Türkiye'de ve Dünyada Spam Karşıtı Politikalar
ve
SPAM ile Savaşmak İçin Geliştirilen Anti-Spam Modeli

Enis Karaarslan*, Erhan Çetin**
* enis@bornova.ege.edu.tr, ** erce@bornova.ege.edu.tr
Ege Üniversitesi Network Yönetim Grubu

ÖZET

Türkiye'de spam ile savaşma ile ilgili bilgilendirme çalışmaları ***Türk Anti-Spam Organizasyonu*** (TASO) tarafından web üzerinden (www.spam.org.tr) yürütülmektedir. Ne yazık ki bu çalışmalar yeteri kadar desteklenmemekte ve henüz spam ile savaşma konusunda Türkiye'de hukuksal bir yaptırım bulunmamaktadır. Bu bildiride dünyanın çeşitli yerlerindeki çalışmalardan örnekler verilmiş ve Ege Üniversitesi'nde uygulanan EÜ-SMES (Ege Üniversitesi Spam Mail Engelleme Sistemi) tanıtılmıştır. Var olan RBL servisinin aksine bu sistem ip adresi yerine mail adresi bloklamaktadır. Bu sistem RBL servisinin eksik kaldığı noktaları gideren yeni bir modeldir. Ayrıca bu bildiride spam'le savaşın kurumlar arası bir yardımlaşma ve dayanışma ile yerine getirilebilmesi için tasarlanmış olan Merkezi ve Dağıtık Sistem Modelleri tanıtılmıştır.

1. SPAM NEDİR?

İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi ***spam*** olarak adlandırılır. Spam çoğunlukla ticari reklam niteliğinde olmaktadır[1]. Spam iletilerinin masrafı düşük olduğundan iletiler gönderilirken bir hedef kitle aranmaz ve bu tür mail'leri almak istemeyen binlerce kişi rahatsız edilir[2]. Spam gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük büyük ölçüde mesajın alıcıları veya taşıyıcı, servis sağlayıcı kurumlar tarafından karşılanmak zorunda kalınır[1]. http://www.caube.org.au/spamstats.html İnternet adresinde verilen istatistiklerde de görüleceği üzere problem her geçen gün daha kötüye gitmektedir.

2. SPAM İLE SAVAŞAN KURULUŞLAR

Spam ile savaşan belli başlı bağımsız organizasyonlar olarak aşağıdakiler verilebilir:

- **TASO** - "***Türk Anti-Spam Organizasyonu***", 1999 yılında kurulmuş sanal bir çalışma grubudur. Organizasyonun hedefi kamuoyunu bilinçlendirmek ve Türkiye'de spam ile mücadele edebilmek için teknolojik çözümleri tartışmak ve oluşturmaktır. Grup çalışmalarını http://www.spam.org.tr web sitesinden ve bir tartışma listesinden yürütmektedir [3].
- **CAUCE** (The Coalition Against Unsolicited Commercial Email) dünya çapında spam ile savaşan bir bağımsız organizasyondur (http://www.cauce.org). Bu organizasyon Avrupa, Kanada ve Hindistan'daki alt kuruluşlarla desteklenmektedir.
- **SPAMCON** Foundation (http://www.spamcon.org/)
- **FREE** (www.spamfree.org)

3. HUKUKSAL BOYUT

CAUCE organizasyonlarının düzenlediği anketler ve çalışmalara göre kullanıcılar spam mesajlarının bir pazarlama aracı olarak yaygın kullanımını kontrol altına alacak yasalar talep etmektedir. Almanya ve Hollanda'da spam mail yasaktır. Avrupa Birliği, ***Opt-in Politikası***'nı kabul etmiş ve kullanıcının daha önceden rızası olmadan ticari mail'lerin gönderilmesine EEA (European Economic Area) içinde izin verilmeyeceğini belirtmiştir[4]. ***Opt-in Politikası***, kullanıcıların ihtiyaç duydukları alışveriş ve pazarlama bilgisini talep etme fırsatını sağlamakta ve böylece pazarlamacılar da hedefledikleri kitleye ulaşmaktadırlar. Böylece İnternet Servis sağlayıcıları da hızlı, efektif ve güvenli elektronik posta akışını sağlayabilme imkanına ulaşmaktadırlar. Opt-out politikasının işe yaramadığı Amerika'daki uygulamalarda tespit edilmiştir[4]. İki politikanın karşılaştırması için [5]'ya bakılabilir.

4. SPAM İLE SAVAŞMA YÖNTEMLERİ

Kurumun Kabuledilebilir Kullanım Politikasında (Acceptable Use Policy) kesinlikle spam'e karşı olunduğu ve öngörülen yaptırımlar belirtilmelidir. Böylece kullanıcılar önceden bilgilendirilmiş olacaktır. AOL'ün kullanım politikası için bakınız [6].

SPAM ile savaşırken unutulmaması gereken en önemli kural sakin davranmak ve ortamın gerginleşmesine izin vermemektir. Spam'e karşı bir saldırı veya spam ile cevap vermenin herhangi bir yarar sağlamayacağı bilinmelidir [7]. SPAM mesajların önlenmesi açısından gerek sistem yöneticilerinin gerekse Internet kullanıcıların alabilecekleri önlemler için bakınız[8].

İletiler yönetilen mail sunucusunun bir ara sunucu (relay) olarak kullanılması şeklinde iletiliyorsa, sunucuda relay özelliğini iptal etmek için gerekli ayarlamalar yapılmalıdır. Detaylar için bakınız[9].

SPAM iletilerinden korunmanın yollarından bir tanesi de, SPAM kaynağı veya açık relay olan mail sunucularının bir listesini kontrol etmek suretiyle, kara listedeki sunuculardan gelen mailleri reddetmektir. Bu alanda faaliyet gösteren üç servis aşağıda kısaca incelenmiştir[10]:

1. **MAPS – RBL (** http://maps.vix.com/rbl): RBL (Realtime Blackhole List, Gerçek Zamanlı Karadelik Listesi) Mail Abuse Prevention Systems (MAPS) tarafından işletilmekte olan bir sistemdir. Serviste açık relay sunucuları olduğu kadar, sadece SPAM kaynağı olan sunucular da listelenir. TASO tarafından Türkiye kaynaklı spam iletilerini önlemek için ***RBL-TR*** adlı servis yürütülmektedir [11]**.**
2. **MAPS – RSS (** http://maps.vix.com/rss): Relay Spam Stopper (RSS) servisi de MAPS tarafından işletilmektedir. RBL servisinden farklı olarak bu serviste, üzerinden spam gönderilen açık relay sunucular listelenir ve veritabanına yapılacak ekleme başvurularında SPAM ve açık relay'in kapatılması konusunda daha önce ilgili kuruma başvurulmuş olunması şartı aranmaz.
3. **ORBS (** http://www.orbs.org) : ORBS servisi RBL ve RSS'den farklı olarak sadece açık relay durumundaki sunucuları listeler. Sunucunun rapor edilmesi için sistem yöneticileri ile konu hakkında görüşülmüş olması gerekmediği gibi, sunucu üzerinden SPAM iletileri gönderiliyor olması da gerekmez.

5. ÖNGÖRÜLEN MODEL

Mail sunuculardа “kara liste servisi” seçildiğinde varsayılan olarak MAPS-RBL servisi kullanıldığından en yaygın olan servistir. RBL servisi ile bir IP veya IP bloğundan gelen mail’ler tümüyle kapatılacağı için kullanıcının bu tür bir kapatma talebinde bulunmadan önce yapması gerekenler şunlardır: ilk olarak spam gönderen site yöneticisine başvurmuş olması gerekmektedir. IP bloğunun tümüyle kapatılabilmesi için, yapılan başvurunun olumsuz sonuçlanması veya 24 saat içerisinde yanıt alınamamış olması gerekmektedir. Kullanıcı bu durumda bir üst sağlayıcı ile görüşerek durumu bildirmeli ve önlem alınmasını istemelidir. Bu durumda servis sağlayan firmadan da bu konuda kullanıcıyı uyardıklarına dair bir mail’in gelebilmektedir. Ancak bu işlemler halledilene kadar spam gönderen kişi mesaj atma işlemine devam etmekte ve bu yolla söz konusu kullanıcının ve hatta diğer mail sahiplerinin mail kotalarını ve zamanlarını harcamaktadır. Kısaca “Kara Listeye Ekleme ve Çıkarma” diye tabir ettiğimiz bu işin ayrıntıları için bakınız[10].

Bu büyük sorunun yükünü ve maliyetini hafifletmek için önereceğimiz modelde yukarıda anlatılan prosedürlere takılmaksızın pratik ve ekonomik bir çözüm ortaya konulmaktadır. Halen Ege Üniversitesi’nde bir bölümüyle uygulanan EÜ-SMES’de (Ege Üniversitesi Spam Mail Engelleme Sistemi) ve bir sonraki bölümde daha ayrıntılı haliyle ele alacağımız modelde, IP adresi yerine mail adresi engellenmektedir. Böylece o anda gelmeye devam eden istenmeyen mesajlar zaman kaybedilmeden engellenmektedir. Ayrıca ağ ve mail sunucuların kaynaklarının daha fazla israf edilmesinin önüne geçildiği gibi kullanıcıların da boşuna zaman harcaması engellenmektedir. Bu modele göre herhangi bir mail adresi bir sunucuda yer alan “spam öneri listesi” veritabanına eklendiğinde sistem yöneticisi elle veya diğer yöntemlerle bu maili “kesin spam listesine” ve mail sunucu veya mail hub’daki “erişim listesine” ekleyerek gönderilen bu spam mail’e karşı önlem almaktadır. Bu yapı bir çok kurum ve kuruluş tarafından kullanılabilir hale getirilip yaygınlaştırılabilir.

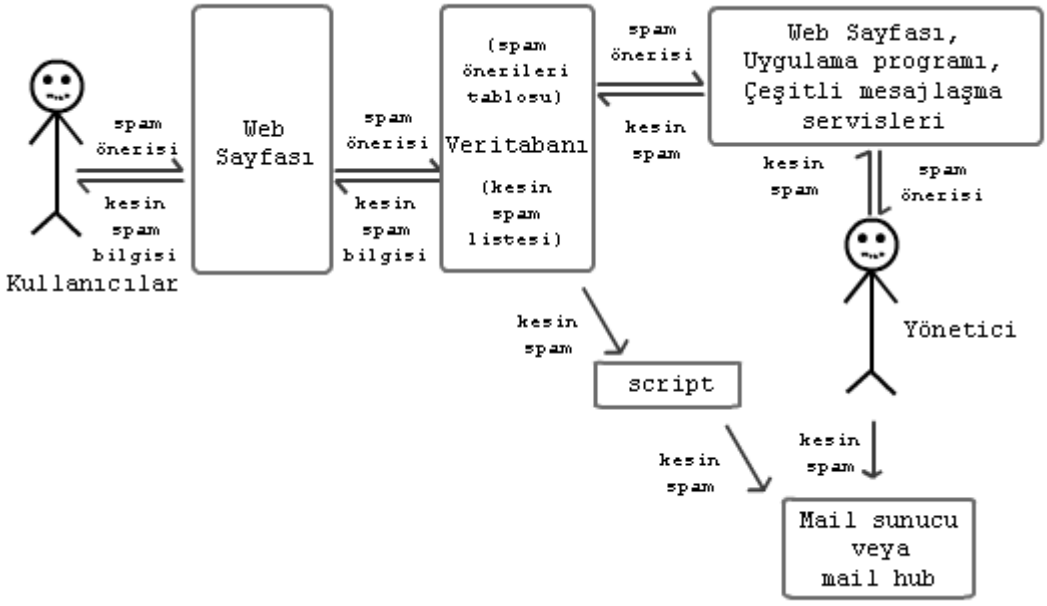
Spam’le savaşın kurumlar arası bir yardımlaşma ve dayanışma ile yerine getirilebilmesi için önereceğimiz ikinci yapı ise dağıtık çalışma modelidir. Bu modele göre her kurum veya kuruluşun kendisine ait sunucuları üzerinde, o kurum veya kuruluşlara ulaşan spam maillerin bir listesi tutulmaktadır. Tutulan her bir listeye birer versiyon numarası verilmektedir. Bu versiyon numaraları listeye bir kayıt eklendiğinde, silindiğinde veya güncelleme yapıldığında değişmektedir. Her sunucu kendi üzerindeki listenin versiyon numarasını belirli aralıklarla kontrol etmektedir. Eğer versiyon numarasında bir önceki kontrole göre bir değişiklik varsa bu değişiklik tetikleme yoluyla diğer kurumlara ait sunuculara iletilmektedir. Birbiriyle sürekli haberleşen sunucular böylece kesintisiz olarak spam listelerini güncellemektedirler. Bu doğrultuda sisteme bağlı olan tüm sunucularda eş zamanlı olarak tüm spam gönderen mail adresleri engellenmektedir.

Öngörülen modellerin detaylarını ele almadan önce bazı kavramların ne olduğunun hatırlanmasında yarar görülmektedir. “Mail Sunucu”, mail göndermek için 25. mail almak için 109. TCP port’unu kullanan mail gönderme ve kabul etme işi için biçimlendirilmiş makinedir. “Mail Hub”, kullanıcılar ile İnternet arasında mail trafiğini kontrol eden bir arayüz olarak görev yapan yerel ağda (LAN) çalışan bir makinedir. Birden fazla mail sunucu olan büyük bir ağda diğer sunuculara gelen

mailler önce mail hub ‘dan geçirilebilir. “Spam öneri listesi”, kullanıcılardan gelen spam mail önerilerinin tutulduğu veritabanı tablosudur. “Kesin spam listesi”, yöneticilerden spam olduğuna dair kesin onay alan spam maillerin tutulduğu veritabanı tablosudur. “Erişim listesi”, seçilen bir domain’den veya adresten mail alınmasını veya gönderilmesini engellemek için oluşturulmuş dosyadır. “Script”, Linux kabuk programı veya “Perl” gibi bir programlama dilinde yazılmış, veritabanını okuyup erişim listesi dosyalarına otomatik olarak yazma kabiliyeti olan programlardır.

Halen Ege Üniversitesinde Kullanılmakta Olan Model

Halen Ege Üniversitesi’nde kullanılmakta olan yapı, önereceğimiz modelin ilk ayağını oluşturmaktadır. Bu yapıya göre sunuculardan bir tanesi merkezi sunucu olarak belirlenmekte ve bu sunucu üzerinde veritabanı tutulmaktadır. Bu veritabanında öneri olarak gelen ve kesin mail adreslerinin yanı sıra gelen maillerin içeriğini tanımlayıcı bilgiler ve eğer gerekli görülüyorsa bilgi edinme amaçlı olarak mail’in bir kopyası ile “mail header” bilgisi tutulmaktadır. Ege Üniversitesi hizmet alanı kapsamında yer alan tüm kullanıcıların sistem ile etkileşim kurabilmeleri için web sayfaları kullanılmaktadır. Modelde yönetimsel fonksiyonları yerine getirmek için bir veya birden çok sistem yöneticisi bulunmaktadır. Son olarak erişim listelerinin güncellenmesi işlemini otomatize etmek için script’ler yer almaktadır. Bu modeli özetleyen çizenek Şekil-1’de gösterilmiştir.



Şekil-1: Ege Üniversitesi Spam Mail Engelleme Servisi Yapısı.

Şekil-1’den de görülebileceği gibi Ege Üniversitesi hizmet alanı içersinde yer alan kullanıcıların tamamı sistem ile kesintisiz olarak etkileşim kurabilmektedir. Kullanıcılar kendilerine gelen spam mail’leri aktif olarak yönetime bildirebilmekte ve kesin spam listelerine ulaşabilmektedirler. Kullanıcıların spam mail önerisinde bulunabilmeleri için kendilerine sağlanmış olan web sayfasındaki spam öneri formunu doldurmaları yeterlidir. Bu form ile kullanıcıya gelen spam mail’in adresi, başlık bilgisi ve bir kopyası ile kullanıcıyla irtibat kurulabilecek bir mail adresi alınması sağlanmaktadır. Bu sayede sistem yöneticileri gelen önerileri değerlendirerek spam veritabanını güncel tutmaktadır. Sistem yöneticileri kendilerine gelen önerileri

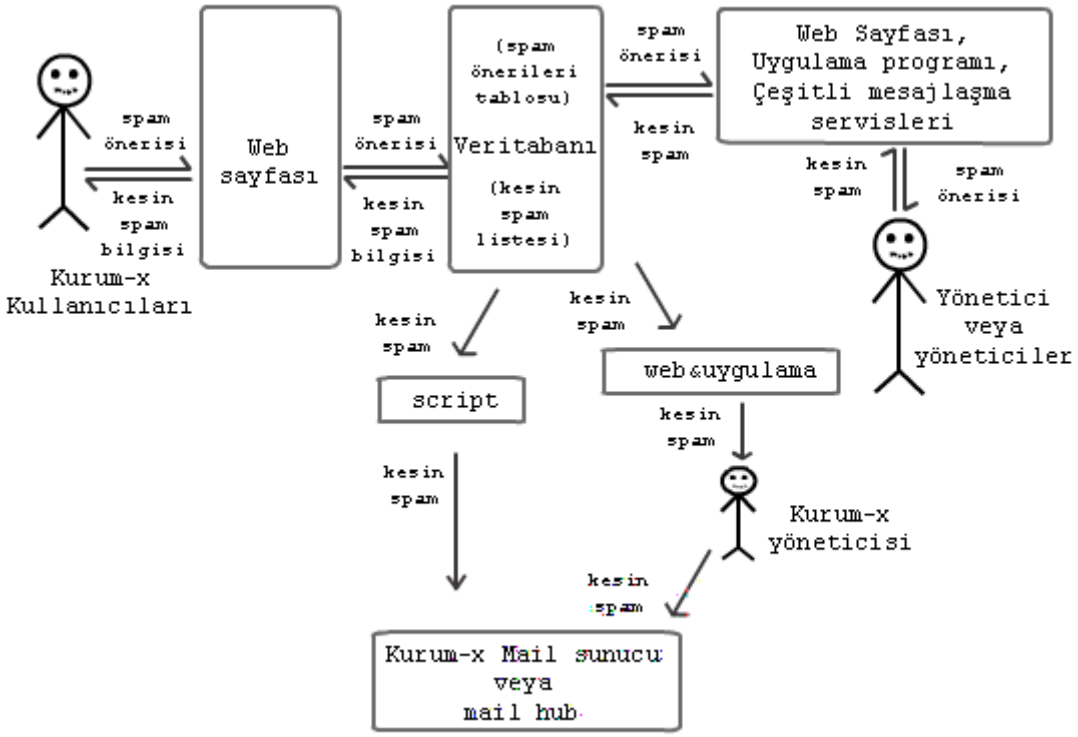
değerlendirip uygun gördükleri spam mail'leri kesin spam listesine eklemektedir. Kesin spam listesine geçen her spam mail aynı anda elle veya script'ler aracılığıyla erişim listelerine aktarılır. Kesin kayda geçen her spam mail yine bir web sayfası aracılığıyla dinamik olarak bilgilendirme amaçlı olarak kullanıcılara bildirilmektedir.

Önerilecek Olan İki Farklı Model

Spam mail ile ulusal boyutta etkin mücadele için önereceğimiz iki farklı model bulunmaktadır. Bu modellerden ilki halen Ege Üniversitesi'nde kullanılmakta olan sistemden esinlenilerek geliştirilmiş olan merkezi sistem modeli, ikincisi ise dağıtık sistem modelidir.

MODEL-1:Merkezi Sistem Modeli

Spam ile mücadele için geliştirdiğimiz ilk sistem modeline sistem mantığının ve veritabanlarının tek bir merkezde toplanması sebebiyle "Merkezi Sistem Modeli" adını verdik. Merkezi Sistem Modeli'nde spam önerilerini ve kesin spam listelerini tutan bir adet veritabanı bulunmaktadır. Üye olan kurum kullanıcıları sistem ile etkileşim kurabilmek için web sayfalarını kullanmaktadır. Sistemde iki çeşit yönetici sınıfı bulunmaktadır. Bunlardan ilki gelen spam önerilerini değerlendirip kesin spam listesini oluşturan "Merkez Sistem Yöneticisi" iken, ikincisi oluşturulmuş olan kesin spam listesini kendi kurumunda bulunan mail sunucu veya mail hub'ın erişim listesine ekleyen "Kurum Yöneticisi"dir. Sistemde kesin spam listesi güncellemelerini otomatik olarak yapmak isteyen kurumlar için script'ler de bulunmaktadır. Merkezi sistem modelinin yapı ve işleyişini özetleyen çizenek Şekil-2'de gösterilmiştir.



Şekil-2: Merkezi Sistem Modeli

Şekil-2'den de görüleceği gibi Merkezi Sistem Modeline üye olan her kuruma ait kullanıcılar spam mail önerisinde bulunmaktadır. Kullanıcılar bu önerileri kendilerine

sunulan spam öneri formunun yer aldığı web sayfaları aracılığıyla yapmaktadır. Kullanıcılardan gelen tüm spam önerileri veritabanının ilgili tablosunda tutulmaktadır. Merkez sistem yöneticisi kullanıcılardan gelen spam önerilerini bir web sayfası, bir uygulama programı veya mail gibi bir mesajlaşma servisi kullanarak kontrol ettikten sonra uygun gördüğü önerileri kesin spam listesine işlemektedir. Her kurumun kendi yöneticisi belirli aralıklarla kesin spam listesini kendisine sağlanan web sayfası veya uygulama programları aracılığıyla tarayabilmektedir. Bu tarama sonucu istediği spam mailleri seçerek kendi sisteminde yer alan mail sunucu veya mail hub üzerindeki erişim listesine eklemektedir. Spam maillerin otomatik olarak kendi mail sunucuları yada mail hub'larındaki erişim listelerine yazılmasını isteyen kurumlar için sistemde yer alan script'ler bu görevi yerine getirmektedir.

MODEL-2: Dağıtık Sistem Modeli

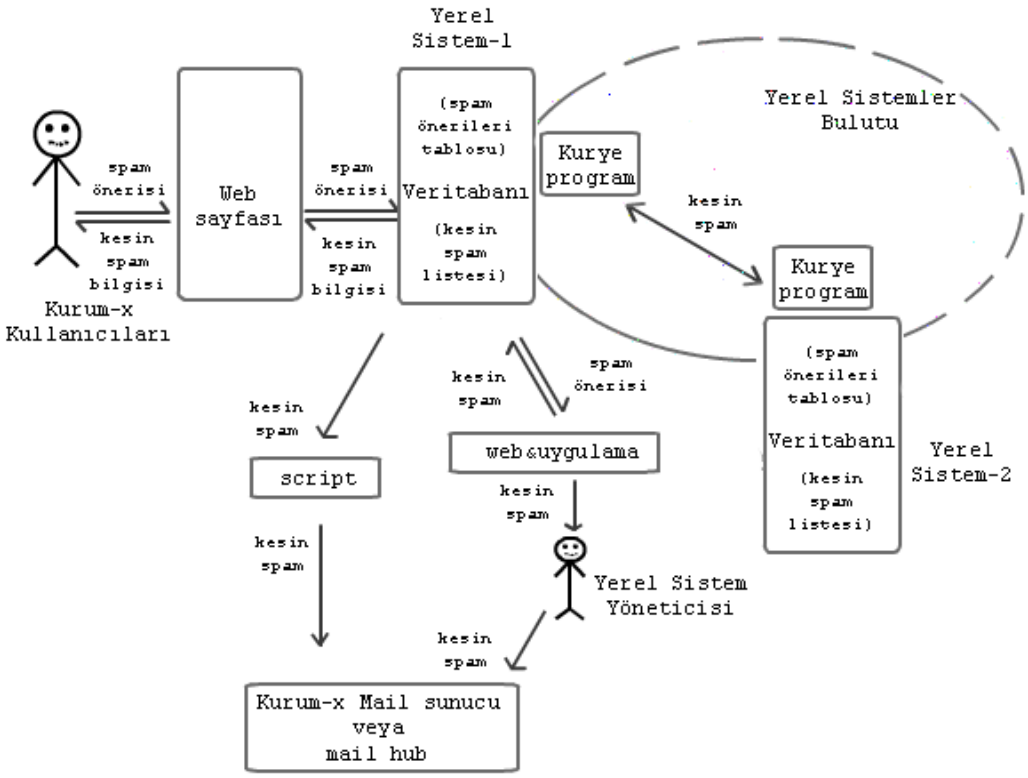
Spam mail ile mücadele için önereceğimiz ikinci model ilk modelden hem işleyiş hem de sistem mantığı olarak farklılık göstermektedir. Bu modelde her kurum için ayrı bir veritabanı ve her kurumun kendi yöneticisi bulunmaktadır. Bu özelliğinden dolayı bu modele "Dağıtık Sistem Modeli" adı verilmiştir. Dağıtık Sistem Modeli'nde her bir kurum veya kuruluş için ilgili kurum veya kuruluşa ait gelen spam önerilerinin ve kesin spam listelerinin üzerlerinde tutulduğu özerk veritabanları yer almaktadır. Yine her bir kurumda gelen spam önerilerini değerlendirerek kesin spam listesini oluşturmak ve kesim spam listesine göre mail sunucu veya mail hubdaki erişim listesini güncellemek üzere yerel sistem yöneticileri bulunmaktadır. Her kurumun kendi kullanıcılarının spam önerisinde bulunabilmesi ve kesin spam listesini görebilmesi için sistemde web sayfaları bulunmaktadır. Erişim listelerinin elle güncellenmesi yerine otomatik olarak güncellenebilmesi için sistemde script'ler yer almaktadır.

Dağıtık sistem modelinde her bir yerel sistemin birbiri ile etkileşim kurabilmesi için "kurye programlar" yer almaktadır. Bu programlar veritabanı ile aynı sunucu üzerinde olabileceği gibi, veritabanı ile iletişim kurabilecek başka bir sunucu üzerinde de olabilir. Bu programlar sabit bir port'u dinlemek ve yine bu port üzerinden komşu sistemlerde bulunan hemcinslerine ileti göndermek üzere tasarlanmışlardır. Burada bahsedilen komşuluk mekanizması ise çeşitli kriterlere göre değişiklik gösterebilmektedir. Dağıtık sistem modelinin yapı ve işleyişini özetleyen çizenek Şekil-3'te gösterilmiştir.

Şekil-3'ten de görüldüğü gibi dağıtık sistem modelinde her kurumun kendi kullanıcıları, kendi yerel sistemlerince sağlanan web sayfalarındaki spam öneri formları aracılığıyla yine kendi yerel sistemlerindeki veritabanlarına spam önerisi ekleyebilmektedir. Her bir yerel sistem yöneticisi kendi veritabanında toplanan spam önerilerini çeşitli kriterlere göre değerlendirir ve uygun gördüklerini veritabanındaki kesin spam listesi tablosuna kaydeder. Bunun akabinde iki durum söz konusudur. Bunlardan ilki mail sunucu veya mail hub'daki erişim listesinin yeni oluşan kesin spam listesine göre elle güncellenmesidir. İkinci yöntem ise script'ler aracılığıyla otomatik güncelleme yapma yöntemidir.

Yerel sistem yöneticisinin kesin spam listesi üzerinde herhangi bir değişiklik yapması halinde bu listeye ait versiyon numarası otomatik olarak değiştirilir. Sistemde yer alan, önceden belirlenmiş bir port'u dinleme ve yine bu port üzerinden mesaj

gönderme yeteneğine sahip olan “kurye program” belirli aralıklarla versiyon numarasını kontrol eder. Eğer versiyon numarasında herhangi bir değişiklik olmuşsa bu değişikliği sunucu üzerinde kendisine tahsis edilmiş port’u kullanmak kaydıyla kendisine komşu olan diğer yerel sistemlere iletir.



Şekil-3: Dağıtık Sistem Modeli

Komşu yerel sistemlerde de yine bu kurye programın birer kopyası bulunmaktadır. Aynı port’u dinlemekte olan bu programlarda gelen mesajı alarak kendi yerel sistemlerindeki kesin spam listesini güncellemektedir. Komşu yerel sistem mail sunucu veya mail hub’ındaki erişim listesini otomatik olarak güncelleme yöntemini benimsemiş ise güncelleme işlemi scriptler aracılığıyla doğrudan gerçekleştirilir. Eğer elle güncelleme yöntemi benimsenmişse, komşu sistemin kurye programı kendi yerel sistemine diğer komşulardan yeni kesin spam bildirisi geldiği yönünde bir mail veya uyarı mesajı ile yerel sistem yöneticisini bilgilendirir.

Yukarıda anlatılanlar özetlenirse Dağıtık Sistem Modeli’nin esas aldığı yapı, yerel sistemlerin kendi içersinde aktif tutulması ve her bir yerel sistemin belirlenen komşuluk prensibi dahilinde birbiri ile haberleşerek “kesin spam listesi” veritabanını güncel tutmasıdır.

6. ÇÖZÜM VE SONUÇLAR

Spam’den zarar gören kişileri korumak için hukuksal düzenlemelerin bir an önce yerine getirilmesi gerekmektedir. Bize düşen İnternet kullanıcılarına bu konuda yeterli eğitimi sağlayarak İnternet etiğinin kazandırılmasını sağlamak olmalıdır. Bunların yanı sıra sistem yöneticileri tarafından kullanıcıların ve yönetilen sistemin bu tür mesajlarla uğraşmasını engelleyecek önlemler alınması gerekmektedir.

Bildiride spam mail'leri engellemek için geliştirilen Merkezi ve Dağıtık Sistem Modelleri anlatılmıştır. Her ne kadar Merkezi Sistem Modeli'nin kurulumu ve kullanımı basit olsa da tek bir merkezden yönetilmesi yönetimsel açıdan bazı sorunlara yol açabilecektir. Bu sorunlardan ilki her zaman görevi başında olması gereken bir yöneticinin bulunması gerekliliğidir. Diğer bir sorun ise merkezdeki yöneticinin yükünün çok fazla olmasıdır. Merkezi Sistem Modeli'nde karşılaşılabilecek bir başka sorun ise merkezdeki makine üzerindeki yükün artması ve yedekleme sorunu olacaktır. Ayrıca merkezdeki sunucuya İnternet üzerinden hem kurum yöneticileri hem de kullanıcılar tarafından sürekli erişim olması band genişliği israfı gibi bazı zayıflıklara sahiptir. Merkez sunucunun devre dışı kalması sonucunda sistemin çalışmayacak olması da bu sistemin en büyük dezavantajıdır.

Merkezi Sistem Modeli'ne alternatif olarak geliştirilen Dağıtık Sistem Modeli yukarıda anlatılan eksikliklere çözüm getirmektedir. Dağıtık Sistem Modeli'nin kullanımı kolay olmasına karşın kurulum aşaması biraz karmaşık olabilecektir. Ancak kurulum olayının bir kereye mahsus olduğu düşünülürse, Dağıtık Sistem Modeli'nin sunduğu etkin ve özerk yönetim, özerk veritabanı, özerk web hizmeti gibi özellikler onu değerli kılmaktadır. Bunun yanı sıra her yerel sistem eşzamanlı olarak güncelleneceği için, yerel sistemlerden bir tanesi çökse bile bu modelde yedekleme sorunu yaşanmayacaktır. Kullanıcıların kendi yerel sunucularını kullanacağı ve veri iletişiminin yalnızca kesin spam listeleri değiştiği zaman gerçekleşeceği için daha az band genişliği kullanılacaktır.

KAYNAKLAR

[1] Spam Nedir?, http://www.spam.org.tr/nedir.html

[2] SPAM Nicin Kotudur ? , Original Text: John Levine, Eklemeler: Arif Oktay, Çev: Çağrı Yücel, http://www.spam.org.tr/nicinkotudur.html

[3] İnternet'te Huzursuzluk Kaynağı: Spam, Burak Dayıoğlu http://www.spam.org.tr/SpamBD.html

[4] 20 reasons to support the culture committee amendment on article 7 of the e-commerce directive, http://www.euro.cauce.org/en/20reasons.html

[5] Opt-in vs. Opt Out, http://www.euro.cauce.org/en/optinvsoptout.html

[6] AUP (Kabuledilebilir Kullanım Politikası) Örnegi II : America Online, Çeviren : Deniz Kanca, http://www.spam.org.tr/aup/aup2t.html

[7] SPAM Karşısında Neler Yapılmamalıdır, http://www.spam.org.tr/yapilmamali.html

[8] Spam Mesajlarının Önlenmesi, http://www.spam.org.tr/onlenmesi.html

[9] Anti-Relay: Mail Relay'i Kapatmak, http://www.spam.org.tr/relayturkce.html

[10] SPAM'dan korunma çözümleri (RBL servisleri), Çağrı Yücel http://www.spam.org.tr/rbl.html

[11] RBL-TR Servisi, http://www.spam.org.tr/rbl/