OPENGATE CAPTİVE PORTAL İÇİN KULLANICI DOSTU BİR UYGULAMA YAZILIMI

Ramazan Özgür DOĞAN[1], Hayati TÜRE[2]

[1] Gümüşhane Üniversitesi, Gümüşhane Meslek Yüksekokulu, Gümüşhane

[2] Karadeniz Teknik Üniversitesi, Bilgiişlem Daire Başkanlığı, Trabzon

ramazan.dogan@gumushane.edu.tr, hture@ktu.edu.tr

ÖZET

5651 sayılı kanunun internet sağlayıcılarına getirmiş olduğu yükümlülükten dolayı kullanıcıların iç dağıtım loglarını elektronik ortamda kendi sistemlerine kaydetmeleri gerekmektedir. Bu yükümlülük internet sağlayıcılarına çeşitli yöntemlerle birlikte kullanıcı adı şifre doğrulaması yapabilme yeteneğine sahip yazılım ve donanımlar kullanmaya yönlendirmiştir. Yapılması istenen işlem için donanımdan bağımsız mevcut sisteme dâhil edilmesi kolay ve aynı zamanda kullanıcıya kolaylık getiren kimlik denetleme sistemleri geliştirilmektedir. Bu ihtiyacı karşılamak için ticari veya açık kaynak kodlu Captive Portal isimli yazılımlar ile ağ üzerinden bir web tarayıcısı ile birlikte kimlik doğrulama işlemini gerçekleştirilebilmektedir.

Bu çalışmada açık kaynak kodlu Captive Portal sistemlerinin kullanıcılara getirmiş olduğu rutin işlemleri kolaylaştıran bir yazılım geliştirilmiştir.

Anahtar Kelimeler: 5651 Sayılı Kanun, Captive Portal, IEEE 802.1X, Opengate

1. Giriş

Günümüzde internet kullanıcı sayısının artışı ile siber suçlarda da artış görülmeye başlamıştır. Bu sorun bilhassa istemci sayısının fazla olduğu kuruluşlarda bilişim suçu işleyen kişilerin tespitini zorlaştırmaktadır. Bu sorunun çözümü için ülkemizde de bilişim suçları ile mücadeleyi amaçlayan 5651 sayılı kanun çıkarılmıştır. Bu kapsamda çok kullanıcılı sistemler için de çalışabilen donanımsal veya yazılımsal çözümler geliştirilmiştir.

Çok kullanıcılı sistemlerde kimlik denetimli internet erişimi için donanımsal çözüm olarak IEEE 802.1X standardı kullanılmaktadır. IEEE 802.1X standardı; noktadan noktaya bağlantılara sahip LAN portuna takılmış cihazların kimlik doğrulama ve yetkilendirilmesine olanak sağlayan port tabanlı ağ erişim denetimidir. Ağda port tabanlı kullanıcı doğrulayabilmek, herhangi bir kullanıcıya ya da gruba 'ağa erişim politikaları' uygulamaya imkân tanır. Kimlik doğrulama ve yetkilendirme başarısızsa o port erişime kapatılır ve bu sayede yerel ağ altyapısı korunmuş olur. Kullanıcı doğrulama; MAC adresi, switch portu ya da harici bir yetkilendirme politikası ile sağlanır. Ağa kimin hangi hakla gireceğinin belirlenmesi, denetlenmesi ve yetkilendirmesi; kullanıcı odaklı, ağ tabanlı erişim kontrolü olan NAC tarafından belirlenir.

Aynı sorun için yazılımsal olarak da donanımdan bağımsız çalışan Captive Portal tekniği kullanılabilmektedir. Captive Portal tekniği http ve https istemcilerini interneti kullanmaya başlamadan önce ağ üzerinden özel bir web sayfası görüntüleyerek kullanıcı bilgileri ile giriş yapmaya zorlamaktadır. Bir anlamda web tarayıcı kimlik denetleme cihazına çevrilmektedir. Bu sistemde kimlik denetimi gerçekleştirilmeden önce porttan veya adresten bağımsız olarak tüm paketler engellenerek istemcinin internete erişimi kısıtlanmaktadır. İstemci tarafından gerçekleştirilen her web sayfası görüntüleme isteği istemciyi kimlik denetiminin gerçekleştirileceği özel bir sayfaya yönlendirmektedir.

Bu çalışmada yazılımsal çözüm olan Captive-Portalın kullanımı esnasında web tarayıcı çalıştırılmadan kimlik doğrulaması yapabilen bir yazılım geliştirilmiştir ve kimlik denetimli internet erişiminde kullanım kolaylığı sağlanacaktır.

2. 5651 Sayılı Kanun

5651 sayılı kanun maddesi internet erişiminin kontrol altına alınmasını amaçlamaktadır. Bu sayede internet üzerinden işlenen bilişim suçlarının önemli ölçüde önüne geçilmekle beraber suç unsuru içeren herhangi bir olay sonrasında suçlu ya da sorumluların tespit edilerek suçsuzdan kolayca ayırılmasını sağlamak. Ayrıca kullanıcıların internet üzerinden aldatılmalarını ve yasal içerikte olmayan kötü amaçlı içeriklerden korunması amaçlanmaktadır.

İster ücretli, ister ücretsiz birden fazla kullanıcıya bir veya birden fazla internet bağlantısı üzerinden erişim hizmeti sağlayan tüm kurum ve kuruluşları kapsamaktadır. Kanun maddesi kendi içerisinde ikiye ayrılmaktadır ve kapsamları farklılık göstermektedir.

1) İnternet erişimini hizmet amaçlı veya işlerinin devamlılığını sağlamak için çalışan ya da ziyaretçilerine kullandıran kurum ve kuruluşlar.

- Kamu kurumları
- Özel şirketler
- Hastaneler
- Okullar
- Alışveriş merkezleri vb. gibi kurumlar

2) İnternet erişimini kazanç elde etmek amacıyla kullanıcıların hizmetine sunan işletmeler.

- İnternet Cafeler
- Oteller
- Ücretli kullanımın söz konusu olduğu Cafe vb. gibi işletmeler.

Yukarıda yazıldığı gibi hizmet veya kazanç amaçlı kurum ve işletmelerin kullanıcılarına kullandırmakta olduğu internet erişim hizmetinin kanun kapsamı dâhilinde kontrol altına alınması istenmektedir. Erişim sağlayıcısının kanun maddesi ile ilgili genel yükümlülüklerini şöyle sıralayabiliriz;

1. Kullanıcıların yasal içerikte olmayan WEB sayfalarına erişimlerinin engellenmesi.

2. Erişim log ve kayıtlarının tutulması. (Zaman ve Tarih Mührü ile)

3. Networklerine bağlı kullanıcıların iç IP loglarının tutulması.

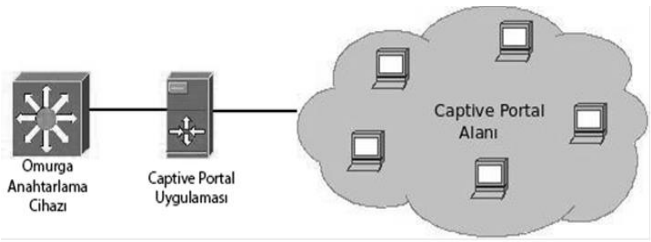
4. Eğer bir Web sayfası mevcut ise ve bu Web sayfasını kendi sunucularında barındırıyor ise dışarıdan gelen erişim log ve kayıtlarının tutulması.

3. Captive Portal

Captive Portal bilhassa aktif ağ cihazlarının IEEE 802.1X desteklemediği alanlarda kimlik doğrulama işleminin gerçekleştirilmesi için kullanılan bir yöntemdir. Açık ve kapalı kaynak kodlu birçok güvenlik duvarı ve hot spot uygulamalarında dünyanın dört bir tarafında kullanılmaktadır.

Kurulumu ve yönetmesi çok kolay olan arayüzler ile 802.1x gibi karışık ve çok vakit harcamamıza neden olan kimlik doğrulama sistemleri yerine pratik kolay kurabileceğimiz ve yönetebileceğimiz sistemler tasarlamamıza yardımcı olmaktadır.

Sistem Omurga Anahtarlama Cihazı ile istemcilerin arasında yönlendirici ve güvenlik duvarı olarak da çalışmakta olan bilgisayara kurulmaktadır. Böylece kullanıcı internete erişmeden hemen önce kimlik denetiminden geçmektedir Şekil 1.



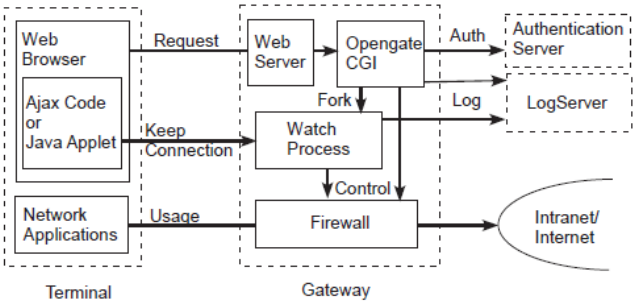
Şekil 1 Captive Portal Çalışma Prensibi

Kimlik denetimi esnasında istemciden kullanıcı adı ve şifre gibi istemciye özel bilgiler alınmaktadır. Bu bilgiler Captive Portal uygulamasında loglama işlemi gerçekleştirilirken istemci etiketi olarak kullanılmaktadır ve sistemde işlenen bilişim suçlarında log dosyalarından gidilerek ilgili istemci anında tespit edilebilmektedir.

4. Opengate

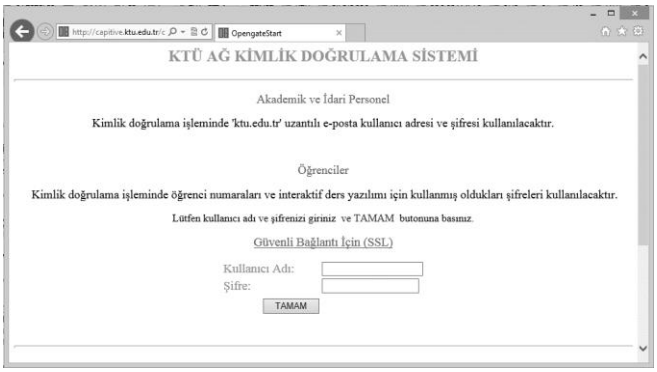
Opengate çok kullanıcılı kuruluşların internet erişiminde istemcilerinin kimlik denetimini sağlamak ve kullanım loglarını kayıt altında tutabilmek için kullanmakta olduğu açık kaynak kodlu bir Captive Portal yazılımıdır. [2]

Opengatein çalışma prensibi Şekil 2 deki gibidir.[3] Bu prensibe göre kullanıcı herhangi bir web sayfasını görüntülediğinde güvenlik duvarı web sayfası görüntüleme istek paketlerini yerel web sunucusuna yönlendirir. Yerel web sunucusu bu istek paketlerine karşılık istemciye kimlik doğrulama sayfasını gönderir Şekil 3. Kullanıcı bu sayfadan kullanıcı adı ve şifre ile giriş yaparak bu bilgileri tekrar yerel web sunucusuna gönderir. Yerel sunucudaki CGI programı kullanıcı bilgilerini kontrol eder ve eğer bilgiler geçerli ise kullanıcının erişebileceği port bilgilerini güvenlik duvarına tanımlar ve istemcinin istekleri bu işlemlerden sonra gerçek adresine yönlendirilmeye başlar.



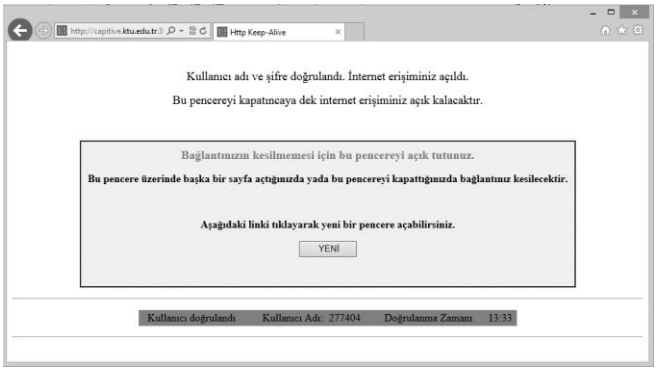
Şekil 2 Opengate yazılımı blog diyagramı

Şekil 3 deki kullanıcı denetimi sayfası üzerinden bilgiler doğrulandıktan sonra kullanıcı faaliyetleri Watch Process üzerinden takip edilir.



Şekil 3 Opengate kullanıcı denetimi sayfası

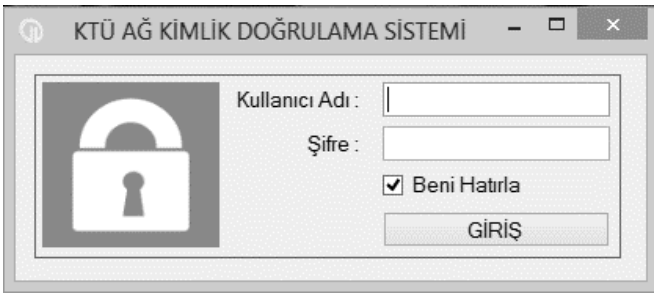
Kullanıcı bilgilerinin doğrulandığını Şekil 4 deki sayfadan görüntüleyebilmektedir. Web sayfası açık kaldığı sürece Watch Process bir Java-Applet ya da Ajax kodu ile canlı tutulmaktadır.[4] Web sayfası kapatıldığında kullanıcı için oluşturulan Watch Process anında sonlandırılmaktadır. Kullanıcı için oluşturulmuş log bilgileri elle silinmedikçe sistemde tutulmaktadır ve gerektiğinde kötü kullanım tespiti için kullanılabilmektedir.



Şekil 4 Opengate kimlik doğrulaması yapılmış web sayfası

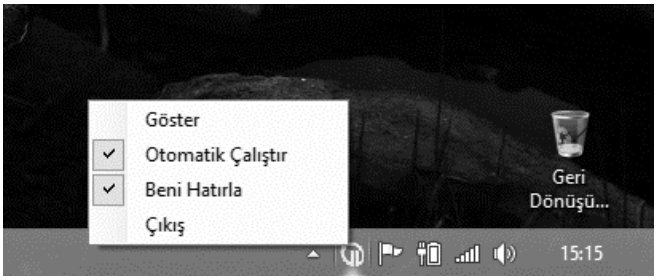
6. Uygulama

Geliştirilen uygulama istemci bilgisayarında çalışmaktadır ve istemciden sisteme giriş bilgilerini bir kereye mahsus uygulamaya girmesi istenmektedir Şekil 5. Bilgiler alındıktan sonra bu bilgiler program veri tabanında şifrelenerek saklanmaktadır.



Şekil 5 Geliştirilen uygulama kullanıcı bilgileri alma ekranı

İstemci sisteme giriş işlemini gerçekleştirdiğinde uygulama web tarayıcının gerçekleştirdiği işlemleri gerçekleştirmektedir ve kullanıcı isterse uygulamayı sistem tepsisine küçültebilmektedir Şekil 6.



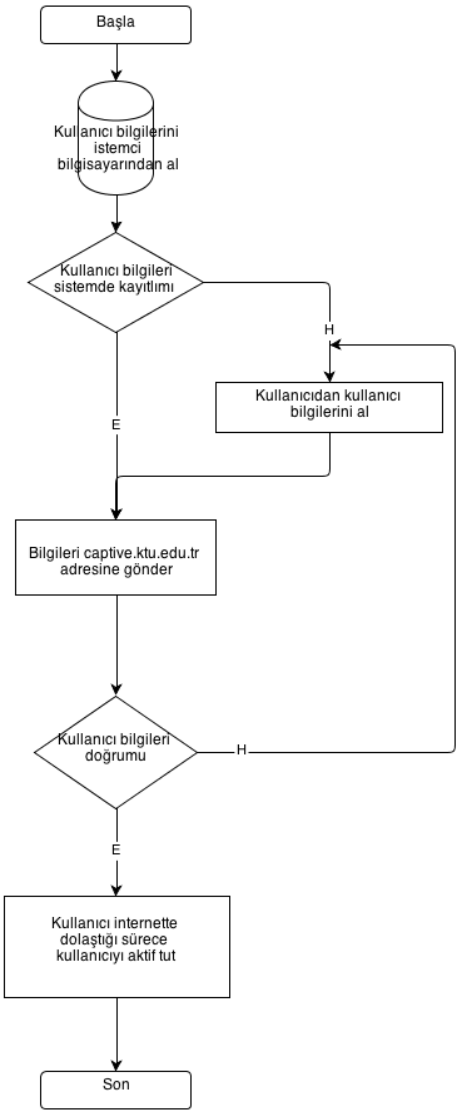
Şekil 6 Uygulamanın sistem tepsisinde gösterimi

Uygulama sistem başlangıcında çalışabilme yeteneğine sahiptir ve kullanıcı isterse bilgisayarını açtığı anda uygulamanın sistemle birlikte otomatik çalıştırılmasını zamanlayabilmektedir.

Geliştirilen program da kullanıcı girişi yapıldıktan sonra kullanıcıya ne zaman sistem tarafından kimlik doğrulaması işleminden geçtiğine dair bilgi gösterilmektedir Şekil 7. Ayrıca kullanıcı istediği anda sisteme kayıtlı bilgilerini silebildiği gibi uygulamadan da çıkış yaparak internet erişimini sonlandırma işlemini gerçekleştirebilmektedir.

Şekil 7 Kullanıcı girişi yapılmış uygulama ekranı

Geliştirilen uygulamanın akış diyagramı Şekil 8 de gösterilmiştir.



Şekil 8 Uygulamanın akış diyagramı

7. Sonuç

Bu çalışmada popüler kullanıcı kimlik denetimi yöntemlerinden biri olan Captive Portalın avantajlarından bahsedilmiştir ve aynı mantıkla çalışan Opengate adlı uygulamayı daha kullanıcı dostu bir uygulama haline getirmeye çalışılmıştır. Çalışma kapsamında geliştirilen yazılım Captive Portal Opengate uygulamasına ek uygulama olarak çalışmaktadır ve kullanıcıyı sürekli doğrulama web sayfasını açık tutma yükünden kurtarmak hedeflenmiştir. Uygulama sayesinde kullanıcıya sürekli kimlik denetimi bilgilerini girdirme işleminin de önüne geçilerek Opengate uygulamasının eksik yönlerinin giderilmesi sağlanmıştır.

8. Kaynaklar

[1] İnternet: İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun, http://www.tbmm.gov.tr/kanunlar/k5651.html

[2] Yoshiaki Watanabe, Opengate Home Page, http://www.cc.saga-u.ac.jp/opengate/index-e.html

[3] Yoshiaki Watanabe, Kenzi Watanabe, Hirofumi Eto and Shinichi Tadaki, An User Authentication Gateway System With Simple User Interface, Low Administration Cost And Wide Applicability, IPSJ Journal, Vol. 42, No. 12, pp. 2802 - 2809 (2001.12)

[4] Makoto Otani, Hirofumi Eto, Kenzi Watanabe, Shin-ichi Tadaki and Yoshiaki Watanabe, Development of the Network User Authentication System Supporting Single Sign-On, IPSJ Journal, Vol. 50, No. 3, pp. 1031 - 1039 (2010.3)