirler.
- "Jitterbug" denilen keyboard kablosuna yerleştirilen dinleme düzenekleri. Şifre gibi klavyeden girilen verileri algılayan bu sistem ile saldırgan şifreli dahi olsa tuşlara basma hareketlerinden gizlenen bilgileri ele geçirebilir.
- Optik dinleme hususunda yüksek çözünürlüklü kameralara sahip uydular. Kullandığımız bilgisayarların ekranının pencereye dönük olması durumunda ekrandaki bilgilerin analiz edilmesi mümkündür.
- Günlük hayatımızın bir vazgeçilmezi olan telefonlardaki risk pek çok insanının inanmak istemeyeceğinden çok daha fazladır. Her geçen gün daha fazla sayıda insan rahatlığı nedeniyle kablosuz telefonlara yönelmekte ancak kolayca dinlenebileceklerini göz ardı etmektedirler. Telefonlar kolaylıkla maniple edilebilir ve uzaktan yapılacak bir müdahale ile kullanıcının kontrolü dışında açık hale getirilebilir. Bu özellik hali hazırda pek çok dijital telefon ve dijital telefon santralinde bulunmaktadır ve bazı üretici ülkelerin bunu ürünü ithal etme şartı olarak öne sürdükleri söylenmektedir.
- Sıradan bir diz üstü bilgisayar da bir yazılım vasıtasıyla açılıp kapatılabilen bir mikrofona sahiptir ve bu bilgisayarlar genellikle internete bağlı olarak çalışırlar, en azından zaman zaman dış ağlarla bağlantı kurarlar. Bu sayede saldırganlar bilgisayarın bulunduğu ortamdaki konuşmaları kaydederek kullanıcının kolaylıkla fark

edemeyeceği bir şeklide kendilere e-posta gibi yöntemlerle yönlendirebilirler.

- Bazı oyuncaklar da bilindiği gibi etrafında yapılan konuşmaları kaydetmekte ve bunları daha sonra rastgele tekrar etmektedir. Böyle masum bir oyuncak bile iş yerimize gelen küçük bir çocuğun gafil muhbirlik yapmasına neden olabilir. Bu konuda yaşanmış örnekler bulunmaktadır.

3. TEMPEST KAVRAMI

TEMPEST, gizlilik dereceli bilgi işleyen elektriksel veya elektronik cihazlardan kaynaklanan istenmeyen elektromanyetik enerji yayılımları ile bu yayılımların araştırılması, incelenmesi ve denetim altına alınması olarak tanımlanır. TEMPEST kaçaklarını bilgi içeren kaçaklar olarak da isimlendirebiliriz.

Bu tanımı detaylandıracak olursak:

- TEMPEST kaçakları istem dışı olarak oluşur; Elektronik cihazlarda işlenmekte olan açık bilgiler cihazın normal çalışma fonksiyonu dışında yaptığı yayımla dışarı kaçabilir.
- TEMPEST kaçakları belli bir frekansta bilgi taşıyan işaretlerdir.
- TEMPEST kaçakları havadan veya kablo üzerinden yayılırlar. Bu işaretlerin değerlendirilebilmesi için anten ile havadan veya bir sonda kullanılarak kablodan elde edilmesi gerekmektedir.
- TEMPEST kaçakları ilk ele geçirildiklerinde çok anlamlı görünmeyebilirler, bu nedenle çözümlenmeleri gerekmektedir. Çözümlemeler sonucu elde edilen bilgiler şifrelenen açık bilgileri içermelidir [4].

TEMPEST kelimesinin bir kısaltmayı ifade edip etmediği halen tartışılan bir konudur. Ancak Amerikan Hava Kuvvetlerinin gizliliğini kaldırarak yayımladığı bir dokümanda TEMPEST "Transient Elektromagnetic Pulse Emanation Standard" ifadesini oluşturan kelimelerin baş harfleri olarak tanımlanmıştır [17].

3.1. Bilgi içeren kaçakların oluşumu

Bilgi içeren kaçakların oluşma mekanizmasının temellerinin anlamak için sayısal devrelerdeki işaret oluşum aşamalarını incelemek gerekir. Sayısal devrelerde işaretler sıfır ve birlerden oluşur. İşaret sıfır seviyesinden bir

seviyesine geçerken tüketilen enerji, o seviyede değişmeden kalabilmesi için gereken enerjinin yaklaşık bin katıdır. Bu fazla enerjinin %1'lik kısmı yeni gerilim seviyenin sürmesine harcanır, yaklaşık %4'ü ısıya dönüşür, geri kalan kısmı ise elektromanyetik dalga olarak ortama yayılır. Bu yayılan dalga yalnızca gürültü içerebildiği gibi oluşumunda etken olan bilgi ile ilgili işaret kaçaklarını da içerebilir. Eğer elde edilen bu işaret gizli bilgi içeriyor ise buna bilgi içeren kaçak denir [4].

3.2. Elektro Manyetik Yayılım Güvenliği

Yayılım güvenliği (Emission Security -EMSEC); cihazların, donanımlarından kaynaklanan elektromanyetik yayılımlar neticesinde sistemin, maruz kalacağı yetkisiz erişimlere karşı hassasiyetinin analizidir. Özellikle bilgisayarlar ve diğer cihazlardan Radyo Frekans (RF) sinyalleri şeklinde yayılan sinyallerin düşmanın eline geçtiğinde verinin yeniden yapılandırılıp elde edilebilmesi nedeniyle askeri kurumlar TEMPEST konusuyla yakından ilgilidir.

Ancak TEMPEST problemi sanıldığı gibi yalnız askeri ve istihbarat kurumları ile sınırlı değildir. Sivil kuruluşlar ve sıradan insanlar da günümüzde kolaylıkla bu saldırılara maruz kalabilmektedirler. Nitekim elektronik seçim karşıtı Hollandalı bir grubun, seçmenlerin oy makinesinden oy kullanmalarının ardından hangi partiye oy verdiğini tespit etmeleri ile elektronik seçimler için de TEMPEST bir sorun haline gelmiştir [18].

Gündelik hayatımızın bir parçası olan akıllı kartlar (Smart Card), düşük maliyetli Donanım Güvenlik Modülü (Hardware Security Module – HSM) üzerinde bulunan yonga sayesinde kripto anahtarlarını ve kriptografik fonksiyonları saklarlar. Banka kartları ve abone tanımlama kartları (Subscriber Identity Modules-SIM) en yaygın kullanılan akıllı kartlardır. Üzerlerinde yüklü anahtarın çözülebilmesi için yonganın karttan sökülerek incelenmesi gerekir, bu oldukça zor ve fark ettirmeden yapılması güç bir iştir. Ancak anahtar bilgilerini yonganın davranışlarından faydalanarak elde etmek mümkündür. Saldırgan tarafından kurulacak basit bir düzenekle işlem esnasında kartın çektiği akımın analiz edilerek şifre veya anahtar bilgisi gibi bilgilerin elde edilmesi ve kartların kopyalanması mümkün hale gelmiştir. Güç Analizi (Power Analysis) olarak adlandırılan bu yöntemde karta herhangi bir müdahale olmadığından yapılan işleme dair herhangi bir iz de bırakılmamaktadır.

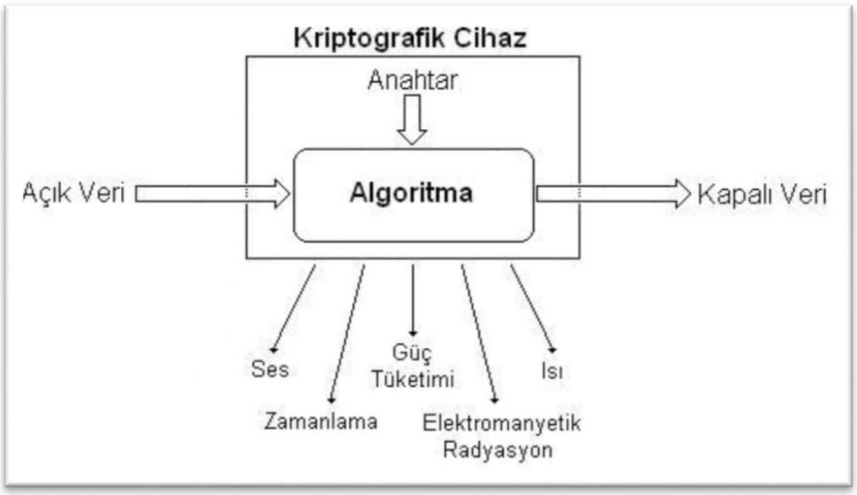
Araştırmacılar aynı zamanda cihazlardan yayılan ışık (optik), ısı (termal) ve ses (akustik) dalgaları vasıtasıyla yapılan saldırılar da keşfetmiştir. Bu

yöntem, haberleşme için kullanılan asıl kanalın haricinde bilgi kaçaklarının gerçekleştiği ikincil bir kanal olan Yan Kanal Saldırıları (Side Channel Attacks) olarak adlandırılır.

TEMPEST saldırıları, saldırganların istihbarat elde edecekleri cihaza müdahale yöntemlerine göre aktif ve pasif TEMPEST saldırıları olmak üzere ikiye ayrılır. Bu saldırılara karşı alınacak EMSEC önlemleri, sistemleri istem dışı olarak yok edebilecek potansiyele sahip, Elektromanyetik Uyum (Elektromagnetic Compabilitiy -EMC) ve Elektromanyetik Girişim (Electromagnetic Interference – EMI) konularıyla yakından ilgilidir.

3.3. Yan Kanal Analizi

Tüm elektronik cihazların çalışmaları esnasında kendi işlevlerinin yanı sıra bazı istemsiz çıkışlar da ürettiğinden daha evvel bahsedilmişti. Bu istemsiz çıkışlar Şekil 1.'deki kriptografik cihaz örneğinde gösterildiği gibi; bir işlemin yapılmasının ne kadar zaman aldığı, cihazın ne kadar güç harcadığı, ne kadar elektromanyetik yayılım yaptığı, nasıl ve ne şiddette sesler çıkardığı veya ne kadar ısı yaydığı olabilir. Bu tür elektromanyetik kaçaklar olarak adlandırılan istem dışı çıkışlar, cihaz içinde saklanan bilginin tamamıyla veya bir parçasıyla ilişkiliyse, bu kaçaklar yan-kanal bilgisi olarak adlandırılır. Yan-Kanal bilgilerinin analiz edilerek yapıldığı saldırılarda, bu bilgiler kullanılarak gizli bilgiye ulaşılmaya çalışılır.



Şekil 1. Kripto cihazlarında meydana gelebilecek istem dışı çıkışlar [19]

Yan kanal analizi saldırıları, şifreleme algoritmaları kullanan sistemler için de büyük bir tehdit oluşturmaktadır. Yapılan araştırmalarda, DES, AES ve RSA'nın da içlerinde olduğu birçok algoritmanın kanal analizi saldırılarına karşı savunmasız olduğu gösterilmiş ve alınabilecek çeşitli önlemler ileri sürülmüştür [19].

Aynı algoritmanın farklı gerçeklemeleri değişik miktar ve biçimlerde yan kanal bilgisi sızdırabilir. Bu nedenle, yan-kanal analizi saldırıları genelleştirilemezler. Ancak bu saldırılar genellikle pratikte kullanılmaya uygundur.

4. TEMPEST SALDIRILARI

Yukarıda verilen bilgiler doğrultusunda, günümüzde varlığından haberdar olunan TEMPEST saldırılarının neler olduğu ve nasıl gerçekleştirildiği ile alınabilecek önlemler aşağıda sunulmuştur.

4.1. Zamanlama Analizi (ZA) Saldırıları

Zamanlama analizi (ZA) saldırılarında, veri işleme zaman süreleri değişken olan şifreleme algoritmalarının sızdırdığı yan-kanal bilgilerinden faydalanılır. Bu tür algoritmalarda her adımda gerçekleştirilen işlem süresi, kullanılan gizli anahtara bağımlı olduğundan saldırgan tarafından sistemden elde edilen yan kanal bilgileri toplanır [9, 19]. Bu bilgiler, anahtara bağlı olarak yapılan dallanma işlemlerinden, farklı karmaşıklıklarda işlemler kullanılmasından, kullanılan iyileştirme tekniklerinden veya önbellek kullanımından kaynaklanabilir. Özellikle asimetrik anahtarlı algoritmalar için bu durum geçerlidir. Simetrik anahtarlı algoritmaların zamanlama karakteristikleri, asimetrik-anahtarlı algoritmalar kadar anahtara bağımlı olmadığı için zamanlama analizi saldırılarına karşı daha güçlüdürler.

4.1.1. RSA Algoritmasına ZA Saldırıları

1996'da Paul Kocher, yaptığı çalışmalarda RSA gibi pek çok açık anahtar uygulama algoritmasının, anahtar bilgisini uygulama çalışma süresi üzerinden sızdırdığını göstermiştir [9]. Aşağıda RSA algoritması üzerinden zamanlama analizi tekniği kullanılarak gizli anahtarın nasıl elde edilebileceği anlatılmıştır. RSA algoritmasında gizli anahtarın kullanıldığı işlem,

$$R=f(x, y) = y^{x} \bmod n,$$

şeklindedir. Burada; n bilinen bir değerdir, y ise giriş değeridir. Saldırganın amacı gizli anahtar bilgisi olan x'in bulunmasıdır.

Kaynak [9]'da önerilen saldırıda kripto cihazına, $y^x \bmod n$ değeri, k adet farklı y değeri için hesaplattırılır. Tüm y değerlerine karşı düşen işlem süreleri saldırgan tarafından kaydedilir. İşlemlerin süresi, saldırgan tarafından, girişlerin hedeflenen cihaza ulaşmasıyla çıkışın üretilmesi arasında geçen zamana bakarak ölçülebilir. Ayrıca saldırının başarılı olabilmesi için, tüm işlemler boyunca aynı x değerinin kullanılması gereklidir.

Saldırı, sabit süreli olmayan işlemler içeren herhangi bir yapı için çalışabilmektedir. Örneğin aşağıdaki, $R = y^x \bmod n$ (x, w-bit uzunluğunda olmak üzere), değerini hesaplamakta kullanılan algoritma ele alınırsa;

$s_0 = 1,$

$0 \le k \le (w-1)$ için;

Eğer $x_k = 1$ ise,

$R_k = (s_k \times y) \bmod n,$

Değilse,

$R_k = s_k$

$s_{k+1} = R_k^2 \bmod n$

Sonuç $= R_{w-1}$

saldırı yöntemi kullanılarak, üssün ilk b biti biliniyorsa, $(b+1)$'inci biti elde edilebilir. Bu şekilde tüm kuvvet terimi bitleri elde edilir. İlk b bit değeri bilindiği için, algoritmanın ilk b adımı hesaplanarak s_b değeri bulunur. Sonraki adım, ilk bilinmeyen bit değerini gerektirir. Eğer bu bit '1' ise, $R_b = (s_b \times y) \bmod n$ işlemi yapılır, bit '0' ise bu işlem atlanır. Saldırıda bu dallanmadan faydalanılır.

Bazı (s_b, y) değerleri için, $R_b = (s_b \times y) \bmod n$ işlemi normalde aldığından çok daha uzun süre alır. Saldırgan sistemin yapısını inceleyerek bu değerleri hesaplayabilir. Eğer, $R_b = (s_b \times y) \bmod n$ hesabını çok yavaşlatan bir y değeri için, toplam üs alma işlemi kısa sürede tamamlanıyorsa, b indisli anahtar biti '0' olmalıdır. Çünkü $R_b = (s_b \times y) \bmod n$ hesabı atlanmış,

böylelikle onun yaratacağı fazladan gecikme oluşmamış olacaktır. Benzer şekilde, $R_b = (s_b \times y) \bmod n$ hesabını çok yavaşlatan bir y değeri için, toplam kuvvet alma işlemi normalden daha uzun sürede tamamlanıyorsa, b indisli anahtar biti '1' olmalıdır. Çünkü $R_b = (s_b \times y) \bmod n$ hesabı yapılmış, böylelikle onun yaratacağı fazladan gecikme toplam işlem süresine eklenmiş olacaktır. Anahtarın ilk biti '0' olarak kabul edilerek yukarıdaki şekilde anahtarın tüm bitleri bulunur. Aynı şekilde ilk bit '1' olarak kabul edilerek yukarıdaki şekilde anahtarın tüm bitleri bulunur. Sonuç olarak iki başlangıç değerinden birisi için doğru sonuca ulaşılır [19].

2003 yılında David Brumley ve Dan Boneh, OpenSSL kullanarak Apache uygulamasına bir Zamanlama Analizi Saldırısı gerçekleştirdiler. Bu çalışmalarında, uzak bağlantıdaki bir sunumcudan milyonlarca şifre çözme işleminin zaman analizini yaparak gizli anahtarın nasıl elde edilebileceğini gösterdiler [25]. Bazı uygulamalar bu duruma engel olmak için "blinding" olarak tabir edilen maskeleme özelliğine sahiptirler. OpenSSL maskeleme seçeneği sunarken Apache uygulamasında bu özellik bulunmamaktadır.

Zamanlama saldırılarına karşı koyabilmek için şifreleme algoritmalarında her bir işlem sabit işletim süresine sahip olacak şekilde tasarlanmalıdır. Zamanlama analizine karşı koyma yöntemlerinden bazıları [26, 27, 28, 29]'da bulunabilir. Bununla birlikte, zamanlama bilgisi diğer yan-kanal bilgileriyle birlikte kullanılabilir. Örneğin zamanlama bilgisi, bir algoritmanın yalnızca belirli parçalarını belirlemek amacıyla kullanılabilir [19].

4.2. Güç Analizi (GA) Saldırıları

Bir kaçak tespit edilene kadar güç filtreleri kullanımının ne kadar önemli olduğu fark edilemez. Bunun en güzel örneklerinden biri akıllı kartlardır. Akıllı kartlar genellikle çok ince bir taşıyıcı zemin üzerine monte edilmiş tek bir silikon yongadan oluşur. Kondansatör, bobin gibi yarı iletken devre elemanlarını kullanarak güç kaynağını filtrelemek için çok az bir alan vardır. Kartların maliyetleri düşünüldüğünde bu tür özelliklerin eklenmesi kart maliyetini artıracağından üreticiler tarafından da pek tercih edilmemektedir.

Sistemin bağlı olduğu güç kaynağı veya akıllı kart okuma düzeneği saldırganların kontrolünde olabilir. 1990'ların başında akıllı kartların yapmış oldukları işlemler hakkında pek çok bilginin, bağlı oldukları güç kaynağından çektikleri akımın incelenmesi sonucu elde edilebileceği tespit edilmiştir. Bu saldırı tipi Güç Analizi (Power Analysis) veya Ray Gürültüsü Analizi (Rail Noise Analysis) olarak bilinmektedir ve cihazın

bağlı olduğu toprak hattına yalnızca 10Ω'luk bir direnç ve bir osilaskobun bağlanarak, cihazın çektiği akımı gösteren dalgalanmaların gözlemlenmesiyle elde edilir. [16].

Her uygulama farklı bir güç tüketim profiline sahiptir ayrıca mikro işlemcide işlenen veri de güç tüketim profilinde değişiklikler meydana getirir. Pek çok elektronik devrede en temel veri bağımlı olarak çalışan eleman veri yolu transistorlarıdır (Bus Drivers). Devrenin tasarımına bağlı olmakla birlikte veri yollarından çekilen akım, burada işlenen her bir bit değişiminde, birkaç yüz nano saniyelik periyotta, mikro amper seviyesinde yüzlerce farklı değer meydana getirmektedir [30].

Bir lojik kapının güç tüketimi giriş değerleri ile doğrudan ilişkilendirilebilir. Giriş değerinin değişmesi, çıkışın konum değiştirmesine ve dolayısıyla dinamik güç tüketimine neden olabilir. Bu nedenle, CMOS kapıların güç tüketimi, kapı girişleri gizli bir bilgiye bağlıysa, yan-kanal bilgisi olarak kullanılabilir [33]. Farklı işlemlerin farklı güç tüketim karakteristiğine sahip olması, saldırıların başarısını arttırır.

Güç analizi (GA) saldırılarında, kriptografik cihazın güç tüketimi ile gizli bilgi ya da yapılan işlemler arasında bir korelasyon kurularak gizli bilgiye erişilmeye çalışılır [24, 34]. Bunun için öncelikle güç tüketiminin ölçülmesi gerekmektedir. Bu amaçla, devre ile kaynak arasındaki hat üzerine küçük değerli bir direnç yerleştirilir ve bu direncin her iki ucundaki gerilim değerlerinin farkından yararlanılarak çekilen akım bilgisi elde edilir [35].

Güç analizi saldırıları ilk kez Kocher tarafından DES algoritması üzerinde uygulanmıştır [33]. Bu uygulamanın başarısının ardından, güç analizi üzerine pek çok çalışma yapılmıştır.

Bir diğer yöntem ise farklı sensörler kullanmaktır. David Samyde ve Jean Jacques Quisquarter, cihazın güç kaynağından elde edilen analiz verileri yerine yonga üzerinde gezdirdikleri bir bobin ile elde ettikleri sinyaller ile elektromanyetik analiz gerçekleştirmişlerdir. Son olarak Sergei Skorobogatov cihaz üzerinde bulunan hedef transistorde lazer aydınlatması kullanarak her bir bite erişim sağlamıştır. Bu yöntemle cihaz epoksi kaplama ile korunmuş olsa da bellek yapısındaki transistorlara ulaşılmaktadır [36].

4.3. Elektromanyetik Analiz (EMA) Saldırıları

Lojik devrelerin güç tüketimi, işledikleri anlık veriye göre farklılıklar gösterir. Bu durum sistemden çektikleri akımın da değişmesine ve dolayısıyla yeni bir yan-kanal bilgisi oluşumuna neden olur. Çünkü devre içerisinde tüketilen akımların değişmesi, devrenin ortama yaydığı elektromanyetik radyasyonun da değişmesine, dolayısıyla yan-kanal bilgisi sızdırmasına neden olur. Ayrıca, devre içerisinde oluşan çeşitli kuplajlar ve frekans modülasyonları da elektromanyetik radyasyona, dolayısıyla yan-kanal bilgisi oluşumuna neden olabilir. Elektromanyetik Analiz (EMA: Electromagnetic Analysis) saldırıları bu yan-kanal bilgisini kullanır.

EMA saldırıları da basit ve diferansiyel olarak ikiye ayrılmaktadır. Ölçüm aşamasından sonra, EMA saldırılarında kullanılan analiz yöntemleri, güç analizi yöntemlerinde kullanılanlarla hemen hemen aynıdır. EMA saldırılarının güç analizi saldırılarına göre önemli avantajları vardır. Öncelikle, GA saldırılarının aksine, ölçümler hedeflenen cihazla hiçbir fiziksel bağlantı kurmadan da belirli bir mesafeden gerçekleştirilebilmektedir. Ayrıca ölçümler cihaz üzerinde istenilen noktalara odaklanabilir [19].

Özel olarak TEMPEST korumalı olarak tasarlanmadıkları sürece tüm ekranlar (Visual Display Unit-VDU) gösterilen resmin biraz bozuk versiyonunu içeren zayıf bir VHF veya UHF radyo sinyali yayarlar. Görüntü sinyali cihaz üzerinde belirli noktalardan elde edilebilir. Bu sinyal, bazıları diğerlerinden daha belirgin bir şekilde ışıyan noktalara ait harmonikler içerir. Uygun bir geniş band alıcıyla bu yayılımlar alınarak tekrar görüntü sinyaline dönüştürülebilir. Kablolar ve diğer bileşenler ise kendi dalga boylarında rezonans sinyallerine sahiptirler. Genel inancın aksine LCD ekranlar da bu tür bilgi kaçaklarına karşı savunmasızdırlar. Kasanın menteşeleri arasından geçerek diz üstü bilgisayarın ana kartı ile LCD bağlantısını sağlayan veri kablosu görüntü sinyalleri içermektedir. Şekil 2'de bir dizüstü bilgisayardan elde edilen ekran görüntüsü yer almaktadır.

Şekil 2. Toshiba dizüstü bilgisayarın arada üç alçıpan duvar bulunan başka bir odadan elde edilen ekran görüntüsüne ait RF sinyali [44]

Bankacılık sektörü de elektromanyetik kaçaklardan kaynaklanan saldırılara maruz kalmaktadır. 1990'ların sonunda Hans Georg Wolf bir ATM makinesine 8 metre mesafeden kart ve PIN bilgilerini ele geçirebilen bir TEMPEST saldırısını ispatlamıştır [45].

TEMPEST önlemleri savunma sektörü dışında çok yaygın olarak kullanılmamaktadır. Ancak son zamanlarda oy kullanım işlemlerinde kullanılan seçim makineleri de bu saldırılara karşı savunmasız hale gelmiştir. Ekim 2006'da elektronik seçim makineleri kullanılarak yapılan oylamalara karşı olan Hollandalı bir grup, Hollanda'da yapılan bir seçimde oyların kullanıldığı seçim makinelerinin %90'ının onlarca metre mesafeden dinlenebildiğini kanıtlamıştır [18]. Bu olaydan sonra Hollanda hükümeti seçim makinelerinin "Zone-1-12db" standartlarında olmasını şart koymuştur.

Bu sistem şöyle çalışmaktadır; Zone.0 olarak sertifikalandırılmış bir cihaz 1 metrelik bir alan içerisinde ele geçirilebilir nitelikte bir sinyal yaymamalıdır. Veriyi yan odalar gibi kısa mesafelerden yapılabilecek elektromanyetik dinlemelere karşı korumalıdır. Zone-1 cihazlar 20, Zone.2 120m., Zone.3 1200 metrelik bir alanda koruma sağlamak üzere sertifikalandırılmıştır [16].

Zone sistemi, soğuk savaşın bitimiyle birlikte hükümetler tarafından da yaygın bir şekilde kullanılmaya başlandı. Hangi cihazın ne kadar yayılıma neden olduğu bilinirse cihazlar bu değerlere göre binaların çevresine en uzak noktalara konumlandırılır ve yalnızca gerekli durumlarda koruma (shield) önlemleri alınır. Milli istihbarat gibi en hassas sistemler ve büyükelçilikler gibi en çok tehdide maruz kalan birimlerde ya korumalı cihazlar ya da korumalı odalar kullanılır. Zone uygulaması yayılım güvenliği konularında yapılan harcamalarda büyük oranda tasarruf sağlar ancak yine de NATO gibi organizasyonlar bu harcamalara milyar dolarlar seviyesinde paralar harcamaktadır.

Bu harcamaları azaltmak maksadıyla Markus Kuhn ve Ross J. Anderson e-posta kriptolama paketinden seçim makinelerine kadar pek çok cihazda kullanılabilecek, daha düşük maliyetli "Soft TEMPEST" teknolojisini geliştirmişlerdir [10]. Soft TEMPEST bir bilgisayar sisteminden yayılan elektro manyetik dalgaları engellemek ve filtrelemek için yazılım tekniklerini kullanan bir teknolojidir.

ABD'de bir organizasyon şirketi olan SFX Entertainment'ın müşteri profilleri oluşturmak maksadıyla, müşterilerinin organizasyon alanlarına gelirken araç radyolarından sızan RF sinyallerini dinleyerek, araçlarında hangi radyoyu dinledikleri verilerini topladığı tespit edilmiştir. Bu durum yasal olmasına rağmen, özel hayatın gizliliğini ihlal ettiğini düşünenleri kızdırmıştır. Ancak aynı yöntemin, otomobil satıcıları, alışveriş merkezleri ve radyo/TV istasyonları tarafından da kullanıldığı bilinmektedir [16].

Bir başka saldırı tipi de klavye dinleme saldırılarıdır. Bilindiği gibi klavyenin içerisinde basit bir mikroişlemci ve tampon bellek bulunmaktadır. Klavyeden herhangi bir tuşa basıldığında, tuş altındaki plastik yay ezilerek altındaki kömür tabaka içerisinde bulunan gümüş nitrat içerikli devreyi kapatır. Kapatılan devre klavye içerisinde bulunan mikroişlemciye sinyal gönderir. Mikroişlemci bu sinyali hex kodları yardımıyla bilgisayara gönderir ve bilgisayar hangi tuşa basıldığını bu hex kodları sayesinde anlar. Aynı şekilde tuş bırakıldığında da bilgisayara bir hex kodu gönderilir ve bu da tuşun bırakıldığını bilgisayara iletmiş olur. Klavye ile bilgisayar arasındaki bu bağlantı tek yönlü değildir. Aynı zamanda bilgisayar da klavyeye sinyal gönderir. Bu, NumLock gibi ledlerin ve tuş tekrarlamalarının ayarlanmasını sağlar. Bu bilgi akışının üzerinden gerçekleştiği klavye kablosu hem ortama yaydığı elektromanyetik dalgalarla hem de üzerine yerleştirilebilecek düzeneklere karşı oldukça savunmasızdır. Klavye kablosuna yerleştirilen bu düzenekler sayesinde, şifreler gibi klavyeden girilen gizli verileri algılayan sistemler

ile saldırgan, şifreli dahi olsa tuşlara basma hareketlerinden gizlenen bilgileri ele geçirebilmektedir.

4.4. Çentik Saldırıları (Glitch Attacks)

Aktif EMSEC saldırıları akıllı kartlar dünyasında da önemli yer tutar, bunlardan en çok bilineni "Glitch Attack" olarak bilinen Çentik Saldırılarıdır. Burada saldırganlar güç ya da frekans değerlerinde ani değişiklikler yaratarak kendilerine yarayabilecek bir hata oluşturmaya çalışırlar. Lazer saldırılarıyla da aynı sonuçlar elde edilebilir [48].

Örneğin eskiden kullanılan banka kartlarında bulunan bir güvenlik açığı nedeniyle çok yüksek seviyedeki saat sinyali birkaç işlem turundan sonra program sayacında bir sıfırlamaya neden olmaktaydı, yani karta dışarıdan uygulanacak böyle bir sinyal girişimi, kartta hata oluşturmak yerine yalnız sıfırlama işlemine neden olmaktaydı. Bu güvenlik açığı sayesinde işlemcide yapılan tüm işlemler durdurularak bir NOP üretilmesi sağlanır. Bu işlem çok güçlü bir seçici kod çalıştırma (selective code execution) saldırısına yol açar. Örneğin saldırgan JUMP sinyallerine sirayet edebilir ve böylece erişim kontrolü engelini rahatlıkla aşabilir [16].

4.5. Y Hata Farkı Analizi Saldırıları

Saldırganların kartın yazılım detayları ile ilgili bilgi sahibi olmadıkları durumlarda dahi çentik saldırıları çok etkili olabilmektedir. Dan Boneh, Richard De Millo ve Richard Lipton bazı açık anahtar kullanan şifreleme algoritmalarında rastgele bir hata oluşturulabilirse şifrenin kırılabileceğini göstermişlerdir [49]. Örneğin RSA algoritmasında Şifre hesaplamasında;

$$S=h(m)^d \ (mod\ p\ q)$$

işlemi sonucunda öncelikle mod p daha sonra da mod q bulunur ve sonuçlar daha sonra birleştirilir. Fakat kart mod p'si doğru mod q'su hatalı bir işaret (Sp) üretirse sistemi kıran saldırgan,

$$p=gcd(pq,S^e_p-h(m))$$

formülüne ulaşılır. Bu saldırılar çentik saldırılarına karşı koruması olmayan kartlara kolaylıkla uygulanabildiği gibi pek çok simetrik algoritma ve protokole de uygulanabilir.

Eli Biham ve Adi Shamir yaptıkları çalışmada, eğer bellekte yer alan bir biti sıfır veya bir yapma imkânımız olursa ve anahtar bilgisinin hafızada

nerede tutulduğu biliniyorsa, anahtarın çözülebildiğini göstermişlerdir. Bunun için öncelikle bir şifreleme yaparak anahtarın ilk biti sıfırlanır, daha sonra tekrar şifreleme yaparak sonucun farklı olup olmadığına bakılır, bir sonraki bit ve diğerleri aynı şekilde denenerek anahtar bulunabilir [50].

4.6. Optik –Akustik ve Termal Saldırılar

Son yıllarda yan kanal saldırılarında ilgi çekici yeni çalışmalar yapılmaktadır. Geceleri çalışan iş yerlerine bakıldığında buralarda bilgisayar karşısında çalışan birinin yüzünde veya üzerindeki gömleğinde ya da odanın duvarlarında ekran görüntüsüne göre çeşitli ışık değişimleri olduğunu görülür. 2002 yılında Markus Kuhn bir osilaskopa yüksek performanslı bir photomultiplier tüpü monte ederek pek çok VDU tüpünde kullanılan mavi ve yeşil fosfordan kaynaklanan ışık huzmelerinin birkaç mikro saniye sonra parçalanarak dağıldığını tespit etti. Dağılarak yansıyan bu ışık huzmelerinde ekrandaki görüntüye ait verilerin pek çoğu bulunmaktaydı. Bu çalışmayla bir teleskop veya photomultiplier tüpü ile uygun bir görüntü işleme yazılımı vasıtasıyla ekranın karşısında duran bir çalışanın yüzünden veya gömleğinden yansıyan ışıkla ekrandaki verinin okunabileceği gösterildi [12].

Daha sonra Lougry ve David Umphress modem, router, PC seri data hattı gibi haberleşme cihazlarının LED durumlarını incelediler. Bunların önemli bir kısmının veriyi optik olarak gönderdiklerini tespit etiler (12 modemin 11'i, 7 Router'ın 2'si ve bir veri depolama cihazı). Bu cihazları tasarlayanlar bir LED'in dinlemeye rahatlıkla maruz kalabilecek bir veri gönderme bant genişliğine sahip olduğunun farkında olmadan seri data hattının sayaç (tell-tale) ışığını kullanıyorlardı [51].

Nokta vuruşlu tazıcılar ve daktilolarda yazılan metinlerin cihazların çıkardıkları sesler yardımıyla elde edilebileceği efsanesi hep konuşulmuştur. Dimitri Asonov ve Rakesh Agraval 2004 yılında yaptıkları çalışmada bir bilgisayar klavyesinin her bir tuşunun ayırt edilebilir nitelikte farklı sesler çıkardığını tespit etmiş ve bir sinir ağı (Neural Network) çalışmasıyla çok düşük hata payıyla, klavye tuşlarından yayılan ses dalgalarını ayrıştırarak yazılan metni ortaya çıkarmışlardır [13]. Dawn Song, David Wagner ve XuQuing Tian, aralarında saldırganlar tarafından tespit edilebilecek zaman farkları olan tuş darbelerinin, bireysel paketler halinde gönderildiğinden, SSH kriptolu oturumlarda önemli miktarda veri sızıntısı olduğunu gösterdiler ve bunun şifrelenmiş haldeki passwordu ele geçiren bir saldırgana, yapacağı tahmin işlemlerinde 50 faktöriyellik bir avantaj sağladığını tespit ettiler [52].

2005 yılında Li Zhuang, Feng Zhou ve Doug Tygar bu tehditlerin bir kombinasyonunu oluşturarak çok daha güçlü bir saldırı metodu geliştirdiler. Her hangi biri tarafından, İngilizce olarak, 10 dakika boyunca, bilinmeyen modelde bir klavye ile yazılmış bir metne ait akustik kayıtları inceleyerek her bir tuş sesini ayrıştırdılar. Daha sonra İngilizcenin bilinen istatistikî bilgileri ve tuşlar arası basma zamanlarını inceleyerek hangi sesin hangi tuşa ait olduğunu tespit ettiler. Böylece daha önce hiçbir şekilde bilgi sahibi olmadıkları, kim tarafından ve hangi model klavye kullanarak yazıldığını bilmedikleri bir akustik kaçak kaydından orijinal metnin elde edilmesi başarılmış oldu [14].

Son gelişmeler ise gizli termal yan kanallardır. 2006 yılında Steven Murdoch uzak mesafeden de ölçülebilen tipik bir bilgisayar saat sinyali eğrisinin rutin bir değişim gösterdiğini ve bu durumun çevre ısısının bir sonucu olduğunu fark etti. Deneylerinde herhangi bir önlem alınmadığı takdirde bilgisayardan kesin zaman bilgilerini çekebilen herhangi birinin CPU yükünü de ölçebileceğini gösterdi. Bu durum beraberinde dünyada herhangi bir noktaya gizlenmiş bir makinenin bu yöntemle bulunup bulunamayacağı sorusunu da gündeme getirmiştir [15].

4.7. Birleşik Saldırılar

Birleşik saldırılar hem aktif hem de pasif saldırı metotlarının kullanıldığı saldırı yöntemlerini ifade eder. Akıllı kart sistemlerinde kullanıcıya bir sayaç vasıtasıyla belirli sayıda giriş hakkı izni veren PIN kodu koruma sistemi kullanılmaktadır. Bu işlem esasında silinebilir bir (Electronically Erasable Programmable Read-Only Memory-EEPROM) belleğe veri girişi anlamına geldiğinden, verilerin yazılması esnasında, kart tarafından tüketilen akım değeri ölçülebilir bir şekilde yükselir. Çünkü Kaynak voltajını Vcc artıran kapasitif devre elemanları bu esnada bu sefer de programlama voltajını Vpp artırmaya başlar. Bu sayede bir saldırgan kartı yalnızca sıfırlayarak PIN sayacını devre dışı bırakıp bir sonraki PIN kodu girişini yapar. Bu yönteme karşı tedbir olarak modern kartlarda öncelikle sayaç azaltılmakta daha sonra PIN sorulmakta ve eğer PIN doğru ise tekrar sayaç artırılmaktadır.

Normal reset işlemini, saat sinyalinin birkaç tur yarım bir halde uygulanmasıdır. Bazı sistemlerde kart sıfırlama işlemlerini kontrol eden, entegre devreler gibi çok düşük veya çok yüksek saat sinyallerini tespit eden özel koruyucu donanımlar kullanır. Böylece bir şekilde izleme fonksiyonlarını devre dışı bırakabilen bir saldırganın kartı sıfırlaması engellenir.

Belleğe yazma anında yapılan bu tür birleşik saldırıların en önemlilerinden biri de Sergei Skorobogatov'un "Optically Enhanced Position-Locked Power Analysis" yöntemidir [53]. Bu yöntemde çentik saldırılarında olduğu gibi, güç analizi işlemi yapılırken hedef transistor bir lazer kullanılarak kısmen iyonize edilir. Bu yöntem hedef transistoru maniple etmek için lazer kaynağının gücü artırılarak tamamen aktif bir saldırıya da dönüştürülebilir.

Günümüzde akıllı kartlar saldırganlar tarafından bir test cihazına konulmakta ve kriptografik bir işlem başlatılmaktadır. Yonga içerisinde lazer kullanarak hassas olarak ölçülen her bir zaman biriminde tek bir işaretin değişmesi sağlanır. Hızlandırılmış bir düzenekle saatte yüzlerce farklı hedef denenebilir [16].

4.8. Ekran Görüntüsü Dinleme Saldırıları

Geniş bant anten, osilaskop ve spektrum analiz cihazlarından oluşan bir düzenek ile ofis ortamında çalışan bilgisayarlardan sızan radyo sinyallerini inceleyerek ekranda işlenen görüntünün elde edilmesi mümkündür. Bu durumun kanıtlanmasının ardından pek çok insan yaptıkları çalışmalarla veri hatlarından, sabit disklerden, CRT (Crystal Ray Tube) ekranlardan ve CPU (Central Processing Unit)'lardan da elektro manyetik yayılımlar vasıtasıyla sızan verilerin elde edilebileceğini gösterdiler.

Geniş bant antenler vasıtasıyla elde edilen, filtreleme, güçlendirme (amplifikasyon) ve anolog-dijital sinyal çevrimi gibi işlemlerden geçirilen sinyal, daha sonra da bağıl filtreleme, tanımlama ve yeniden yapılandırma teknolojilerini içeren bir takım ilave işlemlerden geçirilir.

Bu sinyallerin ele geçirilmesi ve işlenmesi sanıldığı kadar kolay değildir. Her cihaz farklı modülasyon ve bant genişliğinde çalıştığından doğru ara frekansı ve bant genişliğini bulacak tecrübeli operatörlere ihtiyaç vardır. Ayrıca yakalanan sinyalin kalitesi alıcı cihazın kapasitesine bağlı olarak değişim göstereceğinden iyi bir sinyal elde edebilmek için yüksek performanslı geniş bant alıcıları kullanmak gerekir. Ancak bu cihazlar hem çok pahalıdırlar hem de genel olarak çok yer kaplarlar.

TEMPEST saldırılarından en ilgi çekici olanlarından biri de monitörlerdeki görüntünün yalnız ortama yayılan elektromanyetik sinyaller vasıtasıyla ele geçirilmesidir. Bu maksatla, Wenhan YANG, Yinghua LU ve Jun XU tarafından hazırlanan, ofis ortamında çalışan bir bilgisayarın ekranında yer alan metnin nasıl ele geçirildiğini gösteren çalışma [54] aşağıda anlatılmıştır. Bu çalışmada bir geniş bant anten,

preamplifikatör, spektrum analiz cihazı ve bir osilaskop kullanılarak oluşturulan sistem ile yakalanan video sinyalinin çeşitli yazılımlar vasıtasıyla çözümlenerek ekranda görüntülenen metnin nasıl elde edildiği anlatılmıştır.

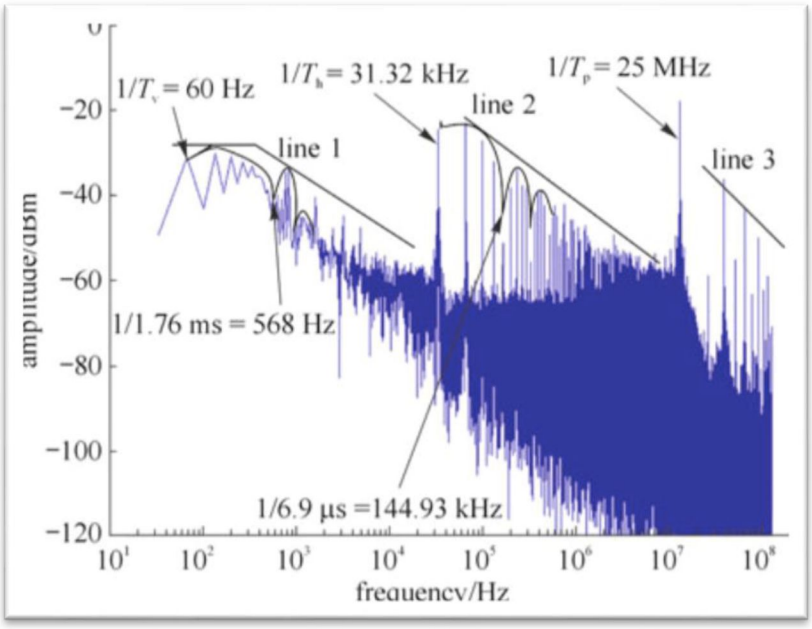
Laboratuar şartlarında yukarıda bahsedilen pahalı teçhizat olmaksızın yapılan bu testlerle bile elde edilebilen veriler, sistemin gerekli yatırım ve araştırmalarla geliştirilmesi durumunda neler yapılabileceğini açıkça göstermektedir. Bu çalışmada hedef bilgisayar 640x480 dpi çözünürlükte ve 60 Hz frekansında olup CRT monitöründe rastgele bir metin yer almaktadır.

Elektromanyetik sızıntılar sonucu yayılan radyo frekans sinyallerini tespit etmek maksadıyla osilaskop (Tektronix TDS5054B), spektrum analiz cihazı (HP8594), geniş bant antenler, preamplifikatör (Langer EMV-Technik PA 303) cihazları ile yazılımları çalıştıran bir bilgisayar kullanılmıştır.

İlk olarak yayılan video sinyalinin ortamda bulunan karmaşık elektromanyetik sinyallerden ayrıştırılarak frekansının ve bant genişliğinin tespit edilmesi gerekir. Bu maksatla;

- **1.Adım:** Bilgisayar kapalı iken ortamdaki elektromanyetik spektrum analiz edilir.
- **2.Adım**: Bilgisayar açık ve ekranında bir görüntü varken ortamda yer alan radyo frekans sinyalleri spektrumu analiz edilir.

Bilgisayardan sızan dalgaların tanımlanmasının ardından 500 Mhz'lik dijital örnekleme ayarlı bir osilaskop yardımıyla 0.04s'lik periyotlarla tek renk sinyalleri alınır. Daha sonra video görüntü sinyalinin yatay ve dikey eşleşmesi *Fast Fourier Transform* (FFT) yöntemi kullanılarak çıkarılır. Elde edilen sonuçlar Şekil 3'te gösterilmiştir.



Şekil 3. FFT yöntemi ile elde edilen temel band görüntü sinyali spektrumu [54].

Yukarıdaki şekilde FFT yöntemi ile elde edilen temel band görüntü sinyaline ait spektrumun 60 Hz'lik alan (field) frekansı, 31.32kHz'lik hat frekansı ve 25 Mhz.'lik uç frekansları içerdiği görülmektedir. Bu spektrumu analiz ederek aşağıdaki parametreleri bulabiliriz.

- Video görüntüsünün alan zaman periyodu: 1.76 ms. ve buna ait ana frekans şablon genişliği 568 Hz.
- Video görüntüsünün hat zaman periyodu 6.9 µs ve buna ait ana frekans şablon genişliği 144.93kHz.
- Video görüntüsünün Uç zaman periyodu 40 ns ve buna ait ana frekans şablon genişliği 25 Mhz.dir.

Böylece Spektrumda yer alan çizgileri tanımlayacak olursak Line 1 video görüntüsünün alan frekansı verilerini, Line 2 hat frekansı verilerini, Line 3 uç frekans verilerini içerdiğini söyleyebiliriz.

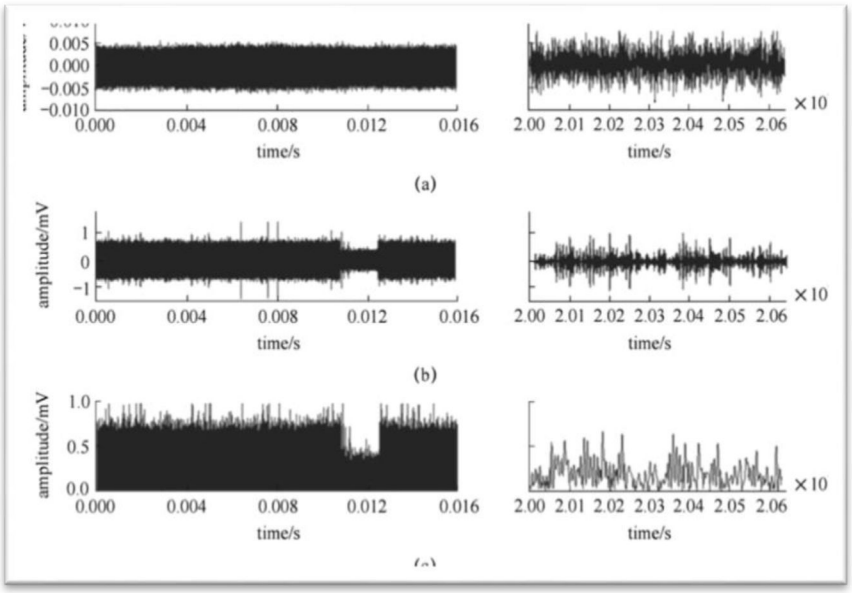
4.8.1. Ekranda Yazılı Metni Görüntüleme

Elektromanyetik yayılımlar geniş band antenler, frekans ayar mekanizmaları (tuning), band geçirici yükselteçler, Analog-Dijital çeviriciler vb. sistemlerin oluşturduğu düzenekler kullanılarak elde

edilebilir. Frame rate (birim zamanda yenilenen görüntü karesi sayısı) kontrol sinyalleri yakalandığında elektromanyetik kaçaklar, filtreleme, tanımlama ve yeniden yapılandırma teknolojileri kullanılarak işlenebilir ve böylece hedef bilgisayarın ekranında yer alan video görüntüsü elde edilebilir.

1992 yılında Joseph Mitola yazılım tanımlamalı radyo frekansı (Software-defined Radio (SDR)) kavramını ortaya çıkardı. Burada ana fikir; açık, standardize edilmiş ve A/D ve D/A çeviricileri antene yakın olan ve açık radyo frekans bağlantısını kurmak için bir takım yazılımlar kullanarak çeşitli fonksiyonları yerine getiren, esnek bir modüler donanım platformu oluşturmaktır [55]. Görüntünün yeniden elde edilmesi süreci yukarıda anlatılan geleneksel yöntemden 2 noktada farklılıklar gösterir. Bunlardan biri A/D çeviricilerin antene daha yakın olması diğeri ise analog işlem üniteleri yerine yazılımsal işlem ünitelerinin kullanılmasıdır. Hazırlanan düzenek yalnız bilgisayardan yayılan video sinyallerini değil aynı zamanda USB (Universal Serial Bus) kablosundan, CPU, sabit disk ve klavye gibi diğer donanımlardan açığa çıkan sinyalleri de alır. Böylece yazılımsal algoritmalar yardımıyla bilgisayardan sızan çeşitli elektromanyetik yayımları analiz edip bunları orijinal hallerine geri döndürerek yeniden yapılandırmak mümkün olur.

Şekil 4'te dijital sinyal işleme sürecine ait dalga formları görülmektedir. Analog RF sinyalinin dijital sinyale dönüşümü Şekil 4 (a)'da görülmektedir. Video verisi gürültü içerisinde tamamen bastırılmış haldedir. Band geçirici filtre (Bandpass Filter) ile elde edilen video IF sinyali Şekil 4 (b)'de gösterilmiştir. Burada video sinyalindeki dikey kesmeler daha net görülmektedir. Son olarak da Şekil 4 (c)'de gösterilen detektör amplifikatör ve gürültü temizleme ile elde edilen temel band görüntü sinyali elde edilir.



***Şekil 4**. Dijital sinyal işleme sürecine ait dalga formları [54].*

Ekrandaki görüntünün elde edilmesinden önce elimizdeki görüntü sinyalinin spektrumu analiz edilerek yatay ve dikey eşleşmeler ayrıştırılmalıdır [56-57]. Bu çalışmada yatay ve dikey senkronlar Th ve Tv olarak kaydedilmiştir. Son olarak metin, senkron sinyaline göre tekrar elde edilebilir. Görüntü sinyali aşağıdaki gibi ifade edilir.

$$S_p(t) = \sum_{n=-\infty}^{+\infty} a_n g_T(t - nT_p),$$

Burada $g_T(t)$, genişliği T_p ve genliği "1" olan ikizkenar (trapezoidal) yamuk şeklindeki sinyal eğrisidir.

Beyazdan siyaha doğru giden 256 seviyeli bir skalada, a_n 256 farklı değerden biri olup 0 ile 0.7 V arasında değerler alır. 0 V siyah pikselleri ifade ederken 0.7 V. beyaz pikselleri ifade eder. Şifre çözme (decoding) tek boyutlu sinyali zaman çerçevesinde iki boyutlu sinyal haline getirmektir. Bu nedenle, ilk olarak a_n skalasından $1 / T_p$ oranında değerler alacak şekilde sinyal maniple edilir. Daha sonra a_n serisi;

$$X_t x\ Y_t \quad (X_t = T_h / T_p \text{ ve } Y_t = T_v / T_h)$$

görüntü pikselleri serisi olarak yeniden düzenlenir. Son olarak, bu görüntüler sırasıyla 1 / *Tv* hızında oynatılarak hedeflenen görüntü sinyali elde edilir.

Geleneksel yöntemde öncelikle eldeki donanım aracılığıyla yatay ve dikey senkron sinyalleri üretilir daha sonra da yakalama ve kuvvetlendirme cihazlarıyla senkron sinyallerine göre örneklem ve düzenlemeler yapılarak görüntü tekrar restore edilir.

Geleneksel yöntemden farklı olarak yazılım frekans tabanlı bu modelde ve algoritmalar ile yapılan çalışmada, görüntü sinyali yalnız yazılımlar kullanılarak elde edilmiştir. Bu mimari hem daha az maliyetli hem de daha esnek bir yapıya sahiptir [54]. Şekil 5'te Elektromanyetik kaçaklar sonucu elde edilen metne ait ekran görüntüsü yer almaktadır.

Şekil 5. *Elde edilen metne ait ekran görüntüsü [54].*

5. SONUÇ VE ÖNERİLER

TEMPEST kavramı diğer Bilişim Güvenliği terimlerine nispeten daha az bilinen ancak gerekli önlemler alınmadığı takdirde çok daha büyük boyutlarda zararlara yol açabilecek nitelikte bir güvenlik bileşenidir. Gizli bilgileri işleyen cihazların çalışırken yaydıkları elektromanyetik enerjinin içinde, bu bilgilerin tekrar oluşturulmasına imkan veren kaçaklar bulunabilir. TEMPEST konusunda alınacak önlemler, bu kaçakların kontrol edilmesini ve bu nedenle oluşabilecek güvenlik ihlallerinin asgari seviyelere indirilmesini sağlar. TEMPEST faaliyetlerinin genellikle espiyonaj maksatlı yapılması nedeniyle bu tarz faaliyetlerde elde edilen teknik ve imkanların mümkün olduğunca gizli tutulduğunu unutmamak gerekir. Bu nedenle gizli nitelikli bilgileri işlerken TEMPEST standart ve yönergelerine azami riayet edilmeli ve muhtemel tehditlere karşı müteyakkız olunmalıdır.

Teknolojik yöntemlerle alınan savunma önlemleri etkili fakat maliyetli, yönetsel önlemler ise ucuz fakat uygulaması zor ve can sıkıcıdır. Özellikle gizlilik dereceli bilgilerin yoğun olarak işlendiği kurumlarda TEMPEST farkındalığının yaratılması maksadıyla sürekli ve güncel eğitimler verilmeli ve bu kurumların TEMPEST denetimleri, oluşturulacak denetleme birimleri tarafından düzenli olarak yapılmalıdır. Bina

TEMPEST değerlerine uygun cihazlar seçilmeli, oluşabilecek elektromanyetik kaçaklara karşı filtreleme ve ekranlama teknolojileri ile gerekli tedbirler alınmalıdır. Ayrıca TEMPEST konusunda yaşanan gelişmeler yakından takip edilmeli ve kullanılan sistemlerin güvenlik açıkları bu gelişmeler doğrultusunda revize edilmelidir. Bankacılık sektöründe yaşanan örnekler ve Hollanda'da seçim makinelerine yapılan TEMPEST saldırısı bu konuyla ilgili standartlara olan ihtiyacı bir kez daha ortaya çıkarmıştır. Burada sunulan çalışmada TEMPEST'in ne olduğu, tarihçesi, güncel TEMPEST saldırıları, bilgi içeren kaçakların nasıl ortaya çıktığı üzerinde durulmuştur.

KAYNAKLAR

[1] JMcNamara, ''The Complete, Unofficial TEMPEST Information Page", at http://www.eskimo.com/~joelm/tempest.html.

[2] Major General RFH Nalder, 'History of the Royal Corps of Signals', published by the Royal Signals Institution (1958).

[3] USA National Security Agency (NSA), TEMPEST: A signal problem; Cryptologic Spectrum, 1972.

[4] Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Dergisi Cilt:2 Sayı:3 "TEMPEST, TEMPEST'in Keşfi ve Sinyal Analizi, Değerlendirme Kriterleri ve Ölçüm Sistemleri, Cihaz Tasarımı". Mayıs-Ağustos 2010.

[5] W Ware, 'Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security', Rand Report R609-1, The RAND Corporation, Santa Monica, CA (Feb 1970), available from http://csrc.nist.gov/publications/history/index.html.

[6] P Wright, 'Spycatcher–The Candid Autobiography of a Senior Intelligence Officer',William Heinemann Australia, 1987, ISBN 0-85561-098-0

[7] W Van Eck, ''Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? in Computers and Security v 4 (1985) pp 269–286.

[8] RJ Anderson, MG Kuhn, ''Tamper Resistance–a Cautionary Note", in Proceedings of the Second Usenix Workshop on Electronic Commerce (Nov 96) pp 1–11; http://www.cl.cam.ac.uk/users/rja14/tamper.html.

[9] P Kocher, ‘‘Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems”, in Advances in Cryptology–Crypto 96 Springer LNCS v 1109 pp 104–113, 1996

[10] MG Kuhn, RJ Anderson, ‘‘Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations”, in Proceedings of the Second International Workshop on Information Hiding (Portland, Apr 98), Springer LNCS v 1525 pp 126–143.

[11] P Kocher, ‘‘Differential Power Analysis”, in Advances in Cryptology–Crypto 99 Springer LNCS v 1666 pp 388–397; a brief version was presented at the rump session of Crypto 98.

[12] MG Kuhn, ‘‘Optical Time-Domain Eavesdropping Risks of CRT Displays” in IEEE Symposium on Security and Privacy (2002)

[13] D Asonov, R Agrawal, ‘‘Keyboard Acoustic Emanations”, IBM Almaden Research Center, 2004.

[14] L Zhuang, F Zhou, JD Tygar, ‘‘Keyboard Acoustic Emanations Revisited” in 12th ACM Conference on Computer and Communications Security (2005).

[15] SJ Murdoch, ‘‘Hot or Not: Revealing Hidden Services by their Clock Skew”, in 13th ACM Conference on Computer and Communications Security. 2006

[16] Ross Anderson “Security Engineering: A Guide to Building Dependable Distributed Systems” Second Edition, Chapter 17, Emission Security, Cambridge, January 2008.

[17] USA Air Force, Emissoin Security Countermeasures Reviews; USA Air Force Systems Security Security Memorandum 7011, 1998.

[18] R Gonggrijp, WJ Hengeveld, A Bogk, D Engling, H Mehnert, F Rieger, P Scheffers, B Wels, ‘‘Nedap/Groenendaal ES3B voting computer–a security analysis”, Oct 2006, at http://www.wijvertrouwenstemcomputersniet. nl/Nedap-en

[19] L. Ordu, S. B. Ors, “Yan Kanal Analizi Saldirilarina Genel Bakis”, Ulusal Elektronik Imza Sempozyumu Bildiriler Kitabi, sayfa: 242-249, 07-08 Aralık 2006.

[20] Anderson, R., Kuhn, M., Tamper resistance – a cautionary note, Proceedings of the 2nd USENIX Workshop on Electronic Commerce, 1-11, 1996.

[21] Kommerling, O. ve Kuhn, M.G., Design principles for tamper resistant smartcard processors, Workshop on Smartcard Technology 1999

[22] [22] Boneh, D., DeMillo, R.A., Lipton R.J., On the importance of checking cryptographic protocols for faults, EUROCRYPT'97, vol 1233, 37-51, 1997

[23] Joye M., Lenstra A.K. and Quisquater J.-J, Chinese remaindering based cryptosystem in the presence of faults. Journal of Cryptology, 4(12) , 241-245, 1999.

[24] Örs, S.B., Hardware Design Of Elliptic Curve Cryptosystems And Side-Channel Attacks. PhD thesis, Katholieke Universiteit Leuven, Faculteit Toegepaste Wetenschappen, Departement Elektrotechniek, Kasteelpark Arenberg 10, 3001 Leuven (Heverlee), Belgium, February 2005.

[25] D Brumley, D Boneh, ''Remote timing attacks are practical", in Computer Networks v 48 no 5 (Aug 2005) pp 701–716

[26] Dhem J.F., Design of an effcient public-key cryptographic library for RISC-based smart cards. PhD thesis, UCL Crypto Group, Laboratoire de microelectronique (DICE), May 1998.

[27] Walter C.D., Montgomery exponentiation needs no final subtraction. Electronic letters, 35(21) 1831-1832, October 1999.

[28] Walter C.D., MIST: An efficient, randomized exponentiation algorithm for resisting power analysis. vol 2271 of Lecture Notes in Computer Science, pages 53-66, San Jose, USA, February 2002.

[29] Hachez G. and Quisquater J.-J.. Montgomery exponentiation with no final subtractions: Improved results. In C. K. Koç and C. Paar, editors,Proceedings of 2nd International Workshop on Cryptographic Hardware and Embedded Systems (CHES), vol 1965 pages 293-301, Worcester, Massachusetts, USA, August 17-18 2000.

[30] TS Messergues, EA Dabish, RH Sloan, ''Investigations of Power Analysis Attacks on Smartcards", in Usenix Workshop on Smartcard Technology, pp 151–161

[31] R Meyer-Sommer, ''Smartly analyzing the simplicity and the power of simple power analysis on Smartcards", in Workshop on Cryptographic Hardware and Embedded Systems (2000); Springer

LNCS v 1965 pp 78–92

[32] Kang S.-M., and Leblebici Y., CMOS Digital Integrated Circuits: Analysis and Design. McGraw Hill, 2002.

[33] Kocher, P., Jaffe, J. ve Jun, B., Differential power analysis, CRYPTO'99, vol. 1666, 388-397, 1999.

[34] Ordu L., AES Algoritmasının FPGA Üzerinde Gerçeklenmesi ve Yan-Kanal Analizi Saldırılarına Karşı Güçlendirilmesi. Yüksek Lisans Tezi, İTÜ Fen Bilimleri Enstitüsü, Haziran 2006.

[35] Oswald E., On Side-Channel Attacks and the Application of Algorithmic Countermeasures. PhD Thesis. June 2003.

[36] J Quisquater, D Samyde, ''ElectroMagnetic Analysis EMA):Measures and Counter-Measures for Smart Cards" in nternational Conference on Research in Smart Cards, Springer LNCS v 2140 pp 200–210.

[37] Messerges T.S., Power Analysis Attacks and Countermeasures on Cryptographic Algorithms. PhD thesis, University of Illinois, 2002.

[38] Borst J., Block Ciphers: Design, Analysis and Side-Channel Analysis. PhD thesis, K.U.Leuven, September 2001.

[39] Şadi Evren ŞEKER, DES (Veri Şifreleme Standardı, Data Encryption Standard), http://www.bilgisayarkavramlari.com/2008/03/13/des-veri-sifreleme-standardi-data-encryption-standard/ (25.07.2013 arihinde erişilmiştir.)

[40] Chari, S., Jutla C.S., Rao, J.R. ve Rohatgi, P., Towards sound approaches to counteract power-analysis attacks, CRYPTO'99, v1666, 398-412, 1999

[41] Goubin, L. ve Patari, J., DES and differential power analysis the "duolication" method, CHES-1999, vol. 1717, 158-172. 1999.

[42] Akkar, M.L. ve Giraud, C., An implementation of DES and AES, ecure against some attacks, CHES 2001, Third International Workshop., vol. 2162, 309-318, 2001

[43] Oswald, E., Mangard, S., Pramstaller, N., Rijmen, V., A side-channel analysis resistant description of the AES S-Box, FSE 2005, vol. 3557, 2005

[44] MG Kuhn, ‘‘Electromagnetic Eavesdropping Risks of Flat-Panel Displays”, in PET 2004, at http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf

[45] S Krempl, ‘‘Lauschangriff am Geldautomaten”, in Der Spiegel Jan 8 1999; at http://web.archive.org/web/20001031024042/http://www.spiegel.de/netzwelt/technologie/0,1518,13731,00.html.

[46] ER Koch, J Sperber, ‘Die Datenmafia’, Rohwolt Verlag (1995) ISBN 3-499-60247-4

[47] US Army, ‘Electromagnetic Pulse (EMP) and Tempest Protection for Facilities’, Corps of Engineers Publications Depot, Hyattsville (1990).

[48] Halil Tosunoğlu, Ortak Kriterler ve Bilgi Güvenliği, TÜBİTAK - BİLGEM –UEKAE 24 Haziran 2011, ANKARA https://www.bilgiguvenligi.gov.tr/dokuman-yukle/6.-kamu-kurumlari-bilgi-teknolojileri-guv.-konf./halil-tosunoglu-8haziran bilgiguvenligigunu/download.html, (14.08.2013 tarihinde erişilmiştir.)

[49] D Boneh, RA Demillo, RJ Lipton, ‘‘On the Importance of Checking Cryptographic Protocols for Faults”, in Advances in Cryptology–Eurocrypt 97, Springer LNCS v 1233 pp 37–51.

[50] E Biham, A Shamir, ‘‘Differential Fault Analysis of Secret Key Cryptosystems”, in Advances in Cryptology–Crypto 97 Springer LNCS v 1294 pp 513–525.

[51] J Loughry, DA Umphress, ‘‘Information leakage from optical emanations”, in ACM Transactions on Information and System Security v 5 no 3 (Aug 2002) pp 262–289

[52] DX Song, D Wagner, XQ Tian, ‘‘Timing analysis of keystrokes and SSH timing attacks,” in Proceedings of 10th USENIX Security Symposium (2001).

[53] SP Skorobogatov, ‘‘Optically Enhanced Position-Locked Power Analysis”, in CHES 2006 pp 61–75

[54] Wenhan Yang, Yinghua Lu, Jun Xu, “Video information recovery from EM leakage of computers based storage oscilloscope” Beijing 2010.

[55] Yang X N, Lou C Y, Xu J L. Theory and Application of Software

Radio. Beijing: Publishing House of Electronics Industry, 2001 (in Chinese)

[56] Zhang H X, Lu Y H, He P F, Wang H X. Text recovery from EM leakage of computers. Journal of Southwest Jiaotong University, 2007, 42(6): 653–658 (in Chinese).

[57] Xiang C B, Zhang H Z, Song J Z, Qiao S. Automatic synchronous signal extraction and steady display of non standard video information. Journal of Data Acquisition & Processing, 2007, 22 (4): 486–490 (in Chinese).