

## Kurumsal Yapılarda Bilişim Güvenliği, TEMPEST Problemi

Aykut Sevim<sup>1</sup>, Hamdi Altınır<sup>2</sup>, O. Serkan Ünek<sup>3</sup>, Mehmet Şam<sup>4</sup>

<sup>1</sup>Beykent Üniversitesi Bilg.Müh.Yük.Lisans, İstanbul

<sup>2</sup>Beykent Üniversitesi Bilg.Müh.Yük.Lisans, İstanbul

<sup>3</sup>Beykent Üniversitesi Bilg.Müh.Yük.Lisans, İstanbul

<sup>4</sup>Beykent Üniversitesi Bilg.Müh.Yük.Lisans, İstanbul  
asevim68@hotmail.com; hamdialtiner@hotmail.com;  
serkanunek@hotmail.com; mehmetşam@hotmail.com

**Özet:** Hayatımızın bir vazgeçilmezi haline gelen bilgisayarlar günümüzde bazen farkında olmadan kendimiz bazen de kötü niyetli kişiler tarafından çok etkin bir ateşsiz silah olarak kullanılmaktadır. İfşa edilen bilgilerle dünya çapında kaoslar oluşturulmakta, sağlık, elektrik, haberleşme hizmetleri gibi hayati faaliyetler durdurulmakta, özel hayatın gizliliği ihlal edilerek hızla büyüyen bir ağ gibi tüm insanlık bu tehditlerden etkilenebilir hale gelmektedir.

Bu tehditler artan hız ve karmaşıklıkta devam etmekte olup bilişim hayatımızın içerisinde yer aldığı sürece de devam edecektir. 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. Gizli bilgilerin işlendiği kurumlarda uyulması gereken güvenlik önlemlerinin başında TEMPEST gelir. TEMPEST, kısaca elektromanyetik enerji yayılımları sonucu oluşan bilgi kaçakları olarak tanımlanabilir. Bilgi güvenliğinin değerini artırdığı günümüzde TEMPEST konusunun önemi daha da belirginleşmiştir. Bu maksatla bizler bu çalışmamızda insanlar ve kurumlar üzerinde bir farkındalık yaratmak amacıyla TEMPEST konusunda alınabilecek yönetsel, kişisel ve teknolojik önlemlerin neler olduğu konuları üzerinde duracağız.

**Anahtar Sözcükler:** TEMPEST, Bilişim Güvenliği, Elektromanyetik Girişim, Elektromanyetik Güvenlik, Elektromanyetik Uyum, Elektronik İstihbarat.

## Information Security in Governmental Organizations, TEMPEST Challenge.

**Abstract:**As an inevitable part of our life, computers sometimes unintentionally by ourselves or by malicious people can be used just like a non-firearm. By disclosed information, worldwide chaos can be created, health, electricity, communication services can be interrupted and all humanity becomes vulnerable by violating private life like a growing network.

Compared to private information security, organizational information security is much more complex, important and a tough process. Therefore, it requires high costs and man power.

Information security consists of many main and sub topics. In the organizations, dealing with secret information, TEMPEST comes as one of the top main precautions. TEMPEST, can be defined as information leakages, growing out, as a result of electromagnetic emissions. TEMPEST comes much more important on this days, in which information security increases prominence. For this purpose; to create a situational awareness on people and organizations, we will give point to managerial, personal and technologic precautions on TEMPEST issue

**Keywords:** TEMPEST, Information Security, Electromagnetic Interference, Electromagnetic Compability, Electromagnetic Security, Electronic Intelligence

## 1. Giriş

Bilgi güvenliğinin değerinin son derece arttığı günümüzde TEMPEST konusunun önemi daha da belirginleşmiştir. Amerikan Ulusal Standart ve Teknoloji Enstitüsü tarafından yayınlanan bir makalede haber alma çalışmaları, elektronik (ELINT) ve insana dayalı (HUMINT) olarak ikiye ayrılmıştır. Geçmişte sadece insanlar kullanılarak bilgi toplama çalışmaları yapılırken teknolojinin gelişmesiyle artık elektronik tabanlı bilgi toplama yaygınlaşmıştır. HUMINT ile yetişmiş bir ajan, düşman arasına girerek bilgi ve belge toplar ancak yakalanması durumunda hem kendisi hem de ülkesi risk altına girer. Ancak ELINT çalışmalarında bu riskler en düşük seviyelere inmektedir. ELINT çalışmalarını yürüten kişilerin yalnızca operatör seviyesinde bilgi sahibi olmaları yeterlidir ve izlenen yere uzak bir konumda çalışmalar yapıldığından yakalanma riskleri de düşüktür. ELINT, bilgi toplanacak ortama önceden bir cihaz (böcek vb.) yerleştirilmesi veya ortamdaki cihazların kendiliğinden yaptıkları yayımların kullanılması ile gerçekleştirilebilmektedir. Bu sınıflandırmaya göre TEMPEST, ikinci sınıfa giren cihazların yayımlarını kullanarak yapılan bir ELINT çalışmasıdır [1].

## 2. TEMPEST Nedir?

TEMPEST konusunu açıklayabilmek için ilk önce

Elektromanyetik Girişim (Electromagnetic Interference - EMI) ve Elektromanyetik Uyumluluk (Electromagnetic Compability - EMC)'dan bahsedilmesi gerekir.

Her elektronik cihaz çalışması esnasında ortama elektromanyetik bir enerji yayar ve bu enerji ortamdaki diğer cihazlar üzerinde bozucu etkiler yapabilir. Tıpkı cihazların içerisine gizlice yerleştirilmiş bir radyo vericisinden gönderiliyormuş gibi çevreye yayılan bu kaçak yayınlar kimi zaman 800 metreye kadar ulaşabilir. Ayrıca bu kaçaklar yalnızca havada yayılmaz, rastgele iletken denilen elektrik kabloları, telefon ve işaret hatları veya kalorifer boruları ile 1600 metreye kadar yayılabilirler. Bunun tersi de mümkündür yani kullandığımız cihaz ortamdaki diğer cihazlardan veya ortamda bulunan enerjiden etkilenebilir. Bu etkilenme hadisesine ve etkilenme sonucunda cihaz veya sistemlerin çalışma düzenlerinde meydana gelen bozulma veya kötüleşmeye Elektromanyetik Girişim (EMI) adı verilir. Cihazların diğer cihazlar üzerinde EMI nedeniyle kötüleşmeye yol açmadan ve ortamda bulunması muhtemel enerjiden etkilenmeden çalışmasına devam etmesine ise Elektromanyetik Uyumluluk (EMC) denir. EMI ve EMC konularında sivil ve askeri pek çok standart vardır.

Özellikle gizlilik dereceli bilgilerin işlendiği bir kripto cihazının çevreye kaçak işaretler yayması cihazın

içerisinde işlenen açık bilgilerin dışarıya yayılmasına neden olabileceği için bu durum istenmez. Bu kaçak kaydedilip çözümlendiğinde cihazın işlediği gizli bilgiler elde edilebilir. Bu tehlike yalnız kripto cihazları için değil gizli bilgi işleyen bilgisayar, yazıcı, tarayıcı, faks, telefon ve fotokopi gibi cihazlar için de geçerlidir. Ancak kripto cihazları için dikkat edilmesi gereken konular vardır. Özellikle anahtar yönetimi ile ilgili oluşabilecek kaçaklar Milli Kripto Algoritmalarının deşifre olması gibi çok ciddi güvenlik ihlallerine sebep olacaktır.

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

Bu tanımları detaylandırarak olursak:

- 1) TEMPEST kaçakları istem dışı olarak oluşur; Kripto cihazının içinde işlenmekte olan açık bilgiler cihazın normal çalışma fonksiyonu dışında yaptığı yayınla dışarı kaçabilir.
- 2) TEMPEST kaçakları belli bir frekansta bilgi taşıyan işaretlerdir.
- 3) TEMPEST kaçakları havadan veya kablo üzerinden yayılırlar. Bu işaretlerin değerlendirilebilmesi için anten ile havadan veya bir prob kullanılarak kablodan elde edilmesi gerekmektedir.
- 4) TEMPEST kaçakları ilk ele geçirildiklerinde anlamlı görünmeyebilirler, bu nedenle çözümlenmeleri gerekmektedir.
- 5) Çözümlemeler sonucu elde edilen bilgiler şifrelenen açık bilgileri içermelidir [6].

TEMPEST kelimesinin bir kısaltmayı ifade edip etmediği ediyorsa hangi kelimelerin kısaltması olduğu da 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 [2].

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 seviyesinin 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 [6].

İşaretin iletim hızı arttıkça gerilim seviyesinde hızlı değişimler olur. Gerilim seviyesindeki hızlı değişimlerde yüksek enerji gerektirir. Bu durum daha yüksek seviyeli ışımalara, böylece kaçakların daha uzaklara ulaşmasına neden olur.

### 3. TEMPEST'in Ortaya Çıkışı :

TEMPEST kavramının ilk ortaya çıkışı üzerine süregelen geniş kapsamlı bir tartışma vardır. Genel olarak söylenen birinci dünya savaşında İngiliz ve Almanlar tarafından bulunduğu ve ikinci dünya savaşında da Amerikalılar tarafından geliştirildiği biçimindedir. Ancak 2007 yılında Amerikan NSA tarafından gizliliği kaldırılan makalede, Amerika'da TEMPEST'in ortaya çıkışı ve tarihi hakkında çok net bilgiler verilmektedir. Diğer taraftan birinci dünya savaşında diğer ülkeler tarafından yürütülen TEMPEST çalışmalarının 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, aşağıda açıklandığı biçimiyle, Amerikalılar tarafından 1943 yılında yapıldığı düşünülmektedir [3].

İkinci dünya savaşı boyunca kara ve deniz gizli haberleşme sistemlerinin omurgasını tek kullanımlık şeritler ve basit kriptoloji cihazları oluşturmaktaydı. Bu sistemler kriptoloji işlemini 131-B2 olarak adlandırılan Bell telefon karıştırıcısını kullanarak gerçekleştirmekteydi. 1943 yılında bu karıştırıcılardan biri Bell laboratuvarında test edilirken bir araştırmacı tarafından laboratuvar içerisindeki uzak bir noktada bulunan osiloskopun ekranında salt rastlantısal olarak, her işlem adımında bir darbe işareti olduğu fark edilmiş ve bu darbe işaretleri dikkatlice incelendiğinde, açık bilginin elde edilebildiği anlaşılmıştır. Böylece ilk 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 kriptoloji merkezinin 25 metre uzağındaki bir binaya konuşlandılar. Bir saat süreyle kriptoloji 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.

- 1) Işıma yoluyla oluşacak kaçaklarayönelik ekranlama (shielding)
- 2) Güç ve işaret hatlarındaki kaçaklara yönelik filtreleme (filtering)
- 3) Hem ışımaya hemde iletken hatlara yönelik maskeleyme (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 temizlenmesini sağlandıysa da ışımaya kaçaklarına yine engel olunamadı ve güvenlik bölgeleri koruma alanlarının 60 metreye çıkarılması gibi pek çok ilave tedbir alındı. Ancak bilinmelidir ki o zamanki radyo frekans alıcıların yeteneğine göre seçilen 60 metre kuralı bu gün çok yetersiz kalmaktadır.

### 5. TEMPEST İle İlgili Bazı Terimler:

TEMPEST konusunu anlatabilmek için konuya özgün bazı terimleri tanımlamamız gerekir. Bu terimler;

**Kırmızı;** Kriptolanmamış gizli bilgiyi taşıyan kabloları, optik fiberleri, elemanları, cihazları, sistemleri ve kırmızı cihazların bulunduğu bölgeleri ifade eden bir terimdir. Örneğin başkaları tarafından ele geçirilmesini istemediğimiz bilgilerin bulunduğu bir bilgisayar ağının bütün bileşenleri kırmızıdır.

**Siyah;** Gizli işaretlerin bulunmadığı kabloları, optik fiberleri, elemanları, cihazları ve sistemleri veya gizlilik dereceli bilginin kriptolu olarak taşındığı kabloları, optik fiberleri, elemanları, cihazları ve sistemleri ifade eden bir terimdir. Hiçbir kırmızı sistemin olmadığı bir bölge de siyah bölgedir. Örneğin bir kriptoloji cihazının kriptolanmamış çıkışı siyahtır. İnternete bağlanan herhangi bir bilgisayar da siyahtır ve bu tür bir bilgisayarın içinde gizli bilgi saklanmamalıdır.

**Bilgi içeren kaçaklar;** Ele geçirilip incelendiğinde iletilen, alınan veya saklanan herhangi bir veri ile ilgili bilgi içeren kaçak işaretlerdir.

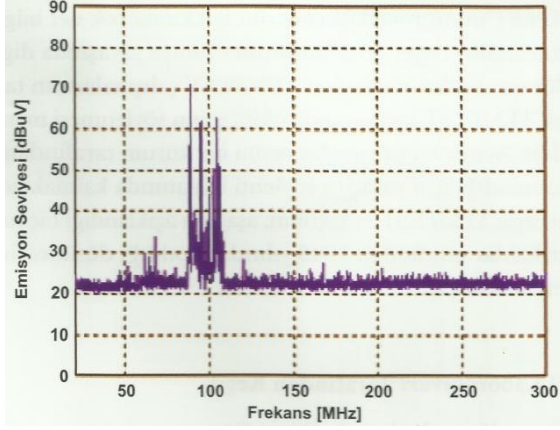
**İletkenden arındırılmış bölge;** Kırmızı cihazın etrafında içinde hiçbir siyah iletken veya cihaz olmaması gereken küresel bir bölgedir. TEMPEST önlemleri açısından bu bölgenin içinde bilgi kaçağı olma olasılığı çok yüksektir ve bu bölgenin büyüklüğü kullanılan cihaza göre değişir [6].

### 5. TEMPEST Ölçümleri ve Kaçak Tipleri:

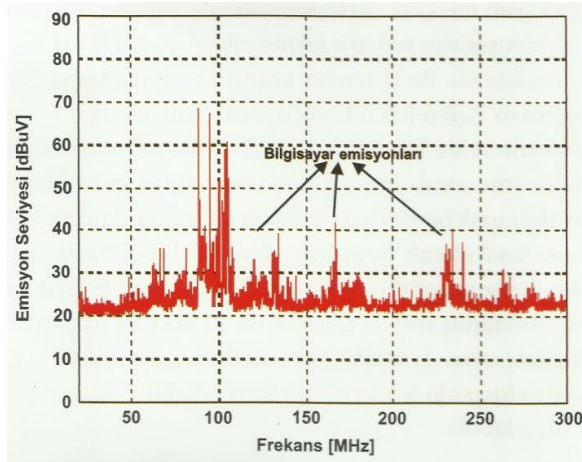
TEMPEST denetlemesi yapılacak cihazların belirli limitlerin altında yayılım seviyelerine sahip

olmaları gerekmektedir. Bu nedenle ilk denetleme frekansa bağlı güç spektrumu elde edilerek yapılır. Cihazların güç spektrumuna katkısını gösterecek bir çalışma

Şekil-1’de verilmektedir.



(a) Bilgisayar Kapalı



(b) Bilgisayar Açık

Şekil 1. Bilgisayar Emisyonlarının Spektrumda Gösterilmesi

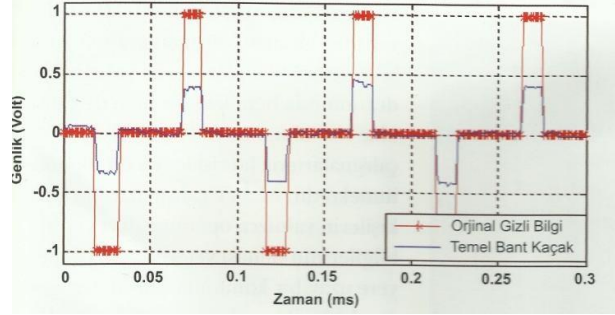
Şekildeki spektrumda sadece 88-108 Mhz. Aralığındaki FM radyo vericileri görülmekte iken kapalı bir bilgisayarın açılması ile farklı frekanslarda da yayılımlar ortaya çıkmıştır. TEMPEST’e göre bu bilgisayar yayılımları TEMPEST limitlerinin altında olmalıdır.

TEMPEST elektronik ve elektromekanik cihazlar için tanımlanır ve bu cihazların tasarım çeşitliliği ile orantılı olarak da çok sayıda bilgi içeren kaçak şekilleri vardır. Bunların en genel olanları; temel bant kaçakları, genlik modülasyonlu (AM) kaçaklar ve darbe kaçaklarıdır [2].

### 5.1. Temel Bant Kaçakları :

Bu çeşit kaçaklarda, işlenen gizli bilgiyi içeren işaret sadece genlik zayıflamasına ve toplamsal gürültü

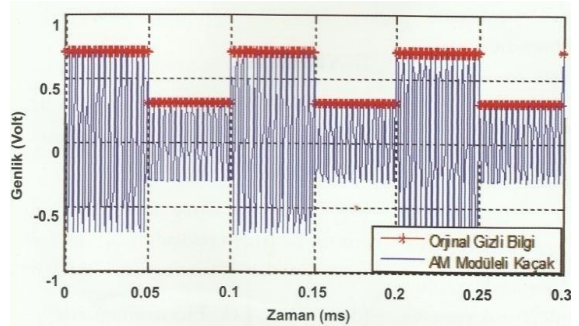
etkisine uğrar. Genel olarak; iletkenlik yolu kaçakları olarak görülür ve gizli bilgiyi işleyen devrelerle ortak bağlantı noktası olan veya ortak bir güç kaynağı kullanan devre hatları üzerinden yayılır. Şekil 2’de HDB3 kodlu sayısal işaretin temel banttaki TEMPEST kaçığı gösterilmektedir. Haberleşme işaretinin genlik değeri +/- 1 Volt iken algılanan kaçak işareti zayıflamış ve üzerine gürültü eklenmiş olarak elde edilmiştir.



Şekil 2. HDB3 kodlu sayısal işaretin temel bant kaçığı

### 5.2. Genlik (AM) Modülasyonlu kaçaklar :

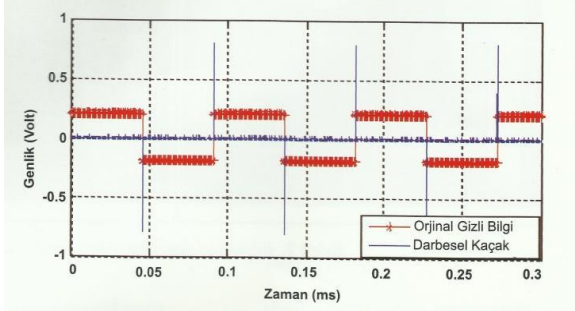
Bu çeşit kaçakta işlenen gizli bilgiyi içeren işaret yüksek frekanslı bir radyo frekans taşıyıcısı modüle ederek yüksek frekanslı bir yayın haline gelir ve uzaklara yayınlanır. Bu tarz bir kaçak Şekil 3’de gösterilmektedir.



Şekil 3. Sayısal verinin AM modülasyon ile oluşturduğu kaçak.

### 5.3. Darbesel Kaçaklar:

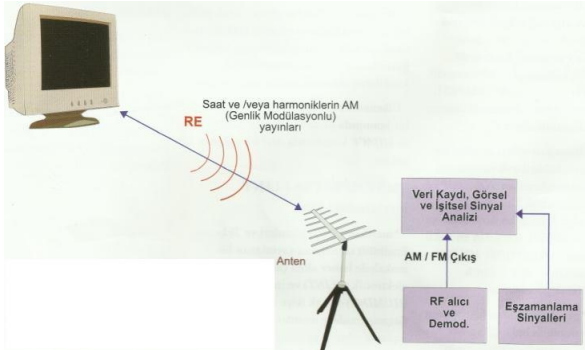
Sayısal işaret işleyen cihazlarda görülebilecek bir kaçak türüdür. Kare dalganın yükselme ve düşme anlarında ortaya çıkmaktadır. Bu çeşit bir kaçak Şekil 4’de gösterilmiştir.



Şekil 4. Sayısal veri darbelerinin oluşturduğu kaçak.

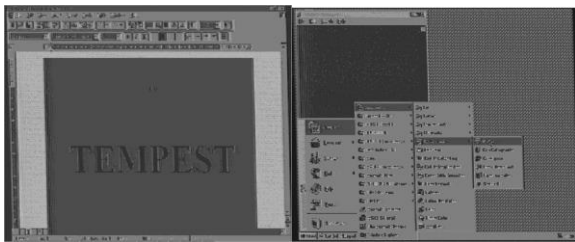
#### 5.4. Bilgisayar Ekran Kaçakları :

TEMPEST kavramının kamuoyu tarafından ilk olarak Duyulması, 1985 yılında Hollandalı araştırmacı Van Eck tarafından gerçekleştirilmiştir [4]. Van Eck bilgisayar ekranlarından yayılan emisyonları işleyerek, orijinal görüntünün elde edilebilirliğini göstermiştir. Kullandığı düzenek Şekil 5'te simgesel olarak verilmiştir.



Şekil 5. Van Eck'in Bilgisayar Ekranı elde etme düzeneği. Daha sonra Kuhn 2003 yılında yayınladığı doktora tezinde,

Bilgisayar ekranlarındaki TEMPEST kaçaklarının yakalanması, çözümlenmesi ve önlenmesi üzerine ayrıntı bir çalışma sunmuştur [5]. Şekil 6'da anten ile alınan bilgisayar ekran kaçaklarıyla ilgili iki örnek gösterilmiştir.



Şekil 6. Bilgisayar ekran kaçağı örnekleri

#### 6. Elektromanyetik Güvenlik (EMSEC) :

EMSEC, TEMPEST'i de içine alan genel bir kavramdır ve gizli bilgi işleyen cihazlardan

elektromanyetik olarak sızan bütün bilgilerin güvenliğini ifade eder. Bu tanımın içerisine NONSTOP ve HIJACK olarak Amerika tarafından isimlendirilen, tanımı ve detayları gizli tutulan iki kavram da eklenmektedir. Dolayısıyla elektromanyetik karşı önlemler denildiğinde TEMPEST, NONSTOP ve HIJACK saldırılarını önleme çalışmaları düşünülmelidir [2].

Amerikan Hava Kuvvetleri tarafından gizliliği kısmen kaldırılarak yayınlanan EMSEC dokümanlarından NONSTOP ve HIJACK kavramlarının bazı detayları anlaşılmaktadır. Aslında bu sınıflandırma ile yapılan, TEMPEST açısından en riskli kaçak yollarının NONSTOP ve HIJACK kapsamına alınarak daha ayrıntılı çalışılması olarak görülebilir.

NONSTOP genel olarak, gizli bilgi işleyen bir cihazın yakınında bulunan radyo frekans verici üzerinden gizli bilginin yayınlanması olarak ifade edilmektedir. Bu kapsamda cep telefonu, telsiz, radar, kablosuz telefon, kablosuz klavye, kablosuz modem, kablosuz alarm sistemi gibi cihazlar gizli bilgi işleyen herhangi bir cihazın yakınına yerleştirilemezler.

HIJACK ise kriptolu cihazlarda işlenen sayısal gizli bilgilerin, kriptolanmış ve dış ortama açık hatlar üzerinden yayınlanmasını ifade eder. Bilgi içeren kaçaklar, NONSTOP'da RF verici üzerinden, HIJACK'de ise kriptolu haberleşme hatları üzerinden uzak noktalara gitmektedir. Bu kaçakları önlemek için aynı dokümanda bazı önlemler tanımlanmıştır. Bunlar genel olarak gizli bilgi işleyen cihazların verici ve kablolarından uzak olarak konumlandırılmasını, kriptolu işaret hatlarının filtrelenmesini ve kabloların ekranlanmasını içermektedir [6].

#### 7. TEMPEST Önlemleri:

TEMPEST önlemlerini belirleyebilmek için, ilk olarak gizlilik dereceli bilginin istenmeyen bölgelere hangi yollarla ulaşabildiğini anlamamız gerekir. Bilgi içeren kaçaklar iki ayrı yolla istenmeyen bölgelere ulaşabilirler.

##### 6.1. Uzaysal Işıma:

Bu durumda yayılımlar havaya yayılan enerji yoluyla iletilirler.

##### 6.2. Elektriksel İletkenlik:

Bu durumda yayılımlar cihazın işaret veya güç kabloları yoluyla ya da cihazın yakınında bulunan herhangi bir metal eleman (kalorifer borusu, su borusu, telefon kabloları vs.) yoluyla iletilir.

Herhangi bir anten kullanarak uzaysal ışımaya veya bir akım sondası kullanarak iletkenlerden elektriksel iletkenlik yoluyla yayılan yayılımların incelenmesi mümkündür.

TEMPEST kaçaklarının engellenebilmesi için alınması gereken çeşitli önlemler vardır. Bunların hepsi temel olarak kırmızı ve siyah sistemlerin kablolarının birbirinden ayrılmasını ve oluşabilecek kaçış yollarının

mümkün olduğunca azaltılmasını içerir. Bu önlemleri aşağıdaki şekilde sıralayabiliriz.

- Kullanılacak cihazları test etmek ve uygun bölgelerde uygun cihazları kullanmak.
- Cihazları doğru yerleştirmek.
- Doğru tipte kablo kullanmak ve kabloları doğru döşemek.
- Gerekğinde uygun güç ve işaret hattı filtreleri kullanmak.
- Doğru topraklama yapmak.
- Binaların olası bilgi kaçaklarına karşı ne derece korumalı olduğunu belirlemek.
- Gizlilik dereceli bilgi işlenen bölgeleri elektromanyetik olarak izole etmek.

Cihazların bağlı olduğu kablolar, çevrelerinde bulunan ve dış ortama bağlantısı olan cihazlar, kalorifer boruları, su boruları gibi metal iletkenlik yolları yaratabilecek elemanlar TEMPEST açısından olası kaçak yolları oluştururlar. İyi bina değeri olan bölgelerde, bu tür iletkenlik yoluyla kaçak oluşması riski daha düşüktür, ancak bazı iletkenlik yolları için bina değeri ne olursa olsun TEMPEST riskleri oldukça yüksektir. Bu nedenle bina ve cihaz değerine bakılmaksızın gizli bilgileri işleyen cihazların tesisatlarında belirli kurallara uyulması gerekir. Bu kurallar daha önce bahsedilen TEMPEST standartlarını belirleyen dokümanlarda yer almaktadır. Gizli bilgileri işlemede kullanılan cihazların ve bu bilgilerin işleneceği bölge veya binaların TEMPEST konusunda oluşabilecek riskleri ortadan kaldıracak şekilde değerlendirilmesinin yapılması gerekmektedir.

## 8. Binaların TEMPEST değerlendirmesi:

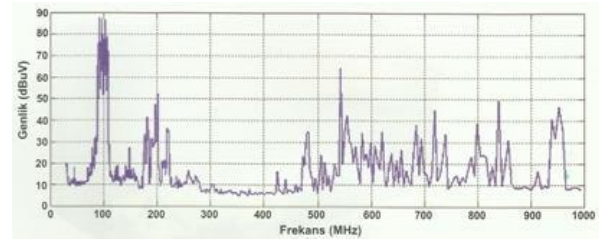
Bina değerlendirmesi gizli bilgilerin işleneceği binaların ve etrafındaki alanın elektromanyetik zayıflatma özelliklerinin yerinde ölçülmesine dayanır. Bu değerlendirme işlemi sonucunda binalara da A, B ve C olmak üzere üç ayrı değer verilir [6].

Bina değeri iyi olan bir bölgede havaya yayılım yoluyla bilgi kaçaklarının oluşma riski de düşük olacaktır. Bu bölgede kullanılacak bilgisayar, yazıcı gibi cihazların TEMPEST değerlerinin çok iyi olması gerekmez. Ancak bulunduğumuz bölgenin bina değeri kötü ise burada kullanacağımız cihazın değeri önem arz eder. Uygun cihazların uygun bölgelerde kullanımı TEMPEST açısından hem az maliyetli bir çözüm olacak hem de kaçak oluşma riskini azaltacaktır.

Bina TEMPEST değerlendirmesi bir bina veya bölge içerisinde kullanılacak cihaz ve sistemlerin doğru konuşlandırılmaları amacıyla bina içindeki ilgili bölgelerin elektromanyetik açıdan zayıflatma karakteristiklerinin yerinde tespit edilerek sınıflandırılmasıdır. Hassas bilginin işlendiği bölgenin binada bulunduğu konum da zayıflatma değerlerine etki eder. Örneğin penceresi olmayan bir oda, zemin

altında bulunan bir bölge veya dış alana uzak mesafede olan bir binanın zayıflatması daha yüksek olacaktır. Aynı şekilde bina ile dış alan arasında ağaçlıklı bir bölge olması veya tamamen açık bir alan olması da sonuçları farklı yönde etkileyecektir. Bina TEMPEST değerlendirmesi binaların olası kaçak işaretlerinin istenmeyen bölgelere ulaşmasına karşı direncini karakterize eder. Genel olarak ölçümlerin alınması, değerlendirilmesi ve bina bölgelendirme haritalarının oluşturulması adımlarından oluşmaktadır. Bina TEMPEST değerlendirmesi ölçmelerinde, ölçüm frekans aralığında çalışan antenler, işaret üreticileri ve alıcılar kullanılması gerekmektedir. Ölçüm işlemi, sırasıyla aşağıda anlatıldığı şekilde gerçekleştirilir.

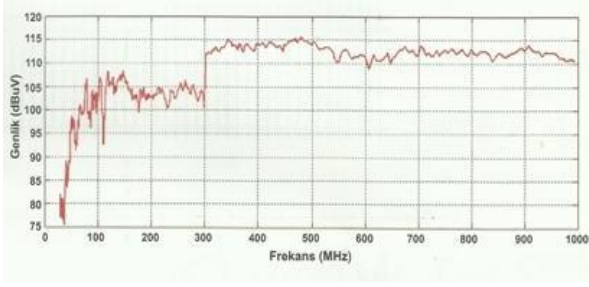
a) Öncelikle ölçüm yapılacak bölgede ilgili frekans bandında çalışan bir anten ve bir alıcı kullanılarak bir ortam ölçümü yapılır. Böylece ortamdaki kaynakların varlığı belirlenir. Şekil 7'de tipik bir ortam ölçüm sonucu örneği görülmektedir. Örneğin bölgede bulunan radyo ve televizyon vericilerinin yayın yaptıkları frekanslarda zaten yüksek seviyelerde işaretler görülecektir.



Şekil 7. Ortam ölçüm sonucu örneği

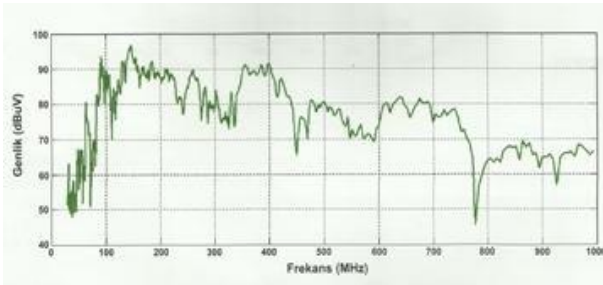
Bu frekanslarda zayıflatma ölçümleri sağlıklı yapılamayacağı için önceden bu tür frekansların belirlenmesi gerekir.

b) Bina TEMPEST değerlendirmesinin ikinci adımında referans ölçümü gerçekleştirilir. Referans ölçümü için alıcı, işaret üretici ve iki set anten gerekmektedir. Referans ölçümünde alıcı ve verici antenler birbirlerine 20 m. mesafede konumlandırılır. Verici antenle belirli bir güç uygulanır ve alıcı antende algılanan değer kaydedilir. Bu işlemin ölçümlerin yapılacağı yerde açıklık bir alanda yapılması gerekir. Referans ölçümlerinin amacı anten, kablo, konektör ve sistemden kaynaklanan zayıflatma ve hataların giderilmesidir. Şekil 8'de Referans ölçüm sonucu örneği yer almaktadır.



Şekil 8. Referans ölçüm sonucu örneği

c) Son adımda bina zayıflatma ölçümleri gerçekleştirilir (Şekil 9). Bu ölçümlerde yine referans ölçümlerindeki cihazlar kullanılır. Bina veya bölge dışında yetkisiz kişilerin yaklaşabilecekleri noktalar belirlenerek alıcı anten bu konumlara yerleştirilir. Verici anten de bina içinde hassas bilginin işlendiği çeşitli noktalarda dolaştırılır ve içeride ve dışarıda seçilen çeşitli konumlarda ölçümler yapılır. Yine verici antenle bir güç uygulanır ve alıcı antenin değeri kaydedilir.



Şekil 9. Bina zayıflatma ölçüm sonucu örneği

Bütün ölçümler ilgili frekans bandında en az 500 farklı frekans noktasında yapılmalıdır. Alıcı ve verici sistemler frekans noktaları arasında eşzamanlı geçiş yapabilmelidir [6]. Bu ölçümlerden elde edilen değerlere göre bina veya platformlar derecelendirilir.

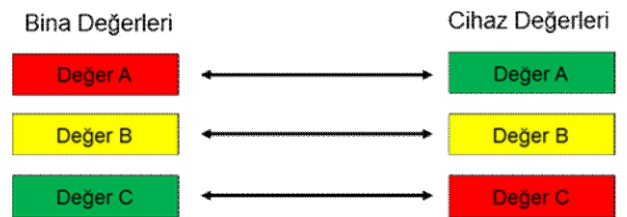
### 9. Cihazların TEMPEST Değerlendirmesi

Başkaları tarafından ele geçirilmesi istenmeyen bilgileri işleyen, ileten veya saklayan bütün cihazlar kırmızı olarak belirlenmelidir. Buna örnek olarak, gizli bilgilerin bulunduğu bir bilgisayar ağındaki bütün cihazlar (bilgisayarlar, ekranlar, yazıcılar, tarayıcılar, ağ cihazları vb.) gösterilebilir. Bu cihazlar çoğu zaman piyasadan satın alınmış herhangi bir TEMPEST önlemi uygulanmamış cihazlardır. Elektromanyetik ışınma özellikleri marka ve modellerine bağlı olarak çok farklılıklar gösterebilir. Bu nedenle bu cihazların gizli bilgilerin işlenmesinde kullanılmadan önce testlerden geçirilmesi gerekir. Cihazların TEMPEST testleri ile ilgili olarak Genelkurmay Başkanlığı tarafından MST 401-1(A) "Türk Silahlı Kuvvetleri TEMPEST Test Standartları" dokümanı yayımlanmıştır. Bu doküman NATO

tarafından yayımlanan SDIP-27 "NATO TEMPEST Requirements and Evaluation Procedures" dokümanının milli eşdeğeridir. Bu dokümanda TEMPEST açısından A, B, C olmak üzere üç ayrı cihaz seviyesi tanımlanmıştır. Gizlilik dereceli bilgi işlenen cihazlar bu standartlara göre test edilir. Ticari Pazar cihazları da MST 401-1(A) standardının Elektrik Işıma test yöntemlerine göre test edilir. "A" en düşük ışımaya karşılık gelen sınır değeri "C" ise en yüksek sınır değeridir. Çıkan sonuçlar MST 401-1(A) standardında verilen sınır değerleri ile karşılaştırılarak Cihaz Değeri belirlenir [6].

Cihaz değerlendirme işlemi gizli bilgiyi işleyecek ticari pazar cihazlarının kullanılabilecekleri bölgelerin belirlenmesi amacıyla kullanılır. Piyasadan alınmış ve üzerinde TEMPEST açısından bir tasarım çalışması yapılmamış herhangi bir cihazın seviyesinin "A" olarak belirlenmesi mümkün değildir. Kripto cihazları ve TEMPEST özellikli olarak tasarlanan cihazlar mutlaka A seviyesinin sınır değerlerine göre test edilmeli ve Elektrik Işıma testleri ile birlikte standartta belirtilen diğer bütün testler de yapılmalıdır.

TEMPEST değerlendirme işlemi gizlilik dereceli bilginin bulunacağı binalar ve gizlilik dereceli bilgiyi işleyecek cihazlar için yapılabilir. TEMPEST değerlendirmesi yapılmış olan bina ve cihazlar standartların öngördüğü kombinasyonlarda eşlenerek tesis edilir (Şekil 10). Bu eşlemede genel kavram, TEMPEST anlamında düşük güvenlikli olarak değerlendirilen binalara bilgi kaçağı düşük, güvenli cihazlar tesis etmek; TEMPEST değerlendirmesi sonucu yüksek kaçak tespit edilen veya değerlendirmesi yapılmamış cihazları ise zayıflatma değeri yüksek, güvenli binalarda kullanmaktır.



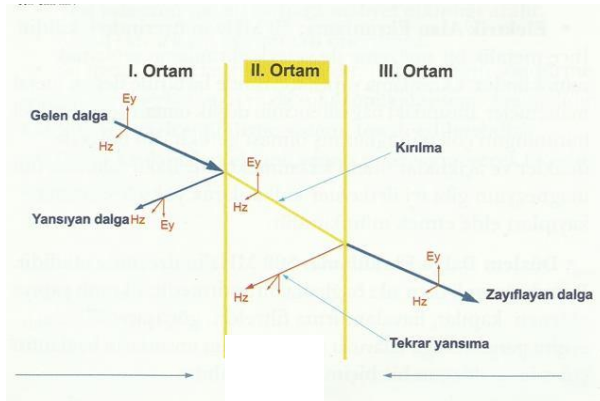
Şekil 10. TEMPEST Bina cihaz eşleştirmesi

Genel olarak bina TEMPEST değeri yeterli olmayan bölgelerde önlem almak veya iyileştirme yapmak maliyeti yüksek, uygulanması zor ve hatta bazen uygulanması mümkün olmayan bir yöntem olduğundan daha az tercih edilir. Bu gibi yerlerde TEMPEST açısından yüksek güvenlikli cihazlar kullanmak gerekir.

Bir cihazın çalışması sırasında uzaysal ışınma veya iletkenlik yoluyla yaydığı bilgi kaçağı, standartlarda verilen sınır değerlere göre değerlendirilir. Belirtilen standartların öngördüğü değerlerdeki (güvenli) cihazlar özel tasarım veya iyileştirme çalışması sonucunda geliştirilen cihazlardır. TEMPEST özellikli

cihazlar özellikle gelişmiş ülkelerde (A.B.D. İngiltere Kanada vb.) üretilmekte ve tasarlanmaktadır. TEMPEST özellikli cihaz tasarımında temel prensip verimli ekranlama, bağlama, topraklama ve filtreleme yapmaktır.

Bilgi teknolojisi cihazlarının çalışırken doğaları gereği çevreye yaydıkları elektromanyetik yayınım bilgi içerebileceği için engellenmelidir. Bu amaçla yapılan ekranlama işlemi cihazın elektronik kartında, kartın devre elemanlarında, cihazı oluşturan alt sistemlerde, iletim kablolarında ve cihazın kendi kasasında uygulanmalıdır. Ekranlamanın temel olarak iki işlevi vardır. Birincisi EM girişimi engellemek, ikincisi ise elektronik dinlemeyi engellemektir. Ekranlama tipi, ekranlı yapı içerisindeki cihazlara/sistemlere ve ekranlamanın işlevine göre değişir. Örneğin yüksek güçlü radar sistemlerine çok yakın bir yerde duyarlı elektronik cihazlar varsa bu cihazları korumak için daha yüksek düzeyli bir ekranlı yapı kurulması gerekirken, elektronik dinlemeyi engellemek için nispeten daha düşük ekranlama düzeyine sahip yapılar kurulabilir. Ekranlama düzeyini belirleyen pek çok değişken vardır. Bunlar ekranlı yapının içinde bulunan cihazların tipi ve aralarındaki uzaklık, işlenen bilginin duyarlılığı vb. gibi unsurlardır. Kaynak ile etkilenen sistem arasında ekran yokken oluşan alan şiddetinin ekran varken oluşan alan şiddetine oranına ekranlama etkinliği denir. Şekil 11'de görüldüğü gibi kalınlığı "t" olan metal bir duvar, EM dalgayı üç yolla zayıflatır. Burada ekran kalınlığı arttıkça metal içindeki yutulma oranı artar. Malzemenin yüksek iletkenlik etkisine sahip olması hem yansıtma hem de yutma kapasitesini artırır.



**Şekil 11.** EM dalga ile ekranlı malzemenin etkileşimi

Ekranlı yapılarda ekranlama etkinliği; metal birleşim yerlerinde, delikler ve aralıkların bulunduğu yerlerde sızıntı nedeniyle azalmaktadır. Ayrıca ekranlı yapının boyutlarıyla bağlantılı olarak belirli frekanslarda ekranlı yapıların rezonatör gibi çalışarak duran dalga etkisi oluşturması nedeniyle de ekranlama etkinliği (EE) azalmaktadır. Bu durum;  $EE = \text{Ekranlama Etkinliği}$

$SE = \text{Sızıntı Eksileri}$

$DDE = \text{Durağan Dalga Etkileri}$

$R = \text{I'inci Ortamdaki Yansıtma Kaybı}$

$A = \text{II'nci Ortamdaki Yansıtma Kaybı}$

$B = \text{III'üncü Ortamdaki Yansıtma Kaybı}$  olmak üzere;

$$EE=R+A+B-SE-DDE \quad (1)$$

Şeklinde formüle edilir [7].

Ekranlama işleminin verimli olabilmesi, düzgün topraklama ve bağlama ile mümkündür. Bağlama sürekli ve düşük empedanslı bir elektriksel yol sağlamak amacıyla iki iletken parçanın mekanik olarak birleştirilmesi anlamına gelir ve mümkün olan en düşük direnci gösterecek şekilde bir iletkenlik bütünlüğünü sağlama açısından önemlidir. Topraklama ise parazitik olarak değerlendirilen veya çalışma prensibi gereği toprak dönüşüne ihtiyaç duyan akımların akması için gereklidir.

Cihaz tasarımında en önemli noktalardan bir diğeri de cihazın çalışacağı çevre koşullarıdır. Bu koşullar göz önünde bulundurularak yapılan tasarımlarda, cihazı oluşturan devre elemanları, cihazın kılıflanması (kutulanması) ve cihazda alınması gereken ilave önlemler hassas seçimler yapmayı gerektirir. TEMPEST özelliği kazandırılmış cihazlarda yapılacak herhangi bir değişimin cihazın TEMPEST profilinde yaratacağı etkiyi öngörmek gerekir.

Filtreler belirlenmiş bir frekans aralığını geçirmek üzere tasarlanmış ve bu bölgenin dışında yüksek zayıflatma özellikleri gösteren, güç ve işaret hatlarında kullanılan cihazları ifade eder. Bu cihazlar kırmızı ve siyah işaretlerin kesiştiği ara yüz cihazlarıdır. TEMPEST filtreler, filtrenin içinden geçen işareti zayıflatmanın yanı sıra giriş işaretinin filtre dışına çıkan işaretine uygulanacak istem dışı bir kuplajı engelleyecek bir tasarıma da sahip olmalıdır. TEMPEST Filtreler kendi başlarına TEMPEST özellikli cihazlar oldukları gibi diğer bazı cihazlara TEMPEST özelliği kazandırılmasında da yardımcı cihaz olarak kullanılırlar [6].

## 10. Sonuç ve Öneriler:

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 konusu, bu kaçakların kontrol edilmesini ve bu nedenle oluşabilecek güvenlik ihlallerinin asgari seviyelere indirilmesini sağlar. Bu nedenle gizli nitelikli bilgileri

işlerken TEMPEST standart ve yönergelerine azami riayet edilmelidir. Özellikle gizlilik dereceli bilgilerin yoğun olarak işlendiği kurumlarda TEMPEST farkındalığının yaratılması maksadıyla 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.

Burada sunulan çalışmada TEMPEST'in ne olduğu, tarihçesi, oluşabilecek kaçakların nasıl ortaya çıktığı, alınabilecek tedbirlerin neler olabileceği ve TEMPEST özellikli bina ve cihazların nitelikleri üzerinde durulmuştur.

## **12. Kaynaklar:**

[1] C. Seline, Eavesdropping on the electronic emanations of digital equipment, *USA National Institute of Standard and Technology (NIST)-Computer Security Division Publications*, 1990.

[2] USA Air Force, Emission Security countermeasures reviews; *USA Air Force Systems Security Security Memorandum 7011*, 1998.

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

[4] W.V. Eck Electromagnetic Radiation from video display units: An eavesdropping risk, *Computer&Security*, p:269-286, 1985.

[5] M.G. Kuhn, Compromising E m a n a t i o n s ; Eavesdropping risks of computer displays, *Phd. Thesis*, 2003.

[6] 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.

[7]L. H. Hemming, *Architectural Electromagnetic Shielding Handbook* IEE Press, 1991