ÖZET

SIP SUNUCULARINI SERVİS DIŞI BIRAKMA ATAKLARINA KARŞI UYARLAMALI BİR GÜVENLİK DUVARI SİSTEMİ

Buluş, haberleşme alanındaki SIP ağlarında meydana gelebilecek kötü niyetli DOS ataklarına karşı koruma sağlamak üzere statik bir güvenlik duvarı yerine kendini dinamik olarak yenileyebilecek üç aşamalı bir koruma yöntemine sahip güvenlik duvarı sistemidir. Bahsedilen koruma yöntemleri; sistem tarafından güvenli olarak kabul edilen IP adresleri dışındaki herhangi bir IP ile iletişime izin verilmemesi, belirli bir süre zarfında belli bir IP'den çok daha fazla sayıda SIP mesajı formatına uymayan paket geliyorsa bu IP ile iletişimin belirli bir süreyle askıya alınması ve belirli bir süre zarfında bir IP adresinden belirlenen limitlerin üzerinde mesaj gelmesi durumunda bu IP'nin geçici süre bloklanması şeklindedir.

Şekil 1

İSTEMLER

1. Üzerinden IP/SIP mesajlarının taşındığı bir ağ sistemi (12), ağ sistemi (12) üzerinden SIP mesajı atan dış SIP sunucuları (11), dış SIP sunucularından (11) gelen mesajları işleyen SIP sunucusu (1), ağ sisteminden (12) gelen paketleri engelleyen ya da SIP sunucusundaki (1) diğer alt sistemlere geçişe izin veren IP filtre sunucusu (7) içeren ve haberleşme alanındaki SIP ağlarında meydana gelebilecek kötü niyetli DOS araklarına karşı koruma sağlamak üzere bir güvenlik duvarı sistemi olup özelliği,
    - SIP sunucusu (1) devreye girdiğinde, SIP sunucusu (1) için güvenli olan IP'leri belirleyen bir erişim kontrol birimi (4), her bir IP'den gelen paketleri sayan ve hafızasında saklayan bir paket sayacı (5), paketlerin formatının SIP formatına uygunluğunu kontrol eden ve her bir IP için gelen bozuk paket sayısını sayan bir paket kontrol birimi (6) içeren DOS kontrol birimi (3),
    - Bahsedilen IP filtre sunucusunun (7);
        - Belirlenen düzeyin üzerinde paket gönderen IP'lerin tutulduğu bir mesaj oranı kontrol listesi (8),
        - SIP formatına uygun olmayan mesajlar gönderen IP'lerin tutulduğu bir saçmalamış düğümler listesi (9),
        - Erişim kontrol birimi (4) tarafından SIP sunucusu (1) için güvenli olduğu belirlenen IP'lerin eklendiği bir erişime izin verilmiş sunucular listesi (10)

    içermesidir.

2. İstem 1'de bahsedilen güvenlik duvarı sistemi aracılığıyla haberleşme alanındaki SIP ağlarında meydana gelebilecek kötü niyetli DOS ataklarına karşı koruma sağlamak üzere bir güvenlik duvarı yöntemi olup özelliği,
    - Bir dış SIP sunucusundan (11) ağ sistemi (12) aracılığıyla gönderilen mesajın SIP sunucusuna (1) ulaşması ile IP filtre sunucusunun (7) devreye girmesi,

- IP filtre sunucusu (7) tarafından mesaj gönderen dış SIP sunucusu (11) IP'sinin erişime izin verilmiş sunucu listesinde (10) bulunup bulunmadığının kontrol edilmesi,
- IP'nin, erişime izin verilmiş sunucu listesinde (10) bulunması durumunda, SIP formatına uygun olmayan mesajlar gönderen dış SIP sunucu (11) IP'lerinin tutulduğu saçmalamış düğümler listesinde (9) ve belirlenen sayının üzerinden mesaj gönderen dış SIP sunucu (11) IP'lerinin tutulduğu mesaj oranı kontrol listesinde (8) bulunup bulunmadığının kontrol edilmesi,
- IP'nin saçmalamış düğümler listesi (9) ve mesaj oranı kontrol listesinde (8) bulunmaması durumunda gelen mesajın DOS kontrol birimine (3) gönderilmesi,
- DOS kontrol birimine (3) yönlendirilen paketin;
    - o ait olduğu IP adresinden belirli bir süre içerisinde belirlenen limitlerin üzerinde mesaj geldiğinin tespit edilmesi durumunda ilgili IP'nim mesaj oranı kontrol listesine (8) eklenmesi,
    - o SIP formatına uygunluğunun kontrol edilmesi ve ait olduğu IP adresinden belirli bir süre zarfında belirlenen limitlerin üzerinden mesaj gönderildiğinin tespit edilmesi durumunda ilgili IP'nin saçmalamış düğümler listesine (9) eklenmesi,
    - o Erişim kontrol biriminin (4) mesaj oranı kontrol listesi (8) ve saçmalamış düğümler listesini (9) belirli aralıklar kontrol etmesi ve daha sonradan bu listeye eklenmiş olan IP adreslerini belirli bir süre sonunda listeden çıkarması,
- DOS kontrol biriminin (3) mesajı SIP çağrı işleme birimine (13) yönlendirmesi işlem adımlarını içermesidir.

3. İstem 2'ye uygun güvenlik duvarı yöntemi olup özelliği, erişim kontrol biriminin (4), gelen bir paket içerisinde erişime izin verilmiş sunucu listesinde (10) yer almayan bir IP adresine kefil olunduğu duruma rastlanması halinde bu IP adresini erişime izin verilmiş sunucu listesine (10) eklemesidir.

TARİFNAME

SIP SUNUCULARINI SERVİS DIŞI BIRAKMA ATAKLARINA KARŞI UYARLAMALI BİR GÜVENLİK DUVARI SİSTEMİ

TEKNİK ALAN

Buluş, haberleşme alanında SIP ağlarında meydana gelebilecek kötü niyetli DOS (Denial of Service-Servis Dışı Bırakma) ataklarına karşı koruma amaçlı geliştirilen adaptif bir sistem ve bu sistem aracılığıyla uygulanan bir yöntem ile ilgilidir.

ÖNCEKİ TEKNİK

Mevcut teknikte SIP sunucular ağdaki tüm IP kaynakları ile iletişime açıktır. Bu durumda mevcut sistemi DOS ataklarına karşı açık ve savunmasız konuma getirmektedir. DOS atakları sistemde iki şekilde gerçekleştirilebilmektedir;

1. Sisteme çok fazla mesaj yollayarak
2. Sisteme bozuk mesaj yollayarak

Yaygın olarak SIP ağlarında statik güvenlik duvarı kuralları tanımlanarak DOS atakları engellenmeye çalışılmaktadır. Fakat bu yöntem, yukarıda belirtilen 2. Tip atağı engellemekte başarısız kalmaktadır.

BULUŞUN KISA AÇIKLAMASI

Mevcut buluş yukarıda bahsedilen dezavantajları ortadan kaldırmak ve ilgili teknik alana yeni avantajlar getirmek üzere geliştirilmiştir.

Buluşun ana amacı, haberleşme alanındaki SIP ağlarında meydana gelebilecek kötü niyetli DOS ataklarına karşı koruma sağlayan adaptif bir sistem geliştirmektedir.

Buluşta, statik bir güvenlik duvarı yerine kendini dinamik olarak yenileyebilecek 3 aşamalı bir koruma yöntemi önerilmektedir. Bu yöntemler;

1. Erişime izin verilmiş sunucu listesi (ACL-Access Control List): sistem tarafından güvenli olarak kabul edilen IP adresleri dışındaki herhangi bir IP ile iletişime izin verilmemektedir. Güvenli IP'ler ikiye ayrılmaktadır:
    a. Sistemin veri tabanında bulunan ve sistem ayağa kaldırılırken belirlenmiş sunucu adresleri,
    b. Sistemin işleyişi sırasında adaptif olarak sisteme eklenen IP adresleridir. Bu IP adresleri sistem tarafından güvenli olarak işaretlenmiş bir sunucu referansı ile listeye eklenen IP adresleridir ve belirli bir süre sonunda bu IP adreslerine tekrar kefil olunmaz ise listeden çıkarılmaktadır.

Özetle sistem ile iletişim kurabilecek IP adresleri, güvenli olarak tanımlanmış IP'ler ile bu IP'lerin referansı ile gelen IP'lerdir. Bu yöntem ile DDOS (Dağıtık Servis Dışı Bırakma Saldırısı) ataklarına karşı da bir koruma sağlanmaktadır. Erişime izin verilmiş sunucu listesi sayesinde tanımlanmamış farklı kaynaklardan gelecek paketler engellenmekte ve güvenli olmayan adresler doğrudan bloklanmaktadır.

2. Saçmalamış düğüm kontrolü: belirli bir süre zarfında belli bir IP'den çok daha fazla sayıda SIP mesajı formatına uymayan paket geliyorsa bu IP ile iletişim belirli bir süre askıya alınmaktadır.

3. Mesaj oranı kontrolü: belirli bir süre zarfında bir IP adresinden belirlenen limitlerin üzerinde mesaj gelirse bu IP geçici bir süre bloklanmaktadır.

Mevcut buluşun yapılanması ve ek elemanlarla birlikte avantajlarının en iyi şekilde anlaşılabilmesi için aşağıda açıklaması yapılan şekiller ile birlikte değerlendirilmesi gerekir.

ŞEKİLLERİN KISA AÇIKLAMASI

Şekil 1, buluş konusu güvenlik duvarı sisteminin şematik görünümüdür.

REFERANS NUMARALARI

1 SIP Sunucusu

2 Güvenilir IP Deposu

3 DOS Kontrol Birimi

4 Erişim Kontrol Birimi
5 Paket Sayıcı
6 Paket Kontrol Birimi
7 IP Filtre Sunucusu
8 Mesaj Oranı Kontrol Listesi
9 Saçmalamış Düğümler Listesi
10 Erişime İzin Verilmiş Sunucu Listesi
11 Dış SIP Sunucu
12 Ağ Sistemi
13 SIP Çağrı İşleme Birimi

BULUŞUN DETAYLI AÇIKLAMASI

Bu detaylı açıklamada, buluş konusu yenilik sadece konunun daha iyi anlaşılmasına yönelik hiçbir sınırlayıcı etki oluşturmayacak örneklerle açıklanmaktadır.

Şekil 1 buluş konusu güvenlik duvarı sisteminin bileşenlerini göstermektedir. 'e atfen buluş konusu sistem;

- Üzerinden IP/SIP mesajlarının taşındığı bir ağ sistemi (12),
- Ağ sistemi (12) üzerinden SIP mesajı atan dış SIP sunucuları (11),
- Dış SIP sunucularından (11) gelen mesajları işleyen SIP sunucusu (1),
- SIP sunucusu (1) için güvenli IP adreslerinin tutulduğu bir güvenilir IP deposu (2),
- SIP sunucusu (1) devreye girdiğinde, SIP sunucusu (1) için güvenli olan IP'leri belirleyen bir erişim kontrol birimi (4), her bir IP'den gelen paketleri sayan ve hafızasında saklayan bir paket sayacı (5), paketlerin formatının SIP formatına uygun olup olmadığını belirleyen ve her bir IP için gelen bozuk paket sayısını sayan bir paket kontrol birimi (6) içeren DOS kontrol birimi (3),
- Ağ sisteminden (12) gelen paketleri engelleyen ya da SIP sunucundaki (1) diğer alt sistemlere geçişe izin veren IP filtre sunucusu (7) ve bahsedilen IP filtre sunucusu (7);
    - o Belirlenen düzeyin üzerinde paket gönderen IP'lerin tutulduğu bir mesaj oranı kontrol listesi,

- SIP formatına uygun olmayan mesajlar gönderen IP'lerin tutulduğu bir saçmalamış düğümler listesi (9),
- Erişim kontrol birimi (4) tarafından SIP sunucusu (1) için güvenli olduğu belirlenen IP'lerin eklendiği bir erişime izin verilmiş sunucular listesi (10),

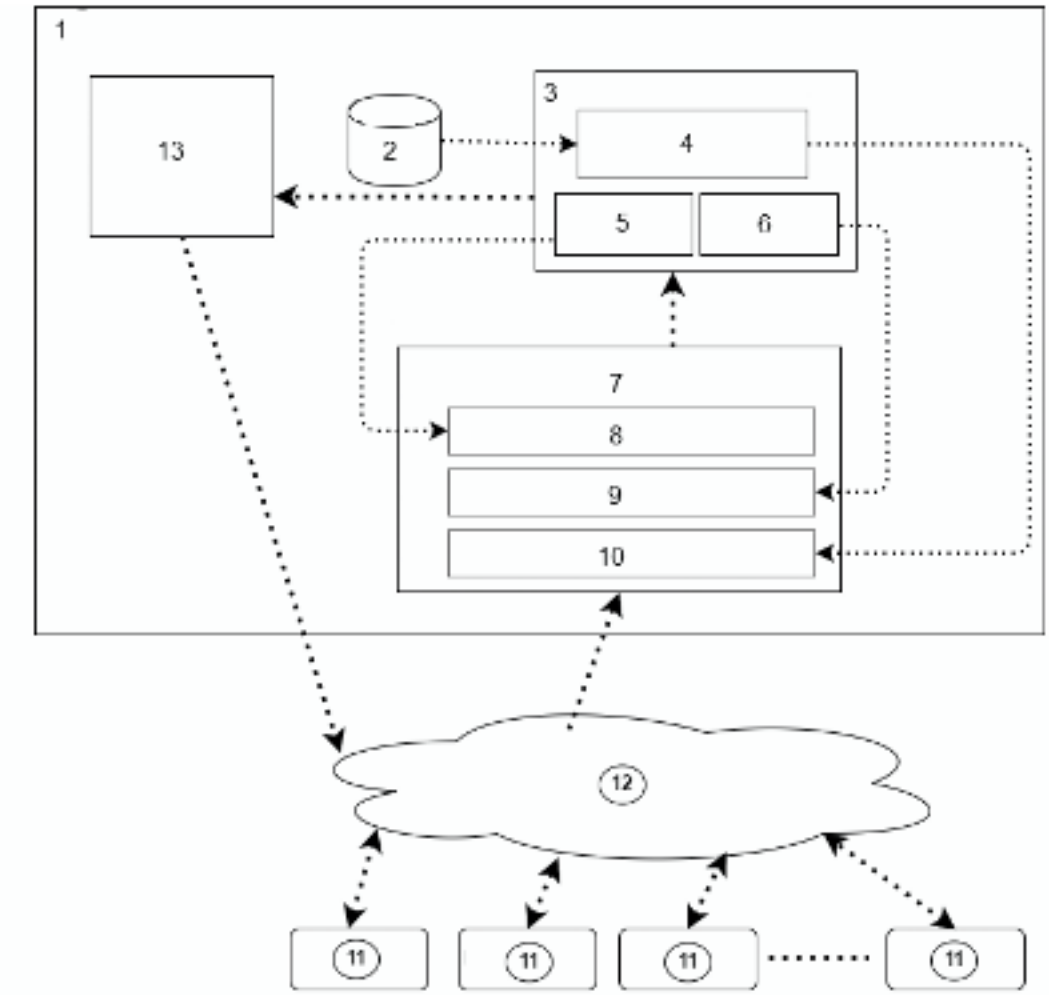
- Gelen SIP çağrıların işlendiği bir SIP çağrı işleme birimi (13) içermektedir.

Buluş konusu sistemin işleyişi şu şekildedir. SIP sunucusu (1) devreye girdiğinde, DOS kontrol biriminin (3) erişim kontrol birimi (4), SIP sunucu (1) için güvenli olan IP adreslerini, IP filtre sunucusunun (7) erişime izin verilmiş sunucu listesine (10) eklemektedir.

Bir dış SIP sunucusundan (11) SIP sunucusuna (1) ağ sistemi (12) aracılığıyla bir paket ulaştığında paket önce IP filtre sunucusuna (7) girmektedir. Burada öncelikle paket gönderen dış ı IP sunucusunun (11) erişime izin verilmiş sunucu listesinde (10) olup olmadığı kontrol edilmektedir. Eğer sunucu IP'si bu listede var ise saçmalamış düğümler listesi (9) ve mesaj oranı kontrol listelerinde (8) kontrol gerçekleştirilmektedir. Sunucu IP'si saçmalamış düğümler listesinde (9) yer almıyor ve IP tarafından gönderilen mesajlar belirli bir süre zarfında belirlenen mesaj gönderim limitini aşmıyor ise gelen paket DOS kontrol birimine (3) yönlendirilmektedir. Aksi takdirde gelen paket SIP çağrı işleme birimine (13) ulaştırılmayıp düşürülmektedir.

DOS kontrol birimine (3) yönlendirilen paketler, paket sayacı (5) tarafından ait oldukları IP adreslerine göre ayrılıp sayılmaktadır. Belirli bir süre zarfında, bir IP adresinden, belirlenen limitlerin üzerinde mesaj gelmesi durumunda bu IP mesaj oranı kontrol listesine (8) eklenmektedir. Paket kontrol birimi (6) ise gelen paketlerin SIP formatına uygunluğunu kontrol etmekte ve belirli bir süre zarfında belirlenen limitlerin üzerinde bozuk formatlı paket gelmesi durumunda bu IP adresini saçmalamış düğümler listesine (9) eklemektedir. Erişim kontrol birimi (4), mesaj oranı kontrol listesini (8) ve saçmalamış düğümler listesini (9) belirli aralıklarla kontrol etmekte ve paket sayacı (5) ile paket kontrol birimi (6) tarafından listeye eklenmiş IP adreslerini belirli bir süre sonra listelerden çıkartmaktadır.

Erişim kontrol birimi (4), eğer gelen pakette erişim izni verilen sunucu listesinde olmayan bir IP adresine kefil olunduğu durumuna rastlarsa bu IP adresini erişime izin verilmiş sunucu listesine (10) eklemektedir. DOS kontrol birimi (3) bu kontroller sonrası gelen paketleri SIP çağrı işleme birimine (13) yönlendirmektedir.



Şekil 1