# IPV6 SALDIRI TRAFİĞİNDEN İMZA ÜRETME

Ümit Çavuş BÜYÜKŞAHİN
Bilgisayar Mühendisliği Bölümü,
Orta Doğu Teknik Üniversitesi, Türkiye
e1560028@ceng.metu.edu.tr

Yavuz GÖKIRMAK
Tübitak, Ulusal Akademik Ağ
ve Bilgi Merkezi
yavuzg@ulakbim.gov.tr

# İçerik

- Amaç
- İmza Üretme Teknikleri
  - Saldırı Tespiti Yaparak İmza Üretme
  - Saldırı Tespiti Yapmadan İmza Üretme
  - Karşılaştırma
- Testler & Sonuçlar
- Sonuç

# Amaç

- İnternet ağlarına yönelik saldırılıların önlenmesi
- Ulusal IPv6 Altyapısı Tasarımı ve IPv6'ya Geçiş Projesi kapsamında IPv6 trafiğinden imza üretme
- İmza üretme teknikleri incelenmesi
- En uygun tekniğin belirlenmesi
- Testler ve sonçlarının incelenmesi

# İmza Üretme Teknikleri

- Saldırı Tespiti Yaparak İmza Üretme
  - Ağ Seviyesinde Saldırı Tespiti ile İmza Üretme
    - Autograph
    - PADS
    - PAYL
  - Cihaz Seviyesinde Saldırı Tespiti ile İmza Üretme
    - COVER
    - DIRA
    - DOME
    - Minos
    - TainCheck
- Saldırı Tespiti Yapmadan İmza Üretme
  - Honeycomb
  - Polygraph
  - EarlyBird
  - Nemean
  - Hamsa
  - Nebula

# Ağ Seviyesinde Saldırı Tespiti ile İmza Çıkarma

Autograph

- Saldırı Tespiti:
  - Başasırız TCP bağlantılarını kayıtlar.
  - Bir kaynağın kaytları eşik değerin üzerindeyse, o saldırgan olarak belirlenir.

- İmza Üretimi:
  - Saldırgan adresinin paketlerinden en sık rastlanan bit dizileri çıkarılır.
  - Kesintisiz bayt dizilimli imza üretilir.

- Örnek imza:

```
drop tcp $HOME_NET any -> $EXTERNAL_NET 5000
(msg:"2712067784 Fri May 14 03:51:00 2004"; rev:1;
Content:"|90 90 90 90 4d 3f e3 77 90 90 90 90 ff 63 64 90 9|";)
```

# Ağ Seviyesinde Saldırı Tespiti ile İmza Çıkarma

PADS (Position-Aware-Distrubition)

- Saldırı Tespiti:
  - İki balküpü kullanılır.
  - Yüksek erişimli balküpünden yakalanan trafikler düşük erişimli balküpüne yönlendirilir.

- İmza Üretimi:
  - Bit pozisyon dağılımlı imza üretir.
  - Belirli tipteki polimorfik solucanları tespit edebilir.

- Örnek imza:

'GET','HTTP/%u9090%u897%ucb%u8%u53ff%u000%u

# Ağ Seviyesinde Saldırı Tespiti ile İmza Çıkarma

PAYL

- Saldırı Tespiti:
  - Belirli bir porttaki paket trafiğini inceler.
  - Anormal paketin geldiği porttan anormal bir paket çıkıyorsa, bu trafiği saldırı olarak niteler.

- İmza Üretimi:
  - LCS (longest-common-substring) algoritması ile en uzun ortak dizi çıkarılır.
  - Kesintili veya kesintisiz bayt dizisi şeklinde imzalar üretilir.

# İmza Üretme Teknikleri

- Saldırı Tespiti Yaparak İmza Üretme
  - Ağ Seviyesinde Saldırı Tespiti ile İmza Üretme
    - Autograph
    - PADS
    - PAYL
  - Cihaz Seviyesinde Saldırı Tespiti ile İmza Üretme
    - COVER
    - DIRA
    - DOME
    - Minos
    - TainCheck
- Saldırı Tespiti Yapmadan İmza Üretme
  - Honeycomb
  - Polygraph
  - EarlyBird
  - Nemean
  - Hamsa
  - Nebula

# Cihaz Seviyesinde Saldırı Tespiti ile İmza Çıkarma

## COVER (COntext-based VulnERability-oriented)

- Saldırı Tespiti:
  - Address-Space-Randomization yöntemini kullanmaktadır
  - Bellek erişim hatasına sebeb olan veriyi saldırı olarak algılar
- İmza Üretimi:
  - Üretilen imza sistem açığına özgüdür.

## DIRA(Detection Identification and Repair)

- Kontrol-Hijacking saldırılarına önler.
- GCC (GNU Compiler Collection ) sayesinde saldırıyı tespit eder
- Haıfıza kütüğünü tutar.
- Bu sayede saldırıyı tanır ve zarar gören yeri onarır.

# Cihaz Seviyesinde Saldırı Tespiti ile İmza Çıkarma

## DOME(Detection of Malicious Execuatable)

- Sistem çağrılarını kullanan zararlı kodları tespit eder.
- İmza üretmez ama var olan imza güncellenir.

## Minos

- Güvenilmeyen girdileri işaretler.
- Program akışını değiştirecek saldırıları önler.
- İmza üretmez.

## TaintCheck

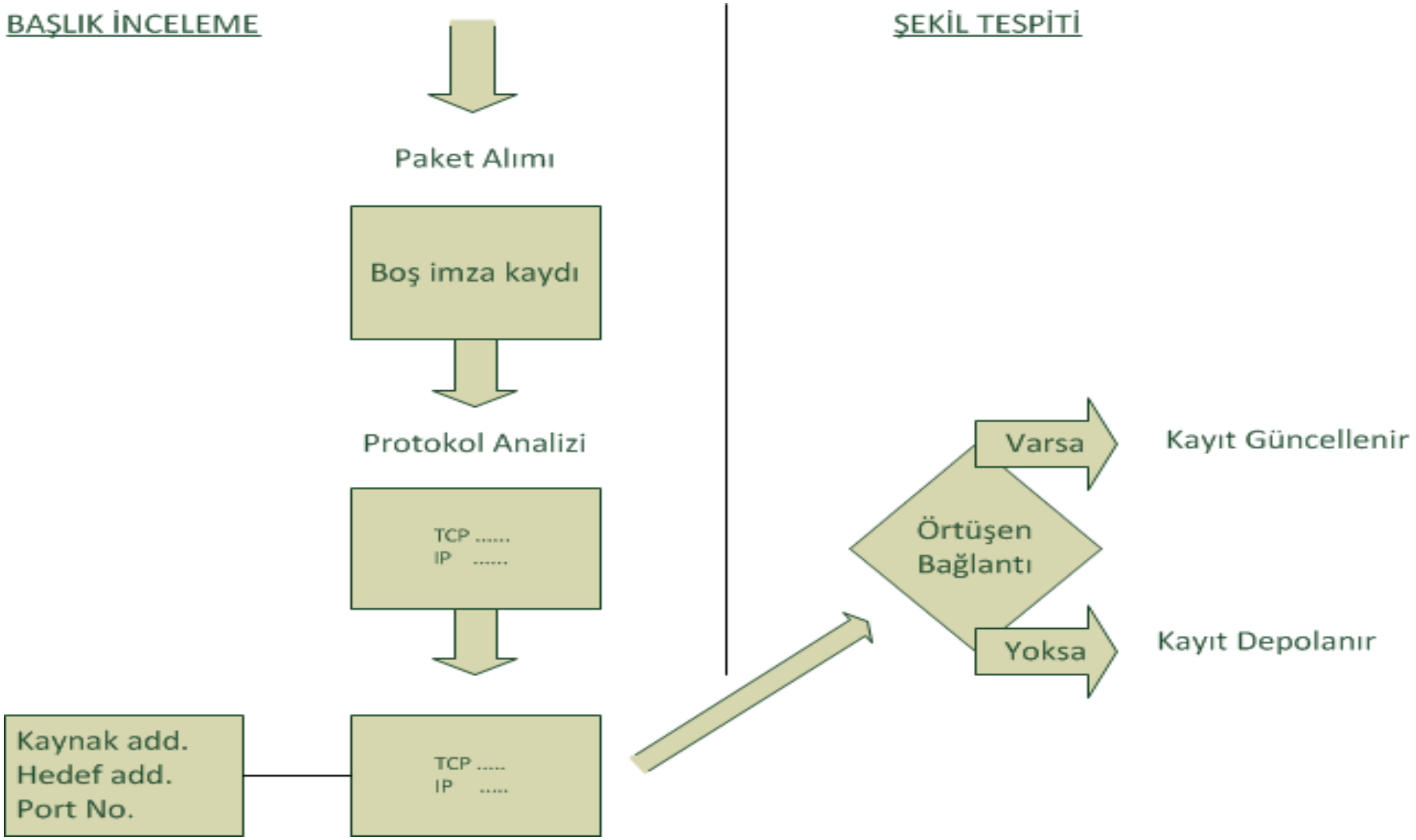
- Minos gibi dinamik veri analizi yapar.
- Tampon taşırma gibi saldırıları tespit eder.
- Üç bayt uzunluğundaki imzalar üretir.

# İmza Üretme Teknikleri

- Saldırı Tespiti Yaparak İmza Üretme
  - Ağ Seviyesinde Saldırı Tespiti ile İmza Üretme
    - Autograph
    - PADS
    - PAYL
  - Cihaz Seviyesinde Saldırı Tespiti ile İmza Üretme
    - COVER
    - DIRA
    - DOME
    - Minos
    - TainCheck
- Saldırı Tespiti Yapmadan İmza Üretme
  - Honeycomb
  - Polygraph
  - EarlyBird
  - Nemean
  - Hamsa
  - Nebula

# Saldırı Tespiti Yapmadan İmza Üretme

## Honeycomb



# Saldırı Tespiti Yapmadan İmza Üretme

Honeycomb

- Paket başlığı izleme ve şekil tespiti olmak üzere iki kısımdan oluşur.
- LCS algoritmasını suffix-tree ile yaparak, lineer zamanda sonuç almaktadır.
- Kesintisiz bayt dizisi şeklide imzalar üretir.
- Bu nedenle, polimorfik solucanlara karşı başarısızdır.

# Saldırı Tespiti Yapmadan İmza Üretme

Polygraph

- Polimorfik solucanların değişmez bayt dizilerinden imza üretir.
- Gelen paketler, şüpheli ve şüphesiz akım havuzlarında toplanır.
- İmza üretme aşamasında iki havuzdan da yararlanılır .
- Şüpheli havuzundan üretilen tokenlarla imzalar üretilir.
- Honeycomb'un aksine protokol temelli saldırılarda başarısızdır.
- 3 çeşit imza türü vardır:
  - Birleşim İmzaları
  - Sıralı token İmzaları
  - Bayes İmzaları

# Saldırı Tespiti Yapmadan İmza Üretme

Polygraph

| | |
|---|---|
| **Birleşim İmzaları** | 'GET','HTTP/1.1\r\n' , ':','\r\n Host:' , '\r\n', ':' , '\r\nHost:' , '\r\n' , '\xFF','\r\n' |
| **Sıralı-token İmzaları** | GET.*HTTP/1.1\r\n.*:.*\r\nHost:.*\r\n.*:.*\r\nHost:.*\xFF\xBF.*\r\n |
| **Bayes İmzaları** | '\r\n': 0.0000, ': ': 0.0000,'\r\n Host: ': 0.02,'GET':0.0035, 'HTTP/1.1\r\n':0.1108,'\xFF\xBF ':3.1517.Threshold:1.9934 |

- Bayes, her token için ayrı değerlendirme yaptığından başarısız imzalar üretir.
- Sıralı-token en başarılı imzaları üretmektedir.

# Saldırı Tespiti Yapmadan İmza Üretme

Earlybird

- Belirli bir adresten gelen gelen trafiklerin yaygınlıkları ölçülür.
- Ağa gelen her paket şu aşamalardan geçer:
  - Paketlere özgü Rabin parmakizi berlilenir.
  - Bu parmakizi, paketin geldiği hedef/kaynak adresine göre yaygınlık tablosuna indekslenir.
  - Bu adreslerden gelen paket sayısını gösteren sayıcılar eklenir.
  - Sayıcı değerinin yüksek olması ,saldırı trafiği olarak nitelendirilmesine neden ollur.

# Saldırı Tespiti Yapmadan İmza Üretme

Earlybird

- Üretilen imzalarda hedef/kaynak adres bilgileri bulunmaktadır.
- Kesintisiz bayt dizisi şeklinde imzalar üretilir.
- Her paket için Rabin parmakizlerinin belirlenmesi, yoğun trafik analizleri için bu tekniği başarısız kılmaktadır.

# Saldırı Tespiti Yapmadan İmza Üretme

Nemean

- İmza üretimi iki aşamada gerçekleştirilir.
  - DAC(Data Abstraction)
    - Gelen paketler normalleştirilerek, protokol belirsizlikleri kaldırılır.
    - Bu paketler tekrar montelenir ve iki düğüm arasındaki oturumlar çıkarılır.
  - SGC(Signature Generation)
    - Oturumlar anlamsal benzerliklerine göre kümelenir.
    - Otomatalar kullanılarak imzalar çıkarılır. Bu sayede imza istenilen saldırı tespit sistemine(IDS) dönüştürülür.
- Anlamsal incelemede protokol bilgisine ihtiyaç duyulur.

# Saldırı Tespiti Yapmadan İmza Üretme

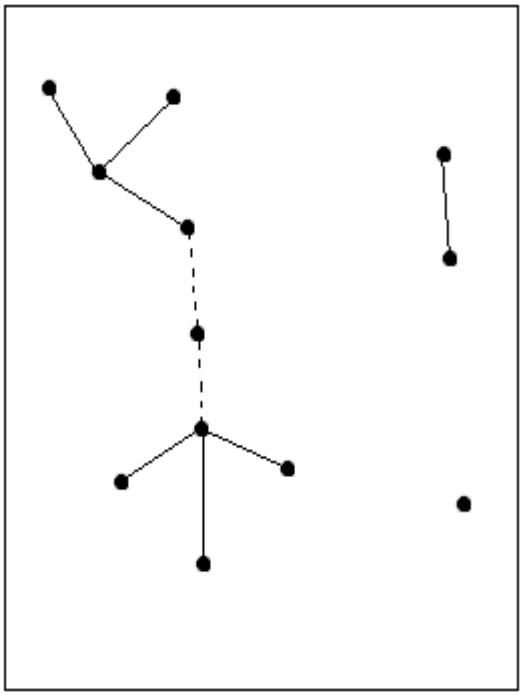
Hamsa

- Solucanların değişmez bit dizilerinden yola çıkar.
- Gelen paketleri protokol bilgilerine göre sınıflandırılır.
- Bilinen saldırı bilgilerine göre paketler şüpheli veya normal havuzlarına eklenir.
- Her iki havuzunda tokenları çıkarılır, normal havuzunda bulunan şüpheli paketler elenir.
- Şüpheli havuzundan LCS algoritmalarıyla imza üretilir.
- Polygraph' a benzesede daha başarılı bir yöntemdir.
- LCS NP-Hard olduğu için, yoğun trafikler için çok genel imza üretir.

# Saldırı Tespiti Yapmadan İmza Üretme

Nebula

- Gelen paketleri benzerlik derecesine göre kümeler(clustering).
- Kümelemedeki temel mantık:
  *"Üretilen imzalar, farklı saldırılar için genel olamalı fakat herbir saldırı için özel olmalı"*
- Gelen paketler eşik mesafesine göre ya bir kümeye katılır ya da ayrık bir değer olur.
- İmzalar bu kümelerden, en uzun bayt dizileri belirlenerek üretilir.
- Burada lineer zamanda sonuç veren suffix-tree' li LCS algoritması uygulanır.



# Saldırı Tespiti Yapmadan İmza Üretme

Nebula

- İmzalarında protokol ve adres bilgileri bulunur.
- İmzasındaki pozisyon ve sıra numaraları doğruluğunu artırmaktadır.
- Örnek imza:

```
alert tcp any any -> $HOME_NET 8800 (msg: "nebula rule 2000001 rev. 2"; \
content: "GET /getad.a2?target=xyz_sitegene|00 00 00 00 00 00 00 00 89 00 00
00|DLT_EN10MB|00 |15 c0|\\'|16 80 bf 03 17 c0|>|07 18|P|94 89 19 c0 94 dc 19 d0
d3 c6 1c|P|15 9b 1d 00 82 8c 1e 00|s|7c 1f 00|dl |00|U\\!|00|FL\"|00|7<#|00|(,|24 00
19 1c|%|00 0a 0c|&|80|  5|05|'p|18 f5|'"; offset: 0; depth: 2629; \
sid: 2000001; rev: 2;)
```

- Posix işletim sistemlerine hepsine uyumludur.
- 2008 de son sürümü yayınlanmış ve geliştiriciler tarafından aktif olarak güncelleştirilmektedir.

# İmza Üretme Teknikleri

- Saldırı Tespiti Yaparak İmza Üretme
  - Ağ Seviyesinde Saldırı Tespiti ile İmza Üretme
    - Autograph
    - PADS
    - PAYL
  - Cihaz Seviyesinde Saldırı Tespiti ile İmza Üretme
    - COVER
    - DIRA
    - DOME
    - Minos
    - TainCheck
- Saldırı Tespiti Yapmadan İmza Üretme
  - Honeycomb
  - Polygraph
  - EarlyBird
  - Nemean
  - Hamsa
  - Nebula

# Karşılaştırma

- Saldırı tespiti olmadan imza üreten tekniklerin analizi:

| Teknik | İmza Çeşidi | Polimorfik Solucan Tespiti | Performans |
|---|---|---|---|
| Honeycomb | Keisintisiz Bayt Dizisi | Yok | Orta |
| Polygraph | Keisintisiz/Kesintili Bayt Dizisi | Var | Orta |
| Earlybird | Keisintisiz Bayt Dizisi | Yok | İyi |
| Nemean | Otomata | Yok | Orta |
| Hamsa | Keisintili Bayt Dizisi | Var | Orta |
| Nebula | Keisintisiz Bayt Dizisi | Var (öngörülmüştür) | İyi |

# Testler & Sonuçlar

- Nebula seçiminin üç temel nedeni:
  - Yüksek performansı
  - Güncel geliştirici desteği
  - Kovan bünyesinde kullanılmaya uygun

- Nebula istemci-sunucu mimarisinde çalışmaktadır.
- Yakalanan trafiğin TCP oturumlarına ayrılması gerekmektedir.
- Bunun için *tcpick* kullanılmıştır.
- Saldırı tespit sistemi olarak *snort* kullanılmıştır.

# Testler & Sonuçlar

## Ipv4 Trafiğinden İmza Üretme

- Ağ trafiğinin TCP oturumlarına ayrılması
  *root# tcpick -r saldırıDosyası.pcap -wR -C*
- Nebula sunucusu çalıştırılır, TCP oturumlarını alacağı port ve eşik değer belirlenir.
  *root# nebula -p 2000  -a imzaDosyası -t 5*
- Nebula istemcisi ile TCP oturumları sunucuya gönderilir.
  *root# nebulaclient -p 2000  -c *.dat*

- Üretilen imza bir kural olarak snort'a eklenir ve çalıştırlır.
  *root# snort -T -c snort.conf*

- Trafiği alan snort, trafiği başarıyla tespit eder.

# Testler & Sonuçlar

Ipv6 Trafiğinden İmza Üretme

- Metasploit saldırı aracından “*Microsoft RPC DCOM Interface Overflow*” saldırısı kullanılmıştır.
- Ipv4 Trafiğinden İmza Üretme basamakları uygulanmıştır.
- *tcpick'*e Ipv6 desteği sağlanmış ve TCP oturumları üretilmiştir.
- Nebula ile üretilen imza üzerinde ufak bir değişiklik yapılmıştır.
- İmza *snort'*a eklenip, çalıştırılınca saldırı trafiği tanınmıştır.

# Sonuç

- Otomatik imza üretme teknikleri ile saldırılardan asgari zarar beklenmektedir.
- Öncelikle Ipv4 ağlarında kullanılan teknikler incelenmiştir.
- Yapılan analizler sonucunda Ipv6 saldırı trafiği Nebula da denenmiştir.
- *tcpick* uygulamasına Ipv6 desteği sağlanmıştır.
- Üretilen imzalar *snort* saldırı tespit sisteminde test edilerek, saldırı trafiği başarıyla tespit edilmiştir.

# TEŞEKKÜRLER...