Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 24, No 4, 715-723, 2009

J. Fac. Eng. Arch. Gazi Univ.
Vol 24, No 4, 715-723, 2009

İZLENEBİLİR ELEKTRİK ENERJİSİ DAĞITIM SİSTEMİNİN BİLGİ GÜVENLİĞİ AÇISINDAN ENDÜSTRİYEL RİSKLERİNİN ARAŞTIRILMASI VE ÇÖZÜM ÖNERİLERİ

Ramazan BAYINDIR, Şeref SAĞIROĞLU, İlhami ÇOLAK ve Alper ÖZBİLEN
GEMEC-Gazi Elektrik Makineleri ve Enerji Kontrol Grubu
Elektrik Eğitimi Bölümü, Teknik Eğitim Fakültesi, Gazi Üniversitesi, 06500 Beşevler Ankara
bayindir@gazi.edu.tr, ss@gazi.edu.tr, icolak@gazi.edu.tr, alper.ozbilen@tib.gov.tr

(Geliş/Received: 20.01.2009 ; Kabul/Accepted: 03.07.2009)

ÖZET

Bu çalışmada, Gazi Üniversitesi Teknik Eğitim Fakültesi Elektrik Eğitimi Bölümünde kurulu enerji dağıtım sistemine ait elektriksel parametreleri görüntüleyen ve saklayan enerjisi izleme sisteminin güvenlik riskleri incelenmiştir. İnceleme kapsamında sistemin bilgi güvenliği açısından açıklıkları araştırılmış ve elde edilen açıklıklardan dolayı oluşabilecek riskler tanımlanmıştır. Bunun yanında, Modbus otomasyon protokolü yetkisiz erişimler açısından gözden geçirilmiş ve sistemde açıklıklar oluşturduğu tespit edilmiştir. Tespit edilen açıklıkları gidermek ve sistemi güvenli hale getirmek için, açık kaynak kodlu çeşitli projeler incelenerek mevcut sisteme güvenlik duvarı eklenmiştir. Sonuç olarak, enerji sistemlerinde oluşabilecek bilgi güvenliği risklerinin azaltılmasına yönelik olarak somut önerilerde bulunulmuştur.

Anahtar Kelimeler: Enerji otomasyonu, bilgi güvenliği, güvenlik duvarı, Modbus protokolü, güvenlik riskleri.

INVESTIGATING INDUSTRIAL RISKS BASED ON INFORMATION SECURITY FOR OBSERVERABLE ELECTRICAL ENERGY DISTRIBUTION SYSTEM AND SUGGESTIONS

ABSTRACT

In this study, computer based central electricity parameter observation and tracking system of energy distribution system at Electrical Education of Gazi University and its security risks have been examined. Determining of security risk due to system vulnerabilities and possibility of unauthorized data access are investigated in respect of information security. In addition, some system security risks are found when unauthorized accesses of Modbus protocol are tested. To avoid detected risks, a firewall is installed to provide secure platform for the system from different open source projects. Finally, some recommendations are outlined to reduce information security risks at energy system.

Keywords: Energy automation, information security, firewall, Modbus protocol, security risks.

1. GİRİŞ (INTRODUCTION)

Coğrafi ve fonksiyonel olarak dağıtık olan endüstriyel uygulamaların merkezi olarak izlenmesi ve yönetilmesine imkan tanıyan Dağıtık Denetim Sistemleri (DDS), iş akışının bir parçası olarak, bağımsız her bir sistem bileşeninin dinamik değişkenlerini, sürecin diğer koşullarını da dikkate alıp merkezi olarak yönetirler. Birbirinden farklı birçok endüstriyel alanlarda kullanılan denetim ve izleme sistemlerinin tümü DDS olarak anılır. Bu endüstriyel alanlara, elektrik güç dağıtım şebekeleri, su ve gaz dağıtım şebekesi, trafik sinyalizasyon şebekeleri, petrol rafine sistemleri ve kimyasal tesisler örnek olarak verilebilir [1-3].

DDS'ler, önceden tanımlı belirli görevlere adanmış bilgisayarlar kullanırlar. İş süreçlerinin farklı bölümlerinde görev alan bu denetim elemanları belirli bir haberleşme protokolü kullanarak birbirleriyle haberleşirler.

DDS'ler, tipik olarak, farklı fonksiyonları olan veya coğrafi yönden dağıtık olan birçok denetleyiciye sahiptir. Endüstriyel uygulamalar içerisinde yer alan ve her sürece ait giriş ve çıkışları (I/O) izleyen denetleyiciler, doğrudan veya başka bir denetleyici üzerinden merkezi birime bağlıdır [2].

Günümüz denetleyicileri, PID (Proportional Integral Derivative) denetim fonksiyonlarına ilaveten mantıksal ve sıralı denetim yeteneklerine de sahiplerdir. Gerek denetleyici bazında, gerekse tüm uygulama bazında artan işlev gereksinimleri, DDS'lere olan ihtiyacı ve önemi daha da arttırmıştır [4].

Elektrik, su, gaz dağıtımı gibi nispeten geniş çaplı sistemler binlerce denetleyici içerebilirler. Bu tür sistemlerde, asıl baş gösteren problem yerel noktalardaki denetleyicilerin hesaplamalarından çok, birbirine merkezi DDS üzerinden bağlı bu denetleyiciler arasındaki bilgi akışını koordine etmektedir [2-4].

Başlangıçta, DDS'ler, denetleyicilerinin üzerinde var olan seri haberleşme portları üzerinde kendi özel protokolleriyle haberleşirken ve çoğunlukla her bir denetleyiciye ait haberleşme kanalı fiziksel olarak diğer haberleşme kanallarından izoleyken; günümüz de DDS'lerinin, sıklıkla Modbus/TCP protokolünü kullanıldığı ve bu protokolün tüm sistem tedarikçilerince de desteklenmeye başladığı görülmektedir. Özel veya genel haberleşme ortamlarında kullanılabilen internet haberleşme protokolü (IP) üzerinde bir üst katman protokolü olarak çalışan Modbus/TCP, tıpkı WEB, e-posta, P2P gibi herhangi bir internet trafiği sınıfında yer almaktadır [3-5]. Bir yandan doğrudan veya dolaylı erişimin olması halinde, sistem yöneticilerine internet üzerinden dahi yönetme imkanı tanıyan bu haberleşme ortamı, diğer yandan geniş kitlelere zarar verebilecek açıklıklar (vulnerabilities) içermektedir.

Yüksek hızda veri haberleşmesinin tamamen IP protokolü üzerinden yapılmaya başlandığı günümüzde, endüstriyel süreç denetim sistemlerine özel olarak daha güvenli arayüz ve protokol tasarımı yapılmasını beklemek mali gerekçeler açısından pek gerçekçi değildir. Zira mevcut durum, tüm tedarikçilerin, ürettikleri merkezi endüstriyel süreç denetim sistemlerine ait haberleşme sistemlerini, bilgisayarlarda kullanılan tipik ethernet kartları ve üzerinde koşan IP protokolüne dayandırdıkları görülmektedir [1-3]. Artık endüstriyel standart haline gelen bu yapı, geleneksel süreç denetim sistemlerini, erişim noktalarının tespiti durumda her türlü siber saldırıya maruz kalabilecek duruma getirmiştir.

Endüstriyel süreç denetim sistemlerine ait merkezi izleme ve yönetim birimleri (MTU: Master Terminal Unit), Unix veya MS Windows işletim sistemleri üzerinde koşan ve çoğunlukla Modbus/TCP protokolü ile kenar denetleyiciler (RTU: Remote Terminal Unit) ile haberleşen yönetim yazılımlarıdır. Diğer yandan kenar denetleyiciler ise önceden belirli denetleme işlevlerini yerine getiren ve merkez ile IP tabanlı Modbus/TCP haberleşmesi yapmakla birlikte, birçok güvenlik mekanizmasının işletilmediği kısıtlı bir işletim sistemine sahip cihazlardır. Kısaca, MTU ile RTU, haberleşme açısından, kendi aralarında internet protokolünü kullanarak haberleşen herhangi iki bilgisayar gibi davranır [5, 6]. Ancak temel görevi kendi sorumlu olduğu süreç parçasını denetlemek olan RTU'ların sahip oldukları kısıtlı işletim sistemi, MTU–RTU haberleşmesinde kalıtsal olarak birçok açığın oluşmasına sebebiyet verebilecektir.

Diğer yandan MTU yazılımlarının koştuğu Unix veya MS Windows işletim sistemlerine ait her türlü güvenlik açığı, endüstriyel sistem güvenliğinin üst sınırlarını doğrudan belirler [7-9].

Bilgi teknolojileri alanındaki var olan her türlü risk endüstriyel süreç denetim sistemleri içinde geçerlidir. Dolayısıyla, dar anlamda endüstriyel süreç denetim sistemlerinin güvenliği, geniş anlamda ise endüstriyel ortam güvenliği, kendi kalıtsal risklerinin yanı sıra "bilgi ve haberleşme teknolojilerinin" sahip olduğu açıklıklara ve risklere tabidir.

Bu çalışmada modern endüstriyel süreç denetim sistemlerinde sıklıkla kullanılan Modbus/TCP protokolün sahip olduğu fonksiyon kodları, haberleşme mesaj başlıkları ayrıntılı olarak incelenmiş ve *netfilter-iptables* güvenlik duvarında kullanılmak üzere tablo yapısı araştırılmıştır. Böylece, Modbus/TCP protokolü, *netfilter-iptables* güvenlik duvarına entegre edilmiş ve izlenebilir elektrik enerjisi dağıtım sisteminde yer alan Modbus sunucu ile istemci arasına yerleştirilerek sunucuya yapılacak yetkisiz erişimlerin engellenmesine yönelik öneriler sunulmuştur.

2. İZLENEBİLİR ELEKTRİK ENERJİ DAĞITIM SİSTEMİNİN GENEL YAPISI VE BİLEŞENLERİ (GENERAL STRUCTURE AND COMPONENTS OF TRACKABLE ELECTRICAL ENERGY DISTRIBUTION SYSTEMS)

Bu çalışma kapsamında, Gazi Üniversitesi Teknik Eğitim Fakültesi (GÜTEF) Elektrik Eğitimi Bölümünde kurulan ve 50 kW güce sahip enerji dağıtım sistemine ait elektriksel parametreleri görüntüleyen ve saklayan enerjisi izleme sistemi kullanılmıştır. Enerji izleme sisteminin temel donanımsal bileşenleri aşağıda verilmiştir [10].

- 'Merlin Gerin PM710' enerji analizörü enerji dağıtım sistemine ait şu değerleri ölçer: Faz akımları; nötr akım; ortalama akım; faz-faz gerilim; faz-nötr gerilim; ortalama faz-faz gerilim; ortalama faz-nötr gerilim; fazların aktif ve reaktif güçleri; frekans; cosφ; aktif, reaktif ve görünür güç tüketimi.

- Analizörden alınan örnekleme bilgilerini bilgisayarın anlayacağı ve erişebileceği anlamlı veriler haline getirmek için Modicon TSX Premium (TSX P57 103M CPU, TSX PSY 1610 güç kaynağı, TSX ETY 4103 ethernet modül, TSX SCP 114 Modbus PCMCI kart).
- Ethernet üzerinden alınan ölçüm verileri saklamak ve değerlendirmek üzere kullanılan bir bilgisayar.

Analizörden alınan veriler, izleme bilgisayarınca yorumlandıktan sonra aynı bilgisayar üzerindeki veritabanında saklanmaktadır. Analizörden alınan bir verinin izleme sisteminin ekranına yansıtılması 200ms aralıklarla yapılmaktadır. Veritabanına kayıt için ise 1 dakikalık aralıklar kullanılmaktadır [10-12].

Analizörden alınan veriler, enerji izleme sistemine ethernet bağlantısı üzerinden gönderilmektedir. Analizör üzerinde kullanılan ethernet modülü, 502. port üzerinden 64 adet farklı birimi tarayabilmektedir.

GÜTEF Elektrik Eğitimi bölümü bünyesinde, 50 KW'lık güç dağıtım sisteminin izlenebilmesi için kurulan sistemin genel görünümü Şekil 1'de verilmiştir [10].

Analizör tarafından ölçülen enerji parametreleri, izleme bilgisayarına aktarıldıktan sonra akım, genlik, güç ve frekans değerleri belirli zaman aralıkları için liste veya grafik olarak görüntülenebilmektedir.

Enerji izleme sistemindeki analizör ile izleme bilgisayarı arasındaki bilgi akışı her iki bileşeninde sahip olduğu ethernet arayüzleri üzerinden Modbus TCP protokolü kullanılarak yapılmaktadır. Bu çalışmada enerji izleme sistemindeki bu bilgi akışının güvenli olarak sağlanması için incelemeler yapılmış ve çözüm önerileri üzerinde durulmuştur.

3. ENERJİ OTOMASYONUNDA KULLANILAN HABERLEŞME PROTOKOLÜ: MODBUS
(COMMUNICATION PROTOCOL USED IN ENERGY AUTOMATION: MODBUS)

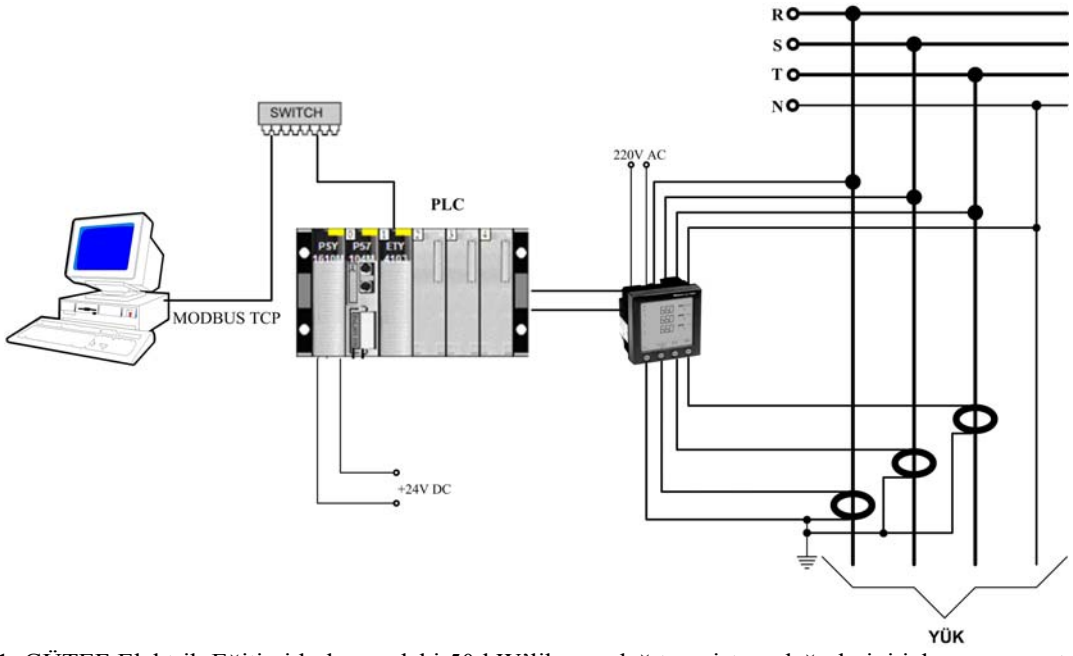
Modbus, günümüzde milyonlarca otomasyon sisteminde kullanılan, istemci sunucu yapısında yer alan bir haberleşme protokolüdür. Uygulama seviyesinde mesajlaşma protokolü olan Modbus, OSI haberleşme mimarisinde 7. katmanda yer almaktadır. Dolayısıyla, seri port ve TCP/IP gibi farklı haberleşme protokol ve standartları üzerinde çalışabilir [13, 14].

1979 yılında Modicom firmasınca tasarlanan Modbus, bu gün otomasyon pazarında *de facto* bir standart haline gelmiş olup, hem üreticiler hem de açık kaynak topluluklarınca sürekli geliştirilen ve desteklenen bir protokol olmayı başarmıştır.

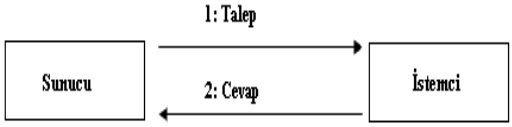
Modbus, istemci-sunucu birimleri arasında talep-cevap (request-response) mekanizmasını yürütür. Birbiriyle konuşan iki birim arasında farklı servisleri tanımlayan fonksiyon kodları (function code) kullanılır [13].

Şekil 2'de verildiği gibi, Modbus protokolünde talepler istemci, cevaplar ise sunucu tarafından gönderilir. Bu anlamda, iletişimin istemci tarafından şekillendirildiği kolaylıkla söylenebilir.

Bu haberleşme protokolü alt başlıklarda kısaca açıklanmıştır.



Şekil 1. GÜTEF Elektrik Eğitimi bölümündeki 50 kW'lik güç dağıtım sistem değerlerini izleyen mevcut sistem (Tracking system of 50 kW power distribution system parameters at Electrical Education of GUTEF) [10]



Şekil 2. Modbus istemci ve sunucu haberleşmesi (Modbus client-server communication)

3.1. Modbus Protokol Veri Birimi (Modbus Protocol Data Unit)

Protokol Veri Birimi (PDU), iletişim içeriğinin tutulduğu, asıl icracı birime verilen addır ve üç sınıfta incelenir. Bunlar;

PDU Talep Paketi: Fonksiyon kodu (1 bayttır) ve fonksiyonun tanımlayıcısı değişkendir.

PDU Cevap Paketi: Talebe karşılık gelen fonksiyon kodu (1 bayt) ve cevap tanımlayıcısı değişkendir.

PDU İstisna Paketi: Hata kodu (Fonksiyon Kodu + 0x80 (128), 1 bayttır) ve istisna tanımlayıcısı (1 bayttır).

Modbus PDU'nun boyutu 256 bayt ile sınırlıdır. Modbus PDU başlık yapısı Şekil 3'de verilmiştir [15].

3.2. Modbus Uygulama Başlığı (Modbus Application Header)

7 bayttan oluşan Modbus uygulama başlığı (Modbus APU) aşağıdaki bileşenlerden oluşur.

Süreç Numarası (Transaction ID,2 bayt): Modbus istemci ve sunucusu arasındaki talep ve cevap sürecini sırayla numaralandıran başlık bilgisidir [15].

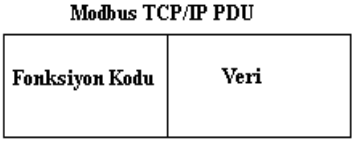
Protokol Numarası (Protocol ID, 2 bayt): Ön tanımlı olarak 0 kullanılır. Diğer değerler gelecek uygulamalar için ayrılmıştır.

Boyut (Length, 2 bayt): Kendisinden sonraki bayt sayısını yazan alandır.

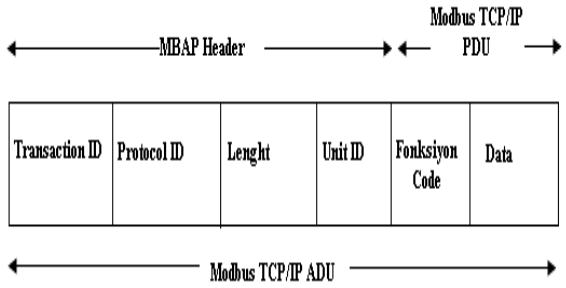
Birim Tanımlayıcısı (Unit ID, 1 bayt): TCP/IP uygulamalarında geçerliği olmayan bir alandır.

Şekil 4'de Modbus APU başlık yapısı gösterilmiştir [15].

Örnek Modbus TCP/IP paket içeriği:
0001 0000 0006 11 03 006B 0003
0001: İşlem Tanımlayıcısı
0000: Protokol Tanımlayıcısı
0006: Mesaj Uzunluğu
11: Birim Tanımlayıcısı
03: Fonksiyon Kodu



Şekil 3. Modbus PDU başlık yapısı (Modbus PDU header structure)



Şekil 4. Modbus AP başlık yapısı (Modbus AP header structure) [15]

006B: Gerekli İlk Yazmaç İçin Veri Adresi (40108-40001 = 107 =6B hex)
0003: Gerekli Yazmaçların Toplam Sayısı (read 3 registers 40108 to 40110)

3.3. Modbus Veri Modeli (Modbus Data Model)

Modbus veri modeli Tablo 1'i esas alır [15].

Tablo 1. Modbus veri modeli (Modbus data model) [15]

Kod Tipi	Nesne Tipi	Erişim Tipi	Açıklamalar
Ayrık Giriş	Tek Bit	OKU	Bu tür veriler giriş çıkış birimlerince sağlanabilir.
Sarmal	Tek Bit	OKU YAZ	Bu tür veriler uygulama programınca değiştirilebilir.
Giriş Kayıtcısı	16 Bit Kelime	OKU	Bu tür veriler giriş çıkış birimlerince sağlanabilir.
Tutucu Kayıtcısı	16 Bit Kelime	OKU YAZ	Bu tür veriler uygulama programınca değiştirilebilir.

3.3.1. Fonksiyon Kodları (Function Code)

Fonksiyon kodları 1-127 (ondalık) tanımlıdır. Her bir fonksiyona karşılık olarak gelebilecek hata kodları ise $129_{(1+128)}$- $255_{(127+128)}$ aralığında tanımlıdır [15].

Fonksiyon kodları üç sınıfa ayrılır[15]. Bunlar;

Genel (Public): Tanımlanmış ve belgelendirilmiş fonksiyonların kullandığı kodlardır. Her türlü topluluk ve üretici tarafından kabul edilen ve kullanılan Modbus fonksiyonlarıdır.

Kullanıcı Tanımlı (User Defined): 65-72 ve 100-110 özel tasarlanan Modbus fonksiyonları için kullanılan kodlardır.

Ayrılmış (Reserved): Üreticilerin daha önceki ürünlerinde kullanmış olduğu ve genel kullanıma kapalı olan kodlardır. Genel fonksiyon kodları Tablo 2'de verilmiştir.

4. MEVCUT ENERJİ İZLEME SİSTEMİNDE GÜVENLİK RİSKLERİ TESPİTİ (DETERMINING SECURITY RISKS AT PRESENT ENERGY TRACKING SYSTEM)

Bu çalışmada enerji sisteminde oluşabilecek güvenlik açıklıklarını tespit etmek için Şekil 5'de verilen deney

Tablo 2. Genel Fonksiyon Kodları (General Function Code) [15]

	Fiziksel Birim	Yürütülen Fonksiyon	Fonksiyon Kodları	
			Desimal	Heksadesimal
Veri Erişimi	Fiziksel Ayrık Giriş Dahili Bitler Fiziksel Sarmal	Ayrık Girişleri OKU	02	02
		Sarmal OKU	01	01
		Tek Sarmal YAZ	05	05
		Çok Sarmal YAZ	15	015
	Fiziksel Giriş Kayıtcısı	Giriş Kayıtcısını OKU	04	04
		Tutucu Kayıtcısı OKU	03	03
		Tek Kayıtcıya YAZ	06	06
	Dahili Kayıtçı veya Fiziksel Çıkış Kayıtcısı	Çoklu Kayıtcıya YAZ	16	10
		Çoklu Kayıtcıya OKU/YAZ	23	17
		Kayıtcıya YAZ	22	16
		FIFO Kuyruğunu OKU	24	18
	Dosya Kayıt Erişimi	Dosya Kayıtcısını OKU	20	14
		Dosya Kayıtcısını YAZ	21	15
		İstisna durumlarını OKU	07	07
	Tanılar	Tanı	08	08
		Port Durum Sayacını AL	11	0B
		Port Durum Günlüğünü AL	12	0C
		Slave ID Raporla	17	11
		Aygıt Tanımlayıcısını OKU	43	2B

düzeneği kurulmuştur. Mevcut yapıda kayıtçı bilgisayar ile Modicon TSX doğrudan Ethernet arabirimleri üzerinden bağlıdır. Yeni yapıda ise kayıtçı bilgisayar ile Modicon TSX arasındaki ethernet bağlantısı bir HUB üzerinden yeniden kurularak, üçüncü bir bileşenin (bilgisayarın) aradaki haberleşmeye dahil olması kolaylıkla sağlanmıştır.

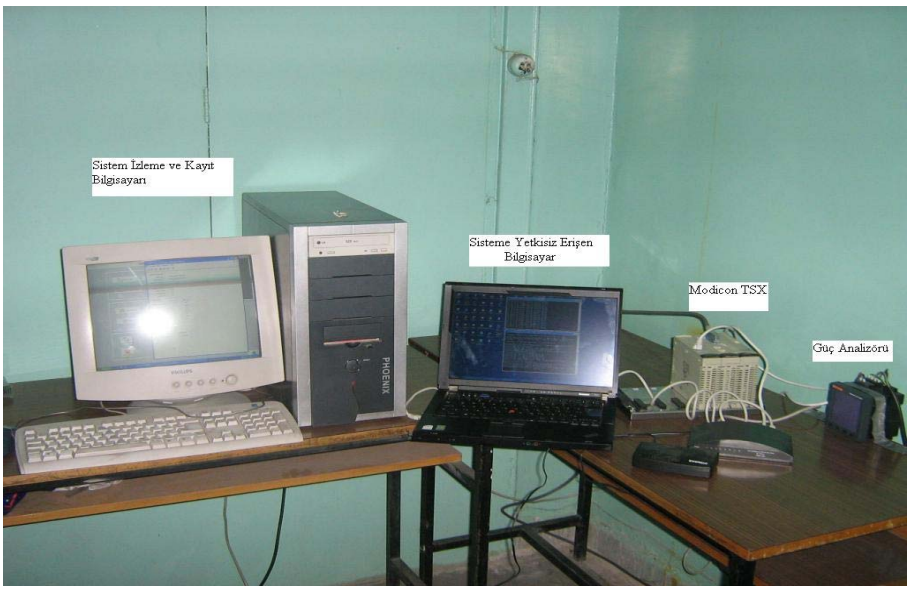
Mevcut deney düzeneğinde, sisteme sonradan dahil edilmiş bilgisayarın yetkisi olmamasına rağmen, Modicon TSX ile kayıt bilgisayarı (mevcut bilgisayar) arasındaki Modbus TCP haberleşmesine erişebilir duruma gelmiştir.

Yetkisiz bilgisayar üzerine kurulu *Paket Koklayıcı (Sniffer/Wireshark)* ile Modbus TCP haberleşmesini tamamen izleyebilir hale gelmiştir. Tasarlanan sistemde, yetkisiz erişimle elde edilen haberleşme bilgisi Şekil 6'da verilmiştir. Şekil 6'da görülebileceği gibi 192.168.15.50 IP'li izleme bilgisayarı ile 192.168.15.10 nolu Modicon TSX sunucu sistemine sahip endüstriyel sistem haberleşmesinin tüm içeriği izlenebilmektedir.

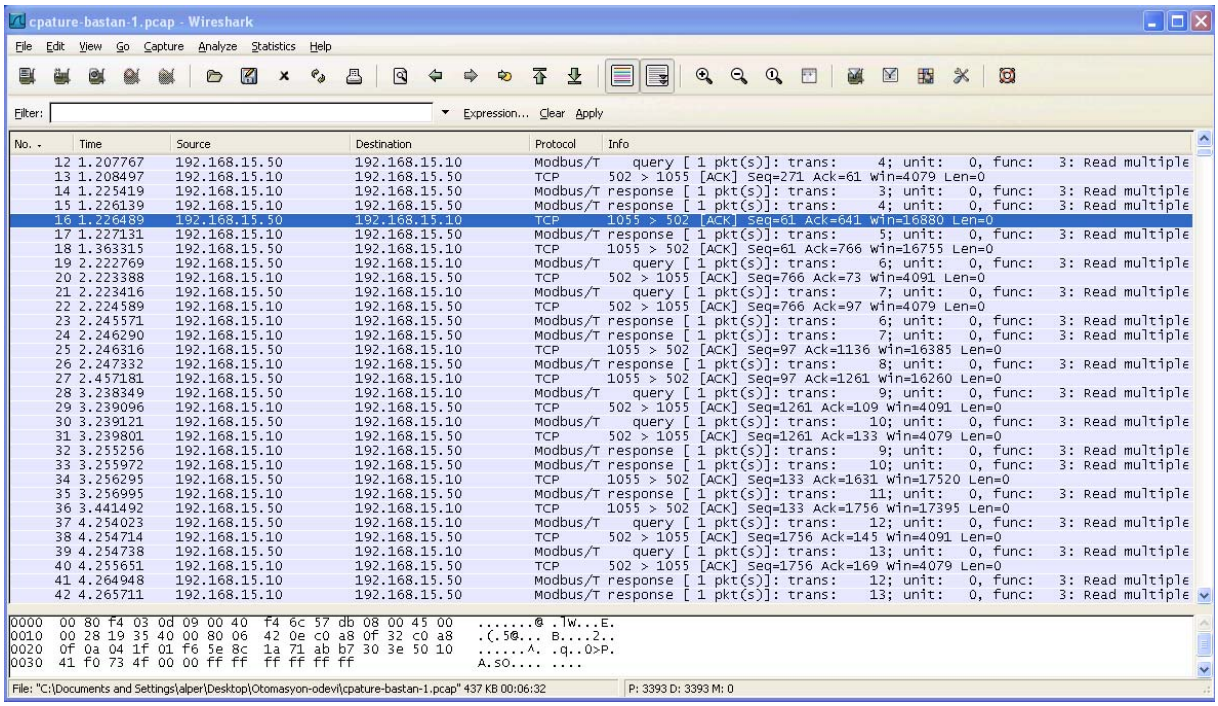
Şu ana kadarki süreçte, sisteme yetkisiz erişimin mümkün olduğu ve enerji dağıtım sistemine ilişkin bilgileri içeren Modbus TCP protokolünün açık olarak (şifresiz ve filtre engeli olmadan) elde edilebileceği gösterilmiştir. Burada yapılan işlem pasif dinlemeden ibarettir.

Enerji İzleme Sisteminde yer alan *Modicon TSX* (Modbus sunucu sistemi) *nmap* ile taranmış ve elde edilen sonuçlar Tablo 3'de verilmiştir.

Tablo 3'de görülebileceği gibi (koyulaştırılmış alanlar), sistemin *21 (FTP), 23 (telnet), 80 (http), 111 ve 502 (Modbus TCP)* portları açıktır. Ayrıca tarama ile Modbus sunucunun koştuğu işletim sistemin adının *VxWorks* olduğu da görülmektedir.



Şekil 5. Enerji izleme sistemine yetkisiz erişim (Unauthorized access to energy tracking system)



Şekil 6. Wireshark ile yakalanan paketler (Packet capturing by Wireshark)

Çalışmanın bu bölümünde yapılan testlerde, endüstriyel otomasyon sistemleri yaygın olarak kullanılan Modbus protokolünün sunucu ve istemci birimler arasında yetkilendirme süreci işletmediği, Modbus istemcisine sahip bir bilgisayarın sunucu sisteme herhangi bir şifre gereksinimi olmadan erişebildiği, Modbus haberleşmesinin şifresiz (clear-text) olarak yapıldığı tespit edilmiştir.

Modbus istemci veya sunucu birimleri, genel veya özel amaçlı işletim sistemleri üzerinde çalışabilirler. Modbus protokolünden bağımsız olarak, bu işletim sistemlerinin sahip oldukları risklerin de ayrıca ele alınması gerekir.

GÜTEF Elektrik Eğitimi Bölümünde kullanılan güç izleme sistemindeki Modbus istemci birimi *MS WINDOWS XP* işletim sistemi üzerinde çalışmakta olup, bu işletim sisteminin çalışmasını aksatacak her türlü zararlı kod ve program doğrudan güç izleme sistemini de etkileyecektir. Diğer yandan, güç izleme sistemindeki Modbus sunucu birimi *VxWorks* endüstriyel işletim sistemi üzerinde çalışmaktadır. Endüstriyel işletim sistemlerin açıklıkları daha az bilinmekle birlikte, sahip oldukları güvenlik fonksiyonları kısıtlı olup güncelleme süreçleri kolay ve tanımlı değildir [1-5].

5. İZLENEBİLİR ELEKTRİK ENERJİ DAĞITIM SİSTEMİNE YETKİSİZ ERİŞİMİN ENGELLENMESİNE YÖNELİK ÖNERİLER (MEASUREMENTS AGAINST UNAUTHORIZED ACCESS TO TRACKABLE ELECTRICAL ENERGY DISTRIBUTION SYSTEMS)

Bölüm 4'de açıklandığı gibi Modbus protokolünde ve işletiminde meydana gelebilecek olası güvenlik açıklıkları güç sistemlerini tehdit edebilecek boyuttadır. Bu tür açıklıkların kapatılması ile kullanılan sistemlerin daha güvenli hizmet vermesi sağlanacaktır.

Mevcut güvenlik duvarları ile IP ve port bazında kısıtlamalar yapmak mümkündür. Ancak günümüz ticari güvenlik duvarlarının Modbus TCP haberleşmesini fonksiyon düzeyinde filtrelemesi henüz mümkün görülmemektedir. Dolayısıyla haberleşmeye IP ve port seviyesinde erişebilen herhangi bir bilgisayarın, aslında yetkili olmasa da her türlü Modbus fonksiyonlarını çalıştırması mümkün olabilecektir.

Modbus TCP istemci birimlerinin IP ve port seviyesinde filtrelenmesi, istemcinin sunucuyla olan haberleşmesini tamamen kısıtlar. İdealde ise endüstriyel ortamlarda, çok sayıda noktayı yöneten veya onlardan bilgi toplayan Modbus sunuculara olan erişim servis seviyesinde (MODBUS Function Code) yetkilendirilebilmelidir. Böylece Modbus sunucunun belirli kayıtçı (register) veya sarmal (coil) bölgelerinde okuyabilen ve/veya yazabilen hizmet tanımları yapılarak kısmen de olsa güvenlik açıklıkları kapatılabilir. Bu çalışma çerçevesinde sunulan çözüm önerileri alt başlıklarda aşağıda açıklanmıştır.

5.1. Netfilter/Iptables Güvenlik Duvarlarının Modbus Protokolü İçin Yeniden Yapılandırılması (Netfilter/Iptables Firewall Reconfiguration for Modbus Protocol)

Netfilter, Linux çekirdek setiyle birlikte gelen ve IP paketlerini yakalama, parçalama, filtreleme ve değiştirme kabiliyetine sahip olan açık kaynak kodlu bir *Güvenlik Duvarı* projesidir. Diğer yandan *iptables* ise kural tanımlarını tutmak için jenerik bir tablo

yapısına sahip olan ve sistem kullanıcıların *netfilter* tablosuna erişimine imkan veren bir uygulama programıdır.

Tablo 3. nmap tarama sonuçları (nmap scanning result)

```
C:\alper>nmap -v -A 192.168.15.10
Starting Nmap 4.50 (http://insecure.org) at 2008-05-15 19:11 GTB Yaz Saati
Initiating ARP Ping Scan at 19:11
Scanning 192.168.15.10 [1 port]
Completed ARP Ping Scan at 19:11, 0.75s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:11
Completed Parallel DNS resolution of 1 host. at 19:11, 12.98s elapsed
Initiating SYN Stealth Scan at 19:11
Scanning 192.168.15.10 [1711 ports]
Discovered open port 21/tcp on 192.168.15.10
Discovered open port 80/tcp on 192.168.15.10
Discovered open port 23/tcp on 192.168.15.10
Discovered open port 502/tcp on 192.168.15.10
Discovered open port 111/tcp on 192.168.15.10
Completed SYN Stealth Scan at 19:11, 1.01s elapsed (1711 total ports)
Initiating Service scan at 19:11
Scanning 5 services on 192.168.15.10
Completed Service scan at 19:12, 71.20s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against 192.168.15.10
Initiating RPCGrind Scan against 192.168.15.10 at 19:12
Completed RPCGrind Scan against 192.168.15.10 at 19:12, 0.00s elapsed (1 port)
SCRIPT ENGINE: Initiating script scanning.
Initiating SCRIPT ENGINE at 19:12
Completed SCRIPT ENGINE at 19:12, 8.52s elapsed
Host 192.168.15.10 appears to be up... good.
Interesting ports on 192.168.15.10:
Not shown: 1706 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp
23/tcp open telnet VxWorks telnetd
80/tcp open http?
|_ HTML title: Site doesn't have a title.
111/tcp open rpcbind 2 (rpc #100000)
502/tcp open asa-appl-proto?
2 services unrecognized despite returning data
```

Linux 2.4 ve 2.6 çekirdek sürümlerinden bu yana çekirdek seviyesindeki (kernelspace) *netfilter* ile kullanıcı seviyesindeki (userspace) *iptables* programları birlikte çalışmaktadır.

Netfilter, tanımlı tüm kural setlerine sırasıyla baktıktan sonra nihai olarak üç fonksiyonu çalıştırır. Bunlar; izin ver (permit), düşür (drop) ve değiştir (modify) işlemleridir. Tipik olarak bu işlemlerde 3. katman (IP katmanı) ve 4. katman (TCP katmanı) paket başlıklarına bakılarak karar verilir.

Netfilter, farklı filtreleme işlevlerine sahip zengin ve iyi belgelendirilmiş API sağlamaktadır. Parametre gerektirmeyen netfilter modülleri için, kullanıcı alanında olan *iptables* tarafında herhangi bir değişiklik yapmaya ihtiyaç yoktur. Ancak ilave edilecek bir modül, kullanıcı alanında parametre alacaksa, doğal olarak *iptables* tablo yapısına Tablo 4'deki ilavelerin yapılması gerekecektir [16].

Bu çalışma kapsamında, Linux işletim sistemi üzerine kurulu olan *iptables* güvenlik duvarına, açık kaynaklı bir proje olan *ModbusFW* projesindeki *libipt_modbus.c* modülü eklenerek tablo yapısı genişletilmiştir. Tabloya sonradan ilave edilen başlık bilgileri Tablo 4'deki gibi tanımlanmıştır.

Tablo 4. iptables'a ilave edilen yeni başlıklar (New header adding to iptalbes) [16]

```
struct modbus_tcp
{
    struct modbus_hdr
    {
    __u16 transaction_id;
    __u16 protocol_id;
    __u16 length;
    }modbus_h;

    struct modbus_data
    {
    __u8 unit_id;
    __u8 func_code;
    __u16 ref_num;
    __u16 word_cnt;
    __u8 byte_cnt;
    }modbus_d;
};
```

Artık *iptables* komutlarıyla alınan veriler, Tablo 4'e yazılacak ve Modbus protokol başlıklarına atanan değerler *netfilter* tarafından okunabilecek hale gelecektir.

5.2. Modbus-Netfilter/Iptables Yapılandırması
(Modbus-Netfilter/Iptables Configuration)

Şekil 2'de Modbus sunucu ve istemcinin herhangi bir kısıtlamaya tabi tutulmaksızın her türlü talep-cevap mekanizmasını işletebildiği gösterilmiştir. Şekil 7'de ise, istemci ve sunucu birimler arasına çift ethernet kartına sahip olan Linux işletim sistemi ve her iki ethernet kartından geçen ağ trafiğini denetleyen Modbus-Netfilter/Iptables güvenlik duvarı görülmektedir.

Aşağıda örnek bir Modbus-Netfilter/Iptables yapılandırılması birkaç adımda anlatılmıştır. İlk olarak, *Modbus Güvenlik Duvarı* bir IP paket geçidi (router) olarak çalışması sağlanmalıdır. Bu, bir ethernet kartına gelen paketin diğer ethernet üzerinden başka bir ağa aktarımına imkan sağlanmasıyla gerçekleştirilir. Bunun için Linux ortamında, farklı ethernet kartlarına farklı subnetlerde IP adresleri verilir ve IP iletme (IP forwading) seçeneğini aktif hale getirilir.

Modicon TSX (Modbus Sunucunun) güvenlik duvarına bağlı olduğu *eth0* ethernet arayüzüne, Modicon

Şekil 7. Örnek Modbus-Netfilter/Iptables Yapılandırması (Modbus-Netfilter/Iptables configuration example)

TSX ile aynı subnette olan 192.168.15.11 IP adresi verilir.

ifconfig eth0 192.168.15.11

Güvenlik duvarının ikinci bacağına ise ona doğrudan bağlı olan Modbus İstemci ile aynı subnetten olan 192.168.20.51 IP adresi verilir.

ifconfig eth1 192.168.20.51

Artık her iki ethernet için paket iletim özelliğini aktif edilerek yapılandırmanın ilk basamağı sonlandırılır.

echo "1" /proc/sys/net/ipv4/ip_forward

İkinci adım olarak, iptables güvenlik duvarının genel filtre tanımları girmeye başlanır. Örneğin Modbus sunucudan istemciye doğru ICMP paketlerinin (ping paketleri) gönderimine izin vermek için:

iptables -A FORWARD -p icmp -j allow

ifadesi komut satırına girilir. Bir başka örnek olarak, Modbus istemcinin, Modbus sunucunun WEB yönetim arayüzüne erişimini engellemek için:

iptables -A FORWARD -p tcp --dport 80 -j ACCEPT
ifadesi komut satırına girilir.

Üçüncü ve son adım olarak, artık güvenlik duvarının Modbus fonksiyon kodları seviyesinde erişim kontrolü yapan tanımları girilmeye başlanır.

Aşağıdaki örnekte de verildiği gibi Modbus istemcinin Modbus sunucu üzerinde fonksiyon kodu 1 olan servisinin çalıştırmasına izin verilir.

iptables -A FORWARD -p tcp -m modbus --funccode 1 --allowtcp 1 -j ACCEPT

Son örnekte ise güvenlik duvarının Modbus fonksiyon kodu 16 olan servisi (çoklu kayıtçıya yazma fonksiyonu) haricindeki hiçbir servise izin vermemesini sağlar.

iptables -A INPUT -p tcp -m modbus --funccode !16 –allowtcp 1 -j DROP

Yukarıda verilen örnekler sisteme uygulanırsa; Şekil 6'da verilen yetkisiz erişim engellenebilecek, sadece önceden tanımlı Modbus fonksiyon kodları çalıştırılabilecek ve endüstriyel güvenlik açığı riskleri ortadan kaldırılabilecektir.

6. SONUÇ VE DEĞERLENDİRME (RESULTS AND CONCLUSIONS)

Bu çalışmada, Gazi Üniversitesi Teknik Eğitim Fakültesi Elektrik Eğitimi Bölümü kurulan ve 50 kW güce sahip Enerji Dağıtım Sistemine ait elektriksel parametreleri görüntüleyen ve saklayan enerjisi izleme sistemi, haberleşme ve işletim güvenliği açısından incelenmiş, potansiyel sistem güvenlik açıkları tespit edilmiş, iyileştirilmelerin nerelerde ve nasıl yapılması gerektiği adım adım gösterilmiş ve alınması gereken önlemler sıralanmıştır.

Enerji otomasyon sistemlerinde bir endüstri standardı olarak kullanılan Modbus protokolü ve bu protokolün sahip olduğu fonksiyon kodları, haberleşme mesaj başlıkları bu çalışmada ayrıntılı olarak incelenmiştir. Ayıca, izlenebilir elektrik enerjisi dağıtım sisteminde kullanılan Modbus istemci ve sunucu birimleri arasındaki haberleşme kanalı çoklanarak, mesajlaşma paketleri harici bir bilgisayarca toplanmış ve analiz edilmiştir. Böylece, herhangi bir şifreleme, kimlik doğrulama mekanizması kullanmayan Modbus protokolüne yetkisizce erişilebileceği, şifresiz gönderilen paketlerin kolaylıkla çözümlenebileceği, hatta yetkisiz bilgisayarın kendisi iletişimin bir tarafı gibi gösterip Modbus mesaj içeriğini rahatlıkla değiştirebileceği görülmüştür.

Bu açıklıkların kapatılması için, uygulama sistemindeki Modbus istemci ile sunucu arasına yerleştirilmek üzere, açık kaynak kodlu *netfilter - iptables* güvenlik duvarı ile Modbus güvenlik modülü projesi olan *modusfw* entegre edilmiş ve Linux işletim sistemine sahip çift ethernet kartlı bir bilgisayar üzerinde koşturulmuştur. Böylece, istemci ile sunucu arasındaki iletişim IP ve MAC adresleri seviyesinde yetkilendirilmiş ve Modbus fonksiyon kodları seviyesinde filtrelenmiştir.

Daha yüksek seviyede bilgi güvenliğinin sağlanmasına yönelik olarak, Modicon TSX üzerinde yazılım geliştirme çalışmaları planlanmış fakat *VxWorks* gömülü işletim sistemi için programlama, derleme ve ekleme işlemlerine ilişkin yeterli dokümantasyon temin edilememiştir. Bu konularda farklı çözüm önerilerinin geliştirilmesine ihtiyaç olduğundan endüstriyel sistem üreticilerin bu konuya daha fazla önem vermeleri faydalı olacaktır.

Son olarak sunulan bu çalışmanın; ülkemizde üzerinde fazlaca çalışma yapılmayan endüstriyel sistemlerin bilgi güvenliğinin sağlanması konularında katkılar sağlayacağı değerlendirilmektedir.

KAYNAKLAR (REFERENCES)

1. Bio, M. J. ve diğerleri, **IEEE Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security**, IEEE Power Engineering Society, New York, 2000.
2. McDonald, J.D., "Developing and Defining Basic SCADA System Concepts",**37th Annual Rural Electric Power Conference**, Kansas City, Missouri, No B3, 1-5, 25-27 April 1993.
3. Amanullah, M., Kalam, A., Zayegh, A., "Network Security Vulnerabilities in SCADA and EMS", **Transmission and Distribution Conference and Exhibition Asia and Pacific**, Dalian, China, 1–6, 15-17 August 2005.
4. Hellerstein, J. L., Diao, Y., Parekh, S., Tilbury, D. M., "Control Engineering for Computing Systems", **IEEE Control Systems Magazine**, 25(6), 56-68, 2005.
5. Ralston, P.A.S., Graham, J.H.ve Hieb, J. L., "Cyber Security Risk Assessment for SCADA and DCS Networks", **ISA Transactions**, 46(4), 583-594, October 2007.
6. Kropp, T., "System Threats and Vulnerabilities", **Power and Energy Magazine**, 4(2), 46–50, 2006.
7. Watts, D., "Security & Vulnerability in Electric Power Systems", **35th North American Power Symposium,** University of Missouri-Rolla, Missouri, 559–662, 19-21October 2003.
8. Tanenbaum, A., Herder, J. ve Bos, H., "Can We Make Operating Systems Reliable And Secure", **IEEE Computer**, 39(5), 44-51, 2006.
9. Qizhi, C., Qinquan, Q., "The research of UNIX platform for SCADA", **IEEE Power Engineering Society Winter Meeting**, Singapore, Cilt 3, 2041-2045, 23-27 January 2000.
10. Bayındır, R., Irmak, E., Çolak, İ., Bektaş, A., "Development of a Real Time Energy Monitoring Platform", **Electrical Power and Energy Systems**, submitted paper, 2008.
11. Bayındır, R., Demirbaş, Ş., Bektaş, A., Çolak, İ.,"Bir Endüstriyel İşletmede Elektrik Enerjisinin İzlenmesi", **Erciyes Üniversitesi, Fen Bilimleri Enstitüsü Dergisi**, 24(1-2), 154-164, 2008.
12. Bektaş, A., Çolak, İ. ve Bayındır, R. "Asenkron Motorun Korunmasına ilişkin PLC Tabanlı Bir Uygulama", **Politeknik Dergisi**, 10(2), 117-121, 2007.
13. Xu, S., Pan, H., Ren, J. ve Su, J., "Design of the Modbus Communication through Serial Port in QNX Operation System", **ISECS International Colloquium on Computing Communication Control and Management**, Guangzhou City, China, 434–438, 3-4 August 2008.
14. Peng, D., Zhang, H.,Yang, L. ve Li, H., "Design and Realization of Modbus Protocol Based on Embedded Linux System" **International Conference on Embedded Software and Systems Symposia 2008, ICESS Symposia 08**, 275–280, Chengdu, China, 29-31 July 2008.
15. **Modbus Application Protocol Specification**, Version 1.1, December 2002. http://www.modbus.org
16. **ModbusFW Açık Kaynak Kodlu Modbus Güvenlik Duvarı Modül Geliştirme Projesi**, 2004. http://modbusfw.sourceforge.net.