HoneyThing: Nesnelerin İnterneti için Tuzak Sistem

Ö. Erdem, Dr. M. Kara, A. İkinci

***Özet*—Teknolojinin gelişmesiyle birlikte internete bağlı cihaz sayısı gün geçtikçe artmaktadır. Günümüzde kişisel, sosyal, sağlık gibi birçok alanda bu cihazların kullanımının yaygınlaşması teknoloji gelişimine bağlı olduğu kadar kullanıcılara sağladığı güvenlik ve mahremiyet yetenekleri ile de ilgilidir. Nesnelerin interneti cihazları bilgisayar, sunucular gibi güçlü donanıma sahip olmadıklarından bu cihazların bünyesinde saldırı tespiti için klasik yöntemler kullanılamamaktadır. Son yıllarda çıkan açıklıklar ve potansiyel kurban sayısının giderek artması saldırganların bu alana yönelmesine neden olmuştur. TR-069, cihazların uzaktan yönetimi için yaygın olarak kullanılan protokollerden biridir. Bu makalede TR-069 protokolünü kullanan nesnelerin interneti cihazlarında saldırı tespiti için tuzak sistem kullanımı ele alınmış ve bu cihazlardan ADSL (Asymmetric Digital Subscriber Line) modem/yönlendiriciler için bir tuzak sistem uygulaması geliştirilmiştir.**

***Abstract*— The number of devices connected to the Internet is increasing day by day with the development of technology. Nowadays, widespread use of these devices in many areas like personal, social, health etc. depends on as well as technology development, it is also related to security and privacy capabilities that provide to users. The conventional Intrusion Detection Systems (IDS) can not be used at internet of thing devices because of limeted hardware (CPU, RAM etc.) and software resources. The vulnerabilities that are found in recent years and the gradual increase in the number of potential victims have led attackers to tend to this field. TR-069, one of the widely used protocols to manage these devices remotely. In this paper, the use of honeypot is presented for intrusion detection on the internet of things devices that use TR-069 protocol and a honeypot application has been developed for IoT.**

***Anahtar Sözcükler*—Nesnelerin interneti, tuzak sistem, TR-069, modem/yönlendirici, RomPager**

I. GİRİŞ

İNTERNETin yaşamımıza girdiği ilk yıllardan itibaren kullanıcı sayısı her geçen gün artmaktadır. Özellikle son yıllarda yaşanan teknolojik gelişmeler ve 1999 yılında ortaya atılan "Nesnelerin İnterneti (Internet of Things-IOT)" kavramı ile birlikte çevremizdeki birçok eşyanın birbirleriyle iletişim kurması, internete bağlanmasına olanak sağlanmıştır [1].

Ö. Erdem TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü, 41470 Gebze/Kocaeli TÜRKİYE (e-mail: omer.erdem@ tubitak.gov.tr).

Dr. M. Kara TÜBİTAK BİLGEM Test ve Değerlendirme Başkan Yardımcılığı, 41470 Gebze/Kocaeli TÜRKİYE (e-mail: mehmet.kara@ tubitak.gov.tr).

A. İkinci Honeynet Projesi Türk Chapter Kurucu Üyesi. VizyonArge Ürün Yöneticisi (e-mail: ali.ikinci@vizyonarge.com.tr).

Bu gelişmelerin sosyal yaşamda sağladığı kolaylıkların kullanıcılar arasında hızla yayılması, bu alana daha fazla yatırım yapılması ve dikkate değer bir pazar haline gelmesine neden olmuştur. Ancak farklı türdeki nesnelerin bilgi paylaşımında bulunması kullanıcı gizliliği ve mahremiyeti konusunda çeşitli problemleri beraberinde getirmiştir. Ayrıca son yıllarda farklı türdeki cihazlarda çıkan açıklıklar ve olası açıklık durumunda potansiyel kurban sayısının çok fazla olması saldırganlar için cezbedici bir ortam oluşturmuştur.

Nesnelerin interneti cihazları arasında buzdolabı, su ısıtıcısı, ütü, televizyon vb. olmak üzere günlük yaşamda aktif olarak kullandığımız birçok farklı türde cihaz sayılabilir. Ev ya da küçük ofis kullanıcılarının internete bağlanmak için kullandığı modem/yönlendirici cihazlar bunlardan biridir. Son 10-15 yıllık zaman dilimi ile birlikte artık herkesin evinden internete bağlandığı düşünüldüğünde bu cihaz sayısında da önemli artışlar olmuştur. Bu durum cihazlarla uğraşan saldırgan, araştırmacı sayısının artmasına ve çeşitli açıklıkların ortaya çıkarılmasına neden olmuştur. Günümüzde hâlâ aktif olan bazı açıklıklarda 2004 yılında yayınlanan ve bu türdeki cihazların uzaktan yönetimini sağlayan TR-069 protokolü kullanılmaktadır. Nesnelerin interneti kullanıcılarının çoğunluğunun teknik olarak bilgi sahibi olması beklenmediğinden açıklıkların kapanması için çeşitli yamalar yayınlansa da bunun tüm cihazlara uygulanması ve yama yönetimi zor olmaktadır. Böylece üretici, sağlayıcı firmanın getirdiği çözümler her cihaza uygulanamamakta ve saldırganların hedef alabileceği kurban sayısı önemli ölçüde kalmaya devam etmektedir.

Cihazların fiziksel ve ağ güvenliğinin sağlanmasına yönelik çeşitli çalışmalar yapılmaktadır. Ancak saldırı tespiti noktasında bazı problemler bulunmaktadır. Bunlardan en önemlisi nesnelerin interneti cihazlarının kısıtlı bantgenişliği, hafıza, hesaplama yeteneği ve enerjiye sahip olmasından dolayı üzerlerinde yüksek işlem gücü gerektiren klasik saldırı tespit sistemlerini kullanmanın imkânsız olmasıdır. Tuzak sistemler, bilgi sistemlerine gerçekleştirilen saldırıların tespitinde kullanılan önemli mimarilerden biridir. Temel amacı hedef sistem gibi davranarak saldırganların dikkatini çekmek ve olası saldırı durumunda bütün aktiviteleri kaydetmektir. Bu uygulamalar doğrudan hedef sistem üzerinde çalışmadığından sistemin sahip olduğu donanımsal eksikliklerden etkilenmemektedir. Güncel olarak SMB, HTTP, FTP, SSH gibi birçok protokolün ve çeşitli işletim sistemlerinin benzetimini yapan tuzak sistemler bulunmakta ve saldırı tespit

noktasında aktif olarak kullanılmaktadır. Ancak önemli bir hedef haline gelen nesnelerin interneti eşyalarından modem ve yönlendiricilere gelen saldırıların tespiti için geliştirilmiş bir tuzak sistem bulunmamaktadır.

Makalenin 2. bölümünde çalışmanın ve geliştirilen uygulamanın anlaşılmasını sağlamak amaçlı farklı başlıklar altında nesnelerin interneti, tuzak sistemler, TR-069 protokolü ile ilgili temel bilgiler, literatür taraması detaylıca ele alınmıştır. 3. bölümde geliştirilen uygulama sistem tasarımından, test ortamına ve kullanım senaryolarına kadar tanıtılmıştır. Bölüm 4'te ise çalışma ile ilgili sonuç ve ileriye dönük çalışmalar için önerilere yer verilmiştir.

II. TEKNOLOJİLER VE LİTERATÜR TARAMASI

A. Nesnelerin İnterneti

Nesnelerin interneti kavramının terminolojideki tanımı üzerine birçok farklı görüş vardır. Bu farklığın sebebi aslında kavramı oluşturan iki sözcükten gelmektedir. Çeşitli ticari şirketler ve araştırma kurumları kendi altyapılarına, ilgi alanlarına göre ya internet kısmına ya da nesne kısmına ağırlık vererek tanım oluşturmuşlardır. Ayrıca kavram anlam bilimsel olarak incelendiğinde ortaya çıkan anlamsal tarafı vardır [2]. Böylece tanımlama yapılırken internet, nesne ve anlamsal olmak üzere 3 yaklaşım esas alınmıştır. Genel olarak nesnelerin interneti "çeşitli iletişim protokollerini kullanarak birbirleri ile haberleşen, bilgi üreten, oluşturdukları ağ sayesinde çevresiyle bilgi alış verişi yapabilen akıllı cihazların oluşturduğu bir topluluk ve pazardır.

Nesnelerin interneti kavramı ilk olarak 1999 yılında MIT Auto-ID Center kurucularından olan Kevin Ashton tarafından Procter & Gamble (P&G) şirketinde tedarik zinciri yönetimini konu aldığı bir sunumun başlığı olarak kullanılmıştır [3]. 2005 yılında International Telecommunication Union (ITU) tarafından yayınlanan "ITU Internet Report 2005: Internet of Things" raporu ile birlikte "Nesnelerin İnterneti" kavramı resmi olarak duyurulmuştur [4]. 2009 yılına gelindiğinde Avrupa Birliği "Nesnelerin İnterneti – Avrupa için Eylem Planı" başlıklı bir eylem planı yayınlayarak konuya verdiği önemi göstermiştir [5]. Cisco IBSG (Internet Business Solutions Group) tarafından 2011 yılında yayınlanan rapora göre 2003 yılında 500 milyon cihaz internete bağlı ve kişi başına düşen cihaz sayısı 0,08 iken 2010 yılında cihaz sayısı 12.5 milyara ve kişi başına düşen cihaz sayısı ise 1,84'e çıkmıştır. Yapılan çalışmalar sonucunda her 5 yılda bu oranın 2 katına çıkacağı öngörülmektedir. 2020 yılına gelindiğinde dünya nüfusunun 7.6 milyar, internete bağlı cihaz sayısının 50 milyar olacağı tahmin edilmektedir [6].

Günlük hayat incelenip gelecek öngörüleri düşünüldüğünde buzdolabı, araba, televizyon, su ısıtıcısı, fırın, ütü, kitap, kamera, klima, modem, yönlendirici benzeri akla gelebilecek birçok cihazın kablosuz ağ ya da RFID teknolojisi sayesinde birbirleri ile iletişim kurup internete bağlanarak yaşamımızı kolaylaştıracağı ve bazı alanlarda işleri daha verimli hale getireceği görülmektedir. Nesnelerin interneti kapsamında geliştirilen uygulamalar ağ erişilebilirliği, kapsam, yinelenebilirlik, taşınabilirlik, kullanıcı bağımlılığı ve etkisi türlerine göre sınıflandırılabileceği gibi kullanıldığı alanlar bakımından şu şekilde gruplandırılabilir [7]:

- *Akıllı Ortam*
- *Sağlık Hizmetleri*
- *Ulaşım ve Lojistik*
- *Kişisel ve Sosyal*
- *Enerji ve Madencilik*

Nesnelerin interneti çözümlerine gizlilik, bütünlük, erişilebilirlik, kimlik doğrulama, yetkilendirme vb. gibi güvenlik özellikleri entegre edilerek uygulamaların kullanılabilirliği arttırılabilir. SANS enstitüsü tarafından 2013 yılında yapılan ve kamu, askeri, sağlık, eğitim gibi birçok farklı sektörden yaklaşık 400 kurumun katıldığı araştırmaya göre katılımcıların %48,8'i nesnelerin interneti uygulamalarının günümüzde diğer sistemlerde karşılaşılan güvenlik problemleriyle aynı seviyede olduğunu belirtmiştir [8]. Karşılaşılan problemlerin çözümü için öncelikle tehdit kaynaklarının tespiti ve saldırı vektörlerinin belirlenmesi gerekmektedir. Ayrıca potansiyel hedef sayısının çok fazla olduğu bu alanda saldırı tespiti de önemli bir konu haline gelmiştir. Potansiyel tehditler ve saldırılar incelendiğinde kötü niyetli kullanıcı, kötü niyetli üretici ve dış saldırganlar olmak üzere tehditlerin kaynağı 3 farklı grupta toplanabilir [9]. Nesnelerin interneti uygulamalarının kullanım alanları çok farklı olduğundan bu uygulamalara yönelik saldırı vektörleri çeşitlilik göstermektedir. Bu durum saldırganların işini kolaylaştırırken savunma tarafındakiler için ele alınması gereken birçok parametre anlamına gelmektedir. OWASP adlı topluluk tarafından 2014 yılında yayınlanan çalışmayla nesnelerin interneti için 10 saldırı vektörü belirlenmiştir. Bunlar arasında web arayüzleri, ağ servisleri, şifreleme eksikliği ve cihaz yazılımları en önemlilerindendir [10].

Günümüzde bilgi sistemlerine gelen saldırıların tespitinde ağ servisi, işletim sistemi veya tüm ağın benzetimini yapabilen tuzak sistemler ve saldırı tespit sistemleri kullanılmaktadır. Nesnelerin interneti cihazları güçlü donanım özelliklerine sahip olmadığından klasik saldırı tespit sistemlerini kullanmak olanaksızdır. Bununla birlikte nesnelerin interneti uygulamalarında saldırı tespiti için çeşitli akademik çalışmalar yapılmaktadır. Raza S. ve arkadaşları 6LoWPAN ağı için geliştirdikleri ve adını SVELTE olarak belirledikleri saldırı tespit sistemi temel olarak sahte bilgi, seçmeli iletim ya da tuzak yönlendirme (sinkhole) gibi saldırıların tespitini amaçlamaktadır [11]. Yine EC FP7 (European Commission 7th Framework Programme) tarafından desteklenen "ebbits" projesi kapsamında hem kablosuz duyarga ağları hem de internet ağından gelebilecek saldırılara karşı savunmasız olan 6LoWPAN cihazları için saldırı tespit sistemi çalışma yapısı

önerilmiştir [12]. Literatürde nesnelerin interneti uygulamalarına gelebilecek saldırıların tespiti için benzer çalışmalar yürütülse de cihazların çalışması veya yönetiminde kullanılan herhangi bir protokol için geliştirilmiş bir tuzak sistem çalışması bulunmamaktadır.

B. Tuzak Sistemler

Tuzak sistem (honeypot - bal küpü) bilgi sistemlerine gerçekleştirilen saldırıları tespit etmek amaçlı geliştirilen mimarilerden biridir. Hedef sistem gibi davranarak saldırganların dikkatini çekmek ve olası saldırı durumunda bütün aktiviteleri kaydetmek üzere tasarlanmıştır. Tuzak sistemlerin temel özellikleri arasında ağ servislerinin, işletim sistemlerinin ya da tüm ağın benzetimini yaparak saldırıları üzerine çekmek, zararlı yazılım örneklerini toplamak, saldırı yönteminin özellikleri ve tekniği hakkında bilgi sağlamak, gerçek sistemlere gelebilecek potansiyel saldırı riskini düşürmek sayılabilir [13]. Tuzak sistemler gerçek bir ağa ait gibi görünse de ele geçirilmesi durumunda gerçek sistemlerin etkilenmesini engellemek amaçlı izole edilmiş bir ağ ortamında çalışırlar. Ayrıca tuzak sistemlerin sahip olduğu IP adresleri duyurulmamış yani herhangi bir yere kaydettirilmemiş, herhangi bir adresle ilişkilendirilmemiş olduğundan kendisine gelen tüm trafik şüpheli olarak düşünülür.

Tuzak sistemler kullanım amacı, üstlendikleri rol, geliştirildikleri donanım türü ve saldırgan ile olan etkileşimlerine göre çeşitli gruplara ayrılırlar. Saldırgan ile olan etkileşimlerine göre tuzak sistemler düşük etkileşimli, orta etkileşimli ve yüksek etkileşimli olmak üzere 3'e ayrılır [14]. Etkileşim saldırganın tuzak sistemle gerçekleştirdiği aktivitelerle ölçülür. Hangi tuzak sistemin ne zaman kullanılacağı çeşitli faktörlere bağlıdır. Etmenler ve tuzak sistem türlerinin bunlarla ilişkisi Tablo 1'de verilmiştir.

TABLO I
SALDIRGAN ILE OLAN ETKILEŞIMLERINE GÖRE TUZAK SISTEMLERIN KARŞILAŞTIRILMASI

Etmenler	Düşük Etkileşimli	Orta Etkileşimli	Yüksek Etkileşimli
Bulaşma derecesi	Düşük	Orta	Yüksek
Gerçek işletim sistemi	Yok	Yok	Var
Kurulum	Kolay	Zor	Çok zor
Bakım	Kolay	Kolay	Zaman alıcı
Risk	Düşük	Orta	Yüksek
Ele geçirilme beklentisi	Yok	Yok	Var
Kontrol gereksinimi	Yok	Yok	Var
Çalıştırmak için gerekli bilgi	Düşük	Düşük	Yüksek
Geliştirmek için gerekli bilgi	Düşük	Yüksek	Orta-Yüksek
Veri toplama	Kısıtlı	Orta	Kapsamlı
Etkileşim	Servis benzetimi	İsteklere göre	Tam kontrol

Düşük etkileşimli tuzak sistemler herhangi bir servisin ya da komple bir işletim sisteminin benzetimini yaparlar. Fakat servisler kullanılarak sistem ele geçirilemez. Orta etkileşimli tuzak sistemler, düşük etkileşimli tuzak sistemler gibi gerçek bir işletim sistemine sahip değildir. Ancak saldırgan ile daha çok etkileşime geçebilmesi ve daha karmaşık saldırıları üzerine çekebilmesi yönüyle düşük etkileşimli tuzak sistemlerden farklıdır. Yüksek etkileşimli tuzak sistemler saldırgan ile olan etkileşimi en yüksek olan tuzak sistemlerdir. Herhangi bir servisin benzetimini yapmak yerine gerçek işletim sistemleri üzerinde açıklık barındıran gerçek ağ servisleri sunarlar.

Tuzak sistem kavramının 1990 yılında Clifford Stoll'un "The Cuckoos Egg" ve Bill Cheswick'in "An Evening with Berferd" yayınlarıyla bilgi güvenliğinde kullanılmaya başlanmasıyla birlikte geliştirilen ve günümüzde aktif olarak kullanılan bazı önemli, açık kaynak kodlu, farklı türdeki tuzak sistemler arasında honeyd, dionaea, kippo, conpot, glastopf, thug sayılabilir [15]. Honeyd, dionaea ve kippo SMB, HTTP, FTP, TFTP, MSSQL ve SSH vb. protokollerin, conpot endüstriyel kontrol sistemlerin kullandığı protokollerin benzetimini yaparken, glastopf web uygulamaları ile ilgili açıklıkların benzetimini yapmaktadır. Thug ise istemci taraflı bir tuzak sistemdir. Bununla birlikte ADSL modem ve yönlendirici cihazlarda kullanılan TR-069 protokolü ile ilgili geliştirilmiş herhangi bir tuzak sistem türü bulunmamaktadır.

C. TR-069

TR-069 (Technical Report 069), Broadband Forum tarafından Mayıs 2004'te yayınlanmış ve CWMP (CPE WAN Management Protocol - Müşteri Tarafı Cihazı Geniş Alan Ağı Yönetim Protokolü) olarak adlandırılan teknik raporun kısa adıdır. İnternete bağlı modem, yönlendirici, ağ tabanlı depolama aygıtları, VoIP telefonlar vb. son kullanıcı cihazlarının uzaktan yönetimi için uygulama seviyesi protokolü tanımlar. Metin tabanlı çalışan TR-069 protokolünde mesajlar ACS (Auto Configuration Server - Otomatik Yapılandırma Sunucusu) ve CPE (Customer Premises Equipment - Müşteri Tarafı Cihazı) arasında transfer edilir. ACS genellikle internet servis sağlayıcı ya da kullanılan cihazı tedarik eden kurum tarafında bulunan sunucu iken CPE son kullanıcı tarafındaki yönlendirici, VoIP telefon gibi herhangi bir cihazdır. Nesnelerin interneti kullanımının yaygınlaşmasıyla protokolü kullanan cihaz sayısının giderek artacağı öngörülmektedir.

TR-069 protokolünün temel kullanım amaçları arasında otomatik yapılandırma, dinamik hizmet tedariki, aygıt yazılımı ve modül yönetimi, durum ve performans izleme, hata tanımlama sayılabilir. Protokol çift yönlü olarak SOAP/HTTP (Simple Object Access Protocol/Hypertext Transfer Protocol) üzerinde çalışmaktadır. Mesajlar XML (Extensible Markup Language) formatında RPC (Remote Procedure Call) yöntemiyle taraflara iletilmektedir [16].

TABLO II
TR-069 PROTOKOL YIĞINI

CPE / ACS Yönetim Uygulaması
RPC Metodları
SOAP
HTTP
SSL / TLS
TCP / IP

ACS ile CPE arasında oturumun kurulması aşamasında oturum her zaman CPE tarafından başlatılır. Oturumun başlatılmasında iki farklı senaryo vardır [17]. İlk olarak CPE herhangi bir nedenle ACS'ye bağlanabilir ki bu durumda CPE istemci iken ACS sunucu durumundadır. İkinci senaryoya göre ise ACS ilk yapılandırma, değişiklik, yazılım güncelleme vb. bir amaçla CPE'ye kendisine bağlanması için istek gönderir. CPE isteği işleyerek ACS'ye bağlantı kurar. Bu durumda CPE sunucu durumundayken ACS istemci durumuna geçmiştir. Ayrıca ikinci durum için cihaz üzerinde açık bir port bulunması gerekir. Bu port aynı zamanda saldırganlar için açık bir kapı anlamına gelmektedir.

ACS ve CPE iletişiminde kullanılan önemli bazı komutlar şunlardır [18]:

- *Inform:* CPE'den ACS'ye her oturum öncesi gönderilen komuttur. Oturum nedenini içerir.
- *GetRPCMethods:* CPE ya da ACS'nin desteklediği komut listesini öğrenmek amaçlı kullanılır.
- *GetParameterNames:* CPE'nin desteklediği parametrelerin listesini almak için kullanılır.
- *GetParameterValues:* İstenilen bir ya da daha fazla parametrenin güncel değerini döner.
- *SetParameterValues:* Bir veya birden fazla parametrenin değerini değiştirir.
- *Download:* CPE'ye belirtilen bir URL'den aygıt yazılımı, yapılandırma dosyası vb. bir dosyanın indirilmesini için kullanılır.
- *Reboot:* CPE'nin kapanıp açılmasını sağlar.

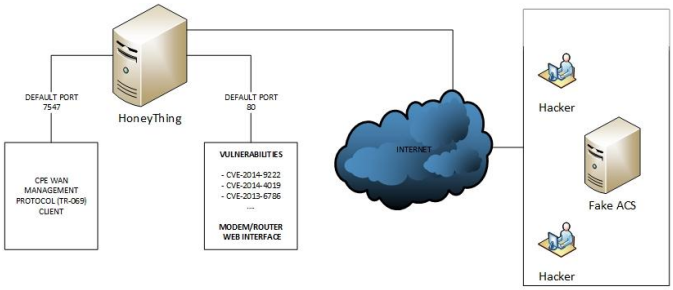
TR-069 protokolü HTTP basic, HTTP digest ya da sertifika tabanlı olmak üzere çift yönlü kimlik doğrulamayı gerektirir. CPE ACS'yi bağlantı isteğinde doğrularken, ACS CPE'yi oturumun başlatılması sırasında doğrular [19]. İletişimde HTTPS kullanılarak olası aradaki adam saldırılarının önüne geçmek hedeflenmiştir. Ancak protokolün işletimini sağlayan ACS/CPE üzerindeki uygulamalarda çeşitli açıklıklar bulunmaktadır. Ayrıca CPE'ler yönetimi için web uygulamalarına sahip olduğundan web tabanlı saldırılara karşı da hedef halindedir.

III. HONEYTHING

Bu bölümde nesnelerin interneti cihazlarından modem ve yönlendiricilere gelen saldırıların tespiti için geliştirilmiş düşük etkileşimli tuzak sistem olan HoneyThing, tasarım ve geliştirme, kullanım önerileri ve test başlıkları altında detaylıca incelenmiştir.

A. *Tasarım ve Geliştirme*

HoneyThing'in temel amacı modem ve yönlendiriciler için son yıllarda çıkmış popüler bazı açıklıklara karşı savunmasız, TR-069 protokolünü destekleyen bir sistem sunmak ve uygulama ile olan tüm etkileşimlerin detaylı bir şekilde kaydını tutmaktır. Bu çalışma kapsamında geliştirilen uygulama iki bölümden oluşmaktadır. Birinci kısımda bazı açıklıkların benzetimi yapılarak bir modem web arayüzü sunulmuştur. İkinci kısımda ise TR-069 protokolünün istemci tarafı komutlarının işletilmesini sağlayan uygulama HoneyThing'e entegre edilerek birlikte çalışması sağlanmıştır.



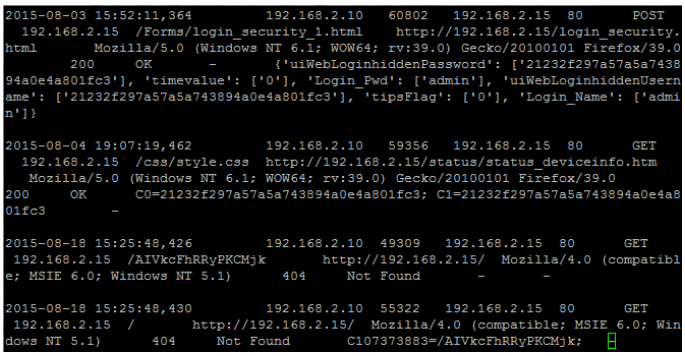
Şekil 1. HoneyThing tuzak sisteminin yapısı

İlk bölümün geliştirilmesi amaçlı farklı marka ve modelden birçok cihaz için açıklıklar araştırılmış ve günümüzde yaygın olarak kullanılan 3 açıklık tespit edilmiştir. Bu açıklıkların ortak yönü Allegro firması tarafından geliştirilen gömülü web sunucusu RomPager uygulamasında çalışmasıdır. TR-069 protokolünün çalıştığı sunucuların %52'sini oluşturan RomPager ve %52 içerisinde %98'lik dağılıma sahip 4.07 versiyonu, günümüzde halen yaklaşık 12 milyon cihaz tarafından kullanılmaktadır [20]. Açıklıklardan en önemlisi Aralık 2014 tarihinde Check Point firması araştırmacıları tarafından bulunan ve cihaz üzerinde yönetici hakkı elde etmeyi sağlayan "Misfortune Cookie"'dir (CVE-2014-9222) [21]. İstenilen yetkiyi elde eden saldırgan, DNS ayarlarını değiştirerek kullanıcı trafiği arasına girebilir, port yönlendirme ile modeme bağlı cihazlara erişebilir ve hassas kullanıcı verilerini ele geçirebilir. ROM-0 (CVE-2014-4019) açıklığında ise saldırgan cihaza ait yapılandırma bilgilerini içeren yedek (backup) dosyasını yetkilendirilmesi yapılmamış bir URL üzerinden indirebilmekte ve çeşitli yöntemlerle bu bilgilere ulaşabilmektedir [22]. Saldırganın sunucu üzerinde olmayan bir URL'ye gönderdiği özel istek sayesinde URL yönlendirme ve siteler arası betik çalıştırmayı sağlayan CVE-2013-6786 bir diğer önemli açıklıktır [23]. Sisteme benzer şekilde yeni açıklıklar eklenebilir. Sonuç olarak birinci bölüm, farklı açıklıklara sahip RomPager web sunucusunun

benzetimini yapmakta ve kullanıcının giriş yapıp çeşitli sayfaları görüntüleyebildiği bir web uygulaması sunmaktadır.

İkinci bölümde TR-069 protokolünün istemci tarafını gerçekleyen çeşitli uygulamalar araştırılmış ve Google çalışanları tarafından geliştirilmiş, açık kaynak kodlu "Catawampus" uygulaması HoneyThing'e entegre edilmiştir [24]. Bu kısımda hedef, TR-069 protokolü kullanılarak yapılabilecek bilinmeyen saldırıların tespiti, saldırgan davranışının kayıt altına alınması ve bu protokole yönelik saldırı miktarı vb. istatistiklerin çıkarılmasıdır.

HoneyThing 3 adet kayıt dosyası tutmaktadır. "http.log", benzetimi yapılan web sunucusunun HTTP iletişimi ile ilgili kayıtları, "tr-069.log" ise TR-069 protokolü haberleşmesi ile ilgili kayıtları tutmaktadır. "honeything.log" dosyasında uygulamanın içsel hata ve bilgilere ait kayıtlar yer almaktadır. Tüm kayıtlar ayrıştırılmasını kolaylaştırmak amaçlı "tab" karakteriyle ayrılmış olarak yazılmakta ve dosyalar metin belgesi formatında tutulmaktadır. Bu format ile gelecekte saldırılar veri tabanlarına aktarılarak detaylı analizler yapılabilecektir.



Şekil 2. HoneyThing HTTP kayıt dosyası içeriği

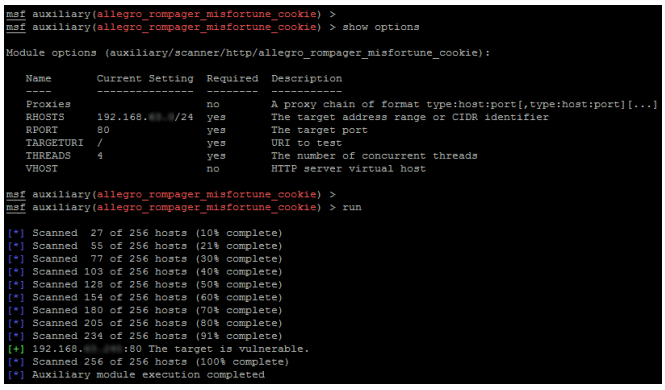
Uygulama Python programlama dili ile geliştirilmiştir. Bu nedenle taşınabilir ve Python çalıştıran herhangi bir işletim sistemi üzerine kolayca kurulumu yapılabilmektedir. Kurulum sonrası port bilgileri, web uygulaması yetkilendirme bilgileri ve modem/yönlendirici cihaza ait çeşitli bilgiler yapılandırma dosyası aracılığıyla değiştirilebilmektedir. Varsayılan olarak uygulama tüm ağ arayüzlerini dinlemekte, HTTP için 80, TR-069 için varsayılan bağlantı isteği portu olan 7547'yi kullanmaktadır.

B. *Kullanım Önerileri*

HoneyThing düşük etkileşimli bir tuzak sistem de olsa izole bir ağ ortamında kullanılması tavsiye edilmektedir. Örneğin TR-069'un "Download" komutu ile sisteme indirilecek herhangi bir zararlı yazılımın çalıştırılması ağdaki diğer makinalara zarar verebilir. Tuzak sistemin farklı lokasyonlarda çalıştırılması durumunda o ülkeye ait ISP'lerin sunduğu modem/yönlendirici cihazlarında bağlantı isteği için kullanılan port'un TR-069 portu olarak ayarlanması sistemin kullanılabilirliğini arttıracaktır. Ayrıca çoklu kullanımda saklanan kayıt dosyaları ayrıştırılabilir formatta olduğundan merkezi bir kayıt sunucuda toplanarak Kibana, Splunk benzeri açık kaynak kodlu bir uygulama ile izlenebilir.

C. *Test*

HoneyThing'in birinci kısmına ait açıklıklar manuel olarak ve Metasploit sızma testi aracı ile test edilmiştir. Metasploit aracı üzerinde bulunan tarayıcılardan "allegro_rompager_misfortune_cookie" modülü ile HoneyThing'in bulunduğu ağ taranmış ve HoneyThing için "Vulnerable" sonucu döndüğü gözlemlenmiştir [25].



Şekil 3. HoneyThing tuzak sisteminin Metasploit uygulamasıyla test edilmesi

İkinci kısımda ise TR-069 protokolünün çalışması için gerekli olan ACS "VMware Workstation" üzerinde sanal olarak hazırlanmıştır. ACS için OpenACS'nin devamı olan LibreACS adlı açık kaynak kodlu uygulaması kullanılmıştır. ACS (LibreACS) ve CPE (HoneyThing) çalıştırıldığında protokolün başarılı bir şekilde gerçeklendiği ve iletişimin kayıt altına alındığı izlenmiştir [26].

IV. SONUÇ VE ÖNERİLER

Nesnelerin interneti kavramının giderek önem kazandığı günümüzde bu kavram kapsamına giren cihazlara gelen saldırılarda da önemli artışlar olmuştur. Donanımsal olarak yetersiz olan bu cihazlarda klasik saldırı tespit sistemleri kullanılamamaktadır. Saldırı tespiti için önemli bir yöntem olan tuzak sistemler günümüzde birçok protokol için geliştirilmiş olsa da nesnelerin interneti cihazlarından TR-069 protokolünü kullanan modem/yönlendiriciler için geliştirilmiş bir sistem bulunmamaktadır. HoneyThing bu eksikliği gidermekle birlikte, bu çalışma farklı türde birçok cihazı içine alan nesnelerin interneti cihazlarında saldırı tespiti için tuzak sistem kullanımını önermektedir.

Nesnelerin interneti için geliştirilecek tuzak sistem uygulamaları normal tuzak sistem uygulamalarından farklı olarak sadece protokolün benzetimini yapmak yerine cihaza özel özellikleri de yansıtması gerekmektedir. Cihazların kullandığı port, komut seti ve benzeri bilgiler tedarikçi firmaya göre değişeceğinden tuzak sistem, hedef alınan kapsama göre yapılandırılabilir olmalıdır.

Geliştirilmesi devam eden HoneyThing'e yeni açıklık modülleri eklenebileceği gibi, kayıtların veritabanı, syslog vb. yerlere yazılması, Honeynet topluluğun veri besleme protokolü olan "hpfeeds"'in desteklenmesi, saldırganın komut satırına düşmesi durumunda belli başlı bazı kabuk komutlarının benzetiminin yapılması benzeri birçok özellik eklenerek daha verimli bir kullanım hedeflenmektedir.

KAYNAKÇA

[1] Y. Liu, G. Zhou, *"Key Technologies and Applications of Internet of Things"*, Fifth International Conference on Intelligent Computation Technology and Automation (ICICTA), p. 197-200, 2012.

[2] L. Atzori, A. Iera, G. Morabito, *"The Internet of Things: A survey"*, The International Journal of Computer and Telecommunications Networking vol.54,p. 2787-2805, 2010.

[3] K. Ashton, *"That 'Internet of Things' Thing"*, RFID Journal, 2009 [Online], Avaliable: http://www.rfidjournal.com/articles/pdf?4986

[4] The Internet of Things, International Telecommunication Union, November 2005 [Online], Avaliable: http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf

[5] Internet of Things - An action plan for Europe, Commission Of The European Communities, Brussels, 278 final, 18.6.2009 COM(2009) [Online], Avaliable: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0278&from=EN

[6] D. Evans, *"The Internet of Things How the Next Evolution of the Internet Is Changing Everything"*, Cisco IBSG, 2011 [Online], Avaliable: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[7] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, T. Razafindralambo, *"A Survey on Facilities for Experimental Internet of Things Research"*, Communications Magazine, IEEE vol. 49, p. 58–67, 2011.

[8] J. Pescatore, G. Shpantzer, *"Securing the 'Internet of Things' Survey"*, A SANS Analyst Survey, 2014 [Online], Avaliable: https://www.sans.org/reading-room/whitepapers/analyst/securing-internet-things-survey-34785

[9] A. Atamli, A. Martin, *"Threat-Based Security Analysis for the Internet of Things"*, International Workshop on Secure Internet of Things (SIoT), p. 35-43, 2014.

[10] OWASP Internet of Things Top Ten Project, 2014 [Online], Avaliable: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

[11] S. Raza, L. Wallgren, T. Voigt, *"SVELTE: Real-time intrusion detection in the Internet of Things"*, Journal Ad Hoc Networks, vol.11, Issue 8, p. 2661–2674, 2013.

[12] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, M. A. Spirito, *"An IDS Framework for Internet of Things Empowered by 6LoWPAN"*, 20th ACM Conference on Computer and Communications Security (CCS), 2013.

[13] Deliverable D5.3: Case Study: Malicious Activity in the Turkish Network, Information & Communication Technologies Trustworthy ICT, Seventh Framework Programme, SysSec, February 2013 [Online], Avaliable: http://www.syssec-project.eu/m/page-media/3/syssec-d5.3-TurkishNetworkCaseStudy.pdf

[14] Abhishek Mairh, *"Honeypot in Network Security: A Survey"*, Department of Computer Sc. Engg. International Institute of Information, p. 600-605, 2005.

[15] R. C. Joshi (Editor), Anjali Sardana (Editor), *"Honeypots: A New Paradigm to Information Security"*, ISBN-13: 978-1578087082, ISBN-10: 1578087082, p. 1-6, 2011.

[16] L. Zheng, Y. Hu, S. Chen, *"Research and Application of CWMP in Distributed Network Management System"*, International Conference on Computer Science and Service System (CSSS), p. 647-650, 2012.

[17] JPM. Rojas, *"Split Management of TR069 Enabled CPE Devices"*, Master of Science Thesis, POLITECNICO DI TORINO, 2011 [Online], Avaliable: http://repository.javeriana.edu.co/bitstream/10554/7075/1/tesis537.pdf

[18] TR-069 CPE WAN Management Protocol, Issue: 1 Amendment 5, November 2013 [Online], Avaliable: https://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf

[19] J. Walls, T. Sheehan, *"TR-069 - A Crash Course"*, Interoperability Laboratory, University of New Hampshire, 2009 [Online], Avaliavble: https://www.iol.unh.edu/sites/default/files/knowledgebase/hnc/TR-069_Crash_Course.pdf

[20] S. Tal, L. Oppenheim, *"The Internet of TR-069 Things: One Exploit to Rule Them All"*, RSA Conference, 2015 [Online], Avaliable: https://www.rsaconference.com/writable/presentations/file_upload/hta-r04-the-internet-of-tr-069-things-one-exploit-to-rule-them-all_final.pdf

[21] Check Point's Malware and Vulnerability Research Group, Misfortune Cookie Vulnerability, 2014 [Online], Avaliable: http://mis.fortunecook.ie/

[22] T. Hlaváček, *"Impact of 'rom-0' vulnerability"*, 2014 [Online], Avaliable: https://ripe69.ripe.net/presentations/61-rom0-vuln.pdf

[23] A. V. Blanco, CVE-2013-6786, 2013 [Online], Avaliable: http://osvdb.org/ref/99/rompager407.pdf

[24] Catawampus, TR-069 management for a CPE device in Python, 2012 [Online], Avaliable: https://code.google.com/p/catawampus

[25] J. Hart, L. Oppenheim, *"Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner"*, 2015 [Online], Avaliable: http://www.rapid7.com/db/modules/auxiliary/scanner/http/allegro_rompager_misfortune_cookie

[26] LibreACS, The fork of OpenACS a still open source TR-069 CWMP server, 2015 [Online], Avaliable: http://sourceforge.net/projects/libreacs

Ö. Erdem, 2012 yılında İstanbul Ticaret Üniversitesi Bilgisayar Mühendisliği Bölümünden mezun oldu. 2013 yılında başladığı İstanbul Şehir Üniversitesi Bilgi Güvenliği Mühendisliği yüksek lisansı tez aşamasındadır. 2012 yılından bu yana TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü bünyesinde araştırmacı olarak görev yapmaktadır. Saldırı tespit ve önleme sistemleri, ağ güvenliği, unix/linux sistemler, web teknolojileri konularında çalışmış olmakla birlikte çeşitli açık kaynak kodlu yazılımlar hakkında tecrübe sahibidir.

M. Kara, 1993 yılında Yıldız Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliği Bölümünden mezun oldu. 1996 yılında Yüksek Lisansını, 2002 yılında da Doktorasını Kocaeli Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Anabilim dalında tamamladı. Doktora tezini Bilgisayar Ağlarında Çok Yollu Yönlendirme konusunda yaptı. 1994-2000 yılları arasında Kocaeli Üniversitesi Bilgisayar Mühendisliği bölümünde Araştırma Görevlisi olarak, 2000-2001 yıllarında Armada Bilgisayar AŞ'de Sistem Mühendisi olarak çalıştı. 2001'den beri TÜBİTAK BİLGEM'de çalışmaktadır. Bulanık mantık, siber güvenlik, ağ ve sistem, protokol güvenlik analizi, kritik altyapı güvenliği, güvenli yazılım geliştirme, Ortak Kriterler, sistem, yazılım/donanım güvenlik testleri konularında çalışmaktadır. Ulusal ve uluslararası dergi ve konferanslarda yayınları bulunmaktadır.

A. İkinci, 2007 yılında Mannheim Üniversitesinden Bilgisayar Yüksek Mühendisi olarak mezun oldu. 2006 yılından bu yana Siber Güvenlik alanında çalışmalar yapmakta ve özellikte tuzak sistemler konusuyla ilgilenmektedir. 2012 yılında Honeynet Projesinin Türkiye bölümünü kurmuştur. 2007'beri zararlı yazılım analizi, sandboxing ve zararlı içerik barındıran web siteleri konularında çalışmaktadır.