SS7'NİN DÜŞÜŞÜ
KRİTİK GÜVENLİK KONTROLLERİ İŞE YARAYABİLİR Mİ?

GIAC (GCCC) Gold Certification
Author: Hassan Mourad, hassan.morad@gmail.com
Translate: Özgür Koca, ozgurkoca@gmail.com

Advisor: Stephen Northcutt

Özet

SS7 iletişim ağı yapısı gereği operatörlerin kapalı ağları içerisinde düğümlerin birbirine doğal güvenleri söz konusudur. Bu kapalı ağa dahil olabilen saldırgan bu doğal güven hiyerarşisini, kullanıcının konumunu belirleme, çağrısını dinleme ve sistemi servis dışı bıkramaya kadar saldırılar düzenleyebilir. Bu güven ilişkisi ülkesel ve global ölçeklerde operatörler arasında da geçerlidir. Operatör ağına sızan birisi roaming özelliğinden ötürü otomatik olarak dünyadaki tüm operatörlerin ağları üzerinde de erişim kazanır. SS7 kapalı ve güvene dayalı bir ağ olduğu için bu konuda yapılan güvenlik araştırmaları sınırlı kalmıştır.

1. Sunuş

2014'ün ağustos ayında Washington Post gazetesinde dünyadaki herhangi bir cep telefonu kullanıcısını takip etme ile ilgili bir haber yayınlamıştı (Timberg 2014). Özellikle SS7'nin kullanıcıları takip etmeye izin veren açıklar telekom cihaz üreticileri tarafından kullanılabilmektedir. Aynı makalede üreticilerin cihaz broşürlerinde abone lokasyonunu nasıl bulduklarını anlattıklarına da değinilmektedir.

2014'ün sonlarına doğru Berlin'de Chaos Communication Congress'de SS7'nin birçok zafiyeti, araştırmacılar tarafından gözler önüne serildi. Bunlardan biri de P1 Security araştırma grubunun oluşturduğu dünya SS7 güvenlik haritasıdır. "Laurent Ghigonis and Alexandre De Oliveira from P1 Security presented their SS7 global security map(P1 Security, 2014)"

SS7 ağlarında güven yapısı operatörler arasında belli kurallar ile oluşturulmuş, sonuç olarak birbirlerine güven ilişkisi ile bağlı kapalı ve güvenilir bir ağ olarak kabul edilir. Bu güven ilişkisi açıkça artık geçerli değildir ve bu tür ağlardaki güvenlik boşluklarını analiz etmek ve bu boşlukları kapatmak için gerekli kontrolleri uygulamak için acil bir ihtiyaç oluşmuştur.

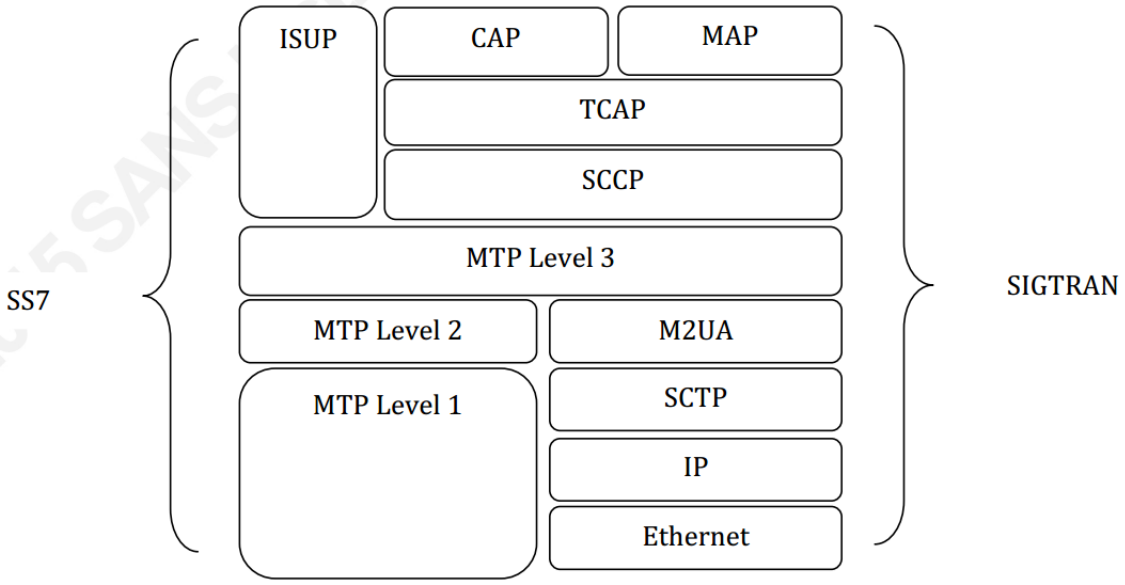
Bu açıkça artık geçerli değildir ve bu tür ağlardaki güvenlik boşluklarını analiz etmek ve bu boşlukları kapatmak için gerekli kontrolleri uygulamak için acil bir ihtiyaç artmaktadır.

Bu yazıda SS7'ye karşı saldırıları ve SS7 güvenlik açıklarını gidermek ve temel ağ güvenliğini artırmak için ilgili güvenlik denetimlerini yapmak maksadıyla kritik güvenlik kontrollerini inceleyeceğiz.

2. Çekirdek Ağ Mimarisi

3. No. 7 Sinyalleşme Sistemi

SS7 1980s in ITU-T Q.700 ile standardize edilmiş bir protokoller kümesidir. 1990 yılında yeni protokoller eklenmiştir. ETSI tarafından 2000 yılında 3GPP destek ve servisi eklenmiştir.



4. SS7 Saldırıları

SS7 doğası gereği kullanıcının konumu çağrı ve SMS detayları hakkında saldırılara açıktır. Finansal sistemler ve diğer kimlik doğrulama sistemleri de bu alt yapıya bağımlıdır ve SS7 tarafından yetkilendirilir.

4.1 Çağrı ve SMS Ele Geçirme

İletişimi ele geçirme konusu her zaman bir istihbarat faliyetinin ana amacı olmuştur. Kablolu telefonların ilk günlerinde saldırganın gidip gelen çağrıları dinlemesi için kabloya fiziksel olarak erişmesi gerekliydi.

Kablosuz iletişime geçildiğinde çağrılar bir radyo sinyali olarak havadan iletilmeye başlandı. Normalde havadan giden trafik şifrelenerek gönderilir. Şifreleme A5/1 ve A5/3 algoritmaları ile yapılır. Uzun süre önce A5/1'in kırıldığı ve ucuz radyo cihazları ve Rainbow tabloları ile çağrı transferinin deşifre edilebildiği kanıtlanmıştır (Nohl, Munant, 2010). Sonuç olarak operatörler bu zafiyetle başetmek için daha güvenli olan A5/3'ü kullanmaya başlamışlardır. Yine de SS7'nin çağrı ve sms izleme hakkında zafiyetleri olduğu yakın zamanda gösterilmiştir.

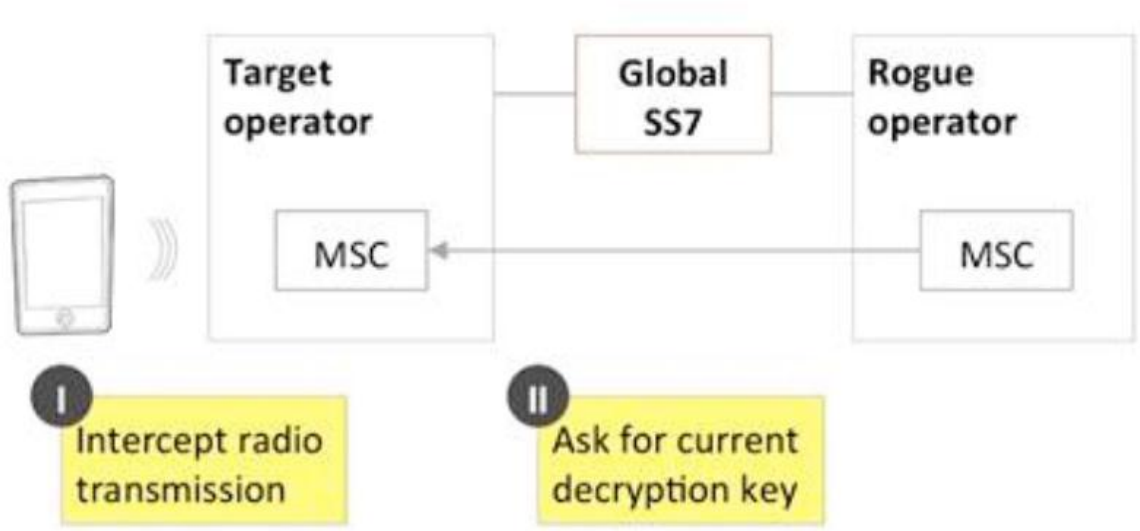
4.1.2 Çağrı yakalama ve kimlik sunma

Çağrı başlatılmadan önce kullanıcın kimliği gizli bir anahtar ile operatör tarafından teyit edilir. Bir çağrı bulunulan hücre içinde başlatıldığında ve kullanıcı konumunu değiştirdiğinde, çağrının başlatıldığı hücre üzerinden verilen yetkinin iletişimin güvenliği açısından operatör tarafından yeni hücreye de aktarılması gerekir. Bu aktarım sendIdentification isimli MAP mesajı ile gerçekleştirilir. Yeni hücre bu mesajı eski hücreye

göndererek bir yetki ister (Dryburgh, Hewet, 2005). Bu yetkinin kapsamın havadaki trafiği şifreleyen anahtarın kendisidir.

Bir saldırı senaryosunda; kurbana fiziksel olarak yakın olan saldırgan havadaki görüşme trafiğini koklar ve kaydeder. Saldırgan SS7 ağı üzerinden yeni hücrenin adresini kullanarak eski hücreye kurbanın yerine sendIdentification mesajı göndererek şifreleme anahtarını elde eder (Nohl, 2014, p7).

Bu saldırının gerçekleşememesi için iletişimin sadece o ağın meşru cihazları tarafından yürütülmesi gerekir. SS7 ağına sızma zafiyet içeren bir operatörün ağı kullanılarak gerçekleştirilir. Dolayısıyla izinsiz cihazların global ölçekte işleyen SS7 ağına dahil olmalarının engellenmesi gerekir.

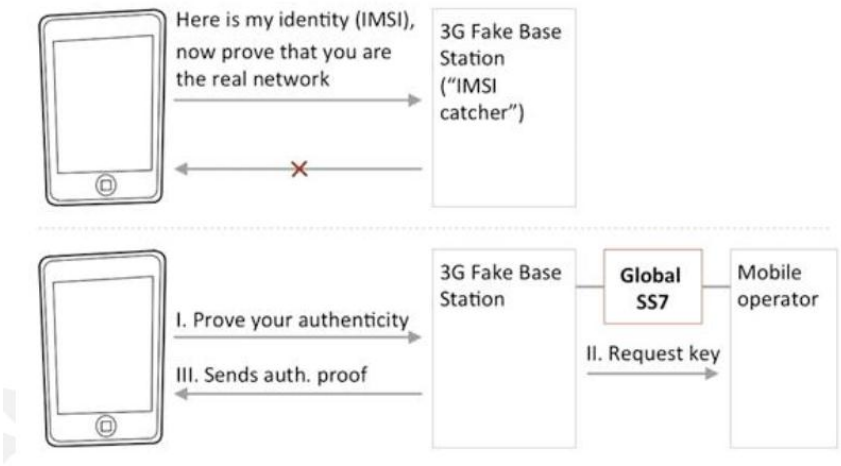


Şekil 1 - Çağrı Elegeçirme için sendIdentification Mesajı Kullanımı

4.1.2 Interception – 3G IMSI Catcher

İkinci nesil şebekelerde cihaz operatör ağı ile bir güven ilişkisi kurmaz. Bağlandığı operatör ağının güvenli bir ağ mı yoksa sahte bir ağ olup olmadığını denetlemez. Hücresel şebeke mantığında cihaz (cep telefonu) tanıtıcı kimlik bilgisi doğru tanımlamış (örneğin operatör ismi. Vodafone, XXXcell vs) cihazdaki tanımla örtüşen sinyali en güçlü ağa cihaza bağlanma eğilimindedir (Strobel, 2007). Böylece cihaz yabancı bir ağa ya da saldırganın yakınlarında konuşlandırdığı bir radyo cihazının ağına otomatik olarak bağlanır.

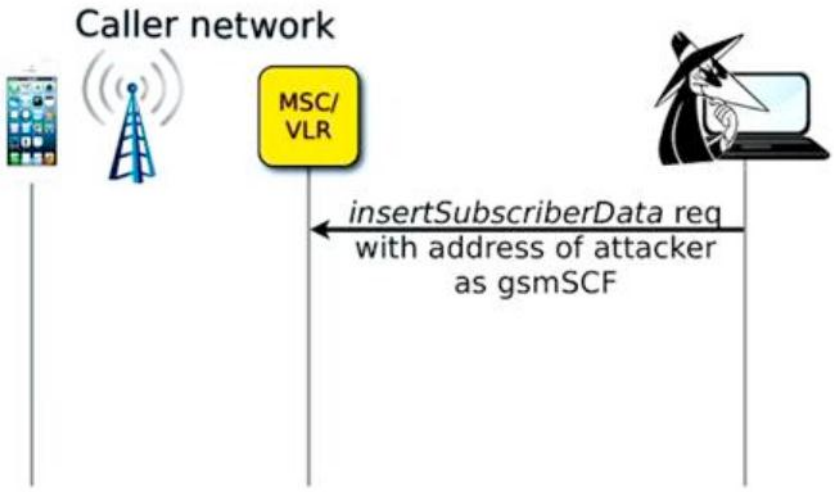
3G ağlarda bu tür bir saldırı mümkün değildir. Bir çağrı kurulmadan önce ağ, çağrı yapana geri bağlanarak kimliğini teyit eder. Ancak saldırgan SS7 ağına bağlanarak sendAuthenticationInfo isimli MAP mesajını göndererek meşru ağın kimliğini öğrenebilir Nohl, 2014, p8). Saldırgan SS7 ağına erişimi genellikle global ölçekte zafiyate sahip bir operatör ağına bağlanarak gerçekleştirir. Ne yazıkki global ölçekte dolaşımı sağlamak için kullanılan bu özellik operatör dışı ağların denetim dışında olmasından dolayı sınırlandırılması mümkün değildir. Esas sorun SS7'nin global ölçekte kapalı bir ağ oluşturmak üzere tasarlanmasından kaynaklanır.



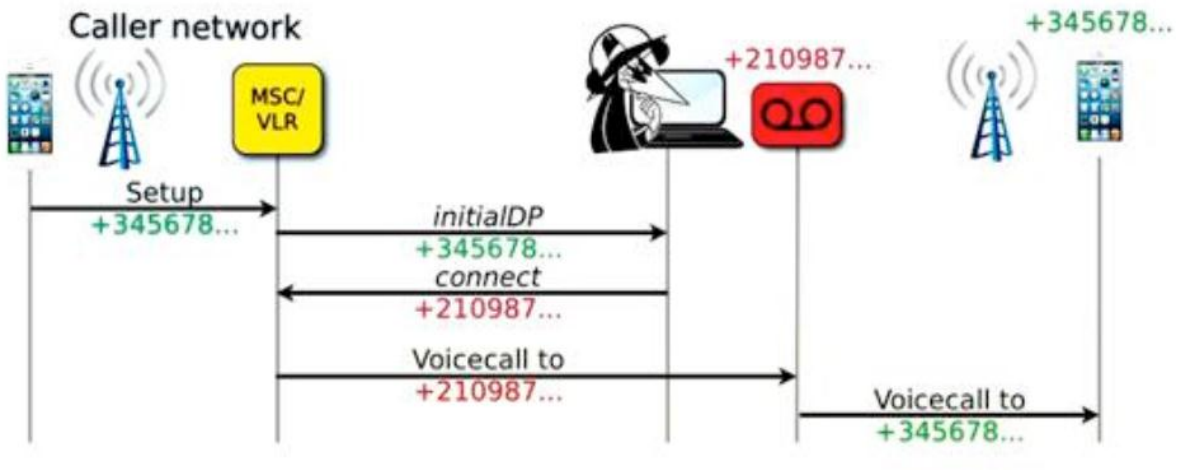
Şekil 2 - sendAuthinticationInfo Mesajı ile 3G IMSI Yakalayıcı

4.1.3. Giden Çağrıların Ele Geçirilmesi – CAMEL gsmSCF

GSM Servis Kontrol İşlevi (gsmSCF), şu işlevleri yerine getirir: CAMEL mantıksal hizmeti SS7 ağı içerisindeki bağlantının başlatılması sürdürülmesini, değişimini ve iptalini sağlayan bir dizi olayların yönetimi yerine getirir (Engel, 2014, s31). Bu özellik alan kodunu değiştirmek veya uluslararası kod ekleyerek giden çağrıların numaraları değiştirmek için kullanılır.



Şekil 3 - Hedef için gsmSCF adresini Manipüle Etmek



Şekil 4 – Saldırganın Giden Çağrı Numarasını Yeniden Yazması

SS7 ağına erişen biri saldırgan insertSubscriberData mesajı ile kurbanın gsmSCF adresini kendi kontrolünde olan bir adres ile değiştirebilir (Engel, 2014,p34). Kurbanın giden çağrıyı yaptığı numarayı kendi numarası ile değiştiren saldırgan çağrıyı hedefine ulaşmadan ele geçirerip kaydedebilir (Engel, 2014, p35). Bu saldırının yapılabilmesi için saldırganın aynı operatör ağı üzerinde olması gerekmediğinden önlem için dış operatörlerden gelen bu mesajlara karşı ayrıca filitreleme yapılması gerekir.

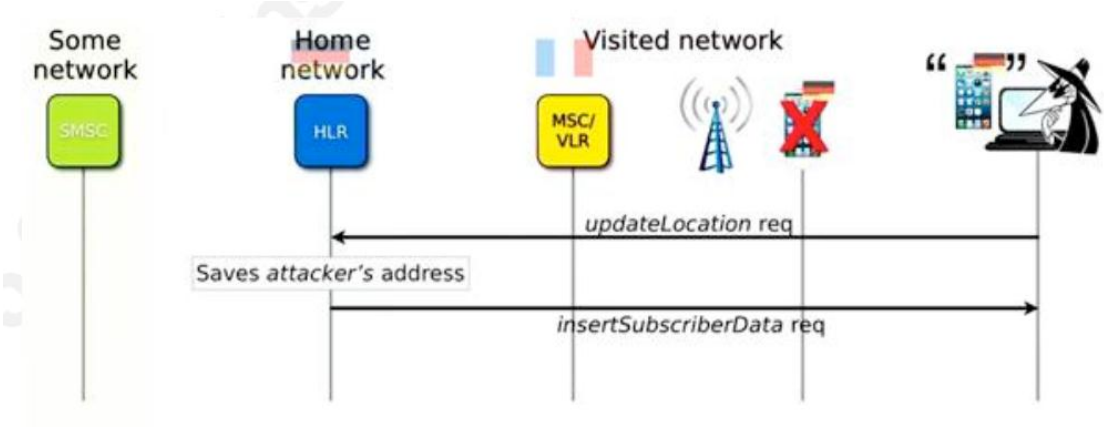
4.1.4. Gelen Çağrıyı Ele Geçirme – Çağrı Yönlendirme

RegisterSS mesajı abonelere yeni hizmetler kaydetmek için kullanılan bir mesajdır. Bu hizmetlerden birisi de çağrı yönlendirmedir (Dryburgh, Hewet, 2005). Bir saldırgan registerSS mesajını kendi kontrolündeki numaraya çağrı yönlendirmek için kullanılır. İşi bittiğinde eraseSS mesajı ile mevcut yönlendirmeyi silerek gerçek aboneye tekrar yönlendirebilir. Bu yöntemle saldırgan gelen çağrıları alıp kaydedebilir.

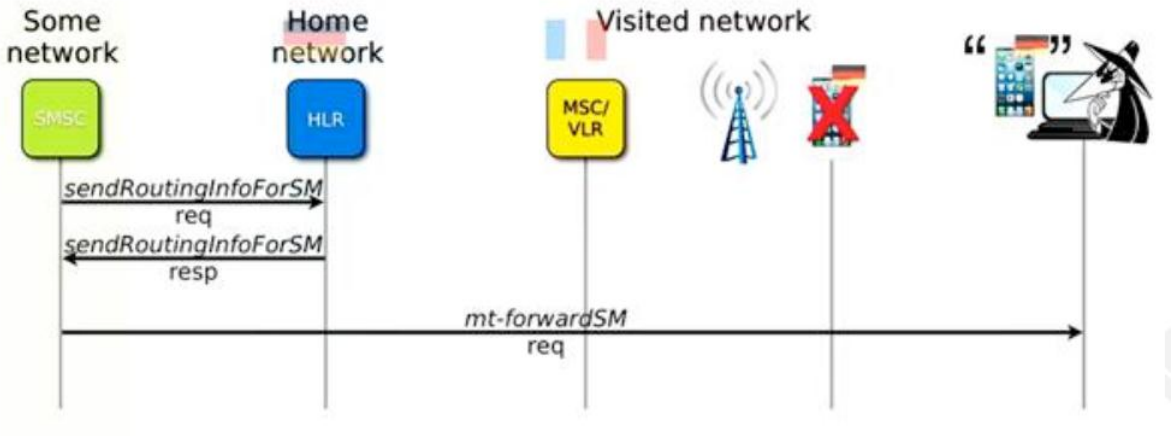
4.1.5. SMS'i Ele Geçirme

updateLocation mesajı abonenin konumunu ağdaki konumunu güncellemek için kullanılır. Bu aynı zamanda abone cihazının hala ağa bağlı olduğunu belirtmek için de kullanılır. Saldırgan sahte updateLocation mesajı ile kendini kurbanın yerine kaydettirerek SMD'leri ele geçirebilir. SMS'ler birçok sistem ve web sitesi tarafından gönderilen şifreler ile kimlik doğrulaması yapmak için kullanılır.

Ne yazıkki updateLocation mesajı roaming kapsamında dış networklerden de gönderilebilir ve bunu önlenemeyebilir.



Şekil 5 - Abone Konumunu Sahte Konum ile Güncellemek



Şekil 6 - Saldırgan Abonenin SMS Mesajlarını Alır

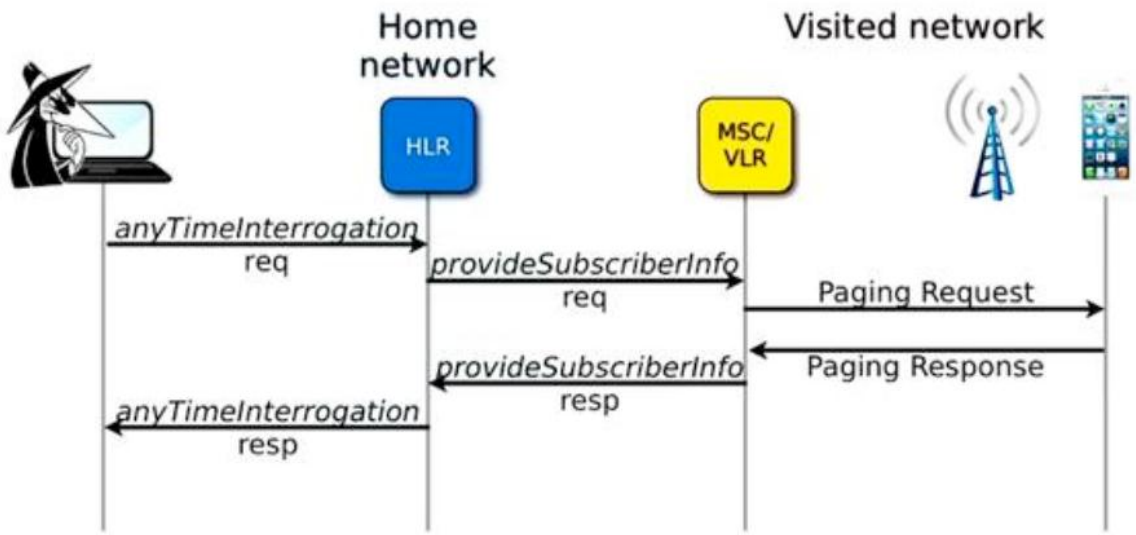
4.2. Konum Takibi

İstihbarat faaliyetleri açısından hedefin konumu çok değerli bir bilgidir. Başka bir ülkedeki hedefinizin konumunu herhangi bir fiziksel takip aracı kullanmadan elde edebileceğinizi düşünün.

4.2.1. Konum Takibi – anyTimeInterrogation (ATI)

Abonenin HLR'sine bir anyTimeInterrogation mesajı gönderildiğinde bir abonenin bağlı olduğu VLR/MSC'ye gönderilen bir provideSubscriberInfo(PSI) mesajını tetikler. Bu diğer bilgilerle birlikte abonenin hücre kimliğini (Cell-ID) bilgisini de geri döndürür.

Saldırgan bu mesajı Cell-ID'yi elde etmek için kullanabilir. Daha sonra bu hücre bilgisi internette açık olarak paylaşılan hücre haritaları ile coğrafi konuma çevrilebilir (Engel, 2014, p13).



Şekil 7 - Hedefin Konumunu Elde Etmek için anyTimeInterrogation Mesajının Suistimal Edilmesi

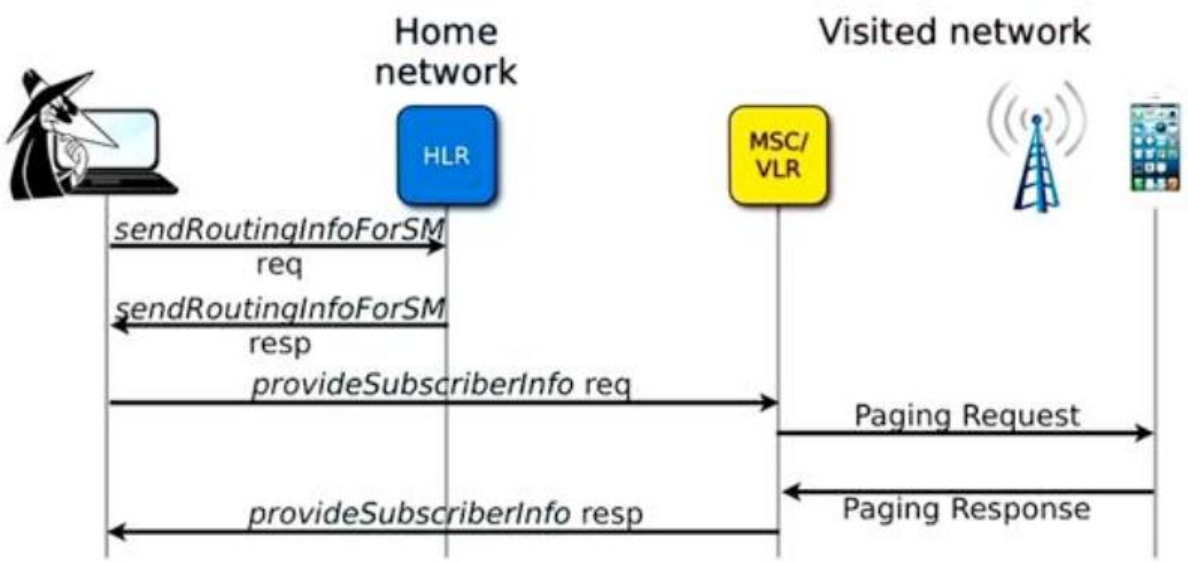
Neyse ki anyTimeInterrogation mesajı dış ağlardan etkilenme durumu yoktur. Operatör ağının girişinde filtrelenebilir.

4.2.2. Konum Takibi – provideSubscriberInfo (PSI)

Bu örnekte ATI mesajları filitrelenmiştir, saldırgan hala abonenin bağlı olduğu MSC/VLR'ye doğrudan provideSubscriberInfo mesajı gönderebilir.

Saldırgan ilk olarak IMSI'yi bulmaya ve MSC'nin adresine gerek duyacaktır. MSC'nin adresini, MSC'nin Global Title (GT) adresini geri döndüren sendRoutingInfoForSM gibi bir mesaj kullanarak elde eder. (Engel, 2014, p17)

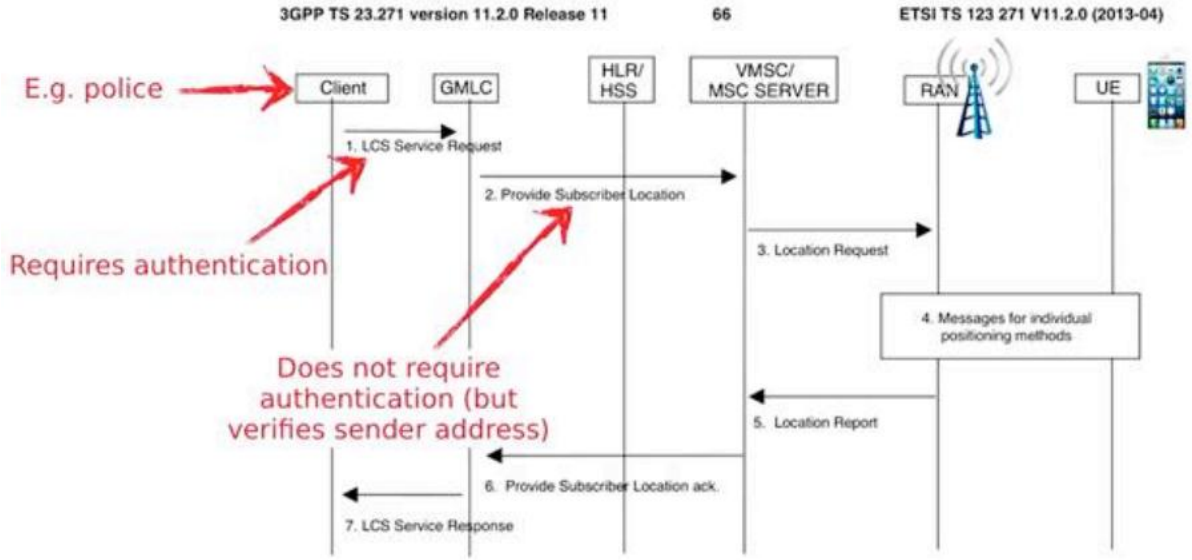
Normal şartlarda PSI mesajı abonenin yer aldığı operatörün ağı dışından alınmaz; fakat dış operatör abonesi dolaşım (roaming) esnasında asıl operatörün ağına girerse, dış operatör tarafından alınabilir durumdadır.



Şekil 8 - provideSubscriberInfo Kullanılarak Hücre Kimliğinin (ID) Elde Edilmesi

4.2.3. Konum Takibi – provideSubscriberLocation

provideSubscriberLocation (PSL) mesajı Gateway Mobile Location Center (GMLC) tarafından abonenin konumunu sağlamak için meşru olarak kullanılır. MSC'nin GMLC sunucunun kimliğini doğrulama yeteneği yoktur fakat gönderenin GT adresini doğrulayabilir (Engel,2014, p24)



Şekil 9 - Konum Servisleri

Ne yazıkki saldırgan hala PSL mesajı göndermek için GMLC'nin adresini taklit edebilir durumdadır.

4.3. Dolandırıcılık

Daha önce bahsedildiği gibi SS7 mobil operatörlere bağlı bir durum olmadığı için güvensiz operatörler üzerinden gerçekleştirilen erişimler artmaktadır.

Bu durum abone üzerinden birçok haksız işlem yapmak için birçok fırsat yaratır. Bu bölümde oluşan dolandırıcılık fırsatları açıklanacaktır.

4.3.1. USSD dolandırıcılığı - processUnstructuredSS

USSD diğer birçok servis gibi operatör tarafından aboneye şifre alma, ödeme yapma ve kredi transferi gibi çeşitli ticari hizmetler vermek için kullanılan bir protokoldür. Tipik olarak abone belli bir işlemi yapmak için bir USSD kodu gönderir.

processUnstructuredSS mesajı kullanılarak saldırgan abonenin yerine USSD kodları göndererek hedef üzerinden muhtemelen kredi ve para transfer işlemi yapmaya yetki alabilir (Engel, 2014, p44).

```
▽ GSM Mobile Application
  ▽ Component: returnResultLast (2)
    ▽ returnResultLast
        invokeID: 1
      ▽ resultretres
        ▽ opCode: localValue (0)
            localValue: processUnstructuredSS-Request (59)
        ▽ ussd-DataCodingScheme: 0f
            0000 .... = Coding Group: Coding Group 0(Language using the GSM 7 bit default alphabet) (0)
            .... 1111 = Language: Language unspecified (15)
          ussd-String: a0e09a5e2fb3d9e539e858a7a3c3e2b25b0782b9703450b1...
          USSD String: Aktuelles Guthaben: 0.84 EUR.
```

Şekil 10 - USSD Kodu Kullanılarak Dolandırıcılık

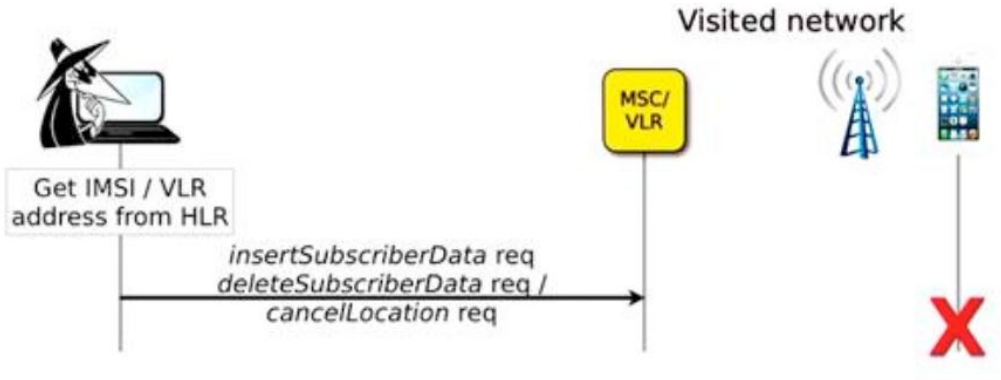
Ne yazıkki birçok durumda operatör dış operatörlerden bu mesajları girişine izin verir, bu durumda başka bir ülkeyi ziyaret eden dolaşımda (roamin) olan aboneler bu servislere erişmeye gerek duyacağından operatörün dış hattında filtrelenmesi çok zordur.

4.3.2. Birinci sınıf dolandırıcılık – Çağrı yönlendirme

Çağrı ele geçirmede olduğu gibi, registerSS mesajı ele geçirilen numaraının yerine ücretli bir numaraya çağrıyı yönlendirmeyi yapılandırmak için de kullanılabilir

4.4. Servis dışı bırakma

Saldırganın belli bir abonenin aldığı şebeke hizmetini engellemek için kullanabileceği birçok yol vardır. Saldırgan insertSubscriberData veya deleteSubscriberData kullanılarak abonenin önemli servisleri veya hiçbir çağrıyı almamasını sağlayabilir. Saldırgan cancelLocation mesajını kullanarak abonenin ağ ile olan bağlantısını kesebilir, böylece çağrıla ve SMS'ler ulaştırılamaz (Engel,!2014,!p30)



Şekil 11 - SS7 Kullanılarak Servis Dışı Bırakma

Düşünülmesi gereken bir nokta da; SS7 güvenliğinde yapılacak küçük bir araştırma ile SS7 uygulamalarının güvenlik zafiyetlerinden uzak olmadığını görebilirsiniz.

5. Zaafiyetlerin sınıflandırılması

Bir önceki bölümde açıklanan saldırıların gerçekleştirilebilmesi için kullanım amallarına göre farklı SS7 mesajlarının sınıflandırılmasına ve açıklanmasına gerek vardır. Önceki bölümde açıklanan saldırıları gerçekleştirmeyi sağlayan mesajları 3 kategoride sınıflandırabiliriz:

- **Kategori 1:** Dış operatör ağları üzerinden kullanılması meşru olmaya mesajlar.
- **Kategori 2:** Operatörün kendi aboneleri için gerekli olmayan fakat dolaşımdaki yabancı abonelerin alması gereken mesajlar.
- **Kategori 3:** Dış operatör ağları üzerinden alınması gereken mesajlar.

Aşağıdaki tablo farklı SS7 mesajlarını, kullanıldığı saldırı senaryolarını ve kategorilerini özetlemektedir.

Mesaj	**Saldırı**	**Kategori**
sendIdentification (SI)	Interception	Category 1
sendAuthenticatioInfo	Interception	Category3
insertSubscriberData+gsmSCF	Interception (Outgoing)	Category2
registerSS–eraseSS	Interception (Incoming),Fraud	Category3
updateLocation	Interception(SMS), Denial of Service	Category3
processUnstructuredSS	Fraud	Category3
insertSubscriberData	Denial of Service	Category2
deletedSubscriberData	Denial of Service	Category2
cancelLocation	Denial of Service	Category3
anyTimeInterrogation	Tracking	Category1
anyTImeModification	Tracking	Category1
provideSubscriberInformation	Tracking	Category2
provideSubscriberLocation	Tracking	Category1
sendRoutingInformation(USM,ULCS)	Facilitates multiple attacks	Category3

6. Kritik Güvenlik Kontrolleri (CSC)

"Etkin Siber Savunma için Kritik Kontroller, bugün yaygın olan çoğu saldırının siber savunması için alınması önerilen bir dizi aksiyonu ifade eder. Bunlar kamu ve özel sektörden yüzlerce güvenlik uzmanının oluşturduğu konsorsiyumlar tarafından geliştirilir ve sürdürülür" (Council on cyber security, 2015)

Bu belgenin içeriğinde, SS7'nin kendisi ve opratör ağları arasındaki güvenliği artırmak üzere daha önceki bölümlerde açıklanan saldırı türlerini engellemeye yönelik alınabilecek güvenlik önlemleri inceleyeceğiz.

6.1. Critical Security Control 13 – Boundary Defenses

CSC13 iç sistemleri sıkı yapılandırılmış bir ağı korumaya adanmıştır (Cole, Tarala, 2015, p. 1-67). Başka bir deyişle ağın sınırlarının belirlenmesidir. Savunma hattının düzgün bir şekilde çizilebilmesi için SS7'ye yönelik güvenlik duvarları ve IDS/IPSs sistemlerinin SS7/MAP trafiğinin anlamladırması, algılaması ve engellemesi gerekir.

Endüstri bu tür özellişmiş sistem ve cihazları üretmeye çalışırken biz IDS/IPS gibi geleneksel sistemler ile yardımcı özelleştirilmiş filtreler kullanarak tespit etmeye ve muhtemel saldırıları bloklamaya çalışırız. Örneğin birinci kategorideki saldırılar basitçe belli MAP mesajlarına bakılarak anlaşılabilir. Aşağıdaki örnekte sendIdentification mesajı kullanılarak gerçekleştirilen çağrı ele geçirme saldırısını tespit etmeye yönelik bir SNORT filtresi yer almaktadır.

```
alert ip $External_Operators any -> $STP any (msg:"Call Interception Attempt sendIdentification"; content:"sendIdentification";
```

İkici kategori saldırılar için, tespit operatörün IMSI aralığında MAP mesajlarının var olup olmadığına bakan filtreler ile gerçekleştirilir. Bu tarz saldırıları tespit eden SNORT filtresi şuna benzer:

```
alert ip $External_Operators any -> $STP any (msg:"Location tracking provideSubscriberInformation"; content:"provideSubscriberInformation"; content: "6201XXXXXXXX";
```

Yukarıdaki yöntemde sinyal trafiğinin IP üzerinden taşındığı varsayılmıştır (SIGTRAN) ancak bu fiziksel yapı TDM sinyalleşmesini IP tabanlı iletişime çeviren özel ekipmanlar ile TDM üzerinden de gerçekleştirilebilir.

Ne yazık ki üçüncü kategori MAP mesajları ile kullanıcının mevcut ve son konumu gibi ileri bilgiler ilişkilendirilmesini gerektirir. Bu önceden tanımlı sabit filtreler ile gerçekleştirilemeyebilir.

6.2. Kritik Güvenli Kontrolü 14 – Bakım, İzleme & Denetim Günlüklerinin Analizi

CSC14, sistemler üzerindeki olayları sonradan analiz etmeyi ve sistemlerin durumunu anlamayı sağlayacak günlük kayıtlarının tutulmasını hedefler (Cole, Tarala, 2015, p102). Günlük kayıtları sistemler üzerinde neler olduğunu anlamak için çok değerlidir. Operatör ağının çekirdek bileşenlerini denetlemek kuruluşların log yönetimi işleminin bir parçasıdır.

Eğer mümkünse, belli MAP mesajlarının kullanımını kayıt altına alın, hem dahili loglama imkanları ile çekirdek ağ bileşenlerini hem de ağ trafiği kalitesi denetlemeye yönelik sistemlerin kayıtlarını beraber değerlendirin. Bu kayıtlar sonradan kategori 1 ve 2 deki anormallikleri tespit etmek, hem de kategori 3 saldırılarını ilişkilendirmek için analiz edilebilir.

Örneğin kısa bir süre içerisinde iç ağdan bir mesaj alındıktan sonra bir dış kaynaktan **updateLocation** mesajı alma arasında bir ilişki kurulabilir. Bu senaryo aslında kullanıcının kısa bir süre içerisinde yurtdışına gittiği anlamına geldiğinden normal değildir ve bu kullanıcıya karşı bir saldırı yapıldığına işaret edebilir.

6.3. Kritik Güvenli Kontrolü 19 – Güvenli Ağ Mühendisliği

İç ağlara yeni tehditlerle birlikte, güvenli ağ mühendisliği konusu mutlak bir gereklilik haline gelmiştir. Temel bir çekirdek ağ, risk altındaki farklı ağ bileşenleri doğru şekilde bölümlendirilmesi ile riskleri azaltabilir. CSC19 sağlam, güvenli ağ mühendisliği işlemleri ve ağ mimarisi konularına adanmıştır (Cole, Tarala, 2015, p103). Ağı farklı güven ilişkisi ve saldırılara maruz kalma seviyesine göre bölgelere ayırmak çekirdek ağın güvenliğini geliştirir. Dış ağdan STP'ye gelecek bir erişim HLR ve MSC gibi ağ bileşenlerinden ayrılmış olur.

6.4. Kritik Güvenli Kontrolü 20 – Sızma Testi ve Kırmızı Takım Pratikleri

Güvenli ve güvensiz iki SS7 ağı arasında kurulan ara bağlantının güvenlik açısından sınırları açıkça belirlenmelidir. CSC20 ticari sistemlerdeki potansiyel sistem zayıflıklarını tanımlamak ve sistemin topyekün güvenliğini geliştirmeye adanmıştır. Zayıflıkları tanımlamaya ek olarak, kırmızı takım pratikleri güvenlik izleme

kusurlarını, karşılık verme prosedürlerindeki boşlukları ve çalışanların fazla güvenme durumlarını açığa çıkartır Cole, Tarala, 2015, p1-127).

İç ağa karşı yapılacak harici ve dahili saldırı testleri yapılmalıdır. Ağın bu bölümünün kritikliği dikkate alındığında, ürün ortamını test eden bir test yatağı oluşturulması şiddetle tavsiye edilir.

6.5. Kritik Güvenli Kontrolü 4 – Güvenlik Açıklarını Sürekli Değerlendirme ve İyileştirme

Harici kaynaklara erişimin artması ile SS7 güvenliği araştırmacılarının sayısının artması, yakın gelecekte daha fazla zafiyetin açığa çıkmasına neden olacaktır.

Milyonlarca kullanıcının hizmet almasını engelleme potansiyeli açısından SS7 zafiyetleri siber savaşta ulus devletler arasında büyük bir silah haline gelebilecektir. SS7 zafiyetlerini belirleyecek araçları ve teknolojileri geliştirmek ve bu sürecin sürekliliğini sağlamaya gerek vardır.

CSC4 bilinen zayıflıkları iyileştirerek sistemlerin korumayı amaçlar. (Cole,Tarala, 2015, p1-63) Bu kuruluşların çekirdek ağ bileşenlerini de içine alan zafiyet yönetim programlarını genişletmeleri çok önemlidir. Kritik yamalar, risk seviyelerine göre mümkün olan en kısa sürelerde test ortamlarında denendikten sonra ve üretim ortamına uygulanmalıdır.

6.6. Kritik Güvenlik Kontrolü 18 – Acil Durumlara Tepki ve Yönetim

SS7 ağlarının doğası göz önüne alındığında, SS7 güvenlik araştırmaları ve uygun bir savunma inşa etmek acil durum gerçekleştiğinde kaçınılmaz olur.

Acil durum kabiliyetlerini geliştirmek çekirdek ağ bölgesindeki olaylara uygun tepkileri vermek için çok önemlidir.

CSC18, acil durum ekipleri kurarak veri kaybı risklerini azaltmayı, kurumların anlamlı süreler içinde acil olayları tanımlama ve tepki verme yeteneklerini geliştirmeyi hedefler. (Cole, Tarala, 2015, p1-83)

Acil durum tepki ekibinin iç ağ bölgesinde uzmanlık alanı prosedürleri uygulamanın yanında acil durumları ele alması da önemlidir. Düzenli talimler farklı saldırı senaryoları için tepki becerilerini değerlendirmek için faydalıdır. (örn: Servis dışı bırakma, Yetkisi Erişim, MAP mesaj suistimali, vb.)

6.7. Kritik Güvenlik Kontrolü 3 – İş bilgisayarları, Sunucular ve Mobil Aaygıtların, Yazılım ve Donanımlarının Güvenli Yapılandırması

CSC3, güvenli yazılım yapılandırması kullanarak sistemleri korumayı hedefler (Cole, Tarala, 2015, p1-27). Çekirdek ağ bileşenleri bu konuda istisnaya sahip değildir. İster işletim sistemlerinin standart güvenli yapılandırmasından emin olunmalıdır. Normal sıkılaştırma faaliyetleri şöyledir: Kullanılmayan servisleri devre dışı bırak, kullanılmayan hesapları kaldır, son yamaları uygula, açık ve kullanılmayan portları kapat.

Benzer sıkılaştırma, hassas bilgileri içeren veri tabanlarına da yapılmalıdır. Çekirdek ağ bileşenlerinin yönetimi güvenli bir kanal üzerinde gerçekleştirilmelidir. Telnet ve VNC gibi açık metin protokoller bu kritik elemanları yönetmek için kullanılmamalıdır. Kullanılmayan MAP işlevleri ilgili ağ cihazı üzerinde devre dışı bırakılmalı sadece gerekli mesajlara izin verilmelidir.

7. Sonuç

Geçmişten miras kalan bir protokol olarak, SS7 güvenlik hassasiyetiyle geliştirilmemiştir. SIP ve DIAMETER gibi sinyalleşme protokolleri hiç bir zaman iyi bir güvenlik kontrol sunamadığı gibi hala belli güvenlik sorunlarını bulundurmaya devam etmektedir.

Çekirdek ağ bileşenleri de yeni güvenlik tehditleri düşünülerek de imal edilmedi. Hali hazırdaki ve gelecekteki tehdirler için özelleşmiş güvenlik çözümlerine ihtiyaç olduğu nettir. Fakat telekom ağlarındaki değişim ticari IT ağağlarına göre daha yavaştır çünkü sistemleri kullanan milyonlarca kullanıcısı vardır. Operatör ağları için yeni savunma çözümleri ile tanışmamız çok uzun zaman alacaktır.

Bu oluncaya kadar elimizdeki güvenlik çözümlerine odaklanmak ve mevcut tehditleri azlatmak mutlak bir gerekliliktir. Kritik güvenlik kontrolleri, hali hazırdaki güvenlik zafiyetlerine karşı iyi bir güvenlik çatısı olarak kendini göstermektedir.

Makaleyi yazan: Hassan Mourad, Hassan.morad@gmail.com
Çeviri: Özgür Koca, ozgurkoca@gmail.com, www.tankado.com

Referanslar

Timberg, C. (2014, August 24). For sale: Systems that can secretly track where cellphone users go around the globe. Washington Post. Retrieved from http://www.washingtonpost.com/business/technology/for-sale-systems-that-cansecretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8af003-11e3-bf76-447a5df6411f_story.html

Washington Post (2013, Jan). Skylock Product Description 2013. Retrieved from: http://apps.washingtonpost.com/g/page/business/skylock-product-description-2013/1276/

Engel, T. (2014, December). SS7: Locate, Track & Manipulate. [Video file] Retrieved from: https://www.youtube.com/watch?v=lQ0I5tl0YLY

Nohl K. (2014, December). Mobile Self Defense. [Video file] Retrieved from: https://www.youtube.com/watch?v=GeCkO0fWWqc

P1 Security (2014, December). SS7 Map. Retrieved from: http://ss7map.p1sec.com/

3rd Generation Partnership project (2015, June 21). Mobile-services Switching Center. In TS 23.002 Network Architecture, Release 13, p26. Retrieved from: http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-d20.zip

3rd Generation Partnership project (2015, June 21). The Home Subscriber Server. In TS 23.002 Network Architecture, Release 13, p22. Retrieved from: http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-d20.zip

The Fall of SS7 – How Can the Critical Security Controls Help? 2 ! 3

Hassan!Mourad,!Hassan.morad@gmail.com! ! !

3rd Generation Partnership project (2015, June 21). The Authentication Center. In TS 23.002 Network Architecture, Release 13, p23. Retrieved from: http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-d20.zip

3rd Generation Partnership project (2015, June 21). The Visitor Location Register. In TS 23.002 Network Architecture, Release 13, p25. Retrieved from: http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-d20.zip

3rd Generation Partnership project (2015, June 21). The Short Message Service Gateway. In TS 23.002 Network Architecture, Release 13, p26. Retrieved from: http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-d20.zip

Dryburgh L., Hewet J. (2005, June). SS7 Network Architecture. In Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services. (Chapter 7) Retrieved from: https://www.informit.com/library/content.aspx?b=Signaling_System_No_7&seqNum=26

Dryburgh L., Hewet J. (2005, June). MAP Operations. In Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services. (Chapter 13) Retrieved from: https://www.informit.com/library/content.aspx?b=Signaling_System_No_7&seqNum=115

IETF (1999, October). Framework Architecture for Signaling Transport. Retrieved from: https://www.ietf.org/rfc/rfc2719.txt

Nohl K., Munaut S. (2010, December). GSM Sniffing. [pdf document] Retrieved from: https://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf

Dryburgh L., Hewet J. (2005, June). Mobility Management. In Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services. (Chapter 13) Retrieved from: https://www.informit.com/library/content.aspx?b=Signaling_System_No_7&seqNum=116
Nohl K. (2014, December). Mobile Self Defense, p.7. [pdf document] Retrieved from: https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf
Strobel D. (2007, July). IMSI Catcher. [pdf document] Retrieved from: http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/slides_imsi_catcher.pdf
Nohl K. (2014, December). Mobile Self Defense, p.8. [pdf document] Retrieved from: https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf
Engel, T. (2014, December). CAMEL. In SS7: Locate, Track & Manipulate, p31. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-trackmanipulate.pdf
Engel, T. (2014, December). Intercepting calls with CAMEL. In SS7: Locate, Track & Manipulate, p34. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf
Dryburgh L., Hewet J. (2005, June). Supplementary Services. In Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services. (Chapter 13) Retrieved from: https://www.informit.com/library/content.aspx?b=Signaling_System_No_7&seqNum=119

Engel, T. (2014, December). HLR: Stealing Subscriber. In SS7: Locate, Track & Manipulate, p42. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf
Engel, T. (2014, December). Cell level tracking with SS7/MAP. In SS7: Locate, Track & Manipulate, p13. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf
Engel, T. (2014, December). Location Services. In SS7: Locate, Track & Manipulate, p24. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locatetrack-manipulate.pdf
Engel, T. (2014, December). HLR: Supplementary Services. In SS7: Locate, Track & Manipulate, p44. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf
Engel, T. (2014, December). Denial of Service. In SS7: Locate, Track & Manipulate, p.30. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locatetrack-manipulate.pdf
Council on Cyber Security (2015). The critical security controls. Retrieved from: http://www.counciloncybersecurity.org/critical-controls/
Cole E., Tarala J. (2015). Critical Security Control 13 – Boundary Defenses. In Implementing and auditing the critical security controls – In depth – Book4, p.1
Cole E., Tarala J. (2015). Critical Security Control 14 – Maintenance, Monitoring & Analysis of Audit Logs. In Implementing and auditing the critical security controls – In depth – Book4, p.1-102

Hassan!Mourad,!Hassan.morad@gmail.com! ! !
Cole E., Tarala J. (2015). Critical Security Control 19 – Secure Network Engineering. In Implementing and auditing the critical security controls – In depth – Book5, p.1-103
Cole E., Tarala J. (2015). Critical Security Control 20 – Penetration Test and Red Team Exercises. In Implementing and auditing the critical security controls – In depth – Book5, p.1-127
Cole E., Tarala J. (2015). Critical Security Control 4 – Continuous Vulnerability Assessment and Remediation. In Implementing and auditing the critical security controls – In depth – Book2, p.1-63
Cole E., Tarala J. (2015). Critical Security Control 18 – Incident Response and Management. In Implementing and auditing the critical security controls – In depth – Book2, p.1-27
Cole E., Tarala J. (2015). Critical Security Control 3 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations & Servers. In Implementing and auditing the critical security controls – In depth – Book5, p.1- 83

Kısaltmalar

- AuC: Authentication Center
- ATI: Any Time Interrogation
- CN: Core Network
- GMLC: Gateway Mobile Location Center
- gsmSCF: GSM Service Control Function
- GT: Global Title
- HSS: Home Subscriber Server
- HLR: Home Location Register
- MSC: mobile Switching Center
- PSI: Provide Subscriber Information
- PSL: Provide Subscriber Location
- SMS-GW: Short Message Service Gateway
- SRI-SM: Send Routing Information – Short Message
- VLR: Visitor Location Register