# Defense and Attack Techniques Against File-Based TOCTOU Vulnerabilities: A Systematic Review Makalesinin Bildiri İncelemesi

## Sorun, Problem, Çözüm ve Kazanımların Özeti:

Bu makale, dosya tabanlı Time-of-Check to Time-of-Use (TOCTOU) zafiyetlerini araştırarak, bu güvenlik sorununu anlamayı, savunma stratejileri geliştirmeyi ve bu tür saldırılara karşı nasıl korunabileceğimizi ele alıyor. Yapılan kapsamlı bir literatür taraması ve analizlerle, TOCTOU zafiyetlerinin savunma açısından nasıl ele alınabileceği üzerinde bir çerçeve sunuyor.

*"Makale, dosya tabanlı TOCTOU zafiyetlerini anlamak, savunma stratejilerini geliştirmek ve bu tür saldırılara karşı koruma sağlamak için önemli bir çerçeve sunmayı amaçlamaktadır."*

## Kuvvetli Yanlar:

TOCTOU zafiyetlerine karşı savunma stratejilerini ayrıntılı bir şekilde açıklaması, bu alandaki temel kavramları anlamak isteyenlere yardımcı oluyor. Farklı savunma stratejilerini kapsayan bu makale, bu stratejilerin nasıl çalıştığını anlamamızı sağlıyor ve güvenlik konusundaki bilgi düzeyimizi artırıyor. Makale, dosya tabanlı TOCTOU zafiyetleri konusunda yapılmış önceki çalışmaları detaylı bir şekilde ele alarak, bu alandaki bilgi birikimine katkıda bulunuyor.

*"Makale, dosya tabanlı TOCTOU zafiyetlerine karşı çeşitli savunma yöntemlerini içererek, bu konuda geniş bir bilgi yelpazesi sunmaktadır."*

## **Zayıf Yanlar**:

Savunma stratejilerine ait kaynak kodları veya araçların eksikliği, bu stratejilerin pratikte nasıl uygulandığını anlamamızı zorlaştırabilir. Gerçek dünya örneklerinin yetersiz olması, okuyucuların savunma stratejilerini daha iyi görselleştirmelerini engelleyebilir.

"Makale, savunma stratejilerini destekleyen kaynak kodları veya somut örneklerle pekiştirmeyerek, okuyucuların bu stratejileri daha iyi anlamalarına katkıda bulunamayabilir."

## Sahayı Nasıl Etkiledi:

### Sahayı (ilgili olduğu bilim alanını) nasıl etkilemiştir?

Özellikle, dosya tabanlı TOCTOU zafiyetleri üzerine odaklanarak dosya işlemlerinde ortaya çıkan ve genellikle bilgisayar sistemlerinin güvenliğini tehdit eden kritik sorunlardan biridir. Bu nedenle, makalenin bu alandaki etkisi büyük önem taşımaktadır ayrıca TOCTOU zafiyetlerini anlamada bir rehber sağlamaktadır.

## Hangi sorular açık kalmıştır? Neler çözülmemiştir?

Etkili Evrensel Çözüm Yokluğu: Makalede vurgulandığı gibi, şu ana kadar dosya tabanlı TOCTOU zafiyetlerine karşı etkili bir evrensel çözüm önerisi bulunmamaktadır. Belirli savunma stratejileri belirli senaryolara yönelik olabilir, ancak evrensel bir çözümün olmaması, bu alanda daha fazla araştırma ve geliştirme ihtiyacını göstermektedir.

Dosya Sistemleri Üzerinde Performansın Belirsiz Etkisi: Makale, belirli savunma stratejilerinin performansını değerlendirmekte ancak bu stratejilerin farklı dosya sistemleri üzerindeki etkilerini daha ayrıntılı incelememektedir. Dosya sistemlerinin çeşitliliği, savunma stratejilerinin genel performansını ve uygulanabilirliğini etkileyebilir.

Savunma Stratejilerinin Uygulanabilirliği: Makale, belirli savunma stratejilerini sunmakta ancak bu stratejilerin gerçek dünya senaryolarında ne kadar uygulanabilir olduğu konusunda daha fazla ayrıntıya odaklanmamaktadır. Pratik uygulanabilirlik, günlük kullanıma yönelik savunma stratejilerinin başarısını etkileyen önemli bir faktördür.

Daha Geniş Kapsamlı ve Evrensel Çözümler: Makale, dosya tabanlı TOCTOU zafiyetleri konusunda belirli savunma stratejilerine odaklanmaktadır, ancak daha geniş kapsamlı ve evrensel çözümlere dair öneriler bulunmamaktadır. Bu alanda yapılacak olan geleceğe dönük araştırmalar, bu tür evrensel çözümleri hedeflemelidir.

Pratik Senaryolarda Daha Detaylı İnceleme: Makale, belirli savunma stratejilerini çeşitli senaryolarda değerlendirmektedir. Ancak, bu senaryolarda stratejilerin etkinliğini ve uygulanabilirliğini daha ayrıntılı bir şekilde inceleyerek, savunma stratejilerinin gerçek dünya kullanımına daha yakın bir perspektif sunabilirdi.

## Hangi deneyler eksik bırakılmıştır? Yapılması ya da tartışılması gerekenler nelerdir?

• Çeşitli Dosya Sistemleri Üzerinde Performans Değerlendirmesi

• Gerçek Dünya Senaryolarında Uygulanabilirlik Testleri

• Farklı Dil ve Çerçevelerde Uygulanabilirlik Testleri

• Alternatif Savunma Stratejilerinin Karşılaştırılması

Bu eksikliklerin giderilmesi, TOCTOU zafiyetlerine karşı daha etkili savunma stratejilerinin geliştirilmesine ve bu stratejilerin pratik uygulanabilirliğinin artırılmasına katkı sağlayabilir.

## Gelecek çalışmalar için öngördükleri problemler ve sorular nelerdir?

Özellikle, belirli savunma stratejilerinin evrensel olmak yerine belirli senaryolara yönelik olabileceği vurgulanmaktadır. Gelecek çalışmaların, dosya işlemlerindeki TOCTOU zafiyetlerine karşı daha spesifik ve etkili savunma stratejileri geliştirmeye odaklanması önerilebilir veya evrensel çözümler üzerine de gidilebilir.

## Sunulan yaklaşımın çalışacağı veya çalışmayacağı bazı örnekler ya da durumlar nelerdir?

Çok Sayıda Paralel İşlem: Savunma stratejileri, sistem çağrılarının paralel yürütüldüğü durumları ele almak için tasarlanmıştır. Bu nedenle, çok sayıda paralel işlemin olduğu durumlarda stratejilerin etkinliği artabilir.

Yüksek I/O Hacmi: Stratejiler, dosya işlemlerinin yoğun olduğu durumları hedef alır. Yüksek I/O hacmi gerektiren uygulamalarda, bu stratejilerin etkili olma olasılığı yüksektir.

Farklı Dosya İşlemleri ve Senaryoları: Savunma stratejileri, farklı dosya işlemlerini ve senaryolarını ele almak üzere tasarlanmıştır. Ancak, her bir stratejinin belirli dosya işlemleri ve senaryoları için ne kadar etkili olduğunu belirlemek için daha geniş kapsamlı testlere ihtiyaç vardır.

Yüksek Sistem Çağrısı Frekansı: Eğer bir uygulama sürekli olarak yüksek frekansta sistem çağrıları yapmaktaysa, savunma stratejilerinin performansı olumsuz etkilenebilir.

Dinamik Dosya İsimlendirme ve Yönetim: Eğer uygulama dinamik olarak dosya isimlendirme ve yönetim işlemlerini sıkça değiştiriyorsa, savunma stratejileri bu dinamizmi takip etmekte zorlanabilir.

## Bugün benzer bir bildiri yayınlanabilir mi? Siz olsaydınız bu çalışmayı nasıl devam ettirirdiniz?

Evet, günümüzde benzer bir bildiri yayınlanabilir. Eksiklikleri giderilip bu konuda daha fazla testler gerçekleştirip buna benzer bir bildiri yayınlanabilir ve referans olarak bu bildiri gösterilebilir.

Eğer bu çalışmanın yazarı olsaydım, performans İyileştirmeleri, gerçek zamanlı izleme ve analiz ve bir çok dosya tipine ve işleme göre testler eklemek isterdim.

## Ortaya attığı, iddia ettikleri fikirler veya düşünceler nelerdir?

Savunma stratejilerini genel olarak iki kategoriye ayırarak, statik ve dinamik savunma yöntemlerini ele almaktadır. Öne çıkan savunma stratejilerinin çoğunun sistem çağrılarına odaklandığı ve kernel seviyesinde uygulandığı belirtilirken, bu yaklaşımın daha etkili bir koruma sağlayabileceği ifade edilmektedir. Makale, Unix benzeri işletim sistemlerine odaklanarak, savunma stratejilerinin uygulanabilirliğini değerlendiren bir çerçeve sunar.

## Bildiri ile ilgili diğer ilginç yorumlarınız nelerdir?

TOCTOU zafiyetleri ve bu tür saldırılara karşı geliştirilen savunma stratejileri konusunda kapsamlı bir bakış sunmaktadır. İlk olarak, savunma stratejilerinin sınıflandırılması ve detaylı analizi oldukça iyi ve anlaşılır ve mantıken bu konuda en azından hiçbir şey bilmeyen biri olarak fikir edinmemi sağladı. Makale, savunma mekanizmalarını farklı kategorilere ayırarak, her birinin avantaj ve dezavantajlarını anlamama yardımcı oluyor.

Ancak, makalenin en belirgin zayıflığı, savunma stratejilerinin çoğunun kaynak kodları veya araçları ile birlikte sunulmamış olması ve bu yüzden bu tür bir araştırmada kaynakların en baştan yapılması gerekir. Bu, diğer araştırmacıların bu stratejileri test etmelerini ve sonuçları tekrarlamalarını zorlaştırabilir. Güncelliğin değerlendirilmesi de bir başka önemli konudur. Makale, 2021'e kadar olan bir süre içinde literatürü gözden geçirmiştir ve 2022 yılında yayınlanmıştır ancak bu tarihten sonraki teknolojik gelişmeleri ve ortaya çıkan yeni sorunları yansıtmayabilir. Makalenin güçlü bir yönü de sahada açık kalan soruları vurgulaması ve gelecek araştırmalar için önerilerde bulunmasıdır. Bu konuda çalışma yapmak istesem bu makale okumam gereken ve bana yönergeler verecek nitelikte bir makaledir.