
GAZİ ÜNİVERSİTESİ
Gazi
1926

MODBUS TEMELLİ SCADA SİSTEMLERİNİN SİBER GÜVENLİĞİ İÇİN YENİ BİR YAKLAŞIM

İsmail ERKEK

YÜKSEK LİSANS TEZİ
BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

OCAK 2018

İsmail ERKEK tarafından hazırlanan "MODBUS TEMELLİ SCADA SİSTEMLERİNİN SİBER GÜVENLİĞİ İÇİN YENİ BİR YAKLAŞIM" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Erdal IRMAK

Elektrik Elektronik Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ...……

Başkan: Prof. Dr. Refik SAMET

Bilgisayar Mühendisliği Anabilim Dalı, Ankara Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……...

Üye: Prof. Dr. Şeref SAĞIROĞLU

Bilgisayar Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……...

Tez Savunma Tarihi: 11/01/2018

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..……

Prof. Dr. Sena YAŞYERLİ

Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İsmail ERKEK

11/01/2018

MODBUS TEMELLİ SCADA SİSTEMLERİNİN SİBER GÜVENLİĞİ İÇİN YENİ BİR YAKLAŞIM

(Yüksek Lisans Tezi)

İsmail ERKEK

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Ocak 2018

ÖZET

Günümüzde enerji, su, ulaşım, sağlık, bankacılık, nükleer/kimyasal tesisler ve haberleşme altyapıları ulusal güvenlik boyutunda değerlendirilmekte olup literatür incelemelerinde kritik altyapılar olarak tanımlanmaktadır. Bahsedilen bu sistemlerin izlenmesi ve denetimi Endüstriyel Kontrol Sistemleri (EKS) veya Danışmalı Kontrol ve Veri Toplama Sistemleri (Supervisory Control And Data Acquisition, SCADA) ile sağlanmaktadır. Özellikle son yıllarda bilgi, iletişim ve internet teknolojisinin gelişmesine bağlı olarak EKS/SCADA sistemleri de bilişim teknolojileriyle bütünleşik çalışır hale gelmeye başlamıştır. Bu duruma paralel olarak bilgi ve iletişim teknolojisinde mevcut olan veya yeni ortaya çıkan güvenlik zafiyetleri SCADA sistemlerini de doğrudan etkileyebilmektedir. Bu nedenle sunulan tez çalışmasında, kritik altyapı olarak değerlendirilen SCADA sistemlerinin güvenliğine yönelik literatür araştırmasında bulunulmuş, SCADA sistemlerini oluşturan bileşenler ve haberleşme protokolleri incelenmiş ve bu bileşenlerin en bilinen zafiyetleri ele alınmış ve SCADA sistemlerine yönelik literatürde bilinen siber saldırılar analiz edilmiştir. Ayrıca EKS'de kullanılan endüstriyel haberleşme protokollerinin istatistikleri çıkarılarak bunlar içerisinde en sık kullanılan protokolün Modbus TCP olduğu tespit edilmiştir. Ayrıca, Modbus TCP protokolünde kaynak IP adresi kontrolünün yapılmadığı ve bunun da istimar edilebilecek bir güvenlik riski oluşturduğu ortaya çıkarılmıştır. Önerilen çalışmada, bu zafiyeti kullanan siber saldırıları başarıyla engelleyebilen yeni bir yöntem geliştirilmiş ve deney düzeneği ortamında doğrulanmıştır. Sonuç olarak, SCADA sistemlerini oluşturan bileşenlerin ve bu sistemlerin haberleşmesinde kullanılan endüstriyel protokollerin zafiyetleri ortaya konularak Modbus TCP protokolünün güvenliğinin iyileştirilmesi hedeflenmiştir. Tez çalışması sonucunda yapılan değerlendirme ve sunulan yeni güvenlik yaklaşımı ile kritik altyapıların güvenliğine katkılar sağlayacağı değerlendirilmektedir.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	Kritik altyapı, SCADA, endüstriyel kontrol sistemi, endüstriyel haberleşme protokolleri, Modbus, siber güvenlik
Sayfa Adedi	:	116
Danışman	:	Doç. Dr. Erdal IRMAK

A NOVEL APPROACH FOR CYBER SECURITY OF MODBUS BASED SCADA SYSTEMS

(M. Sc. Thesis)

İsmail ERKEK

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

January 2018

ABSTRACT

Nowadays, energy, water, transportation, health, banking, nuclear / chemical facilities and communication infrastructures are evaluated in terms of national security dimension and defined as critical infrastructures in literature reviews. Monitoring and controlling of these systems are provided by Industrial Control Systems (ICSs) or Supervisory Control And Data Acquisition (SCADA) systems. Especially, depending on the development of information, communication and internet technology in recent years, ICS/SCADA systems have started to become integrated with these systems. In parallel with this situation, current or existing vulnerabilities in information and communication technology can also affect SCADA systems directly. Within the scope of the study, a literature review for the security of SCADA systems has been made, components and communication protocols of SCADA systems have been examined, the most common vulnerabilities of these components have been discussed in detail and known cyber attacks against SCADA systems in literture have been analyzed. In addition, statistics of the most frequently used industrial communication protocols in ICS have been specified and it has been determined that protocol is the Modbus TCP. Furthermore, it is shown that the source IP address control is not provided in Modbus TCP protocol and this is a crutial security risk that can be easily exploited. In the proposed study, a novel method is developed that is able to block the cyber attacks using this vulnerability. The method proposed is also verified in simulation environment. In conclusion, it is aimed to improve the cyber security of Modbus TCP after examining the vulnerabilities of the SCADA components as well as the industrial protocols using for communicating them. It is evaluated that the findings of this thesis and the proposed new security approach contribute to the cyber security of critical infrastructures.

Science Code	:	92403
Key Words	:	Critical infrastructure, SCADA, industrial control system, industrial communication protocols, Modbus, cyber security
Page Number	:	116
Supervisor	:	Assoc. Prof. Dr. Erdal IRMAK

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren tez danışmanım Sayın Doç. Dr. Erdal IRMAK hocama teşekkürü bir borç bilirim. Bu süreçte destek ve katkılarını hiçbir zaman esirgemeyen Sayın Prof. Dr. Şeref SAĞIROĞLU hocama da şükranlarımı sunarım. Yüksek Lisans eğitimim süresince manevi desteğini esirgemeyen ve kendilerine yeterince vakit ayıramadığım aileme ve kurucusu olduğum Blackbox Siber Mücadele Takımı'nın tüm değerli üyelerine anlayışları için teşekkür ederim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AGA	Amerika Gaz Birliği
API	Amerikan Petrol Enstitüsü
ARP	Adres Çözümleme Protokolü
CIP	Kritik Altyapı Koruma
CPNI	Ulusal Altyapıları Koruma Merkezi
DDOS	Dağıtık Hizmet Engelleme
DHS	Ulusal Güvenlik Dairesi
DNP3	Dağıtık Ağ Protokolü 3
DOS	Hizmetin Engellemesi
EKS	Endüstriyel Kontrol Sistemi
GRI	Gaz Araştırmaları Enstitüsü
HMI	İnsan-Makina Arayüzü
IED	Akıllı Elektronik Cihaz
IGT	Gaz Teknolojileri Enstitüsü
ISO	Uluslar Arası Standartlar Teşkilatı
MITM	Araya Girme Saldırısı
MTU	Merkezi Terminal Birimi
NERC	Kuzey Amerika Elektrik Emniyeti Kuruluşu
NIST	Amerika Ulusal Standartlar ve Teknoloji Enstitüsü
NSTB	Ulusal SCADA Deney Düzeneği
OSI	Açık Sistem Ara Bağlantısı
PLC	Programlanabilir Mantıksal Denetleyici

Kısaltmalar	Açıklamalar
RINSE	Gerçek Zaman Kapsamlı Ağ Simülasyon Ortamı
RTU	Uzak Terminal Birimi
SCADA	Danışmalı Kontrol ve Veri Toplama Sistemi
SQL	Yapılandırılmış Sorgu Dili
STS	Saldırı Tespit Sistemi
TBMM	Türkiye Büyük Millet Meclisi
TCAA	Tehama Colusa Kanal Otoritesi
VCSE	Sanal Denetim Sistem Ortamı
VPST	Sanal Güç Sistemi Deney Düzeneğidir
XSS	Siteler Arası Betik Çalıştırma

1. GİRİŞ

Tarih boyunca toplumların sosyal ve ekonomik gelişim süreci incelendiğinde insanlığın 3 ana evreden geçtiği gözlemlenmektedir. Birincisi; insanların toprağa ve yerleşik düzene geçtiği tarım toplumudur. İkincisi, 18. yüzyılın sonlarına doğru kitlesel üretim, tüketim ve eğitimin önemli olduğu sanayi toplumu ve üçüncüsü ise günümüzde yaşadığımız bilgi teknolojilerinin üretiminin ve kullanımının giderek arttığı, bilginin anında erişilip, iletilip, üretilebildiği ve eğitim, haberleşme, sağlık ve enerji gibi neredeyse her alanda kullanılabildiği bilgi toplumudur.

Günümüzde bilgi teknolojilerinin gelişmesiyle birlikte bilgi, üretimin tek faktörü haline gelmektedir. Bilgi ve iletişim teknolojilerinin kullanımıyla üretilen teknoloji ve pazardaki istatistikleri incelendiğinde 2016 yılı itibariyle dünya piyasasının %97'sinden fazlasını oluşturmaktadır [1]. Bu yüzden içinde bulunduğumuz bilgi çağında ülkelerin güçlü kalabilmek için bilgi üretmesi gerekmekte ve ürettiği bilginin güvenliğini sağlaması gerekmektedir. Toplumlar, bulundukları ülkelerin ekonomik, sosyo-kültürel ve teknolojik birikimlerini göz önünde bulundurarak kendi bilgi politikaları çerçevesinde kendilerine özgü bilgi sistemleri üretmektedir.

Bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişmeler gerek insanların hayatını gerekse özel ve kamu sektöründe sunulan hizmetleri kolaylaştırmakta ve hizmet kalitesini ve sunum şeklini dijital ortamdan sağlayarak çok üst seviyelere çıkarmaktadır. Özellikle ülkemizde 1998 yılından itibaren kamu sektöründe bilgi ve iletişim teknolojilerinin kullanılması amacıyla TBMM'de Bilgi ve Bilgi Teknolojileri Grubunun oluşturulması [2] ve AB uyum paketleriyle AB'ye aday ülkeler için hazırlanan eAvrupa+ girişimine taraf olmasıyla ülkemizde 2000'li yılların başlarında bilgi toplumuna geçiş süreci hız kazanmıştır [3].

Bilgi teknolojilerindeki son 20 yılda gerçekleşen köklü değişiklik ve yenilikler; bireylerin, toplumların, kurum ve kuruluşların ve devletlerin yaşamı ve idaresini kolaylaştırmasından ötürü sosyal, sağlık, ekonomi, enerji, idari, haberleşme, eğitim, finans ve sanayi gibi her sektör ve alanda kullanımı yaygınlaşmış ve bilgi sistemlerinin temel alındığı bir altyapı oluşturmuştur. İnsan hayatının her noktasına değinen bu alanların her birinin işleyişinde veya oluşacak bir arıza durumunda, toplum düzeni ve ulusal güvenlik etkilenebilmektedir.

Kısacası toplumlar ve devletler bilgi ve iletişim teknolojilerine bağımlı hale gelmekte ve siber bağımlılık kavramını ortaya çıkarmaktadır.

Siber bağımlılığın giderek arttığı günümüzde internet teknolojisinin gelişimi ülkeler arasındaki sınırları ortadan kaldırmış, küresel bir bilgi ağı haline gelerek küreselleşme kavramının artmasında da önemli bir rol üstlenmiştir. Özellikle son yıllarda oldukça gelişme kaydeden nesnelerin interneti, büyük veri, bulut bilişim gibi teknolojilerin internet teknolojisiyle entegre çalışarak kullanımının artması toplum hayatını ve yaşam tarzını tahmin edilmesi güç boyutlara götüreceğini düşündürmektedir.

Bahsedildiği gibi bilgi teknolojileri kullanımı hız, kolaylık, şeffaflık ve maliyet etkinlik gibi nedenlerle toplum hayatını kolaylaştırmaktadır. Ancak kullanılan bu teknolojinin sunduğu bu avantajların yanında getirdiği bir takım riskler ve dezavantajlar da mevcuttur. Zafiyet ve riskleri de beraberinde getiren bu sistemlerin güvenliği toplumların refahı ve kamusal düzenin sağlanması açısından önemlidir.

Bilgi ve iletişim teknolojilerinin hemen her alanda kullanılması ülkelerin kritik altyapılarının fonksiyon ve işleyişini de etkilemekte ve köklü değişimler meydana getirmektedir. Özellikle zarar görmesi veya etkilenmesi durumunda toplum hayatını ve ulusal güvenliği sekteye uğratacak veya zarar görmesine sebep olacak bilgi sistemleri veya altyapılar kritik altyapılar olarak tanımlanmaktadır [4]. Bu bakımdan her ülke kendi kritik bilgi sistemleri ve altyapılarını dışarıdan veya içeriden gelebilecek tehditlere yönelik kendi teknolojik birikimleri ve kapasitelerini göz önünde bulundurarak güvenlik önlemleri ve bilgi güvenliği politikaları geliştirmektedirler.

“Kritik Altyapı” son yıllarda hemen hemen dünyanın her yerinde oldukça tartışılan ve henüz ülkeler arasında ortak bir tanımı yapılmayan kavramdır. Fakat, ABD ve AB ülkeleri başta olmak üzere enerji, su, ulaşım, sağlık, bankacılık, nükleer/kimyasal tesisler ve haberleşme altyapılarını kritik sektörler olarak belirlemiş ve bu sektörlere ait altyapıları kritik altyapılar olarak nitelendirmişlerdir. AB komisyonunun 2004 tarihli “Terörizmle Mücadele Kapsamında Kritik Altyapıların Korunması” başlıklı tebliğinde [5] ve ABD mevzuatında kritik altyapı tanımları yapılmış ve “insanların hayati sosyal fonksiyonlarının, sağlıklarının, emniyetlerinin, güvenliklerinin, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve aksama veya yok edilmesi bu fonksiyonları sürdürmede yetersiz kalma sonucunda

bir üye ülkede belirgin etki gösterecek varlık, sistem veya ilgili parçaları" olarak tanımlamışlardır.

Günümüzde elektrik, doğalgaz, su, kanalizasyon, ulaşım, ilaç ve kimya sanayisi, kağıt hamuru ve kağıt sanayisi, yiyecek içecek sektörü ve parçalı üretim sanayisinde kontrolü ve izlenmesi denetim sistemleri ile sağlanmaktadır. Bu sistemlere yönelik gerçekleştirilen fiziksel ve siber saldırılarla yetkisiz erişim elde edilebilmekte ve farklı müdahalelerle bu sistemlerin işleyişi ve fonksiyonu değiştirilebilmekte ve bozulabilmektedir.

Literatürde SCADA sistemleri olarak adlandırılan denetim sistemleri ilk tasarlandığı dönemlerde internet teknolojisi, kablolu ve kablosuz erişim teknolojileri günümüz teknolojisi ile kıyaslanamayacak düzeydeydi [6]. SCADA sistemleri diğer bilgi teknolojileri altyapılarından izole olarak tasarlanmaktaydı [7]. Ayrıca sistemlerin üzerinde çalışan işletim sistemlerinin ve uygulamaların güvenlik açıkları da izole sistemler olma düşüncesiyle dikkate alınmamakta ve göz önünde bulunmamaktaydı. Fakat günümüzde internet teknolojisinin gelişmesiyle birlikte SCADA sistemlerini yöneten operatörler bu sistemleri internet teknolojisini kullanarak izlemekte ve kontrol etmektedir. Ayrıca SCADA sistemi bileşenleri kendi aralarında haberleşmek için yine internet teknolojisini kullanmaktadır. İnternet teknolojisinde ortaya çıkan güvenlik zafiyetleri bu teknoloji altyapısını kullanan SCADA sistemlerini de direk veya dolaylı olarak etkilemekte ve risk altında olmasına sebep olabilmektedir.

Ülkemizde SCADA sistemleriyle izlenen ve kontrol edilen kritik altyapıların güvenliğine yönelik ilk hazırlanan strateji ve eylem planı olarak Ulaştırma Denizcilik ve Haberleşme Bakanlığınca Bilgi Güvenliği Derneğinin katkılarıyla 11.06.2012 tarihinde "2013 – 2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" [8] hazırlanmış ve yürürlüğe girmiştir. Ayrıca son olarak "2016-2019 Ulusal Siber Güvenlik Stratejisi" hazırlanmış ve yürülüğer girmiştir [9]. Bu stratejiler, kritik altyapılara ait bilişim sistemlerini de kapsamaktadır. Öncelikli olarak kritik altyapılara ait bilişim sistemleri olmak üzere kurumsal siber güvenliğin sağlanması için çalışmalar yapılacağı kararı alınmış, kritik altyapılara ait bilişim sistemleri, kritiklik seviyeleri, birbiriyle olan ilişkileri ve sorumlularının belirlenmesi kararı alınmıştır.

Dünya'da kritik altyapıların güvenliği ile ilgili ulusal ve uluslararası birçok kurum ve kuruluş politika, strateji, eylem planı veya rapor hazırlamışlardır. Özellikle uluslararası geçerliliği olan bazı kuruluşların yayınladığı politika ve stratejiler, kritik altyapıların korunması hakkında önemli derecede yol gösterici bir rehber oluşturmaktadır. Amerikan Gaz Birliği (AGA), SCADA sistemlerinin iletişim güvenliğini siber saldırılara karşı korumak için geliştirilen AGA 12, çeşitli sayıdaki gaz ile ilgili kuruluşların çabaları sonucu geliştirilmiştir. Bunlar: Gaz Teknolojileri Enstitüsü (IGT), Gaz Araştırmaları Enstitüsü (GRI), Gaz Teknoloji Enstitüsü (GTI) ve Amerikan Gaz Birliğidir (AGA). AGA 12 kontrol merkezindeki saha cihazları ile kontrol sunucuları arasındaki iletişim bağlantısının güvenliğine odaklanmaktadır. Önerilen uygulamalar gizli ve özgün SCADA iletişimi sağlamak için tasarlanmıştır. AGA 12 gönüllülük esasına göre hazırlanmış bir standarttır ve hiçbir şekilde standartta önerildiği gibi şifreleme teknolojisini yüklemeyi zorunlu kılmamıştır. AGA 12 dört temel başlık altında toplanmıştır. Bu başlıklar: (i) Arka plan, politikalar ve test planı, (ii) Asenkron seri iletişim için güçlendirilmiş bağlantı şifrelemesi, (iii) Ağ sistemlerinin korunması ve (iv) Gömülü SCADA bileşenlerinin korunması [10]. AGA 12 Standardı; siber güvenlik, sosyal mühendislik, fiziksel güvenlik ve gelişmekte olan güvenlik politikaları ve prosedürleri için en iyi uygulamaları sağlar.

Ulusal Altyapıları Koruma Merkezi (CPNI) İngiltere Devleti tarafından 2007 yılında İngiltere'nin kritik altyapılarının belirlenmesi ve korunması için kurulmuş bir servistir. Gizlilik esaslı bir kurum olduğu için literatürde çok fazla bilgi bulunmamaktadır. İngiltere'nin kritik altyapıları olarak; iletişim, acil servis, enerji, yiyecek, kamu hizmetleri, sağlık, ulaşım ve su belirlenmiştir. "Siber Güvenlik ve Birleşik Krallığın Kritik Ulusal Altyapıları" başlıklı çalışmada kritik altyapıların güvenliği sağlanmaya çalışılmıştır [11].

Amerika Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından hazırlanan NIST 800-82 nolu "Endüstriyel Kontrol Sistemleri Güvenliği Rehberi" başlıklı çalışmasının amacı, SCADA sistemlerinin, endüstriyel kontrol sistemlerinin ve kontrol fonksiyonu sağlayan diğer sistemlerin güvenliğini sağlamaya yönelik bir kılavuz teşkil etmektir [12]. NIST 800-82, doğrudan bir güvenlik kontrol listesi sunmamakla birlikte, risk değerlendirmesi çalışmaları için yararlanılacak güvenlik gereksinimleri ve çözümleri sunmaktadır. Endüstriyel kontrol sistemleri altyapısında kullanılan donanımsal veya yazılımsal bileşenleri incelemekte ve daha güvenli ağ-uygulama servisleri için öneride bulunmakta ve örnekler

sunmaktadır. Bu nedenle, pratik inceleme ve düzeltmeler için başvurulabilecek kaynaklar arasında yer almaktadır [13].

Kuzey Amerika Elektrik Emniyeti Kuruluşu (NERC), ilk olarak 2003 yılında Acil Aksiyon Standardı olan "1200 Siber Güvenlik" belgesini yayınlamış ve bunu takiben NERC 1300 çalışmasını başlatmıştır. Bu çalışmaların ardından 2006 ve sonrasında NERC, daha kapsamlı olan ve alt başlıklardan oluşan Kritik Altyapı Koruma CIP:002-1 ile CIP 009-2 arasındaki çalışmalarını yayınlamıştır. NERC 1200, iletim ve dağıtım birimlerini kapsayan bir çalışmayken, CIP 002-1 ile CIP 009-2 serisindeki çalışmalar üretim tesislerini de içerecek şekilde genişletilmiştir [14]. "Elektrik sektörü için NERC güvenlik rehberi" Kuzey Amerika Emniyeti kuruluşu tarafından yayımlanan 73 sayfalık bir belgedir. Rehber, fiziksel ve siber güvenliği de kapsayan 14 bölümden oluşmaktadır. Bu bölümlerde elektrik altyapı sistemlerinin korunmasında uygulanacak genel yaklaşımları, düşünceleri, uygulamaları ve planlama felsefeleri açıklanmıştır. Bu kurallar tavsiye niteliğindedir ve her kullanıcı için nasıl kullanılacağı belirtilmiştir.

API 1164 SCADA güvenliği standardı ilk olarak Eylül 2014'te yayımlanmıştır. SCADA güvenliğine yönelik bu standart SCADA sisteminin bütünlüğünü ve güvenliğini yönetmek için petrol ve doğalgaz işletmecilerine rehberlik etmektedir. API 1164 güvenlik standardı erişim kontrolünü, haberleşme güvenliğini (şifreleme dahil), bilgi dağıtım sınıflandırmasını, fiziksel sorunları (felaket kurtarma ve iş sürekliliği dahil), işletim sistemlerini, işletme ve müşteri arasındaki veri değişimini, yönetim sistemlerini, saha cihazlarının yapılandırılmasını ve yerel erişimi ele almaktadır [15].

ISO/IEC 27002 standardı bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlayan kurumların kullanımı için, bilgi güvenliği yönetimi ile ilgili tavsiyeleri kapsar. ISO/IEC 27002 Bilgi Güvenliği Yönetimi için uygulama kodu, kuruluşların bilgi güvenliği yönetim sistemini kurmaları, uygulamaları, sürdürmeleri ve iyileştirmeleri için hazırlanmış bir kılavuz olup önceki sürümünden farklı olarak, yaşanan problemlerden, arızalardan, kazalardan ders çıkarılması ve tekrar yaşanmaması için gerekli önlemlerin alınması için gerekli olan yönetim mekanizmasının kurulmasını sağlayan Bilgi Güvenliği İhlallerinin yönetimi ile ilgili bilgi güvenliği denetimlerini ve ilgili uygulamaları da içermektedir [16].

11 Eylül 2002 yılından sonra kurulan Ulusal Güvenlik Dairesi (DHS – Department of Homeland Security) tarafından hazırlanan "Denetim Sistemleri Güvenlik Kataloğu: Standart Geliştiriciler için Öneriler" başlıklı çalışma, sağlam güvenlik standartları, rehberleri ve en iyi uygulamaları geliştirmek için çeşitli sanayi sektörlerine gerekli çerçeveyi sağlamak için tasarlanmıştır. Birçok kaynak için önerilen kontrollerin bir listesini içerir. 18 ayrı bölüme ayrılan belgede amaç, sınırlı kaynaklarla çalışırken güvenliği dengeleyebilmeye imkanı sağlamaktır. Doküman güvenlik politikası, konfigürasyon yönetimi, güvenlik farkındalığı, eğitim ve erişim kontrolü konularına değinmiştir [17].

Amerika Enerji Bakanlığının SCADA sistemlerinin güvenliğini 21 adımda kısa ama bilgilendirici bir şekilde anlattığı "SCADA Ağlarının Siber Güvenliğini Arttırmak için 21 Adım" başlıklı çalışmasının konularından bazıları; (i) SCADA bağlantılarının tüm bağlantılarını tanımlama, (ii) Sistemi korumak için üreticiye özgü protokol güvensizliği, (iii) Savunma derinliği ilkesine dayalı bir ağ koruma stratejisinin oluşturulması, (iv) Sistem yedekleme ve felaket kurtarma planlarının oluşturulması olarak sıralanmıştır [18].

Amerika Kongresi için çalışan bağımsız ve tarafsız bir kurum olan Kamu Sorumluluk Ofisi "Kritik Altyapıların Korunması için Siber Güvenlik" başlıklı çalışması; (i) Kritik altyapı koruma sektörlerinin her birinde siber güvenlik gereksinimleri, (ii) Hangi siber güvenlik teknolojisinin kritik altyapı korumasına uygulanabileceği, mevcut siber güvenlik araştırmaları, (iii) Gizlilik ve bilgi paylaşımı gibi politika konuları da dahil kritik altyapıları korumak için kullanılan siber güvenlik teknolojileriyle alakalı uygulama sorunlarını belirlemek gibi konulara odaklanmaktadır [19].

Yukarıda da anlatıldığı gibi SCADA sistemlerinin bilgi ve iletişim teknolojileri ile bütünleşik çalışması sonucu, bu teknolojilerde yaşanan gelişmeler ve ortaya çıkan zafiyetler direk olarak SCADA sistemlerini de etkilemektedir. Bu gelişmelere paralel olarak ABD ve AB ülkeleri başta olmak üzere dünya genelinde bu sistemlerin güvenliğine yönelik stratejiler ve politikalar geliştirilmektedir. Ülkemizde de uluslararası çalışmalar kapsamında kendi kritik bilgi sistemlerinin korunmasına yönelik çalışmalar yapılmaktadır. Bu çalışma kapsamında da EKS'lerin haberleşme protokollerinin en sık zafiyet barındıran bileşen olduğu belirlenmiş ve internete açık SCADA haberleşme protokollerinin kullanım istatistikleri çıkarılmıştır. Yapılan tarama sonucu dünya genelinde %50 oranda en fazla kullanılan Modbus TCP protokolünün güvenliğine yönelik bir çözüm önerisi geliştirilmiştir.

Çalışmanın ikinci bölümünde SCADA sistemleri özelinde EKS'lerin siber güvenliğine yönelik literatürdeki mevcut yöntem ve yaklaşımlar detaylı bir şekilde incelenmiştir. Yapılan bu inceleme, SCADA sistemlerinin güvenliğine yönelik deney düzeneği ortamları, saldırı vektörleri, savunma yöntemleri ve risk değerlendirmeleri kapsamında yapılmıştır.

Çalışmanın üçüncü bölümünde kritik altyapı olarak değerlendirilen SCADA sistemlerinin çalışma mantığı, bileşenleri ve fonksiyonları genel olarak incelenmiştir. Ayrıca Shodan arama motoru kullanılarak EKS'lerde en sık kullanılan haberleşme protokollerinin istatistikleri çıkarılmış ve ülkeler bazında kullanım oranları belirlenmiştir. Mobdus protokolü temel alınarak EKS haberleşme protokollerinin yapısı ve detaylı incelemesi yapılmıştır.

Çalışmanın dördüncü bölümünde SCADA sistemlerinin siber güvenlikle ilişkisi incelenmiş olup SCADA sistemlerinde en sık karşılaşılan zafiyetler ve bu sistemlere gerçekleştirilen siber saldırılar analiz edilmiştir. Bunlara ek olarak, EKS'lerde en sık kullanılan haberleşme protokolü olduğu daha önce belirlenmiş olan Modbus protokolü baz alınarak SCADA sistemlerinin haberleşme protokollerinin zafiyetleri ve bu sistemlere yönelik gerçekleştirilebilecek siber saldırılar detaylı olarak incelenmiştir. Ayrıca literatürde yer alan EKS'lere gerçekleştirilmiş siber saldırılar araştırılmıştır. Bu bölümün son kısmında, SCADA sistemlerinin güvenlik testlerinde kullanılan araçlar incelenmiş ve Gazi Üniversitesi Akıllı Şebekeler Laboratuvarı'nda yer alan test düzeneği ortamında kullanılarak sonuçları analiz edilmiştir.

Son olarak çalışmanın beşinci bölümünde yerel bir ağda Modbus Poll simülasyon ortamı kullanılarak Modbus TCP protokolü Wireshark aracı kullanılarak incelenmiş ve veri transferi sırasında bu protokolün kaynak IP adresi kontrolünü yapmadığı ve herhangi bir şifreleme kullanmadığı tespit edilmiştir. Tespit edilen zafiyetin istismarı gerçekleştirilerek yapılan saldırı paketleri analiz edilmiş ve bu saldırıları engellemeye yönelik çözüm olarak bir güvenlik mimarisi önerilmiş ve bu mimari içerisinde yer alan kontrol ara katmanı olarak tasarlanan, Modbus TCP paketlerinin kontrolünün sağlandığı ve üzerinde Python kodu çalışan bir Modbus Sandbox geliştirilmiştir. Böylece işletme içerisinde çalışan veya bir saldırgan tarafından sahada bulunan cihazların yazmaçlarına belirlenen eşik değerlerin üzerinde bir değer girildiğinde bunun kontrolünün sağlanarak en fazla eşik değerin yazılması hedeflenmiştir.

Bu çalışma kapsamında, EKS'lerde en sık kullanıldığı tespit edilen Modbus TCP protokolünün kaynak IP adresi kontrolü zafiyetini istismar edilmesi ile gerçekleştirilen siber saldırıların engellenebileceği ve sahada bulunan cihazların yazmaçlarına yetkisiz bir şekilde değer girilemeyeceği gösterilmiştir. Ayrıca, bu çalışmanın ülkemizde kritik altyapıların güvenliğine yönelik yapılan çalışmalara katkılar sağlayacağı değerlendirilmektedir.

2. LİTERATÜR TARAMASI

Yapılan literatür araştırmasında kritik altyapıların fiziksel ve siber güvenliğine yönelik geliştirilen test ortamlarında bu sistemlere yönelik gerçekleştirilen siber saldırılar ve farklı güvenlik çözüm önerileri yer almaktadır. Sayegh ve diğerleri dahili bir ağda tasarlanan deney düzeneğinde kullanılan SCADA haberleşme protokollerine yönelik gerçekleştirdikleri siber saldırılarla, alınan güvenlik önlemlerinin çok kolay bir şekilde atlatılabildiğini göstermiştir. Deney düzeneklerinde hizmet engelleme (DoS), replay (yeniden yönlendirme) ve şifreleme saldırılarını gerçekleştirerek SCADA bileşenlerinin ve protokollerinin zafiyetlerini göstermişlerdir [20]. Koutsandria ve diğerleri gerçek bir ağ trafiği kullanarak oluşturdukları siber-fiziksel PLC simülasyon ortamında gerçekleştirilen siber saldırılara karşı saldırı tespit sistemlerinin (STS) güvenlik kurallarını kullanmıştır. Tasarlanan simülasyon ortamı Matlab/Simulink ortamı kullanılarak şebeke üzerindeki alt sistemlerin simülasyon ortamı hazırlanmıştır. Gerçekleştirilen saldırılar sonucunda STS üzerindeki trafik analiz edilmiştir [21].

SCADA sistemlerinin güvenliği için hazırlanan diğer çalışmalarda, Morris ve diğerleri Mississippi State Üniversitesi SCADA Güvenliği Laboratuvarı'nda farklı kritik altyapı denetim sistemlerini içeren deney düzeneği ortamı hazırlamıştır. Bu ortamda endüstriyel kontrol sistemlerine yönelik siber güvenlik çalışmaları, farklı mühendislik ve bilgisayar bilimleri dersleri verilmektedir. Deney düzeneği ortamında keşfedilen siber güvenlik zafiyetlerini istismar etmeye yönelik çalışmalar yürütülmekte olup bu saldırılar sonucunda oluşan etkiler risk analizi başlığı altında incelenmiştir [22]. Adam Hahn'ın yaptığı çalışmada tasarlanan deney düzeneği ortamı, endüstriyel denetim sistemlerinin simülasyon ve emülasyon teknikleriyle katmanlı denetim, haberleşme ve güç sisteminin katmanlı yaklaşımı uygulanmıştır. Aynı zamanda çalışmada elektrik şebeke sistemlerine yönelik gerçekleşen siber saldırıları tespit etmek için kullanılan STS ile farklı siber saldırılar bu ortamda analiz edilmiştir [23]. Hahn ve diğerleri kritik altyapı olarak değerlendirilen akıllı şebekelerin siber güvenliğini sağlamaya yönelik yaptıkları diğer çalışmada, içerisinde denetim grubunun ve siber-fiziksel ortamının sağlanması için gerekli haberleşme ve fiziksel sistem bileşenlerinin olduğu deney düzeneği ortamı hazırlamışlardır [24]. Hazırlanan deney düzeneğinde dahili ve dış ağdan olmak üzere iki farklı DoS ve zararlı kesici saldırıları gerçekleştirilerek sonuçları tartışılmıştır.

Ortak bir ulusal laboratuvar ortamı sunmak için oluşturulan Ulusal SCADA Deney Düzeneği (NSTB – National SCADA TestBed), içerisinde şebeke üretim ve dağıtım bileşenlerini içeren geniş çaplı bir projedir. Bu çalışma sonucunda kritik altyapılara ait çok ciddi siber zafiyetler tespit edilmiş ve SCADA sistemlerine yönelik güvenlik değerlendirme yöntemleri üretilmiştir. Fiziksel olarak deney düzeneğinin oluşturulması ekonomik açıdan maliyetli olacağından pratikte oluşturulması ciddi gayret gerektirmektedir [25]. Sandia Ulusal Laboratuvarı, daha uygun maliyetli ve yeniden yapılandırılabilen bir platform sunmak amacıyla simülasyon, emülasyon ve fiziksel sistemlerle entegre çalışmasına imkan sağlayan Sanal Denetim Sistem Ortamı'nı (VCSE – Virtual Control System Environment) hazırlamışlardır. VCSE, simüle edilmiş ağ ile fiziksel ağ cihazlarının bütünleşik çalışmasını sağlamak amacıyla OPNET döngü sisteminden faydalanmıştır. Bu durum fiziksel ve emüle edilmiş PLC cihazları ve PowerWorld güç sistemi simülatörü arasındaki haberleşmeye imkan sağlamıştır. VCSE aynı zamanda birçok bileşen üzerinde kontrol sağlamak için merkezi simülasyon yönetim aracı olan Umbra'yı kullanmıştır. VCSE işletme eğitimi, zafiyet tanımı, saldırıları indirgeme ve hesaplama aktivitelerine destek sağlamak amacıyla tasarlanmıştır [26]. Simülasyon ve fiziksel elementleri birleştiren bir diğer benzer proje de Illinois Üniversitesi tarafından tasarlanan Sanal Güç Sistemi Deney Düzeneğidir (VPST – Virtual Power System Testbed). Illinois Üniversitesi Gerçek Zaman Kapsamlı Ağ Simülasyon Ortamı (RINSE – Real-Time Immersive Network Simulation Environment) projesiyle bütünleşik çalışacak PowerWorld güç sistemi simülasyon aracı kullanılması açısından VCSE ile benzerdir [27].

Avrupa CRUTIAL projesi kapsamında farklı siber saldırı senaryolarının etkilerini gözlemlemek amacıyla 2 adet deney düzeneği geliştirilmiştir. İlk deney düzeneğinde öncelikli olarak denetim merkezi ve simüle edilmiş alt sistemler arasındaki haberleşme altyapısına dikkat edilmiştir. Bu sistemlerin haberleşme altyapısına yönelik belirli DoS saldırıları analiz edilmiştir. Diğer test düzeneğinde emüle edilmiş Akıllı Elektronik Cihazlar (IED – Intelligent Electronic Device) tarafından kontrol edilen fiziksel mikro şebeke altyapısı temel alınmıştır. Buradaki IED'ler yerel ağ üzerinden Matlab/Simulink kullanılarak haberleşmektedir. Bu ortam Dağıtık Enerji Kaynağı (DER – Distributed Energy Resource) uygulamalarında potansiyel güvenlik açıklarının tespitinde kullanılmıştır [28,29]. Anomali tabanlı STS araştırmaları için SCADA Denetim Sistemlerinin Güvenlik Analizi için Deney Düzeneği (TASSCS - The Testbed for Analyzing Security of SCADA Control Systems) Arizona Üniversitesi'nde geliştirilmiştir. Sandia'daki VCSE projesine benzer OPNET

döngü sistemi emülasyonu ve simüle elektrik şebekesi sağlamak amacıyla PowerWorld yazılımını kullanmıştır. Simülasyon tabanlı kontrol çözümleri PowerWorld simülatörüyle haberleşen ModbusRSim yazılımı kullanılarak sunulmuştur [30].

Dublin Üniversitesi'nde hem saldırıları tespit etmek ve fiziksel etkilerini hesaplamak için DIgSILENT güç sistemi simülatörü kullanılarak bir deney düzeneği hazırlanılmıştır [31]. SCADASim deney düzeneği Royal Melbourne Teknoloji Enstitüsü tarafından siber saldırı altındaki ağ performansını analiz etmek için tasarlanmıştır. SCADASim deney düzeneği sık kullanılan SCADA haberleşme protokollerinden faydalanarak enterkonnekte fiziksel cihazların kullanıldığı emüle edilmiş haberleşme altyapısına odaklanılmıştır [32]. Bu deney düzeneğiyle siber saldırıların sistem haberleşme altyapısı gereksinimlerini analiz etmek için kullanılabilir.

SCADA haberleşme protokollerinden en yaygın olarak kullanılan Modbus protokolünün test edilmesi ve simüle edilmesi amacıyla uygun bir yazılım platformu olan Modbus Poll SCADA sistemlerinin siber güvenlik çalışmalarında kullanılmıştır. Yanfei ve diğerleri Modbus tabanlı ZigBee kablosuz sensör teknolojisi geliştirirken yazılım test aracı olarak Modbus Poll kullanmışlardır [33,34]. Beresford yaptığı çalışmada [35], Siemens PLC'lerin haberleşmesi için kullanılan ISO-TSAP ve Profinet protokollerinin şifreleme kullanmamasını istismar ederek parola özetlerini ve TCP dökümünden önemli bilgileri ele geçirebilmektedir. Böylece bu bilgilerle replay ve MITM saldırıları gerçekleştirebilmektedir. Bu saldırılarla PLC yeniden programlanabilir, CPU açılıp kapatılabilir, kimlik doğrulama işlemi atlatılabilir, kimlik doğrulama parolaları değiştirilebilir veya tamamen silinebilir ve hafıza üzerinde okuma yazma işlemi gerçekleştirilebilir. Sağıroğlu ve diğerlerinin yaptığı çalışmada [36], enerji otomasyon sistemlerinin haberleşmesinde kullanılan Modbus protokolünün güvenlik açıklıkları incelenmiş, tespit edilen güvenlik açığını gidermek ve sistemi güvenli hale getirmek için açık kaynak kodlu güvenlik duvarı kullanılmıştır.

Kritik altyapı olarak değerlendirilen SCADA sistemlerine yönelik DDoS (Hizmet Engelleme) saldırıları da gerçekleştirilebilmektedir. Bu saldırı çeşidine yönelik yapılan literatür araştırmasında, Chabukswar oluşturduğu kimya tesisi simülasyon ortamında [37], DDoS saldırısı gerçekleştirmiş ve hedef sistem yoğun şekilde istek paketleriyle meşgul edilmiş ve sistem normal trafiğini taşıyamaz hale gelmiş veya akan trafik çok yavaşlamıştır.

Steve Mansfield-Devine çalışmasında [38] belirttiği üzere eskiden sadece hactivizm ve politik amaçlı kullanılan DDoS saldırıları artık daha sistemli ve karmaşık yapıda yapılarak, birçok sisteme ağır zararlar vermektedir. Halen birçok kritik altyapıyı yöneten kurumlar da dahil bu konuda yeterince farkındalığın olduğundan bahsetmek çok zordur. Çalışmada bahsedildiği gibi yapılan anket sonucunda birçok çalışan ve yönetici bu durumun kendi başlarına gelmeyeceğini düşünmekte, test ortamı yaratarak mevcut güvenlik sistemlerinin gelişimi için uğraşmamakta ve eğer böyle bir saldırı olursa ne yapacağını bilmemektedir. Ortaya çıkan diğer bir sonuç ise bu konuda sorumlu kişiler özellikle bu konuda yetişmiş personel azlığı, teknoloji yetersizliği ve yetersiz bütçeden yakınmaktadır. Diğer taraftan gün geçtikçe siber saldırganların ve siber tehdit araçlarının sayısı artmakta, kendilerini geliştirmekte ve daha etkili olabilmektedir.

Kakanakov ve Spasov [39] çalışmalarında Linux tabanlı sistemlerin DDoS saldırılarına karşı daha güvenli olduğunu ileri sürmüşlerdir. Bunun sebebi olarak, Linux işletim sisteminde ilk SYN paketini aldıktan sonra bağlantı için kaynak ayırmak yerine SYN çerezleri (cookie) kullanılmakta ve sadece ACK komutunu aldığında kaynak tahsis edilmektedir. Bu nedenle, SCADA sistemlerinde Linux işletim sisteminin kullanılmasının daha doğru olacağı savunulmaktadır. Elbette bu işletim sistemleri için modern sömürücüler vardır; fakat yine de Linux sistemlerin güvenliğini aşmak için diğer sistemlere göre daha fazla çaba gerektirmektedir. Markovic-Petrovic ve Stojanovic [40] makalesinde birçok güvenlik konusunu tanımlamak için SCADA sistem mimarilerinin değerlendirmesini yapmıştır. Özellikle son on yılda dünya genelinde birçok endüstriyel kontrol merkezine saldırı yapıldığından ve SCADA sistemlerindeki açıklıkların arttığından söz edilmektedir. Bunun sebebi olarak da; bilinen açıklıkları standart teknolojiler kullanarak ortadan kaldırmaya çalışmama, kontrol sistemlerinin diğer ağlara bağlı olması, mevcut güvenlik teknolojileri ve uygulamalarının kısıtlanması, güvensiz uzaktan bağlantı, kontrol sistemleri hakkında teknik bilgilere herkes tarafından ulaşılabilmesi sayılmıştır. Bu açıklıklardan dolayı bazı bilgisayarların köle (zombi) haline geldiği ve sistemlere zarar verilebildiği üzerinde durulmuştur. Ortaya çıkan çalışmanın sonucuna göre pratik olarak bu açıklıkların ortadan kaldırılmasının zor olduğu, kritik birçok sisteme zarar verebilecek DDoS saldırılarına engel olabilecek güvenlik mekanizması olmadığı ve bu saldırıların sistemlerde performans kaybına, ekonomide yerine koyulamayacak zararlara sebep olacağı üzerine vurgu yapılmaktır.

MITM saldırısına yönelik güvenlik çözümleri incelendiğinde; Nam ve diğerleri; ARP zehirlemesinden dolayısıyla MITM saldırısından korunmak için mevcut kullanıcılara öncelik vererek, yeni bir düğüm ya da kullanıcı ağa girdiğinde ve MAC tablosuna kendi MAC adresini yazdırma talebini gönderdiğinde, ethernet var olan düğüm tablosuna bakarak, yeni düğüme komşu olan diğer düğümlere sorgu mesajı göndermektedir. Alınan cevaplar kontrol edilerek, bu düğüm ya da kullanıcının, zararlı bir düğüm ya da kullanıcı mı yoksa gerçekten ağa eklenen yeni bir bileşen mi olduğuna karar vermektedir [41]. Bu teknik; kablolu ağlar için, düğümler sabit olduğundan başarılı olabilmektedir. Ancak kablosuz ve mobil ağlarda düğümler sürekli yer değiştirdiğinden başarı oranı oldukça düşük kalmaktadır. Lootah, MCDaniel ve Enck; ARP zehirlenmesine engel olmak amacıyla şifreleme yöntemlerinden yararlanmışlardır. Bilet-Tabanlı ARP (Ticked-based ARP(TARP)) en yaygın bilinen şifreleme-tabanlı yaklaşımdır. Güvenli ARP (S-ARP) ve Yerel Bilet Dağıtıcısı (Local Ticket Agent-LTA) için kullanılan Güvenilir Anahtar Dağıtımı gibi merkezi sunucular belirli noktalardaki problemler için çözüm olabilmektedir [42]. Bu çözüm yine kablosuz iletişim için yeterli olmamaktadır.

MITM saldırılarına karşı korunmak için, Pansa ve Chomsiri MAC-IP veri tabanı merkezi olarak kullanılan DHCP sunucularının kurulumuna yönelik bir yöntemi çözüm olarak tespit etmişlerdir. Bu yöntemde, her bir kullanıcı arasında MAC adreslerinin iletiminin gerçekleştirilmesi için yeni bir DHCP önermektedir [43]. Ancak DHCP, uygulamada oldukça yaygın olarak kullanılmaktadır, ayarlanması zordur ve bu nedenle gerçek hayatta kolaylıkla uygulanabilir bir yöntem değildir. ARP hilesinin yapılabilmesinin en büyük nedeni düğümler arasında MAC adresi değişimi yapılırken kimlik doğrulamasının yapılmamasıdır. Bu nedenle tüm ARP paketleri kötü niyetli kullanıcıların saldırısına uğrayabilir. Hong, Oh ve Lee çalışmalarında, bu saldırıları engellemek maksadıyla, ARP protokolünü korumak için AES ve RSA kriptolama teknikleri kullanılan bir model tasarlamışlardır. Modelde, istemci isteğini MAC dağıtıcısına ilettiğinde, MAC dağıtıcısı açık RSA anahtarını dağıtmaktadır. Buna karşılık istemci AES anahtarını oluşturmaktadır ve bunu açık anahtarla şifrelemektedir. Ayrıca kendi anahtarını MAC dağıtıcısına iletmektedir. AES değişimi sağlandıktan sonra ARP tablo bilgisi AES anahtarını kullanarak güvenli bir şekilde alınıp, iletilebilmektedir. Modelin temel amacı ARP tablosu bilgilerinin şifreli olarak gönderilmesi ve alınmasıdır. ARP istekleri ve cevap paketlerinin sürücüler tarafından bloklanarak, bu sayede ARP zehirlenmesi saldırısının etkisizleştirilmesi hedeflenmiştir [44]. Bu koruma yönteminde, istemci tarafı korunmakla birlikte ağ geçidi kısmı tam olarak

korunamamakta ve ARP zehirlenmesi saldırılarına karşı hassas durumda kalmaktadır. Bu nedenle böyle bir saldırı yapıldığında ağ geçidi tüm istemcilere ağın saldırı altında olduğu mesajını iletmektedir.

Oppliger ve diğerleri, SSL/TLS protokolünde sunucuya erişim yapan kullanıcının Kullanıcı Kimlik Doğrulama Kodu (User Authentication Code-UAC) kullanarak kimlik doğrulama yapmasına yönelik bir model önermişlerdir. Modelin amacı; sunucunun sahte kullanıcıyı tanıyarak düşürmesidir [45]. UAC kullanımında kullanılan sistemin zararlı yazılımlardan korunmuş olması gerekir. Aksi takdirde Truva atı gibi kötücül yazılımlarla kullanıcının PIN'i ele geçirilebilir ve sistem saldırılara açık hale gelebilir. Ciancamerla ve diğerlerinin yaptığı çalışmada [46]; SCADA cihazları, saldırgan ve ağ tabanlı saldırı tespit sisteminden oluşan yerel bir ağda haberleşen hibrit bir deney düzeneği ortamında MITM saldırısı gerçekleştirmiştir. Saldırıda ARP protokolünün şifreleme özelliğinin eksikliğinden faydalanarak SCADA kontrol sunucusu ve PLC arasına girilmiş ve ARP zehirlenmesi gerçekleştirilmiştir. Bu sayede saldırgan iki cihaz arasında akan paketleri yakalamış ve bu paketler üzerinde değişiklikler yapabilmiştir. Lee ve diğerleri [47], DNP3 protokolüne yönelik gerçekleştirdiği çalışmada Ettercap aracını kullanarak ARP zehirlenmesiyle araya girme saldırısı gerçekleştirilmiş ardından yakalanan paketlerin analizi için Wireshark aracını kullanmışlardır. Analiz edilen DNP3 paketleri libpcap aracıyla kullanıcının göndermek istediği paketler değiştirilmiştir.

Morris ve Gao'nun yaptıkları çalışmada, SCADA kontrol sistemlerine yönelik gerçekleştirdikleri bir dizi saldırıyı tartışmışlardır. Bu saldırılar; keşif, tepki, ölçüm ve komut enjeksiyonu ve DoS olarak dört sınıfta incelenmiş ve detaylı bir şekilde açıklanmıştır. Saldırı karmaşıklığına göre komut enjeksiyonu alt gruplara ayrılmıştır. Çalışmada anlatılan her bir saldırı, laboratuvar ortamında endüstriyel denetim sistemlerine yönelik gerçekleştirilmiştir [48]. Aloui yaptığı çalışmada; Stuxnet zararlı yazılımına dikkat çekerek S7-300 PLC cihazına yönelik dinamik kod enjeksiyonunun ne kadar kolay bir şekilde gerçekleştirilebileceğini göstermiştir. Saldırıyı gerçekleştirmek için Snap7 kütüphanesini kullanarak C dilinde bir program geliştirmiş ve dinamik kod enjeksiyonuna yönelik güvenlik önlemleri önermiştir [49].

Zhu ve diğerlerinin yaptıkları çalışmada, SCADA sistemlerine yönelik siber saldırıları sistematik olarak sınıflandırarak tanımlamıştır. SCADA sistemlerinin donanım, yazılım ve

haberleşme bileşenlerine yapılan saldırıları açıklamış; uzaktan yetkisiz erişim kazanma ve cihazın alarm oluşturacağı veya denetim sağladığı eşik değerlerde yapılan değişiklikler donanıma yönelik yapılan saldırılar başlığı altında, gömülü işletim sistemi üzerinde yetki yükseltme, bellek taşması ve SQL enjeksiyonu gibi saldırılar yazılıma yönelik yapılan saldırılar başlığı altında, SCADA haberleşme protokollerinin şifreleme olmaması ve TCP/IP tabanlı olması gibi zafiyetlerden faydalanarak gerçekleştirilen saldırıları haberleşme bileşenlerine yönelik yapılan saldırılar başlığı altında toplanmıştır [50]. Gao ve diğerlerinin yaptığı çalışmada, Mississippi State Üniversitesi SCADA Güvenliği Laboratuvarı'nda geliştirilen test ortamında zararlı komut enjeksiyonu saldırıları gerçekleştirilmiş ve bu saldırıların tespiti için kontrol sisteminin fiziksel özelliklerinin bilgisinde kullanılan yapay sinir ağı (YSA) temelli STS kullanılarak saldırılar sonucunda hatalı tespit oranlarını deneysel sonuçlarla gözlemlemişlerdir. Elde edilen sonuçlar YSA tabanlı STS'lerinin umut verici bir güvenlik mekanizması olduğu üzerinde durulmuştur [51].

Yang [52] replay saldırılarını önlemeye yönelik yaptığı çalışmada tekli oturum açma sistemini önermiştir. Çalışmada önerilen modelde, kimlik doğrulamayı ve yetkilendirmeyi korumak için birçok veri tabanı eklenmiştir. Bu yaklaşımda, kimlik doğrulama sunucusu kullanıcıya kullanıcı ismi ve kullanım süresi gibi bilgileri içeren TGT (Ticket Granting Ticked) gönderir. TGS (Ticket Granting Service) kullanıcı ve uygulama sunucusuna Service Granting Ticket gönderir. TGS ve uygulama sunucusu kendi veri tabanlarına sahiptir ve bu biletleri kendi veri tabanlarında depolarlar. Bir saldırgan TGT'e veya SGT'e yönelik bir replay saldırısında bulunduğunda bunun bir saldırı olup olmadığı kolaylıkla anlaşılabilecektir.

Jian [53] ikinci çalışmasında tekli oturum açma sisteminden farklı olarak dinamik çift parola temelli oturum açma protokolünü önermiştir. Bu protokolde; kullanıcı kaydı ve kayıt dosyaları konseptinin kullanımı süresince ihtiyaç olan iki parola kullanılmaktadır. Kayıt dosyası belirli bir kullanıcının TGT veya uygulama sunucusu gibi kimlik doğrulama sunucusunu ziyaretindeki detayları bulundurur. Uygulama sunucusu kayıt dosyası üretir ve kimlik doğrulama sunucusuna gönderir. Kimlik doğrulama sunucusu bu kayıt dosyasını kullanıcıya yönlendirir. Bu yüzden, kullanıcı kayıt dosyalarının denetimi boyunca parolasının güvenliğini değerlendirebilir ve değiştirebilir. Saldırgan bir parolayı ele geçirdiğinde, kullanıcı kolaylıkla parolasını kayıt dosyalarına bakarak ve analiz ederek değiştirmesi mümkündür. Lokasyon temelli Kerberos kimlik doğrulama protokolündeki

yaklaşımda, sunucu ağdaki tüm kullanıcıların P(Y) kodlarını yakalar ve şifreli oturum anahtarı (TGS ve kullanıcı arasındaki haberleşme için) olarak kullanıcıya TGT gönderir. Kullanıcı mesajı aldıktan sonra GPS kullanarak P(Y) kodu kabul eder ve mesajın şifresi çözülür. Saldırgan mesajı ele geçirirse mesajın şifresini çözemez. Çünkü P(Y) kodun boyutu gigabit boyutundadır. Zaman senkronizasyon probleminden dolayı başarısızlığa uğrar. Burada kullanıcının fiziksel lokasyonu mesaj sağlayıcının fiziksel lokasyonuna karar vermesine yardım eden Kerberos protokolüne ek bir mesaj olarak eklenmiştir. Sunucu, kullanıcıya kullanıcının fiziksel lokasyonunun hash değerli şifreli oturum anahtarıyla TGT gönderir [54]. Bu yüzden saldırgan bir mesaj ele geçirse dahi oturum biletini alma ve bu süreçte biletin süresi olmak üzere iki güvenlik fazını kırmak zorundadır.

Ten ve diğerlerinin kritik altyapıların siber güvenliği üzerine yaptığı kapsamlı çalışmada, SCADA güvenliğini 4 ana başlıkta incelemeyi önermiştir. Bunları; gerçek zamanlı izleme, anomali tespiti, etki analizi ve saldırı hafifletme olarak sıralamıştır. Aynı zamanda, etki analizi için saldırı yöntemini geliştirmiştir. Güç sistemlerine yönelik geliştirilen saldırı ağacı modelinde; sistem, senaryo ve düğüm seviyeli güvenlik açıkları sisteme yönelik tehditler tespit edilerek hesaplanır. Port dinleme ve parola tahmini gibi saldırıları içeren düğüm seviyeli güvenlik açıkları bu yöntemde en sık karşılaşılan saldırılardır [55]. Yang ve diğerlerinin güç şebekelerinde kullanılan SCADA sistemlerinin siber güvenliğiyle ilgili yaptıkları çalışmada, geliştirdikleri test ortamında siber saldırıları hafifletmeye yönelik çok nitelikli STS önermişlerdir. Çok nitelikli STS güvenilir kabul edilen adresler ve davranış temelli bir konsept içerir. SCADA siber güvenliğini artırmak için normal verileri riske atmadan veri bütünlüğü sağlanarak bir güvenlik çözümü önerilmiştir [56].

Shang ve diğerlerinin yaptıkları çalışmada [57] endüstriyel kontrol sistemlerinde karşılaşılan zararlı yazılımlara yönelik STS'leri incelenmiş ve Modbus TCP protokolü uygulama katmanından gelen tehditlere yönelik paket boyutunda derinlemesine analiz edilmiştir. Modbus TCP haberleşmesi için savunma modeli olarak STS tabanlı bir "White list" kuralı önerilmiştir. Bo Chen ve diğerlerinin yaptıkları çalışmada [58] akıllı şebekelerin siber güvenliği için gerçek-zamanlı güç sistemi simülatörü ve haberleşme sistemi simülatörünü entegre çalıştırarak bir deney düzeneği ortamı hazırlamışlardır. Güç sistemi simülasyonu için RTDS (Real-Time Digital Simulator) güç şebekesi simülatörü kullanılmış olup, haberleşme sistemi simülasyonu için Opnet'in SITL (System-in-the-Loop) simülatörü ve açık kaynak kodlu Linux araçları ve sunucuları kullanılmıştır. Bu deney düzeneğinde

Modbus TCP protokolüne yönelik iki çeşit siber saldırı düzenlenmiş ve bu saldırıların tespitine ve engellenmesine yönelik önerilerde bulunmuşlardır.

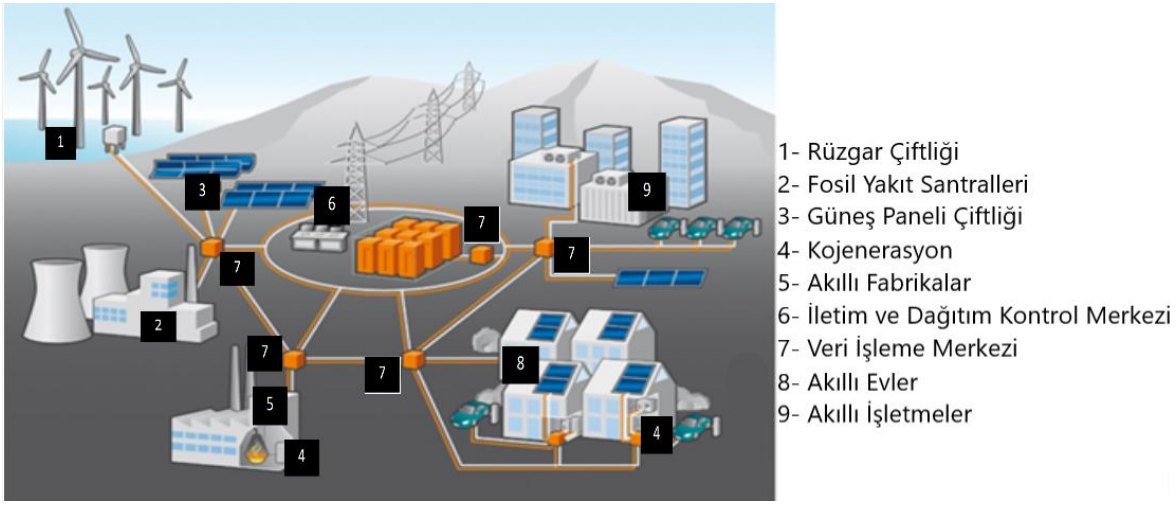
Xiong ve diğerleri Modbus TCP protokolünün zafiyet analizi için geleneksel fuzzing (bulandırma) yöntemleri dışında Modbus TCP protokolüne has özel bir fuzzing metodolojisi geliştirmişlerdir [59]. Geliştirdikleri fuzzing teknolojisini uyguladıkları simülasyon ortamındaki sonuçlarına göre geleneksel fuzzing işlemlerine göre tatmin edici olduğunu vurgulamışlardır. Bhatia ve diğerleri Modbus protokolünün sel (flooding) saldırılarına karşı zafiyet barındırdığını ve bu saldırıların kontrol sisteminin fonksiyonlarını bozmaya yönelik komut enjeksiyonu da içerdiğinden bahsetmişlerdir [60]. Çalışmada, bu saldırıları tespit etmeye yönelik anomali tabanlı tespit algoritması ve imza tabanlı Snort eşik modülü karşılaştırılmıştır. Sonuç olarak, imza tabanlı tespit sisteminin eşik değerlerinin çok dikkatli belirlenmesi gerektiği ve anomali tabanlı tespit sisteminin saldırı belirlemede çok az bir zaman kayması sonucu tespit ettiğini belirlemişlerdir.

Yukarıda özetlenen literatür incelemelerinden açıkça görülebileceği gibi, SCADA sistemlerinin siber güvenliği son derece önemli olup bu konuda yaygın çalışmalar bulunmaktadır. Bu nedenle bu tez çalışmasında da SCADA sistemlerinin zafiyetleri ortaya konulmuş, bu sistemlere yönelik oluşabilecek tehditler belirlenmiştir. Ayrıca tez çalışması kapsamında da istatistiği çıkarılarak belirlenmiş endüstriyel kontrol sistemlerinde en sık kullanılan protokollerden birisi olan Modbus TCP protokolünün kaynak IP adresi kontrolü zafiyetinin giderilmesine yönelik bir güvenlik mimarisi önerilmiştir. Modbus TCP protokolünün güvenliğine yönelik önerilen bu çözüm ile mimarinin bileşenlerinin içerdiği fonksiyonlar sayesinde kullanıcının saha cihazlarına yetkisiz erişiminin ve cihazların yazmaçlarına kontrol dışı değerlerin girilebilmesinin engellenmesi hedeflenmiştir.

3. SCADA SİSTEMLERİ VE ALTYAPI BİLEŞENLERİ

Günümüzde elektrik endüstrisi daha merkezi ve üretici kontrolü temelli bir ağdan oluşur. Bu ağın daha dağıtık ve tüketici tabanlı dönüşümü "Akıllı Şebeke" (Smart Grid) olarak adlandırılır [61]. Elektrik arzının giderek arttığı günümüzde akıllı şebeke ihtiyacı da giderek artmaktadır. Tüketiciler kendi enerji kullanımlarını daha verimli ve ekonomik olarak daha uygun bir yolla yönetme yetkisine sahip olacaklardır. Akıllı şebekeler aynı zamanda güç güvenilirliğinin yanı sıra üretimin ve gücün nasıl dağıtılacağına imkan sağlar.

Ek olarak akıllı şebekeler güç talebinin artması, yapının yıpranması ve elektrik üretimi sırasında oluşan sera gazı çevresel etkisi gibi zorlukların üstesinden gelmeye olanak sağlar. Akıllı şebekenin kullanımı ile güç daha etkin bir şekilde kullanılabilir ve çevrede oluşacak karbon içeriği büyük ölçüde azaltılabilecektir. Bu nedenle yukarıdaki işlevleri sağlamak amacıyla şebekeyi daha otomatik hale getirmek temel odak noktası olmalıdır [62]. Şekil 3.1'de akıllı şebekenin kavramsal mimarisi gösterilmiştir. Jeneratör, merkezi güç santrali, yalıtılmış mikrogrid olarak isimlendirilen bileşenlerin hepsi SCADA (Supervisory Control and Data Acquisition - Danışmalı Kontrol ve Veri Toplama Sistemi) mimarisi ile bağlantılıdır.



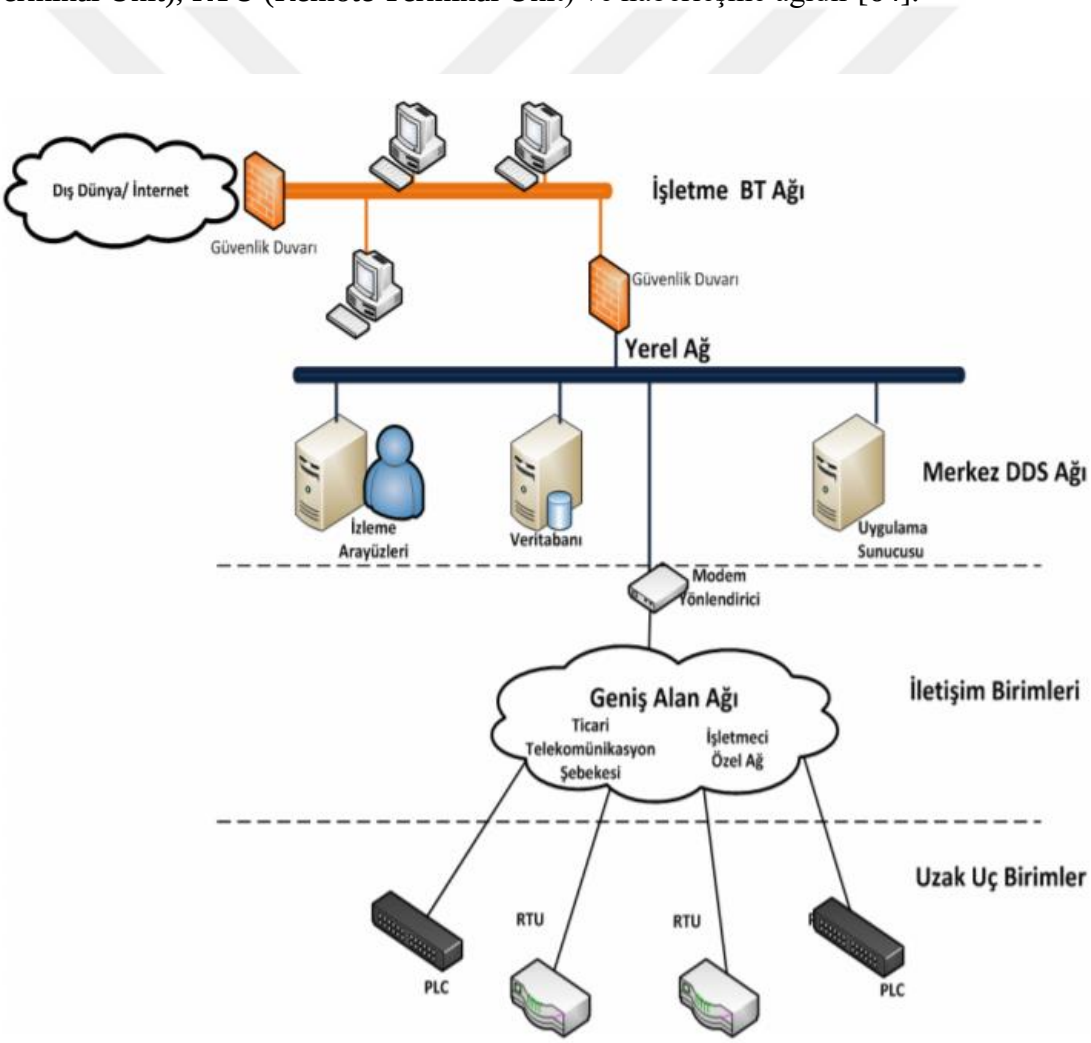
Şekil 3.1. Akıllı şebekenin kavramsal mimarisi [62]

Elektrik güç sistemlerinin kullanımında enerji, bankacılık, iletişim, üretim gibi kritik altyapılarda SCADA sistemleri kullanılır [63]. SCADA sistemleri kritik altyapı endüstrisinde yaygın olarak kullanılan ve uzaktan denetleme ve kontrol sağlayan

sistemlerdir. SCADA sisteminin temel fonksiyonu, elektrik dağıtımından sorumlu olan cihazları izlemek ve denetlemektir. Ek fonksiyon olarak hata tespiti, ekipman izolasyonu ve restorasyonu, yük ve enerji yönetimi, otomatik sayaç okuma ve trafo kontrolüdür.

SCADA, gerçek zamanlı olarak yerel ve coğrafi olarak dağıtık işlemleri ölçen ve raporlayan birbirinden bağımsız sistemler topluluğudur. Kullanıcıya uzaktaki tesislere komut göndermeye ve oradan verileri çekmeye olanak sağlayan telemetri ve veri toplama kombinasyonudur.

Şekil 3.2'de gösterildiği gibi, SCADA kontrol sisteminin temel bileşenleri MTU (Master Terminal Unit), RTU (Remote Terminal Unit) ve haberleşme ağıdır [64].



Şekil 3.2. SCADA ağı ve bileşenleri [13]

3.1. Merkezi Terminal Birimi (MTU)

Merkezi denetleyici veya merkezi terminal birimi olarak isimlendirilen MTU, yerel bir ağ (LAN) ile veya geniş alan ağı (WAN) ile bir sunucu veya bir grup bilgisayarın ana sunucuyla bağlanma formudur. İlerleyen bölümde de anlatılacak olan HMI (İnsan Makine Arayüzü) yazılımı, saha cihazlarından gelecek olan bilgilerin görsellik katması amacıyla MTU'da veya denetim merkezinde yüklüdür. SCADA bileşenlerinin haberleşmesi sırasında operatörün anlayabileceği grafiksel bir arayüz ortamı sağlar [65].

Yıllar önce tasarlanan SCADA sistemlerinde yazılım/donanım bağlantısı veya bilgi/veri gösteriminde uyuşmazlıklar vardı, fakat dağıtık kontrol sistemlerinin gelişimiyle birlikte günümüzde tasarlanan SCADA sistemleri yüksek çözünürlüklü bir arayüz ve bileşenler arasında yüksek performansta uyumluluk sağlar [66].

HMI programı MTU bilgisayarı üzerinde çalışır ve temelde tüm tesisi daha kolay tanımlamak için gerçek sistemi taklit yapan diyagramlardan oluşur. Uzak sistemdeki her giriş/çıkış noktası gösterilen mevcut yapılandırma parametreleri ile grafiksel olarak sunulur. Durdurma değeri ve limitleri gibi yapılandırma parametreleri bu arayüz üzerinden girilir. Bu bilgi ağ üzerinden iletilir ve tüm bu değerleri güncelleyecek olan ilgili uzak lokasyondaki işletim sistemine indirilir.

Özellikle günümüzde kişisel bilgisayarların kullanımının artmasıyla birlikte ofis tabanlı kişisel bilgisayarlar SCADA sistemleriyle aynı ağda bulunmaya başlamışlardır. Böylece günlük hayatta kullanılan yazılımlar ve bilgisayar uygulamaları SCADA sistemlerinin yönetimi için kullanılan sunucu bilgisayarlarında da kullanılmaya başlamıştır. MTU hem son karar verici bileşen olması hem de sistem üzerindeki kayıtları üzerinde barındırması sebebiyle SCADA sisteminin en önemli bileşenidir. Bu bileşenin fonksiyonlarını yerine getirememesi veya bir saldırıya maruz kalması bütün şebekeyi risk altında bırakabilecektir. Bu bakımdan SCADA sistemlerinin yönetimi amacıyla kullanılan bilgisayarlarda istenilmeyen üçüncü parti bir yazılımın olması risk teşkil etmektedir [12].

MTU'nun yaptığı işlemleri kısaca maddeler halinde belirtmek gerekirse;

- Haberleşme ortamı sayesinde bütün SCADA bileşenlerinin haberleşmesini izlemek ve denetlemek.
- HMI yazılımı kullanarak SCADA haberleşmesiyle ilgili bilgi ve verileri grafiksel bir arayüz ile görüntülemek.
- Saha cihazlarına komut göndermek, saha cihazlarından gelen komutları almak ve haberleşme bağlantısını kontrol etmek.

3.2. Uzak Terminal Birimi (RTU)

Uzak terminal birimleri veya uzak uç birimleri olarak isimlendirilen RTU'lar, SCADA mimarisinde köle istasyonları olarak davranırlar. SCADA tarafından kontrol edilen ve izlenen ekipman veya makinalara bağlı olan saha cihazlarından oluşur. Bu cihazlar parametreleri izlemek için sensörleri ve sistemin modüllerini kontrol etmek amacıyla aktüatörü veya uyarıcıyı bünyesinde bulundurur. RTU'lar, MTU istasyonuna geri göndermek üzere sensörlerden gerçek zamanlı bilgileri gönderir ve ana istasyondan gelen bilgileri alır. Felaket, felaket kurtarma, uyarıcı veya sensörlerin fonksiyon kodlarını veya diğer kritik durumlar gibi bilgileri MTU'a gönderir.

RTU cihazları coğrafi olarak farklı birçok konumda konuşlandırılarak dağıtık bir şekilde gerçek zamanlı bilgileri merkezi istasyona LAN/WAN bağlantılarını kullanarak gönderir. Aynı zamanda fiziksel olarak konuşlandırılmış cihazların doğru yapılandırıldığı veya doğru bir şekilde çalıştığı gibi mevcut durum bilgilerini de göndermekle sorumludur [67].

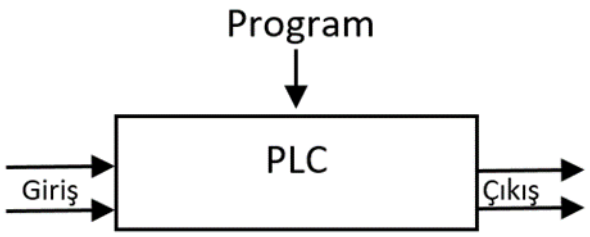
Saha cihazlarının en önemli bileşeni olan PLC (Programlanabilir Mantıksal Denetleyici) cihazları aşağıdaki alt başlıkta detaylı olarak açıklanmıştır.

3.2.1. Programlanabilir mantıksal denetleyici (PLC) sistemler

PLC sistemleri, Şekil 3.3'te gösterilen işlemleri ve kontrol mekanizmasını uygulamak için girilen talimatları depolamak ve sıralama, zamanlama ve sayma gibi fonksiyonları uygulamak için programlanabilir hafızayı kullanabilen mikroişlemci tabanlı denetleyicilerin özel bir formudur. Mantıksal ve anahtarlama işlemlerinin uygulanması bu cihazlardaki öncelikli işlevdir. Operatörün kullandığı bir diğer işlev PLC cihazının hafızasına girdiği

talimatların sıralamasının olduğu programdır. Denetleyici daha sonrasında bu programa göre giriş ve çıkışları izler ve programın denetim kurallarını uygular.

PLC cihazları, temel denetleyici işlemlerini geniş bir alanda kullanmasından ötürü büyük bir avantaj sağlamaktadır. Kontrol sistemini ve kullanılan kuralları değiştirmek için yeniden kablolamaya ihtiyaç duymadan farklı bir dizi talimatlarla gerçekleştirilebilir. Sonuç olarak maliyet etkinliği olan ve kullanımı açısından birçok kolaylık sağlayan PLC cihazları röle sistemleriyle kıyaslandığında, yazılım tarafında yapılan uygulamalarla karmaşık donanımsal problemlerden kurtulunur. Aynı zamanda rölelerin çok sayıda karmaşık mekanik bileşenlerden oluşması bakımından daha güvenli ve sağlam olması ve çalıştırdığı işlemleri daha hızlı bir şekilde işlemesi bakımından tercih sebebidir [68].



Şekil 3.3. Programlanabilir mantıksal denetleyici

İlk olarak 1969 yılında geliştirilen PLC, günümüzde kullanımı yaygınlaşmış ve sahadaki birçok sensörden aldığı verileri modüler sistemlere 20 dijital giriş/çıkış modülü sağlayacak kapasiteye çıkmıştır. Ağırlıklı olarak talaşlı üretim, malzeme taşıma, gaz ve yağ rafine sistemleri, su tedariği ve ulaşım gibi endüstriyel işlemlerin otomasyon tarafında kullanılır.

Aşağıdaki alt başlıklarda PLC cihazının mimarisi, yazılımsal ve donanımsal özellikleri anlatılmıştır.

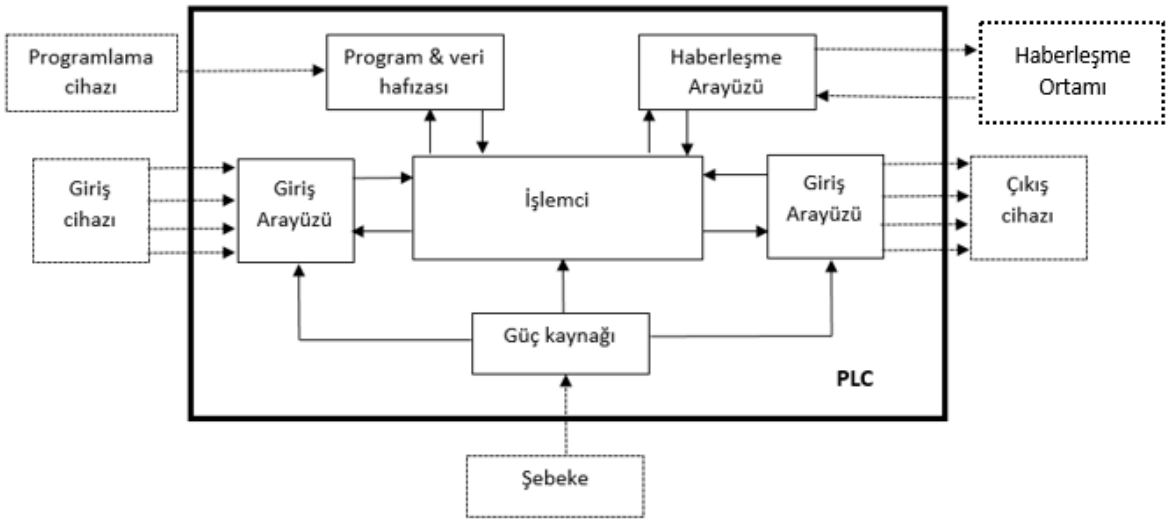
PLC mimarisi

Karakteristik bir PLC cihazında mikroişlemcinin bulunduğu CPU, hafıza ve giriş/çıkış devreleri bulunur. Ayrıca içerisinde yazılımsal olarak çok sayıda röle, saymaç, zamanlayıcı ve veri depolama ünitesi mevcuttur.

Giriş/Çıkış (I/O) birimi PLC cihazının giriş çıkış kanallarıyla bağlantı sağlayarak dış dünyadan gelen bilgileri almasını sağlar. Her I/O noktasının CPU tarafından kullanılan belirli bir adresi vardır. Bu bir yol boyunca sıralanan ev dizisi olarak düşünülebilir. Örneğin 10 numara belirli bir sensörden gelen giriş için kullanılıyorken, 45 numara çıkış biriminde belirli bir motor için kullanılabilir [69].

PLC donanımı

Karakteristik bir PLC sistemi işlemci birimi, hafıza, güç destek birimi, giriş/çıkış arayüz birimi, haberleşme arayüzü ve programlama cihazı gibi temel fonksiyonel bileşenlerden oluşur. Şekil 3.4'te temel bir PLC sistemin bileşenleri verilmiş ve bu bileşenlere ait detaylar aşağıda anlatılmıştır.



Şekil 3.4. PLC sistemi

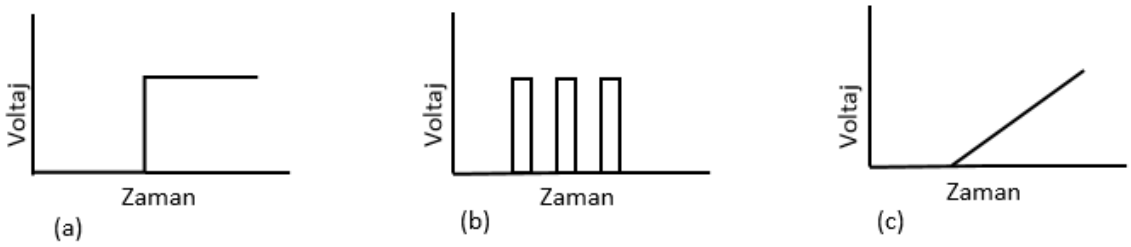
Merkezi İşlemci Birimi (CPU) mikroişlemcinin bulunduğu birimdir. Bu birim giriş sinyallerini yorumlar ve hafızasında depolanan programa göre çıkış sinyallerindeki aksiyona karar verecek şekilde haberleşerek kontrol aksiyonunu gerçekleştirir.

Güç Destek Birimi ana AC voltajı işlemci ve giriş ve çıkış modül arayüzleri için gerekli düşük DC voltajına dönüştürür.

Programlama Cihazı işlemcinin hafızasına gerekli programı girmek için kullanılır. Program bu cihazda geliştirilir ve daha sonrasında PLC cihazının hafıza birimine transfer edilir.

Hafıza Birimi mikroişlemci tarafından depolanan kontrol aksiyonlarının bulunduğu program birimidir ve girişten gelen sinyalleri çıkış sinyallerine işleyen verileri depolar [70].

Giriş ve Çıkış Birimleri dış ortamdan gelen bilgilerin işlendiği ve dış ortamdaki bu cihazlarla haberleşmenin gerçekleştiği birimdir. Giriş birimi anahtar, fotosel, sıcaklık sensörü, akım sensörü gibi sensörlerden oluşur. Çıkış birimi marş motoru, solenoid pompası gibi cihazlardan oluşur. Giriş ve çıkış birimindeki cihazlar Şekil 3.5'te gösterildiği gibi kesikli, dijital veya analog olarak verdikleri sinyallere göre sınıflandırılırlar.



Şekil 3.5. Sinyaller: (a) Kesikli, (b) Dijital, (c) Analog

Haberleşme Arayüzü diğer PLC cihazlarıyla haberleşmek veri alıp transfer etmek için kullanılır. Cihaz doğrulaması veri toplaması, kullanıcı uygulamaları arasında senkronizasyon ve bağlantı yönetimi gibi aksiyonlar bu birimde kullanılır [71].

PLC yazılımları

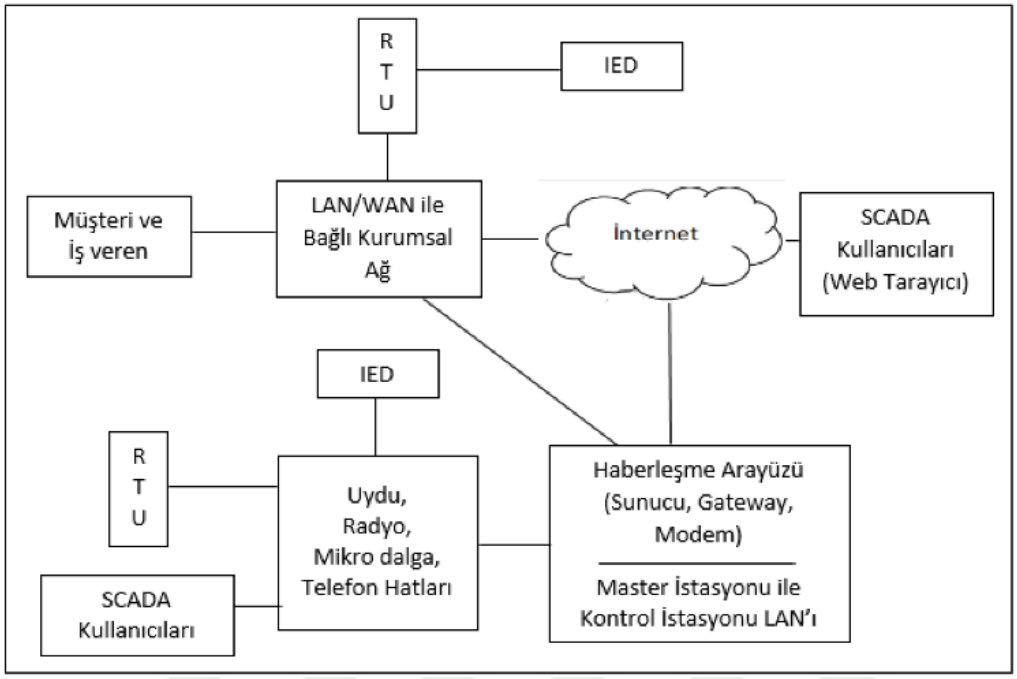
PLC cihazları için kullanılan programlar birçok formatta yazılabilir. Programlamanın kullanımını kolaylaştırmak için çok fazla bilgi gerektirmeyen ladder programlama geliştirilmiştir. PLC üretici firmalarının birçoğu bu yöntemi kullanmaktadır, fakat her üretici kendi versiyonunu geliştirmiş ve böylece PLC programlama için kullanılan ladder programlamada uluslararası standart oluşturulmasına gerek duyulmuştur. Bu nedenle, 1993 yılında Uluslararası Elektroteknik Komisyonu (IEC) 1131-3 koduyla bir standart geliştirilmiştir. 2013 yılında son güncel haliyle IEC 61131-3 versiyonu bulunmaktadır. Ladder programlamayla ladder diyagramlar, sıralı fonksiyon göstergesi ve fonksiyon blok diyagramlar gibi grafiksel elementler kullanılır [72].

3.3. SCADA Haberleşme Ağı

SCADA mimarisinin gelişimi telemetrinin ilk kullanılmaya başladığı 1900'lü yıllara dayanmaktadır. Telemetri, gerçek zamanlı sensör uygulamalarından elde edilen transmisyon ve veri toplama birimlerinden oluşur. Temel SCADA ağlarında da uzak çalışma birimlerinden merkezi işletme birimlerine toplanan verilerin alınmasından oluşur. MTU bilgisayarları, işletme operatörüne okunabilir bir formda sunmak ve saha ekipmanları ve kontrol cihazlarını otomatik olarak denetlemesine imkan vermesi amacıyla sayaç okuma ve ekipman durumları gibi bilgileri sağlar. MTU, uzak terminalde çalışan birimlerle hemen hemen tüm iletişimi başlatan kısımdır [73].

MTU temelde işletme operatörüne verileri sunan merkezi işlem bilgisayarlarını barındırır ve bir sonraki adımda hangi fonksiyonun gerçekleştirileceğine karar verir. Eski SCADA ağları güvenirliği sağlamak yerine işlerliği sağlamak amacıyla tasarlanmıştır. Dolayısıyla MTU 1200 baud (veri iletişim hızı) haberleşme kanalları üzerinden komutlarını gönderir ve RTU fonksiyonu sadece komutu çalıştırır, yeni veriyi algılar ve MTU'a tekrar geri gönderir. RTU birimlerinin hiçbiri yerel zekaya (ölçüm verilerinin, aynı cihaz içerisinde ek işlemlerden geçirilebilme özelliği) sahip değildir.

Yeni haberleşme teknolojilerinin gelişmesi ve haberleşme kanallarının hızlanmasıyla birlikte sistemler yerini yeni teknolojilere bırakmıştır. Dolayısıyla haberleşme kanallarını hızlandırmak ve RTU birimlerini daha akıllı yapmak amacıyla bütün işlem gücü SCADA ağları üzerinden gerçekleşir. IED (Akıllı Elektronik Cihazlar) gelişmesiyle birlikte RTU daha zeki işlem gücüne sahip olmaya başlamıştır. IED'ler sunucu gerektirmeyen basit mantık süreçlerini bağımsız olarak çalıştırma yeteneğine sahiptir. Bu yüzden, RTU cihazları, sistem koruması, yerel işlem kapasitesi ve alt sistemlerden veri toplama gibi birçok fonksiyonel işlemi gerçekleştirmeye olanak sağlar. Şekil 3.6'da SCADA sistemi bileşenlerinin yer aldığı haberleşme altyapısı verilmiştir.



Şekil 3.6. Modern SCADA haberleşme mimarisi [73]

3.3.1. SCADA haberleşme protokolleri

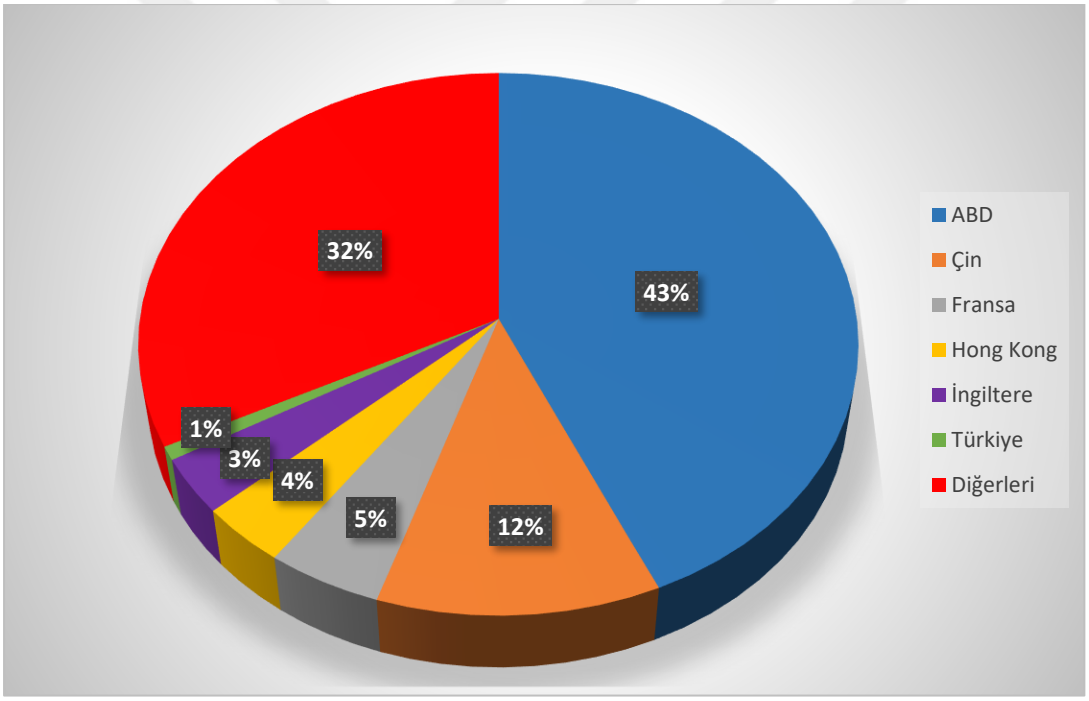
SCADA sistemleri, MTU ve bir veya daha fazla RTU'lar arasında iletişim kurmak için kullanılan açık veya özel haberleşme protokollerini kullanarak tasarlanmıştır. SCADA protokolleri alt istasyon bilgisayarlarının, RTU'ların, IED'lerin ve MTU'ların birbiriyle haberleşmesi için transmisyon özelliklerini sağlar. En çok kullanılan SCADA haberleşme protokolleri aşağıdaki gibidir:

- DNP3 (Distributed Network Protocol Version 3.0)
- Modbus
- Profinet

İlerleyen bölümlerde detaylı olarak anlatılacak olan Shodan arama motoruyla [74] tez kapsamında bir takım port bazlı aramalar yapılarak SCADA sistemlerin haberleşmesinde kullanılan protokollerin ülke bazında kullanım oranlaması yapılmış ve bu protokollerin dünyada kullanım oranları verilerek istatistiki bilgiler elde edilmiştir. Edinilen bu bilgiler Shodan'ın internete açık servisleri tespit etmesinden dolayı tamamen gerçek sonuçlar vermeyecektir. Fakat bu bilgiler SCADA sistemlerinde kullanılan protokollerin istatistiki bilgileri açısından önemli bir rehberlik teşkil edecektir.

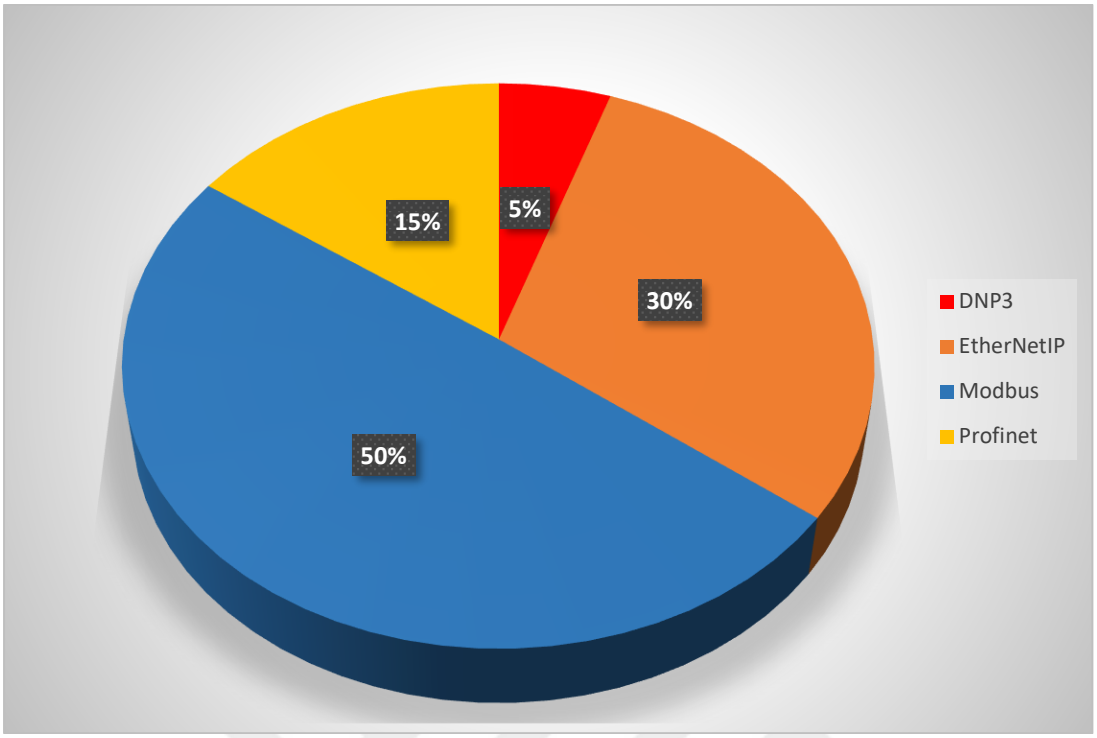
Tez kapsamında yapılan Shodan aramasında SCADA sistemlerinin haberleşmesinde kullanılan ve internete açık saha cihazlarının yani RTU'ların kullandığı protokollerden Modbus TCP, EtherNetIP, Profinet ve DNP3 varsayılan port numaraları aranmıştır. Elde edilen sonuçlar; protokollerin kullanım oranları, ülkeler bazında hangi ülkelerde ne oranda kullanıldığı ve ülkemizin dünyada SCADA haberleşme protokollerini hangi oranda kullandığını göstermektedir.

Şekil 3.7'ye göre Shodan arama motorunda SCADA haberleşme protokollerinin kullandığı varsayılan port numaraları taranmış ve bu portların ülkelere göre dağılım oranları alınmıştır. Bu bilgilere göre ABD ve Çin, endüstriyel sistemlerin haberleşmesinde önemli bir dinamo görevi görmektedir. Ülkemizde 2731 sayısıyla %1'lik bir oranla kullanılmaktadır.



Şekil 3.7. SCADA haberleşme protokollerin ülkelere dağılım oranları

Şekil 3.8'e göre endüstriyel denetim sektöründe en sık kullanılan protokollerin oranları alınmıştır. Bu bilgilere göre Modbus TCP protokolü yarı yarıya kullanılmakta olduğu fark edilmiş, %15 ve %5'lik oranlarla Profinet ve DNP3 protokolleri kullanılmaktadır.



Şekil 3.8. SCADA haberleşme protokollerinin dağılımları

Şekil 3.8 ve 2.9 açıkça göstermektedir ki, EKS ağlarında SCADA sistemlerinin haberleşmesinde Modbus TCP protokolünün yarı yarıya kullanım oranı bulunmaktadır. Elde edilen bu istatistik, Modbus TCP protokollerine yönelik yapılacak olan siber saldırıların etkisi dünya ve ülkemiz genelinde daha geniş çaplı olacağını göstermektedir. Bu sebepten ötürü, Modbus TCP protokolüne yönelik geliştirilecek olan bir güvenlik önerisi dünya genelinde kullanılan EKS ağlarındaki SCADA sistemlerinin güvenliğini daha etkin kılacaktır.

DNP3 (Distributed Network Protokol Version 3.0)

DNP3 protokolü; MTU, RTU ve IED cihazları arasında haberleşmeyi tanımlayan telekomünikasyon standardıdır. Elektrik şirketlerinin müşterek çalışabilirliğini gerçekleştirmek ve SCADA uygulamaları için Harris Controls Division tarafından geliştirilmiştir [75].

DNP3 protokolünün en önemli özelliklerinden birisi açık kaynaklı olması ve önemli sayıda üretici tarafından desteklenmesidir. Açık kaynaklı olması sayesinde farklı birçok üreticinin

cihazlarının karşılıklı olarak çalışmasına olanak sağlar. Aşağıda bulunan DNP3 protokolünün özellikleri kullanıcıya birçok kolaylık sağlar [76].

- Açık kaynaklıdır.
- Birçok tedarikçi cihazın müşterek çalışmasını sağlar.
- Çok sayıda donanım üreticileri tarafından desteklenir.
- IEC geliştirilmiş performans mimarisi modeline uygun katmanlı mimariye sahiptir.
- Güvenli ve verimli SCADA haberleşmesi için iyileştirilmiştir.
- Kapsamlı uygulama test standartları tarafından desteklenir.
- Gelecekteki sistem genişlemesi ve modifikasyonu için birden çok tedarikçiden seçme yeteneği sunar.

DNP3, MTU (kontrol merkezi) ve diğer spesifik cihazlar (RTU, IED) için 3 temel haberleşme modunu destekler [77].

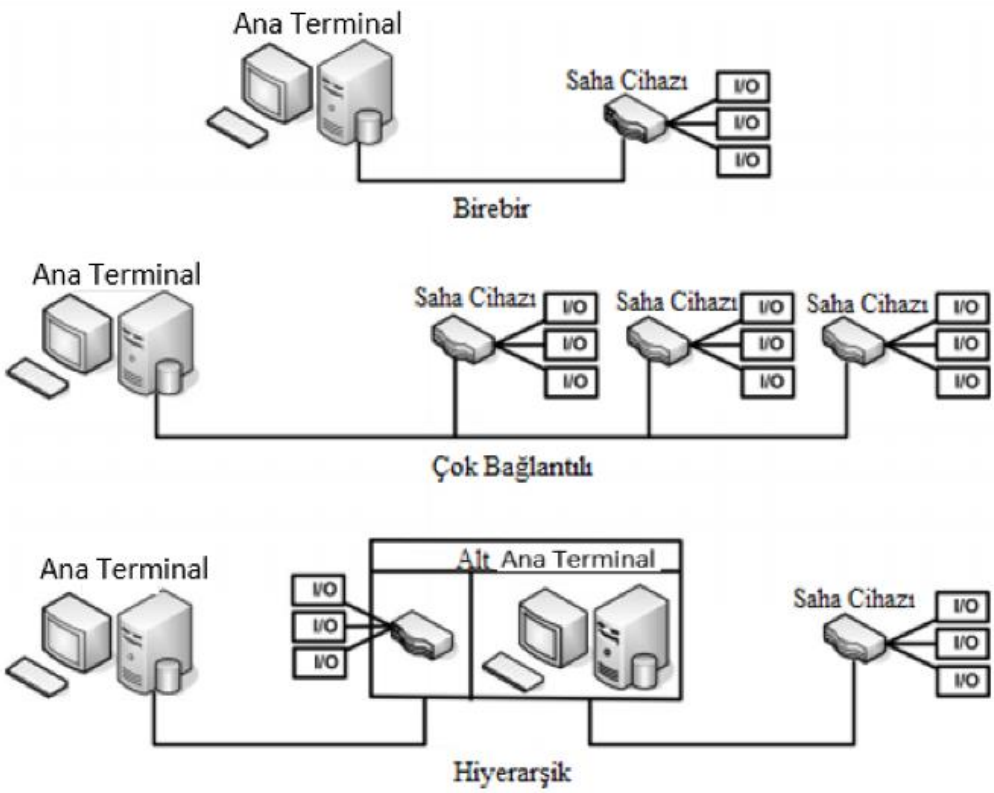
1. Tek yönlü işlem; MTU adresli spesifik cihaza istek gönderir ve bu cihazlar yanıt mesajı döner.
2. Yayınlama işlemi; MTU bütün uzak terminaldeki cihazlara genel bir mesaj gönderir ve bir yanıt mesajının dönmesini beklemez.
3. Talep edilmemiş işlem; Saha cihazları tarafından periyodik güncelleme veya uyarılar gibi bilgilerin gönderilme işlemidir.

DNP3 ağ yapılandırması

DNP3 protokolü birçok ağ yapılandırmasını destekler. Şekil 3.9'da en çok kullanılan yapılandırmalar gösterilmiştir.

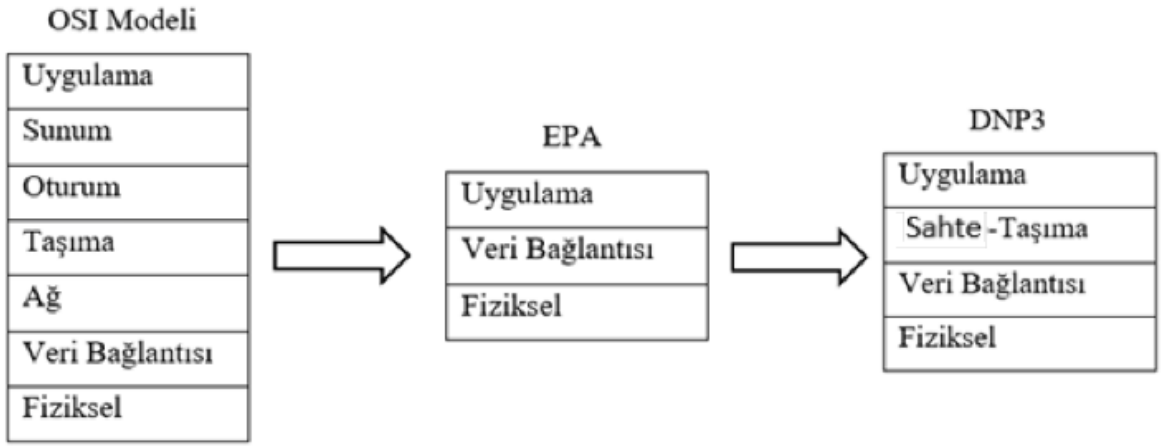
1. Birebir yapılandırma: Bir master ve bir cihaz tek bir bağlantı hattını paylaşır. Bu çevirmeli telefon bağlantısı gibi iki cihaz arasındaki bağlantı gibidir.
2. Çok bağlantılı yapılandırma: Tek bir master ve birçok saha cihazının kullanıldığı yerlerde en çok kullanılan yapılandırmadır. Bütün saha cihazları master tarafından gelen tüm istekleri alır, fakat her bir saha cihazı sadece kendisine adreslenmiş mesajlara yanıt döner.

3. Hiyerarşik yapılandırma: Bir cihaz, bir segmentte saha cihazı olarak ve diğer segmentte master olarak görev yapar ve bu nedenle bu cihaz iki işlevli bir cihazdır. Aynı zamanda bu cihaz alt master olarak isimlendirilebilir.



Şekil 3.9. DNP3 ağ yapılandırmaları [77]

DNP3 protokolü birden fazla katmanı birleştirmek için tasarlanmıştır. 3-katmanlı "Gelişmiş Performans Mimarisi" (EPA), 7-katmanlı OSI modelindeki gereksiz katmanların ortadan kaldırılmasıyla oluşturulmuştur. Fakat EPA modelinde uygulama katmanı veri bağlantı katmanından büyük mesajları almaz, dolayısıyla "sahte taşıma katmanı" olarak adlandırılan yeni bir katman bu dezavantajın üstesinden gelmek için eklenmiştir. Şekil 3.10'da DNP3 protokolünün katmanları gösterilmiştir.



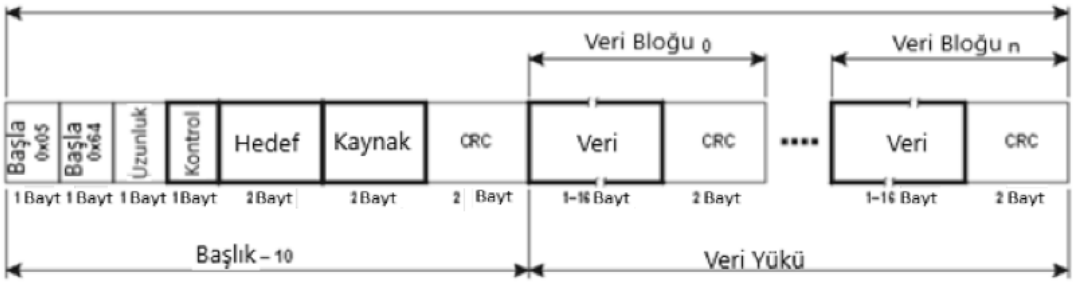
Şekil 3.10. OSI'den DNP3'e geçiş tasarımı [77]

DNP3 fiziksel katmanı

DNP3 protokol katmanları; radyo, uydu, bakır veya fiber gibi fiziksel ortam üzerinden mesajları iletmek için sorumlu olan bir fiziksel katmanın üstünde toplanmıştır. Fiziksel katman, cihazlar arasında sinyalleri göndermek amacıyla elektrik ayarları, voltaj ve zamanlama değerlerine karar verir. Fiziksel katman; (veri gönder), (veri al), (bağlan), (bağlantıyı kes), (durum güncellemesi) olmak üzere 5 servis çalıştırır.

DNP3 veri bağı katmanı

Veri bağlantı katmanının işlevi veri çerçevesini sıralı bir şekilde transfer etmek amacıyla cihazlar arasında güvenilir bir mantıksal bağlantı sağlamaktır. Veri bağlantısı, 10 baytlık sabit başlık (fixed header) ve veri yükü (data payload) olmak üzere 2 kısımdan oluşur. Veri yükü üstteki iki katmana (sahte taşıma katmanı ve uygulama katmanı) çerçeveyi devreder. Alan uzunluğu geri kalan bayt sayısını verir. CRC hariç veri bölümünün (data section) en fazla uzunluğu 250 bayttır (Her 16 baytlık veri için 16 bitlik CRC alanı – 282 bayt). Bu yüzden veri bağlantı çerçevesi en fazla 292 bayttır.

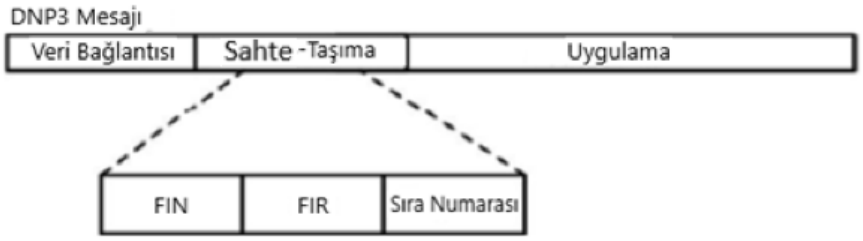


Şekil 3.11. DNP3 veri bağı katmanı çerçeve yapısı [78]

Başlık bölümü çerçevenin başlangıcını belirtmek için sabit bir dizi olan "start bit"ten oluşur. 0x05 ve 0x64 2 baytlık değerlerden oluşur. Bağlantı kontrol alanının fonksiyonları çerçevelerin sıralamasının temini, kontrol mesajı akışı ve aynı zamanda çerçeve fonksiyonunun tespitine yardım eder. Kontrol alanındaki veri, cihazın master veya saha cihazı olup olmadığının tespit edilmesine yardım eder ve işleme hangisinin başladığını ve iki cihaz arasında mantıksal bağlantı kurulmasını sağlar. Veri bağlantı katmanında 16 bitlik hedef adres gönderilmek istenen adresi barındırır, 16 bitlik kaynak adresi orijini tanımlar. 16 bitlik CRC transmisyonun bütünlüğünü doğrulamak için başlık alanında bulunur.

DNP3 sahte taşıma katmanı

Sahte taşıma katmanının işlevleri, paketlerin parçalanması ve yeniden birleştirilmesidir. Bu durum uygulama katmanının veri bağlantı katmanının taşıyabileceğinden daha fazla çerçeveyi almasına imkan sağlar. Böylece uygulama katmanı çerçeveleri birden fazla çerçeve içinde ayrıntılandırılır. Şekil 3.12'de gösterildiği gibi sahte taşıma katmanında 2 baytlık "start" ve "end" çerçeveleri bulunur. Her biri 1 bayttır ve "FIR" ve "FIN" isimli bayrakları bulundurur. Bu bayraklar parçalanan mesajların sırasıyla ilk ve son çerçevelerini gösterir. Her bir başarılı çerçeve için gösterilen sıra numarası (Sequence number), uygulama katmanı tarafından işleme için mesajların yeniden birleştirilmesi amacıyla kullanılır [79].

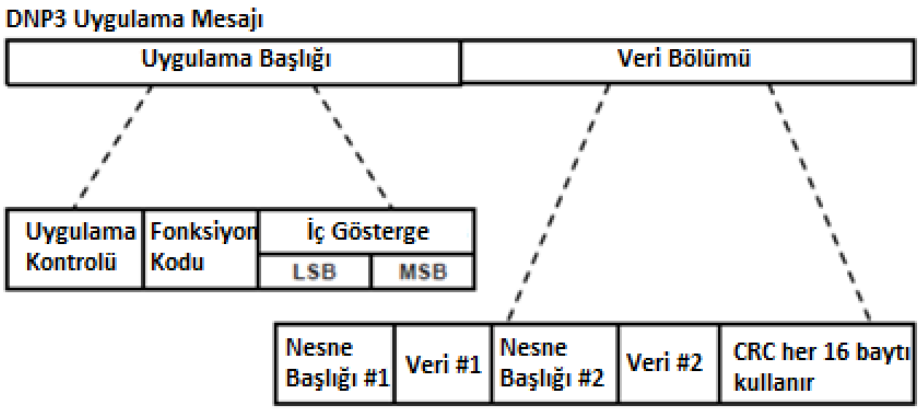


Şekil 3.12. DNP3 sahte taşıma mesajı alanları

DNP3 uygulama katmanı

Uygulama katmanının temel fonksiyonu her bir cihaz için master veya köle olup olmadığının tanımını vermektir. DNP3 istek ve yanıt mesajları için formatları gönderir. İstek mesajı masterdan saha cihazına bazı hesaplamaları veya limit ayarlarını düzenlemek gibi görevleri yerine getirmek için gönderilir. Bu katmanda mesajlar alıcının bellek boyutu tarafından belirlenen maksimum parçalanma boyutunu aştığında daha küçük paketlere bölünür. Normal parçalanma boyutu 2048 – 4096 bayt arasındadır.

Şekil 3.13 uygulama katmanı başlığını göstermektedir. Uygulama kontrol alanı sahte taşıma katmanındaki mesajların ilk ve son segmentleri gönderen fonksiyonla aynıdır. Fonksiyon kodu alanı, mesajın amacının ne olduğu bilgisini taşır. Bu alan istek ve yanıt mesajların her ikisinde de bulunur fakat işlevselliklerinin farklı olmasından dolayı fonksiyon kodlarının kullanımı farklıdır. İstek mesajları için toplamda 23 tanımlı fonksiyon kodu mevcuttur. Bunlar transfer fonksiyonu, kontrol fonksiyonu, donma fonksiyonu, uygulama kontrol fonksiyonu, yapılandırma fonksiyonu ve zaman senkronizasyon fonksiyonu olmak üzere sınıflandırılabilir. Fonksiyon kodunu belirlemek için 2 baytlık iç gösterge (internal indicator) başlığı vardır. Sıradaki başlık, kodlanmış veri sunumlarını ileten veri objeleridir (data objects). Tanımlanan birçok veri objesi vardır, böylece birçok sistemle arayüz kurabilir ve binary girdi, binary çıktı, analog girdi ve analog çıktı gibi çeşitli değişkenle haberleşebilir [79]. DNP3 protokolünün kullandığı fonksiyon kodları Çizelge 3.1'de verilmiştir.



Şekil 3.13. DNP3 uygulama katmanı başlığı

Çizelge 3.1. DNP3 fonksiyon kodları

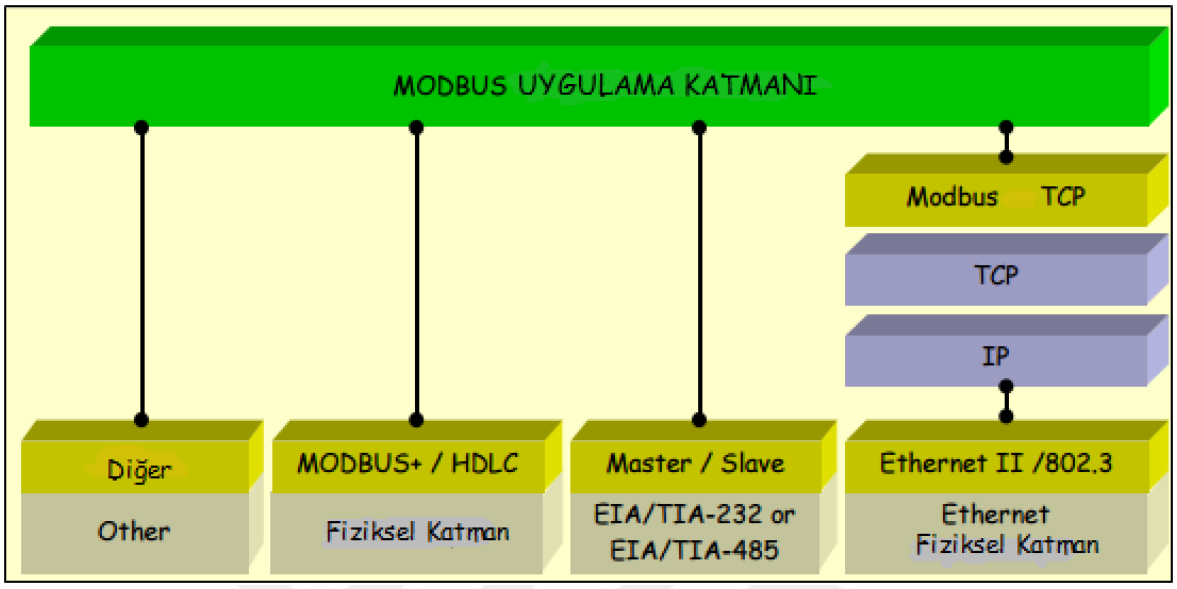
Fonksiyon Kodu	Açıklama	Fonksiyon Kodu	Açıklama
0	Doğrula	10	Uygulamayı başlat
1	Oku	11	Uygulamayı başlat
2	Yaz	12	Uygulamayı durdur
3	Seç	13	Yapılandırmayı kaydet
4	İşlet	14	İstenilmeyenleri etkinleştir
5	Doğrudan onay ile işlet	15	İstenilmeyenleri etkinleştirme
6	Doğrudan onay olmadan işlet	16	Sınıf ata
7	Onay ile işlemi dondur	17	Zaman gecikmesi hesapla
8	Onay olmadan aniden işlemi dondur	18	Mevcut zamanı kaydet
9	Onay ile işlemi dondur ve temizle	19	Dosya aç
A	Onay olmadan işlemi dondur ve temizle	1A	Dosya kapat
B	Zamanında dondur	1B	Dosya sil
C	Onay olmadan zamanında dondur	1C	Dosya bilgisi getir
D	Soğuk yeniden başlatma	1D	Dosyayı kimliklendir
E	Sıcak yeniden başlatma	1E	Dosyayı iptal et
F	Veriyi başlat		

Modbus protokolü

Modbus protokolü SCADA'ya özel geliştirilmiş ve endüstriyel standart haline gelmeye başlamış bir protokoldür. Birçok üretici bu protokolü kullanmakta, sistemlerini geliştirmekte ve cihaz üretimi yapmaktadır [80]. Modbus farklı tip ağlarda bağlı cihazlar arasındaki istemci/sunucu haberleşmesi için uygulama katmanı mesajlaşma protokolüdür. Şekil 3.14'te Modbus haberleşme yapısı verilmiştir. Günümüz uygulamalarında şu şekilde kullanılmaktadır:

- Ethernet üzerinden TCP/IP tabanlı haberleşme,
- Farklı ortamlar üzerinden (kablo: EIA/TIA-232-E, EIA-422, EIA/TIA-485-A, fiber optik, radyo,…) asenkron seri haberleşme,

- Modbus Plus, yüksek hızlı andaç geçirme (token passing) ağı üzerinden haberleşme sağlar.



Şekil 3.14. Modbus haberleşme yapısı [80]

Modbus protokolü, istek mesajını belirli RTU'a gönderdiği ve yanıt olarak geri gönderdiği master/slave (usta/köle) prensibine göre çalışmaktadır. Eğer yayın tipindeyse hiçbir yanıt almaz. Veriler, ASCII - okunabilir ve RTU – sıkı ve hızlı olmak üzere iki transmisyon modunda gönderilip alınabilir. RTU, daha kısa çerçeveye sahip olmasından ve eşlik denetimi, hata denetimi veya CRC olmasından dolayı tercih edilmektedir. ASCII modun daha uzun mesaj çerçevesine sahip olmasından dolayı sistemi yavaşlatmaktadır. Modbus protokolü, Modbus Serial ve Modbus TCP olmak üzere iki adet değişkeni vardır. IP bağlantılı ağlarda çalışan Modbus TCP, mastera çoklu üstün işlem özelliğine olanak sağlar ve RTU'a çoklu sunucudan paralel işlem çalıştırmasına imkan verir. Modbus protokolünün temel fonksiyonları aşağıdaki gibidir:

- Okuma için kontrol sargısı komutları ve tekli veya grup sargı ayarlamaları
- Girdi gruplarının giriş durumlarını okumak için girdi kontrol komutları
- Bekleyen yazmaçları okumak ve ayarlamak için yazmaç kontrol komutları
- Hata bulma testi ve fonksiyon raporu
- Program fonksiyonları
- Sorgulama kontrol fonksiyonları
- Sıfırlama

Modbus özellikleri

Modbus protokolünün mesaj yapısı Şekil 3.15'de gösterilmiştir.

Adres	Fonksiyon	Veri	CRC Kontrolü
8 bit	8 bit	N x 8 bit	16 bit

Şekil 3.15. Modbus mesaj yapısı

Mesaj yapısının ilk alanı adresin depolandığı tek baytlık alandır. İstek çerçevesinde hedef adresin IP adresi, yanıt çerçevesinde masterın IP adresi bulunur. Modbus protokolü en fazla 248 köle cihazına sahip olabilir fakat pratikte tek bir master, 2 veya 3 köle cihazla bağlantılıdır. İkinci alan hedef cihazda uygulanacak fonksiyonları barındırır. İstek çerçevesinde bu bayt uygulanacak hedefin fonksiyonunu tanımlar. İstek hedef istasyonda başarılı bir şekilde tamamlanırsa fonksiyon alanı geri çağrılır diğer türlü başarısız olunursa en soldaki bit gönderilir, böylece problemli yanıt döner. Üçüncü alan veri bölümü olup fonksiyon kodundaki değişkendir. Son iki bayt çerçevedeki hata denetimi için CRC alanıdır. Fonksiyon kodlarının bulunduğu fonksiyon alanı Çizelge 3.2'de gösterilmiştir.

Çizelge 3.2. Modbus protokol çerçevesindeki fonksiyon kodları

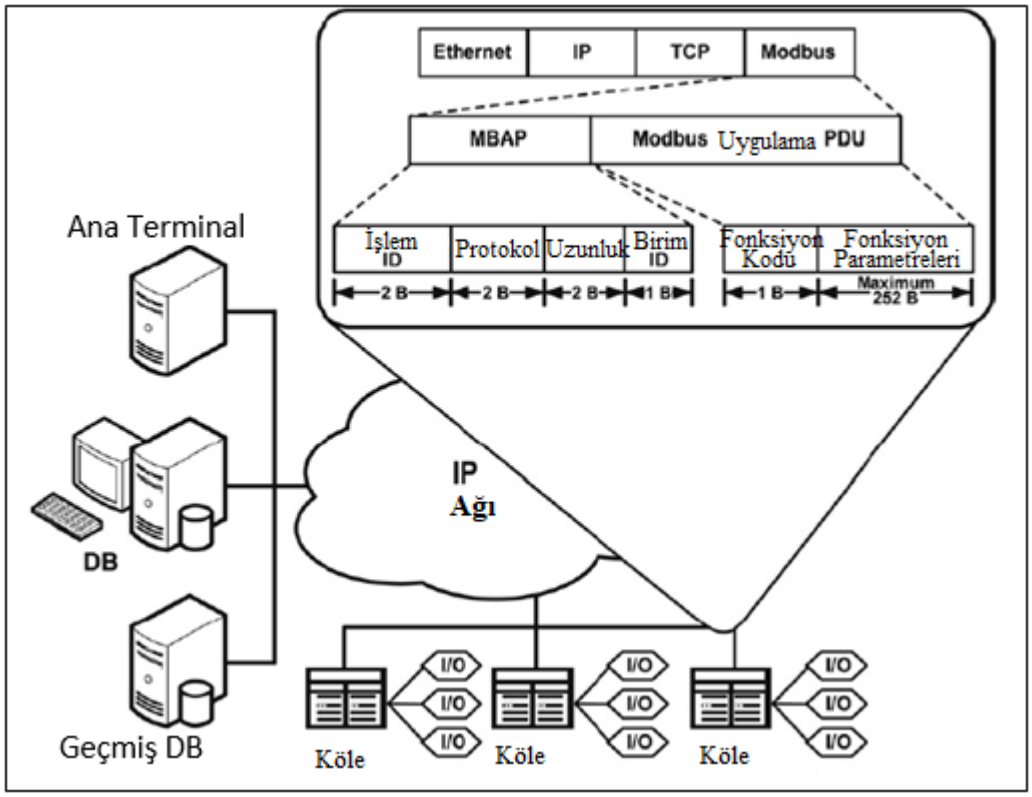
Kod	Hex	Fonksiyon	Tipi	
01	01	Sarmalları oku	Tek bit erişimi	Veri erişimi
02	02	Ayrık girişleri oku		
05	05	Tekli sarmala yaz		
15	0F	Çoklu sarmala yaz		
03	03	Bekletme yazmaçlarını oku	16 bit erişimi	
04	04	Giriş yazmaçlarını oku		
06	06	Tekli yazmaca yaz		
16	10	Çoklu yazmaca yaz		
22	16	Yazmaca yazmayı maskele		
23	17	Çoklu yazmaçları oku/yaz		

Çizelge 3.2. (devam) Modbus protokol çerçevesindeki fonksiyon kodları

24	18	FIFO sorgusunu oku		
20	14	Dosya kaydını oku	Dosya Kaydı erişimi	
21	15	Dosya kaydını yaz	Arıza Tespitleri	
07	07	İstisnai durumu oku		
08	08	Arıza tespit		
11	0B	Haberleşme olay sayacını al		
12	0C	Haberleşme olay kaydını al		
17	11	Sunucu ID raporla		

Modbus TCP protokolü

Bu protokol hem IP tabanlı hem LAN tabanlı ağlarda çalışır. Şekil 3.16'da ana cihaz IP tabanlı ağ üzerinden birçok köle cihaza bağlı olduğu gösterilmiştir. Modbus TCP protokolünde, köle cihaz sadece pasif işlemler yaptığı için ana cihaz istemci olarak tasarlandığında köle cihaz sunucu olarak tasarlanır.



Şekil 3.16. Modbus TCP mimarisi [80]

Modbus TCP protokolü mesajlarını TCP paketlerinde kapsüllediğinden dolayı TCP PDU (Protocol Data Unit), Modbus uygulama protokolünü (MBAP) barındırır. MBAP başlığı; işlem tanımlayıcı, protokol tanımlayıcı, uzunluk ve birim tanımlayıcı olmak üzere dört alan barındırır. İstek ve yanıtların çiftli eşleştirilmesi işlem tanımlayıcısı tarafından gerçekleştirilirken protokol tanımlayıcısı MBAP başlığı (Modbus için 0) tarafından kapsüllenen uygulama protokolünü gösterir. Birim tanımlayıcısı, işlemle ilgili köle cihazları gösterir ve sadece legal sistemleri için kullanılır. Uzunluk alanı veri paketinin kalan bayt miktarını gösterir.

Profinet protokolü

Profinet, Dünya Profibus Birliği, Profinet üreticileri ve kullanıcıları tarafından geliştirilen açık endüstriyel Ethernet standardıdır. Profinet IEC 61158 ve IEC 61784'te standartlaştırılmıştır. Profinet gerçek-zamanlı gereksinimleri geniş bir yelpazedeki uygulamaları kapsar.

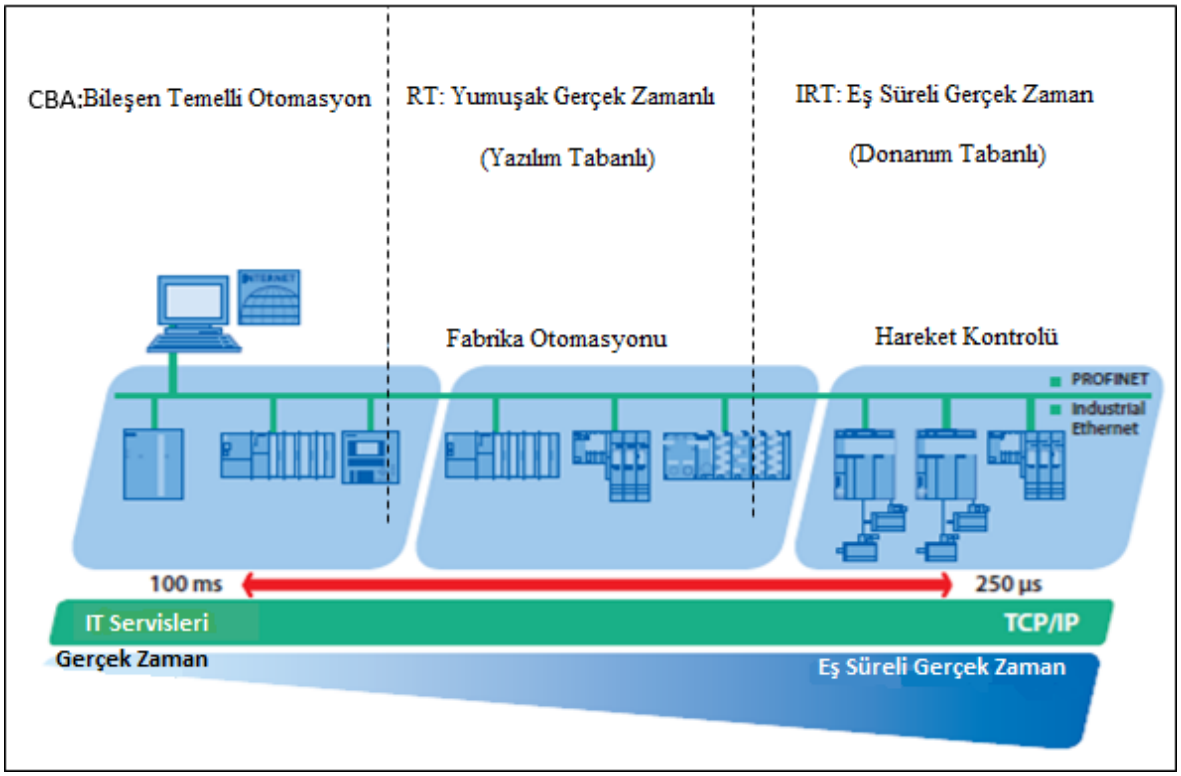
Profinet en çok kullanılan saha haberleşme standartlarından Profibus'ın devamı niteliğindedir. Profibus 25 yıldan fazla süredir kullanılan seri endüstriyel haberleşme standardıdır. Günümüzde Profibus'ın iki varyasyonu kullanılmaktadır. Bunlardan en sık karşılaşılanı Profibus DP (Decentrilized Peripherals – Merkezi Olmayan Çevre Birimi); basit, düşük maliyetli, yüksek hızlı haberleşme özelliklerine sahiptir. Diğer varyasyon Profibus PA (Process Automation – İşlem Otomasyonu); daha çok uygulama tabanlı teknolojidir. Profibus master/slave haberleşme teknolojisini ana cihazlar arasında andaç geçirme ile birlikte kullanmaktadır [73].

Bütün Profinet cihazları endüstriyel çevredeki işlemlere göre aktif ve pasif olarak tasarlanmıştır. Gerçek-zamanlı gereksinimlerde kullanılan ağ cihazları olarak da kullanılabilmektedir.

Profinet'in gelişimi 2000 yılının başlarında başlamış ve ilk teknik özelliği Profinet CBA (component-based automation) olarak yayımlanmıştır. Profinet CBA TCP/IP üzerinden makinadan makinaya haberleşen ve nesne tabanlı programdır. Ayrıca tüm ağ cihazlarıyla uyumludur. Diğer Profinet versiyonu Profinet RT ve Profinet IRT bulunduran Profinet IO'dur.

Profinet versiyonları

Profinet IO ve Profinet CBA olmak üzere Profinet'in bu iki versiyonu denetleyici ve IO cihazları arasındaki haberleşme için tasarlanmıştır Şekil 3.17'de Profinet versiyonlarının gerçek-zaman gereksinimleri gösterilmiştir.



Şekil 3.17. Profinet versiyonların gerçek-zaman gereksinimleri [81]

Şekil 3.17'den fark edildiği üzere Profinet CBA temel olarak Gerçek-Zamanlı olmayan ortamlarda kullanılırken Profinet RT fabrika ve işlem otomasyonunda ve Profinet IRT montaj hatlarındaki robotlarda olduğu gibi en çok talep alan hareket kontrol uygulamalarında kullanılmaktadır.

Profinet CBA

Profinet Sınıf A olarak da bilinen Profinet CBA TCP/IP, üzerinden makinadan makinaya haberleşmek için tasarlanan nesne tabanlı programdır. Profinet CBA'nın arkasındaki temel düşünce, denetleyiciler üzerinden birbiriyle haberleşebilen akıllı ve otonom alt sistemlerin uygulanabilmesidir.

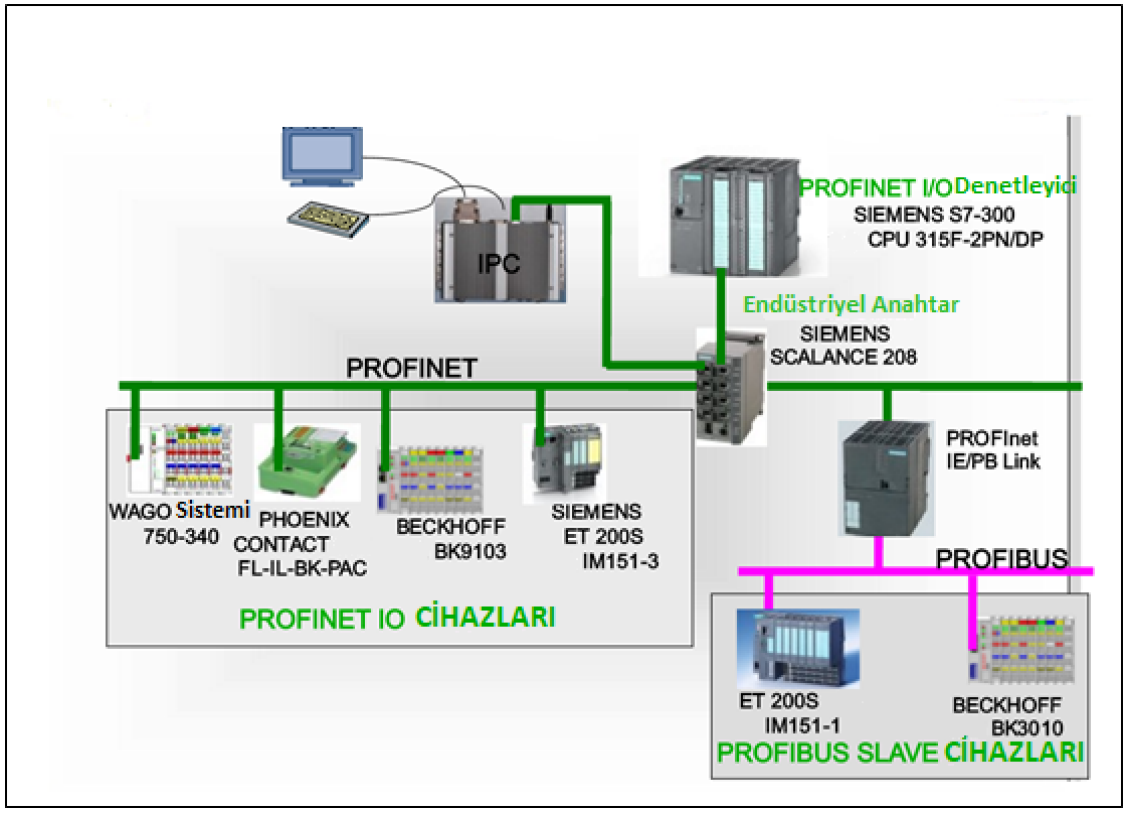
Profinet CBA 10 milisaniyelik tepki süreleriyle döngüsel ve döngüsel olmayan haberleşme kullanan otomasyon konseptidir. Sadece TCP/IP haberleşmesi kullanıldığında Profinet CBA 100 milisaniye ve üzeri tepki süresiyle sistemleri destekler [81].

Profinet IO

Direk olarak Ethernete bağlı dağıtık I/O cihazlarını kullanan Profinet sistemleri Profinet IO olarak isimlendirilir. Üreticinin tüketicide işlenecek veriyi gönderdiği üretici/tüketici modeli kullanılır. Şekil 3.18'de Profinet'in kullandığı bu modelden bahsedilmiştir.

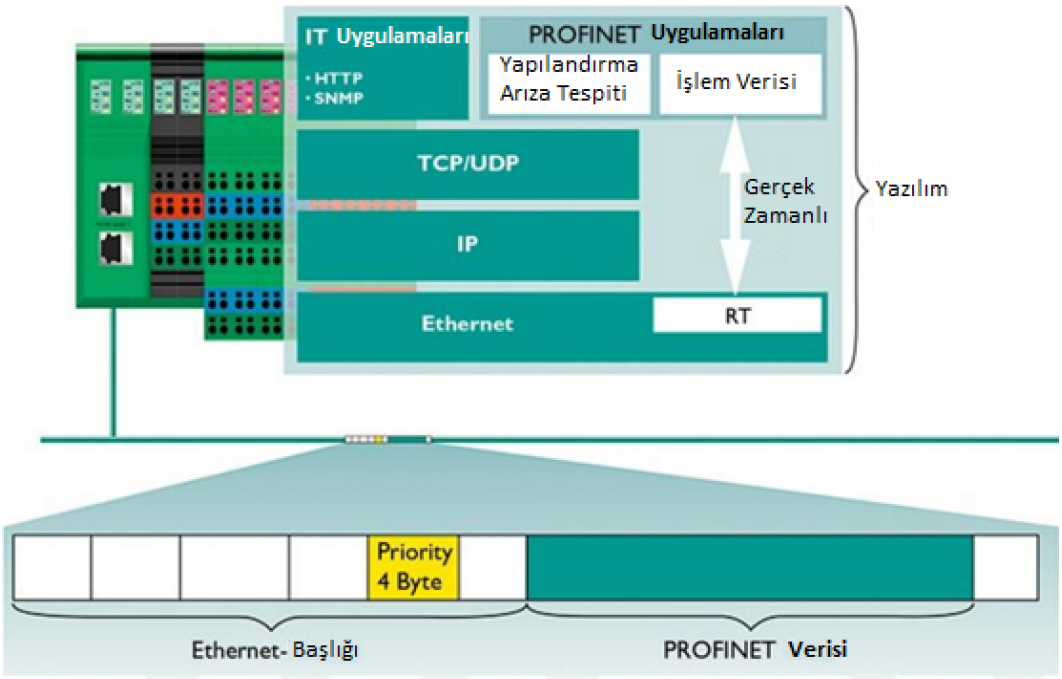
IO denetleyici PLC gibi otomasyon programlarının olduğu cihazlardır. IO cihazlarının çıktıları IO denetleyiciler tarafından yönetilir. IO cihazı bir veya daha fazla IO denetleyicinin Profinet IO üzerinden bağlı olduğu dağıtık I/O saha cihazı olarak çalışır.

IO yönetici programı hata mesajları ve parametrelendirme için mühendislik aracı gibi kullanılır. IO yönetici programı, devreye alma veya hata tanılama amaçları için bir bilgisayar veya HMI olabilir [82].



Şekil 3.18. Profinet IO için haberleşme yolu [82]

Profinet Sınıf B olarak bilinen Profinet RT'de veri haberleşmesi işlemi TCP/IP'e paralel olarak OSI katman 3 ve katman 4 üzerinden gerçekleşir. Her cihaz, HTTP gibi diğer protokoller üzerinden haberleşmeye izin veren TCP/IP aracılığıyla IP adresi alır. Şekil 3.19'da Profinet RT haberleşmesinde Ethernet çerçeve ve protokol yapısı gösterilmiştir.



Şekil 3.19. Profinet RT veri transferinde ethernet çerçevesi [82]

Ethernet çerçevesi, Ethernet başlığı ve Profinet veri kısımlarından oluşmaktadır. Profinet gerçek zamanlı mesajlarının önceliklendirme etiketi Ethernet başlığında bulunmaktadır [83]. Önceliklendirme, VLAN ID 0 ve öncelik sırası 6 olarak atanmasıyla uygulanır. Ethernet tipi 0x8892 olacak şekilde Profinet RT veya IRT ile haberleştiğini gösterir.

Profinet Sınıf C olarak bilinen Profinet IRT hareket kontrol uygulamaları gibi gerçek zaman işlemlerinin en fazla ihtiyaç duyulduğu zamanlarda kullanılırlar. Özellikleri Profinet RT ile aynıdır fakat gerçek zaman performansı bakımından özel bir donanımla artırılmıştır.

Profinet IRT, zaman dilimi gibi teknoloji kullanarak haberleşmesini senkronize etmek amacıyla Profinet ağındaki cihazlara imkan verir. Buradaki zaman dilimi teknolojisi, her haberleşme döngüsünde IRT veri ve saat sinyali için bir slot belirtir.

Profinet IRT ve RT haberleşmeleri OSI katman 3 ve katman 4 protokol yapısını kullanır. Böylece bütün TCP/IP protokol yapısı atlatılır ve IP adresi almaz. Diğer bir deyişle RT ve IRT haberleşmeleri tek bir mantıksal subnetle sınırlandırılmıştır.

Bu bölümde, SCADA sistemini oluşturan MTU, RTU, PLC cihazının yazılım ve donanım mimarisi ve EKS sistemlerinde en sık kullanılan haberleşme protokollerinden DNP3, Modbus ve Profinet bileşenlerinden bahsedilmiştir. Yapılan incelemeye göre Modbus, EKS sistemlerinde en sık rastlanan protokollerin başında olup bu protokolü kullanan SCADA sistemlerine yönelik tehditler sonucu oluşacak riskler geniş alanlara etki edebilmektedir. Bu riski azaltmak için tez çalışmasında Modbus protokolünün güvenliği ele alınmıştır.

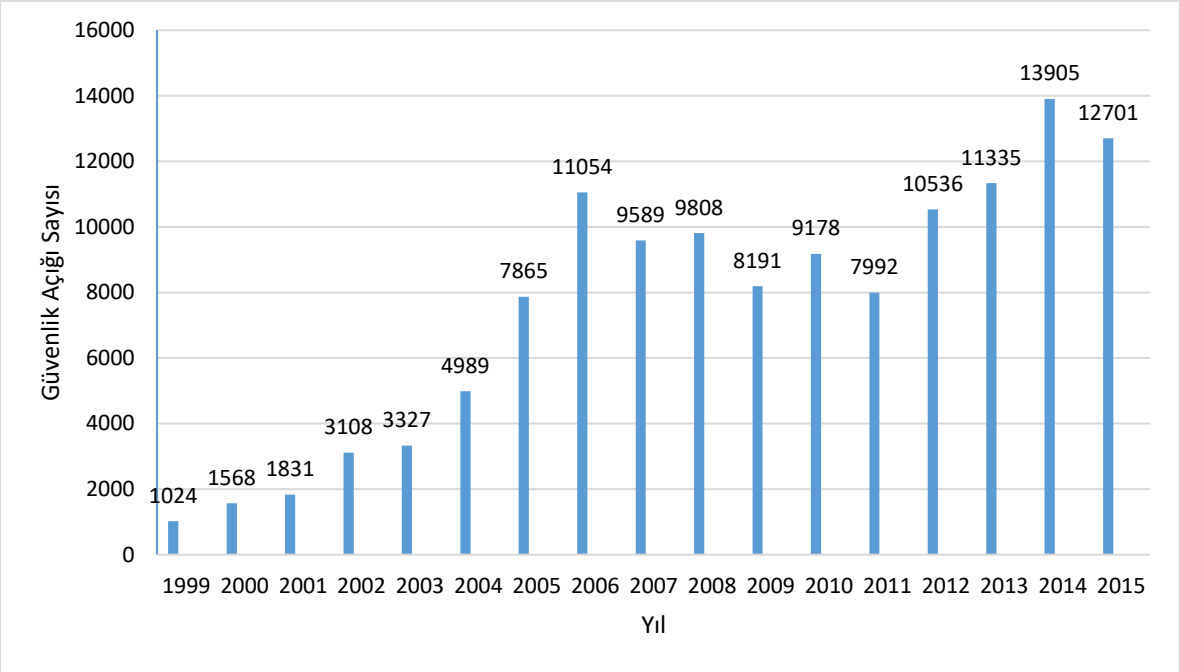
4. SCADA SİSTEMLERİ VE SİBER GÜVENLİK

SCADA sistemi bağımsız bir birim olarak işlenecek şekilde tasarlanmasına rağmen kurumsal bir ortamda çalışır. Kontrol sistemi tasarımının en önemli amacı verimlilik ve güvenliktir. SCADA sistemlerinde görülen bir diğer durum rutin olarak bakım işlemlerini gerçekleştirmek için uzaktan erişim sağlamaktır. SCADA haberleşme protokolleri tasarlanırken güvenlik özellikleri geri planda tutulmuştur. Kritik altyapılardaki bu gibi güvenlik açıkları kritik altyapıları siber saldırılara karşı daha hassas duruma getirmiştir. Saldırganlar, saldırılarını bu güvenlik açıklarını sömürerek gerçekleştirir. Bu saldırıların etkileri ve sonuçlarına aşağıda değinilmiştir [12]:

- Fiziksel etki: SCADA sisteminin işlevsiz kalmasının sonuçları bu alanda değerlendirilir. Bu etkinin en önemli sonucu insan hayatını tehlikeye atacak sonuçlarının olmasıdır. Diğer sonuçlarında veri kaybı ve çevreye olan zararlarıdır.
- Ekonomik etkileri: Ekonomik etkiler siber saldırıdan sonra ortaya çıkar. Fiziksel etkinin dalgalanma etkisi tesis veya firmada ciddi ekonomik kayıpları beraberinde getirir. Daha büyük etkisi yerel, ulusal hatta küresel ekonomi üzerinde ekonomik kayıplara neden olmasıdır.
- Sosyal etkileri: Fiziksel ve ekonomik hasarların sonucu kamu güveni ve ulusal güvenliğin zarar görmesi olacaktır. Sosyal etkiler kamu güvenliğini depresif bir hale getirebilir ya da popüler aşırılığın artmasına sebep olabilir.

Yaygın olarak görülen güvenlik tehditleri ve saldırılarında ortaya çıkan sonuçların büyüklüğünden dolayı daha güvenli bir SCADA sistemi geliştirmek amacıyla çeşitli kurum ve kuruluşlar SCADA sistemlerine yönelik saldırılara karşı kapsamlı çalışma ve araştırmalar yapmaktadır.

Literatürde SCADA sistemlerinde tespit edilen güvenlik açıklarının en güncel istatistiği Şekil 4.1 verilmiş olup bilgi sistemlerinde oluşan güvenlik açıklarının ciddi oranda artış gösterdiği anlaşılmaktadır. Son 15 yılda tespit edilen güvenlik açıklarında yaklaşık 12 kat büyüme olduğu fark edilmiştir. Bilgi teknolojileriyle entegre çalışan SCADA sistemleri de direk olarak bu tehditten etkilenmektedir.



Şekil 4.1. Yıllar bazında güvenlik açığındaki değişim [84]

SCADA sistemleriyle ilgili "SCADA sistemleri fiziksel olarak birbirinden ayrı ve bağımsızdır" düşüncesi genel bir yanlış düşüncedir. Birçok SCADA sistemi ağ bileşenlerinden önce yapılmış ve ağın geri kalanından ayrı tasarlanmıştır, bu durum sistem yöneticilerini diğer kurumsal ağlardan veya erişim noktalarından bu sistemlere erişim olamayacağı düşüncesine inandırmıştır. Maalesef bu düşünce tamamen yanlıştır. Gerçek senaryoda SCADA ağı ve kurumsal ağlar bilgi yönetiminde oluşan değişikliklerden dolayı köprülüdür. Bu değişikliklerde önemli rol oynayanlar aşağıda açıklanmıştır [85]:

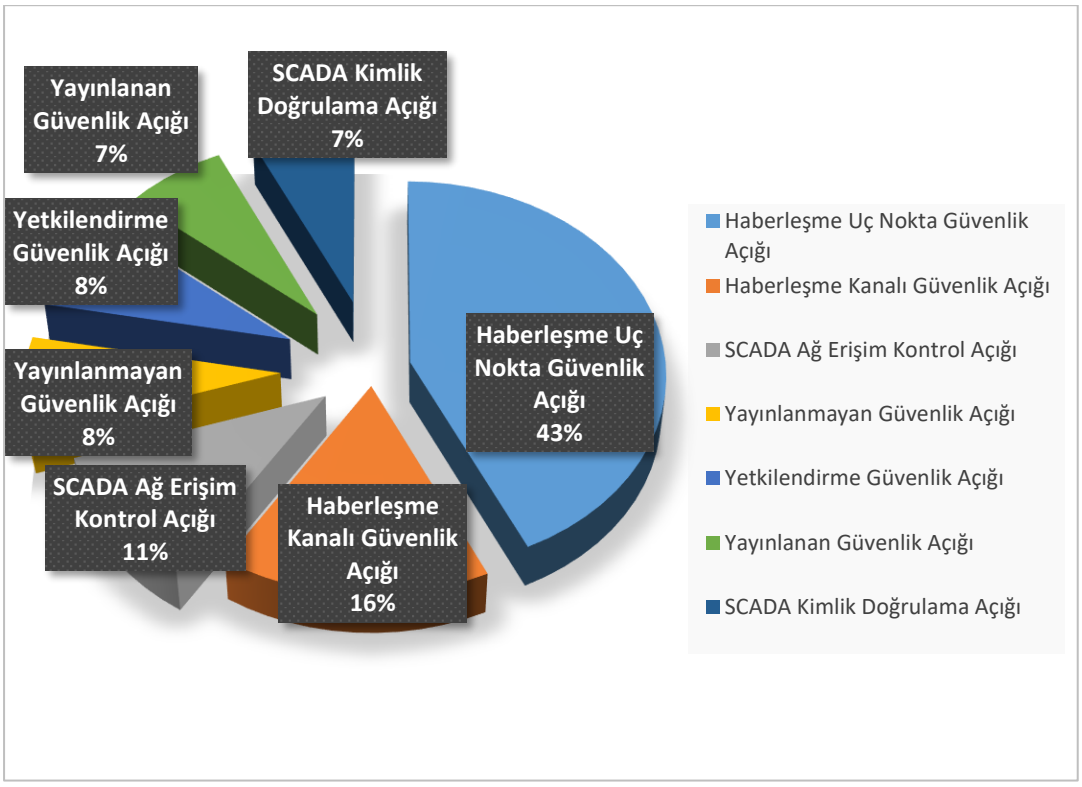
- İlk değişiklik, kurumsal ağda erişim noktasından sistemi uzaktan izleme ve denetleme için SCADA mühendislerine sisteme bağlantı kurmasına olanak sağlayan artan taleptir.
- İkinci temel sebebi kurumsal bir karara yardımcı olmak amacıyla bilgi erişimidir. Birçok kamu kurumunun kritik bilgilere ve işlevsel durumu daha yüksek bir yönetim için veya kurumsal karar almak için ani erişim yapması gibi SCADA sistemlerine kurumsal bağlantı izni vardır.

SCADA sistemleriyle ilgili bir diğer büyük yanlış düşünce; "SCADA sistemleri ve diğer kurumsal ağlar arasındaki bağlantı güçlü bir erişim kontrolüyle korunur" dur. Kurumsal ağ ve SCADA sistemleri arasındaki birçok bağlantı, farklı bağlantı standartları ile sistem entegrasyonuna ihtiyaç duyar. Ağ yöneticilerinin ağ erişim anahtarlarını göz ardı etmesi

nedeniyle kurumsal ağlar üzerinden yetkisiz erişim SCADA sistemi koruması için tasarlanan erişim kontrolü genelde asgari düzeydedir. Güvenlik duvarları ve saldırı tespit sistemlerinin (STS) güçlü parola koruması ile kullanımı tavsiye edilir.

4.1. SCADA Sistemi Güvenlik Açıkları

Idaho Ulusal Laboratuvarı'nın (INL) ABD Enerji Bakanlığı Elektrik Dağıtımı ve Enerji Güvenliği Dairesi'ne sunduğu raporda [86] Ulusal SCADA Test Düzeneği (NSTB) programıyla ulusal enerji altyapısının siber saldırılar karşısında güvenliğinin ve esnekliğinin sağlanması hedeflenmiştir. Bu programın temel amacı SCADA sistemlerindeki güvenlik açıklarını analiz ederek saldırı etkisini hafifletme yaklaşımlarını tanımlayıp saldırılara karşı önlem almaktır. Raporda SCADA sistemine yönelik gerçekleştirilen siber saldırılarda istismar edilen güvenlik açıkları sınıflandırılmış ve analiz edilmiştir. İlgili raporun 2011 yılında yayımlanmış olmasına rağmen, içerdiği bilgiler ve elde edilen sonuçlar literatürdeki SCADA sistemlerinin siber güvenliği ile ilgili teknik çalışmalar içerisinde en kapsamlı olmasından ötürü bu tez çalışmasında ilgili yerlerde bu rapordan faydalanılmıştır. Şekil 4.2'de NSTB'e göre gözlemlenen güvenlik açıklarının çeşitlerine göre yüzdeleri verilmiştir.



Şekil 4.2. NSTB SCADA güvenlik açığı sıklığı [86]

Şekil 4.2'de gösterilen güvenlik açıklarından birçoğu buffer overflow (bellek taşması)'dır. Örneğin gösterilen bir uygulamada 50 saldırı vektöründen 50'sinde bellek taşması tespit edilmiş ve bunların hepsi tek bir güvenlik açığı olarak hesaplanmıştır. Tek bir kimlik doğrulama atlatma tekniği de bir güvenlik açığı olarak hesaplanmıştır.

SCADA sistemlerinde tek bir güvenlik açığı diğer sistemlere oranla çok daha fazla kritik veya geniş kapsamlı olabilir. Örneğin, bir SCADA protokolündeki bir haberleşme kanalının güvenlik açığı tüm sistemi etkileyebilmekte ve bu bir zafiyet olarak sayılmaktadır.

Değerlendirme ekibinin ve SCADA üreticilerinin deneyimiyle belirlenen NSTB değerlendirmeleri SCADA sistemini ele geçirme olasılığı ve etkisi bazında değerlendirme hedeflerine (Kontrol sistemi üzerinde ciddi etkilere sebep olan giriş noktası, işlemler, protokoller,…) öncelik verilmiştir. Çizelge 4.1'de SCADA güvenlik açığı tipleri ve temel SCADA fonksiyonlarına erişebilen ilgili değerlendirme hedefleri açıklanmıştır.

Çizelge 4.1. Temel SCADA fonksiyonlarına erişebilen açıklıklar ve ilgili değerlendirme hedefleri [86]

Güvenlik Açığı Tipi	Değerlendirme Hedefi Kategorisi	Güvenlik Açığı Kaynağı
Bilinen Güvenlik Açıkları	En Muhtemel Saldırı Yolları	SCADA ürünlerine eklenmiş eski veya yamasız üçüncü parti uygulamaları
		SCADA Sunucuları üzerinde koşan yamasız İşletim Sistemleri
Yayınlanmayan Güvenlik Açıkları	Potansiyel 0-gün veya Yamalanmamış Güvenlik Açıkları	Gereksiz Servisler üzerinden SCADA Sunucusunu açıkta bırakma
		Hatalı SCADA Kodu
Haberleşme Kanalı Güvenlik Açıkları	Güvenlik Açığı olan Haberleşme Kanalı üzerinden SCADA İşlevselliğine Yetkisiz Erişim	Spoofing ve araya girme saldırılarına karşı zafiyet barındıran uzaktan erişim protokolleri
Haberleşme Son Nokta Güvenlik Açıkları	SCADA Sunucularına veya Uygulamalarına Yetkisiz Erişim veya DoS	SCADA Haberleşmesi ve veri transferi protokolleri için zafiyet barındıran Sunucu Uygulamaları
		Veri Tabanı Güvenlik Açıkları

Çizelge 4.1. (devam) Temel SCADA fonksiyonlarına erişebilen açıklıklar ve ilgili değerlendirme hedefleri [86]

		Web Güvenlik Açıkları
SCADA Uygulama, Kimlik Doğrulama Açıkları	Kimlik Doğrulama Mekanizmasını İstismar ederek SCADA Uygulamalarına Erişim	Kimlik Doğrulama Atlatma
		Kimlik Bilgileri Yönetimi
SCADA Sunucu Yetkilendirme Açıkları	SCADA Hesabından Sisteme Zarar verebilme	Sunucu yapılandırma güvenliğinde yapılan hata
SCADA Ağı Güvenlik Açıkları	Uygun Ağ Yolları üzerinden SCADA Sunucularına ve İşlevselliğine Erişim	Hatalı Ağ Tasarımı
		Zayıf Güvenlik Duvarı Kuralları
		Ağ Cihazı Yapılandırma Hataları
		Hatalı Ağ İzleme

NSTB değerlendirmesinin sonuçlarına göre SCADA fonksiyonlarını riske atan ve haberleşmesini engelleyebilen veya aksatabilen SCADA sunucularına, uygulamalarına veya verilerine yetkisiz erişim sağlayabilen güvenlik açıkları tanımlanıp analiz edilmiştir. Bu güvenlik açıkları aşağıdaki gibi açıklanmıştır.

4.1.1. Kaynak kodu tasarımı ve uygulaması

SCADA uygulamaları ve servislerindeki güvenlik açıklarını minimize etmek için güvenli kodlama yapılması gerekmektedir. Yazılımda oluşabilecek güvenlik açıkları kötücül amaçlar için istismar edilip SCADA sistemini saldırılara açık hale getirebilir, bu yüzden sistem yöneticileri ilk yapılandırmadan sonra yapacakları değişikliklerde tereddüt içinde olabilirler [87].

SCADA yazılım incelemeleri ve tersine mühendislik çalışmaları SCADA yazılımının her zaman güvenli bir konseptte yapılmadığını göstermektedir. NSTB değerlendirmelerinde gözlemlenen SCADA yazılım açıklarının güvensiz yazılım ve yeterli olmayan testler sonucunda oluştuğu ortaya çıkmıştır. Gözlemlenen en önemli üç açıklık; girdi doğrulaması, kimlik doğrulama ve erişim kontrolüdür. NSTB değerlendirmelerinde ortaya çıkan güvenlik açıklarının birçoğunda tehlikeli fonksiyonlara sebep olan uzaktan kod çalıştırılabilmektedir.

SCADA yazılımları büyük, karmaşık ve eski kod tabanlı olabilirler ve SCADA işlemleri yüksek kullanılabilirliğe ihtiyaç duyabilir ve güncelleme senaryoları karmaşık olabilir. Kullanıma hazır bilgisayar yazılım modeli standartlarının aksine güvenlik düzeltme

maliyeti, desteği ve bakımı SCADA kullanıcısına geleneksel olarak transfer olmuştur. SCADA ürün açıklarının yayınlanması SCADA güvenliği için yeni bir gereklilik ile SCADA üreticileri kod denetimi ve ilgili kod değişikliklerini bulabilirler.

Güvenli kod kaynakları tüm uygulama türleri ve dilleri için bulunabilir. CWE (Common Weakness Enumeration) listesi [88] bilinen birçok SCADA programlama hatalarının dahil olduğu tüm yazılım açıkları hakkındaki bilgiler Çizelge 4.2'de verilmiştir.

Çizelge 4.2. Güvenli olmayan SCADA kod tasarımı ve uygulamasıyla ilgili bilinen açıklıklar [10]

Açıklık Sınıflandırması	Bilinen Açıklıklar
CWE-19: Veri İşleme	CWE-228: Sözdizimsel geçersiz yapının hatalı işlenmesi
	CWE-229: Değerlerin hatalı işlenmesi
	CWE-20: Hatalı girdi doğrulama
	CWE-116: Hatalı kodlama
	CWE-198: Hatalı bayt sıralaması kullanımı
CWE-119: Bellek sınırı içinde sınırlama işlemi hatası	CWE-120: Giriş boyutu kontrolü olmadan bellek kopyalama (Klasik bellek taşırma)
	CWE-121: Stack-based (yığın tabanlı) bellek taşırma
	CWE-129: Dizi indeksini hatalı doğrulama
	CWE-190: Integer taşırma veya silme
	CWE-680: Integer veya bellek taşırma
CWE-398: Kötü kod kalitesi göstergesi	CWE-454:Güvenilir değişkenlerin veya verilerin dışarıdan başlatılması
	CWE-456: Eksik başlatma
	CWE-400: Kontrolsüz kaynak tüketimi
	CWE-252: Denetlenmeyen dönüş değeri
	CWE-772: Eksik kaynak yayınlanması
CWE-442: Web Problemleri	CWE-22: Kısıtlı bir dizine hatalı yol adı limitlemesi (Yol Geçişi)
	CWE-79: Web sayfası koruma alanı hatası (XSS)
	CWE-89: SQL sorgu yapısı koruma alanı hatası (SQL enjeksiyonu)

4.1.2. Bellek taşırma (Buffer Overflow)

Bellek taşırma açığı SCADA sistemlerinde en sık karşılaşılan girdi doğrulama zayıflığından kaynaklanmaktadır. Bellek taşırmalar yazılımın belleğe hafızada ayrılan boşluktan daha fazla veri yazılmasıyla oluşmaktadır. "Extra" veri, bitişik belleğin üzerine yazılır ve programın normal fonksiyonları dışında çalışmasına sebep olur. Dikkatlice planlanmış ve çalıştırılmış bellek yazma, programın saldırgan tarafından çalıştırabilmesine sebep olur. İstismar kodu interaktif bir oturum oluşturmak ve istismar edilmiş programın yetkileriyle kötücül komut göndermek için bellek taşmasını kullanır.

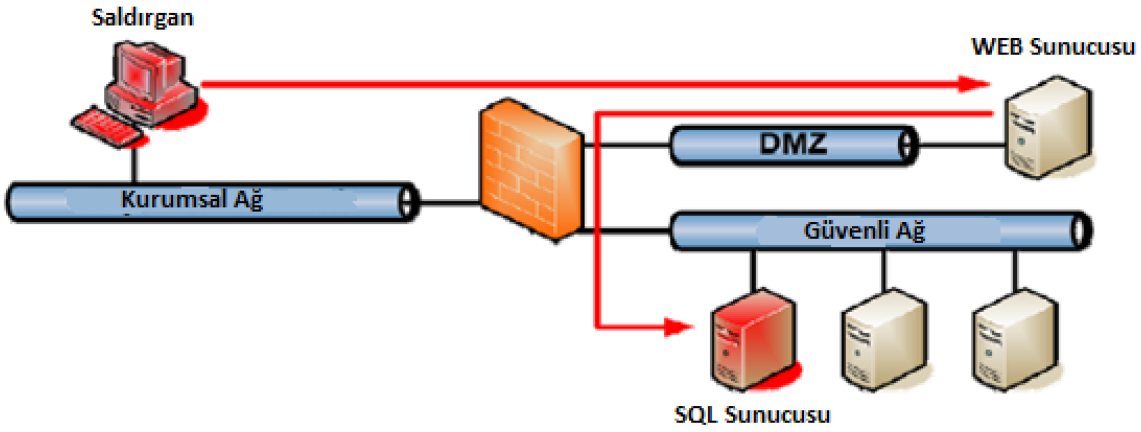
Bellek taşırma, ağ trafiği sürecindeki uygulamalarda veri transferi sırasında girdi değerlerinin durdurulup değiştirilerek istismar edilmesiyle gerçekleştirilir. Sonuç olarak, girdi değerlerinin doğrulamasının olmadığı ağ protokolü uygulamaları bellek taşırma saldırılarına karşı savunmasızdır [50]. Örneğin geliştirici, hiç kimsenin kullanıcı adı olarak 1024 karakterden daha uzun karakter yaratmayacağını düşünebilir. Geliştirici, kullanıcı adı için belleğe 1024 baytlık bir alan oluşturur ve girdi doğrulaması yapmazsa, bir saldırgan, 1024 karakterden daha fazlasını keşfetmek için birçok kullanıcı adını deneyebilir. Geliştirici, girdi alanında depolanan bellek için ayrılan boyutu aşmayacak şekilde girdi boyutunda doğrulama yaparak bu açığı kapatabilir.

4.1.3. SQL enjeksiyonu

SQL sorgu komutunda kullanılan özel karakterlerin bütünlüğünü garanti etmeyen kullanıcı girdilerinin hatalı veya yetersiz filtrelemesi sonucu oluşan SQL enjeksiyonu açığı SCADA geçmiş (historian) veri tabanına etki edebilir. Mesela, bir saldırgan bir veri tabanı sorgusuna hazır bilgi çıkış karakteri eklerse, saldırgan veri tabanına rasgele okuma/yazma erişimi sağlayabilir. SQL komutu veri tabanıyla haberleşmek için kullanılır. Aynı zamanda SQL sorguları kimlik doğrulama gibi güvenlik kontrolleri için kullanılabilir, saldırganlar güvenliği aşmak için bu sorgulardaki mantıklarda değişiklik yapabilir [89].

SQL enjeksiyonu açıkları istemci (genelde Web) uygulamaları üzerinde bulunur. SQL enjeksiyonu SQL komutlarını veri tabanına yönlendirerek veri tabanını istismar eder. Veri tabanı destekli uygulamalar güvenli ağ üzerinde sunucudan veri alabiliyorsa SQL enjeksiyon için bir hedeftir. Örneğin, bir istemci uygulaması Şekil 4.3'te gösterildiği gibi arındırılmış

bölge anlamına gelen ve dış ağlara açık servislerini içeren ve bu servisleri daha büyük güvensiz bir ağa (genellikle internet) maruz bırakan fiziksel veya mantıksal bir alt ağ olan DMZ'da yalıtılmış Web sunucusu üzerinden güvenli ağda veri tabanına bağlanırsa, SQL enjeksiyonu saldırıları SQL sunucusuna güvenli ağ üzerinden yapılabilir. Hatta güvenlik duvarı sunucuya olan diğer tüm bağlantıları engellese bile başarılı bir saldırı, saldırgana güvenli ağ üzerinden SQL sunucusunu kontrol etme olanağı sağlar.



Şekil 4.3. Web uygulamaları üzerinden SQL enjeksiyonu saldırısı [9]

4.1.4. XSS (Cross Site Scripting) açığı

XSS açıklığının temel sebebi SQL enjeksiyonunda olduğu gibi girdi doğrulama eksikliğinden kaynaklanmaktadır. Fakat, XSS saldırılarında web uygulaması kötücül kodu kullanıcıya gönderir. *2010 CWE/SANS En Tehlikeli 25 Programlama Hatası* raporunda [90] XSS en sık kullanılan ve kritik programlama hatası olarak yayımlanmıştır. Saldırgana güvenlik açığı olan web uygulaması ile oluşturulan web sayfasına kod yerleştirmeye olanak sağladığı için oldukça tehlikelidir. Saldırı kodu web sunucusu yetkisiyle kullanıcı tarafında çalıştırılır.

4.1.5. Gereksiz portlar ve servisler

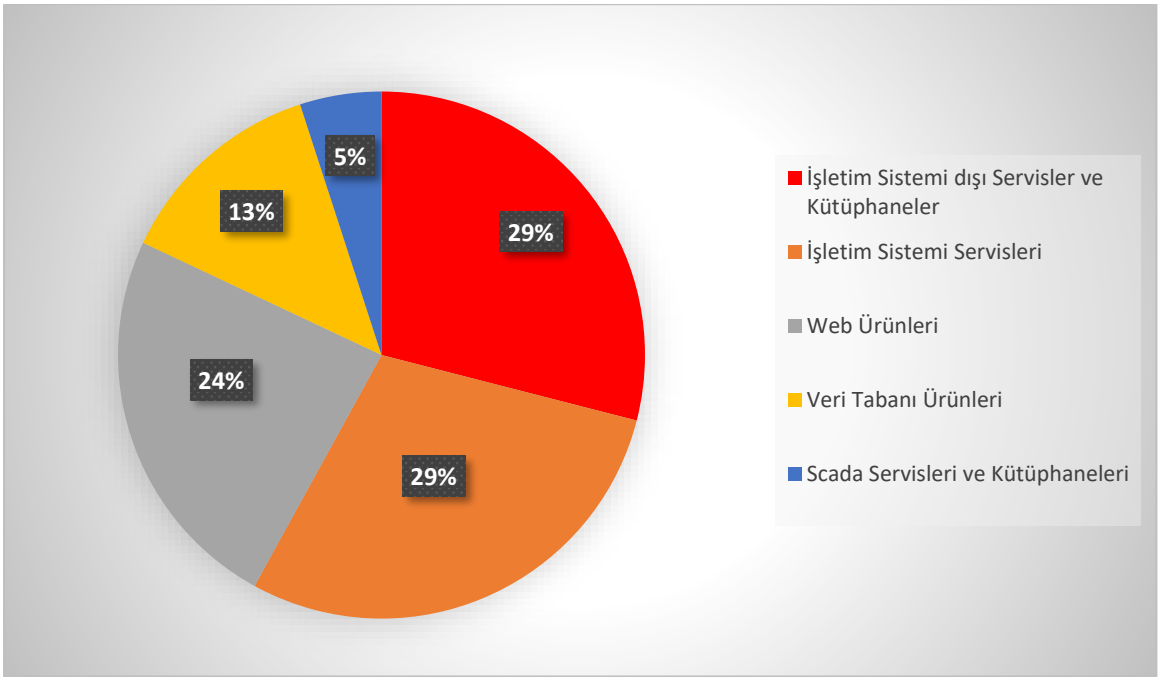
Sistem üzerinde koşan servisler ve uygulamalar dış dünyayla haberleşmek için bazı ağ portlarını açabilir. Bir saldırgan açık port üzerinden SCADA sistemine erişim sağlayıp sistem hakkında bilgi toplayabilir. Her açık port saldırgana istismar kodunu göndermeye ve veri çekmesine olanak sağlayabilir. Saldırgan erişilebilir ağ portlarını dinleyen servislere

uzaktan bağlantı kurarsa, hedef ağ üzerinde kendisine yer bulabilir ve yerel ağ sunucularını dinleyen tüm servisleri hedef alabilir. Güvenlik açığı olan ağ uygulaması, saldırgan tarafından istismar edilebilir ve yetkisiz bir şekilde verileri çekmek için kötücül kod göndermesine sebebiyet verebilir [91].

SCADA sunucuları üzerinde ne kadar çok çalışan servis varsa SCADA sisteminin saldırıya maruz kalması o kadar potansiyel dahilindedir. Sonuç olarak, SCADA sistemi üzerinde mümkün olduğunca gerekli servis ve uygulamalar çalıştırılmalıdır, böylece kullanılmayan portlar kapalı olacaktır.

4.1.6. Etkili yama yönetimi uygulaması

İşletim sistemi, servisler, kullanıcılar ve üçüncü parti yazılımlar için etkili yama yönetimi çok önemlidir. SCADA üreticileri ürünlerinde kullanıcılarına yamaları uygulayarak güvenlik açıklarını hafifletebilirler. Hafifletme uygulanmadan önce güvenlik açıklarının hızlıca tanımlanması ve yamalarının yapılması açıklığın ifşasının riskini minimize eder. Aynı zamanda SCADA üreticileri yamalarını üçüncü parti ürünler üzerinde test eder ve daha sonra temel ürüne yamalar.



Şekil 4.4. SCADA sisteminde yamasız bileşenlerin yüzdeleri [86]

İşletim sistemi yamaları saldırganın işletim sistemi üzerinde kod çalıştırmasına olanak sağlayan güvenlik açıklarını kapatmak için yayımlanır. 2009 Siber Güvenlik Risk raporuna göre [17], son yıllarda uygulamalarda keşfedilen güvenlik açıkları işletim sistemlerinde keşfedilen güvenlik açıklarından çok daha fazladır. Sonuç olarak uygulama programlarında kaydedilen saldırı girişimi daha fazladır.

Şekil 4.4'te NSTB değerlendirmesinde SCADA sisteminde yamasız yazılım bulunan ürünlerin yüzdeleri verilmiştir.

4.1.7. Haberleşme kanalı güvenlik açıkları

SCADA sistemleri, firmaların intranetleriyle ve dış ağda internetle olan bağlantılarının artmasından dolayı siber saldırılara daha fazla maruz kalmaktadırlar. Haberleşme kanalları bu bakımdan önemlidir, çünkü farklı güvenlik alanlarıyla bağlantı kurarlar, erişim yetkilerine sahip olurlar ve SCADA sistemini manipüle etmek amacıyla fonksiyonlarında değişiklikler yapılabilir. Haberleşme kanalı açıkları için aşağıdaki konular incelenmiştir:

- SCADA kimlik bilgileri toplama
- SCADA veri ve komut aldatmacası ve manipülasyonu
- SCADA fonksiyonlarını riske atan haberleşmelere DoS

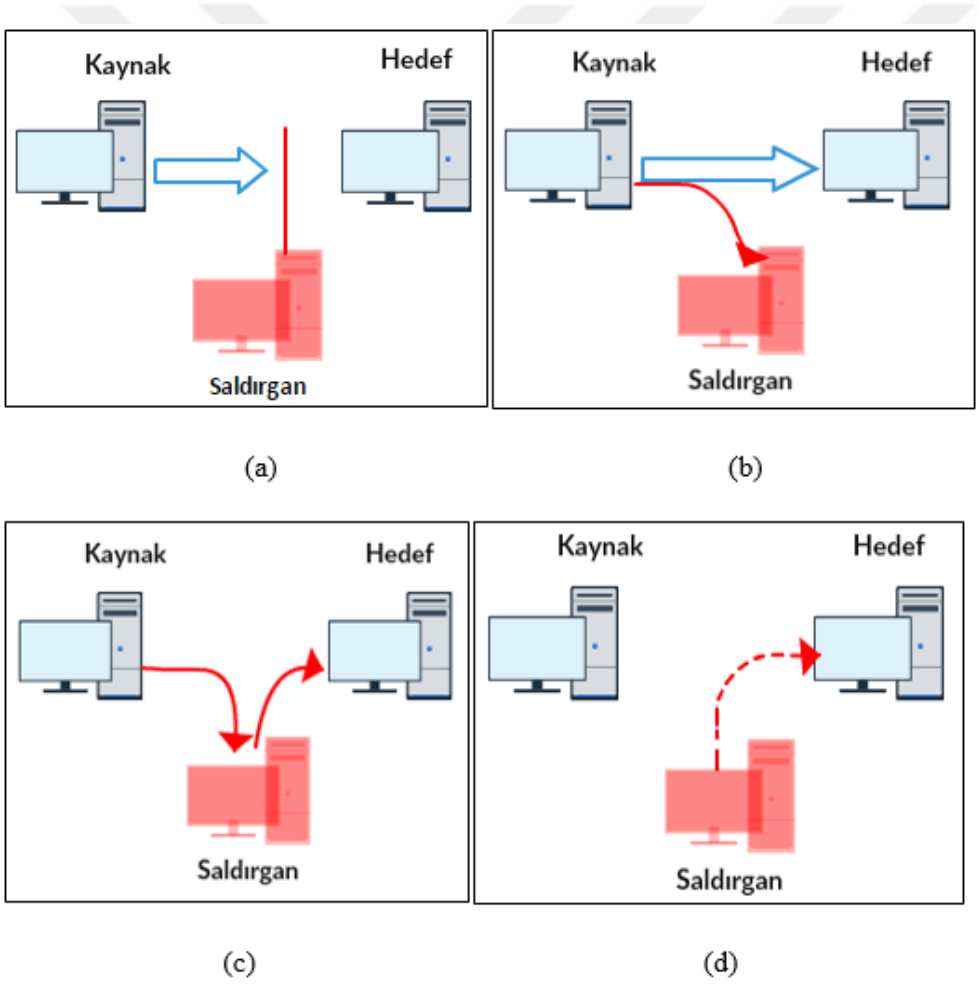
SCADA sistemlerinde; ağ cihaz yönetimi, uzaktan erişim veya dosya transferi gibi normal BT fonksiyonlarında bulunan BT protokolleri kullanılmaktadır. Bu protokollere yönelik tehditler SCADA sistemleri için de geçerlidir. Örneğin; ssh, ftp, telnet ve rlogin protokolleri gibi dosya transferi ve uzaktan erişim protokolleri SCADA sistemi ağlarında da kullanılabilmektedir. Bu protokollerden güvenli olanların tercih edilmesi önemli olmaktadır. Örneğin, haberleşme protokolleri ssh üzerinden tünellenebilir veya http, ssl üzerinden gönderilebilir (https) [92].

4.1.8. Haberleşme protokollerinin açıklıkları

Bu alt başlık altında Bölüm 2'de verilen SCADA haberleşme protokollerinden DNP3, Modbus TCP ve Profinet protokollerine yönelik zafiyetler ve saldırılar anlatılmıştır.

DNP3 açıklıkları ve saldırıları

DNP3 protokolüne yönelik saldırılar; protokolün özelliklerini, üretici uygulamalarını veya altyapısındaki zayıflıklarını istismar ederek gerçekleştirilir. Üretici uygulamalarına yapılan saldırılar, sistemde yapılandırma hatalarının istismarı şeklinde olur. Altyapı saldırıları, politika ve platformlardaki açıklıklar istismar edilerek gerçekleştirilir. Protokol özelliklerine yönelik gerçekleştirilen saldırılar daha çok haberleşme mimarisi ve DNP3 yapısıyla ilgilidir. Saldırılar yoğunlukla MTU, RTU ve haberleşme yolu olmak üzere üç hedefe yönelik gerçekleştirilmektedir. Dolayısıyla saldırılar Şekil 4.5'te gösterildiği gibi hedefe giden trafiği keserek, yakalayarak, değiştirerek ve yeniden üreterek gerçekleştirilir.



Şekil 4.5. DNP3 Saldırıları (a) Kesme (b) Yakalama (c) Değiştirme (d) Yeniden üretme

DNP3 mesajları kimlik doğrulama, yetkilendirme ve şifreleme gibi herhangi bir koruma parametresi uygulanmadan gönderilir. Bu açıklıkları istismar etmek uzak terminalde çalışan

sistemleri tamamen maskeleyebilir ve bu sistemler üzerinde kötücül işlemler çalıştırılabilir. Aşağıda 3 protokol katmanın da etkilendiği saldırılar belirtilmiştir [93].

1. Saldırgan mesajları yakalar. Ağ topolojisini ve cihaz fonksiyonlarını analiz eder ve paketlerden hafıza adreslerini elde eder. Bu yüzden bu tür tehdit veri yakalama kategorisinde değerlendirilir. Bu saldırıyla ana, uzak istasyon ve ağ topoloji verileri yakalanabilir.
2. Saldırgan DNP3 trafik modelini inceler ve ana terminalde çalışan cihaza kötücül yanıtları gönderir. Aynı zamanda kendi mesajlarını üretebilir ve uzak terminal cihazına gönderebilir. Bu tehdit türü yeniden üretme, değiştirme ve kesme kategorilerinde değerlendirilebilir.
3. Diğer saldırı türü olarak ise iki çalışan cihaz arasına yerleşerek gerçekleştirilen araya girme saldırısıyla mesajlar okunabilir ve değiştirilebilir. Bu saldırı türü kesme, yakalama, değiştirme ve yeniden üretme kategorilerinde değerlendirilir.

Bu saldırılar bütün protokol katmanlarına gerçekleştirilen genel saldırılardır. Her protokol katmanına özel o katmanın yapısını istismar etmeye yönelik saldırılar vardır. Bu saldırılar yapılandırma verilerini ve ağ topoloji bilgilerini elde ederek sistemin gizliliğine etki edebilir. Verilerin bütünlüğünü etkilemeye yönelik saldırılar hatalı veri eklenerek veya dış istasyonları yeniden yapılandırarak gerçekleştirilir. Erişilebilirliğe yönelik saldırılar sistemin temel işlevini kaybetmesine veya ana terminalle haberleşmesini engellemesine sebep olur.

Veri bağlantısı katmanına yönelik saldırılar aşağıdaki şekilde sıralanabilir [92]:

1. Veri bağlantısı katmanı çerçeve yapısında uzunluk alanı vardır. Bu alan değiştirilebilir, uzak terminaldeki mesaj işlemi bozulabilir ve tüm trafik akışı yanıltılabilir. Bu tehdit kesme ve değiştirme kategorisinde incelenir.
2. Veri bağlantı katmanı çerçevesinde, dış istasyon cihazının meşgul olup olmadığını ve istek mesajının daha sonraki bir zamanda gönderilmesi gerektiği durumunu gösteren bir bayrak vardır. Bu bayrak değiştirilebilir ve dış istasyon cihazının müsait olduğu gösterilebilir. Ana terminal biriminin uzak terminal birimine yoğun istek mesajlarıyla DoS gerçekleştirebilir. Eğer meşgul olarak ayarlanırsa; MTU, RTU cihazlarının meşgul olduğunu kabul eder ve herhangi bir mesaj göndermez. Böylece RTU beklemede kalır.

3. Paketin hedef adresi değiştirilebilir, böylece paket yeniden yönlendirilebilir veya kaybedilebilir. Paket başka bir sisteme ulaşırsa hatalı bir istek olur ve yanlış bir sonuç döner. Eğer adres yayın adresi olarak değiştirilirse paket bütün sisteme gider ve böylece tüm sistemi etkileyebilir. Bu tehdit türü değiştirme, yeniden üretme ve kesme kategorisinde incelenir.

Sahte taşıma katmanına yönelik saldırılar aşağıdaki gibi listelenebilir [94]:

1. Bu katmanı hedef alan saldırılar sadece bayrak alanını ve sıra numarasını değiştirmeye yöneliktir. Bayrak alanını değiştirmek temel olarak parçalanmış mesajın kesilmesiyle olur. FIR bayrağı bölünmüş mesajın başlangıç sırasını gösterir ve bu yüzden paket diğer bir FIR bayrağıyla yeniden üretilir ve trafik akışına eklenirse tüm sırayı bozar ve bu paketlerin düşmesine sebep olur. FIN bayraklı mesaj yeniden üretilir ve mesajın sonuna eklenirse mesajın tamamlanmaması sebebiyle bu işlem durur.
2. Paketlerin taşınması bir sıra halindedir ve bu sıra numarasıyla işaretlenir. Bir paket elde edilirse sıra numarası okunabilir. Sıra numarasının aritmetik artışı olmasından dolayı, bir mesaj bir sonraki sıra numarası ile üretilebilir ve trafik akışı içine enjekte edilebilir. Bu mesaj MTU'da veya RTU'da işlem hatalarına neden olabilir. Bu tehdit grubu kesme, değiştirme ve yeniden üretme kategorilerinde değerlendirilir.

Uygulama katmanına yönelik gerçekleştirilen saldırılar aşağıdaki gibi listelenebilir [95]:

1. Hedef RTU cihazının içine veri yazan fonksiyon kodu 02 yeniden üretilir ve gönderilir. Bu, sisteme veri yazar ve sistemi çökertir. Bu durum hatalı veriler barındırmasından dolayı RTU cihazlarının hafızalarının düşmesine sebep olabilir. Tehdit kategorisi kesme ve değiştirmedir.
2. Hedef RTU cihazının yazmaçlarındaki işlemleri durdurma ve başlatma görevi olan fonksiyon kodu 9 veya 10'lu olan ve RTU'da bütün verileri temizleyen bir mesaj gönderilir. Bu durum kritik verilerin kaybını, sistemin kötücül çalışmasını veya çökmesine sebep olabilir. Fonksiyon 10'lu mesajın tespit edilmesi çok zordur çünkü mesajın alındığına dair bir bildirim gerektirmez.

3. Mevcut zamanı kaydetme görevi olan fonksiyon kodu 18'le veri paketi gönderilebilir ve böylece RTU cihazlarının fonksiyonları sonlandırılabilir. Bu durum sistemi cevap veremez hale getirir ve böylece hizmet engelleme gerçekleştirilmiş olur.

Yukarıda anlatılan 11 saldırı sistem üzerinde ciddi etkiler bırakabilir. Saldırılar, hizmetin engellemesine ve hatalı veri girerek sistemin bütünlüğünün bozulmasına neden olabilir. Bu saldırıların en tehlikelisi MTU'u aldatan ve MTU'nun bir kısmının veya tamamının kontrolünün ele geçirilmesi ve dolayısıyla sistemin tamamen alt üst olmasına sebep olanıdır. Saldırgan tarafından cihaz yapılandırılması ele geçirildiğinde veri gizliliği kaybedilebilir.

Modbus açıklıkları ve saldırıları

Modbus sistemlerine ve ağlarına yönelik saldırılar bu protokolün özelliklerine, uygulamalarına ve altyapısına göre istismar edilir. DNP3'teki gibi bu protokole yönelik tehditler kesme, yakalama, değiştirme ve yeniden üretme olmak üzere dört kategoride incelenebilir. Modbus Seri Protokolüne yapılan saldırılar ana ve köle cihazlarına ve seri haberleşme ağına yönelik gerçekleşirken, Modbus TCP'e yapılan saldırılar IP ağına, ana ve köle cihazlarına gerçekleştirilir [96].

Bu saldırılarda mesajın içeriğine erişilebilmesinden dolayı taşınan bilginin gizliliğinin ifşa olmasına sebep olunabilir, hizmet engellemesine sebep olduğu için sistem erişilebilirliğine etki eder ve araya girerek ele geçirilen bilginin yeniden üretilebilmesinden dolayı veri bütünlüğü etkilenir. Saldırılar; Modbus seri protokolü, Modbus TCP protokolü ve her iki seri ve TCP protokolleri olmak üzere üç başlık altında incelenir.

Modbus seri protokolü saldırıları

Fonksiyon kodunun değiştirilerek Modbus protokol yapısına yönelik saldırılar son sistemin çökmesine sebep olabilir [97].

- Fonksiyon kodu 08 ve alt fonksiyon kodu 0A hedef cihaza gönderildiğinde saymacı sıfırlar ve hata yazmaç değerlerini değiştirir. Bu durum saha cihazının yapılandırmasını değiştirir ve hata işlemlerini etkiler. Bu tehdit kategorisi saha cihazını değiştirme sınıfında değerlendirilir.

- Fonksiyon kodu 08'in 01'e değiştirildiğinde son cihaz yeniden başlar ve güç açma testi çalışır. Bu mesaj saha cihazının yapılandırma ayarlarını değiştirmesine sebep olur. Bu tehdit kesme ve değiştirme kategorisinde değerlendirilir.

- Fonksiyon kodu 17, saha cihazına gönderildiğinde saha cihazının durum bilgisi döner. Bu bilgisiyle ağ dinlenebilir ve daha farklı saldırıların temeli oluşturulabilir. Bu durum sistemin gizliliğine etki eder.

Modbus seri ve TCP saldırıları

Bu saldırı kategorisinde, Modbus mesajlarının bloklanmasıyla bütün haberleşme yolu hizmet dışı bırakılabilir. MTU'dan kontrolü alabilecek daha ciddi saldırılar mevcut olabilir ve tüm sistemin işleyişi tamamen çökertilebilir [98].

- Araya girme saldırısıyla mesajlar saha cihazlarına yayımlanabilir ve yayın mesajları için yanıt mesajları olmadığından bu saldırı tespit edilemez. Bu saldırı tüm RTU cihazlarını indirebilir ve tüm işlemlere engel teşkil edebilir. Bu tehdit kesme ve değiştirme kategorisinde incelenir.
- MTU ve RTU cihazları arasında akan mesajlar yakalanıp tekrar gönderilebilir. Bu yöntemle son cihazlar yanıltılabilir ve akan işlemlere zarar verilebilir. Bu tehdit kesme, değiştirme ve yeniden üretme kategorilerinde değerlendirilir.
- Saha cihazlarının durum ve yapılandırma bilgilerini ele geçirmek için araya girerek rasgele adresler üretilip saha cihazlarına mesajlar gönderilebilir. Bu tarama saldırısı bilgi gizliliğinin ihlaline sebep olur. Bu tehdit yakalama kategorisinde incelenir.
- Ana cihazdan köle cihazlara akan bilgilerin geciktirilmesiyle bu mesajların düşürülmesi sağlanabilir. Bu saldırı sistemin mesajların kesilmesine ve değiştirilmesine sebep olur.

Modbus TCP saldırıları

Modbus TCP protokolüne yönelik yapılan saldırılar şu şekildedir [99]:

- TCP paketinin çerçeveli yapısına etki etmeye yöneliktir. Çoklu Modbus mesajları tek bir TCP paketinin içinde bulunamaz. Bu yüzden mesajlar MTU tarafından parçalarına ayrılır

ve RTU'a gönderilir. Bu saldırıda hatalı mesajlar enjekte edilebilir veya mesajlar değiştirilerek hedef sisteme gönderilebilir.

- Son çerçeve biti legal olmayan bir paket TCP bağlantısını kesebilir. Bu tip bir paket gönderilecek Modbus mesajlarını sonlandırabilir ve haberleşmede kesmelere neden olabilir.
- Yüksek önceliğe sahip saha cihazlarına veya ana cihaza sık istekte bulunmak veya diğer bir deyişle bombardıman yapmak hizmet kesintilerine neden olabilir.

Yukarıda bahsedilen saldırılar sonucunda sistemde gizlilik kaybı, erişim kaybı ve veri bütünlüğünün bozulması gibi etkiler görülebilir.

Profinet açıklıkları ve saldırıları

ISO-TSAP (Standards Organization Transport Access Point) gibi endüstriyel sistemlerde kullanılan protokoller geliştirildiği dönemin şartlarındaki güvenlik konseptine göre oluşturulmuştur. Kontrol sistemlerinin ve PLC cihazlarının o dönemde tamamen izole olduğu düşünüldüğünden bu protokoller güvenli olarak tasarlanmamıştır.

Günümüzdeki durum düşünüldüğünde artan siber tehditler karşısında bu sistemlerin güvenlik konseptlerinin düşünülmemesi imkansız hale gelmektedir. İleriki bölümlerde anlatılacak olan Stuxnet solucanının yayılmasında olduğu gibi izole veya ayrılmış ağlar, USB aracılığıyla atlatılabilmekte ve bu ağların güvenli olmadığı anlaşılmaktadır [100].

Siemens Simatic S7 PLC istismarı

Simatic S7 istismarı direk olarak Profinet'e yönelik değildir, fakat Profinet istismar edilecek ağa bağlanmak için kullanılmaktadır. Saldırı, Siemens tarafından üretilen bütün S7 PLC'lerin haberleşmesi ve programlanması için Siemens mühendislik yazılımı olan ISO-TSAP'ten faydalanır.

Saldırganın bakış açısından S7 PLC cihazı ISO-TSAP ile 102. porttan haberleşmekte ve iletilen paketler açık metin olarak şifrelenmeden gönderilmektedir. Bu yüzden araya girme ve yeniden yönlendirme saldırıları bu sistem için uygun olmaktadır. Aynı zamanda MTU ve RTU veya PLC cihaz arasında akan bütün trafik kolay bir şekilde yakalanabilmekte ve

böylece saldırganın protokole yönelik tersine mühendislik gerçekleştirmesine ve kötücül amaçları için kendi paketlerini üretmesine imkan sağlamaktadır.

ISO-TSAP'in bir diğer önemli güvenlik açığı, kimlik doğrulamasının zayıf olmasıdır. Kimlik doğrulaması yapılmış paketleri yakalayan bir saldırgan, aynı paketi kullanarak kimlik doğrulama mekanizmasını aşabilir [101].

Kullanıcı kimlik doğrulama paketini PLC cihazına gönderdiğinde, paketteki parola veya parola özeti cihazdaki yapılandırılmış olan parola özetiyle karşılaştırır. Eğer bu karşılaştırma doğruysa cihaz erişime izin verir ve PLC hafızasına okuma/yazma/çalıştırma yetkilerini verir. Bu, saldırganın PLC üzerinde istediği değişiklikleri yapabileceği anlamına gelmektedir.

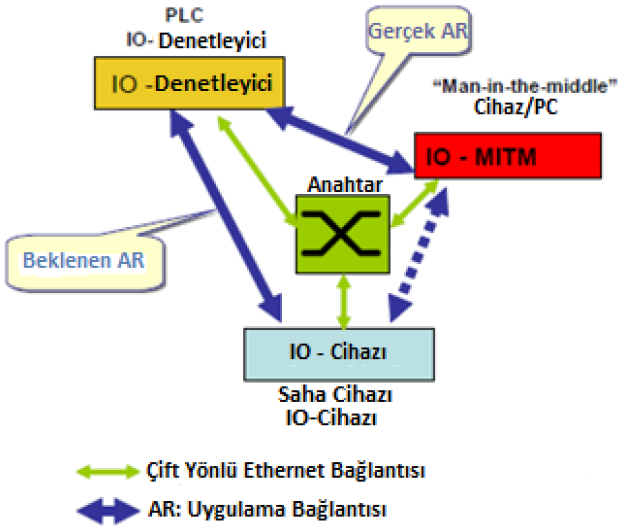
Saldırı vektörü;

1. MTU ve PLC arasında akan trafik Wireshark ve benzeri ağ izleme araçlarıyla yakalanır.
2. Yakalanan paketin istemci kısmı çıkartılır ve istemci ve sunucu arasında akan bilgiler analiz edilir.
3. Çıkarılan istemci kısmından elde edilen bilgilere göre yeni paket oluşturulur.
4. Hazırlanmış paketler PLC'e yeniden yönlendirilir.

Bu tip bir istismar kötücül amaçları olan birinin ağa dahil edilmesini engelleyerek kolayca engellenebilir, fakat günümüzde bütün sistemler birbiriyle bağlantılıdır. Yetkisiz bir şekilde ağa erişen bir saldırgan bu yolla sistemi ele geçirebilir.

Profinet IO cihazlarının emülasyonu

Profinet IO standart Ethernet ağ bileşenlerini kullandığı için Profinet sistemler Şekil 4.6'da gösterildiği şekilde MITM saldırısı gibi standart Ethernet ağlardaki tehditlerle aynı tehditlere maruz kalabilmektedir. MITM saldırısı haberleşen iki cihazın legal bir haberleşme ortağı olarak araya girerek gerçekleştirilir. Bu durum saldırganın haberleşen iki cihaz arasındaki trafiği yakalamasına olanak sağlar ve bilinmeyen uzak sunucuya göndermesine veya paketin yeniden yapılandırıp cihaza enjekte etmesine imkan verir.



Şekil 4.6. Profinet sistemler için MITM saldırısı [102]

Profinet sistemin temel formunda IO denetleyici ve bir veya daha fazla IO cihazı bulunmaktadır. Bu iki bileşen birbirleri arasında Uygulama Bağıntısı (Application Relation - AR) olarak isimlendirilen bağlantı oluşturur. Bu IO denetleyici tarafından istemci/sunucu uygulamaları için çerçeve olan Dağıtık Hesaplama Ortamı/Uzaktan Prosedür Çağrısı (Distributed Computing Environment/Remote Procedure Calls – DCE RPC) ile UDP/IP üzerinden gerçekleşir. Profinet IO denetleyici IO cihazlara IP adresi atanmasından sorumludur.

Profinet IO cihazları sadece IP adresleri ile tanımlanmaz, aynı zamanda Profinet isimleri ile de tanımlanır. Profinet isimleri mühendislik süreci boyunca atanır ve IO cihazın kalıcı hafızasına kaydedilir. Bu isimler daha sonra istenilen IP adreslerinden sorumlu olan IO denetleyicilere yapılandırılır. IO denetleyici, IO cihazın ulaşılabilir olduğunu ve onaylanan bir isme sahip olduğunu doğrulamak için ilk DCP-tanımlayıcı mesajı gönderir. Daha sonra isimlerin sorgusu yapılır ve IP adresleri atanmadan önce IO denetleyici, IO cihazın birden fazla IP adresi alıp almadığını denetlemek için ARP istekleriyle kontrol eder. Eğer birden fazla IP adresi atanmadıysa, IO denetleyici bir IP adresi atar, AR bağlantısı kurar ve IO cihaza TCP/IP üzerinden yapılandırmayı gönderir. Yapılandırmalar gönderildikten sonra periyodik veri transferi yer alır ve yapılandırmaların tekrar değişimine ihtiyaç duyulmayıncaya kadar IP adresi artık kullanılmaz [102].

Yapılandırma dikkatsiz bir şekilde yapıldıysa bu tarz bir yükleme hatalara meyilli olabilir. En kritik ve olası hatalar birden fazla IP adresi verilmesi ve Profinet isimleridir. Bu hatalar

Profinet ağında MITM saldırısı ve ARP zehirlenmesine neden olabilmektedir. Fakat saldırının başarılı bir şekilde gerçekleşebilmesi için bazı şartların oluşması gerekmektedir. Saldırgan makinası ve Profinet cihazının aynı zaman senkronizasyonunda olması gerekmektedir. Örneğin, paketler 1 ms'lik devirle gönderilirse MITM makinası kendi paketlerini yine 1 ms'lik devirle göndermelidir. MITM makinası bunu başaramazsa anahtarın kendi MAC tablosunu her seferinde güncellemesinden dolayı bütün saldırı başarısızlığa uğrayacaktır.

Profuzz

Fuzzing veya fuzz testing (Güvenilirlik test yöntemi), yazılımı test etmek için bilgisayar programının girdilerine rasgele, doğrulanmayan veya beklenmedik verileri enjekte ederek gerçekleştirilen siyah kutu tekniğidir. Yarı otomatik veya tamamen otomatik bir şekilde gerçekleştirilebilir. Fuzzing işleminin temel mantığında, her programın keşfedilmeyi bekleyen bir hatası (bug) olduğu ve sistematik bir yaklaşımla bu hataların keşfedilebileceği yer almaktadır.

ProFuzz, Augsburg Üniversitesi'nde Ronald Koch ve öğrencileri tarafından geliştirilmiş Profinet fuzzer programıdır. ProFuzz, güçlü paket değiştirme programı olan Scapy çerçevesini kullanır. ProFuzz aşağıdaki Profinet çerçeve tiplerini destekler [103]:

- AFR (Rasgele Alarm Çerçevesi)
- AFO (Sıralı Alarm Çerçevesi)
- PNIO (Periyodik Gerçek Zaman)
- DCP (DCP-Tanımlayıcı İsteği)
- PTCP (Hassas Şeffaf Saat Protokolü)

4.2. SCADA Sızma Testi Araçları

Bilgi ve iletişim teknolojileri altyapısıyla entegre bir şekilde çalışan SCADA sistemlerinin güvenlik açıklarının tespiti ve tespit edilen bu zafiyetlerin istismarı, normal bilgi teknolojileri altyapısını kullanan sistemler için yapılan sızma testi araçları veya özel olarak SCADA sistemleri için tasarlanmış araçlar kullanılarak yapılmaktadır.

Çalışmanın bu bölümünde SCADA sistemlerine sızmak için kullanılan araçların bir kısmı gösterilmiştir.

4.2.1. Shodan arama motoru

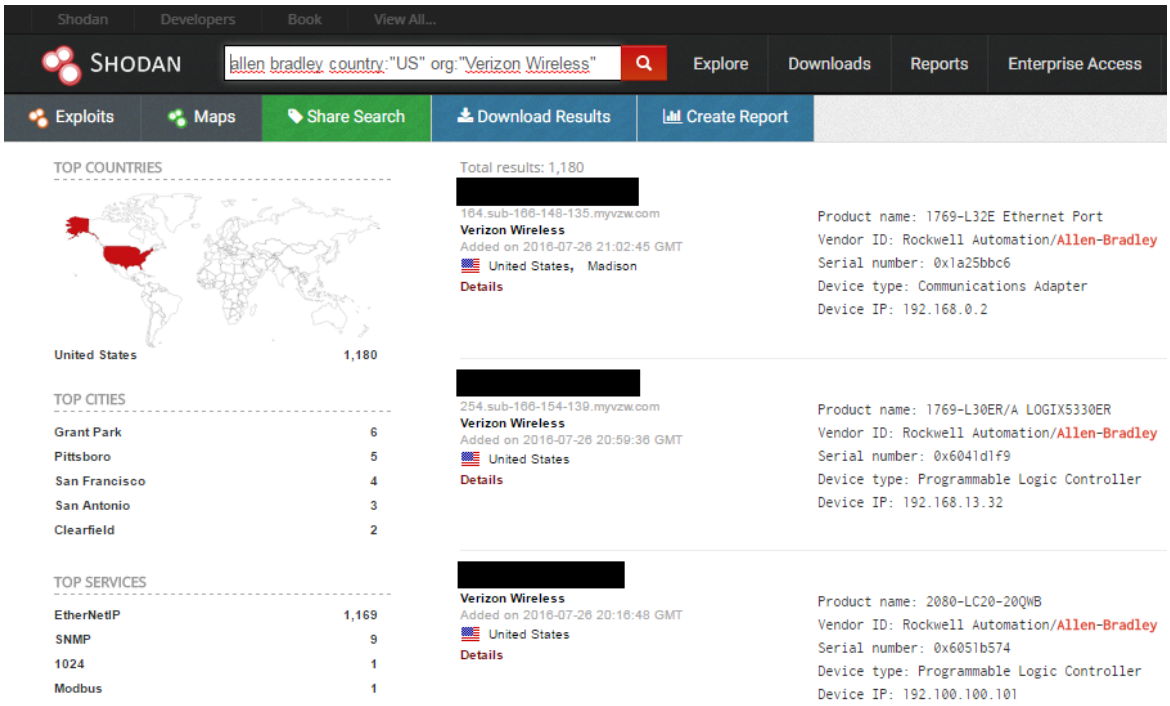
2009 yılında John Matherly isimli bir programcı, internet bağlantılı cihazları tanımlayabilen ve grafiksel ara yüzlü Shodan isimli bir arama motoru yazmıştır [74]. Özellikle; bilgisayar, yazıcı, webcam ve endüstriyel kontrol cihazları gibi yönlendirilebilen IP adresli cihazları tanımlayabilir. Shodan; bütün interneti tarar, cihazları dizinler ve uygun olan servislere sorguda bulunur. Shodan API veya https://www.shodan.io/ üzerinden erişilebilecek aranabilir veri tabanında topladığı cihazların IP adreslerinin port numaralarını ve üzerinde çalışan servislerin ana başlık bilgilerini barındırır. Kullanıcılar; ülke, sunucu adı, belirli IP adresi aralığı, işletim sistemi, cihaz markası veya port bilgilerini barındıran farklı sorgulamalarda bulunabilirler.

2010 yılının Ekim ayında; ICS-CERT, Shodan'ın kontrol sistemleri ara yüzlerine ait güvenlik açıklarını tespit edebilme yeteneğini ve kontrol sistemi cihazlarının internetten izole olmasının öneminin tartışıldığı bir rapor yayımlamıştır [103]. Bu raporun sonucunda ICS-CERT-10-301-01, ICS-CERT-301-01A, ICS-CERT-11-343-01A, ICS-CERT-12-046-01 ve ICS-CERT-12-046-01A olmak üzere 5 tane internetle bağlantılı kontrol sistemleri cihazlarının önemiyle ilgili rapor yayımlamıştır [105].

2011 yılında Leverett [106], 7500'den fazla internete bağlı yönetim sistemleri, sayaç, HMI ve PLC gibi endüstriyel kontrol cihazlarını kullanmıştır. Toplam 29 Shodan sorgusu endüstriyel kontrol cihazlarının tespiti için kullanılmıştır. 2 yıllık bir değerlendirme sonucunda 2013 yılında tespit edilen 7500 cihaz dramatik olarak artmış ve 57409 adet olduğu tespit edilmiştir.

2012 yılında SHINE (Shodan Intelligence Extraction) projesi A.B.D. İç Güvenlik Bakanlığında yürütülen bir proje olup [107], bu proje kapsamında Shodan API kullanılmış ve yaklaşık olarak 700 farklı Shodan sorgusuyla dünya genelinde internete bağlı 500000 adet endüstriyel kontrol cihazı tespit edilmiştir. ICS-CERT ile birlikte 7200 cihaz üzerinde yürütülen projenin devamında çoğu cihazda çok zayıf güvenlik önlemleri alındığı görülmüştür [108].

Shodan web ara yüzü kullanılarak “allen bradley” markalı internet bağlantılı endüstriyel kontrol sistemi sorgulanmış ve elde edilen sonuçlardan sistem üzerindeki zafiyetler tespit edilmiştir. Yapılan sorgulamada cihazın bulunduğu ülke ve şehirler, üzerinde çalışan servis ve portlar, işletim sistemi, markası, üzerinde çalıştığı firma adı ve IP adresi aralığı aranabilmektedir. Şekil 4.7’de yapılan sorgulamaya ait ekran görüntüsü görülmektedir.



Şekil 4.7. Shodan sorgu sonucu

Tespit edilen endüstriyel kontrol sistemlerine girince harita üzerinde sistemin nerede olduğu, üzerinde çalışan servisler ve portlar, cihazın ürün ismi, üreticinin markası, cihazın seri numarası, cihazın tipi ve cihazın yerel IP adresi görülmektedir. Sorgulanan cihazlardan birçoğunda web servisinin çalıştığı fark edilmiş ve bu cihazların web giriş ara yüzü ekranlarına erişim yapılabildiği ve erişim sağlanan uygulama üzerinde şifreleme yapılmadan giriş yapılabildiği tespit edilmiştir. Böylece trafiği dinleyen bir saldırgan, kullanıcının girdiği verileri şifresiz olarak görüntüleyebilmektedir.

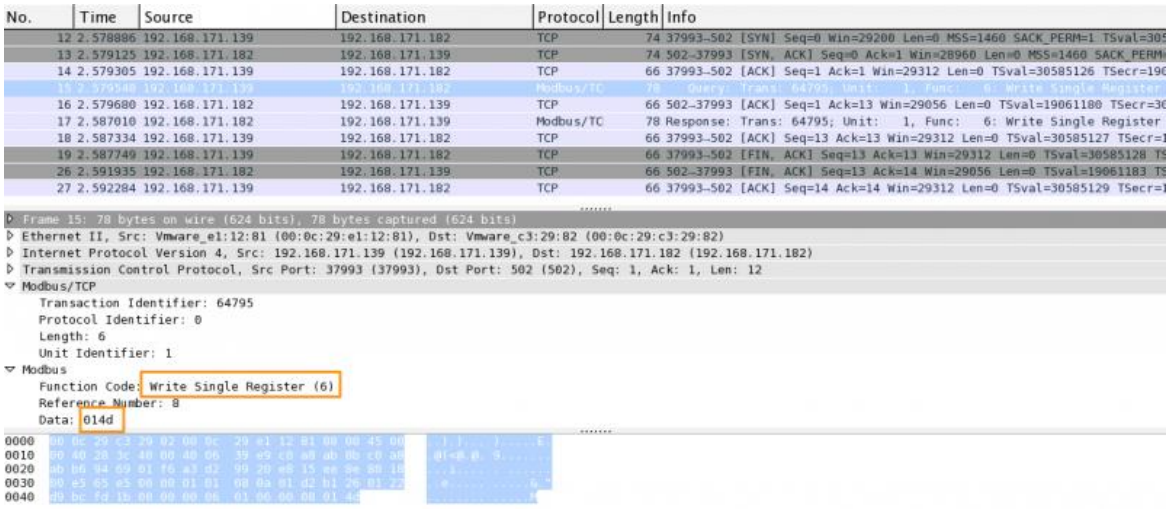
Parola güvenliğinin önemini göstermek amacıyla web servisi üzerinden giriş yapılabilen bir endüstriyel kontrol sistemine giriş yapılırken kullanıcı bilgilerinin sistem yöneticisi veya kullanıcısı tarafından değiştirilip değiştirilmediği kontrol edilmiş ve elde edilen sonuçlara göre birçok sistemde kullanıcı bilgilerinin varsayılan olarak bırakıldığı gözlemlenmiştir. Cihazların türüne göre internette yapılan varsayılan kullanıcı adları ve parolaları arandığında

çok kolay bir şekilde bulunabildiği ve sisteme basit ve yetkisiz bir şekilde erişilebildiği tespit edilmiştir.

4.2.2. Wireshark ağ analiz programı

Wireshark ihtiyaç doğrultusunda ağ üzerinde akan paketleri detaylı bir şekilde görüntülemeye yarayan açık kaynak kodlu bir paket analizi programıdır [109]. Ağ üzerinde akan paketleri yakalar, parçalara ayırıp inceleyerek analiz eder ve analiz ettiği protokole bağlı olarak paketteki "1'ler ve 0'lar"ı yorumlar. Ağ kullanım hesaplamaları gibi farklı istatistiksel analizlere Wireshark'ta parçalara ayrılmış paketlerdeki bilgileri kullanılarak erişilebilir. Bu sayede ağ üzerindeki cihazların birbirleri ile haberleşmesi ve karmaşık elementlerin davranışı sanallaştırılabilir ve anlaşılabilir. Aynı zamanda bu program, açık kaynak kodlu ve UNIX, Windows, MacOs gibi farklı işletim sistemlerinde çalıştığı için yaygın olarak kullanılmaktadır.

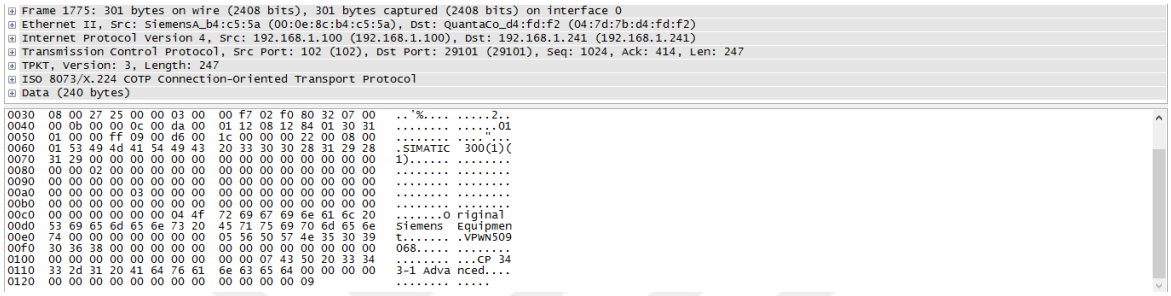
Modbus, Profibus, DNP3 gibi endüstriyel kontrol sistemlerinin haberleşmesi için kullanılan birçok protokol Wireshark tarafından desteklenmekte ve bu protokollerin davranışları sanallaştırılabilmektedir. Şekil 4.8 ve 4.9'da Gazi Üniversitesi SCADA Laboratuvar ortamında tasarlanan Modbus ve Profinet haberleşmelerinden elde edilen Wireshark görüntüleri mevcuttur.



Şekil 4.8. Modbus Wireshark görüntüsü

Şekil 4.8'de verilen Wireshark görüntüsünde Modbus protokolüne yönelik yakalanan paketler gösterilmiştir. Modbus protokolünün fonksiyon kodu ve bu fonksiyon koduyla endüstriyel kontrol sistemine gönderilen veri gösterilmiştir.

Şekil 4.9'da çalışmada kullanılan Siemens Simatic S7-300 cihazının Profinet protokolüne yönelik yakalanan paketleri gösterilmiştir. S7-300 CPU cihazı kullanılan çalışmada Şekil 4.9'dan da görüldüğü üzere CP 343-1 Advanced haberleşme modülü kullanılmıştır.



Şekil 4.9. Profinet Wireshark görüntüsü

4.2.3. Nmap ağ tarama aracı

Nmap, TCP/IP tabanlı çalışan bilgi sistemlerinin açık port ve servisleri gibi potansiyel zafiyetlerini taramak için kullanılan açık kaynak kodlu çok amaçlı bir tarama aracıdır [110]. Aynı zamanda ağ topolojisinin çıkarılması için de kullanılmaktadır. Zafiyet değerlendirmesinin ve bilgi toplama fazının önemli bir kısmı port taramasıyla gerçekleştirilir. Her bir makinanın açık portlarının listesi SCADA sistemine zafiyetlerini istismar edip sızmak için bir adım teşkil eder. Şekil 4.10'da Siemens S7-1200 PLC cihazının kullanıldığı deney düzeneği ortamında nmap taraması sonucu elde edilen açık portların ve servislerin listesi görülmektedir. Yapılan tarama sonucunda varsayılan olarak 102. port üzerinde Profinet protokolünün ve iso-tsap servisinin çalıştığı görülmektedir.

Şekil 4.10. Nmap taraması

4.2.4. Plcscan aracı

Plcscan, ScadaStrangeLove grubu tarafından yayımlanan bir yardımcı programdır. PLC cihazlarının ve ağ üzerindeki diğer Modbus cihazlarının tespitinde kullanılır [111].

Plcscan, TCP/102 ve TCP/502 portlarının durumlarını kontrol etmek için yazılmış bir Python scriptidir. Eğer bu iki portu açık bulursa, bu portlarla ilgili diğer fonksiyon veya scriptleri çağırır. Örneğin TCP/502 portunun açık olduğunu tespit ederse, cihazın tanınması için MEI tipini çekerek Modbus fonksiyonlarını çağırır. Daha sonra cihazın kimliği dönecek ve dönen bu bilgi ekranda görüntülenecektir.

Plcscan, PLC cihazından hızlı sonuç alan temel bir araçtır. Bilgiler doğrudan cihazdan çekilir ve benzeri cihazlarda ilk test olmadan kullanılırsa bazı sorunlara neden olabilir. Bazı konularda sınırlama gerektiren kod içinde bazı hata kontrollerini yapmaktadır. Plcscan tarafından toplanan bu bilgiler Profinet ve Modbus protokollerinin olduğu iki çıkış şeklinde olabilir. Bu cihazlardan toplanan çıktılar donanım yazılımı versiyonlarını içermektedir. Şekil 4.11'de Siemens S7-300 PLC cihazının bulunduğu deney düzeneği ortamında plcscan tarama sonuçları gösterilmiştir. Tarama sonuçlarına göre kullanılan cihazın modül tipi, seri numarası, projede kullanılan modülün ve plc cihazının adı versiyonu ve donanım bilgileri elde edilmiştir.

Şekil 4.11. Plcscan tarama sonuçları

4.2.5. Snmpcheck

Snmpcheck komutunun amacı, Windows, Unix, ağ cihazları, yazıcılar ve PLC cihazları gibi Snmp protokolünü destekleyen herhangi bir cihazın bilgi toplama işleminin otomatize edilmesidir. Snmpcheck, snmp cihazlarını listelemeye ve okunur bir şekilde çıktı alınmasına imkan verir. Sistem izleme veya penetrasyon testlerinde oldukça kullanılmaktadır.

Snmpcheck komutuyla çalışmada kullanılan S7-300 cihazından elde edilen bilgiler Şekil 4.11'de gösterilmiştir. Elde edilen sonuçlara göre CP 343-1 Advanced haberleşme modülünün detaylı versiyon bilgisi ve cihazın ne kadar süredir çalışmakta olduğu gözükmektedir.

Şekil 4.12. Snmpcheck komutu sonuçları

4.2.6. Metasploit framework

Metasploit Framework bilgi güvenliği toplulukları arasında en yaygın ve en bilinen sızma testi araçlarından birisidir. H. D. Moore tarafından 2003 yılında ilk versiyonu yayımlanmıştır. 2007 yılında Moore bu projede perl dilinden vazgeçip ruby kodunda en baştan tekrar yazmıştır. 2009 yılında Rapid7 güvenlik firması bütün Metasploit Projesini satın almıştır.

Metasploit Framework'ü istismar kodu geliştirme toplulukları için yaygın bir şekilde kullanılmaktadır. Güvenlik uzmanları ve geliştiricileri açık kaynak kodlu platformu geniş altyapılı bilgi sistemlerini test etmek ve belirli hedef sistemler için yeni istismar kod yazmak

için kullanmaktadırlar. Mevcut durumda içerisinde farklı sistemler ve yazılımlar için 1800'den fazla istismar kodu bulunmaktadır.

İstismar kodunu başarılı bir şekilde çalıştırmak için 4 temel adım mevcuttur. Bu adımların açıklamaları aşağıda verilmiştir:

İstismar kodu yapılandırması: Hedef sisteme veya yazılıma yönelik saldırı türü seçilir.

Payload yapılandırması: İstismar kodunun çalışması için hedef makine üzerinde hangi kodun çalıştırılacağı belirlenir.

Enkodlama yapılandırması: IPS/IDS sistemlerinden korunmak için yapılacak işlem belirlenir.

İstismar kodunun çalıştırılması: Saldırı işlemi başlatılır ve hedef sistemle haberleşme kanalı açılır.

Scadahacker'ın düzenlemiş olduğu SCADA sistemlerinin zafiyetlerine yönelik yazılmış metasploit modüllerinin bir kısmı Çizelge 4.3'te gösterildiği gibidir.

Çizelge 4.3. SCADA sistemleri için hazırlanmış metasploit modüllerinden bazıları [112]

Araç/İstismar Kod Adı	Geliştirici	Sistem	Metasploit Referans
teechart_pro.rb	BACnet	Operator Workstation	exploit/windows/browser/teechart_pro.rb
simatic_s7_1200_command.rb	Dillon Beresford	Siemens Simatic S7 module	Açık kaynak olarak indirilmektedir.
simatic_s7_300_command.rb	Dillon Beresford	Siemens Simatic S7 module	Açık kaynak olarak indirilmektedir.
modbusclient.rb	EsMnemon and Arnaud Soullie	Modbus Client Utility	auxiliary/scanner/scada/modbusclient.rb
modbusdetect.rb	EsMnemon	Modbus Client Utility	auxiliary/scanner/scada/modbusdetect.rb

Modbusdetect modülü

Çalışmanın bu bölümünde, yukarıda bahsedilen Metasploit Framework modüllerinden modbusdetect ve modbusclient modülleri kullanılarak hedef sistem üzerinde Modbus protokolünün tespiti ve üzerindeki yazmaçlarda yazan değerleri okuyup değiştirme işlemleri yapılacaktır.

Şekil 4.12'de modbusdetect modülü kullanılarak hedef sistem üzerinde bilgi toplama amaçlanmıştır. Modbusdetect Metasploit modülü, hedef sistemde koşan Modbus/TCP protokolünü taramak ve tanımlamak için belirli bir IP adresi aralığındaki Modbus servislerini tespit eder. Bu modül Modbus istek paketlerini hedef sistemin 502. portuna göndererek tespit eder ve aynı İşlem ID ve Protokol ID içeren yanıtları bekler. Modül Modbus/TCP başlığı ve PLC cihazının Birim ID'sini döndürür [113].

```
msf auxiliary(modbusdetect) > show options

Module options (auxiliary/scanner/scada/modbusdetect):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    502              yes       The target port
   THREADS  1                yes       The number of concurrent threads
   TIMEOUT  10               yes       Timeout for the network probe
   UNIT_ID  1                yes       ModBus Unit Identifier, 1..255, most often 1

msf auxiliary(modbusdetect) > set RHOSTS 192.168.206.132
RHOSTS => 192.168.206.132
msf auxiliary(modbusdetect) > run

[+] 192.168.206.132:502 - MODBUS - received correct MODBUS/TCP header (unit-ID: 1)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Şekil 4.13. Modbusdetect modülü

Modbusclient modülü

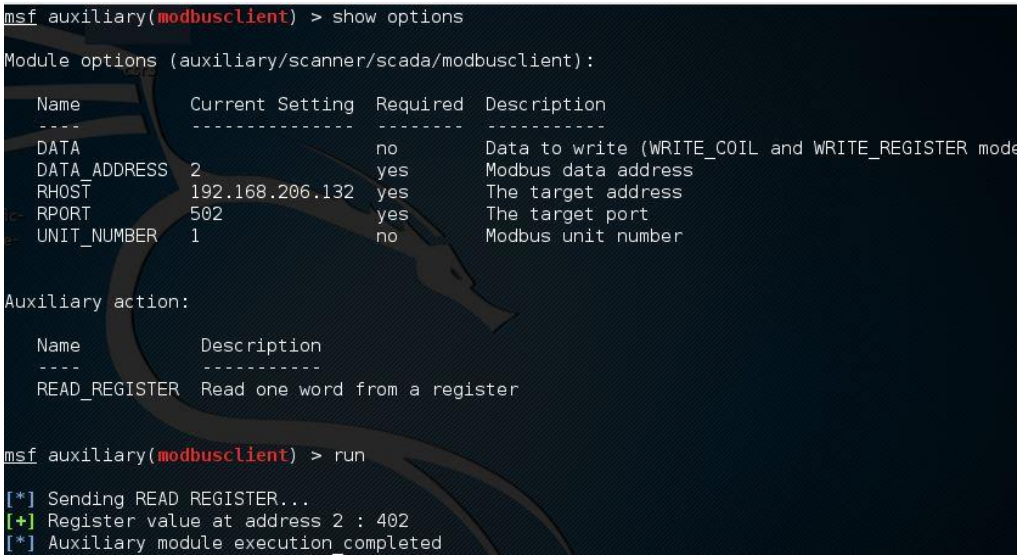
Modbusclient, PLC üzerindeki verileri Modbus/TCP protokolünü kullanarak okumaya veya yazmaya yarayan Metasploit modülüdür. Orijinal modbusclient modülü EsMnemon tarafından protokolün Fonksiyon Kodu'nu 0x06 kullanan salt-yazılır modülüydü ("Write Single Register"). Arnaud Soullie; 0x01 (Read Coil), 0x03 (Read Holding Register) ve 0x05 (Write Single Coil) fonksiyon kodlarını dahil etmek için kod üzerinde değişiklikler yapmıştır [114].

Fonksiyon Kodu 0x01 (Read Coil) kullanılarak başarıyla çalıştırılan modbusclient modülü kullanıcıya uzak PLC cihazındaki 1-2000 arasında komşu sarmalların durumunu okumasına olanak sağlar. Şekil 4.13'de gösterilen DATA_ADDRESS bölümü, döndürülen bobin durumu (0x0000 – 0xFFFF) için 2 baytlık başlangıç adresini belirtir. Modbus sunucusundan dönen cevap veri alanında her bobin için bir biti temsil eden bobin durumudur [80].

Fonksiyon Kodu 0x03 (Read Holding Register) kullanılarak başarıyla çalıştırılan modbusclient modülü kullanıcıya uzak PLC cihazındaki 1-2000 arasında komşu yazmaç girişleri okumasına olanak sağlar. Şekil 4.14'te gösterilen DATA_ADDRESS bölümü döndürülen yazmaç durumu (0x0000 – 0xFFFF) için 2 baytlık başlangıç adresini belirtir. Modbus sunucusundan dönen cevap, cevap mesajında her yazmaç için iki baytlık yazmaç değeridir [80].

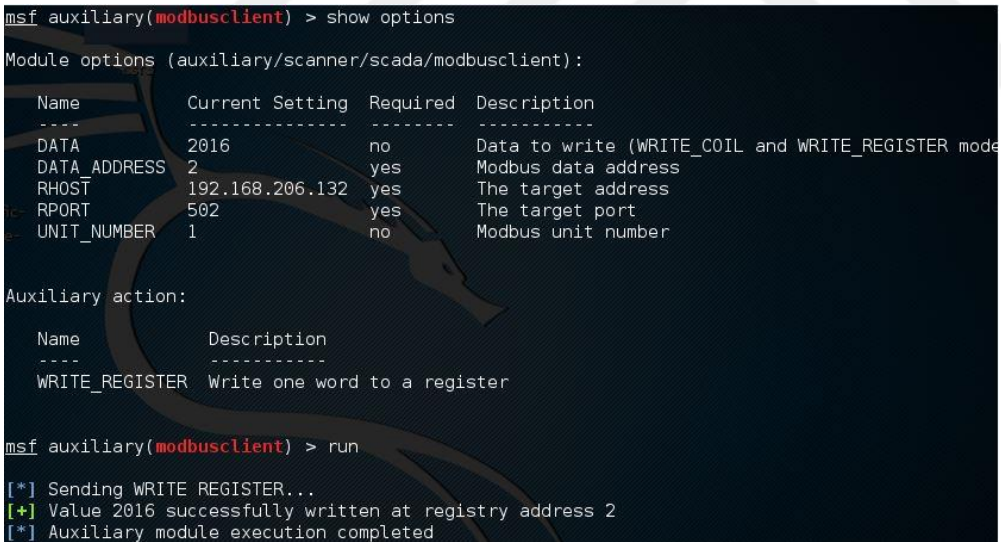
Fonksiyon Kodu 0x05 (Write Single Coil) kullanılarak başarıyla çalıştırılan modbusclient modülü kullanıcıya uzak PLC cihazının bobinine tek çıktı (ON veya OFF) yazmaya olanak sağlar. Şekil 4.14'te gösterilen DATA alanı kullanılarak girdi veri değeri, çıktının ON olması için 0xFF00 değerini, OFF olması için 0x0000 değerini kabul eder. Diğer tüm girdi değerleri geçersizdir ve çıktıyı etkilemeyecektir [80].

Fonksiyon Kodu 0x06 (Write Single Register) kullanılarak başarıyla çalıştırılan modbusclient modülü kullanıcıya uzak PLC cihazındaki tekli meşguliyet yazmacına (single holding register) yazmasına olanak sağlar. Şekil 4.13'de gösterilen DATA_ADDRESS alanı yazılacak yazmaç adresini tanımlar (0x0000 – 0xFFFF). Bu isteğin başarılı bir şekilde çalıştırılması tanımlanan DATA alanının değerini yankılar [80].



Şekil 4.14. Modbusclient READ_REGISTER aksiyonu

Çalışmada Modbusclient modülü kullanılarak hedef sistemde yazmaç üzerindeki değerler sırasıyla Şekil 4.14 ve 4.15'te görüldüğü üzere okunabilmiş ve değiştirilebilmiştir.



Şekil 4.15. Modbusclient WRITE_REGISTER aksiyonu

4.3. Literatürdeki Kritik Altyapılara Yönelik Siber Saldırılar

Bilgi ve iletişim teknolojisinin gelişmesiyle birlikte haberleşme, ulaşım, enerji ve otomasyon gibi kritik altyapı sistemleri bu teknolojiyle entegre çalışır hale gelmiştir. Dolayısıyla bilgi teknolojilerinde oluşabilecek güvenlik açıkları direk olarak bilgi teknolojileri altyapısını kullanan kritik altyapı sistemlerini de etkileyebilmekte ve risk teşkil edebilmektedir. Bu

yüzden bilgi sistemlerine zarar vermek için kullanılan kötücül yazılımlar kritik altyapı sistemlerine zarar vermek için de kullanılabilmektedir. Bu sistemlere yönelik yapılan siber saldırıların motivasyonu genellikle siyasi olmakta ve amacı hedef alınan ülkenin kritik altyapılarına ve projelerine zarar vermektir.

Çalışmanın bu bölümünde ülkelerin toplum ve kamu düzenini ve ulusal güvenliğini ilgilendiren kritik bilgi sistemlerine yönelik gerçekleştirilmiş siber saldırılar incelenmiştir.

4.3.1. Sibirya boru hattı patlaması

1982 yılında yeni inşa edilmiş trans-Sibirya boru hattının büyük bir kısmını buharlaştırarak Sibirya'nın ortasında bir patlama meydana gelmiştir. Bu patlama 2. Dünya Savaşı'nda Japonya'ya atılan nükleer bombanın 1/7 oranında bir etki yaratmış ve Sovyetler Birliğine petrol gelirinden 8 milyar dolar gelir getiren boru hatları ciddi oranda zarar görmüştür. Yalnız son zamanlarda CIA tarafından gerçekleştirildiği kamuoyuna duyurulmuştur [115].

CIA yetkilisinin yaptığı açıklama şu şekildedir: "Böyle muazzam bir tesisteki vanalar, kompresörler ve depolama alanlarının çalışmasını otomatik hale getirmek için Sovyetler karmaşık kontrol sistemlerine ihtiyaç duymuşlardır… Rus boru hattı yetkilileri gerekli yazılım için ABD'ye yakınlaştı fakat geri çevrildiler. Ruslar yılmadan başka yerlere baktı; KGB gerekli kodları çalmak için Kanadalı yazılım tedarikçisine sızma girişiminde bulundu. Amerika istihbaratı ve Rus istihbaratına çift taraflı olarak çalışan Vladimir Vetrov (Kod Adı: Farewell) bu duruma sinirli bazı Kanadalılarla işbirliği içindedir. Boru hattının yazılımı; pompaların, tribünlerin ve vanaların çalışmasını saptırmak içindir. Bir süre sonra pompa hızlarını ve vana ayarlarını sıfırlar ve boru hattının kaynaklarına ve bağlantılarına giden kabul edilebilir basıncı üretir. Sonucunda uzaydan görülebilecek düzeyde devasa bir patlama oldu. Beyaz Saray, kızılötesi uydularından Sovyetler'in ortasında bazı olağan dışı uyarılar aldıklarını belirtti [116]."

4.3.2. The Salt River Proje (SRP) ele geçirme olayı

1994 yılında Lane Jarrett Davis, Salt River Projesi (SRP) bilgisayar ağına çevirmeli modem üzerinden yetkisiz erişim sağlamış ve fatura bilgilerine erişmiştir. Sisteme daha sonra girebilmesi için arka kapı bırakmıştır. Aynı zamanda, SRP SCADA sistemi Phoenix'teki

müşterilere su dağıtımı için kullanılan yaklaşık 210 km'lik kanalı kontrol etmektedir. Mr. Davis kanalları kontrol eden kritik sistem üzerinde en az 5 saatlik bir oturum açmıştır. Su ve güç izleme ve dağıtımı, finans, müşteri ve kişisel bilgileri içeren korumasız verileri ele geçirmiştir. Login ve parola dosyaları, bilgisayar sistem kayıt dosyaları ve "root" yetkilerini ele geçirmiştir. Dahası, SRP ve Ulusal Meteoroloji Servisi'nin Ulusal Şiddetli Fırtına Laboratuvarı arasındaki Doppler-radar araştırma projesine de erişmiştir. SRP, bu saldırı nedeniyle düşük verimliliği hariç tahmini 40,000$ kayba uğramıştır [117].

Bu sızma olayı Roosevelt Barajı'na yapılan saldırıyla bağlantılıdır ve sürekli olarak gündeme gelen bir efsane haline gelmiştir. Daha önce ABD Temsilciler Meclisi'nin yaptığı açıklamada "bir çocuk korsan Arizona'da Roosevelt Barajı'nın faaliyetlerini kontrol eden firmaların ağına yetkisiz erişim sağladı" denmiştir. Aynı zamanda bu saldırı yapıldığında Mr. Davis 27 yaşındaydı ve SRP ve Roosevelt Barajı arasında bir bağlantı olmadığı belirtilmektedir.

4.3.3. Houston limanı sistem arızası

2001 yılında genç bir bilgisayar korsanı (Aaron Caffrey), bir bayan sohbet odasını hedef almak için Texas'taki Houston Limanı bilgisayar sunucularına sızmıştır. Saldırıda, dünyanın en büyük 8. limanında düzenleme yapmak için kullanılan bilgisayar sistemlerine hizmet dışı bırakma saldırısı yapılmıştır. Gemi kaptanları için kritik bilgiler içeren limanın web servisi hizmet dışı kalmıştır. Bu yüzden gemilerin navigasyon bilgileriyle limandan giriş ve çıkışlarından sorumlu olan demirleme ve destek firmaları hizmet veremez duruma gelmiştir [118].

4.3.4. Slammer solucanı

2003 Mayıs'ta kurumsal bir firmada çalışan bir personel, Microsoft SQL versiyonun güncel olmadığının farkına varmadan dizüstü bilgisayarına bir yazılım yüklemiştir. Bir süre sonra, kullanıcı bir internet servis sağlayıcı üzerinden e-posta sunucusuna erişmek için bilgisayarını internete bağlamıştır (şirket politikalarını çiğneyerek). Böylece SQL-slammer solucanı internete bağlı olan makinaya bulaşmıştır. Çalışan daha sonra bilgisayarını ofise getirmiş ve ağa bağlanmıştır. Böylece SQL-slammer solucanı kurumsal ağa bulaşmıştır [119].

Güvenlik duvarı olmayan ve veri toplama sunucusu olan kontrol sistemi ve geliştirme kontrol sistemi enfekte olmuştur. Bu durumda daha fazla bulaşma olmadan sunucu kontrol ağından çıkartılmak zorunda kalınmıştır. Üretimde ciddi bir etki olmamıştır, fakat bazı geçmiş veriler sunucunun durması sürecinde kaybedilmiş ve tekrar manuel olarak oluşturulmak durumunda kalınmıştır.

4.3.6. Kaliforniya kanal sisteminin hacklenmesi

Kaliforniya Kanal Sistemi'nin bir çalışanı Sacramento Nehri'den suyu yönlendirmek için kullanılan bilgisayara yetkisiz bir yazılımı yüklemekten ve zarar vermekten yargılanmıştır. 61 yaşındaki Tehama Colusa Kanal Otoritesi (TCAA) elektrik danışmanı olan Michael Keehn, "yetkisiz bir şekilde kasten korunan bir bilgisayara zarar vermekten" 10 yıl hapis cezasına çarptırılmıştır.

İddialara göre; Keehn, TCAA'daki SCADA sistemine yetkisiz bir yazılımı yüklemiştir. Bu sisteme erişimi 15 Ağustos 2007 yılındadır. Elektrik danışmanı olarak TCAA'daki bilgisayar sistemlerinden sorumludur. 16 personelle birlikte TCAA Kaliforniya'daki tarımsal alanlar için Tehama Colusa ve Corning Kanalı olmak üzere 2 kanalı kontrol etmektedir. Her iki sistem de devletin hüküm ve tasarrufundadır. ABD Adalet Bakanlığı temsilcilerinden Robin Taylor; TCAA SCADA sistemlerine bir saldırı olmasında sistem çevrim dışı kalsa bile kanallar çalışmaya devam eder demiştir. Bilgisayarlar çalışmadığı zaman manuel olarak çalıştırılırlar. Bu sızmanın TCAA'ya 50,000 $'dan fazla zararı olmuştur [120].

4.3.7. ABD'de elektrik şebekesi casusluk ihlali

Wall Street Gazetesi 2009 Nisan'da Rus ve Çinli casusların Amerika elektrik şebekesine sızdıklarını yazmıştır [121]. Milletvekilleri kaçınılmaz tehditlerle mücadele etmek için hükümete yetki verecek tedbirlerin dahil olduğu elektrik sektöründe siber güvenliği artıracak teklifler getirmişlerdir.

Elektrik endüstrisinde siber güvenlik danışmanı Bob West, NERC'in endüstrinin proaktif olması konusunda teşvik edici olduğuna dikkat çekmiştir.

4.3.8. Nitro saldırıları

Nitro saldırıları öncelikle kimyasal ve gelişmiş materyaller üzerinde çalışan, araştırma, geliştirme ve üretim firmalarını hedef almıştır. Saldırganların amacı endüstriyel espiyonaj yapmak, tasarım dokümanları, formülleri ve üretim süreçleri gibi fikri mülkiyetleri toplamaya yöneliktir.

Saldırının metodolojisinde, saldırganlar hedef aldıkları firmaların çalışanlarına içerisinde kötücül eklenti bulunan bir e-posta göndermişlerdir. E-posta içerikleri iş ortağıyla davetiye paylaşmak ve güvenlik güncelleme zamanlarının geldiğiyle ilgilidir. Firma çalışanı e-posta içeriklerini açtıklarında çalıştırılabilir dosya bir arka kapı oluşturur ve bu Truva atı Çin merkezli bir C&C sunucuyla 80. port üzerinden şifreli bir şekilde iletişim kurar. Saldırgan böylece etki alanındaki Windows makinaların parola özetlerini ele geçirir [122].

4.3.9. Stuxnet solucanı

Stuxnet solucanı; siber güvenlik camiası tarafından "ezber bozan" (game-changer) kötücül bir yazılım olarak tanımlanmaktadır [123]. Çünkü, bu kötücül yazılımın karmaşıklığı, amacı ve çıkarımları diğer kötücül yazılımlardan farklıdır. Stuxnet solucanının gelişimi ve yayılımı siber teknolojinin, dünya politikasına yön verebilecek bir tehdit olabileceğini göstermiştir.

Stuxnet solucanı, diğer bilgisayar solucanları gibi güvenlik açığı olan bir bilgisayardan bir diğerine ayrım gözetmeksizin yayılmaktadır. Diğer binlerce bilgisayar solucanından ayıran en büyük özelliği Natanz'da İran'ın nükleer zenginleştirme tesisinin özellikleriyle eşleşen sadece Endüstriyel Kontrol Sistemi'ne (ICS) girdiğinde kendi yükünü ortaya çıkarmak için tasarlanmış olması ve içerisinde 4 adet Windows işeltim sistemlerini istismar eden 0 gün zafiyeti bulunmasıdır. Bu gerçekleştiğinde, Natanz'daki santrifüjlerin kontrolü için kullanılan Programlanabilir Mantıksal Denetleyicilerin (PLC) kodlarını kurcalar. Nihayetinde binlerce santrifüj zarar görmüş ve İran Nükleer faaliyetleri sekteye uğramıştır. Daha önce hiçbir solucan ICS üzerinden fiziksel olarak sistemlere zarar verememiştir.

Stuxnet solucanı, içerdiği fonksiyon ve yapısından dolayı kritik altyapılara yönelik gerçekleştirilen diğer siber saldırılardan daha farklı bir boyutta değerlendirilmelidir. Bu yüzden, bu bölümde Stuxnet'e ait ayrı bir değerlendirme bölümü yapılmıştır.

Knopová çalışmasında [124], 3. Dünya Savaşı'nın siber uzayda gerçekleşebileceğinden bahsetmektedir. Konvansiyonel silahların ve savaşların maddi ve manevi maliyeti çok ciddi rakamlara ve insan hayatına mal olabileceğinden siber savaş gerçeği bu tezi doğrular niteliktedir. Özellikle bu çalışmada anlatılan Stuxnet solucanı ile saldırıyı gerçekleştiren taraf hedef sisteme sızma ve zarar verme işlemini başarıyla gerçekleştirmiş ve bu saldırıyı kaynağını gizleyerek gerçekleştirmiştir. Bu sayede normalde savaş sebebi sayılabilecek bir saldırı yapmaktan ve can kaybına sebebiyet vermeden sadece hedef sistemlere zarar vermiştir. İran yapılan bu saldırıdan sonra saldırının kaynağı olarak iddia edilen ABD ve İsrail'e karşı hukuki bir süreç başlatamamıştır. Çünkü bahsedildiği gibi yapılan saldırının kaynağı ABD ve İsrail'i işaret etmemektedir.

Yukarıda anlatıldığı gibi Stuxnet solucanı içerisinde bulundurduğu 4 adet 0-gün güvenlik açığı ve o güne kadar keşfedilmiş en karmaşık kötücül yazılım olmasından dolayı kötücül yazılım analizcilerine yeni bir alan açmış ve tüm dünyada büyük ses getirmiştir. Aynı zamanda endüstriyel kontrol sistemlerinin denetimini sağlayan PLC cihazlarına yönelik gerçekleştirilmesi kritik altyapıların siber ortamdan korunması ve güvenliğine yönelik yeni çözüm önerilerinin doğmasına ve farkındalığın artmasına imkan sağlamıştır.

4.3.10. Duqu truva atı

2011 yılında Word dokümanlarına yönelik Duqu saldırıları, içerisinde 0-gün açığı bulunan (CVE-2011-3402) güvenlik açığı tespit edilmiştir. Bu istismar saldırganlara bir Word dokümanından kernel moda atlamasına olanak sağlar. Word dosyası açıldığında istismar modülü tetiklenmiş olur ve bu istismar HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\Zones\4\"CF1D" kayıt değerine bakarak ilk olarak bilgisayarın ele geçirilip geçirilmediğini kontrol eden kernel mod shellcode barındırır. Bilgisayar ele geçirildiyse, shellcode mevcuttur. Ele geçirilmediyse; shellcode, Word dokümanından iki çalıştırılabilir dosyanın şifresini çözer: bir driver dosyası ve installer DLL. Daha sonra yükleyici yapılandırma dosyası tarafından tanımlanan services.exe içine kodu enjekte eden çıkarılmış yükleyici dosyasına çalışmayı geçirir. Kod daha sonra installer DLL'i çalıştırır. Sonunda, shellcode kendini hafızadan silerek sıfırlarla yer değiştirir [125].

4.3.11. Shamoon zararlı yazılımı

15 Ağustos 2012 tarihinde Suudi Arabistan'ın milli petrol üretimi, satışı, ham petrol rafinerisi, doğal gaz ve petrol ürünleri firması olan Suudi Arabistan Petrol Firması'nın (Saudi Aramco) yaklaşık 30,000 Windows işletim sistemi tabanlı bilgisayar ağına bir bilgisayar virüsü bulaşmıştır. Saudi Aramco, dünya petrol pazarında çok büyük bir paya sahiptir. Global arzın %10'nu, global üretimin %13'nü elinde tutan ve yıllık 200 milyar $ geliri olan Dünya'nın en büyük petrol üreticisidir.

Shamoon kötücül yazılımı Aramco'daki çalışanların kişisel bilgisayarlarına bulaşmış ve bilgisayarların hard disklerindeki verileri fark gözetmeksizin silmiştir. Herhangi bir petrol sızıntısı, patlaması veya daha büyük bir arızanın olmamasına rağmen bu saldırı firmanın üretim bilgilerinin silinmesi gibi üretim ve iş faaliyetlerini ciddi oranda etkilemiştir. Shamoon aynı zamanda RasGas, Qatar Petrol ve ExxonMobil gibi diğer gaz ve petrol firmalarına yayılmıştır.

Shamoon saldırısı Orta Doğu'da herhangi bir fiziksel hasara sebebiyet vermese de dünya çapında kritik servis sağlayıcıları için risk değerlendirmesine ikincil etkileri olmuştur. Bu olay ABD ve İran arasında ciddi güvenlik kaygılarını artırmıştır. Dönemin ABD Savunma Bakanı Leon Panetta, Shamoon için "çok karmaşık" ve "bu tip araçların kullanımı çok endişe verici" şeklinde açıklama yapmıştır [126].

4.3.12. Flame zararlı yazılımı

Flame virüsü oldukça gelişmiş, Microsoft Windows işletim sistemi tabanlı çalışan bilgisayarlara bulaşan ve casusluk amacıyla yazılan bir yazılımdır. Aynı zamanda, yerel bilgisayar ağları içinde yayılmak için gereken mekanizmalardan biri oldukça dikkat çekicidir. Kendisini Windows güvenlik güncellemesi olarak saklayarak, Windows güncelleme üzerinden yerel ağ üzerinden yayılır.

Budapeşte Üniversitesi CrySyS Lab.'ın yapmış olduğu teknik rapora göre; Flame, klavye girdileri, ekran görüntüleri ve mümkünse mikrofon ve kamera görüntüleri gibi bilgileri toplamaktadır. İlk bulaşmasından sonra indirilebilen birçok modülü mevcuttur. Tamamen yapılandırılmış boyutu 20 mb'tan fazladır. Bu boyut bir kötücül yazılım için oldukça

fazladır. Flame, Windows güncellemeyi kullanarak ağlar arasında yayılır ve aynı zamanda çıkarılabilir sürücü ile hava boşluğunu aşabilir. Flame bir ağ içerisinde bir bilgisayara bulaştığında, kendisini *update.windows.com* için vekil sunucu olarak kaydetmek için WPAD'i (Web Proxy Auto-Discovery Protocol) kullanır ve kendisini ağdaki diğer bilgisayarlara yüklemek için sahte güvenlik güncellemesi hizmeti verir [127]. Flame hızlı bir şekilde yayılmaz, büyük çoğunluğu Orta Doğu'da olmak üzere çok az sayıda bilgisayar bu kötücül yazılımdan etkilenmiştir. İlk varyasyonu İran (CERT) tarafından 2012 Mayıs'ında bulunmuştur. Kaspersky'a göre [9]; en az 2010 yılına kadar aktifti fakat CrySys Lab, 2007 yılında bilgisayar güvenliği firması olan Webroot tarafından bulunan ve Flame'de kullanılan dinamik bağlantı kütüphanesinin adı olan WAVESUP3.DRV dosya ismini raporlamıştır. Bu durum Flame'in veya daha önceki varyasyonlarının o dönemde zaten aktif olduğunu göstermektedir. Bu yazılımın bulaştığı bilgisayarların büyük çoğunluğu İran coğrafyasındaydı. Hedefleri arasında devlet kurumları, özel firmalar, eğitim enstitüleri ve belirli bireyler bulunmaktadır. *The Washington Post* gazetesinde [128] Flame veya benzeri Stuxnet gibi kötücül yazılımların ABD ve İsrail tarafından geliştirildiği iddia edilmektedir.

4.3.13. Doğalgaz boru hattı firmalarına siber saldırılar

2012 yılında 6 ay boyunca, kimliği tam olarak belirlenemeyen (Çin kaynaklı olduğu iddia edilmekte) bir hacker grubu tarafından ABD gaz boru hatlarının kontrol sistemlerine devamlı ve eşgüdümlü bir şekilde siber saldırı düzenlenmiştir. Saldırganlar "spear-phishing" tekniğini kullanarak boru hattı kontrol sistemlerine erişim sağlayıp parolaları çalmayı hedeflemişlerdir. Saldırganlar gönderdikleri e-postaları hedef aldıkları kişilerin arkadaşı veya tanıdığı birinden geliyormuş gibi yapmışlar ve e-postadaki eklenti veya link açıldığında kötücül yazılım hedef bilgisayara bulaşmıştır.

ABD İç Güvenlik Bakanlığına göre gönderilen spear-phishing'lerin ilki Mart 2012'de tespit edilmiş ve gaz firmasındaki küçük bir çalışan grubu hedef almıştır [129].

4.3.14. Ukrayna elektrik kesintisi

23 Aralık 2015 tarihinde Ukrayna'da Ivano-Frankivsk bölgesindeki yerleşkelerin yaklaşık yarısı (1,4 milyon insan) birkaç saatlik elektrik kesintisi yaşamışlardır. ESET firmasındaki siber güvenlik araştırmacılarına göre bu kesintinin sebebi bir siber saldırıdır [130].

ESET çalışanlarına göre; saldırganlar, yeniden önyükleme yapamayacakları şekilde tasarlanan hedef bilgisayarlardaki KillDisk bileşenine "*BlackEnergy*" arka kapısını kullanarak saldırılarını gerçekleştirmişlerdir.

BlackEnergy arka kapısı, truva atı modüler yapısından oluşmakta ve belirli görevleri yürütmek için çeşitli indirilebilir bileşenleri kullanmaktadır. 2014 yılında, Ukrayna'da yüksek profilli devlet kurumlarına karşı bir dizi siber casusluk faaliyetlerinde kullanılmıştır. Elektrik dağıtım şirketlerine karşı son saldırılarda, KillDisk Truva atı indirilmiş ve daha önce BlackEnergy Truva atı bulaşmış sistemler üzerinde çalıştırılmıştır.

BlackEnergy ve KillDisk arasındaki ilk bağlantı Kasım 2015'te Ukrayna CERT-UA tarafından raporlanmıştır. Bu sırada birçok medya kuruluşu Ukrayna yerel seçimleri sırasında saldırıya uğramıştır. Raporda bu saldırılar sonucunda çok sayıda video materyallerinin ve çeşitli dokümanların tahrip olduğu iddia edilmiştir.

Ukrayna güç dağıtım firmalarına yönelik gerçekleştirilen saldırılarda kullanılan KillDisk varyasyonu bazı ek fonksiyonlara sahiptir. Sistemin önyükleme yapamaması için sistem dosyalarını silmesinin yanı sıra bu özel varyant endüstriyel kontrol sistemlere sabotaj düzenlemek için tasarlanmış kodlara sahiptir.

ESET zararlı yazılım analisti Anton Cherepanov; "KillDisk'in normal fonksiyonlarının haricinde aynı zamanda Endüstriyel Kontrol Sistemlerinde sıkça kullanılan platformlara ait işlemleri sonlandırmaya çalıştığını" söylemektedir [130].

Bu işlemler hedef sistemde bulunursa, Truva atı bu işlemleri sadece durdurmaz aynı zamanda sistemin yeniden çalışmasını zorlaştırmak için rasgele verilerle hard disk üzerinde ilgili çalıştırılabilir dosyayı yazar.

Cherepanov aynı zamanda "Ukrayna'da birçok elektrik dağıtım firmalarında tespit edilen KillDisk kötücül yazılımı üzerinde yaptığımız çalışmalar, Kasım 2015'te Ukrayna medyasına düzenlenen saldırılarda kullanılan araçlarla aynı olduğunu göstermektedir" demiştir [130].

BlackEnergy'nin 2015'teki gelişimi

BlackEnergy aktif olduğunda, BlackEnergy varyantları enfekte bilgisayarın gerçekten istenilen hedef olup olmadığını değerlendirmek amacıyla belirli kriterleri kontrol etmeye olanak sağlar. Bu durumda, normal bir BlackEnergy varyantının damlalıkları (dropper) sisteme itilir.

C&C sunucularından farklı olarak BlackEnergy yapılandırması "build_id" değerini barındırır. Bu değer BlackEnergy kötücül yazılımı operatörü tarafından bulaşma girişimini veya ayrı bulaşmaları tanımlamak için kullanılan benzersiz bir metin dizesidir. Harflerin ve sayıların kombinasyonları hedef sistem hakkında açığa çıkan bilgileri kullanabilir.

ESET tarafından 2015 yılında Ukrayna'ya düzenlenen saldırıda tanımlanan "build_id" değerleri aşağıdaki gibidir:

- 2015en
- khm10
- khelm
- 2015telsmi
- 2015ts
- 2015stb
- kiev_o
- brd2015
- 11131526kbp
- 02260517ee
- 03150618aaa
- 11131526trk

Bu değerlerden bazıları belirli anlamlara gelmektedir. Mesela "2015telsmi" değeri Rusçada Sredstva Massovoj Informacii (Kitle İletişim Araçları, SMI) kısaltması veya "2015en" enerji anlamına gelebilir.

Killdisk bileşeni

2014 yılında, bazı BlackEnergy varyantları “dstr” isimli enfekte olmuş sistemi çökertmek için tasarlanmış eklenti barındırıyordu. 2015’te ESET, BlackEnergy grubunun Win32/KillDisk.NBB, Win32/KillDisk.NBC ve Win32/KillDisk.NBD Truva varyantları gibi yeni yıkıcı bileşenler kullandığını tespit etmiştir. Bu bileşenin asıl amacı rasgele verilerle dokümanları üzerine yazarak ve işletim sistemini önyükleme yapmasına engel olarak bilgisayar üzerindeki veri depolama yerine zarar vermektir [131].

```
unicode 0, <a.ivf.ivr.ivs.izz.izzy.jmv.jss.jts.jtv.k3g.kmv.lrec.lrv.l>
unicode 0, <sf.lsx.lvix.m15.m1pg.m1v.m21.m21.m2a.m2t.m2ts.m2v.m4e.m4u>
unicode 0, <.m4v.m75.mani.meta.mgv.mj2.mjp.mjpg.mk3d.mkv.mmv.mnv.mob.>
unicode 0, <mod.moff.moi.moov.mov.movie.mp21.mp21.mp2v.mp4.mp4.infovi>
unicode 0, <d.mp4v.mpe.mpeg.mpeg1.mpeg4.mpf.mpg.mpg2.mpgindex.mpl.mpl>
unicode 0, <s.mpsub.mpv.mpv2.mqv.msdvd.msh.mswmm.mts.mtv.mvb.mvc.mvd.>
unicode 0, <mve.mvex.mvp.mvy.mxf.mxv.mys.ncor.nsv.nut.nuv.nvc.ogm.ogv>
unicode 0, <.ogx.orv.otrkey.par.pds.pgi.photoshow.piv.pjs.playlist.pl>
unicode 0, <proj.pmf.pmv.ppj.prel.pro.pro4dvd.pro5dvd.proqc.prproj.pr>
```

Şekil 4.16. KillDisk.NBB tarafından tahrip etmek için hedeflenen dosya uzantılarının bir kısmının listesi [131]

İletişim firmalarına yönelik saldırılarda kullanılan Win32/KillDisk.NBB varyantı birçok doküman ve dosyayı tahrip etmek için kullanılmaktadır. Üzerine yazmaya ve silmeye çalıştığı uzun bir dosya uzantı listesi vardır. Varyantın tam listesi 4000’den fazla dosya uzantısı içerir ve Şekil 4.15’te ilgili dosya uzantılarının bir kısmı gösterilmiştir.

Ukrayna’da enerji firmalarına yönelik gerçekleşen saldırılarda kullanılan KillDisk bileşeni biraz daha farklıdır. ESET’in analizlerine göre yeni versiyondaki değişiklikler:

- Tahrip yükü aktif olması gerektiğinde belirli bir zaman gecikmesini ayarlamak için komut satırı argümanını kabul eder.
- Windows olay loglarını siler: Uygulama, Güvenlik, Setup, Sistem
- Doküman silmeye daha az odaklıdır. Sadece 35 dosya uzantısı hedef alınmış olup ilgili uzantılar Şekil 4.16’da gösterilmiştir.

```
unicode 0, <.crt.bin.exe.db.dbf.pdf.djvu.doc.docx.xls.xlsx.jar.ppt.pp>
unicode 0, <tx.tib.vhd.iso.lib.mdb.accdb.sql.mdf.xml.rtf.ini.cfg.boot>
unicode 0, <.txt.rar.msi.zip.jpg.bmp.jpeg.tiff>,0
```

Şekil 4.17. KillDisk bileşeninin yeni varyantı tarafından tahrip etmek için hedef alınan dosya uzantılarının listesi [131]

Sistemin önyükleme yapamaması için sistem dosyalarını silmesinin yanı sıra – Böyle tahrip edici trojan için tipik işlevselliği – özellikle endüstriyel sistemleri sabote etmek amacıyla elektrik dağıtım firmalarında tespit edilen KillDisk varyantı bazı ek işlevler içeriyor. Aktif duruma geldiğinde, KillDisk varyantı iki tane standart olmayan işlemi arar ve sona erdirir: komut.exe ve sec_service.exe.

Bu işlemlerden ikincisi (sec_service.exe) bir endüstriyel kontrol sisteminde kullanılan yazılımın (ASEM Ubiquity veya ELTIMA seri-ethernet konnektörü) kullandığı bir işlem ve zararlı yazılım bu uygulamanın çalışmasını engellemekle kalmayıp aynı zamanda rasgele verilerle çalıştırılabilir dosyanın üzerine yazmaktadır.

Bu işlemlerden birincisi (komut.exe) hakkında detaylı bir bilgi yoktur, fakat Türkçede command yerine kullanılan komut anlamına gelmektedir. Bu durum Türkçe işletim sistemlerinin hedef alınabileceğini göstermektedir. Yukarıda açıklanan "build_id" değerlerinden "11131526trk" değerindeki "trk", "türk" olarak temsil edilmiş olabilir, fakat "11131525" rakamlarının anlamları henüz anlaşılamamıştır. Stuxnet solucanındaki 19790509 değerindeki gibi İran-İsrail ilişkilerindeki gerilime manidar bir değer olup olamayacağı araştırmalarına devam edilecektir.

Tezin bu bölümünde EKS sistemlerinde kullanılan bilşenlerin siber güvenlikle ilişkisi, bu bileşenlerin zafiyetleri, bu bileşenlere yönelik tehditler ve olası saldırılar sonucu oluşabilecek risklerden bahsedilmiştir. Ayrıca, SCADA sistemlerinin sızma testlerinde kullanılan araçlardan ve mevcut SCADA sistemlerine gerçekleştirilen siber saldırılardan bahsedilerek bu sistemlere yönelik yapılan siber saldırılar sonucu olası bir fonksiyonel bozukluğun ulusal güvenliği dahi tehdit edebileceği vurgulanmıştır. Bu bölümde özellikle Modbus TCP protokolünün zafiyetlerinden ve bu protokole yönelik saldırılardan bahsedilmesi, tezin ilerleyen bölümünde önerilen Modbus protokolünün güvenliği çalışması için önemli bir altyapı teşkil etmektedir.

5. MODBUS TCP PROTOKOLÜ GÜVENLİĞİNE YÖNELİK ÖNERİLEN ÇALIŞMA

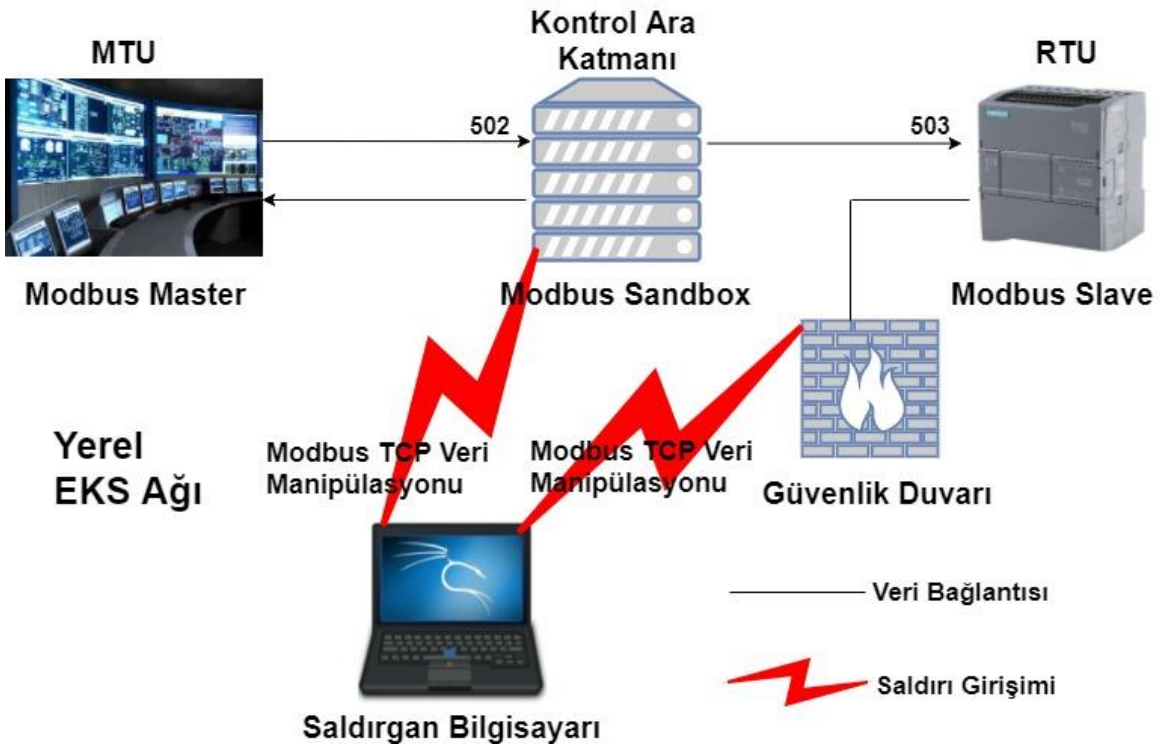
Çalışmanın bu bölümünde daha önce detayları verilen Modbus TCP protokolünün kaynak IP adresi kontrolü ve şifreleme kullanmama zafiyetleri gösterilmiş ve bu güvenlik açıkları araya girme saldırısı (MITM) ile detayları aşağıdaki bölümlerde anlatılacak olan simülasyon ortamında akan Modbus paketleri açık metin olacak şekilde görüntülenebilmiş ve Metasploit Framework modülü olan Modbusclient kullanılarak aynı simülasyon ortamında yazmaç değerlerinin okunup değiştirilebildiği gözlemlenmiştir. Saldırı verileri ve normal veriler gönderilirken Wireshark aracı kullanılarak paketler yakalanmış ve bu veriler karşılaştırılarak analiz edilmiştir. Yapılan bu analiz sonucunda saldırıyı engellemeye veya hafifletmeye yönelik Python programlama dili kullanılarak bir kontrol ara katmanı geliştirilmiştir. Ayrıca kontrol ara katmanına detayları ileri bölümlerde anlatılacak olan kontrol sistemini yöneten operatör tarafından kasti veya yanlışlıkla yazmaç değerlerine belirli bir değer üzerinde değer girmesini engelleyecek bir kontrol fonksiyonu eklenmiştir. Böylece Modbus TCP protokolü ile haberleşen bir kontrol sistemine yönelik iç veya dış ağdan yetkisiz bir şekilde veri girilmesi ve siber güvenlik camiasında en fazla risk teşkil ettiği düşünülen tehditlerden biri olan ve literatürde "intruder" olarak isimlendirilen küskün veya kötü niyetli çalışanın belirlenen bir değerden fazla değer girmesinin engellenmesi veya hafifletilmesi amaçlanmıştır.

5.1. Deney Düzeneği Ortamı

Modbus TCP protokolünün güvenliğini sağlamaya yönelik yapılan çalışmada Modbus TCP paketlerini analiz etmek amacıyla Modbus Poll [132] isimli bir program kullanılarak simülasyon ortamı hazırlanmıştır. Hazırlanan bu simülasyon ortamı yerel bir ağ üzerinden Modbus TCP protokolü ile haberleşmekte olup internet bağlantısı bulunmamaktadır. Saldırıları gerçekleştirmek amacıyla Kali Linux 2.0 işletim sistemi kullanılmış ve kontrol ara katmanı olarak paketlerin kontrol edileceği ve içerisinde çalışma kapsamında geliştirilen Python kodunun çalıştığı Ubuntu işletim sistemi tercih edilmiştir.

Modbus TCP protokolünün güvenliğine yönelik önerilen deney düzeneğinin topolojisi Şekil 5.1'de verilmiştir. Topolojiye göre MTU olarak Windows 7 makinası üzerinde yüklü olan Modbus Master çalışmaktadır. Modbus paketlerini varsayılan 502 portu üzerinden göndermektedir. Varsayım olarak bir üretim tesisinin veya nükleer bir santralin kontrol

sisteminin yönetildiği merkezi sunucu olarak düşünülebilir. RTU olarak Windows XP üzerinde yüklü olan Modbus Slave çalışmaktadır. Bu makinada 503 portu dinlemeye alınmış olup Modbus haberleşmesi bu port üzerinden sağlanmaktadır. Varsayım olarak bir üretim tesisinin sıcaklık değerlerini veya nükleer bir santralin santrifüj dönme frekans değerlerini merkezi sunucuya göndermekle görevli bir PLC cihazı olarak düşünülebilir. Kontrol ara katmanı olarak, belirtilen iki cihaz arasındaki haberleşme sırasında gelip giden paketlerin kontrol edildiği, üzerinde Modbus TCP protokol güvenliği sağlanması amacıyla yazılmış olan Python kodunun çalıştığı Ubuntu makinası bulunmaktadır. Detayları aşağıda anlatılacak olan koda göre makina 503. portunu dinlemeye almış olup MTU üzerinden girilen değerler ilk olarak kontrol ara katmanına gitmekte ve burada paketlerin kontrolünün ardından paketler PLC cihazına gönderilip cihaz üzerindeki yazmaçlara yazılmaktadır. Ayrıca Deney düzeneği sanal bir ortamda geliştirildiği için bu kısımda güvenlik duvarı olarak IP adresi tabanlı çalışan Windows güvenlik duvarı kullanılmış ve güvenlik duvarı üzerinde gerekli ayarların yapılabilmesi için sadece kontrol ara katmanı IP adresine izin verilecek, diğer istek yapan IP adreslerinden gelen isteklerin engelleneceği şekilde yapılandırılmıştır.

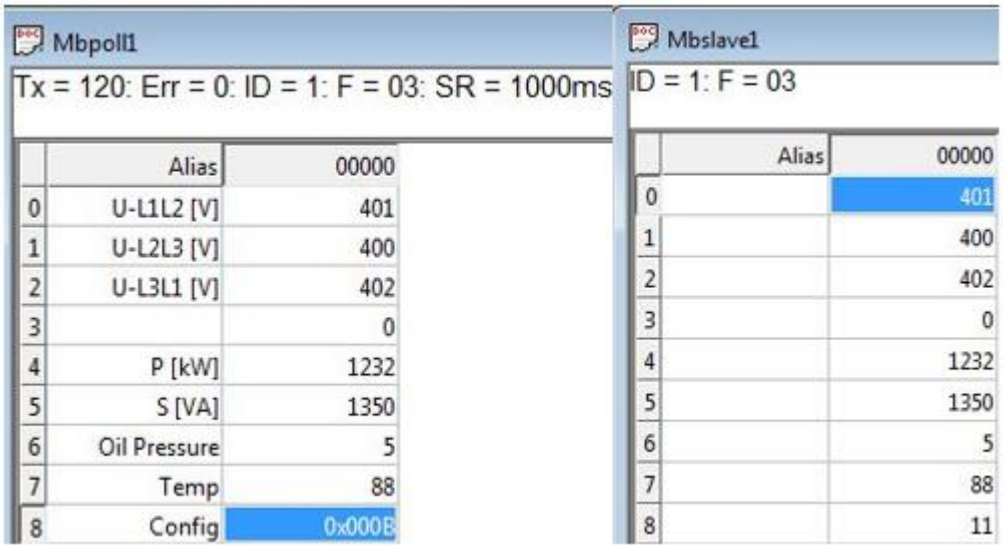


Şekil 5.1. Modbus TCP güvenliği için önerilen deney düzeneği topolojisi

Simülasyon ortamı, bahsedildiği gibi yerel bir EKS ağı için tasarlanmıştır. Bunun nedeni, SCADA sistemlerinin kullanıldığı EKS'lerin, sahada çok yüksek oranda internete açık olarak kullanılmaması ve kapalı bir ağda MTU ve RTU'ların haberleşmesinin gerçekleşmesidir. Dolayısıyla tez çalışması daha geniş bir alana çözüm üretebilmek amacıyla yerel bir ağda tasarlanmıştır.

Modbus TCP protokolüne yönelik paketlerin analizi için Modbus Poll ve Modbus Slave simülasyon ortamı kurulmuştur. Modbus Poll, Modbus protokolünü simule ve test etmek için Modbus Slave veya diğer cihazları geliştiren kişilere yardımcı olması amacıyla tasarlanmış Modbus Master simülatörüdür. Çoklu ara yüzle birçok Modbus Slave veya veri alanı aynı anda görüntülenebilmektedir. Her bir ekranda Modbus Slave ID, fonksiyon ve adres özel olarak belirlenebilmekte ve yazmaçlara okuma ve yazma işlemleri gerçekleştirilebilmektedir.

Önerilen deney düzeneğinde Modbus Master programı Windows 7 işletim sistemi üzerinde çalışmakta olup bu program daha önce detayları verilmiş olan MTU olarak çalışmaktadır. Modbus Slave programı ise Windows XP işletim sistemi üzerinde çalışmakta olup RTU olarak çalışmaktadır. Modbus Master ve Modbus Slave programlarının koştuğu bu işletim sistemleri aynı ağda olup birbirleriyle haberleşebilmektedirler. Böylece Modbus Master üzerindeki yazmaç değerlerine girilen değerler Modbus Slave üzerindeki yazmaçlara Modbus TCP protokolü ile gönderilip yazılabilmekte ve okunabilmektedir.

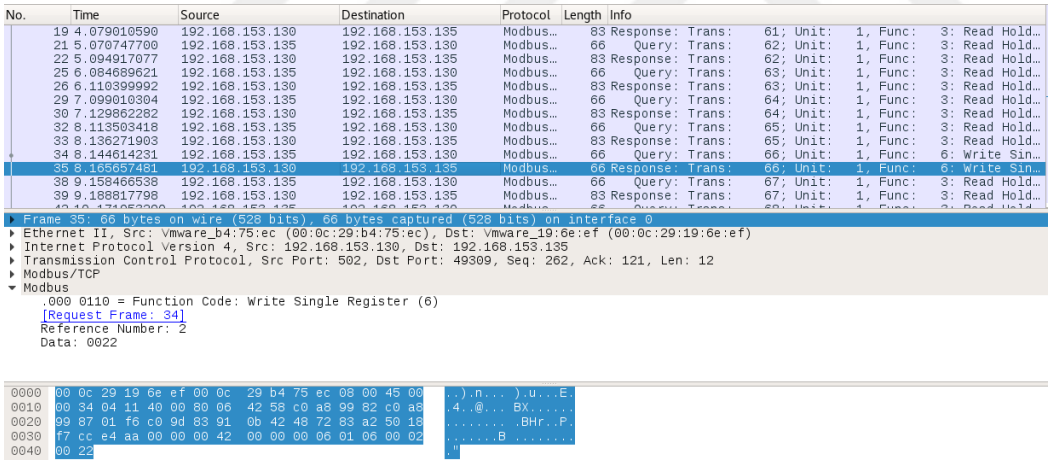


Şekil 5.2. Modbus Master ve Modbus Slave

Şekil 5.2'de çalışmada kullanılan Modbus Master ve Modbus Slave simülatörlerine ait ekran görüntüleri verilmiştir. Modbus Master'da yazmaçlara girilen değerler, aralarındaki Modbus TCP protokolü bağlantısı sayesinde Modbus Slave'deki yazmaçlara gönderilerek yazılmaktadır.

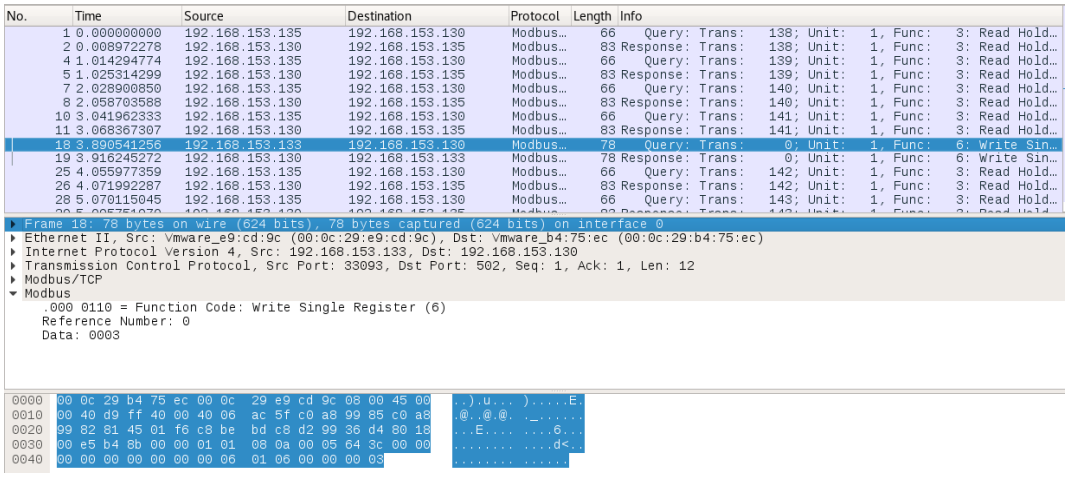
5.2. Paketlerin Analizi

Modbus Master, Modbus Slave ve saldırgan makinaları arasında akan Modbus TCP paketleri Wireshark aracı kullanılarak yakalanıp analiz edilmiştir. İlk etapta Modbus Master ve Modbus Slave makinaları arasında akan normal Modbus TCP paketleri yakalanmış ve daha sonrasında saldırgan makinasıyla Metasploit Framework Modbusclient modülü kullanılarak manipüle edilmiş Modbus TCP paketleri yakalanmıştır. Böylece normal Modbus TCP paketleriyle manipüle edilmiş Modbus TCP paketleri karşılaştırılarak analiz edilmiştir. Şekil 5.3'te Modbus Master ve Modbus Slave makinaları arasında akan Modbus TCP paketlerinin "Write_Register" fonksiyon koduyla Wireshark aracıyla yakalanması gösterilmiştir.



Şekil 5.3. Normal Modbus TCP paketi

Şekil 5.4'te ise saldırgan makinasıyla manipüle edilmiş Modbus TCP paketinin gönderildiği Wireshark çıktısı gösterilmektedir.



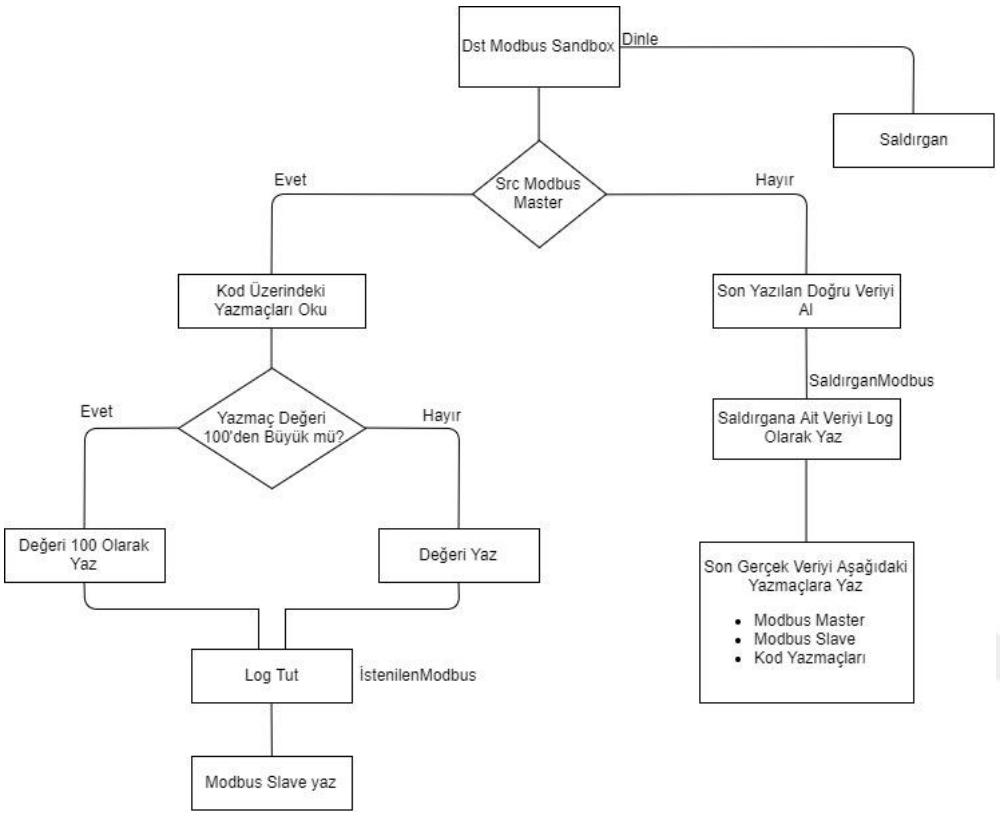
Şekil 5.4. Manipüle edilmiş Modbus TCP paketi

Yakalanan paketlerin karşılaştırılarak yapılan analizi sonucunda 192.168.153.135 IP adresli Modbus Master cihazından 192.168.153.130 IP adresli Modbus Slave cihazına Modbus TCP paketleri gönderilirken manipüle edilen paketlerde 192.168.153.133 IP adresli saldırgan makinesiyle gönderildiği gözlemlenmiştir. Paketlerin diğer parametrelerinde hiçbir değişiklik olmadığı sadece kaynak IP adreslerinin değiştiği ve paketlerin bu şekilde gönderildiği gözlemlenmiştir. Slave cihazı kendisine gelen paketlerde kaynak IP adresini kontrol etmediği fark edilmiştir. Yapılan bu analiz sonucunda iki cihaz arasında gerçekleşen haberleşme esnasında Modbus TCP paketinin gönderildiği kaynak IP adresinin kontrol edilmesi amacıyla Modbus Slave cihazına IP tabanlı Windows güvenlik duvarı kullanılmıştır. Ayrıca cihazlar arasında akan Modbus TCP paketlerini kontrol etmek yani paket içerisindeki veri bölümüne eşik değer olarak belirtilen değerden fazla değer girilememesi amacıyla bir ara katmanın geliştirilmesi amaçlanmıştır. Buna ek olarak, saldırganın kontrol ara katmanına olası bir saldırı yapabileceği ihtimaline yönelik bir güvenlik mekanizması geliştirilmiştir. Bu güvenlik mekanizması sayesinde Modbus Master haricinde gelen Modbus TCP istekleri engellenecektir. Böylece Modbus Slave cihazı sadece kontrol ara katmanından gelen Modbus TCP paketlerini kabul edip kendi yazmaçlarına işleyecek, başka bir IP adresinden gelecek Modbus TCP paketlerini ara katmandaki kontrol sonrasında kendi yazmaçlarına işlemeyecektir.

5.3. Kontrol Ara Katmanı (Modbus Sandbox)

Modbus Master ve Modbus Slave cihazları arasına yerleştirilen ve iki cihaz arasında akan Modbus TCP paketlerinin denetimi için bir kontrol ara katmanı geliştirilmiştir. Bu kontrol

ara katmanı, üzerinde çalışma kapsamında geliştirilen bir Python kodunun çalıştığı Ubuntu işletim sistemine sahip bir makina olup ağ üzerinde akan Modbus TCP paketlerini kendi üzerine alır ve geliştirilen kontrol ara katmanı ile denetim sağladığı için Sandbox olarak da isimlendirilebilir. Kontrol ara katmanının akış diyagramı Şekil 5.5'te verilmiştir.



Şekil 5.5. Kontrol ara katmanının akış diyagramı

Şekil 5.5'te verilen akış diyagramına göre çalışma kapsamında hazırlanan kod ilk başta kendi 502. portunu dinlemeye alır ve kendine gelen Modbus paketlerinin kaynak IP adreslerini alıp Modbus Master IP adresiyle karşılaştırır ve IP adresleri örtüşüyorsa kod üzerindeki yazmaçlardaki değerleri okur. Bu değerler 100'den büyükse yazmaç değeri olarak 100 yazar, 100'den küçükse değeri okuduğu gibi yazar. Burada belirlenen 100 değeri, simülasyon ortamında seçilen varsayılan bir değerdir. Bir sistem odasında ortamın sıcaklık değeri veya bir nükleer santralde santrifüj dönme frekans değeri olarak düşünülebilir. Daha sonra "İstenilenModbus" log dosyasına yazmaçlardaki değerleri kaydedip Modbus Slave cihazındaki yazmaçlara değerler yazılır. IP adresleri örtüşmüyorsa kod bunu saldırı olarak algılayacak ve en son yazdığı doğru veriyi alacaktır. Saldırgana ait veriyi "SaldırganModbus" isimli log dosyasına kaydeder. Daha sonrasında son gerçek veriyi Modbus Master, Modbus Slave ve kontrol ara katmanı üzerindeki yazmaçlara yazar.

Modbus TCP protokolünün güvenliğine yönelik çözüm olarak önerilen deney düzeneğiyle saldırgan Modbus Slave cihazının yazmaçlarına Metasploit Framework Modbusclient modülü kullanarak yetkisiz bir şekilde veri yazmaya çalıştığında Modbus Slave cihazı önündeki IP ve port tabanlı çalışan güvenlik duvarına takılacak ve yetkisiz bir şekilde veri giremeyecektir. Saldırgan, aynı şekilde Modbus Sandbox yazmaçlarına veri girmeye çalıştığında kontrol ara katmanının veri eşik değeri denetim mekanizmasına takılacak ve yetkisiz bir şekilde veri giremeyecektir. Aynı zamanda saldırganın yaptığı işlemler Sandbox tarafında loglanacaktır. Bununla beraber Modbus Master tarafında legal olarak 100 üzerinde bir değer yazılmaya çalışıldığında yazmaçlara en fazla 100 değeri girilebilecektir. Bu sınırlamayla birlikte bir üretim tesisindeki veya bir elektrik dağıtım bölgesindeki kontrol sistemlerinde örnek olarak sıcaklık değeri veya santrifüj dönme frekansı değeri gibi verileri belirlenen bir değer üzerinde girilmesi olanaksız hale getirilmiştir.

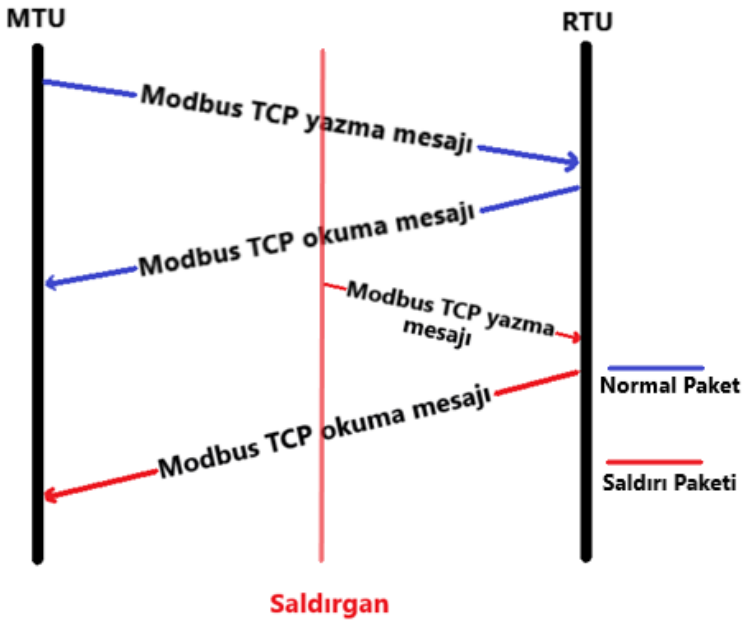
Bu kısımda, geliştirilen kontrol arakatman kullanmak yerine direk olarak MTU üzerinde böyle bir kontrolün yapılabileceği düşünülebilir, fakat böyle bir sistemin kullanılması bütün EKS yerel ağı üzerindeki trafiği kontrol etmeyi olanaksız hale getirecektir. Önerilen kontrol arakatmanı sayesinde saha cihazları ve merkezi sunucu arasında akan bütün Modbus TCP paketleri kontrol edilebilecektir.

5.4. Saldırı Analizi

Şekil 5.2'de gösterildiği gibi tasarlanan deney düzeneğinde Kali Linux işletim sistemine sahip saldırgan bilgisayarında bulunan güvenlik testi araçları kullanılarak sunucu ve port taraması işlemi ve bu işlemler sonucu elde edilen bilgilerle Modbus paketlerindeki veri bölümleri manipüle edilip değiştirilmeye çalışılmıştır. Bu bölümün ilerleyen kısımlarında ekran görüntüleri ile birlikte verilecek olan bu tarama ve veri manipülasyon işlemleri, ilk etapta çalışmada önerilen savunma mekanizması olmadan gerçekleştirilerek gösterilmiş, daha sonrasında tez kapsamında geliştirilen savunma mekanizması kullanılarak gerçekleştirilmiş ve sonuçlar analiz edilmiştir. Böylece savunma mekanizması olarak geliştirilen kontrol ara katmanı olan Modbus Sandbox'ta zafiyet barındırıp barındırmadığı incelenmiş olacaktır.

Geliştirilen simülasyon ortamında MTU ve RTU arasında akan paketlere saldırgan tarafından müdahalede bulunulduğu saldırı senaryosu temel düzeyde Şekil 5.6'da

gösterilmiştir. Görüleceği üzere; saldırgan, simülasyon ortamında RTU cihazına yetkisiz bir şekilde Modbus TCP yazma değeri gönderdiğinde RTU bu veriyi kendi yazmacına yazıp MTU cihazının okuma mesajı cevap vererek kendi yazmaçlarındaki yetki dışı yazılmış veriyi göndermektedir. Sonuç olarak, saldırganın manipülasyon işlemi başarılı olmakta ve hem RTU hem MTU cihazlarının yazmaç değerleri yetkisiz bir şekilde değiştirilmektedir.



Şekil 5.6. Savunmasız sistemde saldırı senaryosu

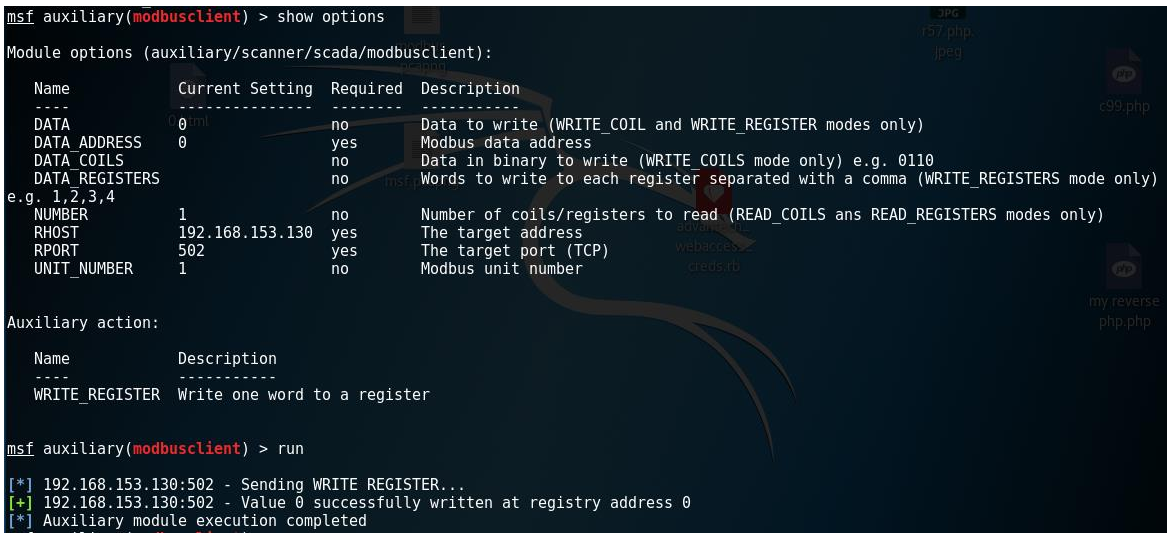
Öncelikle kontrol ara katmanı eklenmeden sadece Modbus Master ve Modbus Slave cihazlarının hiçbir güvenlik önlemi olmadan haberleştiği ortamda saldırı analizi gerçekleştirilmiştir. Bunun için ilk etapta nmap tarama aracı kullanılarak iç ağda bulunan ve Modbus TCP protokolünün varsayılan port olarak çalıştığı 502. port üzerinde modbus servisinin çalıştığı cihazlar tespit edilmiştir. Böylece hedef alınan cihazlar belirlenmiştir. Bu aşamada Modbus Slave cihazının üzerinde 502. portun açık olduğu ve üzerinde modbus servisinin çalıştığı gözlemlenmiştir. Şekil 5.7'de ağ taramasına ait sonuçlar gösterilmiştir.

```
root@kali:~# nmap -sS -p 502 192.168.153.0/24 --open -sV

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-11 17:40 +03
Nmap scan report for 192.168.153.130
Host is up (0.00079s latency).
PORT    STATE SERVICE VERSION
502/tcp open  mbap?
```

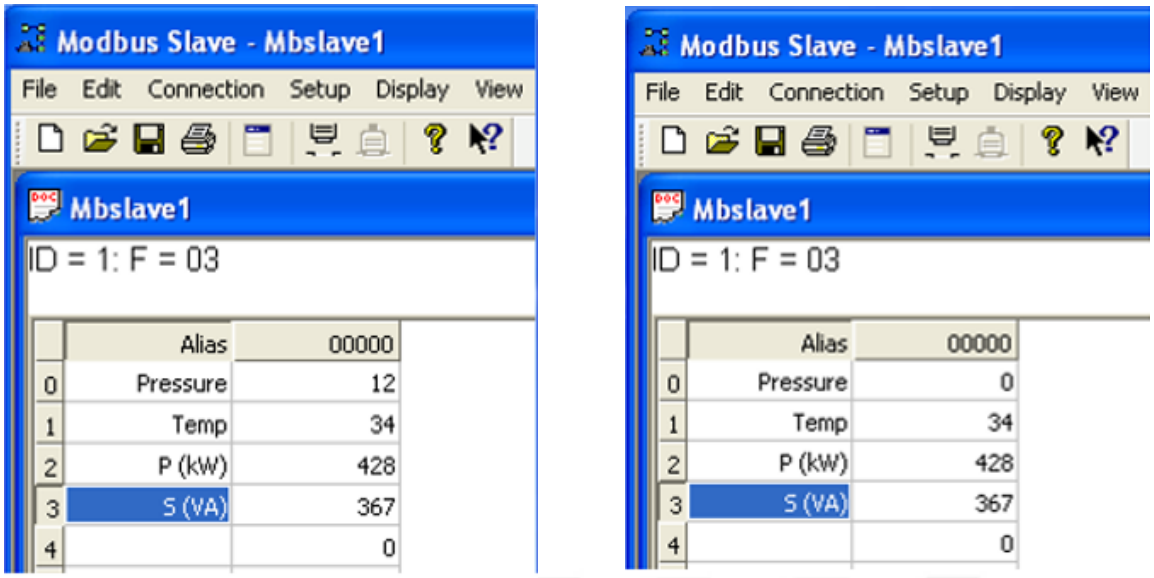
Şekil 5.7. Savunmasız sistemde nmap taraması

Tarama işlemi sonrasında daha önce detayları verilmiş olan Metasploit Framework modbusclient modülü kullanılarak üzerinde modbus servisinin çalıştığı tespit edilen cihaz üzerindeki yazmaç değerleri manipüle edilmeye çalışılmıştır. Bunun için yazmaç adresi 0 olan adres yerine 0 değeri yetkisiz bir şekilde girilmiştir. Manipüle işlemi Şekil 5.8'de, bu işlem sonucunda Modbus Slave cihazı üzerindeki yazmaçlardaki değerlerdeki değişimler saldırı öncesindeki değerler ve saldırı sonrasındaki değerler gösterilerek Şekil 5.9'da verilmiştir.



Şekil 5.8. Savunmasız sistemde manipüle işlemi

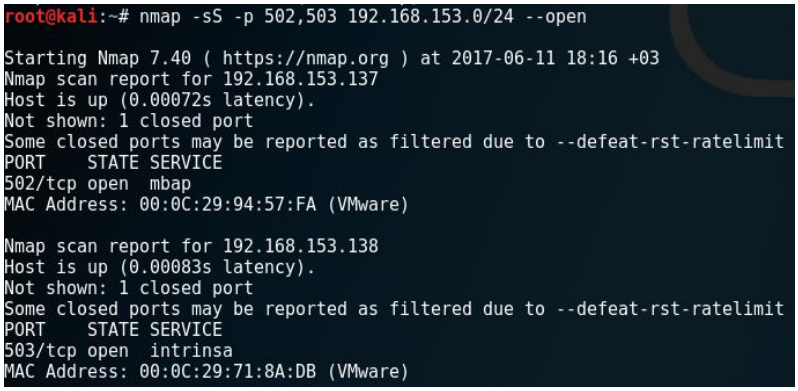
Saldırı sonucunda istismar modülünün içinde yazmaç 0 adresine başarılı bir şekilde 0 değerinin girildiği yazmaktadır. Modbus Slave cihazı üzerinde manipüle işlemi sonrası yazmaç değerleri üzerindeki değişim ve saldırının başarılı bir şekilde sonuçlandığı gözlemlenmiştir.



(a) (b)

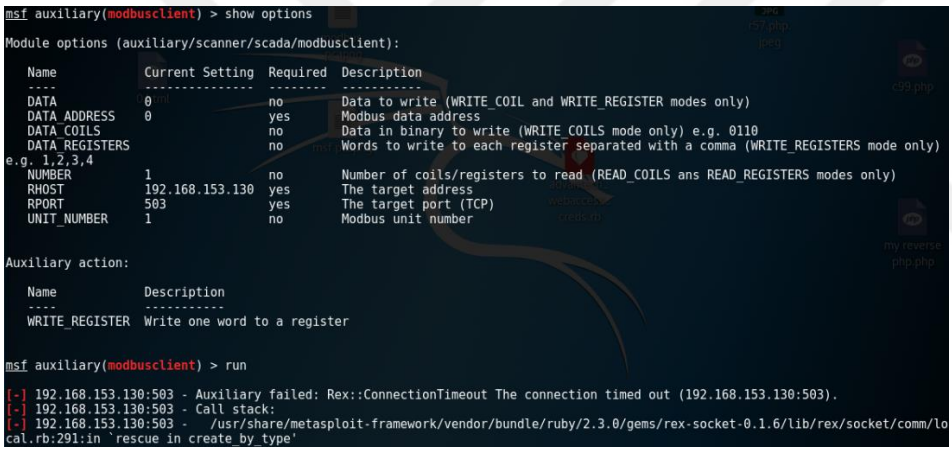
Şekil 5.9. Modbus Slave yazmaç değerleri (a) saldırı öncesi (b) saldırı sonrası

Savunmasız sistemde yani Modbus Master ve Modbus Slave cihazları arasındaki haberleşmede herhangi bir kontrol ara katmanı kullanılmadığında gerçekleştirilen siber saldırının başarılı bir şekilde sonuçlandığı gözlemlenmiştir. İkinci etapta ise Modbus Master ve Modbus Client cihazları arasında savunma mekanizması olarak Modbus Sandbox'ın ve Windows güvenlik duvarının kullanıldığı Şekil 5.2'de gösterilen topolojide siber saldırı gerçekleştirilmiş ve saldırı sonuçları gözlemlenmiştir. Saldırının bu bölümünde de saldırı aracı olarak tekrar ağ taraması için Nmap aracı ve veri manipülasyonu için modbusclient modülü kullanılmıştır. Fakat ağ topolojisine göre Modbus Slave bu sefer varsayılan Modbus portu yani 502. port üzerinden değil 503. port üzerinden haberleşmektedir. Modbus Sandbox ise bu sefer varsayılan Modbus haberleşme portu yani 502. port üzerinden haberleşmektedir. Yani bir bakıma saldırgan ağ üzerinde direk olarak Modbus varsayılan portu açık olan sunucuları tararsa Modbus Slave cihazlarını tespit edemeyecektir. Bu da bir bakıma saldırganın Modbus cihazını varsayılan saldırı vektörleriyle tespit edememesinden dolayı güvenlik önlemi olarak sayılabilir. Bu çalışmada Nmap taramasıyla ağ üzerinde hem 502 hem de 503. portu açık olan cihazlar tespit edilmiş ve bu cihazlar üzerinde modbusclient kullanılarak manipülasyon işlemi gerçekleştirilerek Modbus Slave ve Modbus Sandbox makinalarındaki yazmaçları üzerindeki değerlerdeki değişimler ve saldırının başarılı sonuçlanıp sonuçlanmadığı gözlemlenmiştir. Şekil 5.10'da Nmap tarama sonuçları ve Şekil 5.11'de manipülasyon işlemine ait ekran görüntüleri mevcuttur.



Şekil 5.10. Savunmalı sistemde nmap taraması

Tarama sonucuna göre, yukarda da bahsedildiği gibi Modbus Slave cihazında 503. portun, Modbus Sandox cihazında 502. portun açık olduğu tespit edilmiştir.

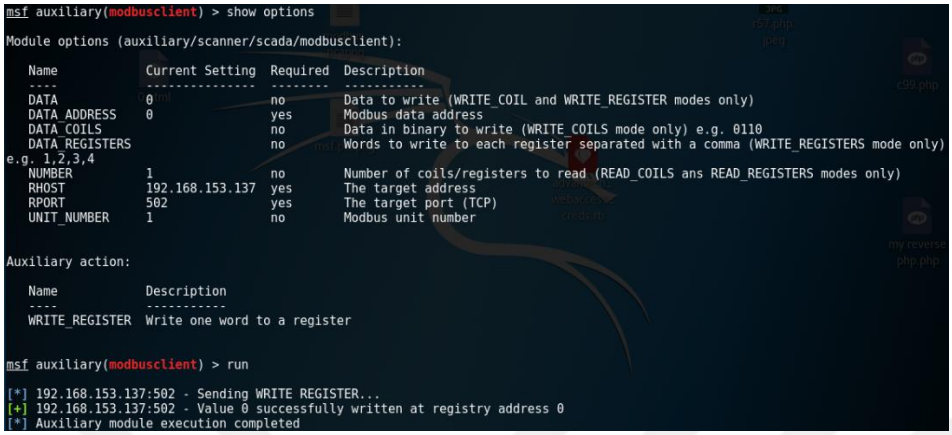


Şekil 5.11. Savunmalı sistemde manipülasyon işlemi

Şekil 5.11'e göre modbusclient modülü kullanılarak Modbus Slave cihazının yazmaç 0 adresine 0 değeri yetkisiz bir şekilde girilmeye çalışılmış, fakat topolojiye göre IP ve Port tabanlı çalışan güvenlik duvarı bu saldırıyı engellemiş ve Modbus Slave cihazındaki yazmaçlara herhangi bir müdahalede bulunulamamıştır.

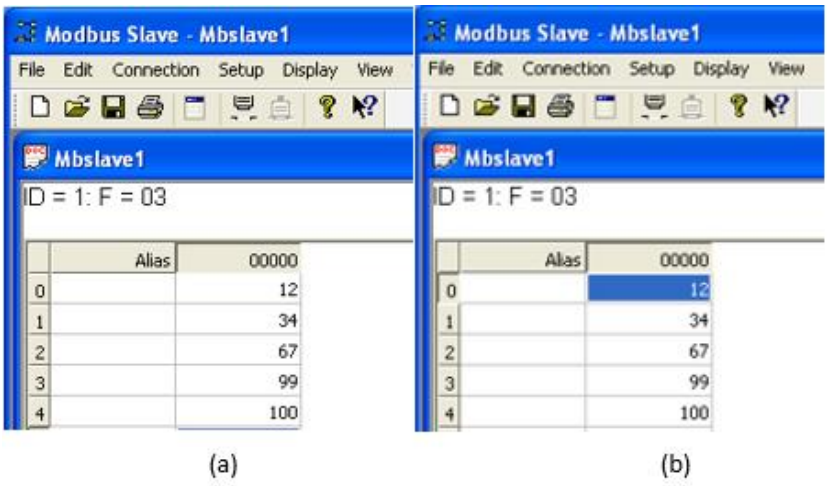
Nmap tarama sonuçlarına göre 502. portunun açık olduğu tespit edilen Modbus Sandbox cihazına yönelik manipülasyon işleminde cihaz üzerinde çalışan ve detayları yukarıdaki bölümlerde verilen kontrol ara katmanı bu saldırıyı engelleyerek saldırgana ait logları "SaldırganModbus" isminde bir dosyaya kaydeder. Aynı zamanda kod içerisinde bulunan kontrol fonksiyonuyla Modbus Master cihazındaki yazmaç adreslerine 100 üzerinde bir değer girildiğinde bu işlem engellenecek ve Modbus Slave cihazındaki yazmaçta ilgili adrese

en fazla 100 olarak yazacaktır. Şekil 5.12'de Modbus Sandbox cihazına yönelik manipülasyon işlemine ait ekran görüntüsü verilmiştir.



Şekil 5.12. Savunmalı sistemde Modbus Sandbox cihazına yönelik manipülasyon işlemi

Bu siber saldırı işlemi sonrasında saldırı opsiyonlarında da belirtildiği gibi 0. yazmaç adresine 0 değeri yetkisiz bir şekilde girilmeye çalışılmış ve saldırı kodu çalıştırıldığında kodun başarılı bir şekilde çalışıp ilgili yazmaca değerin girildiği belirtilmektedir. Fakat Modbus Sandbox ve Modbus Slave cihazlarının yazmaçları incelendiğinde saldırının başarısız olduğu ve yazmaç değerlerinin değişmediği gözlemlenmiştir. İlgili ekran görüntüleri Şekil 5.13'te verilmiştir.



Şekil 5.13. Savunmalı sistemde Modbus Slave yazmaçları (a) saldırı öncesi (b) saldırı sonrası

Şekil 5.14'te Modbus Sandbox cihazındaki yazmaç değerlerinin aktığı komut satırı çıktıları gösterilmektedir.

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
1 packet captured
4 packets received by filter
0 packets dropped by kernel
b'10:22:44.297291 IP 192.168.153.135.49174 > 192.168.153.137.502: Flags [P.], se
q 3606355813:3606355825, ack 1696433380, win 256, length 12\n'
[12, 34, 67, 99, 100, 0, 0, 0, 0, 0]
yazdi
```

Şekil 5.14. Modbus Sandox cihazı yazmaç değerleri

Tüm bunlarla birlikte Modbus Sandbox cihazına yönelik gerçekleşen siber saldırı sonucu oluşan tüm logların kaydedildiği "SaldırganMobdus" isimli kayıt dosyasına ait bir ekran görüntüsü de Şekil 5.15'te gösterilmiştir.

Saldirganmodbus.log ×

```
val 15306 ecr 310854], length 0\n'|[23, 17, 32, 12, 0, 0, 0, 0, 0, 0]|2017-05-29 12:55:06.607648
b'12:55:11.708655 IP 192.168.153.130.503 > 192.168.153.137.52660: Flags [F.], seq 876241342, ack 2582878900, win 64228, options [nop,nop,TS
val 15368 ecr 312393], length 0\n'|[23, 17, 32, 12, 0, 0, 0, 0, 0, 0]|2017-05-29 12:55:12.758107
b'12:55:21.106537 IP 192.168.153.133.39009 > 192.168.153.137.502: Flags [S], seq 3893535546, win 29200, options [mss 1460,sackOK,TS val 307461
ecr 0,nop,wscale 7], length 0\n'|[32, 17, 32, 12, 0, 0, 0, 0, 0, 0]|2017-05-29 12:55:22.124550
b'12:55:25.833798 IP 192.168.153.130.503 > 192.168.153.137.52938: Flags [F.], seq 2493835014, ack 2907254928, win 64228, options [nop,nop,TS
val 15509 ecr 315921], length 0\n'|[23, 17, 32, 12, 0, 0, 0, 0, 0, 0]|2017-05-29 12:55:26.915820
b'12:55:27.396677 IP 192.168.153.130.503 > 192.168.153.137.52998: Flags [F.], seq 2843854897, ack 2572595409, win 64228, options [nop,nop,TS
val 15525 ecr 316315], length 0\n'|[23, 17, 32, 12, 0, 0, 0, 0, 0, 0]|2017-05-29 12:55:28.457186
b'12:55:30.522374 IP 192.168.153.130.503 > 192.168.153.137.53084: Flags [F.], seq 697505040, ack 17119217, win 64228, options [nop,nop,TS val
15556 ecr 317096], length 0\n'|[23, 17, 32, 12, 0, 0, 0, 0, 0, 0]|2017-05-29 12:55:31.675879
b'12:55:51.083957 IP 192.168.153.130.503 > 192.168.153.137.53366: Flags [F.], seq 432146793, ack 2636346539, win 64228, options [nop,nop,TS
val 15761 ecr 322237], length 0\n'|[12, 17, 32, 12, 0, 0, 0, 0, 0, 0]|2017-05-29 12:55:52.205981
b'12:55:52.803434 IP 192.168.153.130.503 > 192.168.153.137.53426: Flags [F.], seq 859298100, ack 880461355, win 64228, options [nop,nop,TS val
15779 ecr 322667], length 0\n'|[12, 17, 32, 12, 0, 0, 0, 0, 0, 0]|2017-05-29 12:55:53.908068
b'12:55:55.959541 IP 192.168.153.130.503 > 192.168.153.137.53512: Flags [F.], seq 1934970970, ack 1384899767, win 64228, options [nop,nop,TS
val 15811 ecr 323456], length 0\n'|[12, 17, 32, 12, 0, 0, 0, 0, 0, 0]|2017-05-29 12:55:57.029306
b'12:56:00.771976 IP 192.168.153.130.503 > 192.168.153.137.53618: Flags [F.], seq 133277498, ack 2309874536, win 64228, options [nop,nop,TS
val 15859 ecr 324659], length 0\n'|[12, 17, 32, 12, 0, 0, 0, 0, 0, 0]|2017-05-29 12:56:02.256591
```

Şekil 5.15. SaldırganModbus log dosyası

5.5. Değerlendirme

Bu çalışma kapsamında Shodan arama motoru ile EKS'lerde haberleşme protokollerinin dünya genelinde kullanım oranlarının belirlenmesi sonucu Modbus TCP protokolünün yarı yarıya kullanıldığı gözlemlenmiştir. Modbus TCP protokolünün güvenliğine çözüm olarak ortaya konulan bu çalışma ile EKS ağlarının haberleşmesine yönelik siber saldırıların ciddi oranda engellenebileceği ve gerçekleştirilen siber saldırıların loglanabileceği gösterilmiştir. Ayrıca ülkemizde de kritik altyapıların güvenliğine yönelik çalışmalara da katkılar sağlayacağı değerlendirilmektedir.

5.6. Modbus Sandbox Sınırlılıkları

Bu çalışmanın tasarlanan deney düzeneğindeki topolojiye göre Modbus TCP protokolünün kaynak IP adresi kontol eksikliği zafiyeti istismar edilerek saha cihazı üzerindeki yazmaçlardaki değerlerin manipüle edilebildiği gösterilmiş ve bu zafiyeti gidermeye yönelik

bir Modbus Sandbox geliştirilmiştir. Tespit edilen zafiyet, Modbus TCP protokolünün verilerin geldiği kaynak IP adresini kontrol etmemesidir. Dolayısıyla Modbus Sandbox makinasıyla kaynak IP adresi kontrolü sağlanarak verilerin geldiği kaynak IP adresi denetlenmekte ve kod içerisinde belirlenen IP adresinden farklı bir IP adresinden veri girilmeye çalışıldığında Modbus Slave cihazı önündeki IP ve Port tabanlı güvenlik duvarı ve Modbus Sandbox bunu engellemektedir. Bu durumda bu güvenlik önlemini atlatmaya yönelik akla gelen ilk yöntem saldırganın IP adresini Modbus Master IP adresiyle aynı IP adresi olacak şekilde Ethernet ara yüzünde gerekli değişiklikleri yaparak Modbus Sandbox makinasını aldatmaktır. Fakat bu yöntem denendiğinde Modbus Master üzerinde "Write Error" hatası alınmış ve saldırı başarıyla sonuçlanmamıştır. Bunun nedeni ağ üzerinde saldırgan makinasının IP adresi ile Modbus Master makinasının IP adreslerinin aynı olmasından dolayı IP adresi çakışmasının yaşanmasıdır.

Öte yandan, Modbus Sandbox makinası içerisinde koşan kodun içerisinde yer alan topolojideki cihazların soketlerinin açıldığı döngü tamamlanmadan saldırgan tarafından yeni bir veri basılmaya çalışılmasında Modbus Sandbox ve Slave cihazlarındaki yazmaçlara yetki dışında veri girilebilmektedir. Bu bakımdan Modbus Sandbox yazmaçlarına saldırgan tarafından gerçekleştirilen bir kaba kuvvet saldırısıyla saldırgan başarılı bir şekilde saldırısını gerçekleştirebilmektedir. Buna önlem olarak hızlı işlem kapasitesine sahip olan FPGA gibi donanımsal araçlar kullanılarak yazılımın hızlı işlemesiyle bu saldırı yöntemi engellenebilir.

6. SONUÇ VE DEĞERLENDİRMELER

Bu çalışmada, enerji, su, ulaşım, sağlık, bankacılık, nükleer/kimyasal tesisler ve haberleşme sistemleri başta olmak üzere kritik altyapıların ve Endüstriyel Kontrol Sistemlerinin en önemli bileşenlerinden birisi olan SCADA sistemleri ve bileşenlerinin güvenlik açıkları ve saldırı vektörleri incelenmiştir. Ek olarak, EKS ağlarında en sık kullanılan TCP/IP tabanlı haberleşme protokolleri Shodan arama motoruyla taranmış, çıkan sonuçlar analiz edilerek istatistikleri çıkarılmış ve Modbus TCP protokolünün dünya genelinde %50 oranla kullanıldığı gözlemlenmiştir. Ayrıca istatistikleri çıkarılan bu protokollerin ülkeler tarafından kullanım oranları da tespit edilmiş ve ülkemizin dünya ülkeleri arasında EKS haberleşme protokollerini %1 oranıyla kullandığı tespit edilmiştir. Bu sonuçlara göre, EKS ağlarında %50 oranla en sık kullanılan Modbus TCP protokolüne odaklanılmış ve bu protokolün güvenliğine yönelik çözüm önerisi geliştirilmiştir.

Tez kapsamında Modbus TCP protokolünün güvenliğine çözüm olarak önerilen güvenlik mimarisi Modbus Poll simülasyon ortamında gerçekleştirilmiştir. Bu mimaride MTU olarak simüle edilen Modbus Master ve RTU olarak simüle edilen Modbus Slave cihazları arasında akan Modbus TCP paketleri Wireshark aracı kullanılarak analiz edilmiştir. Yapılan analiz sonucunda Modbus TCP protokolünün kaynak IP kontrolünü yapmadığı, akan paketlerin şifrelenmeden açık metin şekilde gönderildiği, araya girerek iki cihaz arasında akan bütün paketlerin okunabildiği ve Metasploit Framework kullanılarak paketler üzerinde manipülasyon işlemlerinin gerçekleştirilebildiği analiz edilmiştir.

Modbus TCP protokolünün, paketlerin kaynak IP adresinin kontolünü yapmaması zafiyetini engellemek amacıyla test düzeneği ortamında IP ve port tabanlı Windows güvenlik duvarı kullanılmıştır. Burada kullanılan güvenlik duvarı simülasyon ortamında Windows işletim sistemine ait olup Modbus TCP paketlerini, sadece kontrol ara katmanın 502. portundan gelen paketleri kabul etmesi yönünde yapılandırılmıştır.

Literatürde “intruder” olarak isimlendirilen küskün veya kötü niyetli bir çalışanın veya bilinçsiz bir çalışanın sahada bulunan EKS cihazlarının yazmaçlarına istenmeyen bir değer girmesini engellemek yani Modbus TCP protokolündeki veri kontrolünü sağlamak amacıyla tez kapsamında önerilen test düzeneği ortamındaki kontrol ara katmanında çalışan programa ek bir fonksiyon eklenmiştir. Bu fonksiyon sayesinde Modbus tabanlı EKS saha cihazlarının

yazmaçlarına belirlenen eşik değerin üzerinde bir değer girilemeyecek, girilmesi durumunda yazmaçlara en fazla eşik değer yazılacaktır. Ayrıca saldırganın kontrol ara katmanında bulunan yazmaçlarına yetkisiz bir şekilde veri yazmasını engellemek amacıyla ara katmana gelen tüm paketler dinlenmiş ve bu paketlerin kaynak IP adresleri karşılaştırılmıştır. Gelen paketlerin IP adresleri Modbus Master haricinde bir IP adresinden geliyorsa, sistem bu durumu bir saldırı olarak algılamakta ve yazmaçlara yazılmak istenen değerler ara katman yazmaçlarına yazılmayıp en son yazılı olan yazmaç değerler yazılmakta ve saldırı paketi loglanmaktadır. Böylece literatür taramasında eksikliği görülen EKS ağında akan Modbus TCP paketlerinde veri kontrolüne yönelik yeni bir çözüm önerisinde bulunulmuş ve uygulanabilirliği gösterilmiştir.

Kritik bilgi sistemlerine yönelik risk değerlendirmeleri hayati derecede öneme sahip diğer bir unsurdur. Özellikle ülke güvenliğini ilgilendiren altyapılara yönelik siber saldırılar için risk değerlendirme teknikleri kullanılmalıdır. Bu bakımdan, Irmak ve Erkek'in [133] saldırı ağacı gösterimi ile çok nitelikli fayda teorisini kullanarak önerdikleri çalışma, kritik bilgi sistemlerinde risk değerlendirmesi için önemli bir rehberlik teşkil edebilir.

Bilgi güvenliğinin üç bileşeni gizlilik, bütünlük ve erişilebilirliktir. Bunlardan erişilebilirlik, SCADA sistemlerinin gerçek zamanlı çalışmasından dolayı en önemli bileşendir. Verilerin iletimi sırasında milisaniyeler seviyesinde bir zaman gecikmesinin bile fonksiyonel işlemlerin çok ciddi aksamalarına sebebiyet vermesi olasılığı yüksektir. Bu yüzden gerçek zamanlı çalışan SCADA sistemleri üzerinde güvenlik testlerinin yapılması sakıncalı olabilmektedir. Dolayısıyla SCADA sistemlerinin devreye alınmadan önce güvenlik testlerinin yapılması gerektiği sonucuna varılmıştır. Bu bağlamda, bazı özel sektör kuruluşlarının ve üniversitelerin SCADA sistemlerinin güvenliğine yönelik deney düzeneği ortamlarının var olduğu fakat ulusal çapta çalışmalar için yetersiz olduğu gözlemlenmiştir. Bu bakımdan ülkemizdeki ulusal enerji altyapısının güvenliğini sağlamaya yönelik ulusal bir araştırma geliştirme laboratuvarının ve deney düzeneklerinin kamu, üniversite ve özel sektör işbirliği ile oluşturulması gerektiği önerilmektedir.

Bu çalışma kapsamında dünya genelinde tespit edilen EKS haberleşme protokollerinin kullanım oranları ve dünya genelinde ülkemizdeki kullanım oranları belirlenmiş ve Modbus TCP protokolü belirgin bir şekilde %50'lik oranla kullanıldığı tespit edilmiştir. Bu kapsamda mevcut çalışma Shodan arama sonuçlarının yarısının güvenliğine çözüm üretmektedir.

Ayrıca çalışmanın önceki bölümlerinde bahsedilen ilki “2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı” ve ikincisi “2016-2019 Ulusal Siber Güvenlik Stratejisi” kapsamında siber savunmanın güçlendirilmesi ve kritik altyapıların korunması amacıyla yapılan çalışmalara katkılar sağlayacağı değerlendirilmektedir.

Çalışma kapsamında önerilen, kontrol ara katmanı üzerinde koşan Python koduna ait temel sınırlılık, saldırganın güvenlik sistemine kaba kuvvet saldırısı yaparak saha cihazı üzerindeki yazmaç değerlerini yetkisiz bir şekilde değiştirebilmesidir. Bu saldırı yöntemini engellemeye yönelik paralel işlem yapan ve hızlı işlem gücüne sahip FPGA gibi donanımsal çözümler geliştirilebilir.

Genel bir sonuç olarak, fonksiyonel işlemlerini kaybetmesi, zarar görmesi veya veri iletiminde oluşan manipülasyonlar sonucunda toplum düzenini, insan hayatını, ekonomik kayıpları, ulusal veya global düzeyde güvenliği sekteye uğratabilecek kritik altyapı sistemlerinin güvenlik bilinciyle oluşturulması ve buna uygun tasarlanması gerektiği şüphesizdir. Özellikle ülkemizde elektrik dağıtım firmalarının kullandığı kontrol sistemlerinin haberleşme protokollerinin yeniden gözden geçirilmesi ve siber güvenlik açısından ele alınması gerekmektedir. Kritik altyapılar içerisinde en önemli sistemlerden birisi olan SCADA sistemlerinin güvenliği hayati derecede öneme sahiptir. Bu nedenle, sunulan tezde SCADA sistemlerinin haberleşmesinde en sık kullanılan Modbus protokolünün güvenliğine yönelik bir çalışma önerilmiştir. Önerilen çalışmanın gerçek sistemlerle entegre çalıştırılması, hem iç ağdan hem de dış ağdan gelebilecek siber saldırıların etkilerini hafifletecektir. Böylece, sunulan tez çalışması ile kritik bir altyapı olan SCADA sistemlerinin güvenliğine katkı sağlanacağı değerlendirilmektedir.

KAYNAKLAR

1. İnternet: Department of Foreign Affairs and Trade. Information Technology Agreement. URL: http://www.webcitation.org/query.php?url=http://dfat.gov.au/trade/agreements/pages/information-technology-agreement.aspx&date=2017-05-11, Son Erişim Tarihi: 11.05.2017.

2. İnternet: Türkiye Büyük Millet Meclisi Tutanak Dergisi. 25 inci Birleşim. URL: http://www.webcitation.org/query?url=https://www.tbmm.gov.tr/tutanak/donem21/yil3/bas/b025m.htm&date=2017-05-11, Son Erişim Tarihi: 11.05.2017.

3. Yılmaz, E., Ulus, H. ve Gönen, S. (2015). Bilgi Toplumuna Geçiş ve Siber Güvenlik. ***Bilişim Teknolojileri Dergisi***, 8(3), 133–146.

4. Unver, M. ve Canbay, C. (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik. ***Elektrik Mühendisligi Dergisi***, 438, 94-103.

5. Commission of the European Communities (2004). *Critical Infrastructure Protection in the Fight against Terrorism*, Brüksel.

6. Sanz, R. ve Årzén, K. (2003). Trends in Software and Control. ***IEEE Control Systems Magazine***, 23(3), 12–15.

7. Chandia, R., Gonzalez, J., Kilpatrick, T. ve Papa, M. (2007). Security Strategies for SCADA Networks. ***Critical Infrastructure Protection***, 253, 117–131.

8. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2012).*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*. Ankara: Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

9. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi*. Ankara: Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

10. Alves, R. and Souza, A. (2014). A Summary of Control System Security Standards Activities in the Energy Sector. ***U.S. Department of Energy Office of Electricity Delivery and Energy Reliability***, 1, 1–5.

11. Centre for the Protection of National Infrastructure (2014). *Good Practice Guide Process Control and Scada Security Guide 1: Understand the Business Risk*. İngiltere: Centre for the Protection of National Infrastructure.

12. Stouffer, K ., Falco, J. and Kent, K. (2008). *Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology*. ***Nist Special Publication (800)82***.

13. Özbilen, A. (2012). *TCP / IP Tabanlı Dağıtık Endüstriyel Denetim Sistemlerinde Güvenlik ve Çözüm Önerileri*. Doktora Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

14. North American Electric Reliability Corporation (2011). *Security Guideline for the Electricity Sector: Physical Security*. ABD: North American Electric Reliability Corporation.

15. American Petroleum Institute (2009). *API STANDARD 1164 - Pipeline SCADA Security*. ABD: American Petroleum Institute.

16. Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsa Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. ***Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi***, (23)2, 507–522.

17. Nordlander, J. (2009). *What is Special About Scada System Cyber Security ? A Comparison between Existing Scada System Security What is Special about Scada System Cyber*. Doktora Tezi, Royal Institute of Technology, İsviçre.

18. İnternet: US Department of Energy. 21 Steps to Improve Cyber Security of SCADA. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fenergy.gov%2Fsites%2Fprod%2Ffiles%2Foeprod%2FDocumentsandMedia%2F21_Steps_-_SCADA.pdf&date=2017-04-12, Son Erişim Tarihi: 12.04.2017.

19. Wilshusen, G. C. (2015). Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress. ***U.S. Government Accountability Office***, 16-79, ABD.

20. Sayegh, N., Chehab, A., Elhajj, I. H. and Kayssi, A. (2013). *Internal Security Attacks on SCADA Systems*. 2013 3rd International Conference on Communications and Information Technology, 22–27, Beyrut, Lübnan.

21. Koutsandria, G., Gentz, R., Jamei, M., Scaglione, A., Peisert, S. and McParland, C. (2015). *A Real-Time Testbed Environment for Cyber-Physical Security on the Power Grid*. Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, 67–78, Colorado, ABD.

22. Morris, T., Srivastava, A., Reaves, B., Gao, W., Pavurapu, K. and Reddi, R. (2011). A Control System Testbed to Validate Critical Infrastructure Protection Concepts. ***International Journal of Critical Infrastructure Protection***, 4(2), 88–103.

23. Hahn, A. (2013). *Cyber Security of the Smart Grid: Attack Exposure Analysis, Detection Algorithms, and Testbed Evaluation*. Doktora Tezi, Computer Engineering of Iowa State University, ABD.

24. Hahn, A., Ashok, A., Sridhar, S. and Govindarasu, M. (2013). Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid. ***IEEE Transactions on Smart Grid***, 4(2), 847–855.

25. Kuipers, D. G. (2008). Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program, ***US Department of Energy***, ABD.

26. Mcdonald, M. J., Conrad, G. N., Service, T. C. and Cassidy, R. H. (2008). Cyber Effects Analysis Using VCSE: Promoting Control System Reliability. ***Sandia Report***, 1-57.

27. Bergman, D. C., Jin, D., Nicol, D. M. and Yardley, T. (2009). *The Virtual Power System Testbed and Inter-Testbed Integration*, Proceedings of the 2nd conference on Cyber Security Experimentation and Test, 1-6, ABD.

28. Dondossola, G., Garrone, G., Szanto, J., Deconinck, G., Loix, T. and Beitollahi, H. (2009). *ICT Resilience of Power Control Systems: Experimental Results from the Crutial Testbeds*. Proceedings of the International Conference on Dependable Systems and Networks, 554–559, Lizbon, Portekiz.

29. Dondossola, G., Deconinck, G., Garrone, F. and Beitollahi, H. (2009). *Testbeds for Assessing Critical Scenarios in Power Control Systems*. International Workshop on Critical Information Infrastructures Security, 223–234, Berlin, Almanya.

30. Mallouhi, M., Al-Nashif, Y., Cox, D., Chadaga, T. and Hariri, S. (2011). *A testbed for Analyzing Security of SCADA Control Systems (TASSCS)*. IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT Europe, 1–7, Anaheim, ABD.

31. Wu, J. H., Shyan, S., Alexandru, S., Ahmed, F., Ching, L. C., Pavel, G. and Manimaran, G. (2011). *An Intrusion and Defense Testbed in a Cyber-Power System Environment*. IEEE Power and Energy Society General Meeting, 1–5, İrlanda.

32. Queiroz, C., Mahmood, A. and Tari, Z. (2011). SCADASim A Framework for Building SCADA Simulations. ***IEEE Transactions on Smart Grid***, 2(4), 589–597.

33. Yanfei, L., Cheng, W., Chengbo, Y. and Xiaojun, Q. (2009). *Research on ZigBee Wireless Sensors Network Based on ModBus Protocol.* Proceedings - 2009 International Forum on Information Technology and Applications, IFITA 2009, 1, Nisan, 487–490.

34. Yanfei, L. and Cheng, W. (2009). *An Improved Design of ZigBee Wireless Sensor Network.* 2009 2nd IEEE International Conference on Computer Science and Information Technology, 515–518, Beijing, Çin.

35. Beresford, D. (2011). Exploiting Siemens Simatic S7 PLCs. ***Black Hat USA***, 16(2), 723-733.

36. Bayındır, R., Sağıroğlu, Ş., Özbilen, A. ve Çolak, İ. (2009). Investigating Industrial Risks Based on Information Security for Observerable Electrical Energy Distribution System and Suggestions. ***Gazi University Journal of Faculty of Engineering and Architecture***, 24(4), 715–723.

37. Chabukswar, R., Sinópoli, B., Karsai, G., Giani, A., Neema, H. and Davis, A. (2010). *Simulation of Network Attacks on SCADA Systems*. First Workshop on Secure Control Systems, 1-8, ABD.

38. İnternet: ITProPortal. The Evolution of DDoS. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.itproportal.com%2Ffeatures%2Fthe-evolution-of-ddos&date=2017-05-11, Son Erişim Tarihi: 11.05.2017.

39. Kakanakov, N. and Spasov, G. (2011). Securing against Denial of Service Attacks In Remote Energy Management Systems. ***Annual Journal of Electronics***, Bulgaristan.

40. Petrovic, J. D. and Stojanovic, M. D. (2013). *Analysis of SCADA System Vulnerabilities to DDoS Attacks*. 2013 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, TELSIKS, 2, 591–594.

41. Nam, S. Y., Djuraev, S. and Park, M. (2013). Collaborative Approach to Mitigating ARP Poisoning-Based Man-in-the-Middle Attacks. ***Computer Networks***, 57(18), 3866–3884.

42. Lootah, W., Enck, W. and McDaniel, P. D. (2007). TARP: Ticket-Based Address Resolution Protocol. ***Computer Networks***, 51(15), 106–116.

43. Pansa, D. and Chomsiri, T. (2008). *Architecture and Protocols for Secure LAN by Using a Software-Level Certificate and Cancellation of ARP Protocol*. Proceedings - 3rd International Conference on Convergence and Hybrid Information Technology, ICCIT 2008, 2, 21–26, Güney Kore.

44. Hong, S., Oh, M. and Lee, S. (2013). Design and Implementation of an Efficient Defense Mechanism against ARP Spoofing Attacks Using AES and RSA. ***Mathematical and Computer Modelling***, 58(1), 254–260.

45. Oppliger, R., Hauser, R. and Basin, D. (2006). SSL/TLS Session-Aware User Authentication - Or How to Effectively Thwart the Man-in-the-Middle. ***Computer Communications***, 29(12), 2238–2246.

46. Ciancamerla, E., Fresilli, B., Minichino, M., Patriarca, T. and Iassinovski, S. (2014). *An Electrical Grid and Its SCADA under Cyber Attacks: Modelling Versus a Hybrid Testbed*. 2014 International Carnahan Conference on Security Technology (ICCST), 1–6, Roma, İtalya.

47. Lee, D., Kim, H., Kim, K. and Yoo, P. D. (2014). *Simulated Attack on DNP3 Protocol in SCADA System.* In Proceedings of the 31th Symposium on Cryptography and Information Security, 1–6, Kagoshima, Japonya.

48. Morris, T. H. and Gao, W. (2013). *Industrial Control System Cyber Attacks*. Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research, 22–29, Leicester, İngiltere.

49. Aloui, N. B. (2016). Industrial Control Systems Dynamic Code Injection. ***GreHack***, Grenoble, Fransa.

50. Zhu, B., Joseph, A. and Sastry, S. (2011). *A Taxonomy of Cyber Attacks on SCADA Systems*. Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCom 2011, 380–388, Dalian, Çin.

51. Gao, W., Morris, T., Reaves, B. and Richey, D. (2010). *On SCADA Control System Command and Response Injection and Intrusion Detection*. General Members Meeting and eCrime Researchers Summit, Dallas, ABD.

52. Yang, J. (2010). An Improved Scheme of Single Sign-on Protocol Based on Dynamic Double Password. ***International Journal of Intelligent Information Technology Application***, 3(2), 65–70.

53. Jian, Y. (2009). *An Improved Scheme of Single Sign-On Protocol*. 5th International Conference on Information Assurance and Security, IAS 2009, 1, 495–498.

54. Abdelmajid, N. T., Hossain, M. A., Shepherd, S. and Mahmoud, K. (2010). *Location-Based Kerberos Authentication Protocol*. Proceedings - SocialCom 2010: 2nd IEEE International Conference on Social Computing, PASSAT 2010: 2nd IEEE International Conference on Privacy, Security, Risk and Trust, 1099–1104, Minneapolis, ABD.

55. Ten, C. W., Manimaran, G. and Liu, C. C. (2010). Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. ***IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans***, 40(4), 853–865.

56. Yang, Y., McLaughlin, K., Sezer, S., Littler, T., Im, E. G., Pranggono, B. and Wang, H. F. (2014). Multiattribute SCADA-Specific Intrusion Detection System for Power Networks. ***IEEE Transactions on Power Delivery***, 29(3), 1092–1102.

57. Shang, W. L., Li, L., Wan, M. and Zeng, P. (2015). *Security Defense Model of Modbus TCP Communication Based on Zone / Border Rules*. Network Security and Communication Engineering: Proceedings of the 2014 International Conference on Network Security and Communication Engineering, 79-86 Londra, İngiltere .

58. Chen, B., Pattanaik, N., Goulart, A., Butler-Purry, K. L. and Kundur, D. (2015). *Implementing Attacks for Modbus/TCP Protocol in a Real-Time Cyber Physical System Testbed*. Proceedings - CQR 2015: 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability, 1-6, Charleston, ABD.

59. Xiong, Q., Liu, H., Xu, Y., Rao, H., Yi, S., Zhang, B. and Deng, H. (2015), A *Vulnerability Detecting Method for Modbus-TCP Based on Smart Fuzzing Mechanism*. IEEE International Conference on Electro Information Technology, 404–409, Dekalb, ABD.

60. Bhatia, S., Kush, N., Djamaludin, C., Akande, J. and Foo, E. (2014). *Practical Modbus Flooding Attack and Detection.* Conferences in Research and Practice in Information Technology Series, 149, 57–65.

61. İnternet: US Department of Energy. The Smart Grid: An Introduction URL: http://www.webcitation.org/query?url=https%3A%2F%2Fenergy.gov%2Fsites%2Fprod%2Ffiles%2Foeprod%2FDocumentsandMedia%2FDOE_SG_Book_Single_Pages%281%29.pdf&date=2017-05-13, Son Erişim Tarihi: 13.05.2017.

62. İnternet: Clear Energy Pipeline. Smart Cities in Europe Enabling Innovation. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.cleanenergypipeline.com%2FResources%2FCE%2FResearchReports%2FSmart%2520cities%2520in%2520Europe.pdf&date=2017-05-13, Son Erişim Tarihi: 13.05.2017

63. Acel, Y. (2011). Kritik Enerji Altyapı Güvenliği Projesi Sonuç Raporu, ***Uluslararası Stratejik Araştırmalar Kurumu (USAK)***, 4, Ankara.

64. Mcdonald, J. D. (1993). *Developing and Defining Basic SCADA System Concepts*. Rural Electric Power Conference, 1993 Papers Presented at the 37th Annual Conference, 93, 1–5, Kansas City, ABD.

65. Shahzad, A., Musa, S., Aborujilah, A. and Irfan, M. (2014). The SCADA Review: System Components, Architecture, Protocols and Future Security Trends. ***American Journal of Applied Sciences***, 11(8), 1418–1425.

66. İnternet: National Commuication System. Supervisory Control and Data Acquisition (SCADA) Systems. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fscadahacker.com%2Flibrary%2FDocuments%2FICS_Basics%2FSCADA%2520Basics%2520-%2520NCS%2520TIB%252004-1.pdf&date=2017-05-03, Son Erişim Tarihi: 03.05.2017

67. Krutz, R. L. (2005). *Securing SCADA Systems*, ABD: Wiley.

68. William, B. (2015). *Programmable Logic Controlers*, 6th baskı, İngiltere: Newnes.

69. İnternet: The International Society of Automation. Automation Basics: Programmable Logic Controllers: Hardware, Software Architecture. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.isa.org%2Fstandards-publications%2Fisa-publications%2Fintech-magazine%2F2010%2Fdecember%2Fautomation-basics-programmable-logic-controllers-hardware-software-architecture%2F&date=2017-05-18, Son Erişim Tarihi: 18.05.2017.

70. Alphonsus, E. R. ve Abdullah, M. O. (2016). *A Review on The Applications of Programmable Logic Controllers (PLCs).* Renewable and Sustainable Energy Reviews, 60, 1185–1205.

71. İnternet: The Jet Propulsion Laboratory of NASA. Programmable Logic Controllers. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fengineer.jpl.nasa.gov%2Fpractices%2Fops05.pdf&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

72. Kiran, A. R., Sundeep, B. V., Vardhan, C. S. and Mathews, N. (2013). The Principle of Programmable Logic Controller and Its Role in Automation. ***International Journal of Engineering Trends and Technology***, 4(3), 500–502.

73. Patel, S. C., Bhatt, G. D. and Graham, J. H. (2009). Improving the Cyber Security of SCADA Communication Networks. ***Communications of the ACM***, 52(7), 139–142.

74. İnternet: Shodan. Shodan Search Engine. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.shodan.io%2F&date=2017-05-16, Son Erişim Tarihi: 16.05.2017.

75. Clarke, G. R., Reynders, D. and Wright, E. (2004). Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, Hollanda: Elsevier.

76. Bhattacharyya, D. (2008). The Taxonomy of Advanced SCADA Communication Protocols. ***Journal of Security Engineering***, 5(6), 517–526.

77. East, S., Butts, J., Papa, M. and Shenoi, S. (2009). *A Taxonomy of Attacks on the DNP3 Protocol*. IFIP International Federation for Information Processing, 311, 67–81.

78. İnternet: RACOM. Protocol DNP 3 for MORSE Distributed Network Protocol version 3. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.racom.eu%2Feng%2Fsupport%2Fprot%2Fdnp3%2Findex.html&date=2017-03-10, Son Erişim Tarihi: 16.05.2017.

79. Makhija, J. and Subramanyan, L. R. (2003). *Comparison of Protocols Used in Remote Monitoring: DNP 3.0, IEC 870-5-101 & Modbus*. Electronics Systems Group, 1–19, Bombay, Hindistan.

80. İnternet: Modbus IDA. MODBUS Application Protocol. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.modbus.org%2Fdocs%2FModbus_Application_Protocol_V1_1b.pdf&date=2017-03-10, Son Erişim Tarihi: 10.03.2017

81. İnternet: Siemens System Manual. PROFINET System Description. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.siemens.fi%2Fpool%2Fproducts%2Findustry%2Fiadt_is%2Ftuotteet%2Fautomaatiotekniikka%2Fteollinen_tiedonsiirto%2Fprofinet%2Fman_pnsystem_description.pdf&date=2017-04-15, Son Erişim Tarihi: 15.04.2017

82. İnternet: Phoenix Contact. User Manual Profinet Basics. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.switchingonthefuture.be%2Fdownloads%2Fmanualsfabrikanten%2FPHOENIX+CONTACT%2FProfinet+Basics%2FPN_Basics.pdf&date=2017-05-21, Son Erişim Tarihi: 21.05.2017

83. İnternet: Profinet International White Paper. Profınet and IT. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.automation.com%2Fpdf_articles%2Fprofinet%2Fpi_white_paper_profinet_it_en_v1_0.pdf&date=2017-05-21, Son Erişim Tarihi: 21.05.2017

84. İnternet: Risk Based Security. Our New Year Vulnerability 'Trends' Prediction. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.riskbasedsecurity.com%2F2015%2F12%2Four-new-year-vulnerability-trends-prediction%2F&date=2018-05-10, Son Erişim Tarihi: 10.05.2017.

85. Amanullah, M. T. O., Kalam, A. and Zayegh, A. (2005). *Network Security Vulnerabilities in SCADA and EMS*. Proceedings of the IEEE Power Engineering Society Transmission and Distribution Conference, 1–6, Dalian, Çin.

86. İnternet: Idaho National Laboratory. Vulnerability Analysis of Energy Delivery Control Systems. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fenergy.gov%2Fsites%2Fprod%2Ffiles%2FVulnerability%2520Analysis%2520of%2520Energy%2520Delive

ry%2520Control%2520Systems%25202011.pdf&date=2017-02-02, Son Erişim Tarihi: 02.02.2017.

87. İnternet: US Department of Homeland Security Centre for the Protection Of National Infrastructure. Cyber Security Assessments of Industrial Control Systems: Good Practice Guide. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.ccn-cert.cni.es%2Fpublico%2FInfraestructurasCriticaspublico%2FCPNI-Guia-SCI.pdf&date=2017-04-17, Son Erişim Tarihi: 17.04.2017.

88. İnternet: Toolswatch Hackers Arsenal. ICS / SCADA Top 10 Most Dangerous Software Weaknesses. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.toolswatch.org%2Fwp-content%2Fuploads%2F2015%2F11%2FICSSCADA-Top-10-Most-Dangerous-Software-Weaknesses.pdf&date=2017-04-04, Son Erişim Tarihi: 04.04.2017

89. Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., Soulsby, H. and Stoddart, K. (2015). *A Forensic Taxonomy of SCADA Systems and Approach to Incident Response*. Proceedings of the 3 International Symposium for ICS & SCADA Cyber Security Research, 42–51, Ingolstadt, Almanya.

90. Martin, B., Brown, M., Paller, A., Kirby, D. and Christey, S. (2011). CWE - 2011 CWE/SANS Top 25 Most Dangerous Software Errors. ***MITRE*** versiyon 1.08.

91. İnternet: Industrial Defender White Paper. Report from the Field : Seven Best Practices for Automation System Cyber Security and Compliance. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.isssource.com%2Fwp-content%2Fuploads%2F2012%2F05%2F053012Industrial-Defender-Seven-Best-Practices.pdf&date=2017-06-10, Son Erişim Tarihi: 10.06.2017

92. Graham, J. H. and Patel, S. C. (2004). Security Considerations in SCADA Communication Protocols. ***Intelligent Systems Research Laboratory***, 502, 1–24.

93. Yun, J. H., Jeon, S. H., Kim, K. H. and Kim, W. N. (2013). Burst-based anomaly detection on the DNP3 protocol. ***International Journal of Control Automation***, 6(2), 313–324.

94. Majdalawieh, M., Parisi, F. and Wijesekera, D. (2006). *DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework*. Advanced Computer Information System Science Engineering, 227-234, Dordrecht, Hollanda.

95. Rodofile, N. R., Radke, K. and Foo, E. (2015). *Real-Time and Interactive Attacks on DNP3 Critical Infrastructure Using Scapy*. Conferences in Research and Practice in Information Technology Series, 161(1), 67–70.

96. Huitsing, P., Chandia, R., Papa, M. and Shenoi, S. (2008). Attack Taxonomies for The Modbus Protocols. ***International Journal of Critical Infrastructure Protection***, 1, 37–44.

97. İnternet: MODBUS. MODBUS over Serial Line–Specification and Implementation Guide. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.modbus.org%2Fdoc

s%2FModbus_over_serial_line_V1.pdf&date=2017-01-23, Son Erişim Tarihi: 23.01.2017.

98. İnternet: Modbus-IDA. Modbus Messaging on TCP / IP Implementation Guide. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.modbus.org%2Fdocs%2FModbus_Messaging_Implementation_Guide_V1_0b.pdf&date=2017-02-04, Son Erişim Tarihi:04.02.2017.

99. Morris, T. H. (2009). On Cyber Attacks and Signature Based Intrusion Detection for Modbus Based Industrial Control, ***The Journal of Digital Forensics, Security and Law***, 9(1), 37–56.

100. Yau, K. and Chow, K. P. (2015). PLC Forensics Based on Control Program Logic Change Detection. ***The Journal of Digital Forensics, Security and Law***, 10(4), 59–68.

101. AlShemeili, A., Yeun, C. Y. and Baek, J. (2016). PLC Monitoring and Protection for SCADA Framework. ***Advanced Multimedia and Ubiquitous Engineering***, 354, 259–267.

102. Siven, J. (2015). *Securing Profinet Networks*, Yüksek Lisans Tezi. Helsinki Metropolia University of Applied Sciences, Helsinki.

103. İnternet: Digital Bond. PROFINET Fuzzer Released | Digital Bond. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.digitalbond.com%2Fblog%2F2012%2F12%2F17%2Fprofinet-fuzzer-released%2F&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

104. İnternet: Industrial Control Systems Cyber Emergency Response Team. ICS-CERT Montly Monitor. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fics-cert.us-cert.gov%2Fsites%2Fdefault%2Ffiles%2FMonitors%2FICS-CERT_Monitor_Jan2012.pdf&date=2017-05-22, Son Erişim Tarihi: 22.05.2017.

105. İnternet: Industrial Control Systems Cyber Emergency Response Team. Increasing Threat to Industrial Control Systems (Update A). URL: http://www.webcitation.org/query?url=https%3A%2F%2Fics-cert.us-cert.gov%2Falerts%2FICS-ALERT-12-046-01A&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

106. Leverett, E. (2011). *Quantitatively Assessing and Visualising Industrial System Attack Surface*, Yüksek Lisans Tezi, Advanced Computer Science of University of Cambridge, Cambridge.

107. İnternet: Tofino Industrial Security Solution. Project SHINE: 1,000,000 Internet-Connected SCADA and ICS Systems and Counting. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.tofinosecurity.com%2Fblog%2Fproject-shine-1000000-internet-connected-scada-and-ics-systems-and-counting&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

108. İnternet: Industrial Control Systems Cyber Emergency Response Team. ICS-CERT Monitor. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fics-

cert.us-cert.gov%2Fsites%2Fdefault%2Ffiles%2FMonitors%2FICS-CERT_Monitor_Jul-Sep2013.pdf&date=2017-05-19, Son Erişim Tarihi: 19:05.2017.

109. İnternet: Wireshark. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.wireshark.org%2F&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

110. İnternet: Nmap: the Network Mapper. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fnmap.org%2F&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

111. İnternet: PLCSCAN, Google Code Archive - Long-term storage for Google Code Project Hosting. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fcode.google.com%2Farchive%2Fp%2Fplcscan%2F&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

112. İnternet: SCADAhacker. Metasploit Modules for SCADA Vulnerabilities. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.scadahacker.com%2Fresources%2Fmsf-scada.html&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

113. İnternet: Rapid7. Modbusdetect. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fgithub.com%2Frapid7%2Fmetasploit-framework%2Fblob%2Fmaster%2Fmodules%2Fauxiliary%2Fscanner%2Fscada%2Fmodbusdetect.rb&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

114. İnternet: Rapid7. Modbusclient. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fgithub.com%2Frapid7%2Fmetasploit-framework%2Fblob%2Fmaster%2Fmodules%2Fauxiliary%2Fscanner%2Fscada%2Fmodbusclient.rb&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

115. İnternet: The Telegraph. CIA Plot Led to Huge Blast in Siberian Gas Pipeline - Telegraph. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.telegraph.co.uk%2Fnews%2Fworldnews%2Fnorthamerica%2Fusa%2F1455559%2FCIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

116. İnternet: Central Intelligence Agency. The Farewell Dossier. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.cia.gov%2Flibrary%2Fcenter-for-the-study-of-intelligence%2Fkent-csi%2Fvol39no5%2Fpdf%2Fv39i5a14p.pdf&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

117. Turk, R. J. (2005). Cyber Incidents Involving Control Systems. ***US-CERT Control Systems Security Center***, 1–58.

118. İnternet: BBC NEWS. Technology | Questions Cloud Cyber Crime Cases. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fnews.bbc.co.uk%2F2%2Fhi%2Ftechnology%2F3202116.stm&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

119. İnternet: ComputerWorld. Study: Slammer Was Fastest-Spreading Worm yet. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.computerworld.com%2Farticle%2F2579971%2Fsecurity0%2Fstudy--slammer-was-fastest-spreading-worm-yet.html&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

120. Weiss, J. (2010). *Protecting Industrial Control Systems from Electronic Threats*, ABD: Momentum Press.

121. İnternet: The Wall Street Journal. Electricity Grid in U.S. Penetrated By Spies. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.wsj.com%2Farticles%2FSB123914805204099085&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

122. E. Chien and G. O'Gorman (2011). The Nitro Attacks: Stealing Secrets from the Chemical Industry. ***Symantec Security Response***, 1–8.

123. İnternet: The Register Publication. Stuxnet 'A Game Changer for Malware Defence. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.theregister.co.uk%2F2010%2F10%2F09%2Fstuxnet_enisa_response%2F&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

124. Knopová, M. and Knopová, E. (2014). The Third World War? In The Cyberspace. Cyber Warfare in the Middle East. ***Acta Informatica Pragensia***, 3(1), 23–32.

125. Chien, E., O'Murchu, L. and Falliere, N. (2011). W32.Duqu The Precursor to the Next Stuxnet. ***Symantec Security Response***, 1(4), 1–71.

126. Bronk, C. and Ringas, E. (2013). Hack or Attack? Shamoon and the Evolution of Cyber Conflict. ***Institute for Public Policy Rice University***, 1–30.

127. Fillinger, M. (2013). *Reconstructing the Cryptanalytic Attack behind the Flame Malware*. Yüksek Lisans Tezi, Institude for Logic, Language and Computation of Amsterdam University, Amsterdam.

128. İnternet: The Washington Post. U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.washingtonpost.com%2Fworld%2Fnational-security%2Fus-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say%2F2012%2F06%2F19%2FgJQA6xBPoV_story.html%3Futm_term%3D.0571b41f056c&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

129. İnternet: ABC News. DHS: Hackers Mounting Organized Cyber Attack on U.S. Gas Pipelines. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fabcnews.go.com%2FBlotter%2Fdhs-hackers-mounting-organized-cyber-attack-us-gas%2Fstory%3Fid%3D16304818&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

130. İnternet: ESET Smart Security. ESET Finds Connection Between Cyber Espionage and Electricity Outage in Ukraine. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.eset.com%2Fint%2

Fabout%2Fnewsroom%2Fresearch%2Feset-finds-connection-between-cyber-espionage-and-electricity-outage-in-ukraine%2F&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

131. İnternet: WeLiveSecurity | ESET. BlackEnergy by the SSHBearDoor: Attacks against Ukrainian News Media and Electric Industry. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.welivesecurity.com%2F2016%2F01%2F03%2Fblackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry%2F&date=2017-05-21, Son Erişim Tarihi: 21.05.2017.

132. İnternet: Modbus Poll Simulator. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.modbustools.com%2Fdownload.html&date=2018-05-25, Son Erişim Tarihi: 25.05.2017.

133. Irmak, E. ve Erkek, İ. (2016). Adding New Parameters to Attacker Profile by Using Multi-Attribute Utility Theory, ***Uluslararası Bilgi Güvenliği Mühendisliği Dergisi***, 2(2), 1–9.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : ERKEK, İsmail
Uyruğu : T.C.
Doğum tarihi ve yeri : 03.01.1990, Konya
Medeni hali : Bekar
Telefon : 0 (505) 355 28 08
e-mail : ismailerkek2014@gmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Bilgi Güvenliği Mühendisliği	2018
Lisans	Eskişehir Osmangazi Üniversitesi / Elektrik Elektronik Mühendisliği	2013
Lise	Kalaba Anadolu Lisesi	2008

İş Deneyimi

Yıl	Yer	Görev
2017-Halen	Barikat Bilişim Güvenliği	Sızma Testi Uzmanı
2015-2017	İnnova Bilişim Çözümleri A.Ş.	Bilgi Teknolojileri Uzmanı

Yabancı Dil

İngilizce

Yayınlar

Irmak, E. ve Erkek, İ. (2016). Adding New Parameters to Attacker Profile by Using Multi-Attribute Utility Theory. ***Uluslararası Bilgi Güvenliği Mühendisliği Dergisi***, 2(2), 1–9.

Irmak, E., Erkek, İ. ve Özçelik, M. M. Experımental Analysis of the Internal Attacks on Scada Systems. ***Gazi University Journal of Science,*** 30(4), 216-230.

Ödüller

ISCTurkey Bilgi Güvenliği ve Kriptoloji Konferansı en iyi yayın ödülü (Best Paper Award - Adding New Parameters to Attacker Profile by Using Multi-Attribute Utility Theory).

GAZİ GELECEKTİR...