thinktech
STM Teknolojik Düşünce Merkezi

IoT Güvenliğinde Tehlikeli Boyutlar

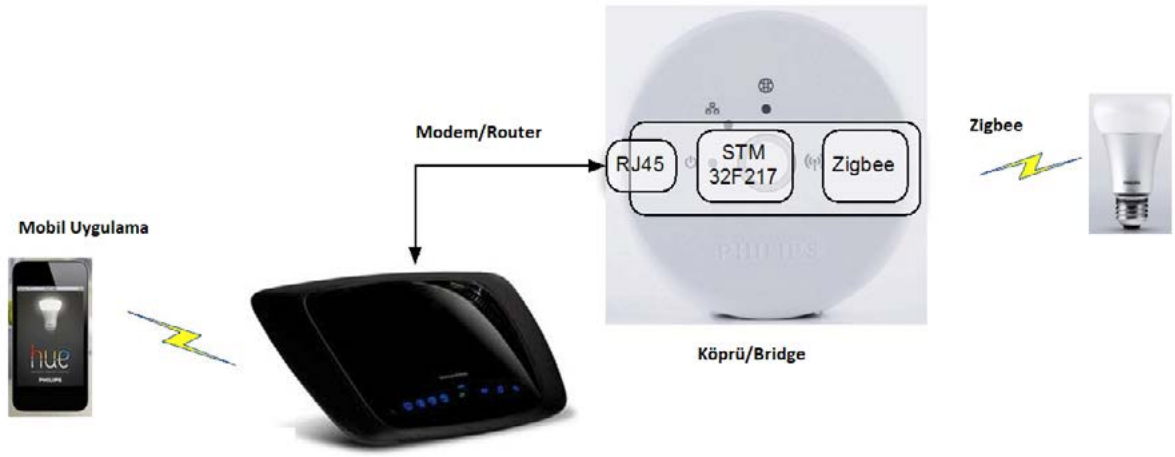
Özkan BOZTAŞ

IoT cihazlar tahminlerin de ötesinde bir hızla günlük hayatımıza girmeye devam ediyor. 2017 itibariyle IoT cihaz sayısı dünya nüfusunu geçmiş durumda[1]. Siber güvenlik bakış açısıyla cihazların en büyük sorunu geliştirme sırasında güvenlik anlayışının ön planda olmayışı. Şirketlerin birbirleriyle kıyasıya rekabeti ve ürünü pazara ilk sunabilen firma olma dürtüsü geliştirme sürecince ölümcül hataların yapılmasına neden olan en önemli sebeplerden. Bu gibi cihazlar zaten piyasaya çıktıktan birkaç ay sonra asla güncelleme alamayacak onlarca zafiyete sahip olacaklar. Bu yazıdaki konumuz hepimizin bildiği, IT ortamlarındaki zafiyetlerin IoT cihazlara uyarlandığı klasik kimlik doğrulama hataları, varsayılan zayıf parolalar, şifresiz haberleşme, web arayüzündeki xss vb. çok bilinen açıklıklar değil. Konumuz, güvenliğin yazılım geliştirme süreçlerine en başından beri entegre olduğu köklü firmaların ürünlerinde bulunabilen ve karmaşık saldırı tekniklerinin sebep olduğu zafiyetler kümesi ve olası çok ciddi fiziksel zararlar!

Prof. Shamir ve ekibinin ortaya çıkardığı, internet bağlantısı gerektirmeden akıllı aydınlatma cihazları üzerinden yayılıp tüm şehri etkileyebilecek yeni bir solucan türü, IoT güvenliği ile ilgili kaygıları kâbusa çevirebilecek kadar etkili gözükmekte[2]. En saygın akademik güvenlik konferanslarından IEEE Security&Privacy'de yayınlanan makalede, birden çok teknik kullanılarak "Philips Hue" akıllı aydınlatma lambaları uzaktan ele geçirilebilmiş. Bununla da yetinmeyen araştırmacılar cihazın donanım yazılımının imzalama anahtarını ele geçirerek üzerinde bazı değişikliklerle zararlı hale getirmişler. Son olarak da lambaların oluşturduğu mesh ağları üzerinden birbirlerini güncellemelerini sağlayarak, zararlı yazılımın herhangi bir internet bağlantısı gerektirmeden kısa sürede bütün bir şehre yayılabileceğini de göstermişler.

Akıllı ev deyince ilk akla gelen akıllı aydınlatma sistemleri, ucuzlayan fiyatları ve artan kullanım alanlarıyla giderek daha çok evde yer almaya devam ediyor. Evdeki modeme bağlı bir köprü (bridge) ve lambalardan oluşan bu basit sistem (Şekil 1), lambaların uzaktan kontrolü, şiddetinin ayarlanması, açılıp kapanması, ortama uygun renk değiştirmesi vb. özelliklere sahip. Köprü, bu ayarlamaları yapabileceğiniz mobil uygulamalar ve lambalar arasında adı üzerinde sanal bir köprü kuruyor. Köprünün bir tarafı cep telefonundan gelen komutları anlarken, diğer tarafı bu komutları lambaların anlayabileceği dile çeviriyor. Köprünün cep telefonu ile konuşan tarafı standart kablosuz ağ protokolü. Bugün, köprünün lambalarla konuştuğu nispeten daha az bilinen Zigbee protokolüne değinelim. Bluetooth ile kıyaslayabileceğimiz bu protokol, Bluetooth'dan çok daha

1 https://www.forbes.com/sites/louiscolumbus/2018/06/06/10-charts-that-will-challenge-your-perspective-of-IoTs-growth/#670b79a13ecc
2 https://ieeexplore.ieee.org/document/8283484/



Şekil 1: Philips Hue Mimarisi

az enerji harcarken (1w'a karşılık 100 mw), ondan çok daha uzun mesafelere ulaşabiliyor (yaklaşık 300 metre). Bu protokoldeki cihazlar birbirleriyle mesh ağı oluşturabiliyor. Böylelikle her cihaz aynı zamanda istemci ve sunucu rolünü üstlenebiliyor. Köprüden oldukça uzakta, örneğin üst katlarda konumlanan bir lambayı düşünün. Lambayı kapat komutunu verdiniz ama köprü lambaya ulaşamayacak mesafede. Bu durumda mesh ağındaki lambalar üzerinden çizilen bir rota ile ilgili lambaya komut iletilebiliyor. Bu özellik ile lambaların birbirlerini güncellemeleri de mümkün kılınmış durumda. Özetle askeri alanlarda kullanılmak üzere tasarlanan mesh ağları artık evlerimizdeki yerlerini de almış durumda.

Köprü ve lambalar üzerinde Philips'in aldığı birçok güvenlik önlemi var. Örneğin yeni bir lambayı ev ağına dâhil etmek için köprüye 45 cm'den daha yakın olmanız gerekiyor. Bu, üst kattaki komşunuzun yanlışlıkla sizdeki lambalardan birini komutu altına almasını engellemek için ve sinyal seviyesinde yapılan ölçümlerle oldukça hassas şekilde hesaplanabiliyor. Hâlihazırda eşleştirilmiş köprü ve lambalarda 32 bitlik Transaction ID adı verilen ve rastgele üretilip iki tarafta da kaydedilmiş bir değer var ki bu değeri bilmediğiniz sürece lambalara komut yollamanız imkânsız. 4 milyardan fazla değer alabilen Transaction ID'yi kaba kuvvet (brute-force) saldırıları ile bulmak, protokolün gerektirdiği düşük bant genişliği (250 kb/s) sebebiyle oldukça zaman alacaktır. Diyelim ki bu değeri ele geçirdiniz ve lambaya da 45 cm yakınsınız (ki bu evin içindesiniz demek!), yapabileceğiniz en fazla şey lambaları söndürüp yakmak olabilir. Zira cihazların üzerindeki donanım yazılımı (firmware) şifreli ve imzalı olduğundan modifikasyonu imkansız! Tabi ki bunlar üreticiler tarafından iddia edilen veriler. Gerçek hayatta bu önlemler ne kadar işe yaramış biraz da onlara bakalım.

Shamir ve araştırmacılar, protokolün açık kaynak kodlarını inceleyerek bir fonksiyon içerisinde Transaction ID değerinin 0'a eşit olma kontrolünün yapılmadığını fark etmişler. Bu değerin 0 olduğu durumda ilgili güvenlik adımının baypas edilebildiğini de belirtelim. Yazılım geliştirici ilgili kodlamanın başında yazdığı açıklama ile sıfıra eşit olma kontrolünün protokolün ilk adımlarında hâlihazırda yapıldığını belirtmiş. Peki, protokolü modifiye edip ilk adımdan başlamazsak? Araştırmacıların bulduğu ilk hata işte bu kadar basit. Bahsi geçen değerin 0 olarak atanması ve protokolün sonraki adımlardan başlatılması ile kimlik doğrulama adımının baypas edilmesinin mümkün olduğunu, akabinde cihazlara komut yollanabildiğini görmüşler. Ancak halen 45 cm kısıtıyla karşı karşıya olduğumuzu belirtelim. Araştırmacılar bunu da atlatabilmenin bir yolunu, cihazların geriye uyumluluk ve diğer üreticilerin cihazlarıyla konuşabilmeleri için almak zorunda oldukları önlemlerde bulmuşlar. Bahsi geçen Philips cihazlar Zigbee Light Link (ZLL) adı verilen bir protokolle konuşuyor. Bu yeni protokol, düşük enerji gereksinimi ve güvenlik önlemleri (yakınlık kontrolü vb.) ile yeni nesil cihazlar tarafından destekleniyor. Ancak eski cihazların ağa katılabilmeleri için de ZLL olmayan standart Zigbee protokollerini de

desteklemek zorundalar. Bir önceki adımda cihaza komut yollayabilecek adıma gelmiştik, yollayacağımız ilk komut da "Reset to factory new request" paketinden ibaret. Bu paket adından da anlaşılacağı gibi cihazı fabrika ayarlarına döndürüp ilgili ağdan çıkarıyor. Bu esnada cihaz çevredeki her tür cihaza bağlanmak için hazır durumda. Tam bu anda ZLL olmayan bir ağdan geliyormuşçasına yolladığınız bir istek paketiyle cihazı kendi ağınıza dâhil ettiğiniz gibi 45 cm kuralını da atlatmış oluyorsunuz. Zira üretici ancak ZLL cihazlarla konuşurken yakınlık kontrolünü geçerli kılmış durumda!

Bundan sonrası cihazın donanım yazılımını değiştirerek kendi kendine yayılan zararlı bir hale getirmekte. Ancak dediğimiz gibi yazılım şifre ve imza korumalı. Bu kısmı atlatmak da tabiri caizse Adi Shamir için çocuk oyuncağı, zira kendisi açık anahtarlı kriptografi denilince ilk akla gelen RSA algoritmasına adını veren üç kişiden bir tanesi! Araştırmacılar test ortamında, cihaz güncellemesi için farklı köprü ve lambalarla bulundukları güncelleme isteklerinden sonra sunucudan hep aynı dosyanın geldiğini görmüşler. Bu durum da yazılımın tek bir anahtarla şifrelendiğini ve bu anahtarın da lamba üzerinde gömülü olduğunu gösteriyor. Gömülü sistemlerin enerji tüketiminin kolaylıkla izlenebilmesi, bu cihazlar üzerinde PC'ler gibi birçok işlemin aynı anda yapılmaması ve böylelikle kriptografik işlemlere ait enerji tüketimlerinin kolaylıkla ayırt edilebildiği bir gerçek. Cihazın üzerindeki işlemlerin test ortamında gerçeklenmesi ve değişik kriptografik anahtarların denenmesiyle elde edilen tüketim değerlerinin kaydedilmesi, sonrasında cihazın gerçek tüketim değeriyle örtüşmesinden elde edilen korelasyon değerleri size basit bir şekilde cihaz üzerindeki gerçek anahtarın hangisi olduğunu da gösteriyor. Anlattığımız kadar basit olmayan ise bu işlemler için oldukça hassas bir laboratuvar düzeneği kurmak ve anahtara bağlı tüketim hipotezinizi doğru oluşturmak. Araştırmacılar aylar süren testlerden sonra anahtarı ele geçirebilmiş ve yazılım üzerindeki tüm haklara sahip olmuşlar. Buna, yazılımın istenilen şekilde değiştirilip cihazlara yeniden yüklenmesi de dâhil!

Bu yazılımın değiştirilmesiyle yapılabileceklerin sınırı yok, en basiti güncellenen yazılım ile lambaları varsayılan olarak kapatıp cihazın yeni güncelleme alma seçeneğini de kapatarak etkilenen tüm lambaları bir daha çalışmayacak şekilde çöpe döndürebilirsiniz. Veya bir zamanlayıcı ile aynı anda tüm lambaları yakıp söndürerek elektrik şebekelerine ciddi yükler bindirilebilir. Lambaların belli frekanslarda açılıp kapanması ve titrek bir ışık elde edilmesiyle ışığa duyarlı insanlarda baş ağrısı vb. sorunlara yol açılabilir. Ancak en ilginç olan bu saldırıyı bir jammer gibi kullanarak tüm şehrin kablosuz ağının kesilebilmesi. Zigbee protokolü kablosuz ağlarla aynı frekansta çalışıyor (2.4 Ghz). Ayrıca bu cihazlar FCC/CE emisyon sertifikalandırma süresince sürekli dalga (continuous wave) modunda çalıştırılabiliyor. Bu test sinyalini modifikasyonlarla kablosuz ağdaki (802.11) kanallarla örtüştürmek mümkün. Böylelikle ele geçirdiğiniz tüm lambaları şehirdeki kablosuz cihazların çalışmasını engelleyecek kadar etkili bir jammer'a dönüştürmeniz mümkün olmakta!

Araştırmacılar çektikleri videolarda[3] araç üzerine kurdukları güçlü antenlere sahip bir düzenekle 70 metreden binadaki aydınlatma sistemlerini ele geçirdiklerini gösteriyorlar. Daha güçlü bir düzeneği drone'lar üzerine monte ederek binaların en üst katlarını bile etkileyebilmişler. Saldırının en can alıcı noktası olan zararlı yazılımın lambalar üzerinden birbirini etkilemesi ise kontrol edilemeyebilir denilerek gerçekleştirilmemiş. Ancak teorik olarak Paris büyüklüğündeki bir alanda 15.000 lamba bulunması durumunda tek bir lambayı etkileyerek başlayacak bir bulaşmanın zincirleme reaksiyon ile tüm şehre dakikalar içerisinde yayılacağını göstermişler. 15.000'li rakamlar Paris gibi büyük şehirlerde şu an bile mevcuttur ve sayının katlanarak arttığı da açık. Ancak şu an korkulu rüya görmemize gerek yok, araştırmacılar Philips ile bağlantıya geçerek bahsi geçen açıklıkları kapattırmış ve hâlihazırda güncelleme yayınlanmış durumda. Ancak çok benzer saldırı tekniklerinin başka ekiplerce başka cihazlara yapılmayacağının garantisi tabii ki yok. Üstelik bu işi akademik kapsamda yapmayacak birçok kimse olduğunu da bilmekte fayda var. Özetle IoT cihazlar ve güvenliği konusu, sonuçlarının fiziksel zararlara yol açmasıyla hem klasik IT saldırılarından daha tehlikeli hem de gün geçtikçe daha çok hedef olmaya devam edecek gibi gözüküyor.

3 http://IoTworm.eyalro.net/