1. TEMPEST NEDİR?

Tempest, Amerika Ulusal Güvenlik Ajansının (NSA) kullandığı bir terim olup, herhangi bir kaynak ile yayınlanan elektrik, mekanik veya ses dalgalarının ele geçirilmesi prensibine dayanan çalışma ve araştırmaların bütününü içermektedir. Tempest bir kısaltma olmamakla birlikte, genellikle "Transmitted Electro-Magnetic Pulse / Energy Standards & Testing" veya "Telecommunications ElectroMagnetic Protection, Equipment, Standards & Techniques" ve daha birçok değişik açılımda çeşitli kaynaklarda geçmektedir.[1]

Elektronik cihazlar çalışırken/kullanılırken birçok elektromanyetik veya akustik dalga yayını yapar. Bunlara kaçak yayın gözüyle bakılabilir. Bu kaçak yayınlar yalnızca havada yayılmaz. Bunun yayılmasına yardım eden elektrik ve telefon hatları, metal kalorifer boruları gibi aracılar ile de taşınabilir. Böylelikle bu kaçaklar uzak mesafelere kadar taşınabilmektedir. Tempest kaçakları elde edildiğinde anlamlı değillerdir ve çözümlenmeleri gerekmektedir. İlgili çözümleme yapılabilirse elde edilen bilgiler anlam kazanır. Tempest bu sebepten dolayı gizli bölgelerde çok dikkat edilmesi gereken bir unsurdur.

2. TARİHÇE

Tempest'in tarihçesi hakkında bilgi 2007 yılında NSA tarafından gizli olarak yayınlanmış bir dokümanın artık zaman aşımına uğramasından dolayı yayınlanması sonucunda elde edilebilmektedir[7]. Bu dokümanda belirtildiği üzere ilk olarak ikinci dünya savaşında rastlantı sonucu keşfedilmiştir. Bell laboratuvarlarının Amerikan ordusu için tasarlamış olduğu bir kripto cihazı aracılığıyla, kripto cihazının kullanımı esnasında oluşturduğu elektromanyetik dalgalar rastlantı eseri bir osiloscop ile tespit edilmiştir. Daha sonra yapılan incelemelerde ise 25 metre uzaktan %75 oranında şifrelenmemiş veri elde edilebilmiştir. Bundan sonra da Amerikan ordusu başta NSA olmak üzere birçok araştırma yapmış ve bu konuda Temptest korumalı cihazlar üretmeye başlamıştır.

3. STANDARTLAR

NATO Dokümanı	Türk Silahlı Kuvvetleri Dokümanı	Açıklama
SDIP-27: NATO Tempest Requirements and Evalutation Procedures"	**MST 401-1(A):** Türk Silahlı Kuvvetleri Tempest Test Procedürü	Tempest Gereksinimleri ve değerlendirme kriterleri belirtilmiştir. Cihaz tempest ölçümleri bu dokümana göre yapılır
SDIP 28: NATO Zoning Procedures	**MY 401-1(A):** Türk Silahlı Kuvvetleri TEMPEST Yönergesi	Genel tempest korumasının nasıl yapılması gerektiğini ve bina güvenlik ölçümleri bu dokümana göre yapılır. Ayrıca gizli bilgi içeren cihazların
SDIP 29: Facility Design Criteria And Installation of Equipment for the Processing		

of Classified Information		nasıl konumlandırılması gerektiğini belirten bir dokümandır.

Genel Kurmay Başkanlığı tarafından başlatılan proje ile Tubitak UEKAE tarafından yukarıda belirtilen NATO'da kullanılan Dokümanların eşleniği olarak Türk Silahlı Kuvvetleri TEMPEST standartları oluşturulmuştur. Bina ve cihazlar A,B ve C olmak üzere 3 ayrı kategoriye ayrılmaktadır. Cihazlarda A en düşük, C ise en yüksek ışıma yapan seviyedir. Yani A tempest açısından en iyi, C ise en kötü cihazdır. Binalarda ise A en az, C ise en fazla zayıflatma yapan binaya karşılık gelmektedir. Yani A tempest'in engellenmesi için en kötü, C ise en iyi zayıflatma yapan binaya karşılık gelmektedir. Aşağıdaki tablo tempest değerlerinin en iyi ve en kötüye göre matriksi vermektedir.

Bina/Cihaz	A	B	C
A			
B			
C			

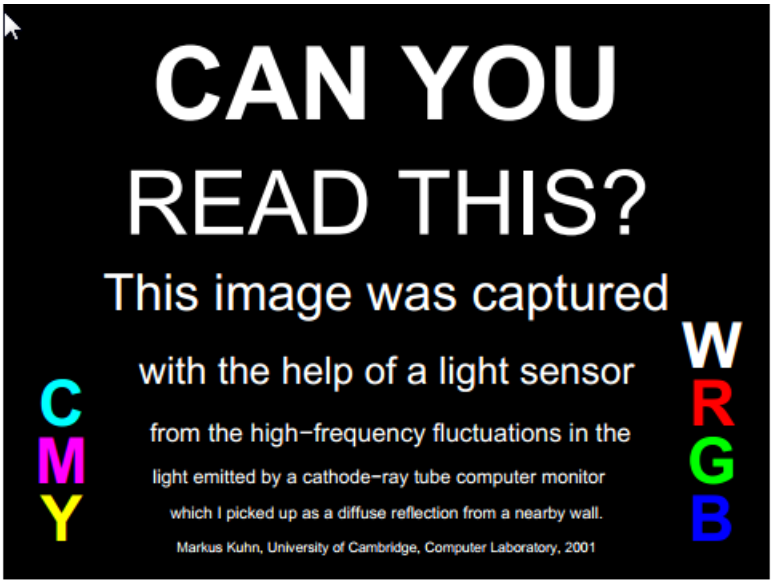
Bu matrikse göre Bina/Cihaz değeri C/A olması tempest açısından en güvenli anlamına, A/C olması ise en güvensiz anlamına gelmektedir. Uygulama gereği Bina değeri A olan bir yerde C seviyesinde ışıma yapan cihaz kullanılmaması tavsiye edilmektedir.

Tempest koruması için Kırmızı ve Siyah bölgelerden bahsedilmektedir. Kırmızı bölgeler gizli bilgi bulunduran ve fakat şifrelenmemiş tüm elemanları (cihaz, kablo, vb) içermektedir. Başkaları tarafından ele geçirilmesi durumunda ciddi sorunlara yol açacak bilgileri bulunduran bir ağın tüm bileşenleri Kırmızı bölge olarak belirlenir. Siyah bölgeler ise gizli bilgi bulundurmayan tüm elemanları veya şifrelenmiş data bulunan tüm bölgeleri adreslemektedir. Örneğin internet bağlantısı için kullandığımız bilgisayarlar Siyah bölgede olmalı ve hiçbir şekilde gizli bilgi bulundurulmamalıdır. Hiçbir kırmızı elamanın olmadığı bölge varsayım olarak siyah bölgedir. Kırmızı olarak belirlenen bir cihaz veya bölgenin küresel alanında siyah cihaz/bölge olmamalıdır. Bu küresel alan ise bölgede kullanılan cihazlara göre değişir. Bazen aynı anda hem kırmızı hem siyah elemanlar aynı cihaz içinde bulunması gerekebilir. Cihazın siyah renk koduna sahip olabilmesi için dışarıya çıkarken kırmızı elemanların filtreden geçirilerek yayınlama etkisi azaltılması gerekmektedir[8].

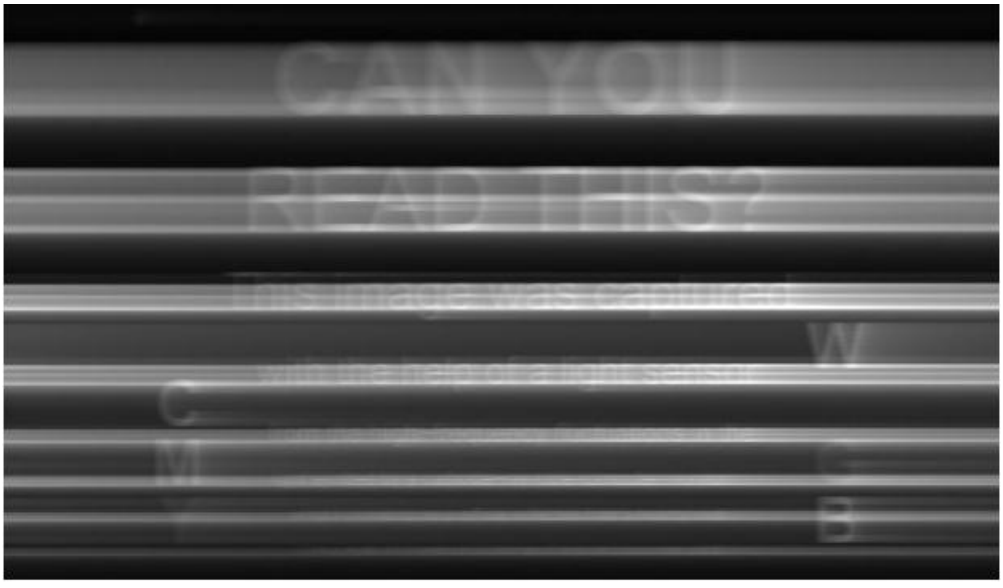
Ölçümleme işi akredite firmalar tarafından yapılmaktadır. Tubitak Bilgem bunlardan biridir. Ayrıca Tempest korumalı PC'de Tubitak tarafından geliştirilmiştir.

4. TEMPEST ATAKLARI

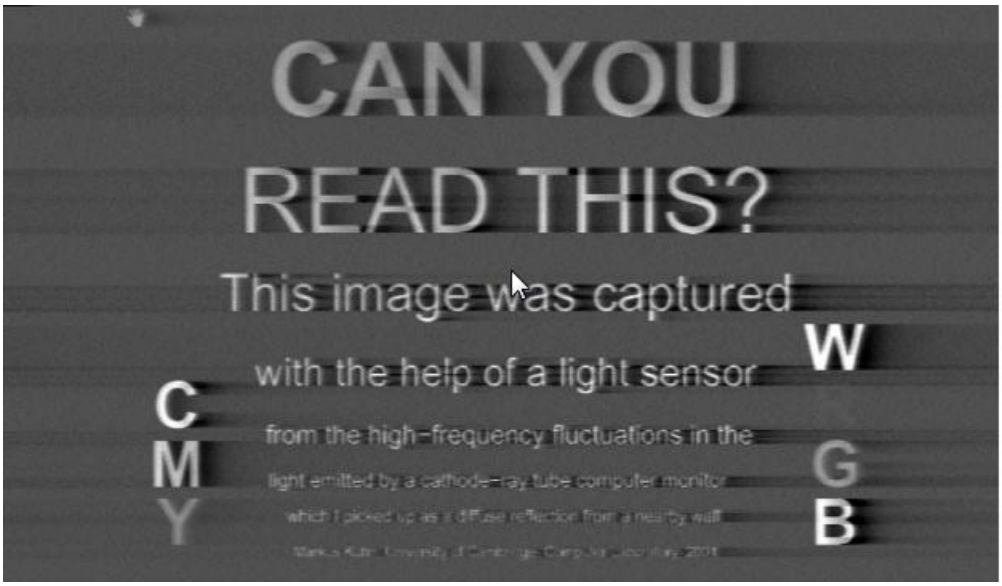
Bu konuyla ilgili ilk akademik çalışma 1985 yılında Wim van Eck adında bir Hollandalı tarafından yapılmıştır. Bu makalede video kartından alınan elektromanyetik sinyaller sayesinde görüntünün başka bir yerde oluşturulmasının başarılabileceği ispatlanmıştır[2]. Bundan sonra yapılan çalışmalar cihazlardan alınabilecek her türlü dalganın bir şekilde analiz edilerek anlamlı veri haline dönüştürebileceğini göstermektedir. Örneğin yapılan bir çalışmada renkli CRT monitörlerden alınan sinyallerin çeşitli filtrelerden geçirilerek çok daha kaliteli görüntü elde edilmesinden bahsedilmektedir[3]. Aşağıda elde edilen görüntüler bulunmaktadır:



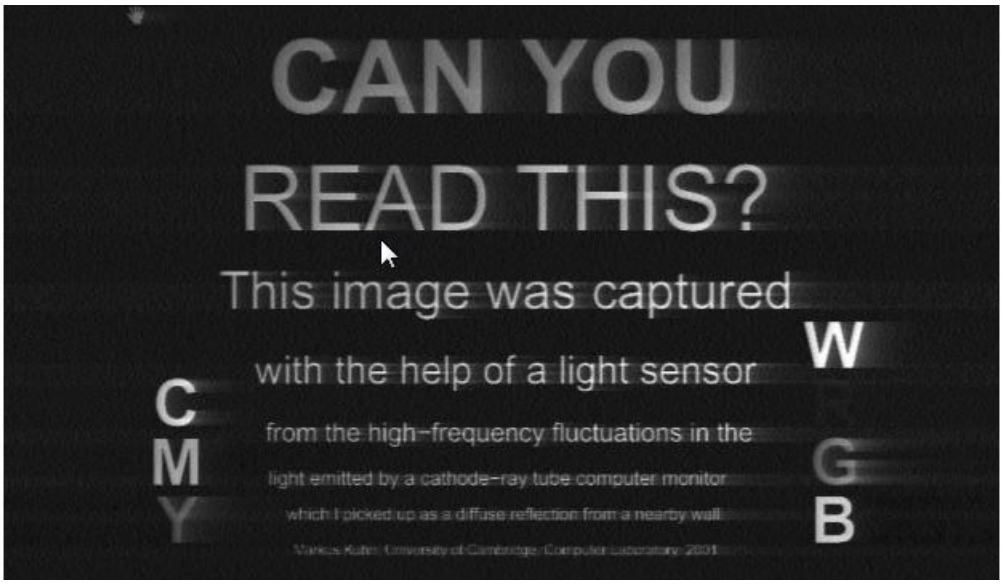
Ekrandaki Orijinal Görüntü



Elde Edilen Görüntü



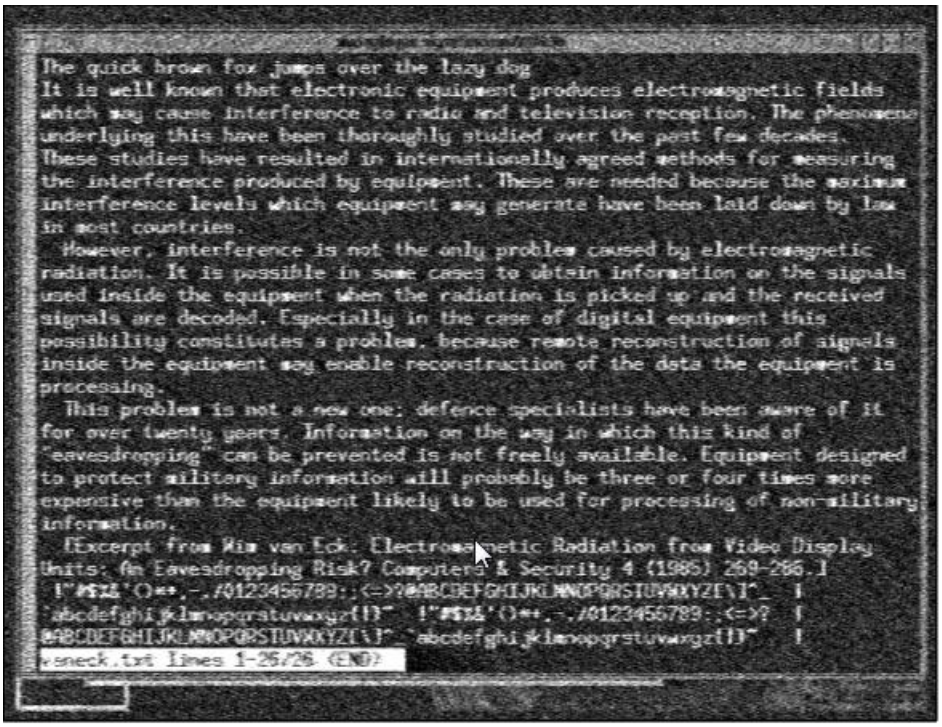
Filtre edilmiş görüntü



Başka bir filtre kullanılarak elde edilen görüntü

Ayrıca sadece CRT monitörlerde değil, flat-panel (LCD,vb) monitörlerde de görüntü elde etmeye dair çalışmalar bulunmaktadır[4]. Aşağıda laptoptan elde edilen görüntüler bulunmaktadır:

3m uzaktaki bir laptoptan alınan Linux açılış ekranı



10 m uzaktaki arada 3 duvar bulunan bir laptoptan alınan görüntü

Görüldüğü gibi yapılan akademik çalışmalar sayesinde hem uzaklık hem de elde edilen bilgilerin kalitesi yükselmektedir. Ayrıca yapılan bir çalışmada klavyeden yazılan yazıların da elde edilebileceği gösterilmektedir[5].

Blackhat konferansında yapılan bir sunumda[6] PS/2 klavye üzerinde yazılan her tuş basımının elektrik hattında oluşturduğu sinyal sayesinde aynı elektrik hattını paylaşan uzak başka bir yerden elde edilebileceği gösterilmiştir. Bu sayede otelde yandaki odadaki yazılanları alabilirsiniz. Ayrıca ATMlerin genellikle PS/2 klavye kullandığı düşünülürse potansiyel atak yeri olarak düşünülebilir. Ek olarak bu sunumda, klavye tuşlarına basarken ekranda oluşan titreşimlerin laser ile alınarak alıcıya yansıtılması sonucunda oluşan sinyallerin analiz edilerek klavyede yazılanların tespit edilebileceği gösterilmektedir.

5. KORUNMA YÖNTEMLERİ

Tempest ataklarından korunmak için aşağıdakiler uygulanmalıdır:

1) Tempest bina ve cihaz ölçümleri akredite kuruluşlara yaptırılmalıdır.
2) Tempest seviyeleri belirlenen cihazların, bina zayıflatma değerlerine gore yerleştirilmesine özen gösterilmelidir.
3) Kırmızı ve Siyah renk kodlamalarına dikkat edilmeli, kırmızı bölgelerin olduğu yerden mümkün olduğunca siyah renk kodlu elemanlar (kablo, cihaz,vb) uzak tutulmalıdır.
4) Elektrik şebekelerine bağlanırken filtreler kullanılmalı, bu sayede kaçak yayınların güç şebekesi üzerinden yayınlanması engellenmiş olacaktır.
5) Kablolamalarda ekranlama (shilding) yapılmış kablolar tercih edilmeli, mümkünse iletişim hatlarında fiber kablolar tercih edilmelidir.
6) Kablolar döşenirken dikkat edilmeli, renk kodları göz önünde bulundurulmalı ve etkileşimde bulunabilecek kablolar yan yana geçirilmemelidir.
7) Görüş mesafesi (line-of-sight) içinde bulunulması durumunda, yukarıda belirtilen atak tipinden etkilenmemek için penceden uzak güvenli bir yerde laptopların konumlandırılması gerekmektedir.
8) Tempest filtrelerinin topraklamaya ihtiyacı olduğu için ve topraklama ne kadar iyi ise o kadar iyi zayıflatma yapacağından, topraklamanın iyi yapılması gerekmektedir.

9) Tempest açısından bakıldığında ses ve elektromanyetik alan geçirmeyen (faraday kafesi) bir oda en güvenli oda olarak kabul edilebilir. Aşağıdaki gibi bir oda yapsanız dahi bu odadan çıkan ağ ve elektrik kabloları verilerinizin ele geçirilmesine sebebiyet verebilir. Bunun için filtreler ve ekranlamalar kullanılması zorunludur.

10) Gizlilik içeren yerlerde Tempest korumalı PCler ve ekipmanlar kullanılabilir. Tubitak'ın üretmiş olduğu SDIP-27 level A değerine sahip Mini Tempest PC kullanılabilir. Tempest korumalı daha bir çok çeşit cihaz bulunmaktadır.

KAYNAKLAR

[1] https://en.wikipedia.org/wiki/Tempest_(codename)

[2] http://ftp.cerias.purdue.edu/pub/doc/equipment/EMRSnooping.pdf

[3] http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf

[4] http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf

[5] http://lasecwww.epfl.ch/keyboard/

[6] http://www.blackhat.com/presentations/bh-usa-09/BARISANI/BHUSA09-Barisani-Keystrokes-SLIDES.pdf

[7] http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf

[8] UEKAE Dergisi 2011 Cilt:2 Sayi:3