LTE ve IMSI Yakalayıcı Efsaneleri

Ravishankar Borgaonkar*, Altaf Shaik, N. Asokan#, Valtteri Niemi§, Jean-Pierre Seifert
* Aalto University
Email: rbbo@kth.se

Technische Universita¨t Berlin and Telekom Innovation Laboratories
Email: (altaf329, jpseifert) @sec.t-labs.tu-berlin.de

Aalto University and University of Helsinki
Email: asokan@acm.org

§ University of Helsinki
Email - valtteri.niemi@helsinki.fi

Çeviri: Özgür Koca, E-posta: ozgurkoca@gmail.com, www.tankado.com

Özet

Mobil cihazlar, LTE ağ servislerinin kullanılabilirliği ve bant genişliğinin artması sayesinde insan hayatında bir zorunluluk haline gelmiştir. LTE (4G) iletişim protokolleri her zaman abonelerin konum mahremiyeti ve çeşitli ağ servislerinin bulunulabilirliği açısından bazı vaatleri yerine getirmiştir. Bu çalışmada LTE'nin ağ güvenlik protokolleri analiz edilerek bazı LTE güvenlik standartları ile LTE için kullanılan ağ cihazlarının çipsetlerinde sorunlar tespit edilmiştir. LTE cihazlara karşı yapılan istismarlar deneysel bir sahte baz istasyonu kullanılarak gerçekleştirilmiştir.

Sunuş

Akıllı telefonların ve yeni mobil uygulama ve hizmetlerin artmasıyla birlikte LTE'nin yüksek hızlı veri bağlantılarının vaat etmesi hayati sosyal faydalar sağlamada ve tüketici deneyimini zenginleştirmede hayati bir rol oynamaktadır. Ancak bu gelişmeler ve mobil cihazlara olan güven acil servis ağları ve mobil ekosistem boyunca yeni gizlilik ve erişilebilirlik sorunlarının ortaya çıkmasına neden olmuştur.

Mobil iletişim ağlarındaki güvenlik, her nesilde artmaktadır. 3G, IMSI Catcher'ların kullanıldığı sahte baz istasyonu saldırıları yapmayı zorlaştıran karşılıklı kimlik doğrulama özelliğini getirmiştir. LTE ise pek çok sinyal protokolünü, kimlik doğrulama ve bütünlük koruması ekleyerek güvenlik açısından sıkılaştırmıştır. Genel kabul gören inanç da, LTE

güvenlik açısından sağlamdır ve özellikle sahte baz istasyonu saldırılarının gerçekleştirilmesi zordur.

Bu çalışmada, LTE 3GPP belirtiminde ve baz bandı yonga setlerinde farklı sorunları keşfettik. Bu sorunlar, bir saldırganın LTE abonelerini izlemek için sahte baz istasyonu saldırıları düzenlemesine ve seçilen ağ hizmetlerini reddetmesine izin verir. Ticari LTE telefonlara yönelik bu saldırıları düşük maliyetle ve gerçek bir operatör ağı için de değerlendirdik. Ek olarak, abonelerin pasif izleme işlemine yardımcı olmaktan sorumlu LTE ağ yapılandırması sorunlarını ele alacağız.

Bu döküman şu şekilde yapılandırılmıştır. Birinci bölümde, abonelerin konumları hakkında bilgi sızdıran aldırılar gösterilmiştir. LTE şebekelerine bağlı abonelere yönelik hizmet reddi saldırıları Bölüm 2'de tartışılmıştır. Etik hususlar ve deney düzeneği 3. bölümde sunulmuştur. Dördüncü bölümde de sonuçlar değerlendirilmiştir.

1. Konum Bilgisi Saldırıları

Zaten 2G (GSM) şebekeleri konum gizliliği önem verilerek tasarlanmıştır. Bir mobil cihaz bir şebekeye bağlandığında, ona TMSI adında geçici bir tanımlayıcı verilir (TMSI - Geçici Mobil Abone Kimliği diye bilinir). Mobil cihaz ve şebeke arasındaki tüm sinyal mesajları, bundan sonra kullanıcının kalıcı tanımlayıcıları yerine sadece TMSI'ye kullanılarak yapılır (Telefon numaraları veya IMSI'ler gibi - Uluslararası Mobil Abone Kimliği). TMSI'ler sıklıkla rastgele değerler ile güncellenirler (örneğin mobil cihaz konum değiştirdiğinde). Bunun amacı, bir saldırganın radyo iletişimini pasif bir şekilde izleyerek, TMSI'leri belirli bir kullanıcının sabit kimlik tanımlayıcısı ile ilişkilendirememesi ve konumunu takip edememesi içindir. Birkaç yıl önce Dennis Foo Kune ve arkadaşları, 2G (GSM) şebekesinde saldırganın, hedef kullanıcıya ait bir telefon numarasını kullanarak bir sayfalama (paging) isteğini tetikleyebilen bir mesajın (sessiz bir metin mesajı göndererek veya bir çağrıyı başlatarak ve hızlı bir şekilde sonlandırarak) gönderilebileceğini gösterdiler [2]. Sayfalama istek mesajları TMSI numaralarını içerir. Böylece TMSI numarası ile hedefin telefon numarası ilişkilendirilmiş olur.

Çağrı isteklerinin, şaşırtıcı bir şekilde sosyal ağ mesajlaşma uygulamalarının kullanıldığı yeni bir yöntem ile etkilenebileceğini keşfettik. Örneğin, Facebook arkadaşınız olmayan birisi size anlık ileti gönderirse, Facebook spam koruması mekanizması gereği olarak mesajı sessizce "Diğer" klasörüne koyacaktır (spamcı Facebook'a 1 Avro ödemediyse). LTE destekli akıllı telefonunuzda Facebook Messenger yüklü ise, gelen Facebook mesajının oluşturduğu trafik, telefonunuzun konumunun izlemesine ve TMSI'nizin Facebook kimliğiniz ile ilişkilendirilmesine izin veren bir sayfalama isteği gönderir (paging request).Konunun daha da kötü yanı TMSI numaraları yeterince sık güncellenmez. Örneğin bir kentsel alanda birden fazla mobil operatörün atadığı TMSI'lerin geçerlilik süresini üç gün olarak gözlemledik. Başka bir deyişle, saldırgan TMSI'nızı bildikten sonra hareketlerinizi pasif olarak üç güne kadar takip edebilir.

Sahte baz istasyonu kullanan aktif bir saldırgan daha da iyi olabilir. LTE erişim ağı protokolleri, ağ hatalarını gidermek, arızaları tespit etmek ve gidermek için çeşitli raporlama mekanizmaları içerir. Örneğin, başarısız bir bağlantı sonrasında, bir baz istasyonu bir LTE cihazından en son hangi baz istasyonlarını hangi sinyal gücüyle gördüğünün raporunu ister. Bir saldırgan böyle bir raporu yakaladığında bu bilgiyi cihazın konumunu bulmak için kullanabilir. Baz istasyonlarının GPS konumları kamuya açık olarak yayınlanmaktadır. Aslında test ettiğimiz en az bir cihaz GPS konumunu tam olarak bildirdi. Arıza giderme mekanizmaları büyük mobil ağların güvenilir çalışması için gereklidir. LTE tasarımcıları, potansiyel kullanıcı gizliliği kaybı ve şebeke güvenilirliğinin sağlanabilmesi arasında dengeli ve zor bir tasarıma sahiptirler.

2. Servis Dışı Bırakma Saldırıları

Başka bir ülkeye seyahat ettiğinizi ve mobil aboneliğinizin dolaşım izni olmadığını hayal edin. Telefonunuz gittiğiniz yerdeki operatöre bağlanmaya çalıştığında bu ağı kullanma izniniz yok şeklinde bir red mesajı alacaktır ("Dolaşıma İzin Verilmedi" gibi). Telefonunuz bu cevabı kesin bir talimat olarak kabul eder siz cihazınızı yeniden başlatıncaya kadar bir daha bağlanmayı denemez. Bu telefonunuzun abonesi olmadığı bir ağa bağlanmayı sürekli deneyerek batarya tüketmesinin önüne geçmek içindir. Aynı zamanda havada gereksiz sinyalleşmelerin dolaşmasını da engeller. Tasarımdaki bu tercih güvenilirlik ve performansdan kaynaklanır. Tahmin edebileceğiniz gibi: bir saldırganın etkin bir şekilde 2G'den hizmet alabilmesi için 4G cihaza verilen 3G ve 4G hizmetlerini engelleyebileceğini göstereceğiz. LTE bağlantısı kurulum aşamasında karşılıklı anlaşılan parametreler zayıftır açısından 2G ile iletişim kurulduğunda zafiyetler doğurur.

3. Deneysel Kurulum ve Hususlar

Saldırıların fizibilitesini yapabilmek için, açık kaynaklı yazılım ve kolaylıkla temin edilebilen donanımsal araçlardan yararlanarak sahte bir baz istasyonu kurduk. Bir LTE test ağı oluşturmak için baz istasyonu görevi gören bir USRP B210 cihazı [3] kullandık. Yazılım tarafında ise ticari LTE cihazlarıyla iletişim kurabilmek için OpenLTE [4] ve srsLTE [5] paketlerinde değişiklik yaparak kullandık. Aşağıdaki fotograf kurulumu göstermektedir:

Denemelerimizin çevredeki diğer telefon kullanıcılarıyla etkileşimini önlemek için önlemler aldık. Aktif saldırılar bir Faraday kafesde [6] yürütülürken, pasif saldırılar için normal kullanıcılara hizmet kesintisi yapmamaya özen gösterdik. Sadece önceden belirlenmiş test cihazlarımızı bir saldırıya maruz bıraktık. Kullandığımız tekniklerin daha ayrıntılı açıklaması [1] 'de bulunabilir. Tespit ettiğimiz güvenlik açıklarını baz bant yonga seti üreticilerine ve standardizasyon kurumlarına bildirdik.

4. Sonuçlar

Bu çalışma ile LTE standartlarında ve baz bant yonga setlerinde, sahte bir baz istasyonu kullanarak abonelerin izlenmesine ve hizmet reddine olanak tanıyan yeni güvenlik açıklarını gösterdik. Saldırı tekniklerimizi birçok LTE cihazı üzerinde test ettik. Ayrıca, deneysel kurulumumuzda Facebook gibi popüler sosyal uygulamalar kullanılarak gizlilik saldırılarının nasıl gerçekleştirilebileceğini gösterdik. Araştırma raporumuz [1] daha teknik ayrıntılar sunmaktadır. Çalışmalarımızla ilgili güncel bilgiler için proje web sitesini ziyaret edebilirsiniz (https://sesy.org/).

Referanslar

1. http://arxiv.org/abs/1510.07563
2. http://www.internetsociety.org/location-leaks-over-gsm-air-interface
3. http://www.ettus.com/product/details/UB210-KIT
4. http://openlte.sourceforge.net/
5. https://github.com/srsLTE/srsLTE
6. http://www.gamry.com/application-notes/instrumentation/faradaycage