Elektronik Doküman/Mektup'ların Kanıt Olabilmesi için Gereksinimler

İbrahim SOĞUKPINAR

Özet— ***Günümüzde, bilgi saklama ve iletişim gereksinimimizin çoğu elektronik ortamlar aracılığı ile gerçekleştirilmektedir. Bu nedenle, gerek elektronik ortamda üretilip saklanan, gerekse iletilen bilgi ve mesajlar, kişilere yönelik hakaret ve suçlamalar bulunduracağı gibi, suç unsuru sayılabilecek içeriğe de sahip olabilmektedirler. Dolayısı ile bu dokümanların içeriğine bakarak sahip olan veya ileten kişiler suçlanabilmekte ve haklarında davalar açılabilmektedir. Ancak, elektronik ortamda saklanan ve iletilen bilgiler üzerinde kolaylıkla sahtecilik yapılabileceği için, elektronik dokümanların kanıt olarak kullanılması durumunda çok dikkatli davranılmalıdır. Bu bildiride, elektronik mesaj/dokümanların üzerinde yapılabilecek sahtecilikler açıklanıp, bu tür dokümanların tartışmasız şekilde kanıt olabilmesi için gerekli olan teknik koşullar tartışılmıştır. Böylece, elektronik dokümanların kanıt olarak gösterildiği anlaşmazlıklarda bilirkişi, sanık, davacı ve yargıç konumunda bulunan kişilerin konuyu daha dikkatli değerlendirmeleri ve yapabilecekleri olası hataların azaltılması amaçlanmıştır.***

Anahtar kelimeler: ***e-doküman, e-imza, e-posta, kanıt***

I. GİRİŞ

BİLİŞİM sistemlerinin sağladığı, bilgiyi üretme saklama iletme ve erişme servisleri sayesinde günlük hayatımızı kolaylaştıran birçok işlem bu ortamda gerçekleştirilebilmektedir. Bununla birlikte, elektronik ortamda üretilen, saklanan ve iletilen bilgiler aracılığı ile kişi veya kurumlara hakaret, tehdit, dolandırıcılık, sahtecilik, servis durdurma, iletişimi engelleme, gizli ve özel bilgileri ifşa etme vs. gibi kötü niyetli eylemler kolaylıkla gerçekleştirilebilmektedir. Bu tür eylemleri belirlemek ve önlemek için yine elektronik ortamda koruma önlemleri(Güvenlik duvarları, nüfuz tespit sitemleri, şifreleme, kimlik doğrulama, sayısal imzalama, vs.) alınabilmektedir. Bütün bu önlemlere karşı gerek elektronik ortamın doğası gerekse bilgi iletim ve erişim protokol/servislerinin zayıflıkları nedeniyle sanal ortamdaki suçların önlenmesi mümkün olamamaktadır. Elektronik posta ile gelen ve içeriğinde kurum ve kişiye hakaret bulunduran bir mesaj veya kişisel bilgisayar da bulunan ve suç teşkil edecek bir eylemin planını açıklayan doküman bunlara örnek olarak gösterilebilir.

Doğal olarak güvenlik güçleri ihbar veya şikâyet üzerine bu mesaj ve dokümanlara göre ilgili kişileri zanlı olarak değerlendirip haklarında kanuni takibat yapmakta, haklarında davalar açılabilmektedir[17,18,19].

Ancak bu gibi durumlarda gönderilen e-postanın gerçekten doğru kişiden gönderilip gönderilmediği içeriğinin değişmediğinin veya kişisel bilgisayarda bulunan bir dokümanın kim tarafından hazırlanıp oraya kopyalandığının anlaşılması günümüzdeki anlaşmazlık konuları içerisinde önemli bir yer tutmaktadır. Bu gibi durumlarda çoğunlukla müşteki, gelen e-postaya bakarak karşı taraf hakkında hukuki işlem başlatmakta, bu süreçte ise yargı makamı, Bilirkişi raporuna dayanarak (e-postanın başlık bilgilerinden hareket ederek) mesajı gönderen bilgisayarın IP(Internet Protokol) adresinin tespit edilerek mesaj kaynağının belirlenmesi yolunu seçmekte ve bu bilgiye dayanarak karar verebilmektedir. Bu şekilde verilen karar ise bir üst mahkeme tarafında yanlış bulunarak bozulabilmektedir[17]. Bazı durumlarda ise bilirkişi raporları çelişebilmektedir[19].

Elektronik ortamda saklanan ve iletilen bilgilerin güvenilir olması için, verinin **gizliliği, bütünlüğü ve kullanılabilirliğinin** sağlanması yanında üretici/gönderici'nin kimliğinin doğrulanması, gereklidir. Bu kapsamda elektronik ortamda üretilen, saklanan ve iletilen bilgilerin güvenilir olması için güvenlik özelliklerini sağlayacak şekilde saklanması ve iletilmesi gereklidir. Çünkü elektronik ortamdaki servis ve protokollerin sağladığı kolaylıkları yanında; **sahtecilik, aldatma, mesaj başlığını/içeriğini değiştirme, yeniden oluşturma** gibi yöntemler kullanılarak farklı kaynaktan, farklı içerikli mesaj gönderilerek alıcı ve göndericinin yanıltılması mümkün olabilmektedir[1,2]. Bu nedenle, gerek, elektronik posta servisleri ile gönderilen mesajlar, gerekse, bilgisayarda saklanan dokümanlar, eğer gerekli güvenlik önlemleri alınmadan saklanıp gönderilmişler ise, güvensiz bilgi kaynaklarıdır.

Dolayısı ile bu tür kaynaklara dayanılarak yapılacak suçlamalarda çok dikkatli davranılması ve kanıtın gerçekten suçlanan kişi tarafından üretildiğinin, bilerek ve isteyerek saklandığı ve gönderildiğinin kanıtlanması gerekmektedir. Bilişim sistemlerinin zayıflıkları nedeniylede mesaj kaynağında aldatma, mesaj içeriğinin değiştirilmesi ve bilgi sistemlerine kişini izni olmadan suç unsuru teşkil edebilecek dokümanların yerleştirmesinin mümkün olabilmesi yanında, bunu gerçekleştirenlerin tespiti de zor olmaktadır.

Bir başka konu, kişilerin tedbirsizliğinden kaynaklanan ihlallerdir ki, bilişim sitemi kullanımının yaygınlaştığı günümüzde, her bireyin uzman olması beklenemeyeceği için

Ibrahim Soğukpınar, Gebze Yüksek Teknoloji Enstitüsü, Bilgisayar Mühendisliği Bölümü, Çayırova Fabrikalar Yolu No: 101 Gebze-Kocaeli-Türkiye, Tel: +90 262 605 2201, Fax: +90 262 605 2205; e-mail: ispinar@bilmuh.gyte.edu.tr).

tedbirsizliği nedeniyle bilgisayarında suç unsuru içeren doküman bulunan tarafın suçlanması ise tartışılması gereken bir konudur.

Bu bildiride, elektronik ortamda saklanan ve iletilen doküman/mesajların oluşturulması ve iletilmesi sırasında olabilecek güvenlik ihlalleri açıklanarak, gerekli olan önlemler ile bu önlemler alınmadığı durumda güvenilirlikleri ve özellikle hukuki delil olup olamayacaklarının teknik yönleriyle tartışılması amaçlanmıştır. Önerilen önlemler ile gerek bilirkişi olarak görevlendirilen, gerekse raporlara göre karar veren yargı makamlarının konuyu farklı bir bakış açısı ile daha dikkatli olarak değerlendirmelerinin sağlanması hedeflenmiştir.

II. Elektronik Doküman Servisleri ve Olabilecek Güvenlik İhlalleri

Elektronik dokümanlar ağ üzerinde iletilmeden önce belirli araçlar ile oluşturularak saklanırlar veya iletilirler. Saklanan ve iletilen dokümanların bu süreç içerisinde bütünlüğünün sağlanması ve kime ait olduğunun bilinmesi önemlidir. Çünkü oluşturulduktan sonra içeriğinin ve sahibinin değiştirilmesine karşı, önlem alınmayan dokümanların oluşturulduğu hali ile saklandığının ispatı zordur. Ayrıca dokümanların veya mesajların kim tarafından oluşturulduğu önemli olmakla birlikte, bunun ispatı için önlem alınmamış ise yine kime ait olduğunun anlaşılması önemli bir problemdir.

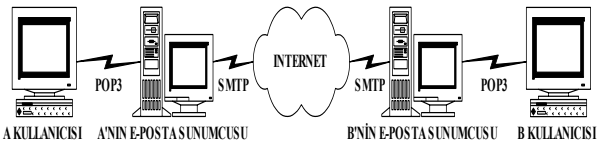
Bilgi ve dokuman iletiminde farklı servisler (Dosya transfer protokolü, mesaj servisleri, e-posta vs.) kullanılmaktadır. Bu bölümde, çok yaygın kullanımı nedeniyle ağırlıklı olarak bilgisayar ağ'ı üzerinde e-posta ile bilgi iletimi ve onun zayıflıkları üzerinde durulmuştur.

A. Internet üzerinde e-posta nasıl iletilir

Bilgisayar ağ'ı üzerinde elektronik postalar iletilirken TCP/IP protokolü ve onun alt protokollerinden SMTP(Simple Mail Transfer Protocol) kullanılır. TCP/IP protokolünü kullanarak iletilen mesajlarda, mesaj paketi gönderici ve alıcının IP adreslerini içerir. Bu adresler kullanıcı bilgisayarlarına sabit veya değişken olarak atanırlar ve bilgisayarları Internet ortamında tanımlamak için kullanılırlar. Normal koşullarda, kullanıcı bilgisayarı iletmek istediği bir mesajın başlık(header) kısmına kendisinin ve mesaj alıcısının IP numaralarını yazması gerekir. Bu işlem mesaj iletimi ve haberleşme için kullanılan yazılımlar ile yapılır.

Şekil 1'de gösterilen Internet üzerinde elektronik posta gönderme/alma işlemi normal koşullarda aşağıdaki gibi yapılır.

- Mesaj göndermek isteyen kullanıcıların kullanacakları E-Posta sunumcular üzerinde hesapları ve bu hesaplar için kullanıcı adı ve şifreleri bulunmalıdır.
- A kullanıcısı, B kullanıcısına bir e-posta göndermek istediği zaman kendisinin sunumcusuna smtp protokolü ile mesajı gönderir. Eğer sunumcu ile aynı ağda bulunmayan bir bilgisayar kullanırsa, göndereceği posta değişik düğümler üzerinden sunumcuya iletilecektir.
- Sunumcu-A, B'nin hesabının bulunduğu sunumcu ile bağlantı kurup postayı Internet üzerinden smtp protokolü ile iletir. Bu aşamada mesaj paketi ağ üzerinde çok çeşitli düğümleri dolaşır.
- B kullanıcısı postalarını okumak için POP3 protokolünü kullanarak hesabının olduğu Sunumcu-B'ye bağlanır ve posta kutusuna gelen postaları okur.



Şekil 1. Internet Üzerinde Elektronik Posta Gönderme İşlemi

B. E-posta iletimindeki zafiyetler

Gerek TCP/IP gerekse smtp protokolünün güvenlik zayıflıkları nedeniyle, normal koşullarda problemsiz olarak iletilebilen mesaj paketleri kötü niyetli internet kullanıcıları(hacker) tarafından değişikliğe uğratılabilir(içerikleri değiştirilebilir) veya farklı göndericiden gelmiş gibi düzenlenebilir. Bu yöntemler ile ilgili bilimsel araştırma sonuçları için kaynak [1,2,3,4, 8]'ye bakılması önerilir.

C. Elektronik mesajlaşma ve bilgi saklamada ne tür ihlaller yapılabilir?

Elektronik ortamda mesaj iletimi ve saklanması yapılırken aşağıdaki güvenlik ihlalleri gerçekleştirilebilir.

- Mesaj paketlerinin gönderici bilgileri farklı yazılabilir. (Bu durumda haberi olmadan bir başkası adına posta gönderilebilir)
- Mesaj içerikleri değiştirilebilir.(Göndericinin mesajı iletim sırasında değiştirilerek farklı içerikte olabilir)
- Bilgisayarlara verilen IP numaralarında sahtecilik yapılarak gönderilen mesajların kendi bilgisayarından gönderildiği gizlenebilir veya başkasının bilgisayarından gönderilmiş gibi gösterilebilir(IP Spoofing). Bir başka ifade ile, Mesaj gruplarından veya dağıtım gruplarından giden mesajlarda mesajın farklı IP numarası ile ve/veya farklı, istenilen adres ve IP numarası ile gitmesi sağlanabilir.
- Bir veya bir kaç bilgisayarın içinden geçilerek özel yol açma programları kullanılarak bu mesaj bilgisayarın sahibinin haberi olmadan o bilgisayardan gönderiliyormuş gibi gönderilebilir.
- Bilgisayarda saklanan doküman izinsiz olarak erişim yapan başkası tarafından değiştirilerek yeniden saklanabilir.
- İzinsiz olarak erişim ile suç teşkil eden dokümanlar kopyalanıp saklanabilir.

Yukarıda açıklanan yanıltma işlemlerini yapabilecek hazır yazılım ve gereçler Internet üzerinden herkes tarafından bulunabilir. Örnek olarak kaynak [9 ve 10]'da belirtilen Mendax, spoofit ,ipspoof, hunt ve address changer programları verilebilir. TCP/IP protokolü ve bilgisayar programlama konusunda biraz bilgisi olanlar bu tür yazılım ve gereçleri

kullanarak yukarıda açıklanan yanıltmaları yapabilirler. Bu nedenle yahoogroups gibi mesaj gruplarından gelen mesajları sağlayan ana servis sağlayıcı (bilişim şirketi) ile hukuki ve bilimsel ölçeklerde bizzat yazışmadan hangi IP numaralarının ne zaman o siteye bağlandığı, gerçek/sahte adreslemi yolladıkları öğrenilemez. Her ne kadar mesaj başlığı içerisinde bulunan IP numaraları gönderici ve alıcının bilgisayarlarının IP numaralarını işaret etse bile bu bilgilerin güvenilirliği düşüktür ve belirleyici kanıt olarak kullanılması yanıltıcı olur. Bir başka ifade ile elektronik posta mesajları ve dokümanlar yalın hali ile "**imzasız şekilde posta ile gönderilmiş mektup"** olarak da değerlendirilebilir.

III. GÜVENLİ DOKÜMAN SAKLAMA VE İLETİM İÇİN NELER YAPILMALIDIR?

Elektronik ortamda saklanan ve iletilen doküman ve mesajların **gizliliğinin sağlanması, kaynağının doğrulanması ve içeriğinin değişmediğinin(bütünlüğünün) doğrulanması** aşağıdaki amaçlar için hayati öneme sahiptir ve gereklidir.

- Eğer doküman/mesaj içeriği, gizli bilgiler taşıyor ise, söz konusu doküman/mesaj ilgisiz kişilerin eline geçmesi durumunda bilginin gizliliğinin önemi kalmayacaktır.
- Gönderilen doküman/mesaj ile alınanın içerikleri farklı olursa yanlış anlaşılmalar nedeniyle doküman/mesaj'ın içerdiği bilgilere dayanılarak hatalı işlemler yapılabilecektir.
- Tarafların doküman/mesaj konusunda itilaflı olduğu durumlarda bilgiyi gönderenin tam olarak saptanamaması durumunda yine hatalı karar verilebilecektir.
- Bilgisayarda bulunan ve suç unsuru teşkil eden bir dokümanın, bilgisayarın sahibi tarafından mı yoksa başkaları tarafından mı üretilip saklandığını ispat etmek çok güçtür. Dolayısı ile bu gibi durumlarda tam olarak doğru karar vermek mümkün olamayabilecektir.

TS ISO/IEC 17799, kurumsal bilgi güvenliği standardında e-posta'ların güvenliği için izlenecek politika aşağıdaki hususları kapsamaktadır[12].

- Elektronik postalara saldırılar. Örneğin, virüsler, çakışmalar,
- Elektronik posta eklerinin korunması,
- Elektronik postanın kullanılmadığı zamanlarda yapılacak işler,
- Şirkete yüklenilmeyen çalışan sorumluluğu. Örneğin, Şirketi lekeleyen elektronik posta gönderimi, tacizkar kullanım, yetkisiz satın almalar,
- Elektronik mesajların bütünlüğü ve gizliliğini korumak için kriptografik tekniklerin kullanımı (Madde 10.3)
- Mahkemeye intikal etmesi durumunda ortaya çıkarılan, saklanan mesajların tutulması.
- Kimden geldiği doğrulanamayan istihbarat mesajları için ilave kontrol tedbirleri.

Mesaj gizliğinin sağlanması için kullanılabilecek yöntem şifrelemedir. Bunun için geliştirilen şifreleme yöntemleri kullanılarak gizlilik sağlanır.

Mesaj kaynağının doğrulanması ve inkar edilememe özellikle elektronik ticaret ve hukuki işlemlerde çok önemlidir. Eğer bir e-posta ile bir başkasına hakaret veya suçlayıcı ifadeler gönderilmiş ise, bu suçu işleyenin tam ve doğru olarak tespit edilmesi, aynı zamanda suçlunun suçunu inkâr edememesinin sağlanması ve hukuki sürecin işletilmesi önemli olmaktadır.

Doküman ve mesajı oluşturan kaynağın tam ve doğru olarak saptanması için sayısal imza ve kaynak doğrulamaya dayanan değişik yöntemler geliştirilmiştir. Bu yöntemler arasında PEM, PGP, S/MIME v2 önde gelen kriptografik mesaj güvenlik protokolleridir. Bunlara ilaveten Eliptik eğri kripto sistem tabanlı güvenli e-posta sistemi de önerilmiştir[13]. E-posta kaynağını doğrulamak amacıyla E-posta liste servisleri, e-posta adreslerinin kriptografik takma adı(alias) ve doğrulama için ilave bilgi (doğrulama merkezi ve buraya verilecek alan anahtarı gibi kaynak doğrulama bilgileri) kullanımı yanında, Internet üzerinde seyreden paketleri, dolaşımları esnasında işaretleyerek geriye doğru izlemek suretiyle kaynağına ulaşmak(Traceback) diğer kaynak doğrulama yöntemleridir [11,14,15,16].

Sayısal imzalama yönteminde, dokümanı veya iletilecek e-postayı oluşturan gönderici, dokümanın öz bilgisini(hash) hesaplayıp ona kendi kimlik bilgisini ve zamanı ekledikten sonra sadece kendisinin bildiği bir anahtar ile bu bilgiyi şifreler ve dokümana ekleyerek saklar veya birlikte gönderir. Alıcı taraf göndericinin diğer anahtarını (açık anahtar) kullanarak imzayı çözer ve mesajın gerçekten gönderen kısmında belirtilen kişi tarafından gönderilip gönderilmediğini anlamış olur. Bu amaç için geliştirilen **PGP(Pretty Good Privacy)** algoritması güvenli e-posta göndermek için kullanıldığı takdirde, e-postayı gönderenin kimliğini saptamak tam ve doğru olarak yapılabilir. Elektronik postaların güvenliği için bu yöntemin kullanımı kaynak [7]'de açıklanmıştır. Gelen mesajların gelirken geçtiği Internet düğümlerinin izlenerek göndericinin IP numarasının saptanması akademik çalışmalar olarak halen devam etmektedir ve henüz pratik kullanımı yoktur. Bu yöntem daha çok servis etkisizleştirme saldırısının(Denial of Service Attacak) kaynağını belirlemek amacıyla kullanılır. Mesaj içeriğinin değiştirilip değiştirilmediğinin anlaşılamadığı bu yöntem ile ilgili bilimsel araştırmalar kaynak [5, 6 ve 11]'de geniş olarak açıklanmıştır

Saklanan dokümanların kimin tarafından oluşturulduğunu anlamak için ise sayısal olarak imzalanması gereklidir. Eğer kendisi kabul etmiyor ise, sayısal olarak imzalanmamış olan bir dokümanı kullanarak kişileri suçlamak tartışılacak bir husustur. Ancak sayısal olarak imzalanmış ise, dokümanın kim tarafından oluşturulduğunun anlaşılması mümkündür.

Eğer oluşturulan doküman/mesaj sayısal imza yöntemi kullanılarak imzalanmış ise, bu dokümanın saklama/iletim

sırasında değişime uğrayıp uğramadığını anlamak tam olarak mümkündür. Böylece içeriğini ve sahibini inkâr edememe tam olarak sağlanmış olur. Açıklanan bu yöntemlerin doğruluğu bilimsel olarak da kanıtlanmıştır. Bu nedenle ancak yukarıda açıklandığı şekilde oluşturulan doküman ve e-posta mesajları güvenilirdir ve içeriğinin değişip değişmediği kolaylıkla kanıtlanabilir.

IV. SONUÇ VE ÖNERİLER

Günümüzde bilişim sistemleri üzerinde doküman/bilgi üretme, saklama ve iletme çok yaygın hale gelmiş bulunmaktadır. Birçok bilgi, bu yol kullanılarak iletilmektedir. Ancak saklanan veya iletilen bilginin varış noktasında, üretenin kimliğinin, doğru kaynaktan geldiğinin, içeriğinin değişmediğinin doğrulanması ve gerekli ise gizliliğinin korunması gereklidir. Eğer bölüm 3'te açıklanan güvenlik önlemleri alınmadan iletilmiş olan bir e-posta mesajı alınmış ise onun içeriğine ve üzerinde yazan gönderici bilgilerine(e-posta adresi ve IP numarası) tam olarak güvenmek ve belirleyici kanıt olarak kullanmak yukarıda açıklanan nedenlerden dolayı yanıltıcı olabilecektir. Bu durumda insanlar neden bu kadar çok olarak e-posta servisini kullanmaktadırlar diye düşünülebilir! Eğer, mesajlaşma yapan her iki taraf birbirine güveniyor, e-postalar ile gizli bilgi iletmiyorlar ve gönderilen bilgilerin içeriğinin iletim esnasında değiştirildiği durumda bir kayıp söz konusu değil ise bu servisin kullanılması son derece kolaydır. Ancak önemli içeriğe sahip olan ve içeriğinin değiştirilmesi halinde tarafların menfaatine zarar getirebilecek içerikteki bilgiler Bölüm 3'te açıklanan yöntemler kullanılmaksızın e-posta servisi ile gönderilmemelidir. Aksi halde anlaşmazlık durumunda, kaynağının ve bütünlüğünün korunduğunun doğrulanması zordur.

Yukarıda açıklanan nedenlerden dolayı;
Eğer bir e-posta mesajı veya elektronik doküman, gönderen/üreten tarafından sayısal olarak imzalanmamış ise imzasız bir mektup'tan farklı bir özelliği olmayacağı için(gerek içeriği ve gönderici bilgileri, gerekse taşıdığı IP numarası açısından) suçlayıcı veya yaptırım amaçlı bir kanıt olarak kullanılması yanıltıcı olabilecektir. Çünkü sayısal imza yöntemi ile imzalanmamış olan bir doküman veya e-posta mesajının kim tarafından üretilip gönderildiğini ve içeriğinin değiştirilip değiştirilmediğini tam olarak anlamak mümkün olamayacağı için bu gibi doküman/e-postaların kanıt olarak kullanılması hatalı sonuçlar doğurabilecektir. Bu nedenle elektronik ortamda oluşturulan dokümanların sayısal olarak imzalanmasının hukukî ve teknik yönleri ile kullanımına ilişkin esasları 5070 sayılı kanunla düzenlenmiştir[20].

Elektronik ortamda üretilen, saklanan ve iletilen dokümanların kanıt olarak kullanılması durumunda bu bilgilerin içeriğinin ve üreticisisin değiştirilmemiş olduğunun kanıtlanması gerekir. Oysa açıklanan nedenlerden dolayı eğer gerekli önlem alınmamış ise bu bilgiler başkaları tarafından kolaylıkla değiştirilebilir. Neticede bu tür bilgilere dayanılarak yapılan suçlamalarda, hatalı karar verilmesini önlemek amacıyla alınabilecek teknik önlemler aşağıda belirtilmiştir.

- Doküman üretme yazılımlarına, üretilen dokümanın üreticisinin kimliğini tartışmasız olarak doğrulayacak mekanizmaların eklenmesinin sağlanması(Örn. Sayısal imza)
- Dokümanların içeriğinin değişip değişmediğinin anlaşılması için yönetim sistemi oluşturulması veya mutlak sayısal olarak imzalanmasının sağlanması. Bilgisayar işletim sisteminin imzasız dokümanları denetleyip ayıklanmasının veya farklı klasörlerde saklamasının sağlanması.
- Internet veya diğer özel ağlarda iletilen tüm mesajların sayısal olarak imzalanmasının sağlanması. İmzasız mesajların kaynağının tanınması için yöntemler geliştirilmesi(örn.kaynağa ulaşma).
- Bu konularda bilirkişilik yapan/yapacakların bilgi güvenliği ve sanal ortam suçları konusunda eğitimli olmasına dikkat edilmesi ve daha duyarlı davranmaları
- Yargı makamlarının bilgi güvenliği ve bilişim suçlarına ilişkin kanıtların özellikleri konusunda bilgilendirilmelerinin sağlanması

Elektronik ortamlarda üretilip iletilen doküman ve mesajlar üzerinde kolaylıkla istenmeyen değiştirme/bozma/yanıltmalar yapılabilmektedir. Dolayısıyla, bu bilgilerin güvenliğinin sağlanması durumunda güvenilir olacaklar hataların azaltılması mümkün olabilecektir.

V. KAYNAKLAR

[1]. Marco de Vivo, Gabriella O. De Vivo, Germinal Iserm, "Internet Security Attacks at the Basic Levels", Operating Systems Review, ACM Press, Vol. 32 No 2, April 1998.

[2]. Cert TR, "Spoofed/Forged Email" http://www.cert.org/tech_tips/email_spoofing.html

[3]. Nelson E.Hastings, Paul A.Mclean," TCP/IP spoofing Fundamentals", Proc. IEEE Fifteenth Annual International Phoenix Conference on Computer and Communications, 1996.

[4]. Marco de Vivo, Gabriella O. De Vivo, Roberto Koeneke ve Germinal Iserm, "Internet Vulnerabilities Related to TCP/IP and T/TCP", *Computer Communication Review*, Vol. 29, No. 1, SIGCOMM, ACM, pp 81-85, January 1999.

[5]. Hassan Aljifri, Marcel Smets ve Alexander Pons, "IP Traceback Using Header Compression", Computers&Security, Vol 22, No 2, pp 136-151, 2003.

[6]. Abraham Yaar, Adrian Perrig, Dawn Song, " FIT: Fast Internet Traceback", Proc. of IEEE INFOCOM, Miami, USA, March 2005.

[7]. Albert Levi ve M.Ufuk Çağlayan, "Elektronik posta Güvenliği için PGP Kullanımı", Açık Sistem '97, Istanbul, sayfa 39 -46, 19 -21 Mart 1997.

[8]. B.Harris, R.Hunt, "TCP/IP Security Threats and Attack Methods", Computer Communications, vol. 22, no. 10, pp. 885-897, 25 June 1999.

[9]. Kapil Sharma, "IP Spoofing", http://www.freelinuxcdrom.com/LDP/LDP/LG/issue63/sharma.html,

[10]. "Anonymous surfing is easy with the IP Address Changer", http://www.iprivacytools.com/

[11]. Hal Burch, Bill Cheswick," TRacing Anonymous Packets to Their Approximate Source", proc. Of 2000 LISA XIV, pp 313-322, Dec 3-8, 2000.

[12]. TSE, TS ISO/IEC 17799 Bilgi Teknolojisi-Bilgi güvenliği Yönetimi için Uygulama Prensibi

[13]. W.Lee, J.Lee, "Design and Implementation of Secure e-mail System Using Elliptic Curve Cryptosystem", Future Generation Computer Systems 20, pp 315,326, 2004.

[14]. P. C. Van Oorschot, "Message authentication by integrity with public corroboration", Proceedings of the NSPW '05, September 2005

[15]. M. Kawashima, T. Abe, S. Minamoto, T. Nakagawa, "Cryptographic alias e-mail addresses for privacy enforcement in business outsourcing", Digital Identity Management 2005, DIM 05, 46-53, 2005

[16]. H. Khurana, A. J. Slagell, R. Bonilla: "SELS: a secure e-mail list service", SAC 2005: pp 306-313.

[17]. K.Varlıakman, Yargıtay 4. Hukuk Dairesi kararı, http://www.hukuki.net/topic.asp?topic_id=9565 ,2005

[18]. Haberx, Ilıcak ve Güzel'den 'andıç' davası..., http://www.haberx.com/n/1011810/ilicak-ve-guzelden-andic-davasi.htm, 2007

[19]. Tarsushaber, Internet yoluyla Hakaret, http://www.hukuki.net/forum/showthread.php?t=810&highlight=e-mail, 2003

[20]. 5070 sayılı Elektronik imza Kanunu, T.C. Resmi gazete sayı:25355, 2004