VIPROY
Information Security

NGN ve VoIP Ağları Güvenlik Denetimi

Fatih Özavcı

Bilgi Güvenliği Araştırmacısı ve Danışmanı

fatih.ozavci at viproy.com viproy.com/fozavci

whois

VIPROY Information Security

- Bilgi Güvenliği Danışmanı @ Viproy / Turkey
- 10+ Yıl Sistem Sızma Denetmenliği
- 800+ Sızma Denetimi, 40+ NGN/VoIP Denetimi
  - NGN/VoIP Sistemleri Güvenlik Denetimi
  - Mobil Uygulama Güvenlik Denetimi
  - IPTV Sistemleri Güvenlik Denetimi
  - Sıradan Denetimler (Ağ Altyapısı, Web, SOAP/XML)

- Viproy VoIP Penetration Testing Kit
- Hacking Trust Relationships Between SIP Gateways

traceroute

VIPROY Information Security

- VoIP Ağları Neden Güvensiz ?
- Neden Yeni Araç, Yeni Modüller ?
- Denetim Süreci
  - Keşif ve Bilgi Toplama
  - Kayıt Olma
  - Çağrı Testleri
  - Çağrı Kayıtları ve Faturalandırma Saldırıları
  - Servis Engelleme

- Anlatılamayacak Konular
  - Sahte Servis Kullanımı ve Kimlik Toplama
  - Sunucu ve İstemci İçin Fuzz Testleri
  - İleri Düzey Fuzz Testleri ve Yeni Yöntemler
  - SIP Sunucusu Güven İlişkileri Analizi

info

VIPROY Information Security

- SIP – Session Initiation Protocol
  - Sadece Çağrı Sinyalleşmesi Olarak Kullanılır
  - SDP Protokolü ile Genişletilmiştir
- NGN – Next Generation Network
  - TDM ve PSTN Ömrünü Tamamladı
  - SIP, H.248 / Megaco, RTP, MSAN/MGW
  - Akıllı Müşteri Modemleri ve Cihazları
  - Yönetim Kolaylığı
  - Güvenlik Gerekli Değil, Sanki?

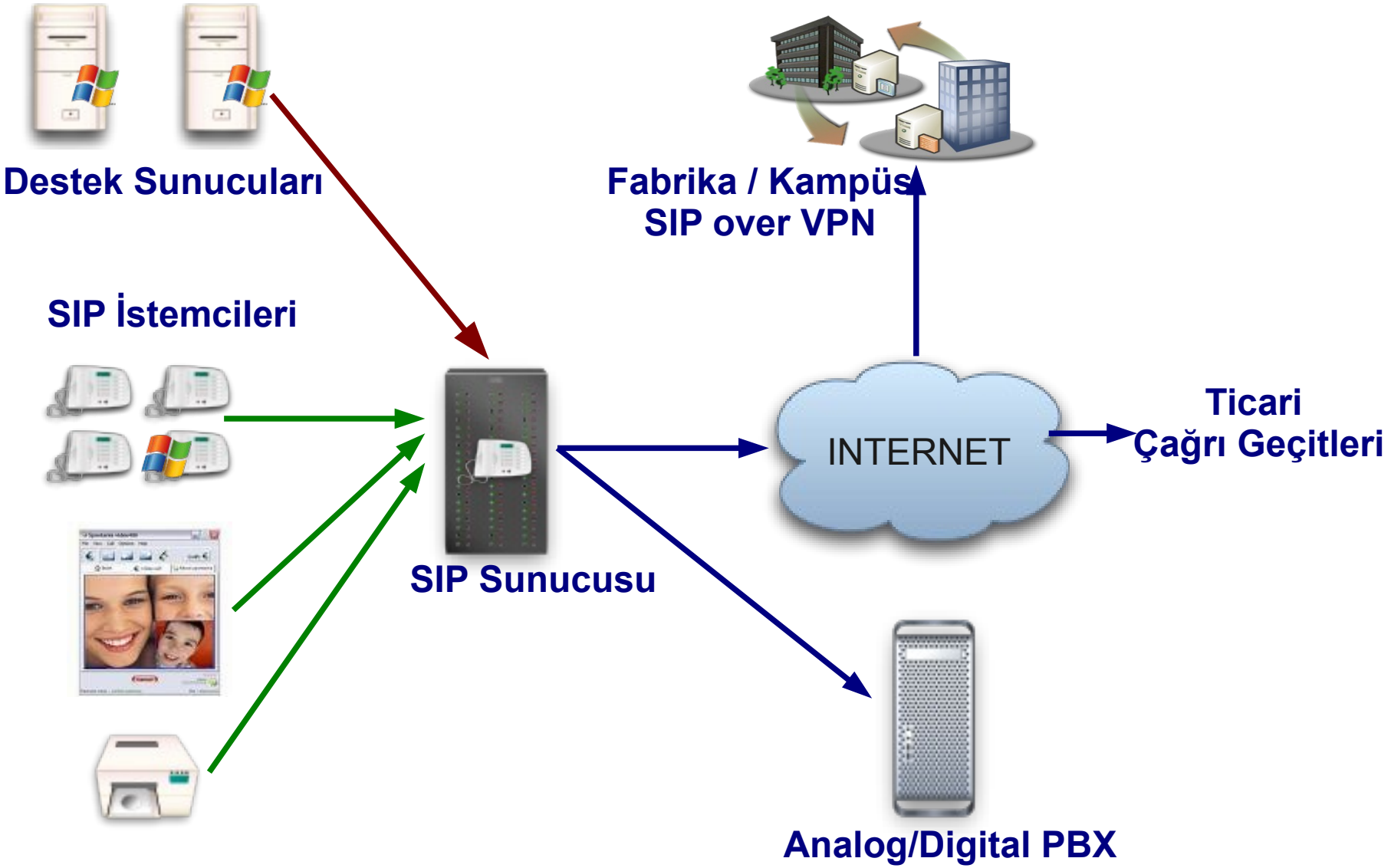
- Yeni Nesil! Çünkü Biz Öyle Söylüyoruz!

Yöneticiler Sanır ki...

VIPROY Information Security

- VoIP Ağları Ayrıştırılmış ve Kapalı Bir Ağ
  - Çoğu Operatörün Altyapısı Fiziksel Olarak Erişime Açıktır
  - Yetersiz Ağ Bölümlendirme
  - Güvensiz Sanal Özel Ağlar (IPSec, MPLS)
- VoIP Saldırıları Yüksek Düzey Bilgi Gerektirir
  - Doğru Araçlarla Bilgi Dahi Gerekmez ki Konu da Budur!
- Çoğu VoIP Saldırısı, Ağ Temellidir veya Ücretlendirme İstismarıdır
  - Çağrı Temelli Servis Engelleme Cevap Temelli Dağıtık Servis Engelleme
  - Müşterileri Casusluk veya Çıkar için Yasadışı İzleme ve Dinleme
  - Oltalama, Sahte Eğlence ve Çıkar için Çağrı Açma, Katma Değerli Servis İstismarı
- VoIP Cihazları Gayet Güvenli Yapılandırılmıştır
  - Çoğu Operatör ve Üreticinin Güvenlik Gereksinimleri Konusunda Fikri Yoktur
  - Parolasız SIP Hesapları, Güven İlişkileri, Yönetim Problemleri
  - Eski Sürüm ve Güvensiz Yazılımlar (Özellikle Veritabanı,VAS,CDR,İşletim Sistemi)
  - Güvensiz Altyapı Servisleri (TFTP, Telnet, SNMP, FTP, DHCP, Soap Servisi)

Dahili IP Telefon Yapısı



Ticari IP Telefon Servisleri

VIPROY Information Security

VAS, CDR, DB Sunucuları

Müşterileri

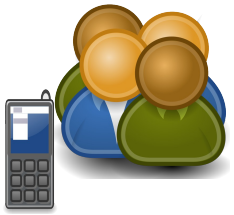
MSAN/MGW
PSTN/ISDN Dağıtımı

SDP Sunucuları

MPLS

Soft Switch
(SIP Snucusu)

INTERNET



Mobil
Müşteriler

RTP, Proxy
Sunucuları

Güvenilen
Çağrı Geçitleri

Viproy

VIPROY Information Security

- Viproy, "Vulcan"ca Bir Kelimedir, "Çağrı" Anlamındadır
- Viproy VoIP Penetration and Exploitation Kit
  - Metasploit için Test Modülleri, MSF Lisansı
  - Eski Teknikler, Yeni Yaklaşım
  - Yeni Modül Geliştirmek için Geliştirme Kütüphanesi
  - Özel Başlık Desteği, Kimlik Doğrulama Desteği
  - Test İçin Yeni Araçlar; Güven Analizi, Proxy, Sahte Servis
- Modüller
  - Options, Register, Invite
  - Brute Forcers, Enumerator
  - SIP Trust Analyzer
  - SIP Proxy, Fake Service

Temel Keşif Analizi

VIPROY Information Security

- SIP Servislerinin ve Amaçlarının Keşfi, Doğrulanması
- Kulanılabilir Yöntem ve Özelliklerin Keşfi
- SIP Yazılımları ve Zafiyetlerinin Keşfi
- Hedef Numaraları, Kullanıcılar ve Alan Adlarının Keşfi
- Kimlik Doğrulamasız Kayıt (Trunk, VAS, Çağrı Geçidi)
- Geçerli Hesapları ve Parolalarını Saptamak
- Kayıt Olmaksızın Çağrı Açmak
- Bir Çağrı Geçidinden Çağrı Açmak
- Çağrı Sahteciliği (Kimlik Doğrulamadan/Doğrulayarak)

- Viproy Pen-Testing Kit ile Keşif Otomatize Yapılabilir

Temel Saldırı Analizi

VIPROY Information Security

- Ücretsiz Çağrı, Çağrı Sahteciliği, Ek Servislerin İstismarı
- Ücretsiz Uluslararası Çağrı, Çağrı Limitlerinin Aşılması
- Sahtecilik Yöntemleri
  - Via , From
  - P-Asserted-Identity, P-Called-Party-ID, P-Preferred-Identity
  - ISDN Calling Party Number, Remote-Party-ID
- Atlatma Yöntemleri
  - P-Charging-Vector (Sahtecilik, Faturalama, Kayıt)
  - Re-Invite, Update (P-Charging-Vector)

- Viproy Pen-Testing Kit Özel Başlık Bilgilerini Destekler

Servis Engelleme

VIPROY Information Security

- Şantaj için Tüm Şirket, Müşteri veya Servislerin Kilitlenmesi
- SIP Servislerinin Servis Engelleme Sorunları
  - Bozuk İsteklere Çok Sayıda Cevap→ DDOS
  - Eş Zamanlı Kullanıcı Kaydı ve Çağrı Limitleri
  - Sesli Mesaj Kutusu, Kayıt Özellikleri, Ek Servisler
  - BYE ve CANCEL ile Çağrı Düşürme
  - Tüm Hesapların Deneme/Yanılma ile Kilitlenmesi
- Çoklu Arama (Kayıt Öncesi/Sonrası, Trunk Üzerinden)
  - Tüm Numaraları Aynı Anda Aramak
  - SIP Sucusunun Çağrı Limitlerini Doldurmak
  - Pahalı Hedefleri, Özel Servisleri ve Yurtdışını Aramak

- Viproy Pen-Testing Kit Has Çok Sayıda DOS Özelliği Sunmaktadır

SIP Sunucularına Güvenlik Denetimi Uygulamaları

https://www.youtube.com/watch?v=AbXh_L0-Y5A

Referanslar

VIPROY Information Security

- Viproy VoIP Penetration and Exploitation Kit

  http://viproy.com/fozavci

  http://viproy.com/voipkit

  http://www.github.com/fozavci/viproy-voipkit

- Attacking SIP Servers Using Viproy VoIP Kit (50 mins)

  https://www.youtube.com/watch?v=AbXh_L0-Y5A

- Hacking Trust Relationships Between SIP Gateways (PDF)

  http://viproy.com/files/siptrust.pdf

- VoIP Pen-Test Environment – VulnVoIP

  http://www.rebootuser.com/?cat=371

Q ?

Teşekkürler