ÖZET

Telekomünikasyon dolandırıcılığı tespit ve uyarı sistemi ve yöntemi

Buluş, temelde, çağrı detay bilgilerini oluşturulduğu çağrı inceleme cihazı (1), kurallar ile eşleşme olup olmadığının kontrol eden saldırı tespit cihazı (2) ve engelleme kuralı oluşturulduğu saldırı engelleme cihazı (3) içeren, telekomünikasyon alanında yapılan ücret dolandırıcılıklarını tespit etmeye ve sonrasında tehlikeli bulunan çağrıları engellemeye yönelik işlem yapacak bir sistem ve yöntem ile ilgilidir.

(Şekil 1)

İSTEMLER

1. Telekomünikasyon alanında yapılan ücret dolandırıcılıklarını tespit etmeye ve sonrasında tehlikeli bulunan çağrıları engellemeye yönelik işlem yapan bir sistem olup, özelliği, bahsedilen sistemin,

- Paketlerin bir ağ anahtarından (E) toplanıp birleştirilmesini sağlayan en az bir trafik kontrol birimi (9),

- bahsedilen trafik kontrol birimi (9) tarafından toplanıp birleştirilen paketlerin iletildiği ve içerisinde en başta kuralların bulunmadığı en az bir engelleme kural çalıştırıcı (10),

- bahsedilen trafik kontrol birimi (9) tarafından toplanıp birleştirilen paketlerin iletildiği, paketin bir çağrı başlatma mesajı olup olmadığının kontrol edilmesini, yeni bir çağrı başlatılacaksa bu çağrı için yeni bir çağrı detay kaydı oluşturulmasını ve paket var olan bir çağrı ile ilgili bir paket ise çağrının detay kayıtlarının yeni gelen pakete göre güncellenmesini sağlayan en az bir SIP durum makinesini (7) içeren en az bir çağrı inceleme cihazı (1),

- bahsedilen çağrı inceleme cihazı (1) vasıtasıyla elde edilen çağrı detay kayıtlarının arayan, aranan ve arayan/aranan olarak birleştirilmesinin sağlayan en az bir toplayıcı (5),

- bahsedilen toplayıcı (5) tarafından gelen çağrı detay kayıtlarının var olan kurallar ile eşleşip eşleşmediğinin tespit edilmesini sağlayan en az bir tespit kural çalıştırıcı (6),

- bahsedilen toplayıcıyı (5) ve bahsedilen tespit kural çalıştırıcıyı (6) içeren en az bir saldırı tespit cihazı (2),

- bahsedilen trafik kontrol birimini (9) ve bahsedilen engelleme kural çalıştırıcıyı (10) içeren, bahsedilen tespit kural çalıştırıcı (6) da gelen çağrı detay kayıtlarının, kurallar ile eşleşmesi durumunda, oluşturulması istenilen kural ile ilgili bilgi iletildiği ve bahsedilen saldırı tespit cihazından (2) gelen bilgiler de kullanılarak bir engelleme kuralı oluşturulmasını sağlayan en az bir saldırı engelleme cihazı (3),

- bahsedilen çağrı inceleme cihazı içerisinde konumlandırılan, birleştirilen çağrı detay bilgileri engelleme kuralı ile eşleşirse, bahsedilen saldırı engelleme cihazına (3) tarafından bilginin iletildiği ve çağrı detay kayıtlarının incelenerek, var olan çağrıyı sonlandırabilen bir mesaj oluşturulmasını sağlayan en az bir çağrı sonlandırıcı (8),

- bahsedilen sisteme kullanıcı tarafından kuralların girilmesini sağlayan en az bir kullanıcı ara yüzü (11),

- çağrı detay kayıtlarının ve bahsedilen saldırı tespit cihazı (2) içerisindeki bahsedilen saldırı engelleme cihazı (3) tarafından oluşturulan kuralların kaydedildiği en az bir veri tabanı (4),

içermesidir.

2. Telekomünikasyon alanında yapılan ücret dolandırıcılıklarını tespit etmeye ve sonrasında tehlikeli bulunan çağrıları engellemeye yönelik işlem yapan bir yöntem olup, özelliği, bahsedilen yöntemin,

- kullanıcının, kuralları, kullanıcı bir ara yüzü (11) aracılığıyla sisteme girmesi,

- paketlerin, bir trafik kontrol birimi (9) tarafından toplanıp birleştirilmesi ve bir engelleme kural çalıştırıcısına (10) iletilmesi,

- bahsedilen engelleme kural çalıştırıcısında (10) hiçbir kural bulunmamasından dolayı, paketlerin kopyasının oluşturularak bahsedilen trafik kontrol birimi (9) tarafından, sıralı bir şekilde bir çağrı inceleme cihazına (1) iletilmesi,

- paketlerin bahsedilen çağrı inceleme cihazı (1) içindeki bir SIP durum makinesine (7) iletilmesi,

- bahsedilen SIP durum makinesinde (7) paketin bir çağrı başlatma mesajı olup olmadığının kontrol edilmesi, yeni bir çağrı başlatılacaksa bu çağrı için yeni bir çağrı detay kaydı oluşturulması ve paket var olan bir çağrı ile ilgili bir paket ise çağrının detay kayıtlarının yeni gelen pakete göre güncellenmesi,

- bahsedilen çağrı inceleme cihazında (1) oluşturulan çağrı detay kayıtlarının oluşturulması bir saldırı tespit cihazına (2) iletilmesi,

- bahsedilen saldırı tespit cihazı (2) içindeki bir toplayıcı (5) tarafından, bahsedilen çağrı inceleme cihazı (1) vasıtasıyla elde edilen çağrı detay kayıtlarının arayan, aranan ve arayan/aranan olarak birleştirilmesi ve bir tespit kural çalıştırıcısına (6) gönderilmesi,

- bahsedilen tespit kural çalıştırıcı (6) vasıtasıyla, bahsedilen toplayıcı (5) tarafından gelen çağrı detay kayıtlarının var olan kurallar ile eşleşip eşleşmediğinin tespit edilmesi,

- bahsedilen tespit kural çalıştırıcı (6) da gelen çağrı detay kayıtlarının, kurallar ile eşleşmesi durumunda, bir saldırı engelleme cihazına (3) oluşturulması istenilen kural ile ilgili bilgi iletilmesi,

- bahsedilen saldırı engelleme cihazında (3), bahsedilen saldırı tespit cihazından (2) gelen bilgiler de kullanılarak bir engelleme kuralı oluşturulması,

- birleştirilen çağrı detay bilgileri engelleme kuralı ile eşleşirse, bahsedilen saldırı engelleme cihazına (3) tarafından bir çağrı sonlandırıcıya (8) bilgi iletilmesi ve çağrı detay kayıtlarının incelenerek, var olan çağrıyı sonlandırabilen bir mesaj oluşturulması,

- bahsedilen çağrı sonlandırıcı (8) oluşturulan mesajların bahsedilen trafik kontrol birimi (9) vasıtasıyla sunuculara ve cihazlara iletilmesi,

- eğer tespit kuralında çağrı kapama seçeneği varsa bahsedilen saldırı tespit cihazından (2) bahsedilen çağrı izleme cihazına (1) uyarı yollanması,

- uygun çağrı kapama mesajının bahsedilen saldırı engelleme cihazı (3) tarafından çağrının iki bacağına yollanması,

- çağrı detay kayıtlarının ve bahsedilen saldırı tespit cihazı (2) içerisindeki bahsedilen saldırı engelleme cihazı (3) tarafından oluşturulan kuralların bir veri tabanında (4) saklanması

işlem adımlarını içermesidir.

TARİFNAME

Telekomünikasyon dolandırıcılığı tespit ve uyarı sistemi ve yöntemi

Teknik Alan

Buluş, telekomünikasyon alanında yapılan ücret dolandırıcılıklarını tespit etmeye ve sonrasında tehlikeli bulunan çağrıları engellemeye yönelik işlem yapacak bir sistem ve yöntem ile ilgilidir. Bu doğrultuda buluş başta VoIP (Voice Over Internet Protocol) olmak üzere, telefon ağlarında dolandırıcılıkları engellemek için kullanılabilmektedir.

Tekniğin Bilinen Durumu

Mevcut uygulamalarda var olan telekomünikasyon güvenlik ürünleri, klasik ağ güvenlik ürünlerinin daha özelleştirilmiş hallerinden oluşmaktadır. Bu ürünler kullanılarak telekomünikasyon cihazlarına yapılabilecek geleneksel ağ saldırılarına karşı koruma sağlansa bile, telefon sistemlerinin genel yapısından kaynaklanan dolandırıcılık girişimlerine karşı koruma sağlanamamaktadır.

Telekomünikasyon dolandırıcılığını tespit etmek için, paketlerin tek veya bir bütün olarak ağ seviyesindeki davranışının incelenmesi yeterli olmamaktadır. Sisteme gelen ağ paketlerinin, telekomünikasyon bağlamında anlam ifade etmeleri gerekir. Telefon çağrıları, kullandıkları protokollere göre değişen farklı mesajlar ile çağrı yapan telefonlar arasında taşınmaktadır. Bu sinyallerin işlenmesi ve kullanılan protokole göre anlamlandırılması gerekmektedir. Mevcut uygulamalarda var olan güvenlik ürünleri kullanılarak, bu anlamlandırma işlemini gerçekleştirilememektedir.

Güvenlik problemine örnek olarak, çağrı yönlendirme dolandırıcılığı gösterilebilir. Bu dolandırıcılıkta bir telefonu, yurtdışındaki kendine ait özel ücretli bir hatta yönlendiren dolandırıcı, telefonu dışarıdan arayarak kazanç sağlamaktadır. Bu kazanç, hat sahibinin faturasına yansımaktadır ve dolandırıcılık sonradan tespit edilse dahi, yurtiçi telefon operatörünün yurtdışındaki hizmet sağlayıcılara ödeme yapması gerekmektedir. Bu saldırıyı mevcut uygulamadaki ağ güvenliği sistemleriyle fark etmek imkânsızdır. Çünkü normal bir arama gerçekleştirilmekte ve paket trafiğinde bir anormallik görülmemektedir. Aynı şekilde paketlerin içeriği de tamamen protokol kurallarına uygundur. Bu dolandırıcılığın tespit edilmesi ancak ay sonunda, dolandırılan kullanıcının faturayı incelemesi sonucunda gerçekleşmektedir.

Sonuç olarak, yukarıda anlatılan olumsuzluklardan dolayı ve mevcut çözümlerin konu hakkındaki yetersizliği nedeniyle ilgili teknik alanda bir geliştirme yapılması gerekli kılınmıştır.

Buluşun Amacı

Buluş, mevcut durumlardan esinlenerek oluşturulup yukarıda belirtilen olumsuzlukları çözmeyi amaçlamaktadır.

Buluşun ana amacı, telekomünikasyon operatörünün bir kurallar listesi hazırlamasına olanak sağlamaktır. Liste hazırlanırken, operatör, çağrı ile ilgili çağrı süresi, çalma süresi, arama sayısı, çağrıda belirli telefon servislerinin kullanılıp kullanılmadığı, çağrıyı yapanın veya alanın kimliği gibi parametreleri kullanmaktadır.

Buluşun diğer bir amacı, operatör üzerinden geçen tüm çağrıları inceleyerek ve durumsal olarak analiz ederek, çağrıların kurallarda kullanılan parametre değerlerini hesaplamak ve kayıt altına almaktır.

Buluşa konu olan sistem, operatör, kuralları oluştururken, kendi sisteminde önceden gördüğü dolandırıcılık girişimlerinden elde ettiği bulguları veya diğer operatörlerin paylaştıkları değerleri kullanabilir. Kurallara takılan çağrılar durdurulmakta ve ikinci bir kural sistemine de bu numaralardan gelen yeni çağrıların engellenmesi için bir kural girilmektedir. Böylelikle hem dolandırıcının tespit edilmesi sağlanmakta hem de dolandırma işlemi başarısızlıkla sonuçlanmaktadır. Ayrıca dolandırıcının aynı numarayı kullanarak başka bir dolandırıcılık girişiminde bulunması da engellenmektedir.

Yukarıda anlatılan amaçları yerine getirmek üzere buluş, telekomünikasyon alanında yapılan ücret dolandırıcılıklarını tespit etmeye ve sonrasında tehlikeli bulunan çağrıları engellemeye yönelik işlem yapan bir sistem olup,

- paketlerin ağ anahtarından toplanıp birleştirilmesini sağlayan en az bir trafik kontrol birimi,

- bahsedilen trafik kontrol birimi tarafından toplanıp birleştirilen paketlerin iletildiği ve içerisinde en başta kuralların bulunmadığı en az bir engelleme kural çalıştırıcı,

- bahsedilen trafik kontrol birimi tarafından toplanıp birleştirilen paketlerin iletildiği, paketin bir çağrı başlatma mesajı olup olmadığının kontrol

edilmesini, yeni bir çağrı başlatılacaksa bu çağrı için yeni bir çağrı detay kaydı oluşturulmasını ve paket var olan bir çağrı ile ilgili bir paket ise çağrının detay kayıtlarının yeni gelen pakete göre güncellenmesini sağlayan en az bir SIP durum makinesini içeren en az bir çağrı inceleme cihazı,

- bahsedilen çağrı inceleme cihazı vasıtasıyla elde edilen çağrı detay kayıtlarının arayan, aranan ve arayan/aranan olarak birleştirilmesinin sağlayan en az bir toplayıcı,

- bahsedilen toplayıcı tarafından gelen çağrı detay kayıtlarının var olan kurallar ile eşleşip eşleşmediğinin tespit edilmesini sağlayan en az bir tespit kural çalıştırıcı,

- bahsedilen toplayıcıyı ve bahsedilen tespit kural çalıştırıcıyı içeren en az bir saldırı tespit cihazı,

- bahsedilen trafik kontrol birimini ve bahsedilen engelleme kural çalıştırıcıyı içeren, bahsedilen tespit kural çalıştırıcı da gelen çağrı detay kayıtlarının, kurallar ile eşleşmesi durumunda, oluşturulması istenilen kural ile ilgili bilgi iletildiği ve bahsedilen saldırı tespit cihazından gelen bilgiler de kullanılarak bir engelleme kuralı oluşturulmasını sağlayan en az bir saldırı engelleme cihazın,

- bahsedilen çağrı inceleme cihazı içerisinde konumlandırılan, birleştirilen çağrı detay bilgileri engelleme kuralı ile eşleşirse, bahsedilen saldırı engelleme cihazına tarafından bilginin iletildiği ve çağrı detay kayıtlarının incelenerek, var olan çağrıyı sonlandırabilen bir mesaj oluşturulmasını sağlayan en az bir çağrı sonlandırıcı,

- bahsedilen sisteme kullanıcı tarafından kuralların girilmesini sağlayan en az bir kullanıcı ara yüzü

içermektedir.

Buluşun alternatif bir yapılanması, çağrı detay kayıtlarının ve bahsedilen saldırı tespit cihazı içerisindeki bahsedilen saldırı engelleme cihazı tarafından oluşturulan kuralların kaydedildiği en az bir veri tabanı içermektedir.

Buluşun yapısal ve karakteristik özellikleri ve tüm avantajları aşağıda verilen şekiller ve bu şekillere atıflar yapılmak suretiyle yazılan detaylı açıklama sayesinde daha net olarak anlaşılacaktır ve bu nedenle değerlendirmenin de bu şekiller ve detaylı açıklama göz önüne alınarak yapılması gerekmektedir.

Buluşun Anlaşılmasına Yardımcı Olacak Şekiller

Şekil 1, buluşa konu olan telekomünikasyon dolandırıcılığı tespit ve uyarı sisteminin tercih edilen yapılanmasının blok diyagram görünümüdür.

Şekil 2, buluşa konu olan telekomünikasyon dolandırıcılığı tespit ve uyarı sisteminin ağ bağlantısı, trank ve telefonlar ile bağlantısının tercih edilen yapılanmasının blok diyagram görünümüdür.

Parça Referanslarının Açıklaması

A. Telekomünikasyon dolandırıcılığı tespit ve uyarı sistemi

B. Telefon santrali

C. Telefon

D. Trank

E. Ağ anahtarı

1. Çağrı inceleme cihazı
2. Saldırı tespit cihazı
3. Saldırı engelleme cihazı
4. Veri tabanı
5. Toplayıcı
6. Tespit kural çalıştırıcı
7. SIP durum makinesi
8. Çağrı sonlandırıcı

9. Trafik kontrol birimi

10. Engelleme kural çalıştırıcı

11. Kullanıcı ara yüzü

Çizimlerin mutlaka ölçeklendirilmesi gerekmemektedir ve mevcut buluşu anlamak için gerekli olmayan detaylar ihmal edilmiş olabilmektedir. Bundan başka, en azından büyük ölçüde özdeş olan veya en azından büyük ölçüde özdeş işlevleri olan elemanlar, aynı numara ile gösterilmektedir.

Buluşun Detaylı Açıklaması

Bu detaylı açıklamada, buluşa konu olan telekomünikasyon dolandırıcılığı tespit ve uyarı sisteminin (A) tercih edilen yapılanmaları, sadece konunun daha iyi anlaşılmasına yönelik olarak açıklanmaktadır.

Şekil 1'de, çağrı engelleme cihazını (1), saldırı tespit cihazını (2) ve saldırı engelleme cihazını içeren buluş konusu telekomünikasyon dolandırıcılığı tespit ve uyarı sisteminin (A) temsili blok diyagram şekli görülmektedir.

Şekil 2'de, telefon (C), telefon santrali (B), trank (D) ve ağ anahtarı (E) içeren sistem telekomünikasyon sistemi içerisinde telekomünikasyon dolandırıcılığı tespit ve uyarı sisteminin (A) temsili blok diyagram şekli görülmektedir.

Çağrı inceleme cihazı (1), sinyalleşme mesajlarını işleyip çağrı detay kayıtlarını oluşturan unsurdur.

Saldırı tespit cihazı (2), çağrı inceleme cihazı (1) tarafından oluşturulan çağrı detay kayıtlarının, kurallarla eşleşip eşleşmediğini kontrol eden ve saldırı engelleme cihazına (3) kurallar girilmesini sağlayan unsurdur.

Saldırı engelleme cihazı (3), saldırı tespit cihazının (3) girdiği kurallarla çağrı detaylarının eşleşip eşleşmediğini kontrol eder ve buna göre işlem yapar.

Veri tabanı (4), çağrı detay kayıtlarını, saldırı tespit cihazı (2) ve saldırı engelleme cihazı (3) kurallarını ve bu kuralların tetiklenme bilgilerini saklar.

Toplayıcı (5), çağrı detay kayıtlarını birleştirip, birleşik çağrı detay kayıtları oluşturarak tespit kural çalıştırıcıya (6) gönderen unsurdur. Toplayıcı (5), gelen çağrı detay

kayıtlarını arayan, aranan ve arayan/aranan olmak üzere üç grupta toplamaktadır. Böylece bir numaranın toplam yaptığı aramaların sayısı ve süresi, bir numaraya yapılan aramaların toplam sayısı ve süresi ve iki numara arasında yapılan aramaların toplam sayısı ve süresi ayrı ayrı ele alınarak kendi aralarında birleştirilmektedir. Bu sayede, belirli bir telefon numarasından veya belirli bir telefon numarasına yapılan aramaların toplam süresi ve sayısı ile ilgili kurallar hazırlanabilmektedir. Ayrıca yine belirli telefon numaralarının belirli telefon numaralarına yapacakları aramalar da kural ile kontrol altına alınabilmektedir.

Tespit kural çalıştırıcı (6), kural oluşturulması ve kural eşleşmesi işlemlerini yapan, eşleşme durumunda saldırı engelleme cihazına (3) bilgi gönderen unsurdur. Tespit kural çalıştırıcı (6), eğer kuralda, var olan çağrıyı sonlandırma isteği de varsa, aynı zamanda çağrı sonlandırıcıya (8) da bilgi gönderir.

SIP durum makinesi (7), çağrıları sinyalleşme protokolüne göre inceleyen ve sistemde kullanılan gerekli parametreleri ayrıştıran unsurdur.

Çağrı sonlandırıcı (8), kuralların eşleşmesi sonucu sonlandırılmasına karar verilen çağrılara, o anki çağrı durumuna uygun şekilde bir sonlandırma mesajı oluşturur ve saldırı engelleme cihazına (3) yollar.

Trafik kontrol birimi (9), paketleri trafikten alır ve dolandırıcılık tespit edilemeyenleri tekrar sunucuya yollar. Ayrıca trafik kontrol birimi (9), çağrı sonlandırıcıdan (8) gelen mesajları sunucu ve telefonlara (C) yollar.

Engelleme kural çalıştırıcı (10), saldırı tespit cihazından (2) gelen bildirimler sonucunda kurallar oluşturan ve gelen paketlerin kurallarla eşleşip eşleşmediğini kontrol eden unsurdur.

Kullanıcı ara yüzü (11), kural oluşturmak ve kurallara takılan çağrıları görmek için kullanıcıya sunulan ara yüzdür.

Gelişen iletişim ağları ve teknolojileri ile birlikte, saldırıları, çağrıların durumlarına göre tespit edebilmek için, her bir çağrı oturumunu durumsal olarak izlemek gerekmektedir. Söz konusu çağrı oturumlarının izlenmesi, herhangi bir sinyalleşme protokolü aracılığı ile ağ üzerindeki iki aygıt arasında çağrı kurulumu gerçekleştiği esnada, çağrı ile ilgili her bir durum değişimini kayıt altına alan altyapıların bulunmasını gerektirir.

Buluşa konu olan telekomünikasyon dolandırıcılığı tespit ve uyarı sistemi (A), Şekil 1'de görüldüğü üzere, temelde, telekomünikasyon paketlerinin yolu üzerinde konumlandırılan çağrı tespit cihazı (1), saldırı tespit cihazı (2) ve saldırı engelleme cihazı (3) ile ücret dolandırıcılığı girişimlerini tespit edip engellemektedir. Çağrı tespit cihazı (1), saldırı tespit cihazı (2) ve saldırı engelleme cihazı (3), iki farklı kural sistemi oluşturmakta ve bu sistemler ile işlevlerini gerçekleştirmektedir. Sistemin çalışma prensiplerini anlatırken, telefon (C) trafiğine cihazların yeni bağlandıkları, yani üzerlerinde herhangi bir engelleme kuralı olmadığı varsayılmaktadır.

İlk kural grubu olan tespit kuralları, kullanıcı tarafından kullanıcı ara yüzünü (11) kullanarak girilmektedir. Kullanıcı, farklı çağrı parametreleriyle dolandırıcılık girişimi kıstaslarını belirleyip kurallar hazırlamaktadır. Dolandırıcılık örnekleri olarak kazanç paylaşımı dolandırıcılığı ve çaldır-kapat dolandırıcılığı verilebilir:

Kazanç paylaşımı dolandırıcılığı

Bu dolandırıcılık, dolandırıcının kurbanın telefonuna (C) çağrı yönlendirme özelliği vermesiyle başlar. Bu özellik, fiziksel olarak telefona (C) ulaşabilen bir kişi tarafından (bir iş yerinin çalışanları tarafından ofis telefonlarının yönlendirilmesi gibi) verilebileceği gibi, yazılımsal telefonlarda (C) şifreyi kırarak uzaktan da verilebilir. Burada önemli olan, çağrı yönlendirme durumunda, yapılan aramanın, çağrıyı yönlendiren aboneye fatura edilmesidir. Bu dolandırıcılık türünde, yönlendirme hedefi olan numaralar, telekomünikasyon dilinde özel hat olarak geçen ve dolandırıcıya ait olan numaralardır. Bu numaraları arayan kişinin ödediği ücret, normal hatlar gibi sadece telekomünikasyon operatörü tarafından alınmaz ve bir kısmı da hattın sahibi olan kişiye aktarılır. Ayrıca, tespit durumunda yasal işlem yapılmasının zorlaşması için genelde uluslararası numaralar kullanılmaktadır.

Bu dolandırıcılık türünde, dolandırıcı, dışarıdan bir numara ile yönlendirme işlemini yaptığı hattı arar, çağrı özel hat numarasına yönlenir ve yönlendiren numara, bu hat ile olan görüşme için faturalandırılmaya başlanır. Bu tür saldırılar, genelde iş yeri telefonlarına (C), mesai saatleri dışarısında yapılmaktadır. Böylece çalışanlar ofiste olmadıkları için dolandırıcılığın fark edilmesi, bir sonraki telefon faturası dönemine kadar gizlenmiş olur.

Bu tür dolandırıcılığı tespit etmek için, buluşa konu olan sistemin bir parçası olan saldırı tespit cihazına (2) kural girilebilmektedir. Buluşa konu olan cihaz, çağrı yönlendirme

yapılan aramaları ayırt edebilme yeteneğine sahiptir ve yönlendirme çağrılarının toplam süresini de tutabilmektedir. Bu durumda, belirli bir süre boyunca yönlendirilmiş çağrı üzerinden konuşulan, mesai saatlerinin dışında ve yurtdışı numaralara yapılan aramaları tespit eden bir kural yazılabilir.

Çaldır-kapat dolandırıcılığı

Bu dolandırıcılık türünde, dolandırıcı tek bir özel numara üzerinden birçok numaraya çok kısa süreli aramalar yapar. Amaç, aranan kişilerin numarayı görmesi ve bu numarayı geri aramalarıdır. Arayan hat özel numara olduğu için, geri arayan kişiler dolandırıcıya para kazandıracaklardır. Yine suç unsurunu azaltmak için, bu saldırılar yurtdışı numaralar üzerinden yapılmaktadır.

Buluşa konu olan sistemin, bu saldırıyı önlemek için kullanacağı kural, operatör tarafından belirlenen kısa süreden daha az zaman tutan çağrıların sayısının yine operatör tarafından belirlenen eşik değerini geçmesinden oluşur. Bu kurala, çağrı kaynağının uluslararası olması veya belirli bir ülkeden geliyor olması gibi fazladan kriterlerde eklenebilir.

Kurallar hazırlanırken, kuralın gelecekteki çağrıları engellemek dışında şu anki çağrıları da kesip kesmeyeceği operatör tarafından belirlenmektedir.

Kurallar, tespit kural çalıştırıcısı (6) tarafından, veri tabanına (4) kaydedilir. Aynı zamanda tespit kural çalıştırıcısı (6) girilen kuralları, bir ağaç yapısı halinde sıralayarak hafızasında tutmaktadır. Böylece, daha sonra bir kurala erişilmesi gerektiğinde tüm kurallar tek tek taranmak zorunda kalmamaktadır.

Buluşa konu olan sistem, telekomünikasyon ağına servis sağlayıcının santral sisteminin de bağlı olduğu bir ağ anahtarı (E) ile bağlanmaktadır. Ağ anahtarı (E) üzerinde dışarıdan gelen paketler saldırı engelleme cihazına (3) yönlendirilmektedir. Paketler, trafik kontrol birimi (9) tarafından toplanıp birleştirilmekte, ardından da engelleme kural çalıştırıcısına (10) yollanmaktadır. Bu noktada daha engelleme kural çalıştırıcısında (10) hiçbir kural bulunmamaktadır. Bu nedenle, paketlerin bir kopyası oluşturularak trafik kontrol birimi (9) tarafından, çağrı inceleme cihazına (1) yollanmaktadır. Paketin kendisi de yine, trafik kontrol birimi (9) tarafından tekrar ağ anahtarına (E) yollanmaktadır.

Çağrı izleme cihazı (1), çağrıları durumsal olarak analiz ederek çağrı detay kayıtlarını oluşturmaktadır. Bunun için, mesaj, çağrı inceleme cihazı (1) içindeki SIP durum makinesine (7) yollanmaktadır. SIP durum makinesinde (7), öncelikle, mesajın bir çağrı başlatma mesajı olup olmadığı kontrol edilmektedir ve yeni bir çağrı başlatılacaksa, bu çağrı için çağrının belirli özelliklerini saklayacak yapıda olan yeni bir çağrı detay kaydı oluşturulmaktadır. Var olan bir çağrı ile ilgili bir mesaj ise de, bu çağrının detay kayıtları yeni gelen mesaja göre güncellenmektedir.

Belirli aralıklarla, oluşturulan çağrı detay kayıtları, saldırı tespit cihazına (2) gönderilmektedir. Saldırı tespit cihazında (2), toplayıcısı (5) tarafından çağrı kayıtları arayan, aranan ve arayan/aranan şeklinde üç gruba ayrılarak birleştirilir. Birleştirme sonucu ortaya çıkan verinin, var olan kurallarla eşleşip eşleşmediği tespit kural çalıştırıcısı (6) tarafından belirlenmektedir. Bu işlemin hızlı olarak gerçekleşebilmesi için, bu bölümde önceden bahsedilen ağaç yapısı kullanılacaktır. Bir eşleşme olursa, birleştirme sonucu ortaya çıkan veri saldırı engelleme cihazına (3) yollanmaktadır. Eğer var olan çağrının sonlandırılması eşleşen kuralda belirtilmişse, saldırı engelleme cihazı (3) tarafından, aynı zamanda, çağrı sonlandırıcıya (8) da bilgi yollanır.

Çağrı sonlandırıcıya (8) bilgi geldiyse, bu birim çağrı detay kayıtlarını inceleyerek, var olan çağrıyı sonlandırabilen bir mesaj oluşturmaktadır. Bu mesaj, çağrı bacaklarına yollanması için trafik kontrol birimine (9) yönlendirilmektedir.

Çağrı sonlandırılması istense de istenmese de engelleme için olan istek saldırı engelleme cihazına (3) ulaştırılır. Saldırı engelleme cihazında (3), engelleme kuralı çalıştırıcısı (10), saldırı tespit cihazından (2) gelen bilgiyi işleyerek bir engelleme kuralı oluşturmaktadır.

Artık anahtar üzerinden yeni bir paket saldırı engelleme cihazına (3) geldiğinde, öncelikle bu kural ile kontrol edilmekte, eğer eşleşme görülürse paket düşürülmektedir. Bu durumda, bu paketin kopyası çağrı inceleme cihazına (1) yollanmamaktadır.

Yukarıda parçaları ve işlevleri bahsedilen telekomünikasyon dolandırıcılığı tespit ve uyarı sisteminin çalışma prensibi şu şekildedir;

- kullanıcının, kuralları, kullanıcı ara yüzü (11) aracılığıyla sisteme girmesi,
- paketlerin, trafik kontrol birimi (9) tarafından toplanıp birleştirilmesi ve engelleme kural çalıştırıcısına (10) iletilmesi,

- engelleme kural çalıştırıcısında (10) hiçbir kural bulunmamasından dolayı, paketlerin kopyasının oluşturularak trafik kontrol birimi (9) tarafından, sıralı bir şekilde çağrı inceleme cihazına (1) iletilmesi,

- paketlerin çağrı inceleme cihazı (1) içindeki SIP durum makinesine (7) iletilmesi ve SIP durum makinesinde (7) paketin bir çağrı başlatma mesajı olup olmadığının kontrol edilmesi, yeni bir çağrı başlatılacaksa bu çağrı için yeni bir çağrı detay kaydı oluşturulması ve paket var olan bir çağrı ile ilgili bir paket ise çağrının detay kayıtlarının yeni gelen pakete göre güncellenmesi,

- çağrı inceleme cihazında (1) oluşturulan çağrı detay kayıtlarının saldırı tespit cihazına (2) iletilmesi,

- saldırı tespit cihazı (2) içindeki toplayıcı (5) tarafından, çağrı inceleme cihazı (1) vasıtasıyla elde edilen çağrı detay kayıtlarının arayan, aranan ve arayan/aranan olarak birleştirilmesi ve tespit kural çalıştırıcısına (6) gönderilmesi,

- tespit kural çalıştırıcı (6) vasıtasıyla toplayıcı (5) tarafından gelen çağrı detay kayıtlarının var olan kurallar ile eşleşip eşleşmediğinin tespit edilmesi,

- tespit kural çalıştırıcı (6) da gelen çağrı detay kayıtlarının, kurallar ile eşleşmesi durumunda, saldırı engelleme cihazına (3) oluşturulması istenilen kural ile ilgili bilgi iletilmesi,

- saldırı engelleme cihazında (3) saldırı tespit cihazından (2) gelen bilgiler de kullanılarak bir engelleme kuralı oluşturulması,

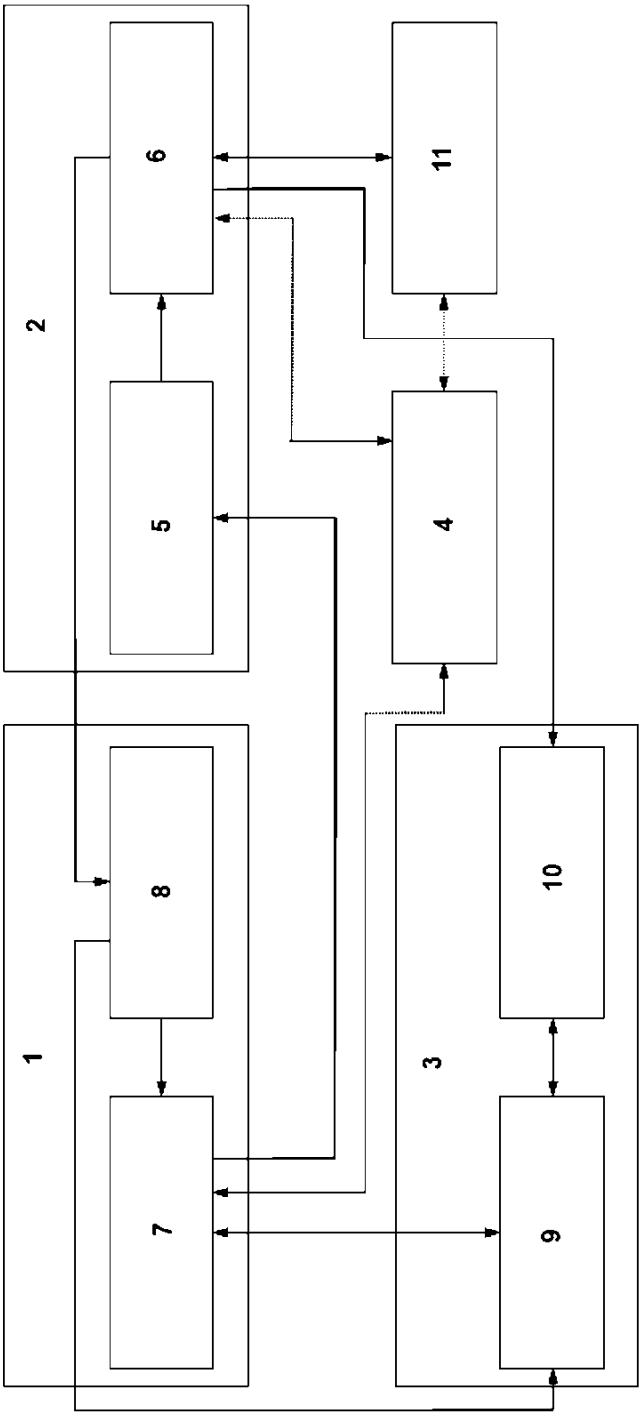
- birleştirilen çağrı detay bilgileri engelleme kuralı ile eşleşirse, saldırı engelleme cihazına (3) tarafından çağrı sonlandırıcıya (8) bilgi iletilmesi ve çağrı detay kayıtlarının incelenerek, var olan çağrıyı sonlandırabilen bir mesaj oluşturulması,

- çağrı sonlandırıcı (8) oluşturulan mesajların trafik kontrol birimi (9) vasıtasıyla sunuculara ve cihazlara iletilmesi,

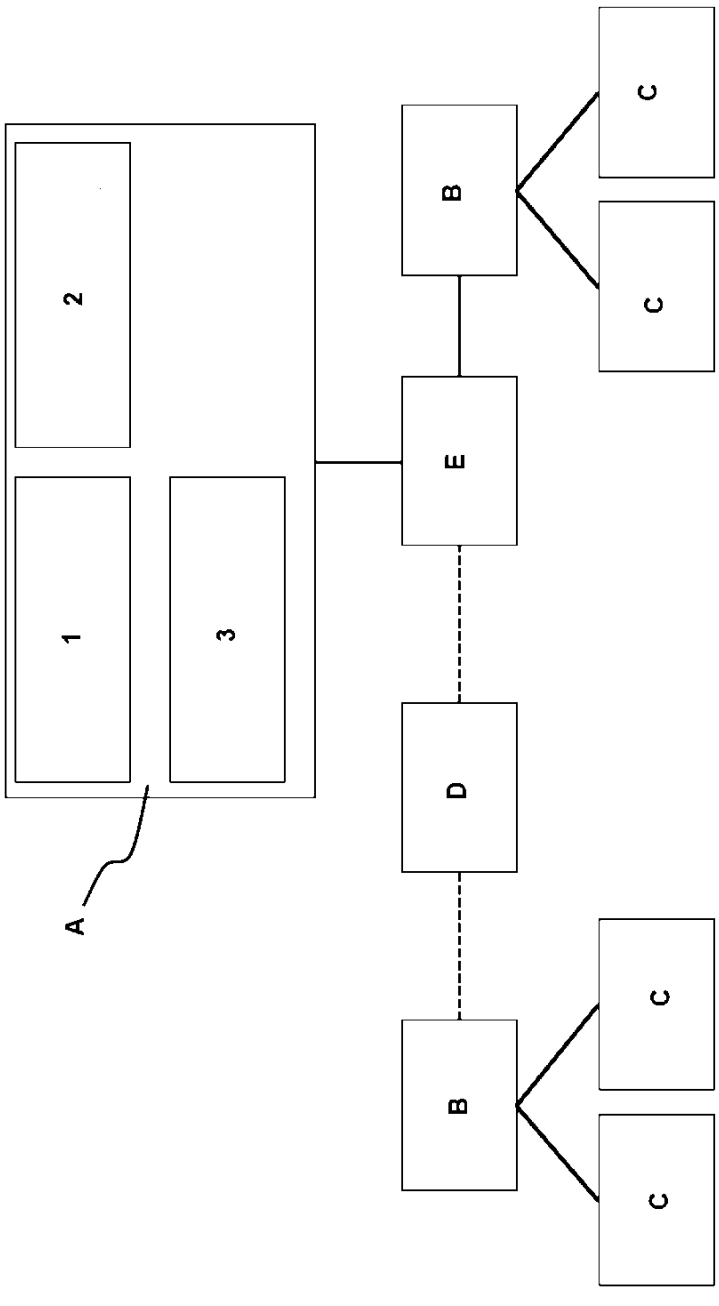
- eğer tespit kuralında çağrı kapama seçeneği varsa saldırı tespit cihazından (2) çağrı izleme cihazına (1) uyarı yollanması,

- uygun çağrı kapama mesajının saldırı engelleme cihazı (3) tarafından çağrının iki bacağına yollanması,

- çağrı detay kayıtlarının ve saldırı tespit cihazı (2) içerisindeki saldırı engelleme cihazı (3) tarafından oluşturulan kuralların veri tabanında (4) saklanması.



Şekil 1



Şekil 2