Necmettin Erbakan Üniversitesi

Bilgi Güvenliği
2022-2023 Güz Dönemi

Dr. Alperen Eroğlu
aeroglu@erbakan.edu.tr

Hafta-12

Siber Güvenlik Teknolojileri ve Sızma Testleri

https://fordefence.com/

Hafta-12

- Yenilikçi siber güvenlik teknoloji çözümleri
- Anti-virüs,
- Anti-casus,
- Anti-spam filtreler,
- IDS/IPS,
- Güvenlik duvarları ve
- Hibrit sistemler,
- Şifreleme teknolojileri,
- Açık anahtar altyapısı,
- Erişim kontrol teknolojileri

Hafta-12

Anti-virüs Yazılımları

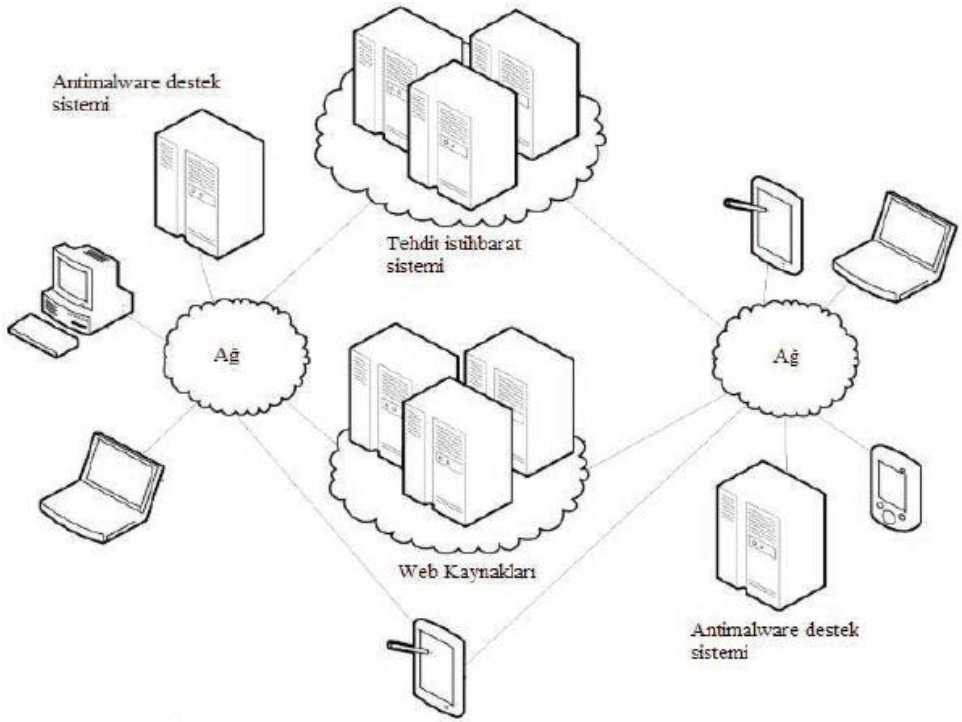
- Anti-virüs yazılımları, çalıştırıldığında diğer bilgisayar yazılımlarını değiştirip, kendi kodunu ekleyerek kendisini çoğaltan virüslere karşı güvenlik önlemi sağlamaktadır.
- Anti-virüs, imza tabanlı ve davranış tabanlı algılama ile zararlı yazılımlara karşı koruma sağlamaktadır.
- İmza tabanlı algılamada, dosya tarama ve virüs imzalarını eşleştirme ile analiz yapılmaktadır. Böylece zararlı yazılım karantina altına alınmakta veya silinmektedir.
- Davranış tabanlı algılamada ise zararlı yazılımın bellek, ağ veya dosya sistemine zarar verebileceği dosya yükleme, bağlantı açma, sistem kaydı (registery) değiştirme, dosya oluşturma/değiştirme davranışı ile tehdit algılanmaktadır. Daha sonra ise belirlenen istenmeyen program davranışı engellenmektedir

Hafta-12

Anti-casus Yazılımlar

- Anti-casus yazılımları ise kötü amaçlı yazılımlar, truva atları, solucanlar gibi zararlı yazılımların engellenmesi, tespit edilmesi ve kaldırılması için tasarlanmış ve kullanılan yazılımlardır..

- Anti-virüs ile anti-casus arasındaki temel fark, anti-virüslerin internet veya harici bellek gibi bilinen kaynaklardan gelen güncel ve/veya belirlenmiş tehditlere karşı, anti-casus yazılımların ise daha önce karşılaşılmamış kaynaklardan gelen zararlı olduğu kesin belirlenemeyen veya karar verilemeyen yazılımlara karşı koruma sağlamasıdır



Anti-casus sistem mimarisi

Hafta-12

Mesaj Sağanağı (Anti-spam) Filtreleri

- E-posta mesaj sağanağı ve benzeri bilgilerin engellenmesi amacıyla anti-spam filtreler sıklıkla kullanılmaktadır.
- Söz konusu filtreler, mesaj sağanağını tanımlayıp, genel özelliklerini belirlemekte ve tanıma göre de filtreleme yapmaktadır. Bu süreçteki en önemli sorun, yaygın olarak kullanılmakta olan basit e-posta aktarım protokolünün (SMTP), mesaj kaynağı kimliğini kontrol etmede güvenilir bir mekanizma sağlamamasıdır. Bu sorunu çözmek için gönderen kimliğinin tanımlanması amacıyla SPF (Sender Policy Framework), DMP (Designated Mailers Protocol), TEOS (Trusted E-Mail Open Standard) ve benzeri yazılım ve protokoller geliştirilmiştir.

Hafta-12

Mesaj Sağanağı (Anti-spam) Filtreleri

- Çeşitli spam filtreleme algoritmaları, e-posta iletimi aşamalarında uygulanmaktadır. Söz konusu aşamalar, yönlendirici, gidilecek e-posta sunucusu, gidilecek e-posta kutusudur.
- Birçok spam filtreleme yöntemi, yapay zekâ tabanlı öğrenmeye dayalı sınıflandırma tekniklerini kullanmaktadır. Söz konusu yöntemlerde e-posta mesajlarının büyüklüğü, içeriği, başlığı öznitelik olarak kabul edilip, elde edilen veriler işlenerek sınıflandırma gerçekleştirilmektedir.
- Resim tabanlı filtrelemede ise OCR ve benzeri öz nitelik çıkarma teknikleri ile elde edilen veriler kullanılmaktadır. Bu alanda literatürde en çok kullanılan yöntemler naive bayes, destek vektör makineleri ve kNN olduğu görülmüştür. Söz konusu bilinen algoritmalar dışında, anti-spam filtrelemeye özel yeni algoritmalar da geliştirilmektedir.

Hafta-12

Saldırı Tespit ve Önleme Sistemleri (IDS/IPS)

Modern IDS'nin gelişmesinden önce, izinsiz giriş tespiti, anormal durumların log ve benzeri kayıt dosyaları üzerinde incelenmesinden oluşmaktaydı günümüzde yeni araştırmalar ile saldırılar tespit edilebildiği gibi saldırı olmadan olası örüntülerde belirlenebilmektedir.

Literatürdeki IDS çalışmaları, anormal durumların istatistiksel, bilgi ve makine öğrenmesi tabanlı analiz edilmesi üzerine odaklanmıştır.

İstatistik tabanlı anormal durum analizinde, normal aktivite hakkında önceden bilgi gerekli olmayıp, kötü amaçlı faaliyetlerin doğru bildirimi ile tek değişkenli, çok değişkenli ve zaman serisi model ile analiz gerçekleştirilmektedir.

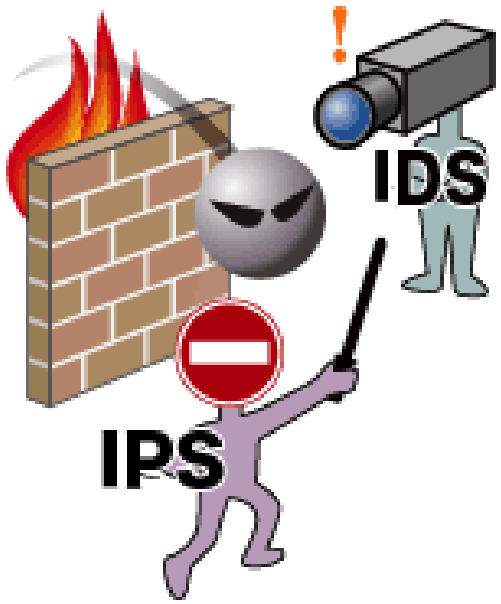
Bilgi tabanlı anormal durum analizinde, yüksek öneme sahip bilgiler açıklama dilleri, uzman sistemler ve sonlu durum makineleri ile değerlendirme yapılmaktadır.

Makine öğrenmesi tabanlı anormal durum analizinde ise yüksek kaynak tüketimi ile bayes ağları, markov modelleri, nöral ağlar, bulanık mantık, genetik algoritma ve kümeleme teknikleri kullanılarak örüntünün sınıflandırılması yapılmaktadır.

Hafta-12

Saldırı Tespit ve Önleme Sistemleri (IDS/IPS)

Makine öğrenmesi tabanlı anormal durum analizinde ise yüksek kaynak tüketimi ile bayes ağları, markov modelleri, nöral ağlar, bulanık mantık, genetik algoritma ve kümeleme teknikleri kullanılarak örüntünün sınıflandırılması yapılmaktadır.



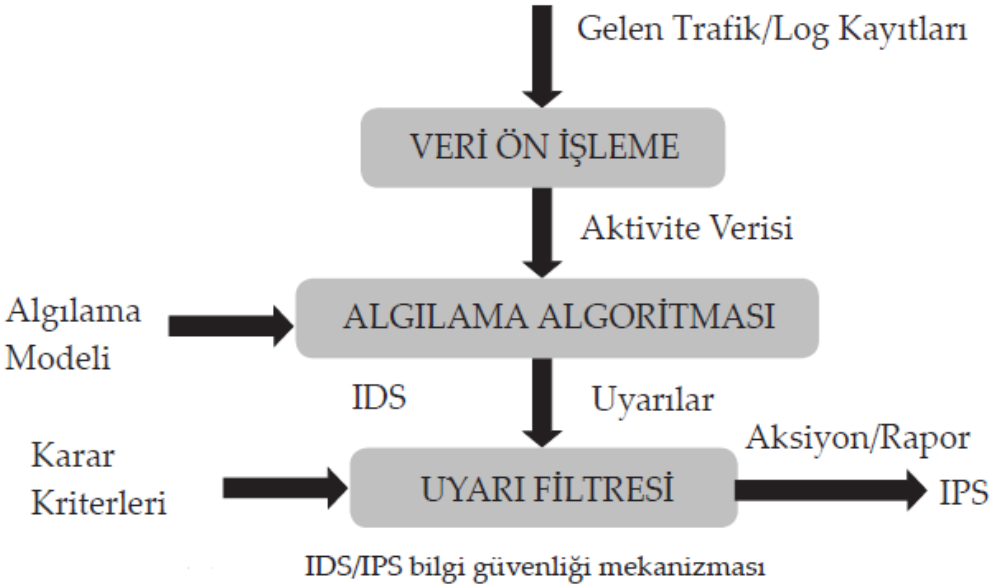
https://aavextechnology.com/2019/09/ids-ips-or-both/

İnceleme Önerisi:
https://ipwithease.com/firewall-vs-ips-vs-ids/
https://medium.com/trendyol-tech/ips-ids-nedir-79a4b4beb966
https://berqnet.com/blog/ips-ve-ids-nedir

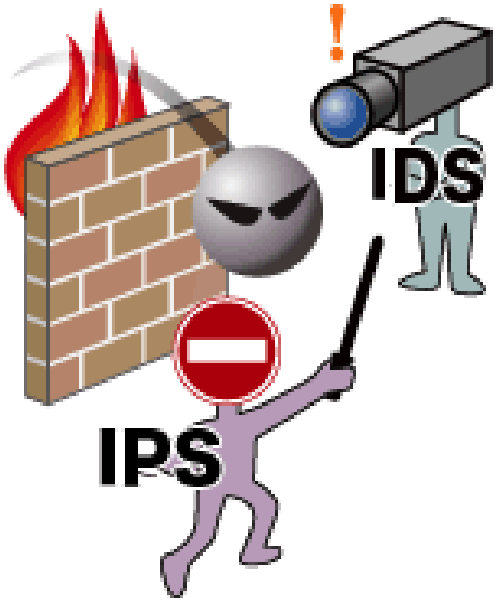
Hafta-12

Saldırı Tespit ve Önleme Sistemleri (IDS/IPS)

Son yıllarda DDoS ve diğer saldırıların artması sonucunda IDS'in yanı sıra bu saldırıları engelleyecek IPS cihazlarına yoğun ihtiyaç Şekil'de verilen ve son yıllarda bilgi güvenliği için IDS ve IPS sistemleri beraber kullanılmaktadır. Öncelikle IDS'lerde bulunan algılama algoritmaları ile tehditler algılanmakta daha sonra çeşitli uyarı filtrelerinin bulunduğu IPS'ler ile tehditler raporlanmakta ve/veya tehditlere karşı çeşitli aksiyonlar oluşturulmaktadır



IDS/IPS bilgi güvenliği mekanizması



https://aavextechnology.com/2019/09/ids-ips-or-both/

Hafta-12

Güvenlik Duvarları ve Hibrit Sistemler

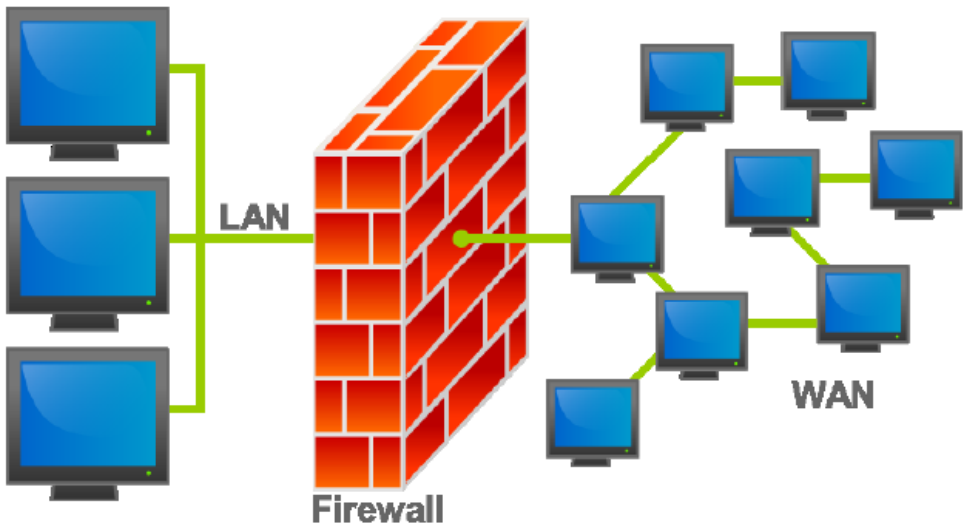
Güvenlik duvarları, iki ağ arasında ilk güvenliği sağlayan ortak bir güvenlik savunma cihazıdır.
Statik paket filtreleme özelliğine sahip güvenlik duvarları, ana bilgisayar/hedef adres veya bağlantı noktası numaraları gibi başlık alanları bilgisine göre gelen ilgili paketlere izin vermekte veya ret etmektedir. Bu cihazlar, pakette kötü amaçlı kod algılama yapamamakta ve her bir paketi ayrı
bir bilgi olarak değerlendirilmektedir.
Fakat paket filtrelemeli güvenlik duvarları, temel durum denetimine sahiptir. Bu cihazın kullanıldığı altyapılarda istemci sunucudan bilgiyi talep etmekte ve bu talebe karşı sunucudan cevap almaktadır. Söz konusu cihaz, durum koruması amacıyla durum tablolarını bellekte tutmaktadır.

Okuma Önerisi:
https://www.ktu.edu.tr/dosyalar/bilgisayar_a93f2.pdf

Hafta-12

Güvenlik Duvarları ve Hibrit Sistemler

Durum denetimli paket filtrelemeli güvenlik duvarlarında ise çoklu port ihtiyacının olduğu ftp uygulamalarında kullanılmaktadır. Bu cihazlar, her protokol için yükü incelemekte, gerekli portu açmakta veya kapatmaktadır. Vekil güvenlik duvarları ise yerel ağı internetten izole etme yeteneğine sahiptir. Bu cihazların en önemli dezavantajı, çok fazla ağ kaynağına ihtiyaç duymasıdır



Okuma Önerisi:
https://www.ktu.edu.tr/dosyalar/bilgisayar_a93f2.pdf

Hafta-12

Şifreleme Teknolojileri

Açık Anahtar Altyapısı

Hafta-12

Erişim Kontrol Teknolojileri

- Erişim kontrol teknolojilerindeki kullanıcıların doğrulanması, kimlik doğrulamayla başlatılmaktadır. Sıklıkla kimlik doğrulandıktan sonra kullanıcılar bir bilgi sistemine erişmektedir.

- Erişim kontrol teknolojileri, kullanıcıların ve sistemlerin diğer sistem ve kaynaklar ile nasıl iletişim kurup, etkileştiklerini kontrol etmektedir. Bu teknolojiler, kaynağın kullanılabilirliğini, bütünlüğünü ve gizliliğini kontrol etme, kısıtlama, izleme ve koruma yeteneğine sahiptir.

Hafta-12

Erişim Kontrol Teknolojileri

- Bilginin güvenlik altına alınması için çeşitli erişim kontrol modelleri kullanılmaktadır.
- Bunların en önemlilerinden bazıları; MAC (Zorunlu Erişim Kontrolü), DAC (İsteğe Bağlı Erişim Kontrolü), RBAC (Rol Tabanlı Erişim Kontrolü) dir [26]. MAC ile DAC arasındaki temel fark erişim modelidir.
- MAC ile erişimde kullanıcı oluşturulan izin düzeyi ve altındaki kaynaklara erişebilmektedir.
- DAC ile erişimde ise izin düzeyi bulunmamaktadır. DAC'da kullanıcı kimliğine göre erişim sağlanmaktadır.
- RBAC'da ise roller ve ayrıcalıklar tarafından tanımlanmış erişim mekanizması ile güvenlik sağlanmaktadır.

Hafta-12

Erişim Kontrol Teknolojileri

- Diğer bir erişim kontrol teknolojisi ise biyometrik kontroldür.
- Biyometrik özelliklerden en yaygın olarak; parmak izleri, el geometrisi, retina taraması, iris tarama, ses tanıma, imza dinamiği, klavye dinamiği, yüz taraması gibi özellikler ile erişim kontrolü sağlanmaktadır.

- Biyometrik erişim teknolojisi, biyolojik ve davranış öznitelikleri ile gerçekleştirilmektedir. Bu teknolojide kart ve benzeri ilave donanıma ihtiyaç olmaması, erişim cihazının taşınmaması ve şifre hatırlanmasına ihtiyaç olmaması en önemli avantajlar arasında yer almaktadır. Fakat, biyometrik özelliklerinin depolandığı sistemlere yetkisiz erişim sağlanıp, ele geçirilmesi durumunda söz konusu biyometrik erişim özniteliklerinin değiştirilememesi en önemli dezavantajdır.

Hafta-12

Erişim Kontrol Teknolojileri

- Diğer bir erişim kontrol teknolojisi ise biyometrik kontroldür.
- Biyometrik özelliklerden en yaygın olarak; parmak izleri, el geometrisi, retina taraması, iris tarama, ses tanıma, imza dinamiği, klavye dinamiği, yüz taraması gibi özellikler ile erişim kontrolü sağlanmaktadır.

- Biyometrik erişim teknolojisi, biyolojik ve davranış öznitelikleri ile gerçekleştirilmektedir. Bu teknolojide kart ve benzeri ilave donanıma ihtiyaç olmaması, erişim cihazının taşınmaması ve şifre hatırlanmasına ihtiyaç olmaması en önemli avantajlar arasında yer almaktadır. Fakat, biyometrik özelliklerinin depolandığı sistemlere yetkisiz erişim sağlanıp, ele geçirilmesi durumunda söz konusu biyometrik erişim özniteliklerinin değiştirilememesi en önemli dezavantajdır.

Hafta-12

Erişim Kontrol Teknolojileri

- Ülkemizde son yıllarda E-imza ile erişim kontrolü yaygın bir şekilde kullanılmaya başlanmıştır. E-imza, özellikle elektronik ortamda hazırlanan bilginin doğrulanması için kullanılan donanım ve şifre doğrulamanın beraber gerçekleşmesini sağlamaktadır.

- E-imzanın, ıslak imzanın yerine kullanılması ile çeşitli resmi işlemlerin internetten ortamında yapılabilmesi ve doğrulanması sağlaması nedeniyle zaman ve maliyet tasarrufu sağlamaktadır

- Captcha, Carneige Mellon Üniversitesi tagüvenliği için kullanılan, kullanıcının robot olmadığını yazı veya soru cevaplanması ile erişim kontrolü rafından tasarlanan, özellikle webdeki bilgilerin yapan teknolojidir

Hafta-12

Güncel Siber Güvenlik Teknolojileri

- **Sosyal Siber Güvenlik Teknolojileri**

Sosyal siber güvenlik, insan davranışındaki siber ortama bağlı (cyber-mediated) değişiklikleri tanımlama, anlama ve tahmin etmeyi sağlayan yeni bir bilim alanıdır.

- **Nesnelerin İnterneti için Siber Güvenlik Teknolojileri**

(IDS-Instrusion Detection Systems)

- **Sağlık için Siber Güvenlik Teknolojileri**

Bulut Bilişim Teknolojileri

- **Büyük Veri için Siber Güvenlik Teknolojileri**

Hadoop güvenliği, bulut güvenliği, izleme ve denetleme, anahtar yönetimi ve anonimleştirme.

Hafta-12

Güncel Siber Güvenlik Teknolojileri

- **Büyük Veri için Siber Güvenlik Teknolojileri**

Hadoop, temelde güvenlik için geliştirilmemiş, büyük veri ile ortaya çıkan dağıtık veri işleme anaçatısıdır. Hadoop üzerindeki güvenlik iki yöntem ile sağlanmaktadır. İlk yöntemde, kullacının ve düğümün oluşturduğu hash fonksiyon değerleri karşılaştırılıp, kimlik doğrulama için SHA-256 hash tekniği kullanılarak sisteme erişim sağlanmaktadır. İkinci yöntemde ise MapReduce ile beraber RSA, AES ve RC6 rasgele şifreleme teknikleri kullanılmaktadır. Hadoop Dağıtılmış Dosya Sistemi (HDFS - Hadoop Distributed File System) güvenliği için ise üç temel yöntem kullanılmaktadır. İlk yöntemde, bilet verme veya servis biletine dayalı Kerberos mekanizması ile kimlik doğrulama gerçekleştirilmektedir. İkinci yöntemde ise Bull Eye algoritması ile hassas veriler sürekli görüntülenmektedir. Bu algoritma, orijinal veriler ile çoğaltılan veriler arasındaki ilişkileri yönetmek için kullanılmaktadır. Son yöntemde ise düğümlerdeki gecikme ve veri kullanılabilirliği sorunları için ana - yedek mekanizması kullanılmaktadır.

Hafta-12

Güncel Siber Güvenlik Teknolojileri

- **Büyük Veri için Siber Güvenlik Teknolojileri**

Büyük veride izinsiz giriş algılama mimarisi ile izleme, Merkle Hash Ağaçları ile denetleme gerçekleştirilmektedir. Anahtar yönetimi için ise Kuantum kriptografisi, çevrimiçi anahtar oluşturma ve benzeri teknikler kullanılmaktadır. Büyük verideki anonimleştirme için ise K-anonimlik tabanlı metrikler, uyarlamalı anonimleştirme modeli ve iki fazlı kümeleme algoritması kullanılmaktadır

Sorular

Bir sonraki ders E-mail, Sosyal Medya, Veri Tabanı ve Web Uygulama Zafiyetleri Ve Önlemler konusuna giriş yapılacak.