Blokzincir Tabanlı Ağ Erişim Kontrol (NAC) Yönetimi İçin Alternatif Modeli ve Tasarımı

Çağatay KORKUÇ
Tuncay DOĞANTUNA
Prof. Dr. Erkan AFACAN
Doç. Dr. Gazi Erkan BOSTANCI

25-26 Eylül 2019, İstanbul

Siber Uzayda Evrimleşen Siber Saldırılar

- DDoS : Dağıtık Servis Dışı Bırakma
- SQL Enjeksiyonu
- Sosyal Mühendislik
- Virüsler, Botnet, Spam
- Fidye Yazılımları (Ransomware)
- APT: Gelişmiş Israrcı Tehditler
- Zero-Day: Sıfırıncı Gün Saldırıları

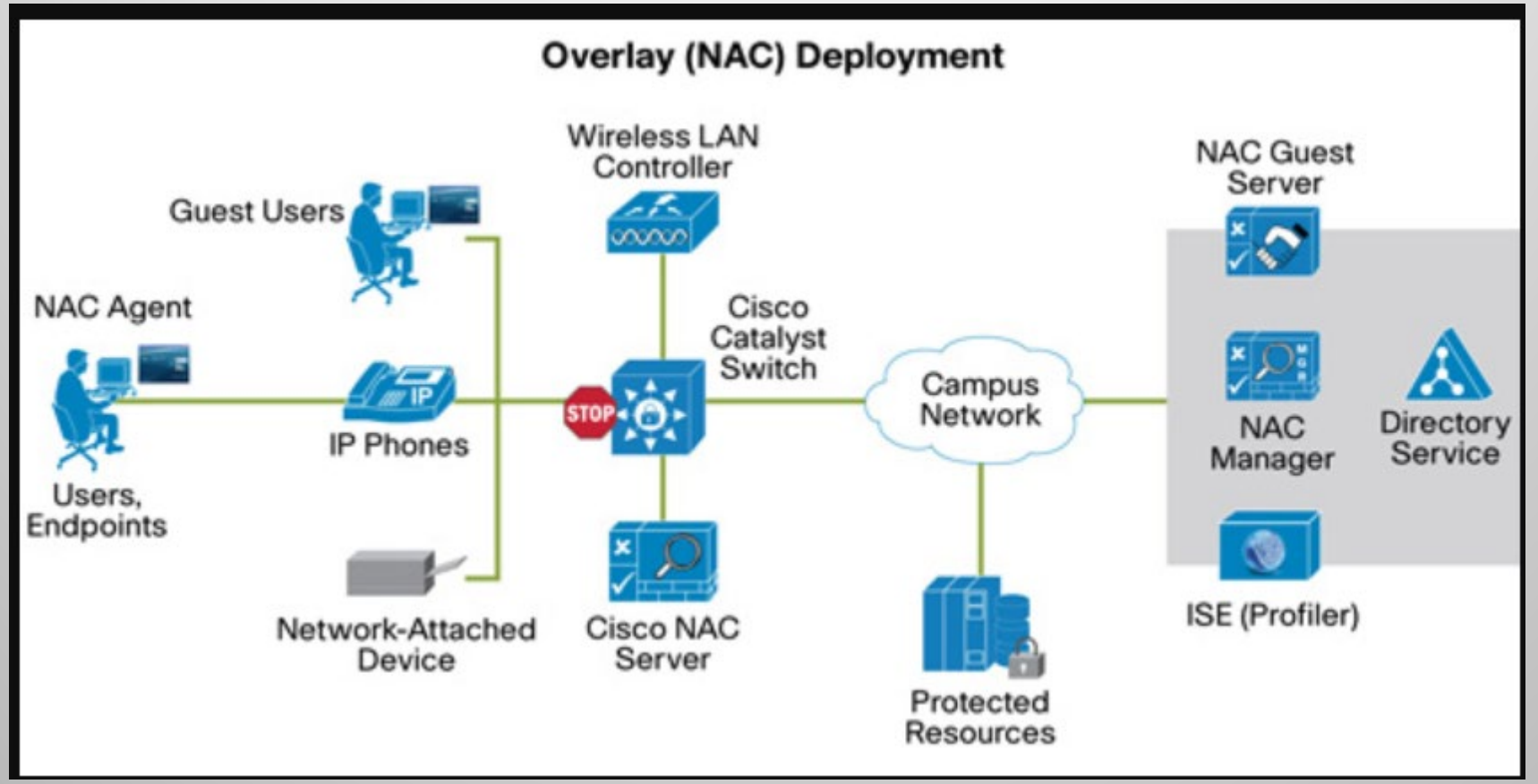
Siber Saldırganlar için En Kolay Fırsat

- Ağ Erişim Kontrolü (NAC) Ürünü olmayan Kurumsal yerel ağ yapısı
- Bilinçsiz Domain kullanıcısı
- Zafiyetli IoT cihazlar
- Bilgi Bilinçsiz personel
- Misafir kullanıcı
- Insider Threat [2]

Ağ Erişim Kontrolü (NAC) Çözümü

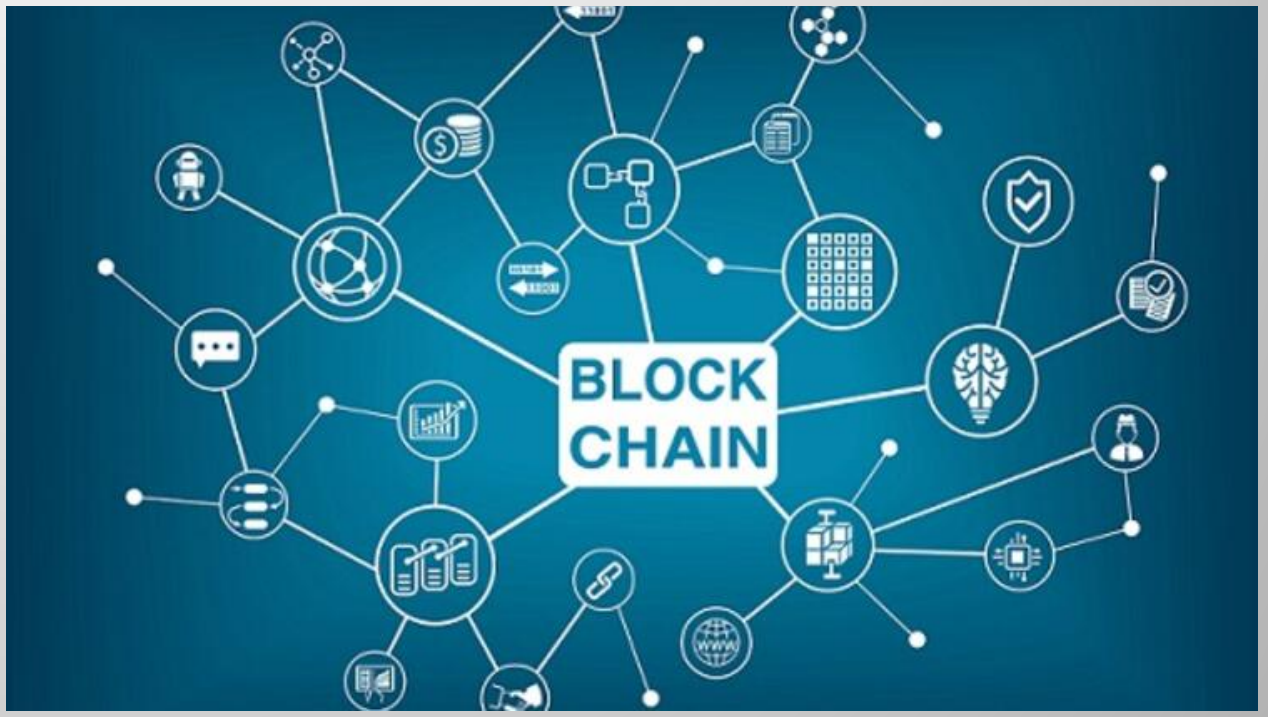
- Sisteme fiziki olarak dahil olmaya çalışan kablolu/kablosuz kullanıcı ve cihazların gerekli ağ/sistem/güvenlik bilgilerini çeker.
- Kurumsal Ağ Güvenliği politikaları ile uyumlu ise, izin verir, değilse bloklar.
- ARP Zehirleme, Switch Port VLAN değiştirme, ACL Atak gibi yöntemler
- Mevcut Ürünler, merkezi olarak kurgulanmış fiziksel veya sanal sunucular üzerinden servis vermektedir.
- Yönetimi için, üzerinde birkaç tane yönetici(administrator) kullanıcı tanımlanır.
- Sızma testi (pentest) çalışmalarında tehdite açık zafiyetler barındırabilir.

Mevcut Ağ Erişim Kontrolü (NAC) Mimarisi



Blokzincir Teknolojisi (BZT)

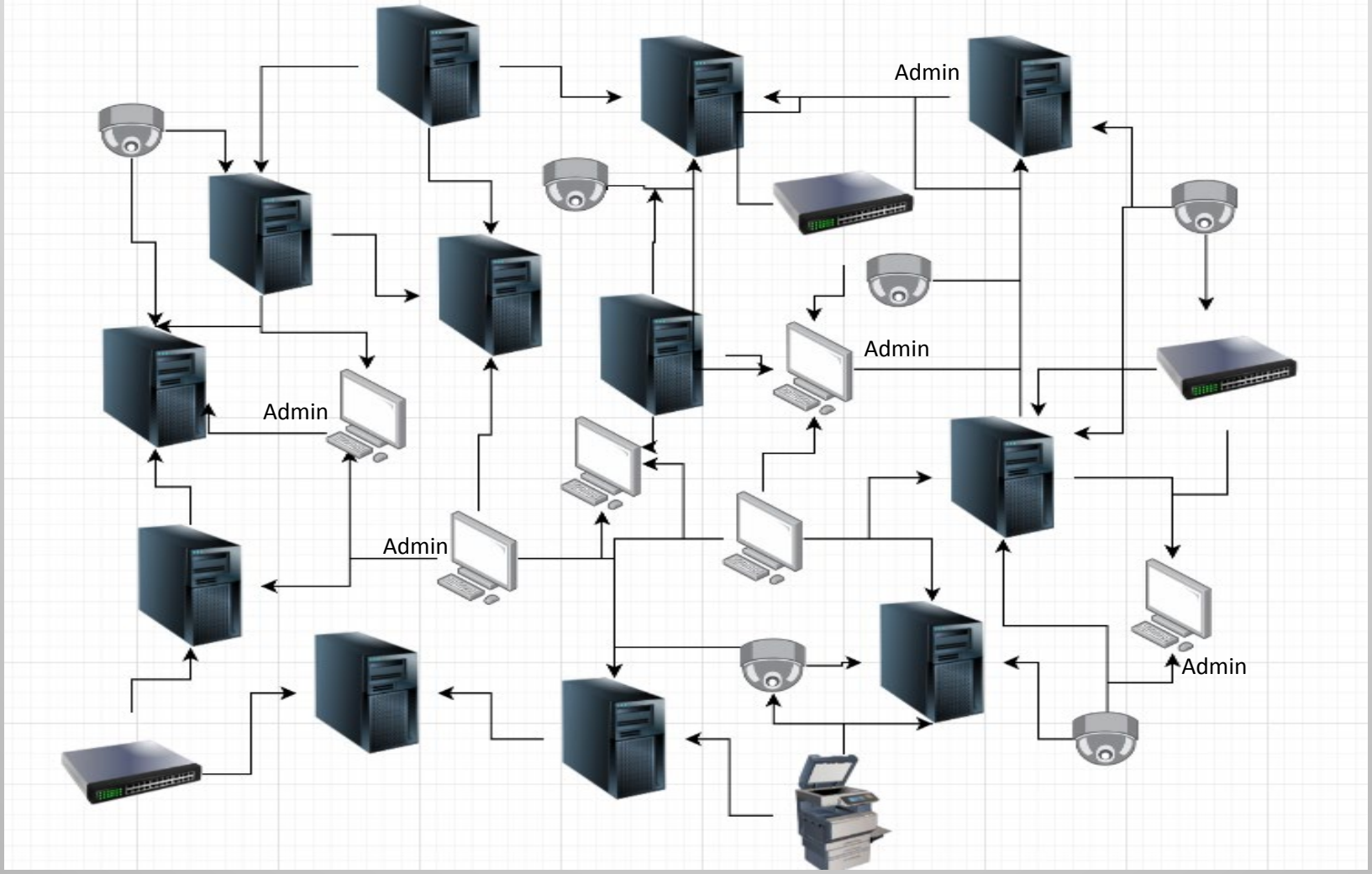
- Özet fonksiyonları (SHA256)
- Sayısal imza algoritmaları
- Dağıtık Kayıt Defteri
- Blok Yapısı
- Akıllı Sözleşmeler



Neden BZT ?

- Merkeziyetsiz ve dağıtık ağ yapısı ile güç ve riski dağıtma
- Özet fonksiyonu ve Açık Anahtar Kriptografi Altyapısı ile değiştirilemezlik, bütünlük ve güvenin garantilenmesi
- Mutabakat Algoritmaları ile katılım sağlayan taraflar arasında şeffaf bir güven mekanizması
- Otonom çalışan Akıllı sözleşmeleri stabil çalıştırması

Blokzincir Tabanlı NAC Çözüm Mimarisi



BZ Tabanlı NAC Çözümü Akış Şeması

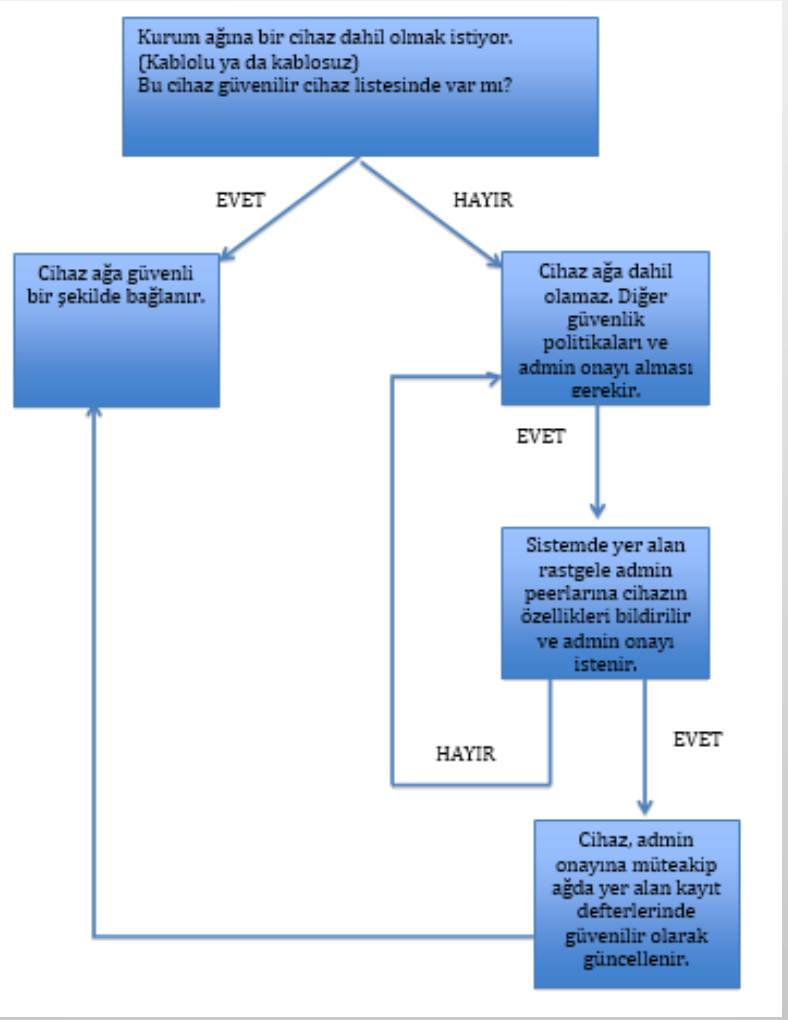
1. Ağa dahil edilecek tüm IP alan cihazların listesi (Mac adresleri, ARP tablosu, Domain bilgisi, WMI ve ağ özellikleri) oluşturulur. Bu liste aslında blokzincirinin ilk bloğu olan genesis bloğunun içinde yer alacak olan bilgidir. Bu bilgileri özetleme (hash) fonksiyonu ile özetlenir.
2. Güvenilir cihaz listesi ağa dahil olacak tüm bilgisayar ve sunuculara bir ajan (agent) yardımıyla kurulur. (Bu liste dışında yer alan tüm cihazlar yani tüm mac adresleri güvensiz olarak kabul edilir.)
3. Ajan kurulu her cihaz, blokzincir ağının dağıtık kayıt defterlerini oluşturur. Bu çalışmadaki NAC yapısı için kurulan örnek ağ Şekil 1'de yer almaktadır.

BZ Tabanlı NAC Çözümü Akış Şeması

4. Ağa bağlanan herhangi bir cihazın, güvenilir cihaz listesinde olup olmadığına bakılır. Güvenilir cihaz listesinde ise cihaz ağa bağlanır. Aktif olmayan bir cihazın MAC adresinin kullanılmaması için, domain bilgisi, makine adı ve son güncelleme gibi bilgiler defterde kıyaslanacaktır.

5. Güvenilir cihaz listesinde olmayan cihazlar için, ajan kurulu cihazlardan (Microsoft tabanlı domain sistem ve ağ mimarisinde SCCM, yani konfigürasyon yönetim konsolu gibi 3. parti araçlar sayesinde) rastgele olarak seçilen cihazlar ile bazı özellikleri incelenir (Domaine dahil olup olmadığı, antivirüs programı içerip içermediği, güncellemelerin olup olmadığı gibi). Bu özellikler, akıllı sözleşmeler (smart contract) aracılığı ile kontrol edilir. Eğer özellikleri tam ise, ağda yer alan yönetici eş'lere (admin peer) cihazın güvenilir olup olmadığı sorulur. Eğer yönetici eş'ler mutabakata göre, örneğin yüzde 50'den fazlası cihazın güvenilir olduğunu onaylarsa, cihaz ya da yeni kullanıcı (misafir de olabilir), ağa dahil olur.

BZ Tabanlı NAC Çözümü Akış Şeması



Protokol Tasarımı

- PBFT: Pratik Bizans Hata Toleransı Mutabakat Algoritması
- $|n-1| \div 3$ hatalı ya da kötücül kullanıcı/cihazı tolere edebilir
- Yetkili kullanıcılar, Genesi blokta belirtilip açık anahtarla tanımlanması
- Mutabakat mekanizması üzerinde rastgele seçim fonksiyonu
- Güvenlik analizi:
- PBFT'nin yapısı ve imza planı zorayıcılığı
- Yetkili yönetici kullanıcıların, ağdaki faaliyetleri takibi

Sonuç

- Akıllı sözleşmeler ile cihazın domainde olup olmadığı, cihazda ilgili güvenlik programlarının ya da güncellemelerinin olup olmadığı gibi kontroller yapıldıktan sonra ilgili yöneticilerin önüne düşeceğinden hata payı ortadan kalkacaktır.
- Yöneticiler ağ içerisinden rastgele olarak seçileceğinden, insan hata payı düşmüş olacak. Kullanılacak mutabakat sistemi ile rastgele seçilen yöneticilerin yüzde 50'sinden fazlası onaylamadan, cihaz ağa dahil olamayacaktır.

Sonuç

- İlk başta oluşturulan güvenli cihaz listesi tüm bilgisayarlara kurulacağından, aslında ürünün log (kayıt) bilgisi de blokzinciri ağı üzerinde tutulmuş olacaktır. Böylece, değiştirilmesi mümkün olmayacaktır. Ayrıca gelecek çalışması olarak, log yönetim sisteminin de, bu sistem ile entegrasyonu üzerine model ve tasarım da geliştirilebilir.
- Tüm bu özellikler göz önüne alındığında, NAC çözümü gibi mevcut bir ağa erişimi kontrol eden siber güvenlik ürününün, blokzincir gibi ağa ihtiyaç duyan bir teknoloji ile entegre olması, sistemi daha güvenli ve daha şeffaf bir hale getirebilecektir.
- BZT kullanarak, kurum içi yerel ağa dahil olan bütün cihazlar ve kullanıcılar arasında şeffaf bir mutabakat mekanizması sağlayan güvenilir bir NAC çözüm platformu önerilmektedir.

TEŞEKKÜRLER, SORULAR ve KATKILAR