HoneyThing: Nesnelerin İnterneti için Tuzak Sistem

Bu tez Bilgi Güvenliği Mühendisliği'nde
Tezli Yüksek Lisans Programının bir koşulu olarak

Ömer ERDEM

tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.

İSTANBUL
ŞEHİR
ÜNİVERSİTESİ

Bu tezi okuduk, kapsam ve nitelik açısından Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans derecesi için tümüyle uygun olduğu görüşüne vardık.

ONAYLAYANLAR:

Dr. Mehmet Kara .....
(Tez Danışmanı)

Prof. Dr. Tahsin Erkan Türe .....

Prof. Dr. Nevcihan Duru .....

Bu tez İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü tarafından belirlenen tüm koşullara uygundur.

ONAY TARİHİ: 24 Aralık 2015

MÜHÜR/İMZA:

Yazarlık Beyanı

Ben, Ömer ERDEM, başlığı, 'HoneyThing: Nesnelerin İnterneti için Tuzak Sistem ' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza: 

Tarih: 24.12.2015

"Şimdiki zaman onlara ait olabilir, ama gelecek, ki ben hep bunun için çalıştım, bana ait."

Nikola Tesla

HoneyThing: Nesnelerin İnterneti için Tuzak Sistem

Ömer Erdem

Öz

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.

İnternete bağlı nesneler bilgisayar, sunucular gibi güçlü donanıma sahip olmadıklarından bu cihazların bünyesinde saldırı tespiti için klasik yöntemler kullanılamamaktadır. Saldırı tespiti amaçlı kullanılan önemli yapılardan biri olan tuzak sistemlerin günümüzde birçok protokol için uygulamaları bulunmaktadır. Tuzak sistemler hedef sistemin benzetimini yaparak saldırgan ve kullandığı yöntem hakkında bilgi toplamayı hedefler. İnternete bağlı nesnelerin uzaktan yönetimi için yaygın olarak kullanılan protokollerden biri olan TR-069 için geliştirilmiş bir tuzak sistem uygulaması bulunamamaktadır.

Son yıllarda çıkan açıklıklar ve potansiyel kurban sayısının giderek artması saldırganların nesnelerin interneti alanına yönelmesine neden olmuştur. Bu çalışmada internete bağlı nesnelerde saldırı tespiti için tuzak sistem kullanımı ele alınmıştır. TR-069 protokolü kullanan modem/yönlendirici gibi cihazlar için tuzak sistem uygulaması geliştirilmiş, yapılan testler sonucunda uygulamanın hedeflenen özellikleri sağladığı gözlemlenmiştir.

Anahtar Sözcükler: Nesnelerin İnterneti, Tuzak Sistem, TR-069, Modem/Yönlendirici, RomPager

Teşekkür

Tez çalışmam süresince her türlü yardım ve fedakârlıkta bulunan; bilgi, görüş, tecrübe ve güler yüzü ile çalışmama ışık tutan saygıdeğer danışmanım Sayın Dr. Mehmet Kara'ya sonsuz teşekkürlerimi sunarım.

Tezimin hazırlanması, konu bulunması sırasında beni cesaretlendiren, ümit veren ve manevi destek sağlayan değerli iş arkadaşlarıma özellikle, Bâkır Emre ve Ulaş Kaya'ya, bu süreçte her zaman yanımda olarak manevi desteklerini eksik etmeyen aileme ve dostlarıma teşekkürü bir borç bilirim.

İçindekiler

Yazarlık Beyanı **ii**

Öz **iv**

Teşekkür **v**

Şekil Listesi **viii**

Tablo Listesi **ix**

Kısaltmalar **x**

1 Giriş **1**

2 Nesnelerin İnterneti **4**
2.1 Giriş . . . 4
2.2 Tarihsel Gelişimi ve Gelecek Öngörüsü . . . 6
2.3 Gerekli Teknolojiler . . . 7
2.4 Uygulamaları ve Etki Alanları . . . 8
2.4.1 Akıllı Ortam . . . 8
2.4.2 Sağlık Hizmetleri . . . 9
2.4.3 Ulaşım ve Lojistik . . . 10
2.4.4 Kişisel ve Sosyal . . . 11
2.4.5 Enerji ve Madencilik . . . 11
2.5 Güvenlik . . . 12
2.5.1 Tehdit Kaynakları . . . 13
2.5.2 Atak Vektörleri . . . 14
2.5.2.1 Web Arayüzleri . . . 14
2.5.2.2 Yetersiz Kimlik/Erişim Denetimi . . . 15
2.5.2.3 Ağ Servisleri . . . 15
2.5.2.4 Şifreleme Eksikliği . . . 15
2.5.2.5 Cihaz Yazılımları . . . 16
2.5.2.6 Fiziksel Güvenlik Eksikliği . . . 16
2.5.3 Önlemler . . . 16
2.5.4 Saldırı Tespiti . . . 17

3 Tuzak Sistemler **19**
3.1 Giriş . . . 19
3.2 Tuzak Sistem Türleri . . . 21

3.2.1 Düşük Etkileşimli Tuzak Sistemler . . . 22
3.2.2 Orta Etkileşimli Tuzak Sistemler . . . 22
3.2.3 Yüksek Etkileşimli Tuzak Sistemler . . . 23
3.3 Tuzak Sistem Örnekleri . . . 24

4 TR-069 **26**
4.1 Giriş . . . 26
4.2 Terminoloji . . . 26
4.3 Kullanım Amaçları . . . 27
4.3.1 Otomatik Yapılandırma ve Dinamik Hizmet Sağlama . . . 27
4.3.2 Yazılım/Bellenim İmaj Yönetimi . . . 28
4.3.3 Yazılım Modül Yönetimi . . . 28
4.3.4 Performans ve Durum İzleme . . . 28
4.3.5 Hata Tanılama . . . 28
4.4 Mimari . . . 29
4.5 RPC Metotları . . . 30
4.5.1 CPE Metotları . . . 30
4.5.2 ACS Metotları . . . 31
4.6 Oturum Yönetimi . . . 32
4.7 Güvenlik Özellikleri . . . 34

5 HoneyThing **35**
5.1 Giriş . . . 35
5.2 Geliştirme Ortamı . . . 35
5.3 Sistem Bileşenleri . . . 37
5.3.1 HTTP . . . 37
5.3.1.1 CVE-2014-9222 . . . 39
5.3.1.2 CVE-2014-4019 . . . 41
5.3.1.3 CVE-2013-6786 . . . 42
5.3.1.4 Modem Yönetim Arayüzü . . . 42
5.3.2 TR-069 . . . 42
5.4 HoneyThing Kayıtları . . . 44
5.4.1 HTTP Kayıtları . . . 44
5.4.2 TR-069 Kayıtları . . . 46
5.4.3 Sistem Kayıtları . . . 46
5.4.4 Kayıtların İzlenmesi ve Analizi . . . 47
5.5 Kurulum ve Kullanım . . . 48
5.6 Test . . . 50
5.6.1 Test Ortamı . . . 51
5.6.2 Test Sonuçları . . . 52

6 Sonuç ve Öneriler **56**

A TR-069 CPE Sunucu Türlerinin Dağılımı **58**

B Yayınlar **60**

Kaynaklar **61**

Şekil Listesi

2.1 Nesnelerin interneti kavramının tanımlanmasında kullanılan yaklaşımlar . 4
2.2 İnternete bağlı nesne sayısının yıllara göre değişimi 7
2.3 Nesnelerin internetinin günlük yaşamdaki uygulamaları 10

3.1 Tuzak sistemlerin izole edilmiş ağ ortamında çalışması 20
3.2 Tuzak sistemlerin bulut ortamında çalışması 23

4.1 CWMP mimarisi 29
4.2 CWMP oturumunun kurulması 32

5.1 PyCharm Python tümleşik geliştirme ortamı 36
5.2 HoneyThing tuzak sisteminin yapısı 37
5.3 TR-069 sunucu türlerinin dağılımı 38
5.4 RomPager gömülü web sunucusunun versiyon dağılımı 38
5.5 "Misfortune Cookie" açıklığı saldırı senaryosu 40
5.6 "Misfortune Cookie" açıklığından etkilenen cihaz sayısının ülkelere göre dağılımı 40
5.7 Test modemi ile kaydedilen TR-069 protokolüne ait örnek iletişim 43
5.8 HoneyThing kayıt dosyalarında yer alan bilgiler 45
5.9 HoneyThing HTTP kayıt dosyası içeriği 45
5.10 HoneyThing TR-069 kayıt dosyası içeriği 46
5.11 HoneyThing sistem kayıt dosyası içeriği 47
5.12 HoneyThing örnek yapılandırma dosyası 49
5.13 HoneyThing test ortamı 51
5.14 HoneyThing üzerinde CVE-2013-6786 açıklığının testi 52
5.15 HoneyThing'den indirilen ROM-0 dosyasından hassas bilgilerin elde edilmesi 53
5.16 HoneyThing üzerinde "Misfortune Cookie" açıklığının testi 53
5.17 ACS üzerinde iletişim kurulan HoneyThing'e ait özet bilgilerin görüntülenmesi 54

Tablo Listesi

2.1 Cihazlarda tespit edilen farklı türdeki açıklıklar. 14

3.1 Saldırgan ile olan etkileşimlerine göre tuzak sistemlerin karşılaştırılması. . 24

4.1 CWMP protokol yığını. 29
4.2 CPE metotlarının kullanım örnekleri. 31
4.3 Inform RPC olay kodu ve tanımları. 33

A.1 TR-069 sunucu türlerinin dağılımı 58

Kısaltmalar

6LoWPAN	IPv**6** (over) **L**ow power **W**ireless **A**rea **P**rotocol
ACS	**A**uto **C**onfiguration **S**erver
ADSL	**A**symmetric **D**igital **S**ubscriber **L**ine
BSD	**B**erkeley **S**oftware **D**istribution
CPE	**C**ustomer **P**remises **E**quipment
CSRF	**C**ross-**S**ite **R**equest **F**orgery
CWMP	**C**PE **W**AN **M**anagement **P**rotocol
DNS	**D**omain **N**ame **S**ystem
DoS	**D**enial **o**f **S**ervice
EB	**E**xa**B**yte
ELK	**E**lasticsearch **L**ogstash and **K**ibana
ERP	**E**nterprise **R**esource **P**lanning
FTP	**F**ile **T**ransfer **P**rotocol
GPS	**G**lobal **P**ositioning **S**ystem
HTTP	**H**yper **T**ext **T**ransfer **P**rotocol
IANA	**I**nternet **A**ssigned **N**umbers **A**uthority
IBM	**I**nternational **B**usiness **M**achines
IBSG	**I**nternet **B**usiness **S**olutions **G**roup
IDS	**I**ntrusion **D**etection **S**ystem
IGD	**I**nternet **G**ateway **D**evice
IoT	**I**nternet **o**f **T**hings
IP	**I**nternet **P**rotocol
ISP	**I**nternet **S**ervice **P**rovider
ITU	**I**nternational **T**elecommunication **U**nion
LOM	**L**ights-**O**ut **M**anagement

LTS	**L**ong **T**erm **S**upport
M2M	**M**achine **to M**achine
MIT	**M**assachusetts **I**nstitute of **T**echnology
NAS	**N**etwork **A**ttached **S**torage
NAT	**N**etwork **A**ddress **T**ranslation
OWASP	**O**pen **W**eb **A**pplication **S**ecurity **P**roject
PLC	**P**rogrammable **L**ogic **C**ontroller
PoC	**P**roof **o**f **C**oncept
RFID	**R**adio-**F**requency **ID**entification
RPC	**R**emote **P**rocedure **C**all
RPM	**R**ed Hat **P**ackage **M**anager
SANS	**S**ysAdmin **A**udit **N**etworking **S**ecurity
SCADA	**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition
SFTP	**S**ecure **F**ile **T**ransfer **P**rotocol
SIP	**S**ession **I**nitiation **P**rotocol
SMB	**S**erver **M**essage **B**lock
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol
SOAP	**S**imple **O**bject **A**ccess **P**rotocol
SQL	**S**tructured **Q**uery **L**anguage
SSH	**S**ecure **Sh**ell
SSL	**S**ecure **S**ocket **L**ayer
STUN	**S**ession **T**raversal **U**tilities for **N**AT
TCP	**T**ransmission **C**ontrol **P**rotocol
TFTP	**T**rivial **F**ile **T**ransfer **P**rotocol
TLS	**T**ransport **L**ayer **S**ecurity
URL	**U**niform **R**esource **L**ocator
USB	**U**niversal **S**erial **B**us
VoIP	**V**oice **o**ver **I**nternet **P**rotocol
XML	E**X**tensible **M**arkup **L**anguage
XMPP	E**x**tensible **M**essaging and **P**resence **P**rotocol
XSS	**Cross S**ite **S**cripting

Bölüm 1

Giriş

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]. Bu gelişmelerin sosyal yaşama getirdiği imkânların kullanıcılar arasında hızla yayılması, nesnelerin interneti alanına 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. Son yıllarda farklı türdeki cihazlarda çıkan açıklıklar ve olası açıklık durumunda potansiyel kurban sayısının çok fazla olması saldırganlar için cezbedici bir ortam oluşturmuştur.

İnternete bağlı nesneler arasında buzdolabı, su ısıtıcısı, ütü, televizyon vb. olmak üzere günlük yaşamda aktif olarak kullandığımız farklı türde birçok cihaz sayılabilir. Ev ya da küçük ofis kullanıcılarının internete bağlanmak için kullandığı ADSL modem/yönlendirici cihazlar bunlardan biridir. Son 10-15 yıllık zaman dilimi ile birlikte artık herkesin evinden internete bağlandığı düşünüldüğünde bu cihazların sayısında önemli artışlar olduğu görülmektedir. Bu durum cihazlarla ilgilenen 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 protokolünün getirdiği yeteneklerden faydalanılmaktadır. 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 bir süreç haline gelmektedir. 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 internete bağlı nesnelerin kısıtlı bant genişliği, hafıza, hesaplama yeteneği ve enerjiye sahip olmasından dolayı üzerlerinde yüksek işlem gücü gerektiren klasik saldırı tespit sistemlerini kullanmanın imkânsız olmasıdır. Ayrıca bu cihazlar kişisel bilgisayarlar gibi sürekli gözetim altında olmadığından olası bir anomalinin tespiti, fark edilmesi zordur.

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, Modbus 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.

Bu tez çalışması kapsamında TR-069 protokolünü kullanan internete bağlı nesnelerde saldırı tespiti için tuzak sistem kullanımı ele alınmış ve bu cihazlardan ADSL modem/yönlendiriciler için bir tuzak sistem uygulaması geliştirilmiştir. TR-069 protokolü ve açıklıklar olmak üzere iki ana bölümden oluşan uygulama farklı ağlarda çeşitli araçlarla test edilmiş ve sonuçları gözlemlenmiştir.

Çalışmanın ve geliştirilen uygulamanın anlaşılmasını sağlamak amaçlı farklı başlıklar altında nesnelerin interneti, tuzak sistemler, TR-069 protokolü konuları ile ilgili temel bilgiler, literatür taraması detaylıca ele alınmıştır. 2. bölümde nesnelerin interneti tarihsel gelişimi, uygulamaları ve güvenlik başlıkları altında incelenmiştir. 3. bölüm tuzak sistem kavramını açıklamakla birlikte, tuzak sistem türleri, geçmişte ve günümüzde kullanılan tuzak sistem türlerine değinmektedir. 4. bölümde TR-069 protokolü özellikleri,

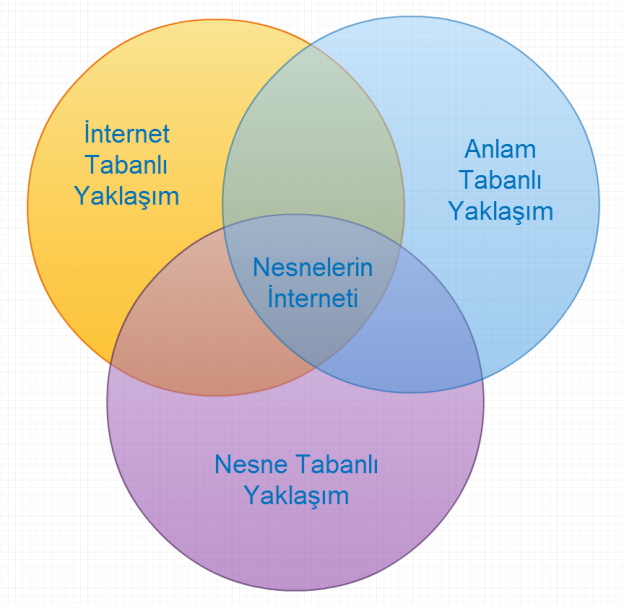
kullanım amaçları, oturum yönetimi ve güvenlik özellikleriyle birlikte anlatılmıştır. 5. bölümde geliştirilen uygulama sistem tasarımından, test ortamına, kurulum ve kullanımdan çıktılarına kadar detaylıca tanıtılmıştır. Bölüm 6'da ise çalışma ile ilgili sonuç ve ileriye dönük çalışmalar için önerilere yer verilmiştir.

Bölüm 2

Nesnelerin İnterneti

2.1 Giriş

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.



ŞEKİL 2.1: Nesnelerin interneti kavramının tanımlanmasında kullanılan yaklaşımlar.

Bu kavram kapsamına giren akıllı nesnelerin sahip olması gereken bazı özellikler şöyle sıralanabilir [3]:

- Büyüklük, şekil gibi çeşitli fiziksel özellikleri olmalıdır.
- Gelen mesajları kabul edip yanıtlama, ağ üzerinde arandığında bulunabilme vb. gibi minimum iletişim gereksinimlerini karşılaması gerekmektedir.
- İletişim sağlanabilmesi ve nesnesin tanımlanabilmesi için bir isim ve tekil bir adrese sahip olmalıdır.
- Gelen mesajları işleyerek pasif RFID etiketi ile ilişkilendirmekten çeşitli ağ işlemleri, servislerin keşfine kadar birçok temel ve karmaşık hesaplama yeteneklerine sahip olması gerekmektedir.
- Fiziksel dünyadaki ışık, ısı, elektromanyetik radyasyon seviyesi gibi değişiklikleri algılaması ya da fiziksel dünya ile etkileşime geçerek ona göre ilgili işlemi uygulaması gerekmektedir.

Nesnelerin internetinin bu özelliklere ve internet, nesne, anlamsal yönlerine göre ortaya çıkan bazı tanımlar şöyledir:

- Standart iletişim protokollerine dayanan, tekil olarak adreslenebilen ve birbirlerine bağlanabilen nesnelerden oluşan ağdır.
- Algıladığı, çevresiyle iletişime geçerek elde ettiği bilgiler ile kendi arasında ve çevresindeki çeşitli iş, sosyal, bilgi süreçleriyle iletişime geçerek çalışan bu süreçleri etkileyip herhangi bir olayı tetikleyebilen cihazların oluşturduğu topluluktur.
- Bilgi ve iletişim teknolojilerini kullanarak bir yerleşim yeri ile ilgili kritik altyapı ve eğitim, sağlık, güvenlik, ulaşım gibi hizmetlerin daha etkili ve etkileşimli kullanılabilmesine olanak sağlayan sistemdir [4].

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.

2.2 Tarihsel Gelişimi ve Gelecek Öngörüsü

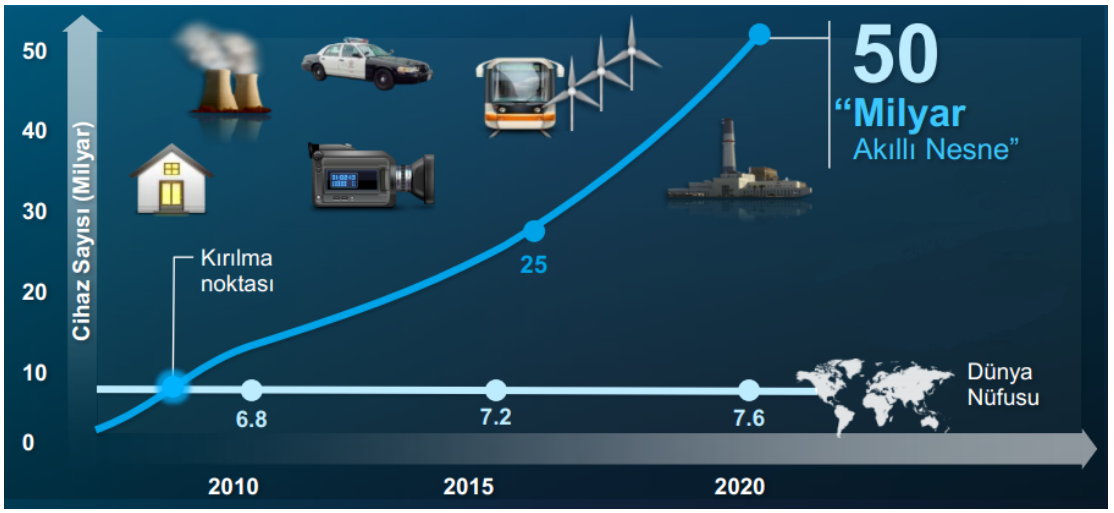
Nesnelerin interneti kavramı ilk olarak 1999 yılında MIT Auto-ID Center kurucularından olan Kevin Ashton tarafından Procter & Gamble (P&G) şirketinde tedarik zinciri yönetimini konu aldığı bir sunumun başlığı olarak kullanılmıştır [5]. MIT Auto-ID laboratuvarı RFID altyapısı üzerinde çalışmakta olduğundan bu tarihle birlikte nesnelerin interneti RFID teknolojisi kapsamında geliştirilmeye devam etmiştir.

2005 yılında International Telecommunication Union (ITU) tarafından yayınlanan "ITU Internet Report 2005: Internet of Things" raporu ile birlikte "Nesnelerin İnterneti" kavramı resmi olarak duyurulmuştur. 6 bölümden oluşan raporda genel olarak nesnelerin interneti için teknik anahtar kavramlar, RFID ile birlikte çeşitli sensör teknolojileri, akıllı nesneler, potansiyel pazar fırsatları, güvenlik, mahremiyet, nesnelerin internetinin gelecek on yılda yaşam biçimini nasıl şekillendireceği vb. konulara değinilmiştir [6].

Avrupa Birliği 2009 yılında "Nesnelerin İnterneti – Avrupa için Eylem Planı" başlıklı bir eylem planı yayınlayarak konuya verdiği önemi göstermiştir. Eylem planında nesnelerin interneti kavramı, teknolojinin yönetimi, var olan uygulamalar, mahremiyet ve kişisel verilerin korunması, standartlaştırma, araştırma/geliştirme, kurumsal farkındalık vb. konular yer almıştır [7].

2005 yılında ITU Strateji ve Politika Birimi'nden Lara Srivastava teknolojinin gelişimine ve hızlı yayılmasına vurgu yaparak *"Teknolojinin bugün 10 yıl öncesinde hayal ettiğimizden çok daha yayılmış olduğundan eminim. Yeni teknolojilerin bize gösterdiği bundan 10 yıl sonra da gelişimin bu yönde devam edeceğidir."* sözlerini ifade etmiştir. Beklenen şekilde teknolojinin gelişmesiyle birlikte internete dâhil olan cihaz/nesne sayısı gün geçtikçe artmış ve artmaktadır.

Cisco IBSG 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 bir bu oranın 2 katına çıkacağı öngörülmektedir. 2020 yılına gelindiğinde dünya nüfusunun 7,6 milyar, internete bağlı cihaz sayısının 50 milyar olacağı tahmin edilmektedir [8].



ŞEKİL 2.2: İnternete bağlı nesne sayısının yıllara göre değişimi.

Nesnelerin internetinin gelişim göstergeleri internetin büyüme hızı ve bu alana yapılan yatırımlardır. İnternet üzerindeki toplam IP trafiği 2012 yılında aylık 43.57 EB (Exabyte) iken, 2014 yılında bu sayı 62.47 EB olmuştur. Trafiğin artışında internete daha çok cihazın bağlanmasına olanak sağlayan IPv6 teknolojisinin etkisi olmuştur. Yapılan yatırımlara bakıldığında ise 2012'den 2014'e bu alanda ürün geliştiren eleman sayısı 122 binden 300 bine, sermaye aktarımı 738 milyon dolardan 960 milyar dolara yükselmiştir [9]. 2013 yılında 613 milyar dolar ekonomik katkısı olan nesnelerin interneti teknolojisinin 2020 yılında değeri 19 trilyon dolar olması öngörülmektedir. Yapılan araştırmalar sonucu elde edilen verilere bakıldığında nesnelerin internetinin günümüz ve geleceğin teknolojisi olarak tanımlamak mümkündür.

2.3 Gerekli Teknolojiler

Nesnelerin interneti teknolojisinin gelişmesine, yaygınlaşmasına katkı sağlayacak bazı önemli teknolojiler şunlardır [10]:

- İki ya da daha fazla düğüm arasında anlaşmayı sağlayacak iletişim protokolleri ve M2M (Machine to Machine) arayüzleri
- Nesnelerin içerisine yerleştirilecek mikro denetleyiciler, gömülü sistem teknolojisi
- Kısa/uzun mesafe, tek/çift yönlü özellikleri sunabilen kablosuz iletişim altyapısı
- Eş zamanlı olarak birçok nesneyi tanımlayabilen RFID teknolojisi

- Güç kaynaklarının yetersiz olduğu durumlarda destek olabilecek alternatif enerji sağlama altyapısı
- Çevresindeki değişiklikleri algılayıp merkezi bir sisteme raporlayabilen sensörler
- İnsanların ve nesnelerin konumunun belirlenebilmesi için GPS teknolojisi
- Dağıtık çalışma, veri yapıları vb. birçok farklı yönü ve yetenekleri olan yazılımlar

2.4 Uygulamaları ve Etki Alanları

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 [11]:

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

2.4.1 Akıllı Ortam

Ev, ofis gibi ortamlarda kullanıcının havalandırma, aydınlanma, ısınma ve güvenlik sistemlerini herhangi bir mobil cihaz ile uzaktan kontrol edebilmesi, cihazların sensörler aracılığıyla ortam değişikliğini algılayıp harekete geçmesidir. Oda sıcaklığının tercihler ve hava durumuna göre ayarlanması, aydınlatmanın günün farklı zaman dilimlerine göre değişmesi, alarm sistemleri sayesinde güvenliğin sağlanması, gereksiz elektronik cihazların

otomatik olarak kapatılıp enerji tasarrufu sağlanması örnekler arasındadır. Bu şekilde kaynaklar verimli tüketilerek hem şahsi hem de ülke ekonomisine katkı sağlanmaktadır.

Nesnelerin birbirleri ile etkileşimin açıklamak amaçlı günlük hayattan birkaç senaryo şöyle sıralanabilir:

- Anahtarı evde unutan bir kişinin tam dışarı çıkarken akıllı kapının bunun farkına varması ve kişinin hatırlayıp geri dönme ihtimaline karşı kilitlemeyi kabul edilebilir bir süre ertelemesi.
- Ocak ya da mum gibi yanan herhangi bir nesneyi unutup yatan kişi uykudayken çıkan yangın sonrası duman sensörünün evdeki hareket sensörlerine sinyal göndermesi, kişinin uyanmaması durumunda hareket sensörünün duman sensörünü uyarması ve sonuçta duman sensörünün en yakın itfaiyeye çağrı yapması.
- Kişi geceleyin yatağında rahatça uyuyamadıysa yataktaki sensörün dijital ajandayı kontrol ederek müsait olması durumunda alarmın bir süre ertelemesi için çalar saate mesaj göndermesi.

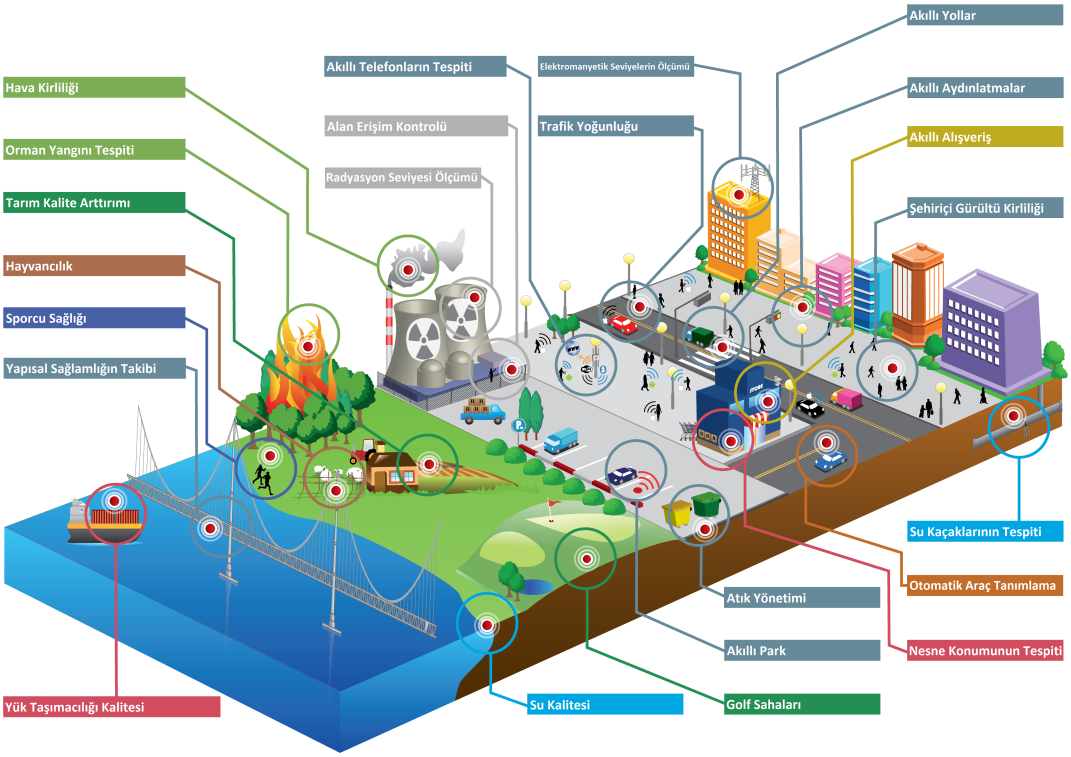
Açıklanan uygulama ve senaryoları gerçeklemek için birçok firma yatırım yapmaktadır. Bunlardan biri olan IBM, akıllı evlerin bulut teknolojisi kullanılarak kontrolü için geliştirdiği sistemi geçtiğimiz yıllarda duyurmuştur.

2.4.2 Sağlık Hizmetleri

Sağlık son zamanlarda nesnelerin interneti uygulamalarının en çok yaygınlaşmaya başladığı alanlardan biridir. Özellikle hasta ve bakıma muhtaç insanların uzaktan takibi ve durumları konusunda ilgili kişi ve kurumların bilgilendirilmesine yönelik çalışmalar yapılmaktadır.

Kullanıcının ateş, kalp atış hızı, kandaki oksijen miktarı, solunum oranı, büyük/küçük tansiyon vb. fiziksel değişimleri ölçerek gerekli alarmları üreten Scanadu Scout taşınabilir elektronik cihazı, geliştirilen önemli uygulamalardan biridir. Klasik endoskopi yöntemi yerine kullanılan, içerisindeki kamera aracılığıyla aldığı görüntüleri iletişim kurduğu cihaza gönderen kablosuz endoskopi kapsülü teknolojisi bir diğer uygulamadır [12]. Ayrıca hastane, sağlık merkezi gibi ortamlarda ilaç vb. envanterin takibinde, yanlış zamanda

veya aşırı dozda ilaç kullanımını önleme amaçlı hastaların tanımlanmasında, hastaların güven ve rahatının sağlanması için sık kullanılan yerlerin tespiti ve personel giriş yetkilerinin belirlenmesinde internet erişimli cihazlar, nesnelerden faydalanılabilir.



ŞEKİL 2.3: Nesnelerin internetinin günlük yaşamdaki uygulamaları.

2.4.3 Ulaşım ve Lojistik

Sensörler ve işlem gücüne sahip cihazlarla donatılan otomobil, tren, otobüs, otoyol, tren rayları, yolcu ve sürücüler için önemli bilgi kaynağıdır. Her bir nesneden ve nesnelerin kendi arasındaki etkileşiminden elde edilen verilerle kişilerin rahat, güvenli ulaşımı için çeşitli uygulamalar geliştirilmektedir.

Trafik yoğunluğunun azaltılması, yön tayini, uygun park yeri seçimi, emisyon ve yakıt tüketiminin düşürülmesi, trafik kontrol cihazları uygulamaları arasında sayılabilir. Devletlerin kullanılan yolları takip ederek yeni yapılacak yollar için plan oluşturması, tehlikeli madde taşıyan araçların takibi, etiketler kullanılarak turistlerin ilgi alanlarına göre bilgi veren haritalar, geleceğin teknolojisi olarak gösterilen otonom araçlar diğer uygulamalarındandır.

RFID tabanlı gerçek zamanlı bilgi işleme, tasarımdan ham madde alımı, üretim ve taşımaya, depolamadan dağıtım, satış ve satış sonrası desteğe kadar tedarik zincirinin her adımında kullanılmaktadır. Walmart, Metro Group gibi büyük şirketlerin stok yönetimi, satış temsilcilerinin ERP uygulamasına bağlanarak ürünün stok durumu ve ürün hakkında daha faydalı bilgi sağlaması uygulamaları arasındadır [13].

2.4.4 Kişisel ve Sosyal

Nesnelerin interneti sosyal ilişkilerin kurulması ve geliştirilmesi amacıyla kişilerin diğer insanlarla olan iletişimde kullanılabilir. Bulunulan yerlerin konum bilgisi ve yapılan bazı aktivitelerin kullanıcının belirlediği kısıtlar doğrultusunda sosyal ağlarda otomatik olarak paylaşılması uygulamalarından biridir. Nesneler ya da olaylar üzerinde yapılan geçmişe yönelik sorgular sonucu kullanıcıların aktivitelerindeki eğilimleri tespit edilebilir. Ardından bu bilgi ışığında kullanıcıya benzer ya da alternatif aktiviteler sunulabilir.

Kişisel olarak bakıldığında nesnelerin interneti kaybedilen bir eşyanın bulunmasında ve hırsızlığın önlenmesinde kullanılabilir. Örneğin, kaybedilen ve RFID etiket taşıyan herhangi bir eşya geliştirilecek web tabanlı RFID arama motoru ile bulunabilir. Kullanıcılar uygulama aracılığıyla eşyanın konumunu, son olarak güncellediği yeri görebilir. Benzer bir uygulama hırsızlığı önleme ve hırsızı yakalama amaçlı olabilir. Ev, ofis gibi önceden tanımlanmış bir yerden herhangi bir nesnenin (dizüstü bilgisayarı, disk, cüzdan vb.) çıkarılması durumunda nesne, SMS, mail gibi önceden tanımlanmış bir yöntemle bunu sahibine ya da güvenlik görevlilerine bildirebilir.

2.4.5 Enerji ve Madencilik

Birçok alanda olduğu gibi enerji alanında da internete bağlı nesnelerin çeşitli noktalarda iş kolaylığı sağlayacağı ve verimi arttıracağı öngörülmektedir. Özellikle günümüzde enerji kaynağı olarak kullanılan fosil yakıtların yerine rüzgâr, güneş gibi yenilenebilir enerji kaynaklarının daha çok kullanılmaya başlanmasıyla nesnelerin interneti uygulamalarına olan ihtiyaç artacaktır. Küçük, orta büyüklükte farklı noktalara dağıtık olarak yerleştirilmiş güneş panelleri ve rüzgâr tribünlerinin birbirleriyle haberleşmesi, yönetimi, arızalı olanların tespiti, güç dengesinin sağlanması, kesintilere hızlı cevap verilmesi uygulamaları

arasındadır [14]. Ayrıca saha içi iletişimde, petrol rafinelerinde, boru hatlarının takibinde nesnelerin internetinden faydalanılabilir.

Akıllı şebeke ve sayaçlar geliştirilebilecek diğer potansiyel uygulamalardandır. Ev içerisindeki elektrik harcayan her bir nokta izlenerek verimli elektrik tüketimi sağlanabilir. Bu bilgiye şehir seviyesinde sahip olunduğunda şebekelerdeki yük dengesi sağlanıp hizmet kalitesi arttırılabilir [15].

Madencilik alanında en önemli konulardan birisi çalışan güvenliğinin sağlanması ve basit hatalardan kaynaklı kayıp sürenin azaltılmasıdır. Zor koşulların yaşandığı, tehlikeli makinalarla çalışılan bu alanda nesnelerin interneti uygulamalarının kullanılabileceği bazı uygulamalar şunlardır [16]

- *Madenci güvenliği ve acil durum*: Çalışanların konumunun, sağlık durumlarının gerçek zamanlı takibi ve bunların ilk yardım ekibi ile entegresi, ortamdaki gaz miktarı, havalandırma sistemlerinin anlık olarak izlenmesi ve olumsuz bir durumda otomatik müdahale edilmesi.
- *Sürücüsüz maden vagonu*: Sürücüsüz vagonlar geliştirilmesi sayesinde sürücü yorgunluğu, hatası ve madendeki kalabalığın azaltılıp güvenliğin arttırılması.
- *Maden uyumlu optimizasyon*: Maden takibi, kalite kontrolü, performans değerlendirilmesi, enerji, yakıt ve su yönetiminin işlenen madenin özelliğine göre yapılabilmesi.

2.5 Güvenlik

Nesnelerin interneti kullanımının yaygınlaşması teknoloji gelişimine bağlı olduğu kadar kullanıcılara sağladığı güvenlik ve mahremiyet yetenekleri ile de ilgilidir. Gizlilik, bütünlük, erişilebilirlik, kimlik doğrulama, yetkilendirme vb. gibi güvenlik özellikleri nesnelerin interneti çözümlerine 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 [17].

Karşılaşılan problemlerin çözümü için öncelikle tehdit kaynaklarının tespiti ve atak vektörlerinin belirlenmesi gerekmektedir. Ayrıca potansiyel hedef sayısının çok fazla olduğu bu alanda saldırı tespiti de önemli bir konu haline gelmiştir.

2.5.1 Tehdit Kaynakları

Nesnelerin interneti uygulamaları birçok saldırgan tarafından hedef alınmaktadır. Potansiyel tehditler ve saldırılar incelendiğinde tehditlerin kaynağı olarak 3 grup ortaya çıkmaktadır [18]:

- *Kötü niyetli kullanıcı*: Üreticinin sırlarını öğrenmek ve kısıtlanmış fonksiyonlara erişim sağlamak amaçlı saldırı gerçekleştiren nesnelerin interneti kullanıcısıdır. Sistemden gizli bilgileri öğrenerek bu sırları farklı firmalara satar ya da elde ettiği bir güvenlik açığını aynı özellikteki diğer cihazlarda kullanır.

- *Kötü niyetli üretici*: Sattığı kullanıcılar ya da onların kullandığı diğer cihazlar hakkında bilgi toplamak amaçlı ürün geliştiren üretici firmalardır. Tasarımda cihazlar üzerinde oluşturulan arka kapı ya da zararlı yazılımlar sayesinde topladığı bilgileri casusluk amaçlı kullanabilir. Ayrıca ortamdaki diğer internete bağlı nesneler ile iletişim kurup zarar vererek onları üreten firmaların güvenilirliğini zedeleyebilir. 2013 yılında Rusya devlet kanalı Rossiya 24, Çin'den ithal edilen ütülere yerleştirilen bir çipin casusluk amaçlı kullanıldığını bildirmiştir. Üzerinde bir adet mikrofon bulunan çip, 200 metre yarıçapındaki kapsama alanında korumasız herhangi bir kablosuz ağa bağlanabilmektedir. Modem, şarj aleti, telefon üzerinde arka kapı barındırdığı tespit edilen diğer cihazlardandır [19].

- *Dış saldırganlar*: Cihaz üzerinde herhangi bir erişimi ve yetkisi olmayan kötü niyetli kişilerdir. Farklı atak vektörleri kullanarak kullanıcı hakkında bilgi toplamak, maddi zarar vermek vb. amaçları vardır. Tehdit kaynakları arasında en yüksek orana sahip gruptur.

2.5.2 Atak Vektörleri

Nesnelerin interneti uygulamalarının kullanım alanları çok farklı olduğundan bu uygulamalara yönelik atak vektörleri çeşitlilik göstermektedir. Bu durum saldırganların işini kolaylaştırırken savunma tarafındakiler için ele alınması gereken birçok parametre anlamına gelmektedir. OWASP adlı topluluk tarafından 2014 yılında yayınlanmış çalışmaya göre en önemli 10 atak vektöründen bazıları şunlardır [20]:

2.5.2.1 Web Arayüzleri

Saldırganlar internete bağlı nesnelerin yönetimini sağlayan web arayüzlerine kullanılan zayıf parolalar, açık metin halinde transfer edilen kimlik bilgileri aracılığıyla erişim sağlayabilir. Ayrıca web uygulamasındaki XSS (Cross Site Scripting), SQL enjeksiyonu veya CSRF (Cross-Site Request Forgery) saldırılarına karşı zafiyet saldırgan tarafından kullanılabilir. Farklı marka modemlerde bulunan ve CVE-2013-6786, CVE-2014-100032 kodlarıyla tanımlanan XSS açıklıkları örnekleri arasındadır [21, 22]. Stanford Üniversitesi tarafından yapılan ve 2009 Black Hat konferansında yayınlanan çalışmada LOM (Lights-out Management), NAS (Network-attached Storage), yönlendirici gibi farklı türdeki internete bağlı nesneler için web tabanlı çeşitli saldırılar denenmiş ve cihazların bu saldırılardan birçoğuna karşı açık durumda olduğu tespit edilmiştir [23].

Tablo 2.1: Cihazlarda tespit edilen farklı türdeki açıklıklar.

Tür	Adet	XSS	CSRF	XCS	RXCS	File Inc.	Auth
LOM	3	■	■	■			■
NAS	5	■	■	■	■	■	■
Resim Çerçevesi	3	■	■	■	■	▪	■
Yönlendirici	1	▪	▪	▪			▪
IP Kamera	3	■				▪	■
IP Telefon	1	■	▪	▪			▪
Anahtarlama Cihazı	4	■	■	■			■
Yazıcı	3	■	■		■		■

Koyu renkli gösterim saldırı kategorisinde etkilenen birden çok cihaz olduğunu ifade ederken açık renkli gösterim tek cihaz olduğunu ifade etmektedir.

2.5.2.2 Yetersiz Kimlik/Erişim Denetimi

Saldırganların cihazlar üzerinde varsayılan olarak gelen ve değiştirilmeyen parolaları kullanması, güvensiz parola kurtarma mekanizmaları, kademeli erişim kontrolünün yetersiz olmasıdır. Bir modem, yönlendirici arayüzünün zayıf ya da varsayılan parolalarla bırakılması sonucu saldırganın cihaz üzerinde yönetici hakkı elde etmesi, gerekli yapılandırmalarla kullanıcılara ait özel bilgilerin (banka hesapları, sosyal medya parolaları) ele geçirilmesi veya cihazın hizmet dışı bırakma saldırısında kullanılması örnekleri arasındadır. Ayrıca 2014 yılı başında duyurulan "ROM-0" açıklığına göre saldırganlar yönlendirici yapılandırma dosyasını yetkilendirilmesi kontrol edilmemiş bir URL üzerinden kolayca indirebilmektedir.

2.5.2.3 Ağ Servisleri

Cihaz üzerinde gereksiz portların açık bırakılması ve zafiyet barındıran uygulamaların bulunmasıdır. Saldırganlar bu servisler aracılığıyla cihazda yetki elde edebilir, bellek taşma ve hizmet dışı bırakma saldırıları gerçekleştirebilir. Zafiyet barındıran servisler ve DoS (Denial of Service) açıklığı bulunduran cihazlar, otomatik tarama araçlarıyla kolayca tespit edilebilir. 2014 yılı başlarında 100.000 buzdolabı ve internete bağlı diğer ev cihazlarının saldırganlar tarafından ele geçirilip çeşitli şirket ve kullanıcılara yaklaşık 750.000 istenmeyen e-posta gönderildiği tespit edilmiştir [24].

2.5.2.4 Şifreleme Eksikliği

Yerel ağ ya da internet üzerinde verinin açık halde taşınmasıdır. Böyle bir durumda ağı dinleyen herhangi bir kişi giden/gelen veriyi kolaylıkla anlayabilir. Ayrıca saldırganlar tarafından SSL/TLS gibi verinin şifrelenmesini sağlayan mekanizmaların yanlış uygulanmasından kaynaklanan açıklıklardan da faydalanılabilir.

2.5.2.5 Cihaz Yazılımları

Cihaz yazılımlarının güncellemesinin yapılamaması, güncelleme dosyalarının şifrelenmemiş bir kanal üzerinden gönderilmesi ve yazılım içerisine hassas kimlik bilgilerinin gömülmesidir. Saldırganlar elde ettiği cihaz yazılımını tersine mühendislik yöntemleriyle inceleyerek kullanıcı adı parola gibi bilgilere ulaşabilir. Aralık 2014 yılında araştırmacılar tarafından ortaya çıkarılan, farklı marka ve modelden yaklaşık 12 milyon modem/yönlendiriciyi etkileyen "Misfortune Cookie Vulnerability (CVE-2014-9222)"'de cihazlarda kullanılan bir uygulamanın açıklık barındıran eski sürümünden faydalanılmıştır [25].

2.5.2.6 Fiziksel Güvenlik Eksikliği

Cihazın tüm dış etkenlere açık halde olması, veri depolama alanlarına kolaylıkla erişilebilmesi, depolanan verilerin şifrelenmemiş halde tutulması, bakım ve yapılandırma için kullanılan USB portları için gerekli güvenlik önlemlerinin alınmamasıdır.

2.5.3 Önlemler

Nesnelerin interneti uygulamaları için belirtilen çeşitli atak vektörlerine karşı geliştirilmiş bazı önlemler şöyle sıralanabilir:

- Varsayılan parolaların kurulum sırasında değiştirilmesi ve karmaşık parola kullanılması
- Yetkilendirme ve parola kurtarma mekanizmalarının güçlendirilmesi, kademeli erişim kontrolünün uygulanması
- Cihaz üzerinde açıklık barındıran uygulamaların güncel sürümlerinin yüklenmesi, gereksiz portların kapatılması
- Verinin taşınması sırasında şifreleme mekanizmaları kullanılması, şifrelemede kullanılan anahtarların pratikte kırılamayacağı öngörülen uzunlukta olması
- Cihazların yeterli bellek alanına sahip olamamasından dolayı kullandığı bulut sistemleri arayüzlerinin kimlik doğrulama, yetkilendirme, parola kurtarma vb. güvenlik özelliklerini sağlaması

- Akıllı evlerin sahip olduğu akıllı ampul, su ısıtıcısı vb. birçok cihazın yönetimini sağlayan mobil cihaz uygulamalarının gerekli güvenlik özelliklerini sağlaması
- Cihaz kullanıcısına karmaşık parola politikalarını uygulayabilmek, görevler ayrılığı ilkesine uygun şekilde yetkilendirme yapabilmek, verinin taşınmasında kullanılacak şifreleme özelliklerini değiştirebilmek gibi yeterli yapılandırma haklarının tanımlanması
- Cihaz yazılımlarında hassas bilgilerin olmaması ya da basit bir şekilde okunamaması, imzalanmış güncelleme dosyalarının kullanılması, güncelleme dosyalarının şifreli kanaldan iletilmesi
- Cihazın çeşitli dış etkenlere karşı korumalı bir ortamda olması, cihaz üzerindeki depolama alanlarının kolaylıkla sökülememesi, gereksiz USB portlarının istenildiği zaman engellenebilmesi

2.5.4 Saldırı Tespiti

Günümüzde bilgi sistemlerine gelen saldırıların tespitinde ağ servisi, işletim sistemi veya tüm ağın benzetimini yapabilen tuzak sistemler ve saldırı tespit sistemleri kullanılmaktadır. Snort, Suricata ve Bro açık kaynak kodlu yazılımları yaygın olarak kullanılan saldırı tespit sistemleridir [26]. Tuzak sistemler ise saldırı tespiti yanında saldırganın kullandığı zararlı yazılımları yakalayarak analiz edilmesine ve benzer saldırıların tanınmasına olanak sağlar. SSH, FTP, SMB, SMTP vb. yaygın olarak kullanılan birçok protokol için geliştirilmiş tuzak sistemler vardır.

İnternete bağlı nesneler kısıtlı bant genişliği, hafıza, hesaplama yeteneği ve enerjiye sahip olduğundan üzerlerinde yüksek işlem gücü gerektiren klasik saldırı tespit sistemlerini kullanmak imkânsızdır. Bununla birlikte nesnelerin interneti uygulamalarında saldırı tespiti için çeşitli akademik çalışmalar yapılmaktadır.

Raza S., Wallgren L. ve Voigt T'nin 6LoWPAN ağı için geliştirdikleri ve adını SVELTE olarak belirledikleri saldırı tespit sistemi temel olarak sahte bilgi, seçmeli iletim ya da sinkhole gibi yönlendirme ataklarının tespitini amaçlamaktadır [27]. 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 [28]. 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.

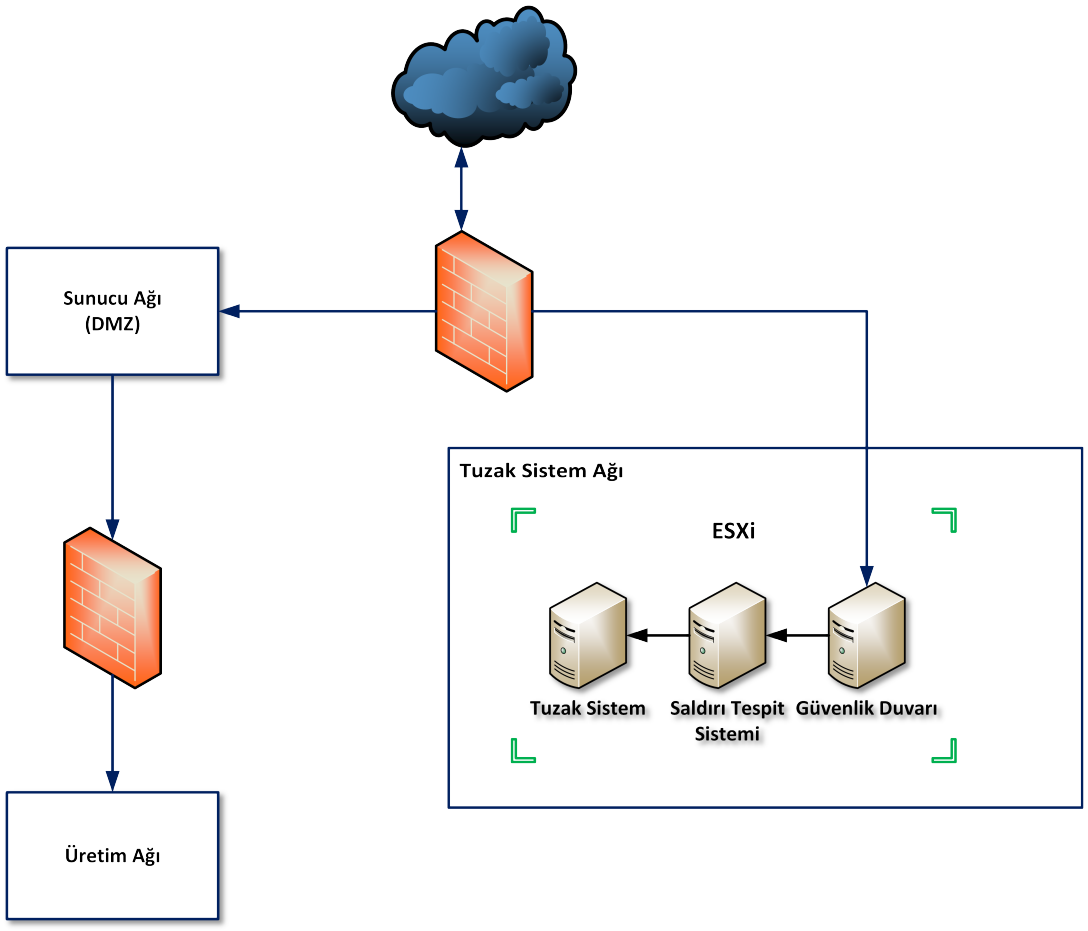
Bölüm 3

Tuzak Sistemler

3.1 Giriş

Tuzak sistem (honeypot, bal küpü) bilgi sistemlerine gerçekleştirilen atakları tespit etmek amaçlı geliştirilen mimarilerden biridir. Hedef sistemmiş gibi davranarak saldırganların dikkatini çekmek ve olası saldırı durumunda bütün aktiviteleri kaydetmek üzere tasarlanmıştır. Bir ağa yerleştirilen tuzak sistemin değeri üzerine çektiği saldırılar, araştırılması ve ele geçirilmesi ile ölçülür [29].

Tuzak sistemlerin temel özelleri arasında ağ servislerinin, işletim sistemlerinin ya da tüm ağın benzetimini yaparak atakları üzerine çekmek, zararlı yazılım örneklerini toplamak, atak yönteminin özellikleri ve tekniği hakkında bilgi sağlamak, gerçek sistemlere gelebilecek potansiyel saldırı riskini düşürmek sayılabilir [30]. Bu işletim sistemi ve servisler kendine özel açıklıklar barındırır. 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.



ŞEKİL 3.1: Tuzak sistemlerin izole edilmiş ağ ortamında çalışması.

Mokube I. ve Adams M.'e göre tuzak sistemlerin avantajları şöyle sıralanabilir [31]:

- Tuzak sistemler saldırı tespit sistemleriyle karşılaştırıldığında ağdaki tüm trafik yerine sadece kendilerine gelen trafik ile ilgilendiklerinden büyük boyutlu log ya da alarm dosyaları yerine daha küçük boyutlu veri setleri üretirler. Tuttukları log dosyalarının boyutları küçük olsa da içerik olarak değerli bilgilerdir.
- Normal kullanıcı tarafından bilinmediğinden gelen trafik çok büyük oranda saldırganlara aittir.
- Sadece belli bir servisin, sistemin benzetimini yapmak ve olumsuz aktiviteleri kaydetmek gibi görevleri olduğundan düşük sistem kaynakları ile kolayca çalışır. Bulut ortamındaki sanal makine, ya da Raspberry Pi cihazı üzerinde çalışabilmektedir [32].
- Basit ve esnek yapıdaki sistemlerdir. Geliştirilmesi için karmaşık algoritmalar gerekmemekle birlikte bakımı ve güncellenmesi de kolaydır.

- Zararlı trafiği kaydetmekle birlikte saldırganların kullandığı yeni saldırı teknik ve araçlarının tespitinde de önemli rol oynar. Sonrasında saldırı tespit sistemi imzası geliştirmek gibi yöntemlerle gelebilecek benzer saldırılar tüm sistemlere tanıtılabilir.

3.2 Tuzak Sistem Türleri

Tuzak sistemler kullanım amacı, üstlendikleri rol, geliştirildikleri donanım türü ve saldırgan ile olan etkileşimlerine göre çeşitli gruplara ayrılırlar.

- Kullanım amacına göre tuzak sistemler:
  - *Araştırma amaçlı*: Amaç saldırgan hakkında maksimum bilgi elde etmektir. Bu yüzden sisteme sızıp istediklerini gerçekleştirebilmesi için saldırgana tam erişim yetkisi verilir.
  - *Ürün ortamında kullanma amaçlı*: Herhangi bir kurumun ya da ağın zararlı aktivitelerden korunmasını sağlamak amaçlı kullanılan tuzak sistemlere denmektedir. Kurumlar güvenlik amaçlı tuzak sistem kullansa bile kullanılmayan servislerin kapatılması, yama yönetimi, güvenlik duvarı, saldırı tespit sistemleri, antivirüs ve güvenli kimlik doğrulama yöntemleri gibi güvenlik politikalarını kullanmaya devam etmelidir.
- Üstlendikleri role göre tuzak sistemler:
  - *Sunucu taraflı*: Pasif tuzak sistemlerdir ve ele geçirilmediği sürece trafiği başlatan taraf olmazlar.
  - *İstemci taraflı*: İstemci taraflı saldırılar için aktif tuzak sistemlerdir. İstemcinin açıklık barındıran uygulamalarla zararlı yazılım içeren web sitelerine, sunuculara erişme senaryosunu gerçekleştirir.
- Geliştirildikleri donanım türüne göre tuzak sistemler:
  - *Fiziksel*: Gerçek işletim sistemi, gerçek servisler çalışan ve ağ üzerinden tek bir IP ile erişilebilen tekil makinalardır.
  - *Sanal*: Tek bir fiziksel makine üzerinde birçok sanal tuzak sistemin çalışmasıdır. Fiziksel tuzak sistemlere göre maliyeti düşük, bakımı ve yönetimi kolaydır.

- Saldırgan ile olan etkileşimlerine göre tuzak sistemler [33]:
  - *Düşük etkileşimli*
  - *Orta etkileşimli*
  - *Yüksek etkileşimli*

3.2.1 Düşük Etkileşimli Tuzak Sistemler

Saldırgan ile olan etkileşim kapasitesi düşük sistemlerdir. Herhangi bir servisin ya da komple bir işletim sisteminin benzetimini yaparlar. Ancak servisler kullanılarak sistem ele geçirilemez. Örneğin 21. portta çalışan FTP servisinin benzetimini yapan tuzak sistem saldırganın sadece oturum açmasını veya FTP ile ilgili belli başlı birkaç komutu çalıştırmasına izin verir.

Düşük etkileşimli tuzak sistemlerin temel amacı saldırı ile ilgili kaynak IP, kaynak port, hedef IP, hedef port gibi bilgilerin tespiti ve saldırgan davranışının ölçülmesidir [34]. Geliştirilmesi, bakımı basittir. Ayrıca bulunduğu ağ için ayrı bir risk faktörü oluşturmaz.

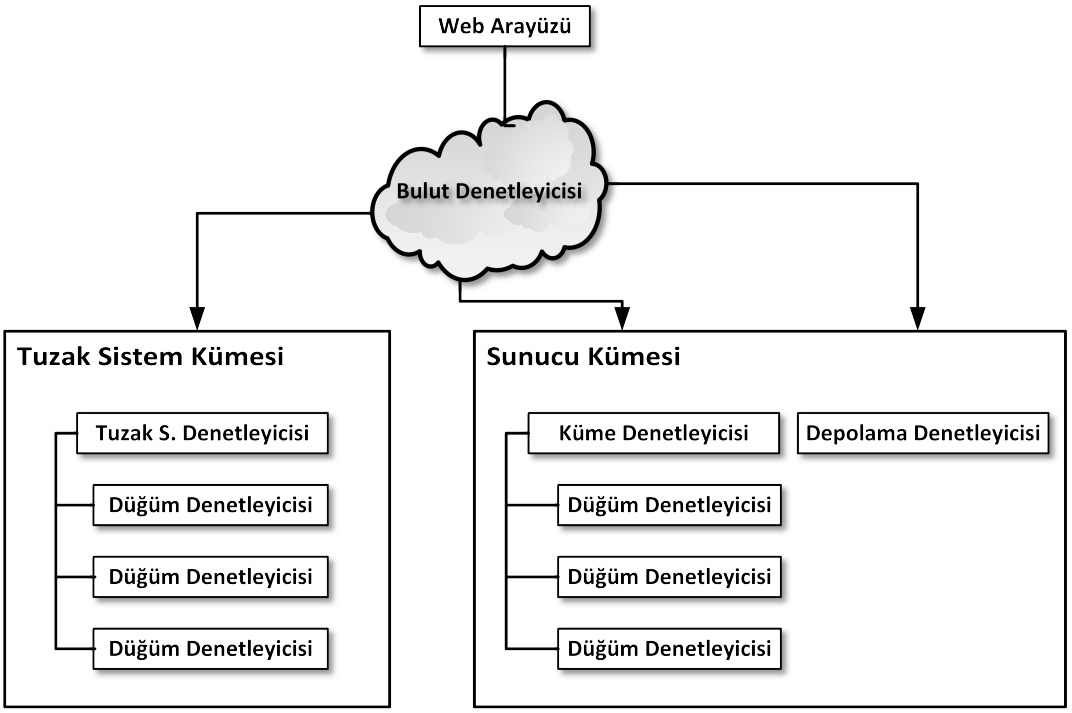
3.2.2 Orta Etkileşimli Tuzak Sistemler

Orta etkileşimli tuzak sistemler düşük ve yüksek etkileşimli tuzak sistemlerin avantajlarını bir araya getirmeyi hedefler. 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. Benzetimini yaptığı servisler çeşitli açıklıklar barındırır ve saldırganın kullandığı zararlı yazılım ile etkileşime geçebilir.

FreeBSD Jails gibi gerçek bir işletim sistemi üzerindeki izole edilmiş bir alan da orta etkileşimli bir tuzak sistem gibi davranabilir. Bu yöntemin dezavantajı izole edilmiş alanı sağlayan sistem üzerinde herhangi bir açıklık olması durumunda saldırganın gerçek işletim sistemini ele geçirme olasılığıdır.

3.2.3 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. Saldırı ile ilgili tüm detaylar kayıt altında tutulduğundan atak yöntemi, kullanılan araçlar hakkında derinlemesine analiz yapılabilir. Ancak tasarlanması, yönetimi, bakımı ve zararlı yazılımlardan temizlenerek tekrar kullanılması zordur. Sanallaştırma uygulamalarından VirtualBox, bulut üzerinde sanallaştırma ortamı sunan OpenStack vb. uygulamalarla bu tip tuzak sistemlerin yönetimi daha kolay olmaktadır.



ŞEKİL 3.2: Tuzak sistemlerin bulut ortamında çalışması.

Yüksek etkileşimli tuzak sistem örnekleri arasında Honeynet organizasyonu tarafından geliştirilen Sebek ve Qemu tabanlı olan Argos sayılabilir. Sebek tuzak sistemlerden veri toplama amaçlı sisteme yüklenen ve gizli olarak çalışan bir çekirdek modülüdür. Çekirdeğe yüklenmesiyle birlikte birçok önemli sistem çağrısının yerine geçer. Böylece sistem üzerinde bu çağrıları tetikleyecek herhangi bir durum olduğunda tüm aktiviteleri yakalama imkânına sahip olur. Bu veriler sonrasında saldırının detaylı analizi için kullanılabilir.

Argos saldırgana gerçek bir işletim sistemi sunar ve saldırgan tuzak sistem üzerinde herhangi bir zararlı aktivite yapmaya çalıştığında sistem kendini kapatarak o anlık RAM ve diskin dökümünü kaydeder. Bu işlem analiz adımı için gerekli verileri sağlayacaktır.

Ayrıca açıklık barındıran, yani yaması yapılmamış Windows XP, Windows Server 2008, Ubuntu Server 12.04 vb. gibi herhangi bir işletim sistemi de yüksek etkileşimli tuzak sistem olarak kullanılabilmektedir. Sadece bu sistemleri uygun şekilde ağa bağlamak ve sistemlerden analiz için gerekli verileri toplamak gereklidir.

Etkileşim saldırganın tuzak sistemle gerçekleştirdiği aktivitelerle ölçülür. Hangi tuzak sistemin ne zaman kullanılacağı çeşitli faktörlere bağlıdır. Etmenler ve tuzak sistem türlerinin bunlarla ilişkisi Tablo 3.1'de verilmiştir [35]:

TABLO 3.1: Saldırgan ile olan etkileşimlerine göre tuzak sistemlerin karşılaştırılması.

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	Zor	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

3.3 Tuzak Sistem Örnekleri

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 şunlardır:

- *Dionaea*: Düşük etkileşimli tuzak sistemdir. Açıklığa sahip Windows 2000 işletim sistemi ile birlikte SMB, HTTP, FTP, TFTP, MSSQL, MySQL, SIP protokollerinin benzetimini yapar. Temel amacı saldırganların açıklık sayesinde sistemi ele geçirmeye çalışırken kullandığı zararlı yazılımım elde edilmesidir.

- *Conpot*: Düşük etkileşimli, sunucu taraflı, endüstriyel kontrol sistemlerin (SCADA) benzetimini yapan bir tuzak sistemdir. Modbus TCP, SNMP ve HTTP protokollerinin içeren Siemens SIMATIC S7-200 PLC'sinin benzetimini yapar.

- *Kippo*: Python programlama dili ile geliştirilmiş, orta etkileşimli, SSH servisinin benzetimini yapan bir tuzak sistemdir. SSH servisine yapılabilecek kaba kuvvet saldırıları ve saldırganın kabuk ile gerçekleştirdiği tüm etkileşimi kayıt altına alabilecek şekilde tasarlanmıştır.

- *Glastopf*: Düşük etkileşimli, dinamik web uygulama tuzak sistemidir. Hedef saldırganın adımlarına karşı mümkün olduğunca doğru cevabı verebilmektir. Dinamik atak yüzeyi sunarak birkaç farklı adım gerektiren atakları destekler.

- *Thug*: Düşük etkileşimli ve istemci taraflıdır. Web tarayıcısı davranışının benzetimini yaparak istemci taraflı saldırıları tespit etmeyi hedefler. ActiveX kontrolleri, temel tarayıcı fonksiyonellikleri ve tarayıcı eklentileri olmak üzere 3 adet açıklık modülü vardır.

- *Ghost*: USB depolama cihazları aracılığıyla yayılmayı hedef almış Stuxnet, Conficker vb. zararlı yazılımların yakalanması için geliştirilen bir tuzak sistemdir. Amaç işletim sistemi tarafından çıkarılabilir aygıt olarak gözüken cihazın benzetimini yapıp benzetimi yapılan cihazı izleyerek zararlı yazılımları tespit etmektir.

Detayları açıklanan Dionaea, Kippo, Conpot, Glastopf, Thug ve Ghost tuzak sistemlerinin dışında ilk tuzak sistemlerden Deception Toolkit, farklı işletim sistemlerine sahip sanal makinelerin ağ seviyesinde benzetimini yapan Honeyd, tuzak sistem, izleme araçları ve alarm sisteminin birleşimiyle Linux/Windows işletim sistemlerini korumayı hedefleyen Artillery, herhangi bir PHP web uygulamasını yüksek etkileşimli bir tuzak sistem halinde çalıştırabilen Hihat, Windows işletim sistemi için özelleşmiş orta etkileşimli bir tuzak sistem olan Honeybot, istemci uygulamalarının ve açıklıklarının benzetimini yaparak istemci taraflı saldırıların tespitini hedefleyen PhoneyC, Wordpress uygulaması için özelleştirilmiş Wordpot, VoIP ağları için tasarlanmış ve SIP protokolünün benzetimini yapan Artemisa, otomatik olarak yayılan zararlı yazılımların yakalanmasını sağlayan Amun diğer tuzak sistemler arasında sayılabilir.

Bölüm 4

TR-069

4.1 Giriş

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 [36]. Ayrıca doküman protokolün uygulanması için gereklilikler ve farklı ağ senaryoları için protokolün nasıl kullanılacağı gibi konuları içermektedir.

4.2 Terminoloji

Protokolün anlaşılmasını sağlayacak temel bileşenler ve çeşitli kısaltmaları içeren terminoloji şu şekildedir:

- *Müşteri Tarafı Cihazı (Customer Premises Equipment - CPE)*: Son kullanıcı tarafındaki modem, yönlendirici, VoIP telefon gibi TR-069 uyumlu herhangi bir cihazdır. Bir CPE en az bir tane CWMP sonlandırma özelliğine sahiptir.
- *Otomatik Yapılandırma Sunucusu (Auto Configuration Server - ACS)*: ACS genellikle internet servis sağlayıcı ya da kullanılan cihazı tedarik eden kurum tarafında

geniş bant ağında bulunan, CPE'nin otomatik yapılandırmasından sorumlu sunucudur.

- *Veri Modeli (Data Model)*: Belirli bir CPE türünün yönetimi için tanımlanmış nesneler setidir. Genellikle Broadband Forum tarafından farklı teknik raporlarla belirlenir.
- *İnternet Ağ Geçidi Cihazı (Internet Gateway Device - IGD)*: Bir CPE cihaz türüdür. Tipik olarak geniş alan ağı ile yerel alan ağı arasında ağ geçidi görevini gören yönlendiricidir.
- *Basit Nesne Erişim Protokolü (Simple Object Access Protocol - SOAP)*: XML web servislerinin kullandığı ve ağ üzerindeki bileşenler arasında mesaj alışverişini sağlayan protokoldür.
- *Uzak Yordam Çağrısı (Remote Procedure Call - RPC)*: İstemci ve sunucu olarak çalışan iki ucun birbirleri arasında yordam çağrıları yapmasını sağlayan SOAP kullanımıdır.

4.3 Kullanım Amaçları

TR-069 (CWMP) protokolü birçok fonksiyonelliği desteklemekle birlikte temel kullanım amaçları şöyle sıralanabilir [37]:

- Otomatik Yapılandırma ve Dinamik Hizmet Sağlama
- Yazılım/Bellenim İmaj Yönetimi
- Yazılım Modül Yönetimi
- Performans ve Durum İzleme
- Hata Tanılama

4.3.1 Otomatik Yapılandırma ve Dinamik Hizmet Sağlama

CWMP ACS'nin bir CPE'yi ya da CPE topluluğunu birçok ölçüte göre yapılandırmasını sağlar. Yapılandırma işlemi CPE'nin geniş alan ağına katıldığı ilk anda ve istenilen herhangi bir zamanda gerçekleştirilebilir. Protokol ayrıca CPE'ye özel geliştirilmiş hizmet

ve uygulamaların yönetimine olanak verir. Bununla beraber, teknoloji gelişimi devam ettiğinden bazı yetenek ve hizmetler CWMP'nin son sürümünde bulunmamaktadır. Ancak protokol bu eksik özelliklerin uygulanabilmesi için geliştirilecek çeşitli eklentileri desteklemektedir.

4.3.2 Yazılım/Bellenim İmaj Yönetimi

Protokol kullanılarak geliştirilen yönetim uygulamalarıyla CPE yazılım/bellenim imaj dosyaları indirilebilir. CPE üzerindeki yazılımın versiyonunun tanımlanması, dosya indirme işleminin başlatılması ve ACS'ye bu işlemle ilgili başarılı/başarısız bilgisinin gönderilmesi protokolün getirdiği diğer özellikler arasındadır. ISP'ler müşterilerindeki cihaz yazılımlarını güncelleyerek çeşitli güvenlik açıklıklarının kapanmasını ve müşterilerinin mümkün olan en kaliteli hizmeti almalarını sağlayabilir.

4.3.3 Yazılım Modül Yönetimi

Protokol ACS'nin CPE üzerindeki yazılım modüllerinin kurulması, güncellenmesi, kaldırılması ve her bir işleme ait başarılı olup olmadığıyla ilgili sonucun ACS'ye iletilmesini sağlar. Ayrıca uygulamaların başlatılıp sonlandırılması ve çalışma ortamlarının aktif/pasif edilmesi protokolün diğer kullanım amaçları arasında sayılabilir.

4.3.4 Performans ve Durum İzleme

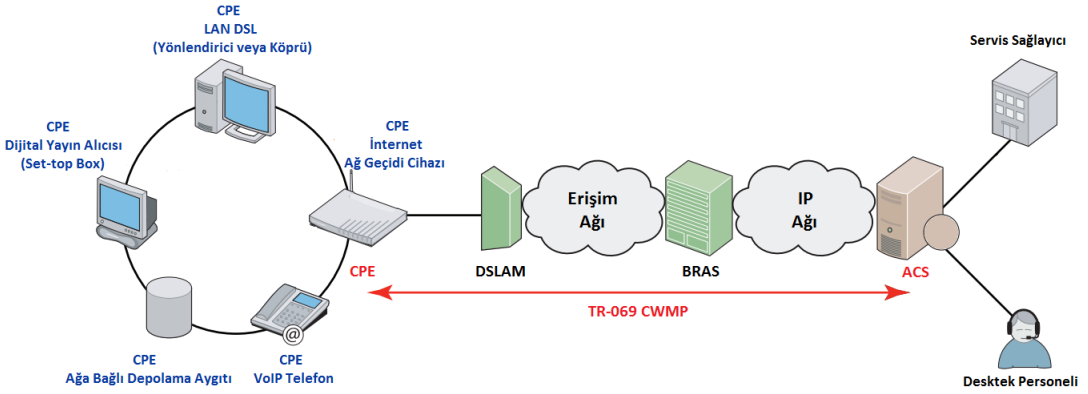
ACS, CPE'nin durumu ile ilgili bilgileri ve performans istatistiklerini periyodik olarak izleyebilmektedir. Elde edilen bu bilgiler ISP tarafında çeşitli araçlarla analiz edilerek hizmet kalitesi arttırılabilir. Bununla birlikte tanımlanan çeşitli mekanizmalarla CPE, durumunda herhangi bir değişiklik olması halinde bunu ACS'ye bildirebilir. Özellikle güvenlik açısından önemli bir yetkinliktir.

4.3.5 Hata Tanılama

CWMP, ACS'nin CPE'den elde ettiği bilgiler ve önceden tanımlı bazı tanılama testlerinin çalıştırılmasıyla hata tespiti, bağlantı ya da çeşitli servis problemlerinin çözümüne olanak sağlar.

4.4 Mimari

Metin tabanlı çalışan CWMP'de mesajlar ACS ve CPE arasında transfer edilir. Bir ya da daha fazla ACS farklı servis sağlayıcılarla ilişkilendirilmiş bir CPE topluluğunu yönetebilmektedir. Yapı olarak klasik istemci sunucu mimarisine benzetilebilir. Normalde CPE HTTP istemci ACS ise HTTP sunucu olarak görev almaktadır. Ancak iletişim sırasında ihtiyaçlara göre ACS istemci olurken CPE sunucu durumuna geçebilmektedir.



ŞEKİL 4.1: CWMP mimarisi.

Protokol standart TCP/IP üzerine inşa edilmiştir ve çift yönlü olarak SOAP/HTTP üzerinde çalışmaktadır. CWMP'de SOAP kullanımının sebebi platform bağımsız olmasıdır. SOAP tek yönlü ve istemci sunucu rollerinin kesin olarak belirlendiği bir protokol olduğundan CWMP bileşenleri arasındaki rol değişimi protokol geliştiricilerini kendi SOAP yapılarını oluşturmaya yöneltmiştir. Bu durum birlikte çalıştıkları bazı uygulamalarda SOAP mesajlarının yanlış yorumlanmasından kaynaklı çeşitli problemlerin ortaya çıkmasına neden olmuştur [38].

Mesajlar RPC yöntemiyle taraflara iletilmektedir. RPC metotları XML tabanlı sözdizimi kullanan SOAP tarafından iletime hazır hale getirilmektedir.

TABLO 4.1: CWMP protokol yığını.

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

İletişim güvenliğini sağlamak amaçlı SSL 3.0 ve TLS 1.0 ile HTTPS, yapılandırma dosyasının indirilmesi, cihaz yazılımının güncellenmesi vb. işlemlerinde de FTP, SFTP ve TFTP protokolleri kullanılmaktadır. Tablo 4.1'in en üst kısmında bulunan CPE/ACS yönetim uygulaması protokole ait değildir. Protokolün işletimini sağlayan bu uygulamalar cihaz sağlayıcıları ve servis sağlayıcılar tarafından geliştirilmekte ya da dış kaynaklardan tedarik edilmektedir.

4.5 RPC Metotları

ACS ile CPE arasındaki çift yönlü iletişimde cihazlar üzerinde tanımlanmış RPC metotları kullanılmaktadır. CPE ve ACS'nin kendine özgü metotları olmakla birlikte her ikisi için de tanımlı olan metotlar vardır [39]. *"GetRPCMethods"* bu kapsama girer. ACS veya CPE tarafından çağrılabilir ve sorguyu yapan taraf karşı tarafın desteklediği RPC metotlarını öğrenmek için kullanır. Dönen cevap standart metotları içerdiği gibi üreticiye özel metotları da içerebilir.

4.5.1 CPE Metotları

CPE üzerinde tanımlanmış metotlardır. ACS tarafından çağrılır. En önemlileri ve sık kullanılanları şunlardır:

- *SetParameterValues*: Bir ya da daha fazla CPE parametresinin değerini değiştirir.
- *GetParameterValues*: İstenilen bir ya da daha fazla CPE parametresinin güncel değerini döner.
- *GetParameterNames*: CPE üzerinde erişilebilir parametrelerin listesini almak için kullanılır.
- *SetParameterAttributes*: Bir ya da daha fazla CPE parametresiyle ilişkilendirilmiş özelliğin değiştirilmesini sağlar.
- *GetParameterAttributes*: Bir ya da daha fazla CPE parametresiyle ilişkilendirilmiş istenilen herhangi bir özelliğin değerini döner.

- *AddObject*: CPE üzerindeki birden çok örnekli nesnelerden yeni bir örnek oluşturmak için kullanılır.
- *DeleteObject*: CPE'de tanımlı herhangi bir nesnenin belirli bir örneğini siler.
- *Download*: CPE'ye belirtilen bir URL'den aygıt yazılımı, yapılandırma dosyası vb. bir dosyanın indirilmesi için kullanılır.
- *Reboot*: CPE cihazının kapanıp açılmasını sağlar.

Bazı CPE metotlarının kullanım örnekleri Tablo 4.2'de görülmektedir [40]:

TABLO 4.2: CPE metotlarının kullanım örnekleri.

Kullanım Senaryosu	**CPE RPC Metodu**
Set ("Device.NAT.PortMapping.2.LeaseDuration", 3600)	SetParameterValues
Get ("Device.DeviceInfo.")	GetParameterValues
GetNames("InternetGatewayDevice.")	GetParameterNames
EnableNotification ("Device.Hosts.HostNumberOfEntries")	SetParameterAttributes
Create ("Device.NAT.PortMapping.")	AddObject
Delete ("Device.NAT.PortMapping.2.")	DeleteObject
Download("http://ftp.example.com/firmware")	Download

4.5.2 ACS Metotları

ACS üzerinde tanımlanmış metotlardır. CPE tarafından çağrılır. En önemlileri ve sık kullanılanları şunlardır:

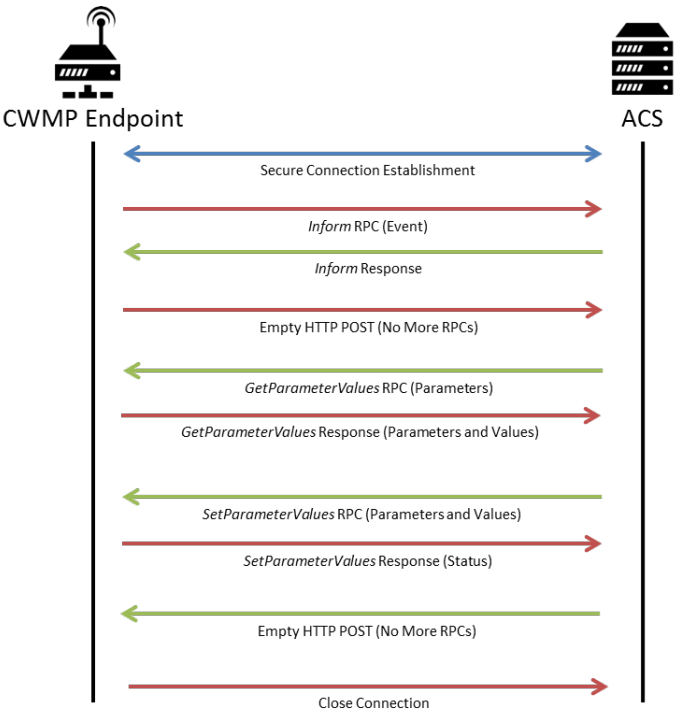
- *Inform*: Her oturum öncesi CPE'den ACS'ye gönderilen ve oturum kurma nedenini içeren komuttur.
- *TransferComplete*: ACS'nin daha önce çağırdığı *"Download"*, *"ScheduleDownload"* ya da *"Upload"* komutlarının başarılı olup olmadığıyla ilgili ACS'nin bilgilendirilmesi amaçlı kullanılır.
- *AutonomousTransferComplete*: ACS tarafından özellikle istenilmemiş bir dosya transfer işleminin sonucu ile ilgili ACS'nin bilgilendirilmesini sağlar.

4.6 Oturum Yönetimi

CWMP'de oturum her zaman CPE tarafından başlatılır. Oturumun başlatılmasında iki farklı senaryo vardır.

İlk olarak CPE servis sağlayıcı tarafından belirlenmiş ACS URL/Port adresine Tablo 4.3'de belirtilen oturum kurma nedenini de içeren *"Inform"* isteğini HTTP POST ile gönderir. Bu istekte ayrıca cihazla ilgili üretici, model, seri numarası vb. bilgiler yer alır. Mesajı alan ACS CPE'ye *"Inform"* cevabı gönderir. CPE buradan *"Inform RPC"*'nin başarılı olduğunu anlar. CPE eğer ACS üzerinde herhangi RPC çalıştırmayacaksa boş bir HTTP POST mesajı gönderir ve bekleme durumuna geçer. Bu mesaj oturum açık kaldığı sürece herhangi bir anda tekrarlanabilir [41].

ACS CPE üzerinde değişiklik yapmak, çeşitli bilgileri öğrenmek isteyebilir. Örneğin CPE'de tanımlı bazı parametreleri değiştirmek için parametre değerlerini içeren *"SetParameterValues"* isteği gönderir. CPE aldığı bilgilere göre değişikliği uyguladıktan sonra ACS'ye işlemin sonucunu *"SetParameterValues"* cevabı ile döner. ACS CPE üzerinde çalıştıracağı herhangi bir RPC kalmadığında daha önce CPE'nin gönderdiği gibi boş bir HTTP POST isteği gönderir. Her iki tarafın boş HTTP mesajlarını göndermesi neticesinde oturum sonlanmış olur.



ŞEKİL 4.2: CWMP oturumunun kurulması.

TABLO 4.3: Inform RPC olay kodu ve tanımları.

Olay Kodu	**Tanımı**
0 BOOTSTRAP	CPE'nin ACS'ye ilk bağlantı isteğinde gönderilir.
1 BOOT	CPE'nin kapanıp açılmasından sonraki ilk bağlantı isteğinde gönderilir.
2 PERIODIC	CPE'nin belirli aralıklarla ACS'ye bağlantı kurması için belirlenmiş zamanın dolmasından sonraki istekte gönderilir.
3 SCHEDULED	Zamanlanmış isteklerde kullanılır.
4 VALUE CHANGE	ACS tarafından belirlenmiş herhangi bir parametrenin değişmesi durumunda ACS'yi bilgilendirmek amaçlı kurulan bağlantıda gönderilir.
6 CONNECTION REQUEST	ACS'nin CPE'ye kendisine bağlanması için istek göndermesi sonrası CPE'nin bağlantısında kullanılır.
7 TRANSFER COMPLETE	ACS'nin bilgilendirilmesi gereken herhangi bir dosya indirme, yükleme işlemi sonrası kurulan bağlantıda gönderilir.
8 DIAGNOSTICS COMPLETE	TR-069 veri modelinde tanımlanan bir ya da daha fazla test işleminin tamamlandığını ACS'ye bildirmek amaçlı kurulan bağlantıda gönderilir.
M <metot ismi>	Inform RPC'nin herhangi bir diğer RPC metodu tarafından tetiklendiğini bildirmek için kullanılır (M=Master). Tetikleyebilecek RPC metotları: - Reboot - Download - ScheduleInform - Upload - <üretici firmaya özel>

Oturumun kurulması için diğer bir senaryo ACS'nin CPE'ye kendisine bağlantı kurması için istek göndermesidir. İsteğin yapılabilmesi için daha önce CPE'nin en az bir kere ACS'ye bağlantı kurmuş ve kendine bağlanılabilmesi için gerekli URL, port ve kimlik bilgilerini göndermiş olması gerekmektedir. İsteği alan CPE, bilgileri kontrol eder ve doğrulaması halinde "HTTP 200 OK" veya "HTTP 204 No Content" cevabını gönderir. Bağlantı isteği geldikten sonra 30 saniye içerisinde CPE, bağlantıyı ACS'nin istediğini belirten olay kodu ile birlikte *"Inform"* isteği gönderir. Ardından normal oturum kurma

adımları devam eder [42]. ACS'nin bağlantı isteği için CPE üzerinde IANA tarafından varsayılan olarak 7547 portu belirlenmiştir. Bağlantı isteği mekanizmasının çalışabilmesi için CPE'ye ACS tarafından HTTP protokolüyle erişilebilir olması gerekmektedir. CPE'nin ağ yapısı olarak doğrudan erişilemeyecek bir noktada olması durumunda bağlantının STUN (Session Traversal Utilities for NAT) ve XMPP (Extensible Messaging and Presence Protocol) tabanlı gerçekleştirilmesi önerilmektedir [43].

4.7 Güvenlik Özellikleri

CWMP iletişimi kimlik doğrulama, gizlilik, bütünlük gibi güvenlik özelliklerine sahiptir. Ayrıca protokol tasarlanırken güvenlik dikkate alınan parametreler arasındadır. Oturumu sadece CPE'nin başlatabilmesi ve CPE'nin herhangi bir yerden kendi başlatmadığı bir mesajlaşmaya ait hiçbir isteği kabul etmemesi bunun örneklerindendir [44].

Protokol HTTP Basic, HTTP Digest ya da sertifika tabanlı olmak üzere çift yönlü kimlik doğrulamayı gerektirir. ACS normal oturum kurma isteğinde CPE'yi doğrularken, CPE ACS'nin kendisine bağlantı kurulması için gönderdiği istekte ACS'yi doğrular.

İletişimde gizlilik, veri bütünlüğünün sağlanması ve sertifika tabanlı kimlik doğrulamasının uygulanabilmesi için SSL/TLS kullanılmaktadır. Tüm bilgiler HTTPS üzerinden gönderilmektedir. SSL/TLS'in olmadığı durumda HTTP Digest kimlik doğrulama yöntemi kullanmak koşuluyla HTTP kullanılabilir.

Bölüm 5

HoneyThing

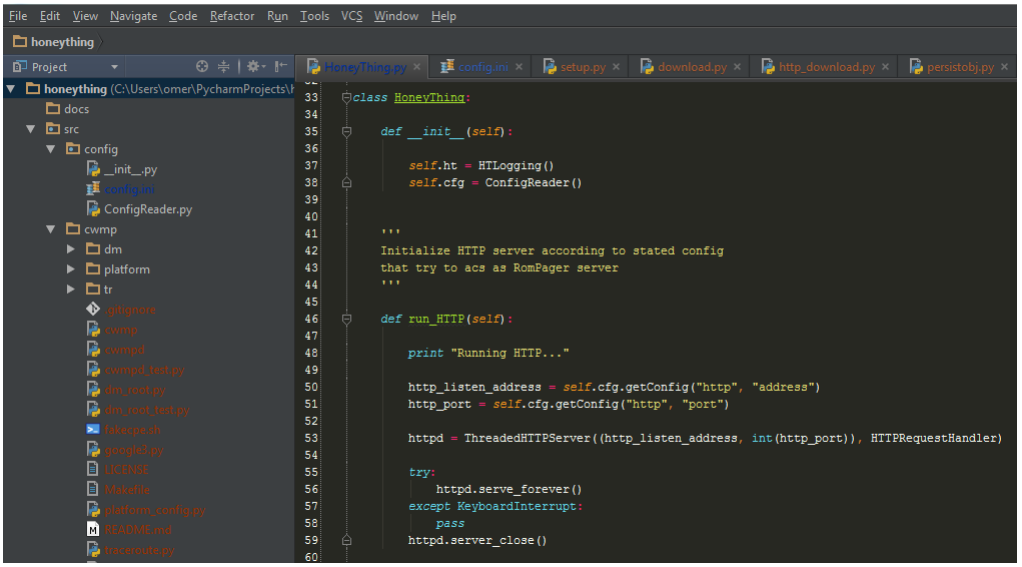
5.1 Giriş

HoneyThing (**Honey**pot for Internet of **Thing**s), internete bağlı cihazlardan modem ve yönlendiricilere gelen saldırıların tespiti için geliştirilen düşük etkileşimli bir tuzak sistemdir. Temel görevi modem ve yönlendiriciler için son yıllarda çıkmış popüler bazı açıklıklara karşı savunmasız, TR-069 protokolünü destekleyen komple bir sistem sunmak ve sistem ile olan tüm etkileşimlerin detaylı bir şekilde kaydını tutmaktır.

5.2 Geliştirme Ortamı

Uygulama nesne yönelimli, modüler, kod okunabilirliği dikkate alınarak tasarlanan, yüksek seviyeli Python programlama dili ile geliştirilmiştir. Python tercih edilmesinin sebebi farklı işletim sistemleri üzerinde çalışabilmesi, pek çok Linux dağıtımında ön tanımlı bir bileşen olarak gelmesi ve derlenmeye ihtiyaç olmadan kullanılabilmesidir.

Geliştirme ortamı Windows ve Windows üzerinde sanal olarak çalışan Linux işletim sistemlerinin birlikte kullanımından oluşmaktadır. Windows üzerinde kodun yazılması ve düzenlemesi amaçlı yaygın kullanıma sahip Python tümleşik geliştirme ortamlarından PyCharm kullanılırken, Linux işletim sisteminde ise uygulamanın çalışması test edilerek hata ayıklama işlemleri yapılmıştır.



ŞEKİL 5.1: PyCharm Python tümleşik geliştirme ortamı.

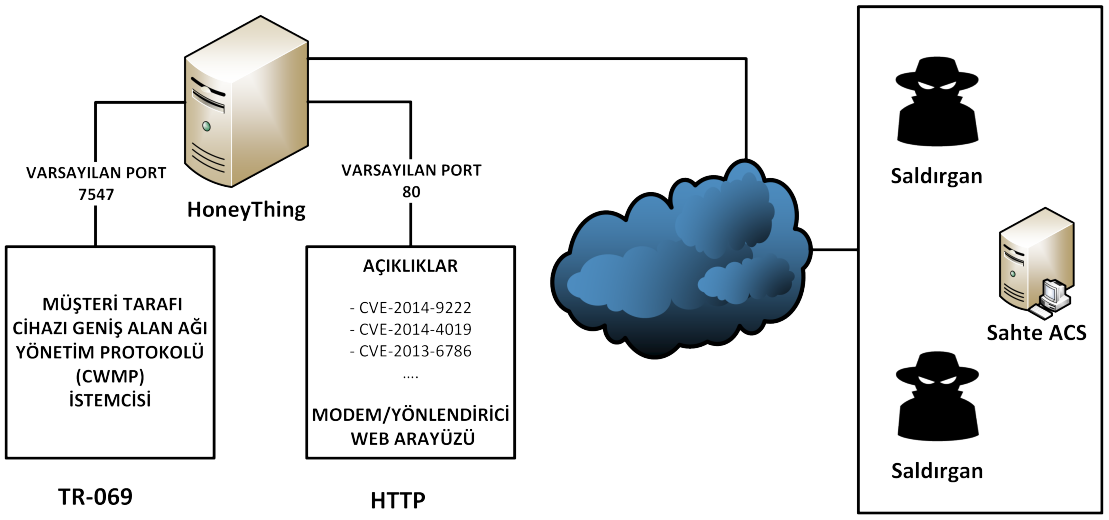
Yazılan uygulamanın geliştirme aşamasında hataların, düzeltmelerin, yeni eklenen özelliklerin takibi amaçlı açık kaynaklı/ticari uygulamaların kod yönetimi ve sürüm kontrolünü sağlayan web tabanlı GitHub uygulaması kullanılmıştır.

Çeşitli açıklıklara karşı cihazların verdikleri yanıtları anlamak, test etmek ve TR-069 protokolünün çalışmasını öğrenmek amaçlı farklı marka modellerden birçok modem/yönlendirici kullanılmıştır. Test edilen cihazlar şöyle sıralanabilir:

- ZyXEL P-600 Series Model Number: P-660R-T1 v3s
- TP-LINK 150Mbps Wireless Lite N Router Model No: TL-WR740N Ver:1.8
- Creative Broadband Bluster DSL Router 8015U-T1
- AirTies 150 Mbps Wireless ADSL2+ Modem Model: Air5342
- TP-LINK TD-W8961ND 300Mbps Wireless N 4 Ports ADSL2+ Modem Router
- Philips Wireless Repeater 11g True Turbo Model: SNR6500
- D-Link ADSL2+ Router Model: DSL-526B
- Netgear 3G/UMTS Mobile Broadband Wireless-N Router MBRN3000
- Belkin High-Speed Mode Wireless G Router 125 HSM Model: F5D7231-4
- TP-LINK 300Mbps Wireless N Access Point Model No: TL-WA901ND Ver:2.3

5.3 Sistem Bileşenleri

Çalışma kapsamında geliştirilen uygulama iki ana bölümden oluşmaktadır. Birinci kısımda popüler bazı açıklıkların benzetimi yapılarak bir modem web arayüzü HTTP protokolü aracılığıyla sunulmuştur. Amaç bu açıklıkları kullanmaya çalışan saldırganlar hakkında detaylı bilgi elde etmek ve web arayüzü kullanımından (kullanıcı adı/parola denemeleri, en sık ziyaret edilen URL vb.) istatistiki bilgiler çıkarmaktır.



ŞEKİL 5.2: HoneyThing tuzak sisteminin yapısı.

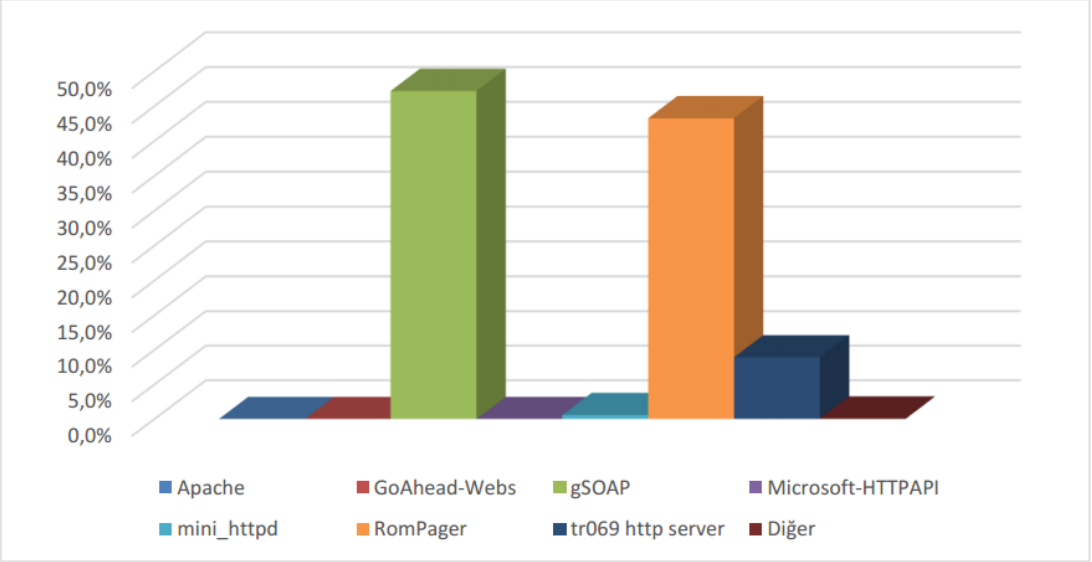
İkinci kısımda TR-069 protokolünün istemci tarafı komutlarının işletilmesini sağlayan CPE uygulaması HoneyThing'e entegre edilerek birlikte çalışması sağlanmıştır. Bu bölümde hedef, TR-069 protokolü kullanılarak yapılabilecek bilinmeyen saldırıların tespiti, saldırgan davranışının kayıt altına alınması ve bu protokole yönelik saldırı miktarı vb. istatistiklerin çıkarılmasıdır.

5.3.1 HTTP

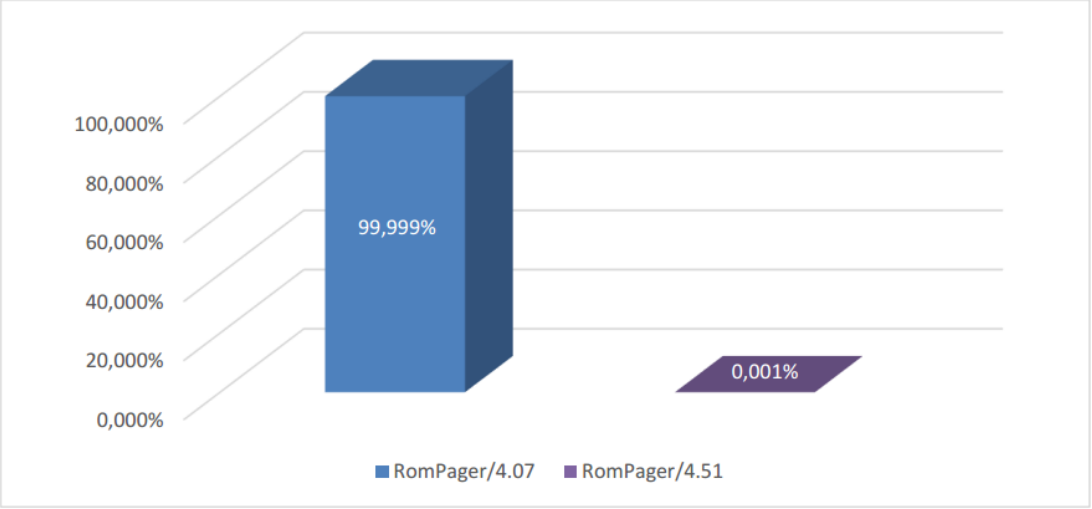
İlk bölümün geliştirilmesi amaçlı farklı marka/modelden birçok cihaz için açıklıklar araştırılmış ve günümüzde potansiyel kurban sayısının fazla olduğu 3 açıklık tespit edilmiştir. Bu açıklıkların ortak yönü gömülü web sunucusu RomPager uygulamasında çalışmasıdır. Allegro firması tarafından ilk olarak 1996 yılında geliştirilen RomPager, düşük boyutlu disk ve bellek kullanan sistemler için tasarlanmıştır [45]. Güncel versiyonu 5.4'tür.

TR-069 protokolünün çalıştığı sunucuların %52'sini oluşturan RomPager ve %52 içerisinde %98'lik dağılıma sahip 4.07 versiyonu, 2002 yılında çıkmış, günümüzde halen 50 farklı

marka ve tanımlanan 200 farklı modelden yaklaşık 12 milyon cihaz tarafından kullanılmaktadır [46]. Michigan Üniversitesi ZMap takımının belirli periyotlarla yaptığı varsayılan TCP/7547 port tarama sonuçları analiz edilerek TR-069 CPE sunucu türlerinin dünya üzerindeki dağılımına ilişkin veriler elde edilmiştir. Detaylara Ek A'dan erişilebilir. Benzer bir çalışma olarak olası saldırılarda Türkiye'deki potansiyel kurbanların tespiti, RomPager dağılımının Türkiye'deki durumunu görmek amaçlı 7547 TCP portu taranmıştır. Tarama açık kaynak kodlu ağ tarayıcısı ZMap aracıyla gerçekleştirilmiştir. ZMap, tek bir makine ile Gigabit Ethernet'in teorik limitine erişerek, IPv4 adres uzayını 45 dakikanın altında bir sürede tarayabilme yeteneğine sahiptir [47]. Tarama ile ilgili sonuçlar Şekil 5.3 ve Şekil 5.4'de gösterilmiştir.



ŞEKİL 5.3: TR-069 sunucu türlerinin dağılımı.



ŞEKİL 5.4: RomPager gömülü web sunucusunun versiyon dağılımı.

Elde edilen tarama sonuçlarına göre ülkemizde 1 milyon cihazın TR-069 protokolü için 7547 portunun açık olduğu, bu cihazların %43'ününün üzerinde RomPager gömülü web sunucusunun çalıştığı, RomPager web sunucuları arasında ise %99'luk oranla birçok açıklığa sahip 4.07 versiyonunun kullanıldığı gözlemlenmiştir.

Türkiye ve diğer ülkelerdeki modem/yönlendirici cihazlarda kullanılan web sunucuları ve versiyonlarının dağılımı incelendiğinde geliştirilen tuzak sistemin RomPager 4.07 sunucusu gibi davranması ve onun sahip olduğu açıklıkların benzetimini yapması gerektiğine karar verilmiştir. Bu amaçla istenilen özelliklere sahip *"TP-LINK TD-W8961ND"* cihazı seçilmiş ve davranışı analiz edilmiştir.

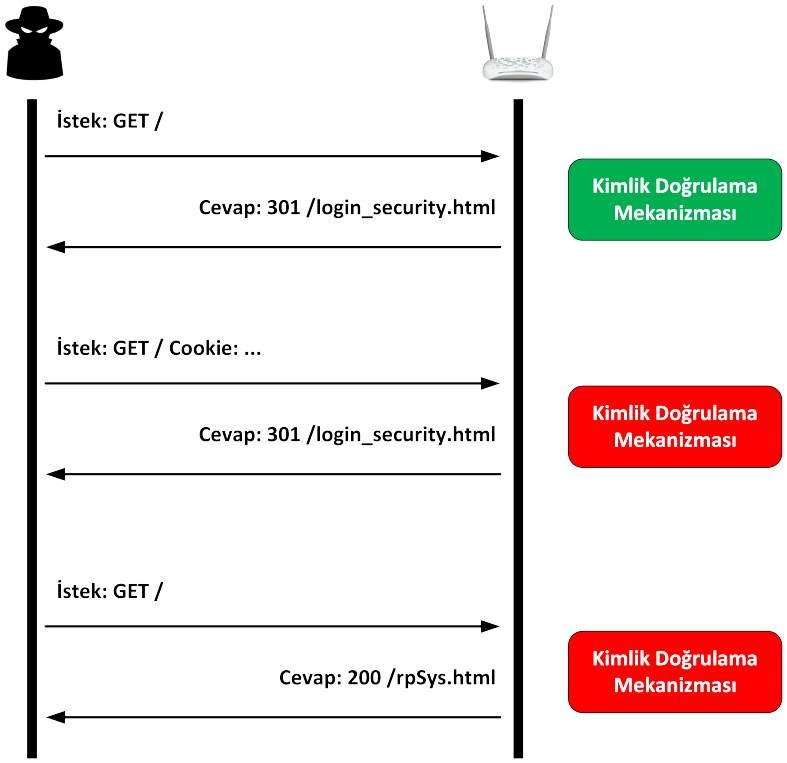
HTTP bölümünün yetenekleri arasında GET, POST isteklerine RomPager web sunucusu zannedilmesi amaçlı özel başlık bilgileri ile (sistem, sunucu versiyonu vb.) cevap verebilmek, kullanıcı kimlik doğrulaması ve oturum yönetimini sağlamak, açıklıkların benzetimini yapmak sayılabilir.

5.3.1.1 CVE-2014-9222

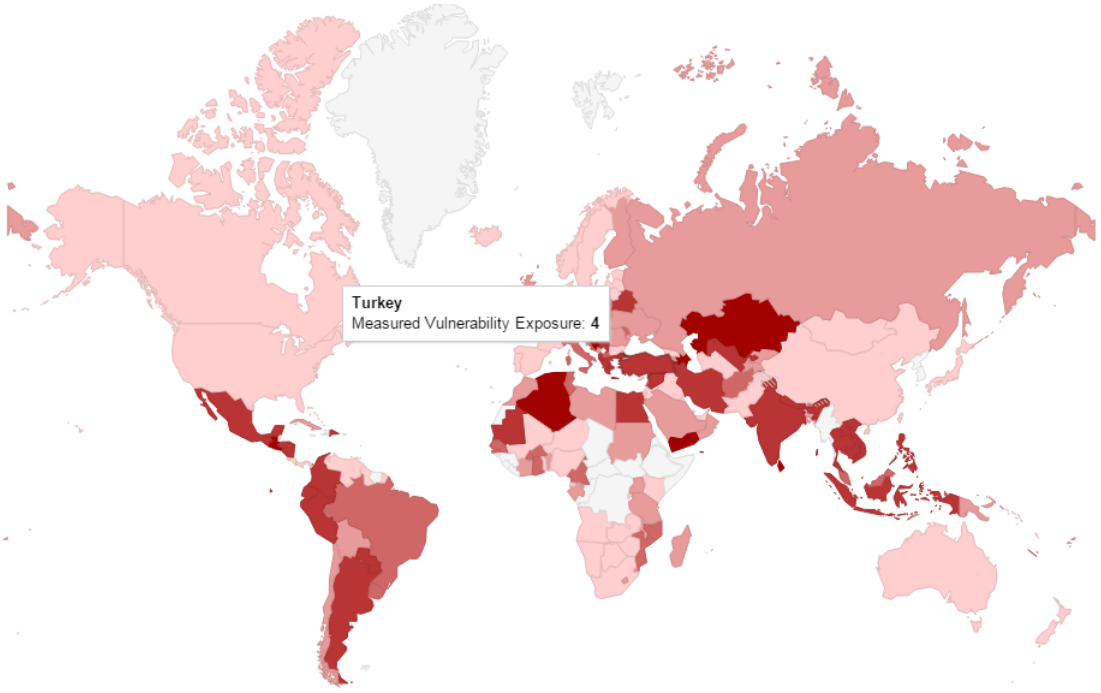
Aralık 2014 tarihinde Check Point firması araştırmacıları tarafından tespit edilen ve modem/yönlendirici cihazlar üzerinde yönetici hakkı elde etmeyi sağlayan açıklıktır. "Misfortune Cookie" olarak adlandırılmıştır. Saldırıda TR-069 protokolünün ACS'den gelen bağlantı istekleri için açık bulunan 7547 portu kullanılmaktadır.

Açıklık RomPager web sunucusunun HTTP çerez yönetim mekanizmasındaki hatadan kaynaklanmaktadır. Saldırgan düzenlediği özel çerez değeriyle gönderdiği isteğin kaderini (nasıl işleneceğini) belirleyebilir. Bu şekilde istekler gönderen saldırgan, cihazın hata vermesini sağlayabilir ve yönetici haklarıyla kullanıcı arayüzüne erişim sağlayabilir. Yapılacak saldırılar için herhangi bir özel araç gerekmez. Sadece amaca uygun paket oluşturup cihaza göndermek yeterli olacaktır.

189 farklı ülkeden yaklaşık 12 milyon cihaz açıklıktan etkilenmiştir. Şekil 5.6'da etkilenen cihaz sayısının ülkelere göre dağılımını gösteren dünya haritası görülmektedir. Dağılımın oluşturulması için yapılan taramada varsayılan 7547 portu kullanılmıştır. Ülkelere göre servis sağlayıcıların protokol için kullandıkları port dikkate alınarak tarama yapılması daha kesin sonuç verecektir. 1'den 5'e kadar yapılan derecelendirmede, 1 açıklığa sahip cihaz sayısının minimum olduğunu gösterirken, 5 maksimum değerdir [48].



ŞEKİL 5.5: "Misfortune Cookie" açıklığı saldırı senaryosu.



ŞEKİL 5.6: "Misfortune Cookie" açıklığından etkilenen cihaz sayısının ülkelere göre dağılımı.

Bilgisayar, yazıcı, telefon, güvenlik kamerası, buzdolabı gibi birçok cihazın bağlı olabileceği modem üzerinde istenilen yetkiyi elde eden saldırgan, ağ trafiğini dinleyebilir, DNS ayarlarını değiştirerek kullanıcı trafiği arasına girebilir, port yönlendirme ile cihazlara erişebilir ve hassas kullanıcı verilerini ele geçirebilir. Açıklığın kapatılması için önerilen, cihaza ait varsa güncel yazılımın yüklenmesidir. Teknik bilgiye sahip kullanıcı bunu kendisi yapabileceği gibi servis sağlayıcısından da talep edebilir. Servis sağlayıcılar CPE'leri (modem, VoIP telefon vb. cihaz) herhangi bir değişiklik olması durumunda ACS'yi bilgilendirecek şekilde yapılandırabilir. Böylece ele geçirilen cihazın tespiti kolay olacaktır [49].

Geliştirilen sistemde açıklığın uygulanabilmesi için açıklığı bulan ekibin iddialarını kanıtlamak (PoC) için yayınladıkları özel HTTP çerez ismi kontrol edilmiş ve karşılık gelen değer ile ilgili işlem açıklanan şekilde yapılmıştır. Açıklığı tespitte kullanılan araçlar da bu özel değeri kullanmaktadır.

5.3.1.2 CVE-2014-4019

ROM-0 (CVE-2014-4019) açıklığında ise saldırgan cihaza ait servis sağlayıcı bağlantı parolası, kablosuz ağ bağlantı parolası, yönetim arayüzü parolası vb. hassas yapılandırma bilgilerini içeren yedek (backup) dosyasını yetkilendirilmesi yapılmamış bir URL üzerinden indirebilmekte ve çeşitli yöntemlerle bu bilgilere ulaşabilmektedir [50]. Ayrıca açıklığa sahip cihazın tespiti ve indirilen dosyadan hassas bilgilerin elde edilmesi sürecini otomatikleştiren çeşitli araçlar geliştirilmiştir.

İlk kez 2014 yılında yayınlanan açıklıkla ilgili yapılan ilk taramada 1.219.985 cihazın saldırıya açık olduğu gözlemlenmiştir [51]. Alınabilecek önlemler arasında modemin 80 portunun ağ üzerinde kullanılmayan bir IP adresine yönlendirilmesi, varsa cihaz tedarikçilerin yayınladıkları güncellemenin uygulanması ve cihazın uzaktan yönetimi ile ilgili tüm bağlantı özelliklerinin güvenlik duvarı üzerinden kapatılması sayılabilir.

Açıklığın geliştirilen sistem üzerinde uygulanabilmesi için ilk olarak test modemi rastgele bilgilerle yapılandırılmıştır. İşlemin tamamlanmasının ardından yedekleme dosyası modemden alınarak geliştirilen HTTP web sunucusuna konulup "/rom-0" veya "/ROM-0" URL'lerinden herhangi bir kimlik doğrulaması yapılmadan indirilmesine izin verilecek şekilde düzenlenmiştir.

5.3.1.3 CVE-2013-6786

Saldırganın sunucu üzerinde olmayan bir URL'ye gönderdiği özel istek sayesinde URL yönlendirme ve siteler arası betik çalıştırmayı (XSS) sağlayan bir diğer önemli açıklıktır. ZyXEL, TP-LINK, D-Link ailesinden birçok cihazı etkilemektedir [52]. URL yönlendirme atağı sayesinde zararlı bağlantılara erişim sağlanabilir, XSS açıklığı kullanılarak çalıştırılacak betiklerle kullanıcı bilgileri elde edilebilir. Açıklığı gidermek için önerilen çözüm RomPager versiyonunun 4.51'e yükseltilmesidir.

Açıklık sistem üzerinde olmayan sayfalara gelen istekler için 'Referer' başlığının kontrolü ve başlık değerlerine uygun hata sayfasının özelleştirilmesiyle gerçeklenmiştir.

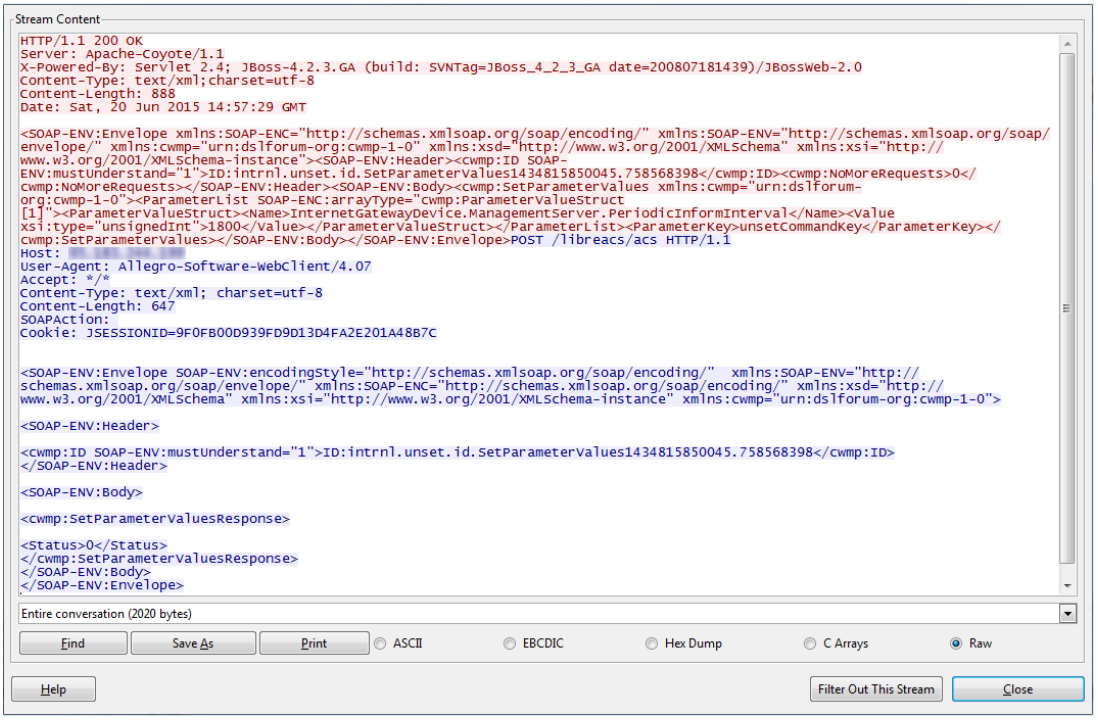
5.3.1.4 Modem Yönetim Arayüzü

HoneyThing'e tüm özellikleriyle bir modemi yansıtabilmesi için yönetim arayüzü eklenmiştir. Arayüz için gerekli dosyalar test amaçlı kullanılan modemden ve cihazı üreten firmanın aynı modele ait web sitesinden sunduğu simülasyon uygulamasından elde edilmiştir.

Arayüz dosyaları üzerinde olmayan sayfalar için İngilizce dil desteği eklenmiş, kimlik doğrulama için denenen parola bilgisinin açık bir şekilde kayıt dosyalarında görünmesi amaçlı düzenlemeler yapılmış ve hata sayfaları RomPager'a uygun şekilde özelleştirilmiştir.

5.3.2 TR-069

TR-069 protokolünün çalışmasını anlamak amaçlı dokümanlardan faydalanmakla birlikte test edilen modem üzerinde protokol çalıştırılmıştır. Bu amaçla modem ADSL hattına bağlanmış ve internet üzerinde bir sunucuya da ACS uygulaması konulmuştur. Aralarındaki trafik PCAP formatında kaydedilip, sonrasında detaylı analiz yapılmıştır. Kaydedilen trafikten alınan örnek bir iletişim Şekil 5.7'de görülmektedir.



ŞEKİL 5.7: Test modemi ile kaydedilen TR-069 protokolüne ait örnek iletişim.

HoneyThing'in bu bölümünü geliştirme amaçlı TR-069 protokolünün istemci tarafını gerçekleyen çeşitli uygulamalar araştırılmıştır. Saldırganın protokolün tüm detayları ile uğraşması ve protokole özel gözden kaçabilecek küçük detaylara özel istek göndermesi durumunda karşısındakinin tuzak sistem olduğunu anlaması ihtimaline karşın protokolü tam olarak gerçekleyen bir uygulama kullanımına karar verilmiştir. Freecwmp, Mini CWMP, Catawampus ve EasyCwmp benzeri uygulamalar araştırılmış, kurulup test edilmiştir. Seçilecek uygulamada aranan özellikler, açık kaynak kodlu olması, Python programlama dilinde geliştirilmiş olması ve protokolün çoğu özelliklerini desteklemesidir. Bu nedenle "Catawampus" uygulamasında karar kılınmıştır.

Catawampus, Google çalışanları tarafından geliştirilmiştir. İsim, CWMP harflerinin sırasıyla yer almasından dolayı tercih edilmiştir [53]. Temel özellikleri arasında CWMP'nin 10'dan fazla CPE komutunu ve SSL'li iletişimi desteklemesi, tek başına çalışabilmesi için yerel ACS uygulaması bulundurması, IPv6 ping isteklerini kabul etmesi, güvenlik amaçlı ACS sunucu URL'lerinin kısıtlanabilmesi sayılabilir.

Uygulamanın HoneyThing ihtiyaçlarına uygun olarak çalışması için çeşitli değişiklikler yapılmıştır. Önemlileri şöyle sıralanabilir:

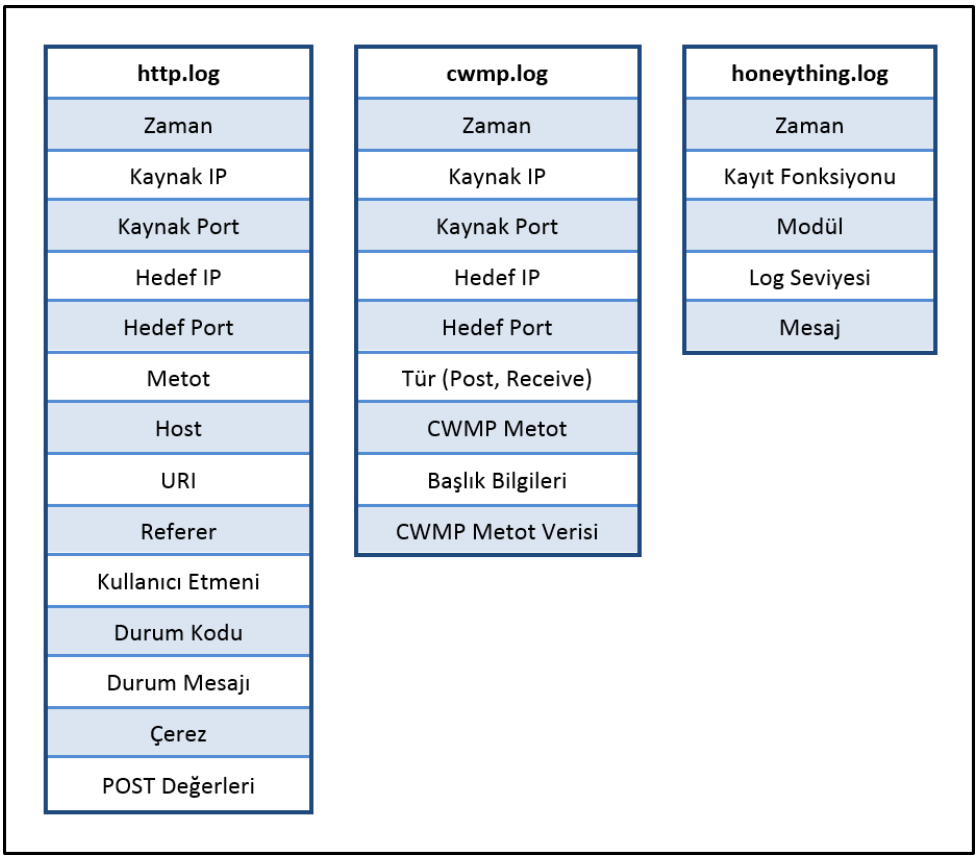
- ACS'den gelen istekte, CPE üzerinde tanımlanmamış herhangi bir kullanıcı adı parola ile bağlantı kurulabilmesi sağlanmıştır. Böylece sahte ACS'lerin bağlanabilmesine olanak tanınmıştır.
- CPE üzerine yazılım ve yapılandırma dosyalarının indirilmesini sağlayan "Download" komutu kısmı düzenlenerek dosyanın indirildikten sonra istenilen dizinde saklanması özelliği eklenmiştir.
- Uygulamanın çalışması ve benzetimini yaptığı cihaz ile ilgili tüm bilgilerin yapılandırma dosyasından okunarak değiştirilebilir olması sağlanmıştır.
- Protokolün çalışması ve uygulamanın içsel durumları ile tüm kayıtların detaylı analiz için belirtilen bir log dosyasına yazdırılması özelliği eklenmiştir.
- ACS'ye gönderilen başlık bilgilerinde CPE'nin bir benzetim uygulaması olduğunun anlaşılmasını sağlayacak bazı parametreler değiştirilmiştir.

5.4 HoneyThing Kayıtları

Saldırgan ile tuzak sistem arasındaki HTTP, CWMP iletişimleri, sistemin içsel durumu ile ilgili bilgiler, kolay okunabilmesi ve detaylı analiz yapılabilmesi amaçlı metin belgesi formatında kaydedilmektedir. "http.log", "cwmp.log" ve "honeything.log" olmak üzere 3 adet kayıt dosyası tutulmaktadır. Tüm kayıtlar ayrıştırılmasını kolaylaştırmak amaçlı "tab" karakteriyle ayrılmış olarak yazılmakta ve olaya ilişkin zaman bilgisi ile başlamaktadır. Kayıt dosyalarında yer alan bilgilerle ilgili detaylar Şekil 5.8'de gösterilmiştir.

5.4.1 HTTP Kayıtları

HTTP iletişimine ilişkin kayıtları tutar. Yapılan tüm GET, POST işlemlerine ait bilgiler ve trafik ile ilgili temel IP, port bilgileri dosyaya yazılmaktadır. Kayıt parametrelerinin belirlenmesinde açık kaynak kodlu Bro IDS uygulamasının ürettiği HTTP kayıtlarından faydalanılmıştır.



ŞEKİL 5.8: HoneyThing kayıt dosyalarında yer alan bilgiler.

HTTP kayıtlarının dosyaya yazılmasında yapılandırma dosyasından düzenlenebilecek şekilde iki farklı durum vardır. İlki IP, port, metot gibi temel bilgilerin kaydedildiği normal moddur. Genişletilmiş modda ise iletişim ile ilgili çeşitli başlık bilgileri de dosyaya yazılır. Kaydedilmiş örnek bir HTTP iletişimi Şekil 5.9'da görülmektedir.

```
2015-08-03 15:52:11,364         192.168.2.10   60802   192.168.2.15  80      POST
  192.168.2.15  /Forms/login_security_1.html    http://192.168.2.15/login_security.
html       Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
        200     OK      -       {'uiWebLoginhiddenPassword': ['21232f297a57a5a7438
94a0e4a801fc3'], 'timevalue': ['0'], 'Login_Pwd': ['admin'], 'uiWebLoginhiddenUsern
ame': ['21232f297a57a5a743894a0e4a801fc3'], 'tipsFlag': ['0'], 'Login_Name': ['admi
n']}

2015-08-04 19:07:19,462         192.168.2.10   59356   192.168.2.15  80      GET
  192.168.2.15  /css/style.css  http://192.168.2.15/status/status_deviceinfo.htm
   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
200     OK      C0=21232f297a57a5a743894a0e4a801fc3; C1=21232f297a57a5a743894a0e4a8
01fc3       -

2015-08-18 15:25:48,426         192.168.2.10  49309   192.168.2.15  80      GET
 192.168.2.15  /AIVkcFhRRyPKCMjk       http://192.168.2.15/  Mozilla/4.0 (compatibl
e; MSIE 6.0; Windows NT 5.1)      404     Not Found       -       -

2015-08-18 15:25:48,430         192.168.2.10  55322   192.168.2.15  80      GET
 192.168.2.15  /       http://192.168.2.15/  Mozilla/4.0 (compatible; MSIE 6.0; Win
dows NT 5.1)      404     Not Found       C107373883=/AIVkcFhRRyPKCMjk;
```

ŞEKİL 5.9: HoneyThing HTTP kayıt dosyası içeriği.

5.4.2 TR-069 Kayıtları

TR-069 protokolü haberleşmesi ile ilgili kayıtları tutmaktadır. CPE'nin gönderdiği ve ACS'den gelen mesajların içerikleri, iletişim ile ilgili başlık bilgileri dosyaya yazılmaktadır. Mesajların XML formatında ve mesaj veri miktarının fazla olmasından dolayı içeriğin sözcük dizisi (string) halinde dosyaya yazılması okunabilirliği azaltmaktadır. Bu amaçla mesaj verisinin HEX formatında yazılabilmesi seçeneği sisteme eklenmiştir. Bu tercih yapılandırma dosyası kullanılarak belirlenebilmektedir.

```
2015-09-02 14:30:04,768         192.168.2.15  59001   192.168.2.20  8080    CPE_POST
       Inform  {'SOAPAction': '', 'Content-Type': 'text/xml; charset="utf-8"'}
74657374206D6573736167657465737420 6D6573736167657465737420 6D6573736167657465737420 6D
6573736167657465737420 6D6573736167657465737420 6D6573736167657465737420 6D65737361676
74657374206D6573736167657465737420 6D6573736167657465737420 6D6573736174657374206D6573
7361676574657374206D6573736167657465737420 6D6573736167657465737420 6D6573736167657465
7374206D6573736167657465737420 6D6573736167657465737420 6D6573736167657465737420 6D6573
7361676574657374206D6573736167657465737420 6D6573736167657465737420 6D6573736174657374
206D657373616765

2015-09-02 14:30:04,806         192.168.2.20  8080    192.168.2.15  59001   CPE_RECE
IVED    InformResponse  {'Content-Length': '581', 'X-Powered-By': 'Servlet 2.4; JBos
s-4.2.3.GA (build: SVNTag=JBoss_4_2_3_GA date=200807181439)/JBossWeb-2.0', 'Set-Cook
ie': 'JSESSIONID=5B10F059090A02A005CFD3AD68B5505D; Path=/', 'Server': 'Apache-Coyote
/1.1', 'Date': 'Wed, 02 Sep 2015 11:30:04 GMT', 'Content-Type': 'text/xml;charset=ut
f-8'}       74657374206D6573736167657465737420 6D6573736167657465737420 6D65737361676
74657374206D6573736167657465737420 6D6573736167657465737420 6D6573736167657465737420 6D
6573736167657465737420 6D6573736167657465737420 6D6573736167657465737420 6D65737361676
746573742

2015-09-02 14:30:04,808         192.168.2.15  59001   192.168.2.20  8080    CPE_POST
       -       {'Cookie': 'JSESSIONID=5B10F059090A02A005CFD3AD68B5505D; Path=/'}
```

ŞEKİL 5.10: HoneyThing TR-069 kayıt dosyası içeriği.

5.4.3 Sistem Kayıtları

Sistemin içsel hata ve bilgilerine ait kayıtları tutmaktadır. Uygulamanın başlanıp sonlanması, kimlik doğrulama işlemleri, bağlantı problemleri vb. olaylarla ilgili bilgiler dosyaya yazılmaktadır. *"CRITICAL"*, *"ERROR"*, *"WARNING"*, *"INFO"*, *"DEBUG"* olmak 5 farklı seviyede olaylar kaydedilebilmektedir. Örnek kayıt dosyası içeriği Şekil 5.11'de görülmektedir.

```
2015-09-03 13:51:02,963         honeything      HoneyThing      INFO    Starting Ho
neything...
2015-09-03 13:51:03,997         honeything      http    INFO    TR-069 CPE at http:
//*:7547/cpe
2015-09-03 13:51:03,997         honeything      http    INFO    TR-069 callback at
http://*:7547/tr069
2015-09-03 13:51:04,313         honeything      http    ERROR   HTTP ERROR 599: HTT
P 599: Failed to connect to 192.168.2.20 port 8080: No route to host
2015-09-03 13:51:04,472         honeything      digest  WARNING         please auth
enticate
2015-09-03 13:51:04,476         honeything      digest  INFO    Expected: 5e77b3ef1
ec41728921e6b55455f022e
2015-09-03 13:51:05,476         honeything      digest  INFO    Actual: 5e77b3ef1ec
41728921e6b55455f022e
2015-09-03 13:51:05,477         honeything      digest  INFO    Digest Auth user 't
est_user' successful for realm 'Authusers'. URI: '/tr069', IP: '192.168.2.20'
2015-09-03 13:51:06,145         honeything      http_download   INFO    starting (a
uth_header=None)
2015-09-03 13:51:15,007         honeything      download        INFO    Download co
mplete callback.
2015-09-03 13:51:20,225         honeything      http    INFO    Idle CWMP session,
terminating.
```

ŞEKİL 5.11: HoneyThing sistem kayıt dosyası içeriği.

5.4.4 Kayıtların İzlenmesi ve Analizi

Kayıtlar HoneyThing'in tek başına çalışması durumumda doğrudan sistem üzerinde incelenebilir. Basit Linux araçlarıyla kayıt takibi yapılabilir ve istatiksel bilgi elde edilebilir. HoneyThing'in birçok farklı coğrafi yerde çalışması durumunda ise kayıtlar istenilirse merkezi bir kayıt toplama sunucusuna gönderilebilir. Toplanan kayıtlar bir veritabanına kaydedilip açık kaynak kodlu herhangi bir görselleştirme aracı ile izlenebilir. Bu senaryo için yaygın olarak kullanılan ELK (Elasticsearch, Logstash, ve Kibana) araçlarından faydalanılabilir. Ayrıca kayıtlar MySQL veya PostgreSQL gibi bir veritabanına kaydedilip Splunk benzeri bir araçla da izlenebilir.

Sistem üzerine indirilen dosyalar yazılacak basit betiklerle istenilen protokol üzerinden belirlenen bir sunucuya gönderilebilir. Dosyalar analiz amaçlı VirusTotal benzeri çoklu virüs tarama platformlarından birine ve çevrimiçi ya da çevrimdışı sandbox'lara gönderilip sonuçları analiz edilebilir. Bu şekilde kullanım sistemden elde edilen verimi arttıracaktır.

5.5 Kurulum ve Kullanım

HoneyThing sistem üzerine kurularak çalıştırılabileceği gibi derlenmeye ihtiyaç duymadığından doğrudan da kullanılabilir. Her iki durumda da sistemde Python (2.7 veya üzeri) ve PycURL uygulamaları kurulu olmalıdır. Doğrudan çalıştırma durumunda *"PYTHONPATH"* çevresel değişkeninin ayarlanması, Python kurulum betiği kullanılması halinde ise sistemde Python "setuptools" paketinin olması gerekmektedir. Ayrıca kurulum için Unix/Linux tabanlı farklı işletim sistemlerinde çalışabilen HoneyThing için oluşturulmuş Debian ve RPM dosyaları da kullanılabilir.

Paketlerin kurulup gerekli ayarlar yapılarak uygulamanın kullanıma hazır hale gelmesinden önceki son adım yapılandırma dosyası aracılığı ile bazı çalışma ayarlarının düzenlenmesidir. Bu ayarları içeren "config.ini" dosyasındaki *http*, *authentication*, *cwmp*, *cpe* ve *logging* başlıkları altında çeşitli parametreler bulunmaktadır.

- http bölümünde bulunan "address" ve "port" satırları uygulamaya gelecek HTTP isteklerinin dinleneceği adresleri gösterir. İnternet üzerinden gelen isteklerin kabul edilmesi için varsayılan olarak adres 0.0.0.0'a ayarlanmıştır. "directory" parametresi ise sunulan web uygulaması ile ilgili dosyaların bulunduğu dizini işaret eder.

- authentication bölümünde modem yönetim arayüzüne giriş yapılabilmesi için tanımlı kullanıcı adı, parola bilgileri bulunmaktadır.

- cwmp bölümünde TR-069 protokolüne gelecek bağlantı isteklerinin dinleneceği adres, port bilgileri, CPE'nin bağlantı kuracağı ACS adresi, protokol aracılığıyla indirilecek dosyaların saklanacağı dizin, TR-069 bağlantı istek yolu vb. parametreler düzenlenebilmektedir. ACS adresinin boş bırakılması durumunda sistem sadece varsayılan porttan gelecek bağlantı isteklerini dinleyecektir.

- cpe bölümünde benzetimi yapılan cihaz ile ilgili iletişim sırasında karşı tarafa gönderilecek çeşitli bilgiler yer almaktadır. "manufacturer", "serial_number", "hardware_version", "model_name" vb. bunlar arasında sayılabilir. Bilgiler isteğe göre düzenlenebilir.

- logging bölümünde uygulamanın tuttuğu 3 adet kayıt dosyasının isimleri ve sistem üzerinde hangi dizine kaydedilecekleri belirlenmektedir. Uygulama çalıştırılmadan önce belirtilen dizinlerin sistem üzerinde var olduğundan emin olunmalıdır.

"http_extended" parametresi HTTP iletişimi kaydedilirken temel bilgilerin yanında ekstra parametrelerin olup olmayacağını (yes, no), "cwmp_data_format" ise TR-069 haberleşmesinde mesaj verisinin yazılacağı formatı belirler (hex, text).

Varsayılan değerlere göre düzenlenmiş örnek bir yapılandırma dosyası Şekil 5.12'de görülmektedir.

```
[http]

address=0.0.0.0
port=80
directory=www/TD-8951ND

[authentication]

http_user=admin
http_pass=admin

[cwmp]

address=0.0.0.0
port=7547
acs_url=http://192.168.2.20:8080/libreacs/acs
download_dir=/opt/honeything/download
cwmp_dir=/opt/honeything
socket_file=/opt/honeything/run/cwmpd.sock
request_path=tr069

[cpe]

manufacturer=TP-LINK
manufacturer_oui= 001D0F
product_class=DSL Gateway
serial_number=30B5C2C1BC0C
model_name=TD-8951ND
description=SOHO Router
hardware_version=TD-W8961ND V3
software_version=Build 140425 Rel.09888
firmware_version=V6_150522

[logging]

file_http=/var/log/honeything/http.log
file_cwmp=/var/log/honeything/cwmp.log
file_honeything=/var/log/honeything/honeything.log
http_extended=yes
cwmp_data_format=hex
level=INFO
```

ŞEKİL 5.12: HoneyThing örnek yapılandırma dosyası.

Uygulamanın çalıştırılması için "honeything" betiği kullanılmaktadır. Desteklediği özellikler betiğin herhangi bir parametre verilmeden çalıştırılmasıyla görüntülenebilir. Temel olarak kullanılan parametreleri şöyle sıralanabilir:

- *start*: Uygulamanın başlatılmasını sağlar.
- *stop*: Uygulamanın sonlanmasını sağlar.
- *restart*: Uygulamayı sonlandırıp yeniden çalıştırır. Genellikle yapılandırma dosyasındaki değişikliklerden sonra kullanılmaktadır.
- *status*: Uygulamanın çalışma durumu ile ilgili bilgileri gösterir.

HoneyThing düşük etkileşimli 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 makinaları etkileyebilir. Bununla birlikte tuzak sistemin üzerinde çalıştığı işletim sisteminin güvenlik güncellemeleri periyodik olarak yapılmalıdır.

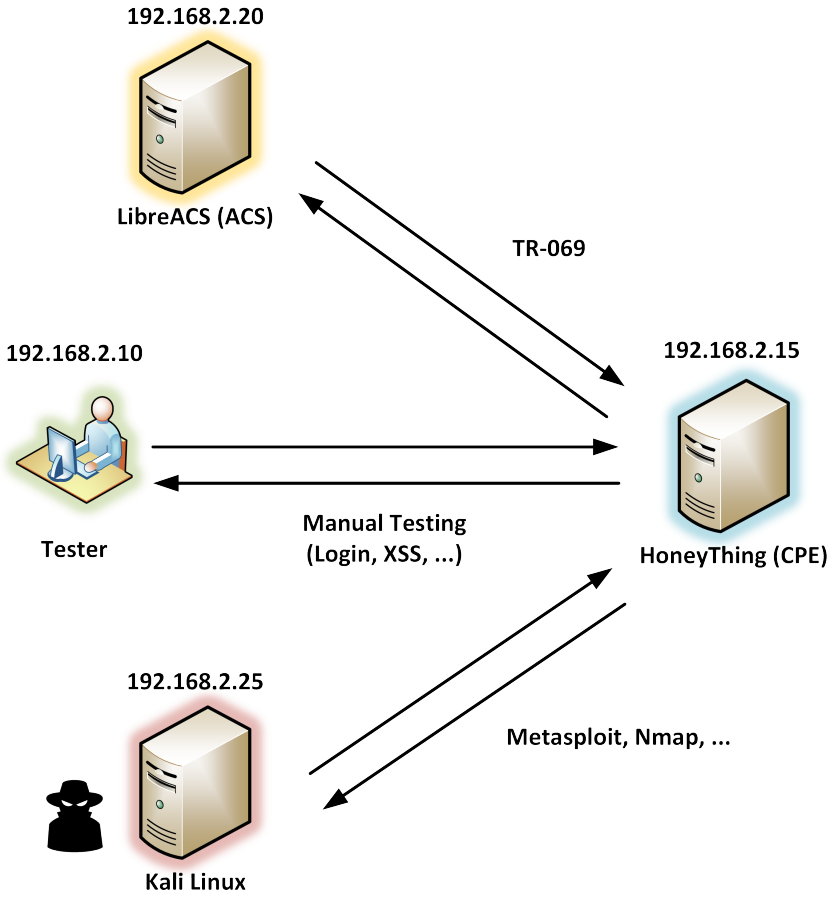
Tuzak sistemin farklı lokasyonlarda çalıştırılması durumunda o ülkeye ait ISP'lerin sunduğu modem/yönlendirici cihazlarında bağlantı isteği için kullanılan portun TR-069 portu olarak ayarlanması sistemin kullanılabilirliğini arttıracaktır. Aynı ülkede kullanılan farklı TR-069 portları için tuzak sistemler ayrı ayrı yapılandırılarak portların kullanım oranları ile ilgili bilgiye erişilebilir. Ayrıca yapılandırma dosyasında yönetim arayüzü için farklı zorluklarda belirlenecek kullanıcı adı parola çiftleriyle çeşitli istatistiki bilgi elde edilebilir.

5.6 Test

HoneyThing uygulamasının genel ve fonksiyonellik testleri yerel alan ağında gerçekleştirilmiştir. TR-069 protokolü için hazırlanan ACS'nin testi ise internet ağında ADSL hattına bağlı gerçek bir modem ile yapılmıştır. Testlerdeki hedef birinci bölüm için açıklıkların manuel olarak tespit edilebildiğini ve uygulamalar tarafından tanındığını, ikinci bölüm için ise TR-069 protokolünün doğru bir şekilde çalıştığının gösterilmesidir.

5.6.1 Test Ortamı

Test amaçlı HoneyThing, Kali Linux, LibreACS ve test bilgisayarı olmak üzere 4 adet makine kullanılmıştır. İlk üçü "VMware Workstation" sanallaştırma uygulaması üzerinde hazırlanmış sanal makineler olup test makinesi fiziksel masaüstü bilgisayarıdır. Tüm makineler aynı alt ağdadır.



ŞEKİL 5.13: HoneyThing test ortamı.

Manuel test için kullanılan masaüstü bilgisayarı Windows 7 x64 işletim sistemine sahip olup üzerinde Internet Explorer, Google Chrome ve Mozilla Firefox tarayıcıları bulunmaktadır.

HoneyThing'in çalıştığı makine Ubuntu 14.04.2 LTS'dir. Ubuntu yerine isteğe bağlı olarak CentOS veya benzeri bir Linux dağıtımı da kullanılabilir.

Kali, HoneyThing'in birinci kısmındaki bazı açıklıkları test etmek amaçlı kullanılmıştır. Üzerinde kurulu gelen Nmap, Metasploit vb. araçlardan faydalanılmıştır.

HoneyThing'in ikinci kısmında ise TR-069 protokolünün çalışmasında gerekli bir bileşen olan ACS için birkaç uygulama kurularak test edilmiştir. Bunlar arasında Perl CWMP, TR-069 D-Link, GenieACS ve OpenACS'nin devamı olan LibreACS adlı açık kaynak kodlu uygulamaları sayılabilir. Yazılacak basit betiklerle istenilen komutun çalışması ve kolay yönetim arayüzü sebebiyle LibreACS uygulaması tercih edilmiştir. JBoss uygulama sunucusunda çalışmakta ve MySQL veritabanını kullanmaktadır. Uygulama Ubuntu Server 14.04.2 LTS işletim sistemi üzerine kurulmuştur. *GetRPCMethods*, *SetParameterValues*, *GetParameterValues*, *Download* vb. sık kullanılan komutlar ACS'ye eklenen 4 adet betik ile test edilmiştir.

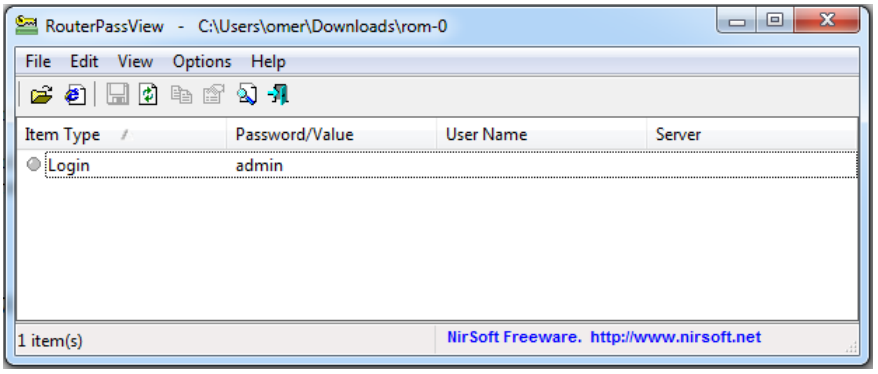
5.6.2 Test Sonuçları

HoneyThing'in benzetimini yaptığı açıklıklar manuel olarak ve Kali Linux makinesiyle test edilmiştir. CVE-2013-6786 kodlu açıklığın testi için, açıklığın detaylarında anlatılan yöntem uygulanmıştır [54]. İlk olarak Nmap aracıyla yapılan taramada HoneyThing makinasında RomPager gömülü web sunucusunun zafiyet barındıran versiyonunun çalıştığı gözlemlenmiştir. Sonraki adımda basit bir betik kodu sunucu üzerinde olmadığı tahmin edilen URL'ye "Referer" başlığında gönderilmiş ve gelen cevapta kodun sunucu tarafından betik etiketleri temizlenmeden, olduğu gibi, cevabın "body" kısmına yerleştirildiği görülmüştür.

```
root@kali:~# nmap --open -sS -sV -T4 192.168.2.15 -p 80 -oG - | grep 'open' | grep RomPager
Host: 192.168.2.15 () Ports: 80/open/tcp//http//Allegro RomPager 4.07 UPnP|1.0 (ZyXEL ZyWALL 2)/
root@kali:~#
root@kali:~# curl -v http://192.168.2.15/nonexistingdata -H \
> "Referer: http://google.com/\"><script>alert(document.cookie)</script&gt;"
* Hostname was NOT found in DNS cache
*   Trying 192.168.2.15...
* Connected to 192.168.2.15 (192.168.2.15) port 80 (#0)
> GET /nonexistingdata HTTP/1.1
> User-Agent: curl/7.38.0
> Host: 192.168.2.15
> Accept: */*
> Referer: http://google.com/"><script>alert(document.cookie)</script&gt;
>
* HTTP 1.0, assume close after body
< HTTP/1.0 404 Not Found
< Server: RomPager/4.07 UPnP/1.0
< Date: Tue, 29 Sep 2015 10:26:10 GMT
<
<html>
<head>
<title>Object Not Found</title></head><body>
<h1>Object Not Found</h1>
The requested URL '/nonexistingdata' was not found on the RomPager server.
<p>Return to <A HREF="http://google.com/"><script>alert(document.cookie)</script&gt">last page</A><p>
</body></html>

* Closing connection 0
```

ŞEKİL 5.14: HoneyThing üzerinde CVE-2013-6786 açıklığının testi.

ROM-0 açıklığına sahip cihazların tespiti için Nmap betiklerinden faydalanılabilir. HoneyThing üzerinde ROM-0 açıklığının benzetiminin yapılması için ilgili adrese konulan yapılandırma dosyası web tarayası aracılığıyla herhangi bir kimlik doğrulaması olmaksızın indirilmiştir. İndirilen dosya NirSoft tarafından geliştirilmiş ve Windows üzerinde çalışan "RouterPassView" aracına verilerek test amaçlı oluşturulmuş modem yönetim arayüzü giriş parolasının elde edildiği gözlemlenmiştir.



ŞEKİL 5.15: HoneyThing'den indirilen ROM-0 dosyasından hassas bilgilerin elde edilmesi.

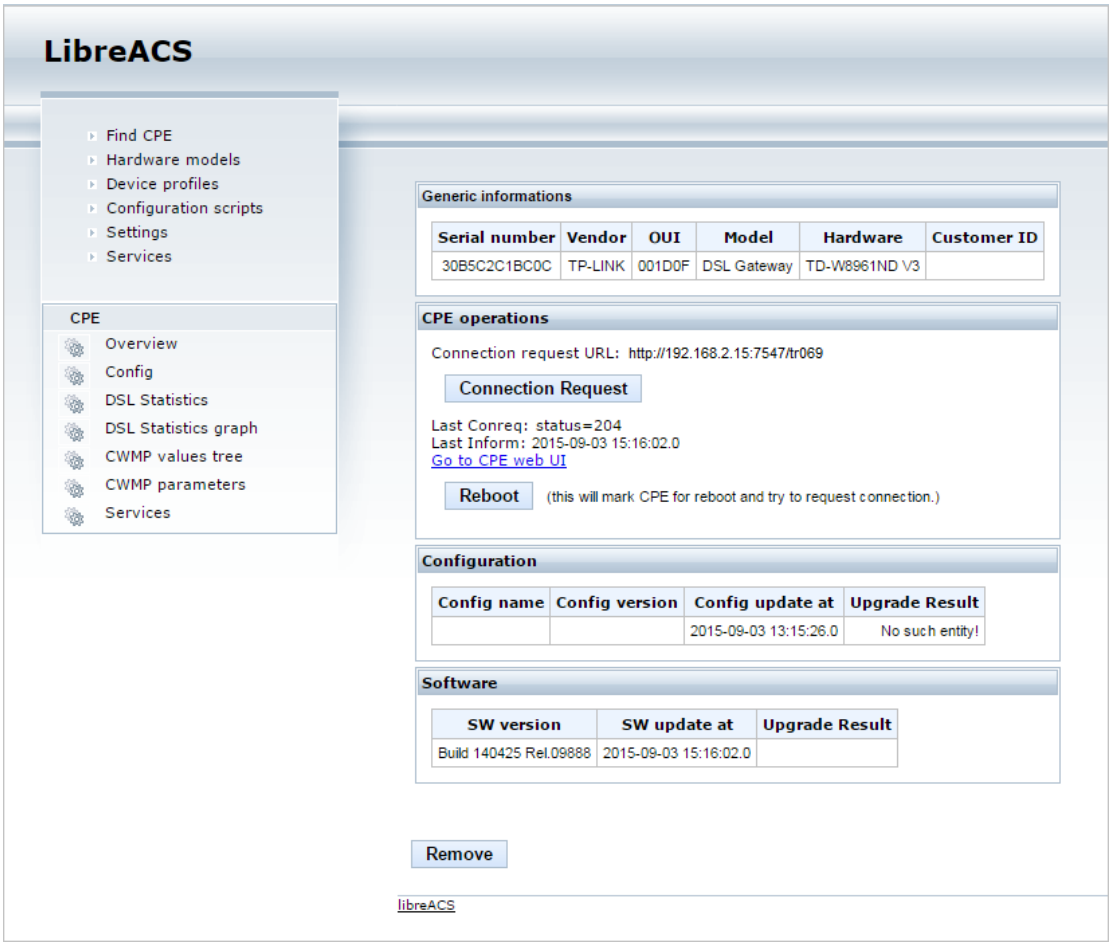
"Misfortune Cookie" açıklığının testi için Kali Linux üzerindeki Metasploit aracı kullanılmıştır. Araç üzerinde bulunan tarayıcılardan *"allegro_ rompager_ misfortune_ cookie"* modülü ile HoneyThing'in bulunduğu ağ taranmış ve HoneyThing için açıklığa sahip anlamında *"Vulnerable"* sonucu döndüğü gözlemlenmiştir.

```
msf auxiliary(allegro_rompager_misfortune_cookie) >
msf auxiliary(allegro_rompager_misfortune_cookie) > show options

Module options (auxiliary/scanner/http/allegro_rompager_misfortune_cookie):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.2.0/24   yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port
   TARGETURI  /                yes       URI to test
   THREADS    4                yes       The number of concurrent threads
   VHOST                       no        HTTP server virtual host

msf auxiliary(allegro_rompager_misfortune_cookie) >
msf auxiliary(allegro_rompager_misfortune_cookie) > run

[+] 192.168.2.15:80 The target is vulnerable.
[*] Scanned  27 of 256 hosts (10% complete)
[*] Scanned  55 of 256 hosts (21% complete)
[*] Scanned  77 of 256 hosts (30% complete)
[*] Scanned 103 of 256 hosts (40% complete)
[*] Scanned 128 of 256 hosts (50% complete)
[*] Scanned 154 of 256 hosts (60% complete)
[*] Scanned 180 of 256 hosts (70% complete)
[*] Scanned 205 of 256 hosts (80% complete)
[*] Scanned 234 of 256 hosts (91% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

ŞEKİL 5.16: HoneyThing üzerinde "Misfortune Cookie" açıklığının testi.

Honeything'in web arayüzü ile ilgili testler bir web tarayıcı aracılığıyla test bilgisayarı üzerinden yapılmıştır. Yönetim arayüzüne giriş için denenen kullanıcı adı parola çiftlerinin ve başarılı giriş sonucu ziyaret edilen URL'lerin kayıt dosyasına (http.log) yazıldığı anlık olarak takip edilmiştir.

TR-069 protokolünün işletilmesini sağlayan ikinci kısmın testi amaçlı LibreACS uygulaması çalışan makina kullanılmıştır. Uygulamanın bağlantı adresi HoneyThing yapılandırma dosyasında ilgili bölüme eklenmiştir. CPE ve ACS çalıştırıldığında CPE bilgilerinin ACS'ye gönderildiği, komutların ACS üzerindeki betiklere göre çalıştığı ve iletişimin kayıt altına alındığı gözlemlenmiştir.



ŞEKİL 5.17: ACS üzerinde iletişim kurulan HoneyThing'e ait özet bilgilerin görüntülenmesi.

"Download" komutunun testi için verilen URL'den HoneyThing'in dosyayı, türüne bakmaksızın indirdiği ve belirtilen dizine kaydettiği görülmüştür. İlk bağlantı ya da periyodik bilgilendirme ile ACS'ye bildirilen bağlantı istek URL'sine LibreACS üzerinden gönderilen her isteğin kullanıcı ad, parola önemli olmaksızın kabul edildiği ve protokole uygun

yanıt verildiği izlenmiştir. Tüm iletişimin mesaj verileriyle birlikte kayıt dosyalarında saklandığı gözlemlenmiştir.

Bölüm 6

Sonuç ve Öneriler

Nesnelerin interneti kavramının giderek önem kazandığı günümüzde bu kavram kapsamına giren cihaz sayısında da önemli artışlar olmuştur. Günlük yaşamda kullandığımız birçok eşya arasında yerini alan bu cihazlarda çeşitliliğin ve sayının fazla olması saldırganlar için hedef alınabilecek yeni bir alan anlamına gelmektedir. Bu durum kavram kapsamına giren cihazlarda daha fazla açıklık araştırılmasına ve saldırıların artmasına neden olmuştur.

Donanımsal olarak yetersiz olan internete bağlı nesnelerde klasik saldırı tespit sistemleri veya zararlı yazılımları tespit edebilecek bir antivirüs uygulaması kullanılamamaktadır. Ayrıca bu cihazların yönetimini sağlayan uygulama ve protokoller ile etkileşim günlük yaşamda daha sık kullandığımız dizüstü bilgisayarı, telefon gibi cihazlara göre düşük olduğundan herhangi bir saldırı veya girişiminin tespiti zordur.

Günümüzde saldırı tespiti amaçlı tuzak sistemler yaygın olarak kullanılmaktadır. Saldırganların hedef aldığı sistemin benzetimini yapan tuzak istemler, gerçek sistemin sahip olduğu herhangi bir kısıta bağlı olmadan istenilen bir işletim sistemi veya ağ topolojisinde çalışabilmektedir. Tuzak sistemlerin birçok protokol için geliştirilmiş uygulamaları kullanılmakta olsa da internete bağlı cihazlardan modem/yönlendiricilerin uzaktan yönetimini sağlayan TR-069 protokolü için geliştirilmiş bir sistem bulunmamaktadır. Çalışma kapsamında geliştirilen ve HoneyThing olarak adlandırılan uygulama bu eksikliği gidermekle birlikte, bu çalışma farklı türde birçok eşyayı içine alan internete bağlı nesnelerde saldırı tespiti için tuzak sistem kullanımını önermektedir.

HoneyThing, TR-069 protokolünü uygulamakta ve benzetimi yapılan cihazlarda çıkmış popüler açıklıkları içermektedir. Kullanılacak açıklıklar Dünya ve Türkiye üzerindeki potansiyel kurban sayısı istatistiğine bakılarak tespit edilmiştir. Uygulama hedeflenen temel özelliklerin yanında taşınabilirlik ve kullanım kolaylığı göz önünde bulundurularak tasarlanmıştır. Geliştirilen sistem klasik sızma testi araçlarıyla ve manuel olarak test edilerek benzetimi yapılmak istenen cihaz özelliklerinin tam anlamıyla yansıtıldığı gözlemlenmiştir.

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 geliştirilecek tuzak sistem, hedef alınan kapsama göre yapılandırılabilir olmalıdır.

HoneyThing'e yeni açıklık modülleri eklenebileceği gibi, kayıtların veritabanı, syslog vb. yerlere yazılması, Honeynet topluluğunun 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 sunulabilir. TR-069 protokolü ile birlikte sunulan modem yönetim arayüzünün çeşitliliği arttırılarak yapılandırma adımında istenilen cihaz modelinin seçilmesi sağlanabilir. Sistem farklı coğrafi bölgelerde çalıştırılarak o bölge için ve genel olarak saldırı istatistiği çıkarılabilir. Ayrıca sistem tarafından yakalanması muhtemel bir zararlı yazılım analiz edilerek saldırı yöntemi, saldırgan davranışı ve internete bağlı nesneler için geliştirilmiş zararlı yazılım türleri hakkında bilgi edinilebilir.

Ek A

TR-069 CPE Sunucu Türlerinin Dağılımı

Michigan Üniversitesi ZMap takımı tarafından 11.09.2015 tarihinde yapılan TCP/7547 port tarama sonuçlarının analizi sonucu tespit edilen sunucu versiyonları ve adetleri Tablo A.1'de gösterilmiştir. (Tabloya 100 ve üzeri adetteki sunucu türleri eklenmiştir.)

Tablo A.1: TR-069 sunucu türlerinin dağılımı

Sunucu Türü ve Versiyonu	**Adet**
WebServer UPnP/1.0	116
Apache-Coyote/1.1	189
squid	217
H150N (gSOAP/2.7)	219
nginx/1.1.19	296
nginx	392
AIM/1.0	460
nginx/0.8.54	544
Conexant-EmWeb/R6_1_0	608
WebServer/1.1	619
Lanswitch - V100R003 HttpServer 1.1	660
nginx/1.0.15	709
Microsoft-HTTPAPI/2.0	763
Apache/2.0.40 (Red Hat Linux)	874
DataflexViNE-Webserver/1.0.0	996
Devamı sonraki sayfada	

Tablo A.1 – önceki sayfadan devam

Sunucu Türü ve Versiyonu	**Adet**
fcwmp	1801
Apache/2.2.22 (Ubuntu)	2556
Microsoft-IIS/7.5	2960
dptech server	3282
RomPager UPnP/1.0	5150
TR069Agent	5631
Switch	5696
RG/Device 10.x	7748
ZyXEL-RomPager/4.34	8051
GoAhead-Webs	9160
TR069 client TCP connection request Server	16756
CPE FILE Server	20201
AVS libcwmp/3.x	27557
NetPort Software 1.1	36508
gSOAP/2.6	39062
Novus Infosys/2.0.40 (Ubuntu)	39297
Allegro-Software-RomPager/4.03	41630
YAPS	66517
WSTL CPE 1.0	71973
WebServer/1.0 UPnP/1.0	98632
RomPager/4.51 UPnP/1.0	143218
Unknown/0.0 UPnP/1.0 Conexant-EmWeb/R6_1_0	242527
tr069 http server	345858
TR069 Connect Request Server	452853
KTT-SOAP/1.0	1066163
mini_httpd/1.19 19dec2003	1339459
Cisco-CcspCwmpTcpCR/1.0	3162422
Apache	3295677
gSOAP/2.7	5128858
RomPager/4.07 UPnP/1.0	9660890

Ek B

Yayınlar

Tez Çalışması Kapsamında Yapılan Yayınlar

Erdem Ö., Kara M., İkinci A., (2015) "HoneyThing: Nesnelerin İnterneti için Tuzak Sistem", International Conference on Information Security and Cryptology, ISCTurkey 2015, 30-31 Ekim, Ankara, Türkiye.

Kaynaklar

[1] Y. Liu and G. Zhou. Key technologies and applications of internet of things. In *Intelligent Computation Technology and Automation (ICICTA), 2012 Fifth International Conference on*, pages 197–200. IEEE, 2012.

[2] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer networks*, 54(15): 2787–2805, 2010.

[3] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497–1516, 2012.

[4] J. Belissent. Getting clever about smart cities: New opportunities require new business models, 2010. URL `http://193.40.244.77/iot/wp-content/uploads/2014/02getting_clever_about_smart_cities_new_opportunities.pdf`.

[5] K. Ashton. That 'internet of things' thing, 2009. URL `http://www.rfidjournal.com/articles/pdf?4986`.

[6] International Telecommunication Union (ITU). The internet of things, 2005. URL `http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf`.

[7] Commission Of The European Communities. Internet of things - an action plan for europe, 2009. URL `http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0278&from=EN`.

[8] D. Evans. The internet of things how the next evolution of the internet is changing everything, 2011. URL `http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf`.

[9] A. Erdal. Nesnelerin interneti (iot) ve herşeyin interneti (ioe), 2014. URL `http://www.cisco.com/assets/global/TR/campaigns/ciscoconnect2014/pdf/NesnelerinInterneti.pdf`.

[10] G. M. Lee, N. Crespi, J. K. Choi, and M. Boussard. Internet of things. In *Evolution of Telecommunication Services*, pages 257–282. Springer, 2013.

[11] A. Gluhak, S. Krco, M. Nati, Dennis Pfisterer, N. Mitton, and T. Razafindralambo. A survey on facilities for experimental internet of things research. *Communications Magazine, IEEE*, 49(11): 58–67, 2011.

[12] R. Benabdessalem, M. Hamdi, and T. Kim. A survey on security models, techniques, and tools for the internet of things. In *Advanced Software Engineering and Its Applications (ASEA), 2014 7th International Conference on*, pages 44–48. IEEE, 2014.

[13] S. Karpischek, F. Michahelles, F. Resatsch, and E. Fleisch. Mobile sales assistant-an nfc-based product information system for retailers. In *Near Field Communication, 2009. NFC'09. First International Workshop on*, pages 20–23. IEEE, 2009.

[14] O. Vermesan and P. Friess. *Internet of things applications - from research and innovation to market deployment*, pages 45–50. River Publishers, 2014. ISBN 978-8793102941.

[15] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660, 2013.

[16] B. McBeath. How the internet-of-things is transforming mining, 2014. URL `http://www.clresearch.com/research/detail.cfm?guid=A5E6FEAF-3048-79ED-99C9-EA62EBCCD605`.

[17] J. Pescatore and G. Shpantzer. Securing the internet of things survey. *SANS Institute*, 2014.

[18] A. Atamli and A. Martin. Threat-based security analysis for the internet of things. In *Secure Internet of Things (SIoT), 2014 International Workshop on*, pages 35–43. IEEE, 2014.

[19] P. Paganini. China is planting spying microchips in electric iron and kettles that scan wi-fi devices to serve malware, 2013. URL `http://thehackernews.com/2013/11/russia-finds-spying-microchips-planted_1.html`.

[20] OWASP. OWASP internet of things top ten project, 2014. URL `https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project`.

[21] CVE-2013-6786, 2013. URL `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6786`.

[22] CVE-2014-100032, 2014. URL `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-100032`.

[23] H. Bojinov, E. Bursztein, E. Lovett, and D. Boneh. Embedded management interfaces: Emerging massive insecurity. *Black Hat USA*, 2009, 2009.

[24] S. Khandelwal. Refrigerators and other home appliances hacked to perform cyber attack, 2014. URL `http://thehackernews.com/2014/01/100000-refrigerators-and-other-home.html`.

[25] E. Kovacs. Misfortune cookie vulnerability exposes millions of routers, 2014. URL `http://www.securityweek.com/misfortune-cookie-vulnerability-exposes-millions-routers`.

[26] Ö. Erdem and U. Kaya. Saldırı tespit sistemleri (snort, suricata, bro), 2014. URL `https://www.bilgiguvenligi.gov.tr/saldiri-tespit-sistemleri/saldiri-tespit-sistemleri-snort-suricata-bro.html`.

[27] S. Raza, L. Wallgren, and T. Voigt. Svelte: Real-time intrusion detection in the internet of things. *Ad hoc networks*, 11(8):2661–2674, 2013.

[28] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito. Demo: An ids framework for internet of things empowered by 6LoWPAN. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 1337–1340. ACM, 2013.

[29] L. Spitzner. *Honeypots : tracking hackers*. Addison-Wesley, Boston, 2003. ISBN 0321108957.

[30] N. E. Siseci, B. Emre, and H. Tirli. Deliverable d5.3: Case study: Malicious activity in the turkish network, 2013. URL `http://www.syssec-project.eu/m/page-media/3/syssec-d5.3-TurkishNetworkCaseStudy.pdf`.

[31] I. Mokube and M. Adams. Honeypots: concepts, approaches, and challenges. In *Proceedings of the 45th annual southeast regional conference*, pages 321–326. ACM, 2007.

[32] J. Muniz and A. Lakhani. *Penetration testing with Raspberry Pi : construct a hacking arsenal for penetration testers or hacking enthusiasts using Kali Linux on a Raspberry Pi*, pages 110–117. Packt Publishing, Birmingham, UK, 2015. ISBN 978-1784396435.

[33] A. Mairh, D. Barik, K. Verma, and D. Jena. Honeypot in network security: a survey. In *Proceedings of the 2011 International Conference on Communication, Computing & Security*, pages 600–605. ACM, 2011.

[34] M. Marchese, R. Surlinelli, and S. Zappatore. Monitoring unauthorized internet accesses through a 'honeypot'system. *International Journal of Communication Systems*, 24(1):75–93, 2011.

[35] R. C. Joshi and A. Sardana. *Honeypot a new paradigm to information security*, pages 14–19. Science Publishers Distributed by CRC Press, Enfield, N.H. Boca Raton, FL, 2011. ISBN 978-1578087082.

[36] TR-069 (Technical Report 069). URL `https://en.wikipedia.org/wiki/TR-069`.

[37] W. Lee. More details about tr-069 cpe wan management protocol, 2005. URL `http://www.slideshare.net/wiliwe/more-detail-about-tr069-cpe-wan-management-protocol`.

[38] J. P. M. Rojas. Split management of tr069 enabled cpe devices. Master's thesis, Politecnico di Torino, Torino, Italy, 2011.

[39] The Broadband Forum. Tr-069 cpe wan management protocol, issue: 1 amendment 5, 2013. URL `https://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf`.

[40] J. Walls. Tr-069: A brief overview, 2014. URL `http://www.ieee1904.org/events/2014_06_workshop/s3_walls_tr069.pdf`.

[41] Axiros. Introducing tr-069 with axiros, 2015. URL `http://www.slideshare.net/axiros/axiros-tr069crashcoursepart1`.

[42] Tr-069 training series: Connection request basics, 2015. URL `http://www.qacafe.com/knowledgebase/tr-069-training-series-connection-request-basics/`.

[43] I. Savić, M. S. Savić, and G. Velikić. Implementation of tr-069 connection request mechanism. *X International Symposium on Industrial Electronics (INDEL)*, 2014.

[44] A brief survey of cwmp security, 2012. URL http://blog.3slabs.com/2012/12/a-brief-survey-of-cwmp-security.html.

[45] Allegro Software. Rompager basic web server, 2012. URL http://www.allegrosoft.com/wp-content/uploads/2012/01/RomPager_Datasheet.pdf.

[46] S. Tal and L. Oppenheim. The internet of tr-069 things: One exploit to rule them all, 2015. URL https://www.rsaconference.com/writable/presentations/file_upload/hta-r04-the-internet-of-tr-069-things-one-exploit-to-rule-them-all_final.pdf.

[47] Z. Durumeric, E. Wustrow, and J. A. Halderman. Zmap: Fast internet-wide scanning and its security applications. In *Usenix Security*, pages 605–620, 2013.

[48] Check Point Software Technologies. Misfortune cookie vulnerability, 2014. URL http://mis.fortunecook.ie/.

[49] Check Point Software Technologies. Protecting against misfortune cookie and tr-069 acs vulnerabilities, 2014. URL http://mis.fortunecook.ie/misfortune-cookie-tr069-protection-whitepaper.pdf.

[50] B. Prince. Widespread attack campaign highlights router security woes, 2014. URL http://www.securityweek.com/widespread-attack-campaign-highlights-router-security-woes.

[51] T. Hlaváček. Impact of "rom-0" vulnerability, 2014. URL https://ripe69.ripe.net/presentations/61-rom0-vuln.pdf.

[52] Allegro rompager http referer header uri redirection and cross site scripting vulnerabilities, 2013. URL http://www.securityfocus.com/bid/63721/discuss.

[53] D. Gentry and A. Pennarun. Catawampus tr-069 management for a cpe device in python. URL https://code.google.com/p/catawampus/.

[54] A. V. Blanco. Cve-2013-6786, 2013. URL http://osvdb.org/ref/99/rompager407.pdf.