SCADA Güvenliği ve Saldırı Vektörleri

SCADA Security and Attack Vectors

Mustafa Pişirici
İstanbul Ünivesitesi-Cerrahpaşa
mustafa.pisirici@ogr.iu.edu.tr

Ebu Yusuf GÜVEN
İstanbul Ünivesitesi-Cerrahpaşa
eyguven @istanbul.edu.tr

Mehmet Yavuz YAĞCI
İstanbul Ünivesitesi-Cerrahpaşa
myy@istanbul.edu.tr

Muhammed Ali AYDIN
İstanbul Ünivesitesi-Cerrahpaşa
aydinali@istanbul.edu.tr

***Özetçe*— SCADA 20. Yüzyıl teknolojisinde özellikle endüstriyel sektöründe denetleme, kontrol etme, veri toplamak için büyük bir önem taşımaktadır. Hayati bir öneme sahip olan bu sistemin güvenlik zafiyetleri de bulunmaktadır. SCADA sistemlerinin fiziksel, yazılımsal, mimari gibi SCADA'nın birçok karakteristik sorunu bulunmaktadır. Litaretürde bulunan birçok çalışmada SCADA sistemlerinin karakterislik özelliklerine değinilmiştir. Bu makalede SCADA'nın birçok farklı sorunu toplanmıştır. Ayrıca SCADA'ya yapılan saldırı çeşitleri, fiziksel ve yazılımsal açıklarına kullanıcıların sebep olduğu zafiyetler üzerinde durulmuştur. Bu çalışmada SCADA'ya yapılan birçok atak çeşitleri, sistemi kontrol eden makinelerin güvenliği, yazılımsal, fiziksel eksiklikleri ve kullanıcı hatasından kaynaklanabilecek açıklar gibi büyük yıkımlara sebep olabilecek ve devletlerin birbiri arasında siber silah olarak kullanabileceği güvenlik konuları incelenmiştir.**

Anahtar Kelimeler — SCADA; Güvenlik; Siber Saldırılar Kritik altyapı

Abstract— SCADA is of great importance in 20th century technology, especially in the industrial sector for controlling, controlling and collecting data. This vital system has security vulnerabilities. SCADA systems have many characteristic problems of SCADA, such as physical, software, and architecture. In many studies in the literature, the characteristics of SCADA systems have been mentioned. In this article, many different problems of SCADA have been collected. In addition, the types of attacks on SCADA and the vulnerabilities caused by the users of physical and software vulnerabilities were emphasized. In this study, many types of attacks to SCADA, security of the machines controlling the system, software, physical deficiencies and vulnerabilities that can be caused by user error can be caused and the security issues that can be used as a cyber weapon between the states are examined.

Keywords — SCADA, Security; Cyber Attack; Critical infrastructure

I. GİRİŞ

SCADA (Supervisory Control And Data Acquisition - Merkezi Denetleme Kontrol ve Veri Toplama) sistemi hidroelektrik, nükleer güç üretimi, doğalgaz üretimi gibi birçok endüstriyel sistemde işletilmesinde, kilometrelerce uzunluktaki elektrik aktarım hatlarını açma kapama düğmelerinin kontrolü ve hatlardaki ani yük değişimlerinin dengelenmesi gibi çok farklı alanlarda kullanabilir. Mekanik ve elektronik aygıtların birbirine bağlanılabilir. Alınan veriler SCADA sistemine iletilebilir. Bu sisteme iletilen bilgilerle analiz yapılabilir. SCADA'ya verilen komutlarla sisteme komut gönderilebilir. Endüstriyel sistemde insanlar yetersiz kalabilir. Verilerin toplanmasında ve hızlı bir müdahale için SCADA sistemlerine ihtiyaç duyulabilir fakat bu sistemlerinin güvenliği hakkında endişe edici durumlar mevcuttur. Bu nedenle SCADA sistemleri art niyetli kişiler tarafından kullanılırsa devletler arası savaşlara sebep olabilecek potansiyele sahiptir.

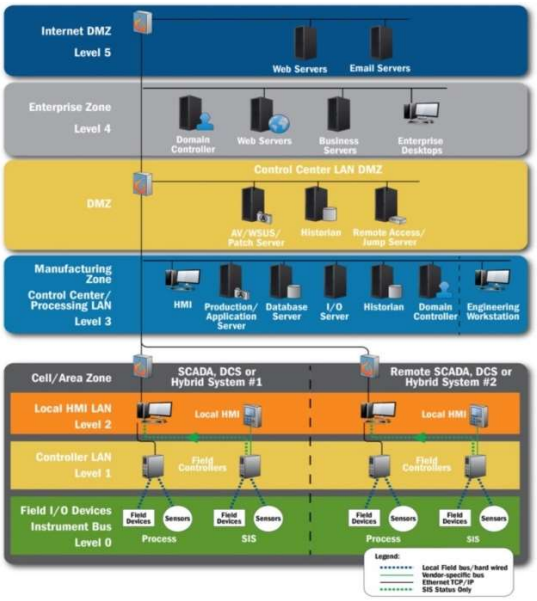
Malware atakları, MITM Saldırısı, Network Saldırıları kullanıcı kaynaklı hatalar, TCP/IP protokolünün tamamıyla güvenli olmaması, ICS (Endüstriyel Kontrol Sistemleri) zafiyetleri, katmanlı ağ sebebiyle ağ karmaşıklığı, Modbus atakları gibi birçok saldırı, zafiyet bulunmaktadır [1,2,3,6,7].

SCADA güvenliği birçok akademi çalışmasına konu olmuş ve birçok farklı durum hakkında akademik makaleler yazılmıştır.

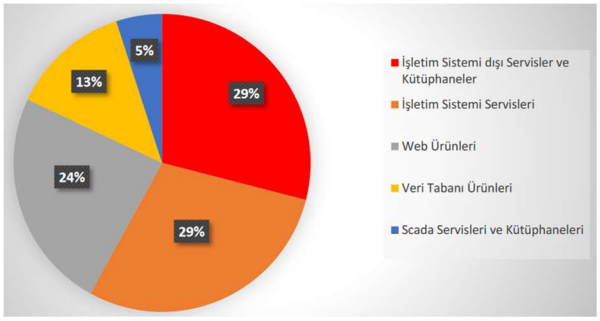
Bu makalede SCADA sistemlerinin çeşitli zafiyet oluşturabilecek durumları yazılmıştır. Bu zafiyetlerin önemi vurgulanmıştır.

SCADA sistemleri 21.yüzyılda kullanılan endüstriyel sistemlerinde önemli bir faktör olduğu için son zamanlarda SCADA güvenliği önemli bir hale gelinmiştir. Bu nedenle birçok akademik çalışmalarda konu olmuş ve testler yapılmış olup makaleler yazılmıştır. Bu makalede atak çeşitleri, zafiyetler toplanmıştır.

SCADA güvenliği özellikle 21. Yüzyılda önemi giderek artmıştır.1990 yılında kişisel bilgisayar ağ ortamında endüstriyel sistemlerde kullanılması ile birçok zafiyet ortaya çıkmıştır. Bu çalışmadaki amaç çeşitli SCADA ataklarını ve zafiyetlerini anlatmaktır. **Şekil-1**'de SCADA genel bir ağ mimarisi gösterilmiştir.



Şekil. 1. Genel SCADA Ağ Mimarisi [8]



Şekil. 2. SCADA Sistemlerinde Yamasız Bileşenlerin yüzdesi [9]

Yukarıdaki grafikte SCADA sistemlerinin temel hangi bileşenlerden oluştuğu gösterilmiştir.

II. ARKA PLAN

Bu çalışmada SCADA güvenliği hakkında yapılan çalışmalar incelenmiştir. SCADA hakkında yapılan saldırı çeşitleri, SCADA sistemlerinin zafiyet oluşturan veya oluşturma ihtimali bulunan durumları bir araya toplanmasına çalışılmıştır. Toplanan bu bilgilerin fiziki, yazılımsal, kullanıcı tarafından oluşturulan durumlar, saldırı çeşitleri, makine zafiyetleri, sosyal mühendislik gibi sınıflandırma yapılarak genel olarak SCADA güvenliği ve terminolojisi hakkında bilgi sunulmaktır. Araştırmalarda fazlaca bahsedilen konuların üzerinde durulmuş ayrıca zafiyet oluşturabilecek durumlara da yer vermeye çalışılmıştır.

III. LİTERATÜR ÖZETİ

SCADA sistemlerinin denetleme, veri analizi, kontrol gibi birçok yenilik getirmesi endüstriyel sistemlerde yeni bir çağ açmıştır [10]. Fakat farklı sebeplerle birçok sıkıntılarda oluşturmuştur [4]. Kullanıcı hatalarından kaynaklı hatalar, makinelerin başta güvenlik kaygısı olmadan yapılması protokollerin güvenli olmaması gibi sorunlar oluşmuştur [1][3][6]. SCADA sistemin uzaktan kontrol için yapılan ağa bağlanması doğal olarak bir zafiyet oluşturmuştur [8]. Birçok saldırı çeşidi denen SCADA sistemlerinde bazı düşündürücü sonuçlar alınmıştır [12][13]. Basit görünen durumlarda bile sıkıntılar oluştuğu görülen SCADA da hayati önlemler alınması gerekmektedir [5]. Birçok yapılan SCADA saldırılarında bu olay açıkça görülmektedir [1][2][3][7]. Yapılan kullanıcı kaynaklı hatalar dahi SCADA sistemlerine büyük zarar verebilmektedir [3][4].

IV. SCADA

SCADA sahada dağıtılmış bileşenlerin dijital ortama taşınmasını sağlar. SCADA verilerin uzaktan kontrol edilmesini yönetilmesini sağlar. SCADA sistemlerinde operatörün sistemde beklemesine gerek kalmaz uzaktan yönetilebilir. SCADA sistemi aşağıdaki fonksiyonları rahatlıklar sağlanmaktadır:

- Veri Toplama
- Denetleyici Kontrol
- Alarm işleme
- Bilgilendirme Raporları
- Veri Hesaplama
- Disk Bilgileri ve Raporları

V. SCADA GÜVENLİĞİ

Kritik altyapılarda kullanılan SCADA sistemlerinde birçok atak çeşitli veya zafiyet bulunabilmektedir. Ancak bu SCADA sistemleri genellikle kapalı devre sistemler olması nedeniyle saldırıların uzaktan gerçekleşmesi zor saldırılar arasındadır. Ancak son dönemde gelişen dağıtık SCADA sistemleri güvenlik mimarisi iyi düşünülmeyen sistemlerde zafiyetlere neden olmaktadır. Bu zafiyetleri fiziksel ve yazılımsal zafiyetler olarak iki başlıkta incelenmiştir.

A. Fiziksel Zafiyetler

SCADA kapalı devre çalışan internete kapalı sistemlerde yapılan saldırıları uzaktan yazılımsal olarak gerçekleştirmek mümkün değildir. Fiziksel güvenliği sağlanamayan sistemlerin yazılımsal olarak güvenliğini sağlamak oldukça zordur. Kapalı devre sistemlere yazılımsal saldırıların bile gerçekleştirilebilmesi için fiziksel sızma işlemi gerektirmektedir. Güvenli cihaza bağlaman bir usb bellek ya da güvenli ağa bağlanan saldırgan cihazı ile yazılımsal saldırıların yapılması mümkündür. Bunların dışında cihazları ve sensörleri fiziksel olarak yanıltarak da saldırı yapılabileceği unutulmamalıdır. Yangın sensörlerinin tetiklenerek yangın söndürme sistemlerinin devreye alınması da fiziksel bid saldırı olarak değerlendirilebilir. Kritik sistemlerde bütünsel güvenlik anlayışı ile risklerin yönetilmesi mümkündür. Ancak fiziksel saldırıların da kritik altyapılarda ciddi hayati ve maddi tehlikelere neden olabileceği unutulmamalı ve fiziksel güvenlik yazılımsal güvenlikten temel seviye olarak belirlenmelidir.

Kullanılması gerekmeyen portların kapatılması ya da sökülmesi, servis pinlerinin kesilmesi alabilecek bir dizi önleme örnek olabilir.

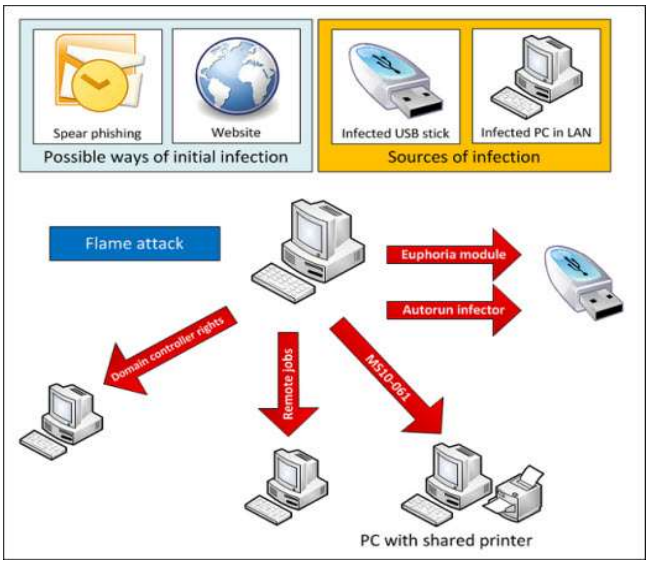
B. Yazılımsal Zafiyetler

SCADA sisteminde yaygın olarak kullanılan ticari işletim sistemleri sistemlerinden olan Windows ve Unix sistemleri kullanılmaktadır. Bu sistemlerin ortalama ömrü 20 ila 30 yıl arasındadır. Güncelleme yapılamaması ve sistemin kapatılamayacak olması sebebiyle kişisel bilgisayarlarda zafiyetler oluşmaya başlar.

VI. SALDIRI ÇEŞİTLERİ

A. Malware (Zararlı yazılım) Saldırıları

Malware Saldırıları bilgisayar ve mobil cihazların işlevlerini bozmak, kritik bilgileri toplamak, özel bilgisayar sistemlerine erişim sağlamak ve istenmeyen reklamları göstermek amacı ile kullanılan yazılımdır. Kötü amaçlı yazılım SCADA sistemleri için ciddi bir tehdit oluşturmaktadır.BT ve iletişim sistemi taramasında bulunan güvenlik açıkları virüsler ve kötü amaçlı yazılımlar tarafından kullanılabilir. Birçok şekilde malware atak yapılabilir. Şekil 3 de çeşitleri gösterilmiştir.



Şekil. 3.Flame enfeksiyon çeşitleri [12][13]



Şekil. 4. Flame tarafından hedeflenen ilk 7 ülke[12][13]

B. Network Saldırıları

İletişim protokolü saldırıları SCADA İletişimi için kullanılan yüzlerce iletişim protokolü vardır. DNP3 protokolüne DOS (Denial Of Service) saldırısı modelleme sağlanarak basit bir DOS saldırısı, veri toplayıcıdaki olay arabelleğini doldurmaktadır. Böylece meşru aygıtlardan gelen kritik uyarılar, kontrol istasyonunun durumsal farkındalığını etkileyen arabelleğe alınamaz

C. MITM (Ortadaki Adam) Saldırıları

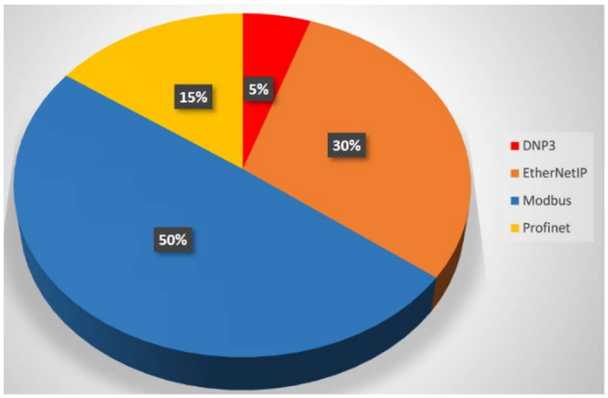
Bu, uygulanması ve başlatılması kolay olduğu için en iyi çalışılan saldırı türü olmuştur. Kötü niyetli bir aracı protokol sömürü yoluyla belirli bir cihaz sömürülebilir. Kablosuz paketlerin kullanımı kolay olabilir çünkü saldırgan ağ trafiğine erişmek için ağa (kablolu gibi) fiziksel olarak bağlı olmak zorunda kalmayabilir.

D. Bütünlük Saldırıları

Bir saldırgan, sensörlere ve/veya aktüerlere erişebilir ve yazılımı, tarafından bildirilen koordineli bir saldırı başlatmak için değiştirebilir. Sensör veya kontrol sinyallerinin manipüle edildiği veri bütünlüğü saldırıları, operatörün yanlış eylemler yapması için yanlış yönlendirilebileceğinden ciddi sonuçlar doğurabilir. Bu saldırıların başlangıcı DOS saldırıları kadar açık olmadığı için üstesinden gelmek daha zordur.

E. Protokol Saldırıları

Haberleşme protokolü mesaj yapısını tanımlar. Şekil 5 da görüldüğü üzere birçok protokol çeşidi vardır. Modbus Protokolü de bu protokollerden biridir. Modbus Protokolü sniffer ve mesaj kullanımını gerektirir. Jeneratör, ana cihaza bağlantı ile birlikte veya seri iletişim bağlantısı gerekmektedir.



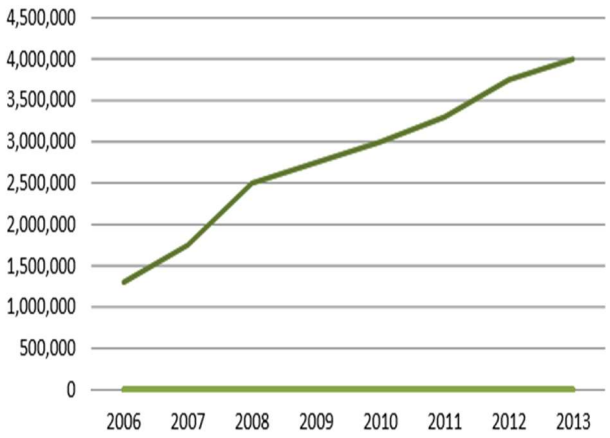
Şekil. 5.SCADA da kullanılan protokoller [9]

F. Kullanıcı Kaynaklı Zafiyetler

Sadece kullanıcı bazlı hatalar da zafiyet oluşumuna sebep olunuyor. SCADA sistemlerinde katmanlı ağ kullanılır. Kullanıcı yanlışlıkla diğer ağa bağlanıp sistemi savunmasız hale getirilmesine sebep oluyor. Güncelleme gibi olayları kullanıcı bilinçsiz bir şekilde uygulandığı zaman sistemin kapanmasına ve büyük maddi manevi zararlara sebep olabilir.

G. PLC Saldırıları

Endüstriyel kontrol sistemi (ICS) ağlarında uygulanan doğal olarak güvensiz protokollerin dağıtımı, benzeri görülmemiş bir oranda artmaktadır. Bunun nedeni, esas olarak performans, esneklik ve ürün özelliği isteklerinin genellikle güvenlik konusunda öncelik alması gerçeğidir. ICS bileşeni olan PLC'ler, evlerimize, işletmelere ve fabrikalara akan elektriği koruyan çok sayıda görevi otomatikleştirmeye yardımcı olur. Yaşam tarzımız için çok hayati ve önemli görünen bir şey için, PLC satıcıları ürünlerini tasarlarken güvenlik hususlarının bu kadar tamamen göz ardı edileceği düşünülemez görünüyor. Güncelleme ve bazı durumlarda, bu cihazların değiştirilmesi, canlı dağıtımlarda bunları kullanan kuruluşların çoğu için önemsiz bir görev olmasa da geri adım atmak ve yeni standartları uygulamak ve güvenliği en öncelikli hale getirmek için yolları yeniden değerlendirmek için çok geç değildir. Örneğin 2011 yılında Siemens makinelerinde yapılan çalışmalarda Siemens SIMATIC S7 PLC'ler, Ethernet'e dayanan ve birçok kişi tarafından şu anda kullanımda olan en güvenilir Fieldbus standardı olarak kabul edilen PROFINET'İ kullanmaktadır. Siemens'in PROFINET'İ neden kullandığı açık olsa da bu ürünlerin başlangıçta tasarlandığı zaman güvenliğin hesaba katılmadığı talihsiz bir durumdur. Wireshark, Ethernet mesaj çerçevelerinin analizine izin verecek PROFINET kaydını desteklemektedir. SIMATIC TIA ve Step 7 mühendislik yazılımı, yönetim için ISO-TSAP protokolüne güveniyor. Bu, Siemens tarafından yapılan tüm S7 Programlanabilir mantık denetleyicileriyle iletişim kurmak ve programlamak için standart protokoldür.



Şekil. 6.PROFİNET Düğümlerinin kullanımı 2013 yılına kadar [6]

VII. SONUÇ

SCADA sistemleri endüstriyel alanda etkili bir sistemdir. Lakin sistem güvenlik tarafında birçok zafiyet barındırmaktadır. Burada biraz genel olarak SCADA zafiyetlerin çeşitlilikleri anlatılmıştır. SCADA sistemlerinin zafiyeti için araştırma yapmak isteyen kişilere ufuk açıcı olmaya çalışılmıştır. Bu alanın önemi vurgulanmış olunup ihmal edilmemesi gereken bir husus olduğu değinilmiştir. Ülkelerin milli güvenlik meselesi haline gelmesi gerekmektedir. Aksi halde ülkelerin büyük bir güvenlik açığına sebep olabileceği ve askeri operasyonlardan daha ucuz bir yöntemle birçok ülkenin endüstriyel sistemine etki edebileceği ve büyük zararlara uğratabilecektir. Bu zararlar hem maddi olarak hem de manevi anlamda ülkelere zarar verebilmektedir. Bu kadar avantajlı olan SCADA sistemleri belirtilen olumsuz yıkımları önlemek için zafiyetleri belirlemek, önlem almaya çalışmak ve güvenlik altyapısını geliştirmek önemlidir.

BİLGİLENDİRME

Bu çalışma İstanbul Kalkınma Ajansı tarafından desteklenen Nesnelerin İnterneti Güvenlik Test ve Değerlendirme Merkezi araştırmacıları tarafından hazırlanmıştır.

KAYNAKLAR

[1] Peter Huitsing, Rodrigo Chandia, Mauricio Papa, Sujeet Shenoi, Attack taxonomies for the Modbus protocols, 800 S. Tucker Drive, Tulsa, OK 74104, USA

[2] Sarah Feldman, IT Says SCADA Will Continue to Be a Frequent Threat Mar 6, 2019

[3] Mo Y, Chabukswar R, Sinopoli B. Detecting integrity attacks on SCADA systems. IEEETrans Contr SystTechnol 2014;22(4):1396–407.

[4] Brent Monterey, The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010Kesler, California.

[5] Sajid Nazir, Shushma Patel, Dilip Patel, Assessing and augmenting SCADA cyber security: A survey of techniques School of Engineering, London South Bank University, London SE1 0AA, UK b Firstco Ltd., London W2 6EU, UK

[6] Dillon Beresford, Exploiting Siemens Simatic S7 PLCs Prepared for Black Hat USA+2011 July 8, 2011

[7] Eric Byres, Flame Malware and SCADA Security: What are the Impacts? 2012-05-29

[8] Halil Öztürkçi, URL:http://halilozturkci.com/eks-scada-sistemlerinde-antivirus-guncellemeleri [Erişim zamanı;Eylül,30,2019]

[9] Ismail Erkekyüksek, Modbus Temelli Scada Sistemlerinin Siber Güvenliği Için Yeni Bir Yaklaşim Lisans Tezibilgi Güvenliği Mühendisliği Anabilim Daligazi Üniversitesi Fen Bilimleri Enstitüsü Ocak 2018

[10] Iveta Zolotová, Lenka Landryová, SCADA/HMI Systems and Emerging Technologies, IFAC Proceedings Volumes, Volume 33, Issue 1, 2000, Pages 17-20

[11] Blickey,G,.(1985)SCADASystemsAffectedbyDistributedControl.ControlEngineering,March1985, pp.79-81

[12] Securelist, URL: https://securelist.com/the-flame-questions-and-answers 51/34344/ [Erişim zamanı; Eylül, 30, 2019]

[13] Tofinosecurit, URL: https://www.tofinosecurity.com/blog/flame-malware-and-scada-security-what-are-impacts [Erişim zamanı; Eylül, 30, 2019]