Telekom Sistemlerinde Fraud (Sahtekarlık)

Telekom sahtekarlığı, Telekom endüstrisinin en büyük sorunlarından biridir. Yeni nesil haberleşme teknolojilerinin *(Next Generation Nextworks, NGN)* ortaya çıkmasını takiben yeni tür hileli kazanç yöntemlerinde artış gözlemlenmektedir. Communications Fraud Control Association *(cfca.org)* 2009 yılındaki sahtekarlık girişimlerinin sebep olduğu kaybın 70 ila 78 milyar dolar arasında gerçekleştiğini tahmin etmektedir. Telekom pazarındaki rekabetçi baskılar, Telekom firmalarının sahtekarlıktan kaynaklanan gelir kayıplarının azaltılması konusunda daha etkili çalışmalar yapmaya yöneltmiştir. Telekom sahtekarlığı yalnızca telekom operatörlerinin değil, aynı zamanda son kullanıcıların da zarar görmesine neden olan kanun dışı faaliyetlerdir. Firma itibarını korumak amacı ile, müşterilere sunulan hizmetlerin yetkisiz kullanımını engellemek de Telekom operatörlerinin ilgi alanındadır.

Telekom endüstrisi, gelir artışını sağlayacak yeni tür servislerin sunulmasına olanak sağlayan NGN mimarisine doğru yol almaktadır. Yeni mimari ve alt yapının karmaşık yapısı da yeni tür hileli kazanç ve sahtekarlık türlerinin ortaya çıkmasına yol açmaktadır. Kurumlar, gelir ve müşteri kaybını engellemek, hizmet kalitesini artırmak, yasal düzenlemelere uymak ve ayrıca pazardaki itibarlarını korumak için sahtekarlık girişimlerine karşı önlem alma ihtiyacı duymaktadırlar.

Hali hazırda Sahtekarlık Denetim Sistemlerine *(Fraud Management System, FMS)* sahip olan Telekom firmaları, NGN sistemlerine geçiş yaparken, eski sistemlerin mevcut hizmetlere has tespitler yaptığını göz ardı etmeden, yeni nesil sahtekarlık girişimlerine karşı yeni güvenlik tedbirleri almalıdırlar.

FMS'ler, müşterilerin kullanım raporlarını analiz ederek sahtekarlık girişimlerini tespit etmek için tasarlanmış sistemlerdir. FMS, tipik bir veri madenciliği *(Data Mining)* uygulamasıdır[1]. FMS'ler geçmişe dönük kullanım verilerinden her müşterinin kullanım eğilimlerini belirleyen bir tür parmak izi veri tabanı oluşturulmasını sağlar.

Sahtekarlık girişimlerinin ana hedefi sistem açıklarından faydalanarak haksız kazanç sağlamaktır. Sistem açıkları teknolojiden ya da iş modelinden kaynaklanabilir. Söz konusu kazanç her zaman yasadışı olmayabilir; ara bağlantı sözleşmelerinde veya tarifelerde operatörler tarafından yapılan ihmaller de bu tür haksız kazançlara yol açabilir. Telekom hizmetlerinde sahtekarlık girişimlerine ayrıca aşağıdaki sebeplerden ötürü de girişilebilmektedir:

- Alınan hizmet için daha düşük ödeme yapmak
- Diğer suçları işlerken kimliği gizlemek
- Hizmeti sunan firmanın itibarını zedelemek

1. Tarihçe

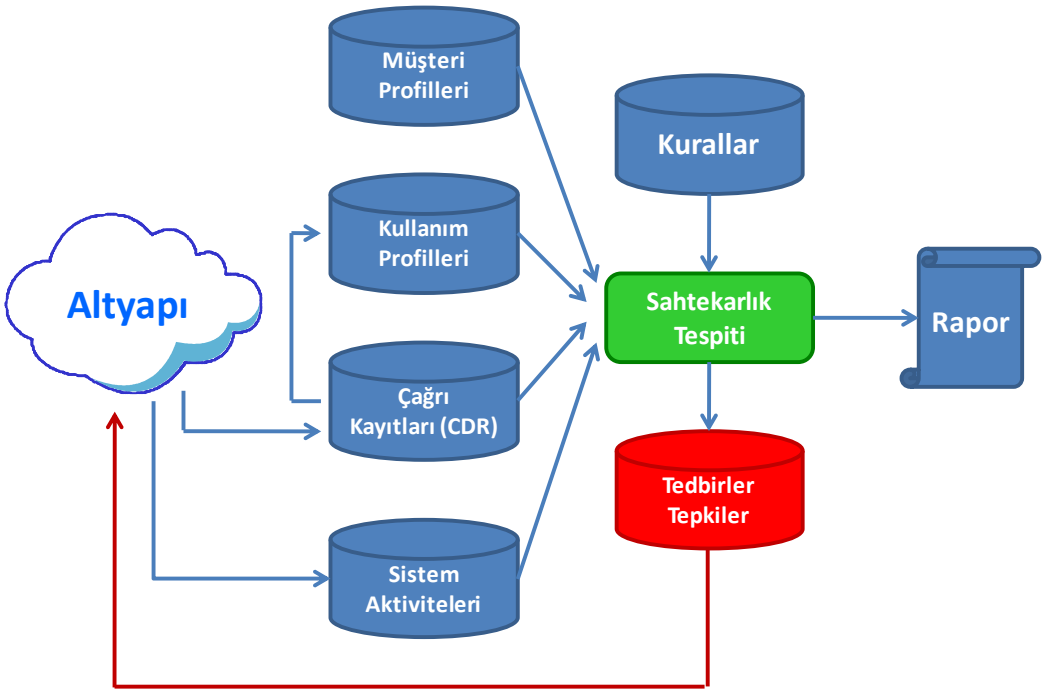
Telekom sistemlerinde sahtekarlık, telekom endüstrisinin tarihi kadar eski bir geçmişe sahiptir. En eski sahtekarlık yöntemlerinden biri, abone hattına fiziksel olarak yapılan paralel bağlantılarla, abone hesabından pahalı istikametlere arama yapılmasıdır *(Clip-on veya Teeing-in)*. Günümüzde bu, GSM altyapılarında da SIM kartı klonlama ile gerçekleştirilebilmektedir. Telekom şebekelerinde, çağrı kurulumu

[1] Introduction to Data Mining and Knowledge Discovery, http://www.twocrows.com/intro-dm.pdf

için ses frekansında tonlar ile band içi işaretlemenin kullanıldığı eski sistemlerde *(CCITT No.5 gibi)* 70'li yıllardan 90'lı yılların başına kadar kullanılan Blue Boxing yöntemi ile ücretlendirmeyi önleyerek uzak mesafe çağrıları yapmak mümkün olmaktaydı. Ancak sahte kimlik bilgileri ile abone hesabı açtırarak, ödeme yapmadan kayıplara karışmak gibi, teknolojinin kullanılmadığı çok daha yaygın yöntemleri de zikretmek gerekir *(Subscription Fraud).*

2. Yöntemler ve Önlemler

Telekom hizmetlerinde sahtekarlık pek çok şekilde gerçekleştirilebilmektedir. Burada söz konusu sahtekarlıklar yapılış şekillerine göre dört ana başlık altında incelenmektedir;



Şekil – Sahtekarlık Denetim Sistemi bileşenleri

2.1. Alt Yapıdaki Sistem Açıkları Kullanılarak Gerçekleştirilen Sahtekarlıklar (Hacking, Phreaking)

Alt yapıdaki sistem açıkları kullanılarak gerçekleştirilen sahtekarlıklar, Internet ya da telefon hatları üzerinden telekomünikasyon şebekelerinin alt yapısını oluşturan sistemlere sızılıp, doğrulama ve ücretlendirme sistemleri devre dışı bırakılarak telefon görüşmelerinin gerçekleştirilmesidir.

Yeni nesil Telekom sistemleri ve kullanılan teknoloji halen gelişmekte olup, operatörler ve kurumları, henüz çokça bilinmeyen ve önlem alınmamış birçok güvenlik açığı ile karşı karşıya bırakabilmektedir. Genel yaklaşım olarak her operatör ve kurumun olağan dışı telefon trafiklerini tespit etmek ve belirlenen eşik değerlerine ulaşıldığında sunulan hizmeti kısmen veya tümüyle durdurabilecek erken uyarı sistemlerinin kullanılması gerekmektedir.

Bir kurum ya da son kullanıcının kullanım deseni birkaç haftalık süre zarfında marjinal değişiklikler sergilemez. Geçmişe dönük belirli bir periyottaki istatistikler kullanılarak anormal kullanım değişiklikleri tespit edilebilir. Bu yöntemin yanlış alarmlar üretmesi olasıdır ancak sistemin yanlış alarm üretmesini engellemek için aynı anda birden fazla parametrenin kontrolü yapılabilir. *(Aynı anda eş zamanlı aktif çağrı*

sayısı, ortalama çağrı süresi, birim zamanda gerçekleşen çağrı sayısı analizi gibi). Bu tür bir sistem devreye alındıktan sonra elde edilen kullanım istatistikleri gerçek zamanlı ya da gerçek zamana yakın kullanım desenleri ile karşılaştırılır. Güncel kullanım verileri ile de istatistiki veriler düzenli olarak güncellenir. Aynı anda kontrol edilen parametre sayısı arttıkça sistem üzerindeki yükün artacağı göz ardı edilmemelidir. Aşağıda bu tür kontroller için kullanılabilecek parametreler listelenmiştir;

- **Eş zamanlı aktif çağrı sayısı.** Yasal olmayan bir aktivitede ilk göze çarpan anormallik, eş zamanlı çağrı sayısında olağan dışı bir artış olacaktır. Sahtekarlık girişimleri genellikle sistemlerin daha az izlendiği mesai dışı saatlerde ve hafta sonu günlerinde gerçekleştirilir. VoIP teknolojileri ile hizmet verildiği durumlarda, bir kullanıcı hesabından yapılan eş zamanlı çağrılar farklı IP adresli sistemlerden kaynaklanıyorsa sahtekarlık girişimi olasılığı yükselecektir.
- **Ortalama çağrı süresi.** Sistemin açıkları üzerinden yapılan çağrılar, sahtekarlığı gerçekleştiren kişi ya da kurumlar tarafından piyasa fiyatlarının altında satıldıklarından, yapıladıkları istikamete göre normalden daha uzun süreli çağrılar olarak göze çarpacaklardır.
- **Birim zamanda gerçekleşen çağrı sayısı** *(Başarılı ve başarısız)*. Sahtekarlık girişimlerinin hemen hepsinde, sahtekarlık girişim, tespit edilene kadar mümkün olduğunca çok çağrı sonlandırılmaya çalışıldığından, birim zamanda normalde gerçekleşenden daha çok çağrı gerçekleşmesi sahtekarlık girişimlerini ele verecektir.
- **Belirli bir istikamete doğru yapılan çağrı sayısı** *(Başarılı ve başarısız)*. İstikamet bazında çağrı süreleri hesaplanıp, sıralandıktan sonra, normal işletimde alt sıralarda olan bir istikamet tespit edilebilir. Sıralamada bir değişiklik olmasa dahi, geçmiş verilerle karşılaştırıldığında belirli bir istikamete doğru çağrı sayısı ve süresinin artması tespit edilirse, daha yüksek çözünürlükte bir analizle hangi spesifik istikametin trafik artışına sebep olduğu belirlenmelidir. Operatör tarifelerinde yüksek fiyatlı bir istikametin daha düşük fiyatla daha genel bir istikamet altında yer alması, hizmet alan kurum veya diğer operatörler tarafından istismar edilebilir.

  Ayrıca kullanıcı profiline göre olağandışı istikametlere yapılan çağrı sayısında artış da bir sahtekarlık girişimine işaret edebilir. Bu yüzden sahtekarlık analizleri yapılırken yalnızca çağrı adetleri değil, kullanıcı profili de bir parametre olarak kullanılabilir.
- **Belirli bir operatöre doğru yapılan çağrı sayısı** *(Başarılı ve başarısız)*. Yönlendirme tablosunda az sayıda istikamet için kullanılan ara bağlantılarda, anormal çağrı adetlerinin gözlenmesi durumunda da kaynak analizi yapılmalıdır.

Bu parametrelerin kontrolü, yapılan tüm çağrılar veya bir abonenin yaptığı çağrılar bazında kontrol edilebilir. Elde edilen raporlar yalnızca sahtekarlık girişimlerinin tespiti için değil, aynı zamanda Telekom firmalarının düşük kullanımlı aboneleri tespit edilerek, müşteri tarafındaki sorunların pro-aktif bir yaklaşımla çözülmesi için değerlendirilebilir. Zira kalite ve servis sürekliliği yaşayan aboneler, sunulan hizmetleri daha düşük seviyelerde kullanma eğiliminde olacaklardır.

Sahtekarlık girişiminde bulunan kişi veya kurumların yukarıda değinilen parametrelerle yapılacak analizlerde fark edilmemek için daha düşük profilli aramalar gerçekleştirebilecekleri gözden kaçırılmamalıdır. Bu yüzden yapılacak analizle yalnızca gün veya hafta gibi kısa süreli periyotlarda yapılmamalıdır.

Özellikle kurumların telekomünikasyon altyapıların kullanılan sistemlerin yapılandırma ve yazılımları sıkça güncellendiğinden, periyodik sızma testleri ile güvenlik açıkları kontrol edilmelidir. Kurum bünyesinde kullanılan ve IP ağları üzerinden telefon çağrıları kurabilen cihazlar, IP filtreleri ve Firewall'lar ile korunmalıdır. İdeal olarak VoIP teknolojileri telefon hizmeti veren firmalar, müşteri tarafında kurulan VoIP cihazlarında Internet üzerinden erişilemeyen IP adresler kullanmalıdırlar. Kurulan tüm cihazlar yalnızca güvenilen IP adresli sistemlerden çağrı kabul edecek şekilde yapılandırılmalı ve cihaz şifreleri kesinlikle fabrika çıkış değerlerinden farklı olan şifrelerle değiştirilmelidir. Cihaz şifreleri periyodik olarak güncellenmelidir.

Internet üzerinden SIP veya H.323 protokolleri ile ara bağlantı yapan operatörler, ara bağlantıları sonlandırmak için Session Border Controller cihazları ile topolojilerini saklamalıdır. Yeni nesil operatörler tipik olarak, VoIP teknolojilerini kullanarak çağrı aldıkları diğer operatörlerin trafiklerini birbirlerinden ayırmak için, aranan numaranın başına karşı taraftaki operatör tarafından nümerik bir ön ek, prefiks, eklenmesini talep ederler. IP adresi ile birlikte prefiks doğrulaması yapılarak, belirli bir prefiks ile yalnızca belirli bir kaynak IP adresli sistemden çağrı kabul edilmelidir. Firewall'lar belirtilen tüm IP adreslerinden trafiği kabul ettiklerinden dolayı, bir operatörün başka bir operatörün prefiks'i ile çağrı göndermesini engellemek için prefiks ile birlikte IP adresi doğrulaması yapılmalıdır. Örnek uygulama için "Prefix and Source IP Authentication for Incoming VoIP Traffic" [3] dökümanını inceleyiniz.

Altı haneli arama kartı PIN numaraları, yalnızca 1 milyon adet farklı numaranın üretilmesi için kullanılabilir. Yedi hane kullanıldığında bu sayı yalnızca 10 milyon adet olmaktadır. Eğer bir telekom firması 10.000 adet müşteriye sahipse, kart numaralarını tahmin etmeye çalışan bir kişi 6 haneli kart numaraları kullanıldığında 100 denemede bir, 7 haneli kart numaralarının kullanıldığı durumda 1000 denemede bir adet PIN numarasını doğru olarak tahmin etme şansına sahip olacaktır. PIN numaraları üretilirken ardışıklığı engellemek atlanan kombinasyonlar da hesaba katıldığında, geçerli olarak tahmin edilen numaraların frekansı artacaktır. Numara tahmininin elle tuşlayarak yapmak kolay bir iş değildir. Ancak bu işi yapabilecek bilgisayar yazılımları mevcuttur. PIN numaralarının tahmin edilmesine yönelik girişimlerin tespiti için ayrıca servis için kullanılan erişim numaralarına yapılan çağrılar için de ayrıca gerçek zamanlı ya da gerçek zamana yakın analizlerin yapılması gereklidir.

Sistem üzerinden gerçekleşen tüm çağrılar için çağrı detay kayıtlarının doğru bir şekilde oluşturulduğu ara bağlantı kurulumu sırasında ve ayrıca periyodik olarak kontrol edilmelidir. Örneğin bazı veri tabanı sistemleri, veri tabanındaki bazı sahaların alabileceğinden büyük değerler kaydedilmeye çalışıldığında kayıt yapmayabilirler. Kötü niyetli bir firma arayan tarafın numarasını *(Caller ID)* normalden uzun bir karakter dizisi olarak göndererek çağrı kaydı oluşturulmasını engelleyebilir.

2.2. Operatör Tarifelerindeki Açıklar ve Sunulan Hizmetin İstismarı

Operatör tarifeleri, ücretleri farklı tüm istikametleri içerecek çözünürlükte hazırlanmalıdır. Göz ardı edilen pahalı istikametler, kurumlar ve ara bağlantı yapılan diğer operatörler tarafından tespit edilerek istismar edilebilir.

Operatör hatasının kaçınılmaz olduğu durumlarda, normalden ucuza trafik kabul edilen istikametlerden dolayı ara bağlantı mahsuplaşması yapılırken zararı en aza indirmek için mahsuplaşma periyodu bir aydan daha kısa bir süre olacak şekilde *(Örneğin iki haftada bir)* düzenlenebilir. Böylelikle bir sonraki mahsuplaşma periyodundan önce zarar tespiti yapılarak, tarife düzenlemesi yapılabilir.

Ortalama kullanım istatistikleri üzerinden yapılan değerlendirmelerle oluşturulan kampanya paketleri, makul kullanım sınırı ile tüketime sunulmalıdır. GSM'de SIM Boxing, piyasadan temin edilen, özellikle kampanya hatlarının hizmetin istismar edilmesi yoluyla haksız kazanç sağlamak için kullanılan bir yöntemdir. SIM Box, VoIP ile alınan bir çağrının mobil operatör şebekesine aktarılmasını sağlar.

2.3. Bayi Sahtekarlıkları

Alt yapı sağlayan operatörden kiraladığı tool-free numaralar üzerinden arama kartları ile hizmet sağlayan bayilik sözleşmesi yapmış kötü niyetli firmalar, sunmadıkları hizmet için son kullanıcıları dolandırma girişiminde bulunabilirler. Kart üzerinde belirtilenden daha az krediye sahip kartlar piyasaya sunulabilir. Hatta bazı firmalar, alt yapıyı sağlayan operatörle hiçbir anlaşması olmadığı halde, sahte PIN numaraları ile kartlar üretip, paralel birçok kanaldan piyasaya sürerek organize dolandırıcılık girişimlerinde bulunabilirler.

2.4. Kimlik Sahtekarlığı ve Sosyal Mühendislik

Sahte kimlik bilgileri ile sahip olunan telefon hatları, pahalı istikametlere arama yapmak, SIM Box'lar ile trafik sonlandırmak ve başka suçlar işlemek için kullanılabilirler. Kendilerini emniyet birimleri ya da telefon firmalarının yetkilileri gibi tanıtıp hesap bilgilerini edinme, kredi ya da kontör talep etme girişimleri de sosyal mühendislik girişimlerine tipik örneklerdir. Teknolojinin doğrudan kullanılmadığı bu tür sahtekarlıklar en fazla karşılaşılan sahtekarlık türlerinden biridir.

3. Genel Değerlendirme

Telekomünikasyon teknolojileri ilerledikçe yeni sahtekarlık türlerinin ortaya çıkacağı muhakkaktır. Ancak trafik raporlarının, birden fazla parametre kullanılarak analizi ile erken uyarı sistemlerinin oluşturulması ve kayıpların asgari mertebede tutulması mümkündür. Günümüzde henüz gerçekleşmemiş ancak gerçekleştirilmesi olası sahtekarlık girişimlerine örnek olarak kurumların IP tabanlı telefon sistemlerine, kurum bilgisayarlarına bulaştırılacak Truva atları ve virüslerle açılacak tünellerle sızma girişimleri verilebilir. Bu yüzden kurumların dış tehditlerin yanı sıra yeni nesil dahili telefon sistemlerine IP ağı altyapısından erişimleri de denetlemesi gerekmektedir.

Her kurumun sunmuş olduğu telekomünikasyon hizmetleri, telekomünikasyon alt yapısında kullanılan sistem ve teknolojiler farklılık arz ettiğinden, her kurumun sahtekarlık girişimlerini tespit etmek için kendi güvenlik politikalarını belirlemesi, bu konuda yapılacak çalışmaların bir proje olarak ele alınarak gerekli sistemlerin *(Analiz ve raporlama)* geliştirilmesi en sağlıklı yaklaşım olacaktır.

4. Kaynaklar

1. Phreaking, http://en.wikipedia.org/wiki/Phreaking
2. The History of Phone Phreaking, http://www.historyofphonephreaking.org/
3. Prefix and Source IP Authentication for Incoming VoIP Traffic, http://www.yasinkaplan.com/docs/ipprefix.pdf
4. Telecom Fraud Management: A Strategic Perspective , http://www.equinoxis.com/fraud-management-benefits.html
5. Becker, R. A., Volinsky, C., and Wilks, A. R. (2010), "Fraud Detection in
6. Telecommunications: A Historical Perspective and Lessons Learned", American Statistical Association and the American Society for Quality TECHNOMETRICS, FEBRUARY 2010, VOL. 52, NO. 1 DOI 10.1198/TECH.2009.08136
7. VoIP Fraud List, http://www.voipfraud.net/