

## İnternet’de Saldırı Tespiti Teknolojileri

Burak DAYIOĞLU ve Attila ÖZGİT  
{dayioglu,ozgit}@metu.edu.tr

### 1. Bilgi Güvenliği Durum Tespiti

Modern iletişim teknolojileri kullanıcılara yepyeni hizmetlerin sunulmasını mümkün kılmaktadır. Ağ üzerinden sunulan hizmetlerin sayısı ve çeşitliliği günden güne baş döndürücü bir hızla artmaktadır. Bu alandaki çalışmalar ile ağ üzerinden her türlü hizmetin herhangi bir anda ve herhangi bir yerdeki kullanıcılara ulaştırılabilmesi hedeflenmektedir. Ağ üzerinden sunulan hizmetlerdeki yüksek çeşitlilik beraberinde çeşitli düzeylerde karmaşıklık getirmektedir.

Artan bir biçimde, ağ teknolojileri ve üst katmanında dağıtık sistemler teknolojileri günlük yaşamın her alanında kendini göstermektedir; sağlık kayıtları, banka hesapları vb. dağıtık sistemler ile işlenmektedir. Kritik sayılabilecek bilgilerin dağıtık sistemler aracılığı ile idare ediliyor olması, bu sistemlerin bulunurluğunu (ing. *availability*), doğruluğunu ve eksiksizliğini son derece önemli kılmaktadır.

Dağıtık sistemlerin karmaşıklığı arttıkça bu sistemlerin doğruluğunu ve eksiksizliğini denetlemek ve sistemlerin kesintisiz işlerliğini sağlamak daha da güçleşmektedir. Sistemler ve bu sistemler tarafından işlenen bilgilerin güvenliği de göz önünde bulundurulduğunda, karmaşıklığın daha da artması kaçınılmazdır.

Doğruluğun ve eksiksizliğinin denetiminin son derece güç olduğu durumlarda bilgi güvenliğinin her üç temel eksenine (gizlilik, bütünlük ve bulunurluk) ilişkin gereksinimlerin eksiksiz biçimde karşılanamaması durumunda kurumları ciddi tehlikeler beklemektedir.

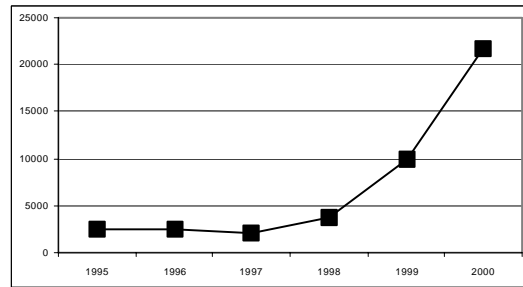
İnternet’in geçtiğimiz otuz yıl içerisindeki gelişim macerası, dağıtık sistemler için yepyeni ufukların ortaya çıkmasına neden olmuştur. Başlangıcında yalnızca akademik amaçlı bir araştırma ağı olan İnternet, bugün gelinen noktada önemli toplumsal dönüşümlere altyapı

sağlar duruma gelmiştir. Ancak ilk yıllarda lüzumsuz ya da önemsiz olarak nitelendirilebilen güvenlik konusu, İnternet’e bağlı kurum sayısı arttıkça ciddi bir problem haline gelmiştir. İnternet’in temelini oluşturan protokollerin büyük bölümünün güvenliğe pek az önem verilerek tasarlanmış olması (örn. SMTP) bu yaklaşımı doğrular niteliktedir.

İnternet’in ilk yıllarından itibaren önemsiz sayılan güvenlik konusu, özellikle 1988 yılındaki Morris Kurdu (ing. *worm*) faciası [Spafford1988][Spafford1989][Eichin1989] ile dikkatleri üzerine çekmiştir. Kurt, başarılı bir biçimde binlerce bilgisayara sızmayı başarmış ve bu bilgisayar sistemlerini çalışamaz hale getirmiştir.

Morris Kurdu ile yaşanan dönüşüm sonrasında bilgi güvenliği konusunda doğrudan askeri amaçlı olmayan çalışmalar hız kazanmış, 1990’lı yılların başlarında ilk güvenlik duvarı uygulamaları ile [Mogul1989][Cheswick1990] [Corbridge1991][Avolio1994] bir takım teknik güvenlik önlemlerin alınması konusunda referans çalışmalar başlamıştır.

Bilgi güvenliği konusunda endüstrinin bu günkü durumu hiç de iç açıcı görünmemektedir. CERT/CC’nin istatistiklerine göre [CERT2001], 1997 ve 2000 yılları arasında rapor edilen güvenlik ihlallerinin yıllara göre sayısı geometrik olarak artmaktadır:



Bilişim suçları ile savaşılabilmek, sistemlerin ve bilgilerin güvenliğini sağlamak için sistematik çalışmaların gerekmektedir. Kurumsal güvenlik düzeyini arttırmak için yapılması gereken çalışmalar üç temel alanda toplanır. Bu alanlar sırası ile

- Güvenlik Politikaları ve Prosedürler
- Teknoloji
- Eğitim ve Bilgilendirme'dir.

Her üç alanda da çalışmaların yapılması zorunludur; bir alanda eksik bırakılacak çalışmalar diğer alanlarda yapılan çalışmaların etkisini ciddi biçimde azaltacaktır.

Güvenlik politikalarının ve buna bağlı olarak prosedürlerin oluşturulması kurumun birinci önceliği olmalıdır. Güvenlik ile ilgili kurum politikası bu konuda (ya da bu konuya etki edebilecek) her türlü çalışma için esas teşkil edecektir. Güvenlik politikalarının hazırlanmasına ilişkin önemli bir kaynak [Wood1997]'dir.

Teknoloji, kurumun güvenlik politikalarının yaptırımının sağlanması ve/veya politika ihlallerinin tespit edilmesi için kullanılacak bir araçtır, tek başına güvenlik problemlerinin tümüne bir çözüm teşkil etmez. Şifreleme ve uygulamaları, güvenlik duvarları, gelişmiş tanımlama ve yetkilendirme mekanizmaları gibi muhtelif teknolojik çözümler, kurumların belirledikleri güvenlik politikalarının yaptırımının sağlanması noktasında bir araç teşkil ederler.

## 2. Saldırı Tespiti

Politikanın yaptırımının sağlanması kadar, ihlallerinin tespiti de önem arz etmektedir. İhlallerin tespit edilebilmesi için monitorizasyon işlevini yerine getiren teknolojilerden faydalanılır. Saldırı tespiti (ing. *intrusion detection - ID*), "Sistemleri yetkisiz kullanma ya da yetkilerini aşan işlemleri yapma girişiminde bulunan kişileri (ya da programları) tespit etme çalışması" olarak tanımlanmaktadır [Mukherjee1994].

Saldırı tespitinin gerekliliği Denning tarafından aşağıdaki maddelerle verilmektedir [Denning1986]:

- Mevcut sistemlerin bir çoğunda saldırıya, sızmaya ve muhtelif diğer biçimlerde zarar verilmesine imkan verecek zaafklar bulunmaktadır; tüm bu zaafkların bulunması ve düzeltilmesi teknik ve/veya ekonomik nedenler ile mümkün olamamaktadır.
- Bilindik zaafkları olan mevcut sistemler, daha yüksek güvenlik sağlayan alternatifleri ile değiştirilememektedir. Bunun ana nedeni ya mevcut sistemlerde var olan bazı özelliklerin daha yüksek güvenlik sağlayan alternatiflerinde var olmaması ya da ekonomik nedenlerle değiştirilememesidir.
- Mutlak güvenliğe sahip sistemlerin geliştirilmesi imkansız değilse bile son derece güçtür ve
- En yüksek güvenlik düzeyine sahip sistemler bile yetkilerini kötüye kullanan kullanıcılarının zarar verebilmesine imkan verir durumdadır.

Saldırı tespit sistemlerinin kullanımı üç temel başlık altında özetlenebilecek faydalar sağlamaktadır:

- Erken tespit: Saldırı tespit sistemleri, başlayan bir ihlali sorumlu sistem yöneticilerinden çok önce tespit edebilir. Bu özellik sayesinde olay ile ilintili olarak sistem sorumlusunu SMS, e-posta, telefon ya da çağrı cihazı gibi farklı biçimlerde anında uyarabilir ve ihlalin etkisinin en kısa sürede minimize edilmesini sağlayarak riskin sınırlanmasına destek olabilir.
- Detaylı bilgi toplanması: Saldırı tespit sistemlerinin kullanılması sayesinde, sistem yöneticileri sürmekte olan ya da geçmişte gerçekleşmiş saldırılara ilişkin detaylı bilgi edinebilirler. Bu bilgiler saldırıların kaynağı, çapı ve hedefler üzerindeki etkilerinin incelenmesi noktasında son derece değerlidir.
- Toplanan bilgilerin kanıt niteliği: Sistem tarafından toplanan bilgiler,

hukuki yollara başvurulduğunda kanıt teşkil edebileceği gibi, bir diğer kurumdan kaynaklanan bir ihlalde, ilgili kurumun yetkilileri ile temasa geçildiğinde de görüşmeler için zemin teşkil edebilir.

Saldırı tespiti alanında bu güne değin yapılan çalışmalar iki temel kategoride incelenebilir; anormallik tespiti (ing. *anomaly detection*) ve kötüye kullanım tespiti (ing. *misuse detection*).

Kötüye kullanım tespitinde, önceden bilinen politika ihlali olasılıkları (ya da yöntemleri) önce senaryolara dönüştürülür. Senaryolar daha sonra saldırı imzalarına (ing. *attack signature*) indirgenir. Saldırı imzaları, belirli bir saldırıya ilişkin olası tüm senaryoların ana eksenini oluşturan bir özet olarak nitelendirilebilirler. Saldırı imzalarının oluşturulmasından sonra bu imzalar, sistemin anlayacağı makinaca okunabilir biçime dönüştürülür. Makinaca okunabilir biçim, bu güne kadarki uygulamaların büyük bir bölümünde kural temelli bir dil olarak seçilmiştir [Kumar1995] [İlgin1995][Porras1997]. Sistemin kaynak girdisi (ağ trafiği, sistemlere ilişkin günlük kayıtları vb.) üzerinde yapılan analizler ile bilinen zaafılara yönelik saldırıların ya da ihlallerin gerçekleşip gerçekleşmediği tespit edilmeye çalışılır; tespit edilmesi durumunda alarm üretilir.

Anormallik tespitinde ise, kaynakların (kullanıcılar, programlar, sistemler vb.) normal durum davranışı istatistiksel yöntemler ile tespit edilir ve profil olarak adlandırılan özet bilgiler oluşturulur. Kaynakların davranışındaki tüm değişimler düzenli olarak değerlendirilerek ilgili profilin de güncellenmesi sağlanır. Kaynağında davranışında istatistiksel olarak ani bir değişim görüldüğünde bir “anormallik” olduğu öne sürülerek alarm üretilir.

Saldırı tespiti ile ilgili çalışmaların ilk yıllarında, günün şartlarında karmaşık sayılan saldırıların nasıl yapıldığına ilişkin bilgilerin araştırmacıların elinde olmaması nedeni ile kötüye kullanım tespiti modeli gelişme gösterememiştir. İstatistiksel anormalliklerin tanımlanması yöntemi, daha az konu uzmanı bilgisi gerektirmesi nedeni ile tercih edilmiştir. Ancak İnternet üzerindeki bilgi güvenliği ile

ilgili forumların ve tartışma listelerinin hızla artması, bu ortamlarda saldırı tekniklerine ilişkin derin teknik tartışmaların yapılabilmesi kötüye kullanım tespiti modelinin uygulanabilirliğini son yıllarda ciddi biçimde arttırmıştır. Endüstride yoğun biçimde kullanılan tüm ürünler ağırlıklı olarak bu modelde işlemektedirler.

Saldırı tespit sistemlerine ilişkin bir diğer sınıflama, sistemin girdisine göre yapılan sınıflamadır. Sunucu temelli (ing. *host based*) sistemlerde, sistemin girdisi sistem günlükleri (örn. UNIX syslog'u) ve uygulama kayıtları (örn. web sunucu erişim kayıtları) gibi doğrudan sistem üzerinden temin edilebilen bilgilerin toplamıdır. Sistem üzerinden toplanabilecek bilgiler kümesinin olabildiğince geniş olması, bu modelde bir uygulamanın gerçekleştirilebilmesi için önemli bir gereksinimdir; muhtelif sistemlerin sağladığı olanaklar ve yeterlilikleri [Price1997]'de tartışılmaktadır.

Ağ temelli sistemlerde, ağ üzerinden akan trafik sistemin girdisidir. Bu modelde çalışan bir sistemin birden fazla sisteme ilişkin trafiği izlemesi hedeflenmektedir. Ağ temelli sistemler, trafik akışını tümüyle uç sistemlerin algıladığı biçimde yorumlama durumundadır, aksi durumda muhtelif biçimlerde sistemin bertaraf edilmesi mümkün olabilmektedir [Ptacek1998].

Ağ temelli sistemler, daha az çabayla daha yüksek sayıda kaynağın davranışının izlenebilmesine ve politika ihlallerinin tespit edilebilmesine imkan verdiği için tercih edilmektedir. Ancak bu sistemlerin trafiği uç sistemlerin algıladığı biçimde yorumlama konusundaki zaafıları kullanılabilirliklerini ciddi biçimde etkilemektedirler. Keza, ağ temelli sistemlerin şifreleme teknolojilerinden faydalanan uygulamalar için, trafiği inceleyemiyor olmak gerekçesi ile, çalışamaz duruma gelmesi önemli bir zaafıdır.

### 3. ODTÜ'de Süren Çalışmalar

ODTÜ Bilgisayar Mühendisliği bünyesinde yazarlar tarafından sürdürülen çalışmalar ağ temelli saldırı tespit sistemlerinin etkinliğini arttırmaya odaklanmıştır. Yapılan çalışmalar iki

temel ekseninde toplanmaktadır; TCP akış birleştirmesinin (ing. *TCP Stream Reassembly*) daha yüksek başarımla gerçekleştirilmesi ve yanlış alarm (ing. *false positive*) sayısının azaltılması.

TCP bağlantıları üzerinden gerçekleştirilen iletişimlerde saldırı tespitinin başarılı bir biçimde yapılabilmesi için, kullanılan saldırı tespiti modelinden bağımsız olarak, iletişime esas TCP paketlerinin hedef sistem tarafından kabul edilip edilmediğinin ve kabul edildiler ise nasıl algılandığının tespit edilebilmesi gerekmektedir.

Bu bağlamda, hedef sistemin çakışan paket parçalarını (ing. *overlapping fragments*) nasıl birleştirdiği (önce gelen parça korunur ya da sonra gelen parça üzerine yazılır), paketi kabul edilir bulup bulmadığı (paket sağlaması (ing. *checksum*) denetimi vb.), paketin gerçekten hedef sisteme kadar ulaşıp ulaşmadığı (IP TTL denetimi vb.) gibi konular dikkatle incelenmeli ve TCP bağlantılarının takibi bu bilgilerin ışığında yapılmalıdır. Aksi durumda bir saldırganın, saldırı tespit sistemine görünmeden saldırılar gerçekleştirilmesi mümkün olacaktır.

TCP akışlarının doğru birleştirilebilmesi için paketlerin hedefi durumunda olan sistemin işletim sisteminin ve bu işletim sisteminin içerisinde yer alan IP yığınının (ing. *IP stack*) davranışının önceden bilinmesi gerekmektedir. Bu bilgilerin her ikisine de sahip olmadan çakışan paket parçalarının hedef sistem tarafından gerçekleştirildiği biçimde birleştirilmesi mümkün olamayacaktır. Hangi işletim sisteminin ne biçimde çakışan parça birleştirdiğine ilişkin kısıtlı bir liste [Ptacek1998]'de yer almaktadır.

Saldırı tespit sistemi tarafından korunan bilgisayar sistemlerinin hangisinin hangi işletim sistemini çalıştırdığı bilgisi, doğal olarak, kuruluştan kuruluşa farklılık gösterecektir. Bu durumda, bilgisayar sistemi ve işletim sistemlerini gösteren bir tablonun ya çalışma öncesinde sisteme sağlanması ya da dinamik olarak bu bilginin sistem tarafından öğrenilmesi gerekmektedir.

Çalışma öncesinde bilgi sağlanması yöntemi basit görünse de, değişen kurum koşullarına

otomatik olarak adapte olamaması ve insan faktörü nedeni ile hatalara ihtimal vermesi nedeniyle tercih edilmemelidir.

Dinamik olarak bu bilginin toplanması iki farklı yöntem ile gerçekleştirilebilir; bunlardan birisi düzenli olarak ağı taramak (ing. *scanning*) ve işletim sistemlerini tespit etmek, diğeri ise yalnızca akan paketleri inceleyerek aynı bilgiye ulaşmaya çalışmaktır. İlk yöntem, aktif ağ haritalaması (ing. *active network mapping*), ikinci yöntem ise pasif ağ haritalaması (ing. *passive network mapping*) olarak bilinir.

Aktif haritalama yöntemi saldırı tespit sisteminin iki yönlü bir iletişime geçmesini zorunlu kılmakta, bu ise sistemin yalnızca izleme görevini üstlenmiş olması ile çelişmektedir. ODTÜ'de süregelen çalışmalarda, pasif ağ haritalamasının saldırı tespit sistemlerindeki kullanım alanları araştırılmaktadır.

Gelinen noktada, pasif ağ haritalaması yöntemi ile işletim sistemi tespiti başarılı bir biçimde Snort saldırı tespit sistemine [Roesch1999] entegre edilmiştir. Asimetrik yönlendirme (ing. *asymmetric routing*) yapılmayan ağlarda hedef sistemler ile saldırı tespiti sistemi arasındaki uzaklığın ölçümü (hop cinsinden) çalışmaları da son aşamasına gelmiştir.

Toplanan bilgiler ile akışların doğru birleştirilmesi ve TTL değiştirilerek yapılan aldatmacaların önlenmesi konularında uygulama geliştirme çalışması da son aşamasına gelmiştir.

Yapılan çalışmaların ikinci ekseninde yer alan yanlış alarmların azaltılması konusunda da yine pasif ağ haritalaması teknolojisinden faydalanılmaktadır. Snort kurallarına her bir saldırı kuralı için "saldırıdan etkilenen işletim sistemi" alanı eklenmiş ve mevcut tüm Snort kurallarına etkilenen işletim sistemlerinin eksiksiz bir biçimde eklenmesi, ArachNIDS [ArachNIDS2001] veritabanının yöneticisi Max Butler'ın da desteği ile sağlanmıştır.

Snort kurallarının bu biçimde daha spesifik hale getirilmesi sonucunda sistemin ürettiği alarm sayısında %10 dolayında bir düşme kayıt edilmiştir ve detaylı ölçüm çalışmaları halen sürdürülmektedir.

### 3. Sonuç

ODTÜ Bilgisayar Mühendisliği Bölümü bünyesinde süren çalışmalar ile ağ temelli saldırı tespit sistemlerinin temelini oluşturan akış birleştirme modelinin geliştirilmesi hedeflenmiş ve bu amaçla pasif ağ haritalaması tekniğinin bir uygulaması gerçekleştirilmiştir.

Saldırı tespit sistemlerinin yaygınlığı için en önemli gereksinimlerden birisi olan sifıra yakın alarm düzeyine ulaşabilmek için yine pasif ağ haritalaması tekniğinin bir uygulaması gerçekleştirilmiş ve belirgin bir başarımlı artışı sağlandığı gözlenmiştir.

### Referanslar

[ArachNIDS2001] ArachNIDS Açık Saldırı Tespit Kural Veritabanı, <http://www.whitehats.com> adresinden erişilebilir

[Avolio1994] F. Avolio ve M. Ranum, A Network Perimeter With Secure External Access, Proceedings of the Internet Society Symposium on Network and Distributed Systems Security, 1994

[CERT2001] CERT/CC Web Sitesi, <http://www.cert.org> adresinden erişilebilir

[Cheswick1990] B. Cheswick, The Design of a Secure Internet Gateway, Proceedings of the USENIX Anaheim Conference, 1990

[Corbridge1991] B. Corbridge ve diğerleri, Packet Filtering in an IP Router, Proceedings of the 5th LISA Conference of USENIX Association, 1991

[Denning1986] D. Denning, An Intrusion Detection Model, Proceedings of the IEEE Security and Privacy Conference, 1986

[Eichin1989] M. Eichin ve J.A. Rochlis, With Microscope and Tweezers: An Analysis of the Internet Virus of November 1998, Proceedings of the 1989 IEEE Symposium on Research in Security and Privacy, 1989

[Ilgun1995] K. Ilgun ve diğerleri, State Transition Analysis: A Rule Based Intrusion Detection Approach, IEEE Transaction on Software Engineering, Vol. 21, No. 3, 1995

[Kumar1995] S. Kumar ve G. Spafford, A Software Architecture to support Misuse

Intrusion Detection, Technical Report 95-009, Department of Computer Sciences, Purdue University, 1995

[Mogul1989] J. Mogul, Simple and Flexible Datagram Access Controls for UNIX-based Gateways, Proceedings of the 1989 Summer Conference of the USENIX Association, 1989

[Mukherjee1994] B. Mukherjee ve diğerleri, Network Intrusion Detection, IEEE Network, Vol. 8, No. 3, 1994

[Porras1997] P. Porras and P. Neumann, EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances, Proceedings of the National Information Systems Security Conference, 1997

[Price1997] K. Price, Host Based Misuse Detection and Conventional Operating Systems' Audit Data Collection, M.Sc. Thesis Dissertation, Department of Computer Sciences, Purdue University, 1997

[Ptacek1998] T. Ptacek and T. Newsham, Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection, Technical Report, Secure Networks Inc., 1998

[Roesch1999] M. Roesch, Snort - Lightweight Intrusion Detection for Networks, Proceedings of the 13th LISA Conference of USENIX Association, 1999

[Spafford1988] E. Spafford, The Internet Worm Program: An Analysis, Purdue Technical Report CSD-TR-823, 1988

[Spafford1989] E. Spafford, The Internet Worm Incident, Proceedings of the 1989 European Software Engineering Conference, 1989

[Wood1997] C. Cresson-Wood, Information Security Policies Made Easy: A Comprehensive Set of Information Security Policies, Baseline Software, 1997