BİLİŞİM SUÇLARI KAPSAMINDA DİJİTAL DELİLLER

THE DIGITAL EVIDENCES IN TERMS OF CYBER CRIME

Yusuf UZUNAY
Ankara Emniyet Müdürlüğü
Bilgi İşlem Şube Müdürlüğü
Bilişim Suçları Büro Amirliği, Ankara,Türkiye
yuzunay@ankara.pol.tr

Mustafa KOÇAK
Ankara Emniyet Müdürlüğü
Bilgi İşlem Şube Müdürlüğü
Bilişim Suçları Büro Amirliği, Ankara,Türkiye
mkocak@ankara.pol.tr

Özet. *Günümüzde adını çok sık duymaya başladığımız bilişim suçları, hacmini gittikçe arttırarak geleceğe yönelik büyük tehditler oluşturmaktadır. Bilişim suçlarının tespit edilmesi ve cezalandırılmasında en önemli hususlardan bir tanesi de olay yerinden elde edilen dijital delillerdir. Dijital deliller yapı itibariyle çok hassas olup, kolay bir şekilde değiştirilmeye veya bozulmaya müsait verilerdir. Bu yüzden delillerin tespiti, toplanması, taşınması, analiz edilmesi gibi konularda belirli prosedür ve metotlar izlenmeli ve aynı zamanda dijital delillerin mahkeme esnasında mutlak delil özelliği gösterebilmeleri için toplandığı andan itibaren hiçbir şekilde değiştirilmediğinin, bütünlüğünün bozulmadığının, hangi tarihte kimlerden ve kimler tarafından alındığının mutlak suretle ispat edilmesi gerekmektedir. Bu makalede bilişim suçları kapsamında dijital deliller çeşitli boyutlarıyla ele alınacak olup, mevcut sıkıntılar ve geleceğe yönelik çözüm önerileri değerlendirilecektir.*

Anahtar Kelimeler: *Bilişim Suçları, dijital delil, dijital delillendirme, bilgisayar adli tıbbı*

Abstract. *Cyber crime, the name of which we are more aware of today, leads new future threats by increasing its scale. One of the most important issues in detection and prosecution of a cyber crime is the digital evidences seized from the crime scene. Digital evidences have a fragile structure and are convenient to be easily changed and disrupted. For this reason it must be followed some particular procedures and methods while seizing, transferring, analyzing the evidences. For the digital evidences in order to be able to have certain evidence properties in the course of trial, it must be proved that they haven't been changed since they were seized, by whom and at which date they were seized. In this paper digital evidences in terms of cyber crime will be covered from different aspects and the exiting difficulties and the future proposals will be evaluated.*

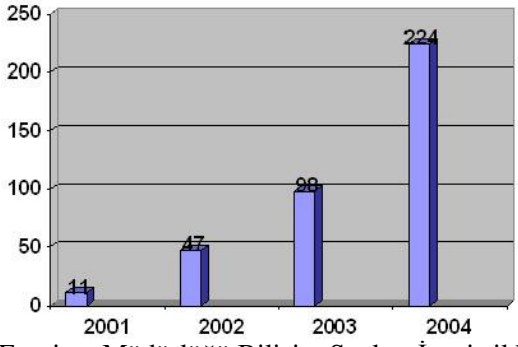
Keywords: *Cyber Crime, Digital Evidence, Digital evidencing, Computer Forensic*

1 GİRİŞ

Bilişim teknolojilerinin akıl almaz bir hızla gelişmesi ve insan hayatına sağladığı kolaylıklar sayesinde, banka ve kredi kartı işlemleri gibi çok hassas işlemler, bilişim teknolojileri kullanılarak gerçekleştirilmeye başlanmış ve bunun sonucunda bilişim güvenliği kavramı da ön plana çıkmıştır. Yıllar geçtikçe bilişim güvenliğini tehdit eden faktörler çoğalmış ve hatta günümüzdeki en önemli suç tiplerinden birini oluşturan bilişim suçlarını doğurmuştur.

Bilişim suçlarının çok geniş bir kapsama alanı bulunmakla birlikte, kesin olarak günümüzde bir sınır çizilememiştir. Dolayısıyla günümüze kadar yapılmış bir çok tanım göze çarpmaktadır. Örneğin Amerikan Adalet Departmanına göre ceza kanununu ihlal eden, işlenmesinde, veya araştırılmasında bilgisayar teknolojisi bilgilerini içeren her suç bilişim suçu olarak tanımlanmaktadır [USDOJ, 2004]. Yine Amerika Birleşik Devletleri Kanunlarında bilgisayarla ilintili suçlar olarak yargılanabilecek bazı illegal eylemler tanımlanmıştır. Örneğin ulusal güvenlik bilgileri, devlet kurumlarının bilgileri, banka ve finans bilgileri, eyaletler arası ve uluslar arası ticaret bilgileri veya korunmuş bilgisayar bilgileri gibi federal kanunlarla korunan bilgilere yönelik suçlar bu alanda değerlendirilmektedir [USC, 2002]. Teksas Ceza Kanunlarında ise "Bilerek bilgisayara, bilgisayar sistemlerine, bilgisayar ağlarına sahibinin izni olmaksızın girmek" şeklinde sadece bilişim suçlarının dar bir boyutunu ele alan bir tanım yapılmıştır [TPC, 2002].

Ankara Emniyet Müdürlüğü tarafından yapılan istatistiklere göre, Türkiye'de bilişim suçlarının sayısı yıllar geçtikçe katlanarak artmaktadır (Bkz: Şekil 1). Günümüzde bilişim suçlarının çoğu, İnternet üzerinden gerçekleştirilmekte ve en sık rastlanan suçlar olarak çocuk pornografisi, kredi kartı dolandırıcılığı, bilgi hırsızlığı, sistemlere izinsiz erişim ve telif haklarının ihlali göze çarpmaktadır.



Şekil 1: Ankara Emniyet Müdürlüğü Bilişim Suçları İstatistikleri [AEM, 2004]

Bilişim suçları ile mücadele kavramı, özellikle Türkiye için oldukça yeni bir kavramdır. Mücadele anlamında gerek hukuki gerekse teknik anlamda bazı sıkıntılar bulunmaktadır. En önemli sıkıntıların kaynaklandığı nokta bilişim suçlarının tespiti ve değerlendirilmesinde hem teknik hem de hukuki bilgilerin entegre bir şekilde kullanılmasıdır. Bu bir nevi sanal bir ortamı fiziksel bir ortam olarak ele almak anlamına gelmektedir.

Suçların tespiti ve yargılanmasındaki en önemli husus delillendirmedir. Delillendirme kısaca, bir suç ile ilgili o suçun kim tarafından ve ne şekilde işlendiğini ispat edici nitelikte bilgiler elde edilmesi ve bunun adli mercilere sunulması şeklinde tanımlanabilir.

Bu makalede özellikle olay yerinden toplanan dijital delillerin bütünlüğünü ve güvenilirliğini ispat konusunda bilişim güvenliği alanında bugüne kadar önerilen teknolojiler gözden geçirilip, bilişim suçları bağlamında mahkeme esnasında gerçekten delil niteliği taşımasını sağlamak adına ne gibi sıkıntılar bulunduğu vurgulanacak olup, yapılabilecek çalışmalara yönelik önerilerde bulunulacaktır.

2 DİJİTAL DELİLLER

Bir bilişim suçu ile ilgili, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen bilgilere kısaca dijital delil ve bunların ilgili birimlere sunulmasına da dijital delillendirme diyebiliriz. Dijital deliller bir çok tipte karşımıza çıkmaktadır. Bunlardan bazıları şu şekildedir:

- Veri dosyaları
- Kurtarılmış silinmiş dosyalar
- Kayıp alanlardan kurtarılmış veriler
- Dijital fotoğraf ve videolar
- Sunucu kayıt dosyaları
- E-posta
- Chat Kayıtları
- İnternet Geçmişi
- Web Sayfaları
- Kayıt Logları
- Abone Kayıtları

Dijital deliller, normal delillere göre yapı itibariyle bazı sıkıntıları barındırmaktadır [Hosmer, 2002]:

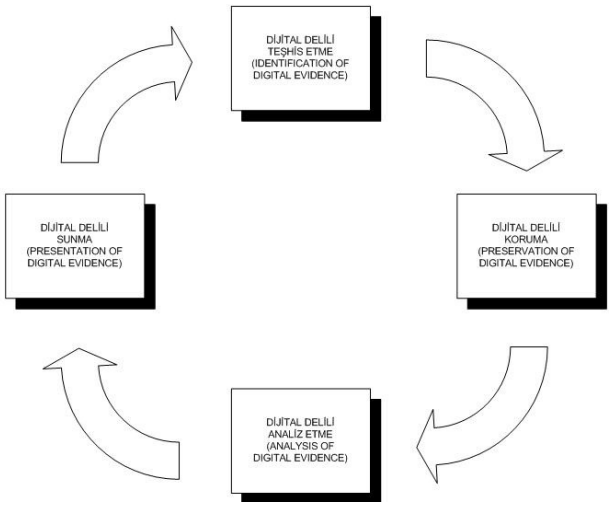
- **Dijital Delillerin Bütünlüğü (The Integrity of Digital Evidence):** Dijital veriler üzerinde çok kolay bir şekilde değiştirme, silme ve yenisini oluşturma gibi işlemlerin yapılabilmesi bu delillerin bütünlüğünü sağlamayı çok zorlaştırmaktadır.
- **Dijital Delillerin Doğrulanması (The Authentication of Digital Evidence):** Bir kişiyi dijital delillerle birlikte yakaladıktan sonra mahkeme sürecinde o verilerin gerçekten o kişiye ait olduğunun ispatı gerekmektedir. Fakat delil olarak ele geçirilen verilerin aynısı her hangi bir kişi tarafından da oluşturulabilir. Hatta sanık bu verilerin daha sonra, polis tarafından bile oluşturulduğunu iddia edebilir.
- **Dijital Delillerin İnkar Edilememesi (The Nonrepudiation of Digital Evidence):** Dijital delillendirme işlemindeki dijital delilin sahibi, onu ele geçiren şahıslar (Ör: Polis), delilin alındığı medya, delilin ele geçirildiği zaman, delilin içeriği gibi bütün unsurların daha sonradan inkar edilememesi gerekmektedir.
- **Dijital Delillerin Doğruluğu (The Accuracy of Digital Evidence):** Dijital delillerin ele geçirilmesi esnasında kullanılan teknikler ve kullanılan bilgilerin (Örneğin delilin ele geçirilme zamanı) doğruluğunun ispatı gerekir.
- **Dijital Delillerin Daha Sonradan Ele Alınabilirliği (The Accountability of Digital Evidence):** Dijital deliller oluşturulduktan sonra, bu delilleri üçüncü bir şahıs inceleyebilmelidir.

Dijital delillerin keşfedildiği alanlardan en çok göze çarpanları ise şunlardır:

- Kuruluş kaynakları
- Geniş Alan Ağları
- Bilgisayarlar (Masaüstü, Laptob, PDA, Sunucu, istemci)
- Elektronik Aygıtlar
- Veri Havuzları
- Bir sistemde yapılan işlemleri gösteren kayıtlar, geçmiş bilgileri, erişim listeleri
- Yedekleme Üniteleri
- Yazılımlar
- E-Postalar
- İnternet ile ilgili dosyalar (Ör: çerezler)

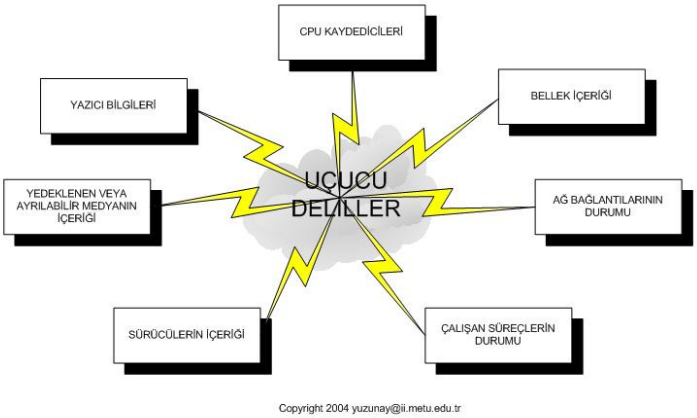
3 DİJİTAL DELİLLENDİRME DÖNGÜ MODELİ

Bilişim suçunun vukuu bulduğu yerden dijital delillerin toplanıp, mahkemeye sunulmasına kadar geçen süreçte belirli basamaklardan söz edilebilir. Aşağıdaki şekilde bu süreçleri içeren bir döngü modeli gösterilmiştir.



Şekil 2 : Dijital Delillendirme Döngü Modeli

Döngü modelinde ele alınabilecek ilk safha, olay yerine gidildiğinde dijital delillerin teşhis edilmesidir. Bu safhada bilişim suçları uzmanları tarafından nerelerde delil olabileceği saptanır. En önemli konulardan birisi, özellikle delil niteliği taşıyabilecek uçucu bilgilerin (volatile data) bozulmadan korunmaya alınmasıdır. Uçucu veriler, bilgisayar sistemleri üzerinde, geçici kayıt bölgelerinde tutulan ve elektrik gücü kesildiğinde içeriği sıfırlanan verilerdir (Bkz: Şekil 3) [Shinder, 2002].



Şekil 3: Uçucu Deliller

Bir bilişim suçu olayının başarılı bir şekilde yargılanması için doğru, kabul edilebilir ve hukukun delil ve delillendirmeye yönelik prosedürlerini izlemek çok büyük önem arz etmektedir. IACIS tarafından dijital delillerin toplanmasına yönelik belirli standartlar belirlenmiştir [IASIS, 2004]:

- Orijinal deliller ilk bulundukları durum ve şartlara benzer şartlarda korunmalıdır.

- Orijinal delillerin bütünlüğünü bozmamak için mümkünse bire bir kopyası alınmalıdır.
- Kopyanın üzerine alınacağı medya "Adli Tıp yönünden steril – Forensically sterile" olmalıdır, yani üzerinde daha önceden herhangi bir data bulunmamalıdır ve virüs ve diğer zararlı kodlara karşı kesinlikle temiz olmalıdır.
- Deliller mutlak suretle etiketlenmeli, korunmalı ve belgelendirilmelidir.
- Adli inceleme esnasındaki bütün basamaklar ve yapılan işlemler yazılı hale getirilmelidir.

Deliller başarılı bir şekilde toplandıktan sonra delilleri koruma aşaması gelmektedir. Bu aşama iki boyutta ele alınabilir.

- Dijital olarak koruma
- Fiziksel olarak koruma

Dijital olarak koruma, delillerin ilk alındığı andan itibaren değişmediğini, bütünlüğünün bozulmadığını ispatlayacak çeşitli mekanizmaları kapsar. En çok kullanılan tekniklerden bir tanesi verilerin kriptografik olarak özetlerinin (Hash) alınmasıdır. Fiziksel olarak koruma ise delillerin incelenecek yere bozulmadan taşınması, mahkeme esnasına kadar uygun ortamlarda saklanması ve yine mahkemeye gidiş esnasında her hangi bir bozukluğa uğramamasını içerir. Deliller mümkün olduğunca toplandığı ortam koşullarına benzer ortamlarda taşınmalı veya saklanmalıdır. Unutulmaması gereken başka bir nokta toplanan bütün delillerin etiketlenerek, uygun şekilde paketlendikten sonra mühürlenmesidir.

Dijital delillerin analiz safhası genellikle bilgisayar adli tıbbı uzmanları tarafından gerçekleştirilir. Elde edilen bütün deliller uygun ortam koşullarında açılıp, bir araya toplandıktan sonra eğer daha önceden yapılmamışsa ilk yapılacak şey, birebir kopyalarının alınıp, orijinallerinin korunmaya alınmasıdır. Genellikle kopyalar dörder adet olmaktadır. Bir tanesi mahkeme için, ikincisi analiz için, üçüncüsü savcı için dördüncüsü de savunma tarafı için çoğaltılır. Yapılacak bütün işlem ve analizler önceden planlanmalı, hangi kişinin hangi deliller üzerinde ne gibi işlemler yaptığı mutlaka belgelendirilmeli ve aynı zamanda uzmanları doğrulayacak sistemler ile oluşturulacak imzalar (Dijital imza) belgelere eklenmelidir. Analiz safhası, en çok teknik bilgi gerektiren ve en uzun sürecek safhadır.

Bütün incelemeler bittikten sonra, son aşama bu delillerin mahkemeye sunulmasıdır. Hazırlanan bütün rapor ve belgeler bir araya toplanıp, delillerin mahkemeye sunumu için uygun formatta dökümanlar oluşturulur. Bütün işlemler titizlikle yapılmalı ve bütün süreçler açık bir şekilde dökümanda ifade edilmelidir. Delillerin bütünlüğü ve doğrulamasını sağlamak için kullanılmış olan bütün sistemler ayrıntılı bir şekilde açıklanmalıdır.

4 BİLİŞİM SUÇLARINA MÜDAHALE

Bilişim suçlarına müdahale oldukça kritik ve çok hassas bir konudur. Çünkü toplanacak deliller dijital delillerdir ve bu deliller yapı itibariyle bozulmaya ve değiştirilmeye müsait verilerdir. Bilişim suçuna müdahale aslında suçun ilk tespit edildiği anda başlar. En kritik nokta da bu aşamadır. Eğer suçu ilk fark eden kişinin bu alanda yeterli bilgisi yoksa, çok önemli bilgi ve delilleri istem dışı yok edebilir. Bu yüzden ilgili kişilere mutlaka konu ile ilgili bilgi ve eğitimler verilmeli, olağan dışı herhangi bir olay fark ettiklerinde bilişim suçları konusunda eğitilmiş bir güvenlik görevlisine ulaşmaları sağlanmalıdır.

Olay yerine gelen güvenlik görevlisinin, eğer saldırı hala devam ediyorsa ilk yapacağı şey saldırıyı herhangi bir dijital delile zarar vermeyecek şekilde kesip(Örneğin ağ üzerinden gelen bir saldırıysa, bilgisayarı kapatmak yerine, ağ kablosunun çekilmesi daha mantıklıdır), bütün her şeyi olduğu gibi dondurup, bilişim suçları araştırma ekibine haber vermektir. Bilişim suçları ekibi gelene kadar olay yerine herhangi bir müdahale gerçekleşmemelidir.

Bilişim suçları araştırma ekibi en az şu kişilerden oluşmalıdır [Shinder, 2002]:

- Üst düzey operasyon yöneticisi : Bilişim suçlarında olay yerine müdahale konusunda uzman, olay yerinin nasıl çevrilip, korunacağını, nerede ve nasıl bir araştırma yöntemi izleyeceklerini planlayan, araştırmadan sorumlu en üst düzey kişidir.
- Polis : Olay yerine giriş, olay yerini koruma, ilgili delillerin ve şüphelilerin alınıp gerekli adli işlemlerin yapılmasını sağlar.
- Müdahaleci : Olay yerine ilk ulaşan personel, güvenlik görevlisi v.b
- Bilişim suçu olay yeri inceleme uzmanları: İlgili delillerin standartlara uygun şekilde bozulmadan toplanıp, aktarılmasını sağlar.

Bilişim suçları araştırma ekibi, olay yerinde gerekli bütün işlemleri yaptıktan sonra, elde edilen delilleri bilgisayar adli tıbbı uzmanlarına (Computer Forensic Specialists) iletir. Bilgisayar Adli Tıbbı, potansiyel delilleri tespit etmek üzere bilgisayar araştırma ve analiz tekniklerinin uygulanması şeklinde tanımlanmaktadır [Robins, 2004].

5 DİJİTAL DELİLLERİN TEKNİK OLARAK DOĞRULANMASI

Verilerin güvenliğinde bahsedilebilecek 3 önemli husus vardır [Kurose and Ross, 2003][Gollmann, 1999]. Bunlar:

- *Verilerin gizliliğinin sağlanması :* İletilen verilerin üçüncü kişiler tarafından öğrenilememesi
- *Verilerin bütünlüğünün sağlanması:* Alıcıya ulaşan verilerin, göndericiden ilk çıktığı hali ile aynı olduğunun ispatı
- *Verilerin inkar edilememesinin sağlanması:* Göndericinin gönderdiği verilerin gerçekte kendisi tarafından gönderilmediğini iddia edememesi

Doğrulama(Authentication), yine dijital güvenlik alanında çok sık bahsedilen kavramlardan biri olmakla birlikte, yukarıdaki maddelerin her biri içinde genellikle yer aldığı için ayrı bir başlıkta ele alınmamıştır. Bahsedilen güvenlik tekniklerinin, dijital delillerin olay yerinden toplandığı andan itibaren mahkeme esnasına kadar bütünlüğünün bozulmadığının ispatı ve inkar edilememesinde oldukça büyük önemi bulunmaktadır. Bugüne kadar bu teknikleri kapsayan bir çok güvenlik metodu geliştirilmiştir. Genel olarak veriler üzerindeki bütünlük sağlama, doğrulama, şifreleme, inkar edememe gibi konular Kriptoloji bilimi altında incelenmiştir. Kriptoloji alıcı ve gönderici arasında iletilen veriler üzerinde belirli matematiksel işlemler gerçekleştirip, güvenlik için çeşitli mekanizmaları sağlar. Şimdi günümüzde kullanılan ve dijital deliller kapsamında da kullanılabilecek metotlardan bazılarına kısaca göz atalım:

Mesaj Doğrulama Kodu (Message Authentication Code-MAC)

Doğrulamada kullanılan tekniklerinden bir tanesi , gizli anahtar kullanarak doğrulama kodu olarak bilinen ve iletilen mesaja eklenen küçük bir data bloğu oluşturmaktır. Burada gönderici gizli anahtarıyla iletilecek mesajı işleme tabi tutar ve bir MAC elde eder. Bu MAC'i mesaja ekleyerek gönderir. Alıcı gelen mesajı kendi gizli anahtarıyla işleme tabi tutar ve elde ettiği MAC'i gönderilen MAC ile karşılaştırarak doğrulama sağlar. Burada simetrik şifre kullanılmıştır ve gizli anahtarın sadece gönderici ve alıcıda olduğu varsayılmıştır.Bu sayede alıcı mesajın değişmediğinden emin olur. Saldırgan doğrulama kodunu değiştirmeden mesajı değiştirirse, alıcı tarafından doğrulama kodu ile yapılan işlem sonucunda mesajın değiştiği çok rahat bir şekilde anlaşılacaktır. Gizli anahtar saldırganda olmadığı için doğrulama kodunu da değiştiremeyecektir. Alıcı mesajı gönderen kişinin gerçekten o kişi olduğuna emin olur. Çünkü gizli anahtarı başka bir kimse bilmediği için, bu tip bir mesajı da hazırlayamayacaktır [Stallings, 2002].

Eğer mesajda bir de sıra numarası (sequence number) varsa (örneğin TCP ve HDLC'de olduğu gibi), bunun değiştirilmesi mümkün olmayacağı için alıcı, ilgili mesajın beklenilen sırada gelip gelmediğini de anlayabilecektir.

Tek Yollu Hash Fonksiyonu :

Mesaj doğrulama kodunun son zamanlarda daha çok önem arz eden bir varyasyonu da Tek Yollu Hash Fonksiyonudur. Mesaj doğrulama kodunda da olduğu gibi bir hash fonksiyonu değişken uzunluklardaki mesajı alıp işleme tabi tuttuktan sonra, sabit uzunlukta bir çıktı üretir. MAC'den farklı olarak Hash fonksiyonu girdi olarak gizli anahtarı kullanmaz. Mesajı doğrulamak için üretilen hash çıktısı, doğrulanmış olarak mesajla birlikte gönderilir.

Tek yollu hash fonsiyonları ve güvenli hash fonksiyonları sadece mesaj doğrulamada değil dijital imzalarda da önemlidir. Güvenli bir hash algoritmasının özellikleri şu şekildedir [Stallings, 2002]:

1. H herhangi boyutta bir veri bloğuna uygulanabilmelidir.
2. H sonuçta sabit uzunlukta bir çıktı üretmelidir.
3. H(x) hem yazılım hem de donanım uygulamalarında pratik olarak verilen her x değeri için kolay hesaplanabilir olmalıdır.
4. H(x)=h eşitliğinde bilinen h kodundan x'i bulmak matematiksel açıdan mümkün olmamalıdır.
5. Verilen her hangi bir x bloğu için, H(x)=H(y) gibi bir sonuçtan birbirinden farklı x ve y değerleri bulmak matematiksel açıdan mümkün olmamalıdır.
6. H(x)=H(y) olan herhangi bir (x,y) çifti bulmak matematiksel açıdan mümkün olmamalıdır.

Dijital İmzalar

Bir A şahsının B şahsına mesaj göndermek istediğini düşünelim. A şahsı B şahsının gerçekten mesajı gönderen kişinin kendisi olduğuna emin olmasını istiyor. Göndereceği mesajın başkaları tarafından görülmesinin de bir önemi yok. Dolayısıyla A şahsı mesajı kendi özel (private) anahtarıyla şifreler ve gönderir. Alıcı konumunda olan B şahsı ise A'nın açık anahtarını kullanarak şifreli mesajı açar. A'nın açık anahtarıyla açılabilen böyle bir mesaj sadece A'nın özel anahtarıyla oluşturulabileceği için ve bu özel anahtar da sadece A şahsında bulunduğu için mesajın A şahsından geldiğine kesin olarak emin olunur. Bu mesajın bu şekilde şifrelenmiş haline dijital imza diyoruz. Mesajın içeriği özel anahtar olmadan değiştirilemeyeceği için bir taraftan da veri bütünlüğü sağlanmış olur. Yalnız bu işlemde A şahsının açık anahtarı herkese açık olduğu için, isteyenler mesajı okuyabilecektir. Yani mesaj gizliliği yoktur.

Genellikle mesajın bütünü şifrelendiğinde çok büyük bir kaynak harcaması meydana gelmektedir. Bu yüzden bütün mesajı şifrelemek yerine, mesajın bir fonksiyonu olan küçük bir data bloğunu şifrelemek daha verimli bir yöntem olacaktır. Böyle bir bloğa tanılayıcı (authenticator) diyoruz. Tanılayıcı mesajın öyle bir fonksiyonu olmalıdır ki, tanılayıcı değişmeden mesajda bir değişiklik yapmak mümkün olmamalıdır. Bu tanılayıcıyı da, bir özel anahtarla şifrelenirse kaynak,içerik ve sıra kontrolü yapan bir dijital imza elde edilmiş olur. SHA-1 (güvenli hash kodu) bu görevi yerine getirebilir.

Şu unutulmamalıdır ki; anlattığımız bu yöntem mesajı, değiştirilmeye (alterations) karşı korur fakat dinlenilmeye (eavesdropping) karşı koruyamaz. Çünkü mesajda okunmaya karşı yapılmış bir kripto söz konusu değildir.

Dijital Sertifikalar

Açık anahtar teknolojisi, adından da anlaşıldığı gibi herkese açık bir alanda işlem yapar. İletişime geçilecek kişinin açık anahtarına herkes ulaşabilir. Zaten açık anahtar teknolojisinin de mantığı budur. Bu yöntem uygun bir yöntem olarak görünse de, önemli bir zayıflığı mevcuttur. Bir şahıs kendisini başka biriymiş gibi gösterip, açık anahtar dağıtabilir. Dolayısıyla o kişiye gizli olarak gönderilen bütün mesajları da okuyabilecektir.

Bu problemin çözümü, açık anahtar sertifikalarında yatmaktadır. Bir dijital sertifika, bir açık anahtar , bu açık anahtarın sahibinin kimliğiyle ilgili bilgiler ve bütün bu bilgilerin güvenilir bir kurum tarafından imzalanmasıyla oluşturulur. Bu kuruma Sertifika Otoritesi (Certificate Authority-CA) denir. Sertifika otoritesi halk tarafından güvenilir bir kuruluş, bir enstitü veya hükümetin bir birimi olabilir. Kullanıcı güvenli bir yolla açık anahtarını otoriteye verir ve bir sertifika temin eder. Daha sonra kullanıcı herkese açık olan alanda sertifikasını yayınlar. Kullanıcının açık anahtarına ihtiyacı olan bir kimse ise bu sertifikayı alır ve eklenmiş olan dijital imzadan bu sertifikanın geçerli bir sertifika olup olmadığını(Yani bu sertifikanın gerçekten sertifika otoritesi tarafından oluşturulup oluşturulmadığını) onaylar [RSA, 1978]. Evrensel olarak kabul edilmiş bir sertifika formatı vardır. Bu formata X.509 standartı denir. X.509 sertifikaları, IPSec, SSL(Secure Sockets Layer), SET (Secure Electronic Transactions) ve S/MIME gibi çoğu ağ güvenliği uygulamalarında kullanılmaktadır.

Bu yöntemler ile ilgili veya kriptoloji konusunda daha detaylı bilgilere [Schneier, 1996]' dan erişilebilir. Aynı zamanda dijital delillendirmede, mevcut çözümlere ek olarak dijital bildiriler [Maurer, 2004] de kullanılabileceği gibi, dijital delillerin yerini ispat etme konusunda da özellikle kablosuz ağ teknolojileri kullanılarak değişik çalışmalar yapılabilir [Sastry, 2003].

6 SONUÇ VE ÖNERİLER

Özellikle elektronik hizmetlerin gün geçtikçe artmasıyla birlikte, bilişim suçlarında da çok büyük artışlar gözlemlenmektedir. Geleceğin en büyük tehditlerinden biri olarak görülen bilişim suçlarıyla mücadele kaçınılmazdır. Özellikle emniyet güçlerinin konuya daha hakim olmaları ve kendilerini bu suçlarla mücadele edebilmek için en iyi şekilde yetiştirmeleri gerekmektedir.

Bir suçun aydınlatılmasındaki en önemli husus, olay yerinden alınan delillerdir. Bilişim suçları bağlamında ise dijital delil kavramı vardır. Dijital deliller, üzerinde çok kolay bir şekilde oynanabildiği için, oldukça hassas bir yapıya sahiptir. Dolayısıyla bilişim suçlarında delillerin standartlara uygun bir şekilde toplanması ve korunması çok büyük önem arz etmektedir. Bu işlemler mutlaka konusunda uzman kişilerce yapılmalıdır.

Dijital deliller konusunda en çok tartışılan noktalardan bir tanesi de, bu delillerin mahkeme esnasında nereden, kimlerden, ne zaman alındığını ve ilk alındığı andan itibaren bütünlüğünün bozulmadığının nasıl ispat edileceğidir. Günümüzde bu tip sorunlara değişik kriptografik çözümler getirilmiştir. Fakat dijital delillerin ispatında bu sistemlerin yalnız başına kullanılması yetmemektedir.

Geleceğe yönelik çalışmalar olarak şunlardan bahsedilebilir:

- Mevcut kriptografik çözümler veya daha değişik yöntemler kullanılarak dijital delillerin mahkeme esnasında geçerliliklerinin sağlanması için entegre çözümler, sistemler üretilebilir.
- Bilişim suçlarının içinde yer alan "Dijital Delillendirme", "Bilgisayar Adli Tıbbı", "Bilişim Suçu Araştırması" gibi konularda Emniyet Güçleri çok iyi bir şekilde eğitilmeli, bilişim suçlarına müdahaleden, analiz ve mahkeme esnasında delillerin sunulmasına kadar geçen süreçlerde görev alacak uzman ekipler oluşturulmalıdır.
- Yüz tanıma sistemleri gibi biyometrik sistemler kullanılarak operasyonlar sonucunda elde edilen dijital delillerle ilgili bir çok veritabanı oluşturulabilir ve operasyonlar bu sayede birbirleriyle ilişkilendirilebilir.
- Yine yüz tanıma sistemleri olay yerindeki kişilerin yüz izlerini veritabanına alıp, verilerin bütünlüğünü sağlamada ek bir parametre olarak kullanılabilir.
- Bilişim suçları, hem adli hem de teknik boyutu içeren bir konu olduğu için mutlak suretle polis ve üniversitelerin işbirliği yapmaları gerekir.
- Türkiye'de bilişim suçlarıyla ilgili oluşan her bir olaya, tek bir belirleyici numara atanıp,CVE, Bugtraq gibi zafiyet veritabanlarının benzeri, merkezi bir bilişim suçları veritabanı oluşturulabilir.

- Teknik çalışmaların yanı sıra vatandaşımızın bu konularda daha çok bilinçlendirilmesi için de çeşitli çalışmalar yapılmalıdır.

REFERANSLAR

[AEM, 2004] Ankara Emniyet Müdürlüğü Bilgi İşlem Şube Müdürlüğü Bilişim Suçları Büro Amirliği Tespitleri, 2004

[USDOJ, 2004] U.S Department of Justice, FBI Law Enforcement Bulletin, August 2004

[USC, 2002] Title 18 of the U.S Code, in Chapter 47, Section 1030, taken in 2002

[TPC, 2002] Texas Penal Codes Section 33.02, taken in 2002

[Hosmer, 2002] Chet Hosmer, "Proving the Integrity of Digital Evidence with Time", International Journal of Digital Evidence, Spring 2002 Volume 1

[IACIS, 2004] International Association of Computer Investigative Specialists, "Guide for Forensic Examinations", Available at: www.cops.org/html/procprint.htm , December 2004

[Shinder, 2002] Debra Littlejohn Shinder, "Scene of Cybercrime – Computer Forensics Handbook", Syngress Publishing, USA, 2002

[Robins, 2004] Judd Robins, "Computer forensic definition", available at: http://rr.sns.org/incident/legal-standarts.php 2004

[Kurose and Ross, 2003] James. F. Kurose, Keith W. Ross, "Computer Networking", 2003 Pearson Education, 2. Edition

[Stallings, 2002] William Stallings, "Network Security Essentials Applications and Standarts" New Jersey, Prentice Hall 2002

[Gollmann, 1999] D. Gollmann, "Computer Security", John Wiley & Sons Ltd., 1999

[RSA, 1978] R.L.Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Commun. ACM, vol.21, no.2, 1978

[Schneier, 1996] B.Schneier, Applied Cryptography, 2nd ed. New York: Wiley, 1996

[Maurer, 2004] Ueli Maurer, "New Approaches to Digital Evidence", Proceedings of the IEEE Vol. 92, No.6 June 2004

[Sastry, 2003] N. Sastry, U. Shankar, D. Wagner, "Secure Verification of Location Claims", WISE'03 San Diego, California, USA September 2003