INTERNET'TE KİŞİSEL BİLGİ GÜVENLİĞİ İÇİN ANONİMLEŞTİRİCİ SERVİSLER ÜZERİNE BİR İNCELEME

Hande Sayar*, Mehmet E. Dalkılıç**

***Biritish American Tobacco, İzmir**
****Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü, 35100 Bornova/İzmir**

***Hande_Sayar@bat.com, **dalkilic@ube.ege.edu.tr**

1. GİRİŞ

Internet günümüzde hayatın vazgeçilmez bir parçası haline gelmiş olmasına rağmen, düşünüldüğü kadar güvenli bir ortam değildir. Internet'i kullanan kişi sayısı ve kullanım alanları genişledikçe, Web üzerinde mahremiyetin korunması da her geçen gün zorlaşmakta, yeni tehditler ortaya çıkmaktadır. "Siz Internet'te gezinirken; eriştiğiniz tüm Web sayfaları, çevrimiçi (online) yaptığınız tüm alışverişler, gönderdiğiniz her e-posta vs. üçüncü şahıslar tarafından izleniyor olabilir" (Golberg et. al., 1996).

Bu makalede; Internet üzerindeki mevcut tehditler ve bu tehditlerden korunma yöntemleri ele alınarak, Internet üzerinde mahremiyet ve güvenliği korumanın en önemli ve etkili yollarından biri olan anonimlik farklı yönleriyle ele alınacaktır.

1.1 Internet Üzerindeki Mevcut Tehditler

IP adresinin görüntülenmesi; IP veya Internet adresi, bilgisayarı tanımlar ve ziyaret edilen tüm Web siteleri tarafından saklanır. Bu bilgi, kullanıcıların kişisel bilgilerinin ve tüm Internet hareketlerinin kapsamlı bir profilinin yaratılması için alınıp satılabilir, kullanıcıların coğrafik yerlerini belirlemek, reklam postaları göndermek veya farklı amaçlar için kullanılabilir.

Tarayıcı (Browser) bilgileri; Web siteleri kullanıcıların işletim sistemi ve tarayıcı bilgilerini öğrenerek kullanıcıya daha iyi bir gezinti olanağı sunabilirler. Buna karşın, bu bilgiler kötü amaçlar için de kullanılabilir. Ör; bilgisayar korsanları ve virüsler işletim sistemi ve tarayıcıdaki zayıflıklara göre saldırılarını düzenleyebilir, kullanıcı bilgilerini çalabilir, bilgisayarı kullanılamaz hale getirebilir ya da sistemin çeşitli suçları gerçekleştirmek için kullanılmasını sağlayabilirler.

Saklı izleme dosyaları (cookie); Internet'te gezinirken reklam şirketleri tarafından bilgisayarlara izleme dosyaları yerleştirilebilir. Bu dosyaların bir kısmı; çevrimiçi alışveriş yapmayı sağlama veya Web sayfalarını kullanıcıya göre şekillendirme gibi yararlar sağlamasına rağmen, kullanıcının mahremiyetini ve kişisel bilgilerini tehdit eden izleme dosyaları da bulunmaktadır. Kullanıcıların Web üzerindeki hareketlerini izleyen ve güncel bilgilerini takip etmek için de kullanılan bu dosyalar, elde ettikleri bilgileri saklayıp ilgili kişilere gönderirler.

***Clipboard'*un okunabilmesi;** Kullanıcıların, bilgisayarlarının *clipboard*'larına kopyaladıkları bir e-posta, isim, telefon numarası, adres ya da kredi kartı numarası ziyaret ettikleri siteler veya Web üzerindeki diğer casuslar tarafından görüntülenip bu yolla çalınabilir.

1.2 Internet'te Anonimliği ve Güvenliği Sağlamak İçin İzlenmesi Gereken Kurallar

Internet, mahremiyetin en az korunduğu iletişim ortamıdır. Bu nedenle Internet sitelerine bilgi girişi yapılırken dikkatli olunmalıdır. Bir Web sitesinin kişisel bilgileri sorması, vermek zorunda olunduğu anlamına gelmez. Cevapların yasal olarak doğruluğu gerekli değilse; yanlış isimler, adresler, yaşlar, meslekler vs. kullanılabilir. Çevrimiçi yarışmalara girilmemelidir çünkü bunlar çoğunlukla reklamcıların kullanıcılar hakkında daha detaylı bilgi toplamak için kullandıkları basit hilelerdir.

Eğer bir Web sitesine e-posta adresi vermek zorunda kalınırsa, ilerde mesaj almaya devam etmek istememe veya e-posta adresinin ilgili şirketlere satılması olasılığına karşı, Hotmail veya Yahoo gibi geçici e-posta adresleri kullanılmalıdır. Bilinmeyen, şüpheli kaynaklardan gelen e-postalardaki Web linkleri takip edilmemelidir. Bu durum, özellikle Web sitesinin özel ya da finansal bilgiler istemesi durumunda daha da önem kazanmaktadır. Suçlular, güvenli bir Web sitesi görünümü vermek için sahte bir URL kullanabilirler.

Bilgisayarlar düzenli olarak casus yazılımlara karşı taranmalıdır. Casus yazılımlar; oyunlar, yararlı araçlar ve bedava indirilen programların çoğu ile bilgisayarlara yüklenen programlardır. Ana fonksiyonları, kişisel bilgileri ele geçirip, reklam şirketlerine ulaştırmaktır. Bu bilgiler daha sonra, çeşitli ürünler sunmak veya diğer reklam şirketlerine satmak için kullanılabilir. Casus yazılımlar klasik *Trojan* tanımına uymaktadır ve bir ürünü bilgisayara indirmeyi kabul ederken kullanıcının bilgisi dışında gerçekleşen bir olaydır. Casus yazılımlar, aynı zamanda Internet bağlantısını da yavaşlatabilirler. Casus yazılımlardan korunmak her geçen gün daha da zorlaşmaktadır çünkü bedava yazılım dağıtan şirketler tarafından kar sağlama aracı olarak seçilmeye başlanmıştır. Bu tür yazılımların iletişimlerini görüntülemek için bir güvenlik duvarı kullanılabilir. Ancak en iyi yöntem bir casus yazılım temizleme programı yüklemek ve bunu bir

virüs tarayıcı gibi kullanmaktır. (Ör; www.lavasoftusa.com/, http://grc.com/optout.htm) (Theraider, 2003)

IRC, ICQ, AIM vb., bağlantılarda, nerede yaşandığı, çalışıldığı vs. ile ilgili kişisel bilgiler verilmemelidir. Mesajların direkt olarak gönderilmesi yerine, ICQ sunucu ile gönderilip alınması tercih edilmelidir. Her direkt bağlantı, saldırganların IP adresini öğrenmesini sağlar. Mesajlar, uygun bir yazılım ya da şifreleme araçları ile şifrelenmelidir. (Theraider, 2003). Internet'te gezinmek için anonimleştirilmiş aracı (proxy) kullanılmalıdır. Bu, IP adresinin Web sunucusu kayıtlarında (log) saklanamamasını garantiler. Internet üzerinde anonim gezintiyi sağlayan bazı anonim aracı servisleri şunlardır; Aixs (http://aixs.net/), Rewebber (http://www.anon.de/), Anonymizer (http://www.anonymizer.com/), The Cloak (http://www.the-cloak.com/) (Theraider, 2003). Eğer aracı kullanmamaya karar verilirse, en azından tarayıcıdan kişisel bilgilerin çıkarılması unutulmamalıdır. Bu kişisel bilgiler çıkarıldığında, bir Web sitesinin elde edebileceği tek bilgi ISP (Internet Servis Sağlayıcı) adresi ve coğrafik yer olur.

Sistem yöneticilerine ve diğer kullanıcılara güvenilmediği durumlarda, IRC(Internet Relay Chat) ağlarına bağlanmak için bir yansıtıcı (bouncer) kullanılmalıdır. Yansıtıcı, IRC'ye bağlanırken kimliği saklamak için kullanılan bir programdır. Yansıtıcı kurulu olduğunda, bir kabuk (shell) fonksiyonu, kullanıcı ile IRC sunucusu arasında bağlantı sağlar. Dolayısıyla asıl talebi yapan kişinin kimliği belirlenemez. Bir IRC yansıtıcı kullanabilmek için yansıtıcı yazılımı indirip, kurmak gereklidir (ör;http://gotbnc.com/) (Theraider, 2003).

Web üzerinden gönderilen verileri korumanın en güvenli yollarından biri de onları şifrelemektir. PGP (Pretty Good Privacy) gibi programlar şifreleme ve şifre çözme için kullanılan araçlardır. PGP, bir mesaj dosyasının değiştirilmediğine, okunmadığına, düşündüğünüz kişiden geldiğine emin olmak için kullanılan bir yazılımdır.

Web sunucusundan tarayıcıya gönderilen herşey genellikle düz metin (plaintext) formatındadır. Bunun anlamı, tüm transfer edilen bilgilerin kolaylıkla incelenebilir olmasıdır. Gizli, önemli bilgileri (kredi kartı numaraları, şifreler vs) göndermek ve almak için SSL'i (Secure Socket Layer) olan bir Web sunucusu kullanılmalıdır.

Bu kurallara uyulduğu sürece Internet'te güvenli gezintiler yapmak mümkün olacaktır.

2. ANONİMLİK

Internet üzerinde mahremiyet ve güvenliği korumanın en önemli ve etkili yollarından biri anonimleştirmedir. Anonimlik; tüm Web servislerini, kimsenin verileri izlemesine olanak vermeyecek şekilde kullanabilmeyi sağlar. Internet üzerinde, anonimliğin sağlanmasının ilk hedefi;

Internet servislerini kullanırken, IP'nin diğer kullanıcılar veya sunucuların sistem yöneticileri tarafından görülemez olmasının garantilenmesidir (Theraider, 2003).

Anonimlik, ağ güvenliğinin bir parçasıdır. Sistem içerisindeki bir varlığın anonimlik özelliğinin olabilmesi için; başka hiçbir varlığın kendisini tanımlayamıyor olması, kendisine geri ulaşılabilecek hiçbir bağlantının bulunmaması ya da iki anonim hareketin aynı varlık tarafından gerçekleştirildiğine dair bir kanıtın bulunmaması gerekir (Malkhi, 2002).

Internet üzerinde anonim iletişimi sağlamak için birçok farklı protokol uygulanmaktadır; ör; *Crowds, Onion Routing, Hordes, APFS, Chaum Mixes, DC-Net* vb. (Wright et. al., 2002). Anonimliği sağlayan ürünler de bu protokollerin uygulamalarıdır.

Anonimlik iki gruba ayrılabilir: kullanıcıların tüm bağlantılarında fiziksel kimlikleriyle (gerçek isimleriyle) ilişkilendirilemeyecek bir kimlik kullandıkları sürekli anonimlik (pseudonymity) ve her bağlantıda ayrı kimlik kullandıkları tek-kullanımlık anonimlik. "Sürekli anonim" kimliğe birbirleriyle ilişkilendirilebilen ancak gerçek kullanıcıyla ilişkilendirilemeyen mesajlar gönderilebilir. Tek-kullanımlık anonim kimlikte ise hiçbir mesaj birbiriyle ve kullanıcının gerçek kimliğiyle ilişkilendirilemez (Golberg et. al., 1996).

Bir Web sitesine girildiğinde ve Web sunucusundaki herhangi bir dosyaya erişildiğinde, Web sitesinin sahibi, kullanıcıya ait birtakım bilgilere ulaşabilir hale gelir (IP adresi, hostname, kıta, ülke, şehir, Web tarayıcısı, işletim sistemi, ekran çözünürlüğü, ekran renkleri, önceki URL, ISP vs.). Bu durum, IRC ağları ve oyuncuların birbirlerinin IP adreslerini görebildikleri çevrimiçi oyunlar için de geçerlidir (Rave, 1999).

E-posta adresleri kişilerin geçmişleri hakkında bilgiler içerebilir. Adres, belirli bir üniversitenin hangi bölümünde okunduğunu, hangi şirkette çalışıldığını gösterebilir. Soyad, ad ya da ikisinden de bağımsız belirleyici bazı kodlar içerebilir. Amerika'da bazı adresler sosyal güvenlik numarasına dayanmaktadır. Diğerleri 'u2338' gibi bir formatta olup yeni kullanıcılar katıldıkça artan bir düzendedir. Standart Internet adresleri coğrafik yer ve milliyet bilgileri de içerebilir. Örneğin; .us-Amerika, .uk-İngiltere, .ca-Kanada, .au-Avustralya vb., .edu-universite, .com-ticari organizasyon, .gov- hükümet, .mil-askeri site vb. (Detweiler, 1993).

Ağ anonimliğinin gerekli olduğu konulardan bazıları şu şekilde sıralanabilir; (Malkhi,2002; Daneziz, 2004) E-ticaret yapan şirketler, ilgili oldukları konuları, Internet üzerinde yaptıkları araştırmalarını ve işlemlerini rakiplerinden saklamak isteyebilirler. Şirketlerin yanısıra Web üzerinde alışveriş yapan, açık arttırmalara katılan, elektronik ödeme yapan bireyler de ziyaret ettikleri sitelerin ve hareketlerinin izlenmesini istemeyebilirler. Bunun yanısıra elektronik oylamalarda gizliliğin sağlanabilmesi, korkusuzca ve sansürsüz sosyal ve politik konuşmaların yapılabilmesi, çeşitli amaçlarla anonim mesajlar gönderilebilmesi, veri iletişimlerinde trafik analizinin önlenebilmesi, iki ya da daha fazla katılımcı arasındaki VPN (*Virtual Private Network*)

varlığının gizlenebilmesi anonimliğin sağlanmasını gerekmektedir. Özel ilgi grupları ile ilgili veritabanlarına erişen kişiler bu durumun gizli kalmasını isteyeceklerdir. Örneğin; AIDS taşıyıcısı olan ve bu nedenle ilgili veritabanlarına erişen bir kişi ya da çeşitli suçların (tecavüz, şiddet vs.) tanıkları, kurbanları destek gruplarıyla iletişimlerinde kimliklerinin bilinmesini istemeyeceklerdir. Özel araştırmalar yürüten, örneğin bir patent veritabanına erişmek için Internet'i kullanan bir araştırmacı odaklandığı konunun başkaları tarafından öğrenilmesini istemeyebilir. Bu ve bu gibi durumlarda anonimliğin sağlanması kullanıcılar açısından büyük önem taşımaktadır.

2.1 Çevrimiçi Anonimleştirme Nasıl Çalışır ?

Internet üzerinde anonimliğin sağlanmasının en yaygın ve en az karmaşık yollarından biri birçok anonimleştirici servisten birini kullanmaktır. "*Remailer*" denen bu anonimleştirici servisler, temel olarak Internet üzerinde e-postaları diğer ağ adreslerine ileten yönlendirici bilgisayarlardır (Rigby, 1995).

Temel olarak 3 tip yönlendirici bulunmaktadır; Johan Helsingius tarafından Kasım 1992'de tanıtılan *anon.penet.fi (type 0)* bunlar arasında en çok bilinenidir. Basitliği ve kullanımı kolay arayüzü sayesinde en çok kullanılan e-posta yönlendirici servislerinden biri olmasına rağmen, yasal baskılar nedeniyle Mart 1993'te kapanmıştır (Wells, 2001). Mesajı göndermeden önce belirleyici başlık kısmını çıkararak, gönderici anonimliği sağlamıştır. Aynı zamanda alıcılar için rastgele bir sahte kimlik yaratılarak alıcı anonimliği de sağlanmıştır. Kullanıcının gerçek e-posta adresi ile bu sahte kimliğini eşleştiren gizli bir tablo sayesinde, gelen mesajlar ilgili kullanıcının gerçek adresine ulaştırılmıştır. Dezavantajı; daha zayıf güvenlik sağlamış olmasıdır. Bu tablonun ve verilen kimliklerin güvenli bir şekilde korunduğunun ve kötü amaçlar için kullanılmayacağının bir güvencesi verilememiştir. Aynı zamanda, *anon.penet.fi* üzerinden geçen e-posta trafiğinin izlenmesi ile gelen-giden mesajların ilişkilendirilerek gerçek kimliklere ulaşılması da önlenememiştir (Golberg et. al., 1996).

Cypherpunk-stili (type I) yönlendiriciler bu tip tehditleri ortadan kaldırmak için tasarlanmıştır. İlk olarak bu sahte kimlikler ve gizli tablo kaldırılmış ve izlenebilme tehlikesi azaltılmıştır. Daha fazla güvenlik için, bir mesajı birçok anonim mesaj yönlendiriciden geçirerek iletme tekniğini uygulanmıştır.

Günümüzde, en yeni ve en gelişmiş e-posta yönlendirme teknolojisi Mixmaster (type II) yönlendiricileridir. Araya giren kişilerin gerçekleştirebileceği saldırılara karşı daha fazla güvenlik sağlamak hedeflenmiştir. Zincirleme ve zincirin her bağlantısında da şifreleme uygulanmıştır. Ayrıca, sabit-uzunlukta mesajlar kullanılarak gelen ve giden mesajların boyutlarından bir ilişkilendirilmeye gidilmesi engellenmiştir. Mesajın değiştirilerek yeniden gönderilmesi saldırılarına karşı korumalar içermektedir. Gelişmiş, mesajları yeniden sıralandırma kodu ile

zamanlama rastlantılarına dayanan pasif ilişkilendirme saldırıları önlenmeye çalışılmaktadır (Golberg et. al., 1996).

2.2 Anonimliğin Sağladığı Yararlar ve Riskleri

Internet üzerinde anonimliğin sağlanmasının getirdiği birçok yarar vardır. Anonimlik, kişilerin korkusuzca yasadışı eylemleri yetkililere ihbar edebilmelerini, politik konularda yorum yapabilmelerini sağlar. Bazı polis birimleri suçların anonim olarak ihbar edilebilmesi için çeşitli servisler kurmuşlardır. Anonimlik, tıbbi araştırmalarda, teşhislerin konmasında çok önemli ve potansiyel bir hayat kurtarıcı olabilir. Alkol, uyuşturucu bağımlısı, aile içi şiddete, çeşitli cinsel tacizlere maruz kalan, AIDS vb. fiziksel ya da ruhsal hastalığa yakalanmış kişiler, yüzyüze ya da telefonla görüşmeler, kimliğin belli olduğu açık mesajlaşmalar veya herkesin ne okuduğunu görebileceği kütüphane araştırmaları yerine, Internet üzerinden anonim bilgi sağlamayı veya mesajlaşmayı tercih etmektedir. Anonimlik olmadan bu eylemlerin yapılması, toplum içinde aşağılanma, fiziksel saldırılar, işin ya da statünün kaybedilmesi ve bazı durumlarda yasal soruşturmalara maruz kalma gibi sonuçlara yol açabilir. Bu tip sosyal nedenlerden dolayı oluşabilecek zararlardan ilgili kişilerin korunması, Internet üzerinde anonimliğin sağlanmasının yararları konusunda belirli bir örnektir. Anonim olarak gerçekleştirilen elektronik oylama hükümetin de bazı durumlarda anonimliğin önemini anlamış ve kabul etmiş olduğunu göstermektedir (Rigby, 1995, Kling et. al., 1999).

Anonimliğin varlığı da yokluğu kadar önemli bir konudur. Anonimlik, kullanımına bağlı olarak, problemlere de yol açabilecek güçlü bir araçtır. Anonim servislerden yararlanan çok sayıda kullanıcının bulunması, bu servislerin gerçekten gerekli olduğunun ve belirli bir ihtiyacı karşıladığının kanıtıdır. Ancak anonimliğin gün geçtikçe artan bilişim suçlarının takibini ve ortaya çıkarılmasını güçleştirmesi bazı önlemlerin alınması gerekliliğini ortaya koymaktadır.

Internet'in aracı olarak kullanıldığı suçların başında, Internet üzerinden yapılan ağır hakaretler, haksız rekabet, yasadışı eylemler ve fikri haklara tecavüz gelmektedir. Bu tür suçlarda, suçun işlendiği yer ve hangi ülkenin kanunlarının uygulanacağı, hukuki ve cezai sorumlulukların tespiti konularında sorunlar yaşanmaktadır. Internet aracılığıyla işlenen suçlar konusunda birçok ülkede düzenleme eksiklikleri vardır. Ayrıca Internet'te işlenen suçların takibi, faillerinin tespit edilmesi ve bu suçlara müdahele edilmesi konularında teknik yetersizlikler mevcuttur.

Ülkemizde Türk Ceza Kanunu'nda 1991 yılında, 3756 sayılı Kanun ile yapılan değişiklikle "Bilişim Alanında Suçlar" başlığı altında 525. Maddenin (a-b-c-d) bentlerinde bu türden suçlar düzenlenmiştir (Özel, 2000). Bu maddelere göre, ör; bir resmi dairenin sistemine girerek var olan bilgileri öğrenmek, değiştirmek ya da silmek, bir bankanın bilgisayar sistemine girerek kredi kartı borcunu silmek, bir virüsü Internet üzerinden yaymak, herhangi bir bilgi işlem sisteminin bozulmasına bu yolla neden olmak, bilgisayar programlarının güvenlik kodlarının kırılması ve dağıtılması (yazılım hırsızlığı), bir şekilde elde edilen e-posta adreslerine devamlı olarak reklam ya

da herhangi bir konuda yorum içeren e-postaların gönderilmesi, Internet ortamındaki kullanıcılar hakkında, haberleri olmaksızın veri toplanması gibi fiiller suç olarak tarif edilmiştir.

Ülkelerin Internet suçları ile ilgili yasal düzenlemelerinde farklılıklar bulunmaktadır. Örneğin Japonya'da bir sisteme izinsiz giriş yapmak, o izinsiz giriş ile elde edilen bilgiler satılmadıkça ya da bozulmadıkça suç sayılmamaktadır. Ülkemizde 1997 yılında İstanbul Emniyet Müdürlüğü Bilişim Suçları Bürosu kurulmuştur ancak çalışmaları teorik ve danışmanlık düzeyindedir. Amerika'da bilişim suçları ile ilgili mücadele için "*Commision of Critical Infrastructure Protection*" kurulmuştur. Bunun dışında, *"FBI National Infrastructure Protection Center", "Information Technology Association of America", "Trap and Trace Center Authority", "Carnegie Mellon's Emergency Response Team"* ve bazı üniversiteler bünyesinde kurulan birçok birim bulunmaktadır. Avrupa Birliği'nin bilişim suçları konusunda geçtiğimiz yıllarda yoğun bir çalışması olmuş ve bu çalışma sonucunda 8 Ocak 2001 tarihli "İnternet ve Bilgisayar Suçları ile İlgili Sözleşme Taslağı" hazırlanmıştır. Taslağın temel amacı bilişim suçları konusunda temel ve ortak bir mevzuat yaratmaktır çünkü bu tür suçlar dünyanın herhangi bir yerinden, ülke sınırları tanımaksızın işlenebilmektedir. Bunların dışında da birçok ülkede bilişim suçlarına karşı çeşitli birimler görev yapmaktadır. Bilişim suçlarına verilen cezalar da ülkeden ülkeye farklılıklar göstermektedir (Küçükgörkey, 2002).

3. SONUÇ

Web ortamında güvenlik ve mahremiyet ile ilgili yetersizlikler, kullanıcılar tarafından da net bir şekilde görülmeye başlandığından, bu konudaki çözümler her geçen gün daha da önem kazanmaktadır. Bu tehditlerden korunmak için kişisel önlemler almak zorunludur, ancak yeterli değildir. Anonimlik, mahremiyeti ve güvenliği sağlamak için kullanılabilecek önemli bir araçtır. Anonimliğin sağladığı birçok avantaj bulunmaktadır, bu nedenle kullanım alanları ve kullanıcı sayısı hızla artmaktadır.

Sağladığı tüm yararlara rağmen, Internet üzerinde anonimliğin sağlanması konusu henüz olgunlaşmamış bir tartışmadır. Beraberinde getirdiği riskleri en aza indirecek çözümler arttıkça ve tüm ülkelerde ortak bir görüş ve mevzuat oluşturuldukça daha güvenli ve yaygın kullanımı söz konusu olabilecektir.

KAYNAKLAR DİZİNİ

Chaum, D., February 1981, "Untraceable Electronic Mail, Return addresses and Digital Pseudonyms", *Communications of the ACM,* vol. 24 no. 2.
http://www.eskimo.com/~weidai/mix-net.txt

Cotrell, L., 1995, 'Mixmaster & Remailer Attacks'
http://www.obscura.com/~loki/remailer/remailer-essay.html

Daneziz, G., Feb 2004, Anonymous Communications & Traffic Analysis, University of Cambridge
http://www.cl.cam.ac.uk/~gd216/prez-17Feb04.pdf

Detweiler, L., 1993, Identity, Privacy and Anonymity on the Internet
http://www.rewi.hu-berlin.de/jura/proj/dsi/Netze/privint.html

Federrath, H., July 2000, Preproceedings of the Workshop on Design Issues in Anonymity and Unobservability, ICSI Berkeley, CA
http://www.icsi.berkeley.edu/ftp/pub/techreports/2000/ tr-00-011.pdf

Golberg, I., Wagner, D. and Brewer, E., 1996, Privacy-enhancing technologies for the Internet, University of California, Berkeley
http://www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html

Kling, R., Lee, Y., Teich, A., Frankel, M., Feb 1999, Assesing Anonymous Communication on the Internet: Policy Deliberations
http://www.indiana.edu/~tisj/readers/full-text/15-2%20kling .pdf

Küçükgörkey, A., Jan 2002, Dünyadaki ve Ülkemizdeki Bilişim Suçları ile İlgili Yasal Düzenlemeler
http://dergi.tbd.org.tr/yazarlar/02012002/asli_kucukgorkey.htm

Malkhi, D., 2002, Anonymity - Lecture Notes, Hebrew University
http://www.cs.huji.ac.il/~ns/Anonymity.doc

Özel, C., 2000, Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı
http://www.hukukcu.com/bilimsel/kitaplar/ bilisimsuclari_TCKtasarisi.htm

Rave, N., 1999, Black Sun's Anonymity Tutorial
http://old.astrolox.com/libraryc/anon.html

Reiter, M. K. and Rubin, **A. D.** November 1998, "Crowds: Anonymity for Web Transactions", *ACM Transactions on Information and System Security*, vol. 1, no. 1, pp. 66-92.
http://avirubin.com/crowds.pdf

Rigby, K., 1995, Anonymity on the Internet Must be Protected, MIT
http://www.swiss.ai.mit.edu/6095/student-papers/fall95-papers/rigby-anonymity.html

Stalder, F., Nov 1998, DigiCash: Learning from Failure, Telepolis Magazine
http://www.heise.de/tp/english/inhalt/te/1643/1.html

Stallings, 2003, Cryptography and Network Security, 2nd ed.

Theraider, 2003, Anonymity complete GUIDE
http:// www.governmentsecurity.org/articles/ AnonymitycompleteGUIDE.php

UGW, i.t. 2004, Securtiy Information Base, Anonymity Tutorial
http://www.under-host.com/hosts/ugw/tutorials/ anonymity.html

Web 1, 2003, Glossary of Security and Privacy Terms
http://security.resist.ca/glossary.shtml

Web 2, 2003, Anonymizer, PrivacyTest
http://www.anonymizer.com/privacytest/2.0/ privacytest.cgi?test=1

Web 3, 2004, ODTÜ, BİDB Enformatik Grubu Elektronik ve Bilgisayar Terimleri Sözlüğü (İngilizce-Türkçe)
http://www.bidb.odtu.edu.tr/index.php?go=ig&sub=dictio

Web 4, 2003, Anonymizer, Ten Steps to Privacy
http://www.anonymizer.com/tensteps/index.shtml

Web 5, 2000, Protection of Privacy on the Internet, JAP
http://anon.inf.tu-dresden.de/index_en.html

Web 6, 2003, Anonymizer, Product List
http://www.anonymizer.com/products.shtml

Web 7, 1999, How PGP Works, Introduction to Cryptography, Chapter1,
Network Associates, Inc.
http://www.pgpi.org/doc/pgpintro/

Web 8, 2004, A Crime By Any Other Name, Freedom Magazine
http://www.theta.com/goodman/crime.htm

Web 9, i.t. 2004, Ray Dillinger, Cyclopedia Cryptologia - an online encyclopedia of cryptographic protocols.
http://www.disappearing-inc.com/

Web 10, 2000, The Onion Routing home page.
http://www.onion-router.net/

Web 11, i.t. 2004, CookieCooker
http://cookie.inf.tu-dresden.de/index_en.html

Web 12, Apr 2004, Electronic Money, or E-Money, and Digital Cash
http://www.ex.ac.uk/~RDavies/arian/emoney.html

Wells, J., 2001, Existing Anonymity Solutions
http://io.irean.vt.edu/~wells/rapport/node35.html

Wright, M., Adler, M., Levine, B.N. and Shields, C., February 2002,
An Analysis of the Degradation of Anonymous Protocols, *Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS 2002)*
http://www.cs.umass.edu/~mwright/papers/wright-degrade.pdf