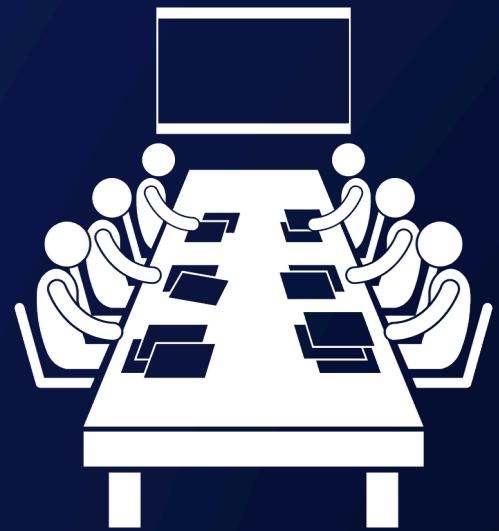


ASYNC 10

Güvenli Sarj, Güvenli Yolculuk





TOPLANTI NOTLARI



Toplantı

de
udem
emih
ur
erif
sena
guzhan
velanur

Toplantıya Katılım
non toplam yük

CUMARTESİ

SWOT Analizi (Her Kişi en az 1 tone)

Anomali Raporu (Simülasyon üzerinde) nasıl çalışacağı
↳ Her Kişi 1'er tone Grupla var.
En iyisı seçilebilir.

Puanlama listesi oluşturulum. (Excel)

Slayt içeriğini oluşturulum.
- Problemler
- Anomalleri
- Kullanılacak Teknoloji
- İzlenenek Standartları.

1 Kasım Cumartesi

İstekler

Sena
Südem
Sude
Uşur
Enes
Seda
İbrahim
Semih
Düzgün
Düşhan

Github Klasör Yapısı

- Anomaliler
 - Kendi ismin
 - Hafta 1
 - ⋮
- Simülasyon
 - Kendi ismin
 - Hafta 1
- Swotlar
 - Kendi ismin
 - Hafta 1
- Logo, slogan, linkedin
- Github

Seçilen

projenin
molasını → Makalenin
bul.
incele

Makalenin
SWOT → Kendi proje
(anomali) → Github'a
yüklemeye
detayları

3 Kasım Pazarı

İstekler

Semih
Sela
Güthon
Düzgün
Sude
Sudem
Erif
Uşur
Sena
İbrahim

Sınav Çözümü

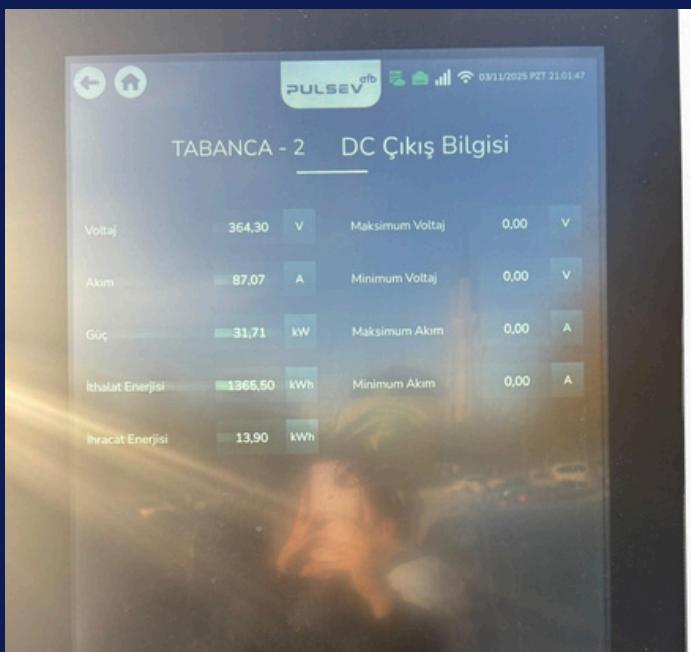
Sena
Semih
Sela
Sudem
Sude
Sudem
Erif
Uşur
Sena
İbrahim

→ Simülasyon Çalışması
→ Google Sheets'e ekleyelim

TOPLANTI FOTOĞRAFLARIMIZ



ŞARJ İSTASYONU İNCELEME FOTOĞRAFLARIMIZ



incelediğimiz EVSE
My Charge

EKİP DİZİNİMİZ

<https://drive.google.com/drive/folders/1OEBfGbOYEHpot2-dG808dLnjQzYaQdvk>



Drive

Drive'da arayın

+ Yeni

Ana sayfa Etkinlik Çalışma alanları Drive'im Benimle paylaşılanlar En son Yıldızlı Spam Çöp kutusu Depolama alanı 12,29 GB kullanılıyor

Benimle paylaşılanlar > Async10

Tür Kullanıcılar Değiştirilme: Kaynak

Adı ↑

Adı	Sahibi	Değiştirilme tarihi	Dosya boyutu	Sıralama
AKILLI ŞARJ PROFİLİ MANİPÜLASYONU.pdf	ben	2 Kas ben	514 KB	⋮
Anomaly_Raporu_SemihTEPE.pdf.pdf	semihtepe09	2 Kas	108 KB	⋮
developerguide.odt	ben	13:59 ben	317 KB	⋮
EV_Şarj_Siber_Güvenlik_Ağ_Geçidi.pdf	ben	13:58 ben	13,3 MB	⋮
GenelBilgi.odt	ben	24 Kas ben	35 KB	⋮
Man-in-the-Middle Saldırılarına Karşı Korunma Swot Analizi.docx	ben	2 Kas ben	16 KB	⋮
OCPP MitM ile Yetkilendirme Değişikliği Anomali Senaryosu.docx	ben	29 Eki ben	531 KB	⋮
OCPPSchemaDrift_AnomaliSenaryosu.docx	selanurayaz0@gmail.com	1 Kas	18 KB	⋮
Örnek Anomali Firmware_Update_Injection.docx	OĞUZHAN ERDOĞAN	1 Kas OĞUZHAN ERDOĞAN	21 KB	⋮
Örnek Anomali Time_Drift_Explotation.docx	OĞUZHAN ERDOĞAN	1 Kas OĞUZHAN ERDOĞAN	21 KB	⋮
Proje Özeti	enesmalik1245	2 Kas	6 KB	⋮
ProjeyeGenelBakış.odt	ben	07:41 ben	82 KB	⋮
RAPOR: ANOMALİ SENARYOSU 1	ozgundenizsevilmis	1 Kas	8 KB	⋮
RAPOR: ANOMALİ SENARYOSU 2	ozgundenizsevilmis	18 Eki	5 KB	⋮
SWOT Analizi (EmuOCPP).docx	OĞUZHAN ERDOĞAN	4 Kas OĞUZHAN ERDOĞAN	21 KB	⋮
SWOT ANALİZİ: Elektrikli Araç Şarj İstasyonlarında Güvenlik	ozgundenizsevilmis	18 Eki	5 KB	⋮
UgurBerkatas.pdf	ÜĞUR BERKTAŞ	1 Kas ÜĞUR BERKTAŞ	108 KB	⋮
UgurBerkatasSWOT.pdf	ÜĞUR BERKTAŞ	1 Kas ÜĞUR BERKTAŞ	49 KB	⋮



GÖREV DAĞILIMLARI VE ZAMAN ÇİZELGEMİZ

görev dağılımı 000

Yapılacaklar

- Haftalık toplantıların raporu
- Anomali senaryolarının alfa sürümüne (güncelsimülasyonumuz branchi) entegrasyonu.
- ML model eğitiminin sisteme entegre edilmesi
- Tüm sistemin uçtan uca entegrasyon testlerinin tamamlanması
- Dokümantasyonun final teslim formatına getirilmesi

Yapılıyor

- hocanın attığı tüm videoları izleme
- Oluşturulacak simülasyon ortamı ile ilgili araştırma yapma ve şahsi anomali senaryoları için simülasyonda olması gereken ek bileşen ve konfigürasyon/parametre varyasyonlarını raporlama.
- bulunan makalenin swot analizi
- anomali senaryoları ve swot analizlerini githuba ekleme

Tamamlandı

- anomali senaryosu raporu
- bulunun anomali ile ilgili makale bulma.
- bulunan makalenin swot analizi

Kişi bazlı görevler

- Her toplantının özetini ve katılımcıları tutma
- Şarj istasyonlarının yazılımsal güvenlik açıklarının fiziksel yolla nasıl önünün açıldığına araştırması
- Farklı simülasyon ortamları, araçları ve uygulamalar hakkında araştırma

+ Kart ekle

Bilet

- BSG-1 Bir makale seçilmiş anomali senaryosu çıkartılmalı
- > BSG-3 Seçilen makalenin swot analizi çıkartılmalı
- BSG-5 Sunum için slayt hazırlanmalı
- < BSG-6 Linux ortamı sanal veya bilgisayar kurulmalı
 - ↳ BSG-7 Mac sahibi olanlar sanal ortamdan erişebilir.
- < BSG-8 Simülasyon ortamı kurulmalı
 - ↳ BSG-9 Oluşturulan ortam raporlanmalı githuba atılmalı
- < BSG-10 Sektörel araştırma yapılmalı
 - ↳ BSG-11 Tüm araştırmalar githuba raporlanmış şekilde atılmalı
- < BSG-12 Herkesin kendi anomalisine uygun simülasyon ortam araştırması
 - ↳ BSG-13 yapılan araştırmaların githuba raporlanması
- < BSG-14 Oluşturulan simülasyon ortamına bireysel anomali senaryolarının entegrasyonu
 - ↳ BSG-16 Tüm 5 yeni senaryonun IDS tarafından algılanması ve blockchain'e entegrasyonu
- < BSG-15 Simülasyonda ML ile model eğitimi
 - ↳ BSG-17 Dashboard'da ML-IDS alert'lerinin rule-based IDS ile birlikte görünecek şekilde gösterilmesi

November	December
Timeline bar for November tasks	Timeline bar for December tasks

TRELLO

JIRA

LINKEDIN HESABIMIZ

<https://www.linkedin.com/in/security-volt>

LinkedIn profile page for Async 10. The profile picture shows a car being charged. The bio reads: "Güvenli Şarj, Güvenli Yolculuk". The summary says: "Teknoloji, Bilgi ve İnternet · 5 takipçi · 2-10 çalışan". The activity feed shows a post from Async 10 about OCPP protocol robustness analysis.

Async 10
Güvenli Şarj, Güvenli Yolculuk
Teknoloji, Bilgi ve İnternet · 5 takipçi · 2-10 çalışan

Uğur ve 1 bağlantı daha bu sayfayı takip ediyor

[Mesaj](#) [Takip Ediliyor](#) [...](#)

Ana Sayfa Hakkında [Gönderiler](#) İş İlanları Kişiler



Async 10
5 takipçi
7 saat · [...](#)

Merhaba LinkedIn,
Elektrikli araçlar (EV) hayatımızın ayrılmaz bir parçası haline gelirken, onlara güç veren şarj istasyonlarının teknik altyapısı da giderek karmaşıklıyor. Peki, bu altyapı beklenmedik durumlara ne kadar hazır?
Biz, Async 10 ekibiyiz.
Adımız, bu sistemlerin temelindeki "Asenkron" (Asynchronous) iletişim protokollerinin karmaşıklığından geliyor. Bilgi Sistemleri Güvenliği dersi kapsamında, değerli hocamız [Fatih Özkaynak](#)'nın rehberliğinde bir araya gelmiş 10 kişilik bir proje ekibiyiz.
Misyonumuz Nedir? EV şarj ekosistemi 10 farklı ve kritik anomali senaryosu üzerinden analiz ediyoruz. Amacımız, bu sistemlerin sadece normal çalışma koşullarını değil, aynı zamanda standart dışı veya beklenmedik durumlara karşı tepkilerini de derinlemesine anlamak.
Felsefemiz: Riski minimize etmek. (İsmimizdeki 'R' harfinin eksikliği, bu 'Risksiz' hedefimize bir göndermedir.)
Neden Bizi Takip Etmelisiniz? Önümüzdeki haftalarda, bu 10 farklı anomali senaryosunu ve bulgularımızı haftalık olarak buradan sizlerle paylaşacağız.
Geleceğin şarj altyapısını daha güvenli ve daha sağlam temellere oturtmak adına çıktığımız bu akademik yolculukta, bulgularımızı tartışmak ve birlikte öğrenmek için bizi takip edin!

#Async10 #BilgiSistemleriGüvenliği #EVCharging #EVSE #OCPP #AnomaliTespit

Async 10
6 takipçi
15 saat · [...](#)

Elektrikli araç ekosisteminin kalbi olan OCPP (Open Charge Point Protocol), istasyonlar ve yönetim sistemleri (CSMS) arasındaki iletişimi sağlar. Peki, ya bu iletişim kanalına "beklenmedik" misafirler dahil olursa? 🤔
Ekip olarak gerçekleştirdiğimiz son simülasyonda, OCPP protokolünün sağlamlığını (robustness) test etmek için "Fuzzing" teknijini kullandık. Amacımız sadece sistemin doğru çalışıp çalışmadığını değil, hatalı durumlarda nasıl tepki verdiği görmekti.
💡 Senaryomuz Neydi? Standart bir istemci gibi davranışarak sisteme kasıtlı olarak bozuk, aşırı uzun veya anlamsız veri paketleri gönderdik. Normalde bir şarj başlatma komutu bekleyen sisteme, binlerce karakterlik anlamsız veri yolladığımızda ne olduğunu gözlemediğimiz.
💡 Sonuç: Simülasyonumuzda, yeterli "Girdi Doğrulama" (Input Validation) yapılmayan sistemlerin, bu beklenmedik veriler karşısında çöktüğünü (DoS) veya hizmet veremez hale geldiğini tespit ettik.
💡 Çıkarımız: Güvenli bir şarj altyapısı için sadece "çalışan kod" yetmez; "kırılmayan kod" gereklidir. Beklenmedik girdileri reddeden, hatayı yönetebilen ve çalışmaya devam eden sistemler geliştirmek zorundayız.
Detaylar ve teknik analizlerimiz devam edecek! 🚀
[#OCPP #CyberSecurity #ElectricVehicles #Fuzzing #SoftwareTesting](#)

OCPP PROTOCOL ROBUSTNESS ANALYSIS: FUZZING ANOMALY DETECTED

FUZZER SCRIPT OUTPUT

```
> Starting fuzzing attack on OCPP target...
> Sending Packet ID: 1233, Type: BootNotification, Payload: {"vendor": "NORMAL_VENDOR"}
> Sending Packet ID: 1234, Type: BootNotification, Payload: {"vendor": "VERY_LONG_STRING_AAAA..."}
> Sending Packet ID: 1235, Type: InvalidCommand, Data: "random#@!data" ...
```

CSMS SERVER LOGS

```
[2025-11-02 14:35:12] ERROR: Unhandled exception
in handler: ValueError: invalid literal for
int() with base 10: 'VERY_LONG_STRING...
[2025-11-02 14:35:13] CRITICAL: Server crashed
due to unhandled payload.
[SERVICE STOPPED]
```

Async10 Ekip Nabzı

Form açıklaması

1. Yeterince üstünde durmadığımızı düşündüğünüz veya belirtemediğiniz fikriniz var mı?

Kısa yanıt metni

2. Bu hafta yapılacak görevlerden şahsen yapmaktan zevk duyacağınız hangisi?

Kısa yanıt metni

3. Hangi görevi asla yapmak istemezsiniz?

Kısa yanıt metni

4. Sizce bu haftanın favori ekip üyesi kim olmalı?

Kısa yanıt metni

1. Yeterince üstünde durmadığımızı düşündüğünüz veya belirtemedi	2. Bu hafta yapılacak görevlerden şahsen yapmaktan zevk c	3. Hangi görevi asla yapmak istemezsiniz?	4. Sizce bu haftanın favori ekip üyesi kim olm	5. İsimlerinizi girin:
toplantılara hazırlıksız geliyoruz	Sunum	Sudem Cüçemen	Özgün	
Ne olursa olsun, fazla kasıldığı düşünüyorum. Sadece herkes kendi üst	gergin sudem	semih		
Web sitesi oluşturup canlıya almak, LinkedIn açmak, toplantı rap	Herhangi bir şey yapmam gerekiyorsa yaparım.	Sena Ateş	Sena Ateş	
yok	araştırma, raporlama	slayt, sunum	Oğuzhan Erdoğan	
Simülasyonları düşünüyordum ancak onları da yapmaya başladık	Açıkçası ortam oluşturmak ve test etmek heyecan verici geliyor	Açıkçası görevin türüne göre değişir boş işler diyebilirim	Yani Sudem anladık sensin (şaka amaçlı yazıyorum	
Yok	fark etmez, elimden geldiğince yapmaya çalışırım.	asla demem de fark etmez yani sunum hazırlamak pek alanım	İbrahim Kerem Güven	
	Yazılım kısımları	Rapor yazmak	Sena Ateş	
	Fark etmez	Fark etmez	Uğur Berktaş	
Yok			Enes Malik Ari	
			Sudem cüçemen	
			Sude demir	

TAKIM MEMNUNİYETİ VE İŞ YÜKÜ ANALİZİ

Bu anket, ekip üyelerinin haftalık görevler, memnuniyet, tercih ve zorluklarla ilgili hızlı geri bildirim vermesini sağlamak amacıyla hazırlanmıştır. Ekip içi iletişimini güçlendirmek, sprint planlamasını iyileştirmek ve bireysel yükleri daha dengeli dağıtmak için kullanılır.

GITHUB REPOMUZ



<https://github.com/sennaates/elektrikli-arac-sarj-istasyon-guvenligi-g10>



main · 13 Branches · 0 Tags

Go to file · Add file · Code

Sude-Demir Sude Demir · 9490b39 · 1 hour ago · 140 Commits

Commit	Message	Time
1.Hafta	birkaç senaryo üstünden ilk çıktılarımız	last month
2. Hafta	Özgün Deniz Sevilmiş	2 weeks ago
3. hafta	Sude Demir	1 hour ago
4. Hafta	Add files via upload	2 hours ago
Anomali Senaryoları	Add files via upload	last month
ProjeHakkında	Add files via upload	3 weeks ago
Swot Analizleri	Add files via upload	last month
README.md	Revise README for Secure OCPP-to-CAN Bridge	last month

Proje Özeti

Bu proje, **OCPP (Open Charge Point Protocol)** komutlarını **CAN-Bus** frame'lerine güvenli bir köprü sistemidir. Sistem, **blockchain teknolojisi** ile veri bütünlüğünü garanti altına alır ve **hibrit IDS (Intrusion Detection System)** ile gerçek zamanlı saldırı tespiti yapar.

Temel Özellikler

- Blockchain-Based Security: Her OCPP ve CAN mesajı SHA-256 hash chain'e kaydedilir
- Hybrid IDS: Rule-based + ML-based (Isolation Forest) anomalı tespiti
- Digital Signature: ECDSA ile blok imzalama
- Real-Time Dashboard: Streamlit ile canlı izleme
- Alert System: Otomatik saldırı tespiti ve alarm
- ML-Ready: Scikit-learn ile eğitilebilir anomalı modeli
- Attack Simulator: Test senaryoları için saldırı simülatörü

güncelsimülasyonumuz · 2 Branches · 0 Tags

Go to file

This branch is 2 commits ahead of and 95 commits behind main .

Sudemc feat: Secure OCPP-to-CAN Bridge projesi eklendi · a70:

tests	feat: Secure OCPP-to-CAN Bridge projesi ekle
training	feat: Secure OCPP-to-CAN Bridge projesi ekle
utils	feat: Secure OCPP-to-CAN Bridge projesi ekle
.gitignore	feat: Secure OCPP-to-CAN Bridge projesi ekle
DASHBOARD_TEST_REPORT.md	feat: Secure OCPP-to-CAN Bridge projesi ekle
FINAL_PROJECT_REPORT.md	feat: Secure OCPP-to-CAN Bridge projesi ekle
GIT_SETUP.md	feat: Secure OCPP-to-CAN Bridge projesi ekle
LICENSE	feat: Secure OCPP-to-CAN Bridge projesi ekle
PROJECT_SUMMARY.md	feat: Secure OCPP-to-CAN Bridge projesi ekle
PUSH_INSTRUCTIONS.md	feat: Secure OCPP-to-CAN Bridge projesi ekle
QUICK_REFERENCE.md	feat: Secure OCPP-to-CAN Bridge projesi ekle
QUICK_START_FOR_TEAM.md	feat: Secure OCPP-to-CAN Bridge projesi ekle
README.md	feat: Secure OCPP-to-CAN Bridge projesi ekle
README_SCENARIO_01.md	feat: Secure OCPP-to-CAN Bridge projesi ekle
README_SCENARIO_02.md	feat: Secure OCPP-to-CAN Bridge projesi ekle
README_SCENARIO_03.md	feat: Secure OCPP-to-CAN Bridge projesi ekle

ARAŞTIRMA VE DOKÜMANLARI MIZ

<https://github.com/sennaates/elektrikli-arac-sarj-istasyon-guvenligi-g10/tree/main/1.Hafta>

En Çok Tercih Edilen Sarj İstasyonlarının Tercih Edilme Nedenleri

Elektrikli Araç Sarj İstasyonlarının Fiziksel Güvenlik Risk Analizi Raporu

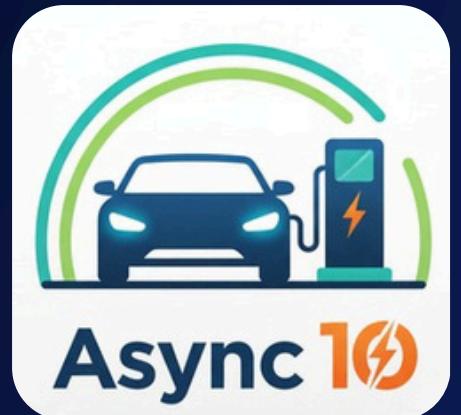
Simülasyonda CSMS rolü ve STEVE kullanımı

Şarj İstasyonları Güvenliği ve Türkiye Pazar Analizi

Simülasyon Proje Dokümantasyonu

Simülasyon Programcı Kılavuzu

Simülasyon Hakkında Genel Bilgi



ANOMALİ SENARYOLARIMIZ VE İNCELEDİĞİMİZ MAKALELER



Sude Demir - OCPP Mesaj Yoğunluğu Saldırısı (DoS Hazırlığı)

- Federated detection of open charge point protocol 1.6 cyberattacks

Sudem Cücemen - Enerji Akış Parametrelerinin Değiştirilmesi (MitM)

- Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks

Sena Ateş - OCPP Protokolünde Fuzzing Tabanlı Zafiyet Tespiti: Protokol Sağlamlık Analizi

- OCPPStorm: A Comprehensive Fuzzing Tool for OCPP Implementations

Enes Malik arı - Sahte Rezervasyon (A4: Duplicate Booking) Kullanarak Yetkisiz Şarj Erişimi

- Cyber defense in OCPP for EV charging security risks

Uğur Berktaş - AI Tabanlı Faturalandırma Sistemlerinde Gecikme Kaynaklı Zafiyet

- Federated Detection of Open Charge Point Protocol 1.6 Cyberattacks

İbrahim Kerem Güven - Adaptif Örnekleme Manipülasyonu (Sampling Manipulation)

- Privacy-Aware Smart Metering: Progress and Challenges

Semih Tepe - Fail-Open Davranisi - Auth Servis Kapali

- Cybersecurity Risk Analysis of Electric Vehicles Charging Stations

Özgün Deniz Sevilmiş - Sahte Firmware Güncellemesi ile Şarj İstasyonunu Ele Geçirme (Ransomware)

- MitM Cyber Risk Analysis in OCPP enabled EV Charging Stations

Şerif Bayram - CLAC-SCO: Coordinated Load Alteration via Compromised Smart Charging Orchestrator

- MaDEVIoT: Cyberattacks on EV Charging Can Disrupt Power Grid Operation

Oğuzhan Erdoğan - Sensör Verisi Zehirleme (SDP)

- EmuOCPP: Effective and Scalable OCPP Security and Privacy Testing

Selanur Ayaz - OCPP Schema Drift ile Uygulama Katmanı Zafiyet Analizi

- OCPPStorm: A Comprehensive Fuzzing Tool for OCPP Implementations

elektrikli-arac-sarj-istasyon-guvenligi-g10 / Anomali Senaryolar /

OguzhanErdogan23 Add files via upload

Name

- ..
- ADAPTİF ÖRNEKLEME MANİPÜLASYONU (Sampling Manipulatio...
- CLAC-SCO_Anomali_Senaryosu_Raporu_Turkce_MakaleEkli_v2.pdf
- Faturalandırma_Gecikme_Kaynaklı_Zafiyet.pdf
- OCPP Mesaj Yoğunluğu Saldırısı (DoS Hazırlığı) Anomali Senaryo...
- OCPP MitM ile Yetkilendirme Değişikliği Anomali Senaryosu.docx
- OCPP Protokolünde Fuzzing Tabanlı Zafiyet Tespiti.pdf
- OCPPSchemaDrift.docx
- OCPP_v2_0_1_L02_Firmware_Saldırısı_Raporu.pdf
- Sahte Rezervasyon (A4: Duplicate Booking) Kullanarak Yetkisiz Ş...
- Sensör Verisi Zehirleme.docx
- fail_open_davranisi.pdf

elektrikli-arac-sarj-istasyon-guvenligi-g10 / Swot Analizleri /

OguzhanErdogan23 Add files via upload

Name

- ..
- Enes
- Ağır şarj noktası protokolünün birleştirilmiş tespiti Swot Analizi.d...
- CLAC-SCO Senaryosu SWOT Analizi.docx
- EV Şarj Altyapısı Güvenliği.docx
- EmuOCPP.docx
- Faturalandırma_gecikme_SWOT.pdf
- FuzzingToolSwot.pdf
- Man-in-the-Middle Saldırılarına Karşı Korunma Swot Analizi.docx
- SWOT_Analizi_Brown_Makalesi_OCPP.pdf
- Swot Analizi Adaptif İbrahim.pdf
- fail_open_davranisi.pdf



HEDEFLERİMİZ

1. Hafta – Araştırma & Organizasyon

SMART Hedef:

1 hafta içerisinde elektrikli araç şarj istasyonları ve anomali tespiti üzerine ilgili akademik makaleler bulunacak, incelenecuk ve ekip içi görev dağılımı netleştirilecektir.

Yapılanlar / Çıktılar:

İlgili makaleler ve benzer çalışmaların bulunması

Anomali senaryolarının belirlenmesi

Trello & Jira üzerinden SMART hedeflerin tanımlanması

Görev dağılımının yapılması

Google Drive ekip dizininin oluşturulması

Ölçüt:

Makale listesi

Aktif Trello/Jira panosu

Paylaşımı Drive klasör yapısı

2. Hafta – Analiz & Saha Çalışması

SMART Hedef:

2. hafta sonunda incelenen makaleler için SWOT analizleri tamamlanacak ve gerçek bir elektrikli şarj istasyonu fiziksel olarak inceleneciktir.

Yapılanlar / Çıktılar:

Makalelerin SWOT analiz raporlarının hazırlanması

Fiziksel şarj istasyonu incelemesi

En popüler şarj istasyonlarının tercih edilme nedenlerinin araştırılması

Toplantı sonrası ekip bildirim formu ile memnuniyet ve yetkinlik ölçümü

Ölçüt:

SWOT raporları

Fiziksel güvenlik gözlem notları

Tercih analizi raporu

Ekip geri bildirim formu sonuçları

HEDEFLERİMİZ



3. Hafta – Güvenlik & Simülasyon Araştırması

SMART Hedef:

3. hafta sonunda şarj istasyonlarına yönelik fiziksel güvenlik risk analizi ve simülasyon mimarisi netleştirilecektir.

Yapılanlar / Çıktılar:

Elektrikli Araç Şarj İstasyonları Fiziksel Güvenlik Risk Analizi Raporu

Simülasyon ortamı üzerine araştırmalar

CSMS rolü ve STEVE kullanımının incelenmesi

Simülasyon mimari raporu

LinkedIn proje/ekip hesabının açılması

Ölçüt:

Risk analiz raporu

CSMS & STEVE araştırma dokümanı

Aktif LinkedIn hesabı

4. Hafta – Beta Simülasyon Geliştirme

SMART Hedef:

4. hafta sonunda temel işlevleri çalışan bir beta simülasyon ortamı oluşturulacaktır.

Yapılanlar / Çıktılar:

Beta simülasyonun kurulması

Anomali senaryolarının simülasyona entegrasyonu

Dashboard görüntüsünün simülasyona eklenmesi

Ölçüt:

Çalışan beta simülasyon

Dashboard ile görüntülenebilir test ortamı

HEDEFLERİMİZ



5. Hafta – Test, ML ve Arayüz İyileştirme

SMART Hedef:

5. hafta sonunda tüm anomali senaryoları test edilmiş, ML entegrasyonu tamamlanmış ve dashboard arayüzü iyileştirilmiş olacaktır.

Yapılanlar / Çıktılar:

Tüm saldırı/anomali senaryolarının test edilmesi

Veri modeli eğitimi ve ML entegrasyonu

Dashboard kullanıcı arayüzü iyileştirmeleri

Ölçüt:

Test sonuçları

ML çıktıları

Güncellenmiş dashboard

6. Hafta – Dokümantasyon

SMART Hedef:

6. hafta sonunda simülasyonla ilgili tüm teknik ve kullanıcı dokümantasyonları tamamlanacaktır.

Yapılanlar / Çıktılar:

Simülasyon Proje Dokümantasyonu

Simülasyon Programcı Kılavuzu

Simülasyon Hakkında Genel Bilgi Raporu

Proje kapanış değerlendirmesi

Ölçüt:

3 adet tamamlanmış doküman

Teslim edilebilir proje paketi

BETA SİMÜLASYONU ÇIKTILARI

The image shows three terminal windows side-by-side, each displaying log output from a simulation environment.

- CSMS (plain_ws) Terminal:** Shows logs for the CSMS simulator starting up on port 9000, establishing a plain WebSocket connection, and handling OCPP messages related to a charge point (cp001).
- CAN Traffic Terminal:** Shows logs for a CAN bus interface (vcan0) with ID 200, indicating the creation of a socket, the start of a CAN bus at 500000 bps, and the configuration of a gateway CAN listener.
- Charge Point (plain_ws) Terminal:** Shows logs for a charge point (CP Simülörü) starting up, connecting to the CSMS server, and handling OCPP messages for a remote start transaction and a charging session (Connector 1).
- Debug Console / Terminal / Ports:** A summary log window showing the final statistics for the MitM test scenario, including connection details, message counts, and error counts.

```
2025-11-03 18:22:19,741 - __main__ - INFO - CSMS simülatörü başlatıldı: localhost:9000
2025-11-03 18:22:19,751 - src.security.tls_config - INFO - Plain WebSocket (güvenlik yok)
2025-11-03 18:22:19,751 - __main__ - INFO - CSMS WebSocket server başlatılıyor
r: plain_ws
2025-11-03 18:22:19,751 - __main__ - INFO - CSMS hazır: ws://localhost:9000
2025-11-03 18:22:19,762 - websockets.server - INFO - server listening on 127.0.0.1:9000
2025-11-03 18:22:21,604 - websockets.server - INFO - connection open
2025-11-03 18:22:21,604 - __main__ - INFO - Yeni CP bağlantısı: cp001
2025-11-03 18:22:21,605 - __main__ - INFO - BootNotification tamamlandı: cp001
2025-11-03 18:22:24,745 - __main__ - INFO - cp001 için RemoteStartTransaction gönderilir...
2025-11-03 18:22:24,745 - __main__ - INFO - RemoteStartTransaction gönderildi : cp001
2025-11-03 18:22:21,591 - __main__ - INFO - CP Simülörü başlatıldı: CP001
2025-11-03 18:22:21,593 - can.interfaces.socketcan.socketcan - INFO - Created a socket
2025-11-03 18:22:21,593 - src.can_bus.can_simulator - INFO - CAN bus başlatıldı: vcan0 @ 500000 bps
2025-11-03 18:22:21,593 - src.bridge.gateway - INFO - Gateway CAN listener'ları kuruldu
2025-11-03 18:22:21,593 - src.can_bus.can_simulator - INFO - CAN dinleme başlatıldı
2025-11-03 18:22:21,594 - __main__ - INFO - CSMS'e bağlanılıyor: ws://localhost:9000/charge_point/cp001
2025-11-03 18:22:21,604 - __main__ - INFO - CSMS bağlantısı kuruldu
2025-11-03 18:22:21,604 - __main__ - INFO - BootNotification gönderildi
2025-11-03 18:22:21,605 - __main__ - WARNING - Action bilgisi yok
2025-11-03 18:22:24,746 - __main__ - INFO - OCPP mesajı alındı: RemoteStartTransaction
2025-11-03 18:22:24,747 - src.bridge.gateway - INFO - OCPP-CAN: RemoteStartTransaction → ID=0x200
2025-11-03 18:22:24,747 - __main__ - INFO - Şarj başlatıldı: Connector 1
2025-11-03 18:22:24,749 - __main__ - WARNING - Action bilgisi yok
2025-11-03 18:22:19,741 - __main__ - INFO - CSMS simülatörü başlatıldı: localhost:9021
2025-11-03 18:22:19,751 - src.security.tls_config - INFO - Plain WebSocket (güvenlik yok)
2025-11-03 18:22:19,751 - __main__ - INFO - CSMS WebSocket server başlatılıyor: plain_ws
2025-11-03 18:22:19,762 - websockets.server - INFO - server listening on 127.0.0.1:9021
2025-11-03 18:22:21,604 - __main__ - INFO - CP Simülörü başlatıldı: CP_MITM_TEST
2025-11-03 18:22:21,605 - __main__ - INFO - Created a socket
2025-11-03 18:22:21,605 - INFO - CAN bus başlatıldı: vcan0 @ 500000 bps
2025-11-03 18:22:21,605 - INFO - Gateway CAN listener'ları kuruldu
2025-11-03 18:22:21,605 - INFO - CAN dinleme başlatıldı
2025-11-03 18:22:21,605 - INFO - CSMS'e bağlanılıyor: ws://localhost:9021/charge_point/cp_mitm_test
2025-11-03 18:22:21,605 - INFO - connection open
2025-11-03 18:22:21,605 - INFO - Yeni CP bağlantısı: cp_mitm_test
2025-11-03 18:22:21,605 - INFO - CSMS bağlantısı kuruldu
2025-11-03 18:22:21,605 - INFO - BootNotification gönderildi
2025-11-03 18:22:21,605 - INFO - BootNotification tamamlandı: cp_mitm_test
2025-11-03 18:22:21,605 - WARNING - Action bilgisi yok
2025-11-03 18:22:21,605 - INFO - RemoteStartTransaction gönderildi: cp_mitm_test
2025-11-03 18:22:21,605 - INFO - OCPP mesajı alındı: RemoteStartTransaction
2025-11-03 18:22:21,605 - INFO - OCPP-CAN: RemoteStartTransaction → ID=0x200
2025-11-03 18:22:21,605 - INFO - Şarj başlatıldı: Connector 1
2025-11-03 18:22:21,605 - WARNING - Action bilgisi yok
2025-11-03 18:22:21,605 - INFO - Final stats: {'connected': True, 'cp_id': 'CP_MITM_TEST', 'scenario': 'plain_ws', 'gateway_stats': {'ocpp_to_can': 1, 'can_to_ocpp': 0, 'errors': 0, 'total_messages': 1}, 'an_stats': {'total_messages': 1, 'sent_messages': 1, 'listeners': 1, 'id_distribution': {512: 1}}}
2025-11-03 18:22:21,605 - INFO - MitM senaryo başarılı!
2025-11-03 18:22:21,605 - INFO - CAN bus durduruldu
2025-11-03 18:22:21,605 - INFO - CP bağlantısı kapatıldı: cp_mitm_test
2025-11-03 18:22:21,605 - INFO - connection closed
2025-11-03 18:22:21,605 - INFO - CP simülörü durduruldu
2025-11-03 18:22:21,605 - INFO - CSMS durduruldu
```

ALFA SİMÜLASYONU



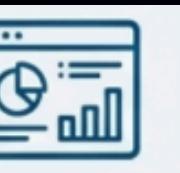
Blockchain Tabanlı Güvenlik

Her OCPP ve CAN işlemi, SHA-256 hash zinciri ve ECDSA dijital imzaları ile kriptografik olarak güvence altına alınır. Veri bütünlüğü ve değiştirilemezlik garanti edilir.



Hibrit Saldırı Tespit Sistemi (IDS)

Kural tabanlı kontroller bilinen tehditleri arasında yakalarken, Makine Öğrenmesi (*Isolation Forest*) modeli sıfır gün (zero-day) anomalilerini tespit eder.



Gerçek Zamanlı Ekosistem

Streamlit ile geliştirilmiş canlı izleme paneli, 8 endpoint'lu REST API ve 8 farklı senaryoyu test edebilen saldırı simülatörü.



- **REST API:** FastAPI ile geliştirilmiş 8 endpoint, sistemin tüm istatistiklerine (sağlık, blockchain, IDS) anlık erişim sağlar.



- **Canlı Dashboard:** Streamlit ve Plotly kullanılarak geliştirilen interaktif panel, 3 saniyede bir kendini yenileyerek sistem metriklerini, blockchain büyümесini ve saldırısı uyarılarını görselleştirir.



- **Saldırı Simülatörü:** CAN ve OCPP tabanlı 8 farklı saldırı senaryosunu (CAN Flood, Replay, MitM, vb.) komut satırından tetikleyerek sistemin savunma mekanizmalarını test etme imkanı sunar.

GÜVENLİK KATMANI 1: DEĞİŞİRTİLEMEZ KAYIT ZİNCİRİ (BLOCKCHAIN)

GÜVENLİK KATMANI 2: İKİ AŞAMALI AKILLI TEHDİT SİSTEMİ (HİBRİT IDS)

ALFA SİMÜLASYONU ÇIKTILARI

Saldırı Test Paneli

Bir senaryo seçin

- Genel Bakış
- MitM OCPP
- CAN Flood
- Sampling Manipulation
- Fail-Open Attack
- Ransomware
- Latency Exploit
- Replay Attack
- High Entropy
- Sensor Poisoning

Genel Bakış

Tüm sistem durumunu ve tespit edilen tehditleri görüntüleyin

Sistem Güvenli

Şu anda aktif bir saldırı tespit edilmedi

CAN Bus Normal	✓
OCPP Bağlı	✓
ML-IDS Aktif	✓
Blockchain Çalışıyor	✓

Test Edilebilir Saldırı Senaryoları

Sol menüden seçerek test başlatın

- MitM OCPP**
OCPP protokolü üzerinden Man-in-the-Middle saldırısı.
 Henüz Test Edilmedi
- CAN Flood**
CAN Bus'ı yüksek frekanslı mesajlarla doldurma saldırısı.
 Henüz Test Edilmedi
- Sampling Manipulation**
Enerji ölçüm verilerinin örnekleme oranını manipülasyonu.
 Henüz Test Edilmedi
- Fail-Open Attack**
Sistemi offline moda zorlayarak güvenlik kontrolleri devreden geçirme saldırısı.
 Henüz Test Edilmedi
- Ransomware**
Sahte firmware güncellemesi ile sistemi ele geçirme saldırısı.
 Henüz Test Edilmedi
- Latency Exploit**
Sistem gecikmelerini kullanarak saldırı pence.
 Henüz Test Edilmedi
- Replay Attack**
Geçerli CAN mesajlarını kaydedip tekrar gönderme saldırısı.
 Henüz Test Edilmedi
- High Entropy**
Rastgele yüksek entropi verileri göndererek tespit etme saldırısı.
 Henüz Test Edilmedi
- Sensor Poisoning**
Sensör verilerini yavaşça değiştirerek tespit etme saldırısı.
 Henüz Test Edilmedi

ALFA SİMÜLASYONU ÇIKTILARI

🔒 Bu Sistem Ne Yapar?

Bu güvenlik sistemi, elektrikli araç şarj istasyonlarına yapılabilecek **siber saldırıları tespit eder ve engeller**. Sol menüden bir saldırıyı seçtiğinizde, o saldırının nasıl simülasyonu gerçekleştirileceğini görebilirsiniz.



ML-IDS

Yapay zeka ile
otomatik tespit



Blockchain

Değiştirilemez
olay kaydı



Kural Tabanlı

Bilinen saldırıları
anında yakalar

Saldırı Test Paneli

Bir senaryo seçin

- Genel Bakış
- MitM OCPP
- CAN Flood
- Sampling Manipulation
- Fail-Open Attack
- Ransomware
- Latency Exploit
- Replay Attack

MitM OCPP

OCPP protokolü üzerinden Man-in-the-Middle saldırısı

⚠ DİKKAT: Şarj istasyonunuz ile merkez sistem arasındaki iletişim ele geçirildi!

Bir saldırgan, aracınız şarj olurken istasyon ile sunucu arasındaki mesajları okuyup değiştiriyor. Şarj ücreti manipüle edilebilir, oturumunuz çalınabilir veya sahte komutlar gönderilebilir.

⌚ Olası Riskler:

⚡ Şarj ücretiniz değiştirilebilir

🔑 Oturum bilgileriniz çalınabilir

⚡ Şarj işlemi aniden durdurulabilir

ALFA SİMÜLASYONU ÇIKTILARI

Saldırı Test Paneli

Bir senaryo seçin

- Genel Bakış
- MitM OCPP
- CAN Flood
- Sampling Manipulation
- Fail-Open Attack
- Ransomware
- Latency Exploit
- Replay Attack
- High Entropy

Sistem Bu Saldırıyı Nasıl Önledi?

Güvenlik sistemimiz, OCPP mesajlarındaki anormal değişiklikleri tespit etti. Mesaj bütünlüğü kontrolü sayesinde manipüle edilmiş komutlar reddedildi.

Uygulanan Güvenlik Adımları:

- Kural Tabanlı IDS: OCPP mesaj yapısındaki anormallik tespit edildi
- ML-IDS: Mesaj içerisindeki beklenmedik değişiklikler yakalandı
- Önlem: Şüpheli mesajlar bloke edildi, oturum güvenli tutuldu
- Blockchain: Saldırı girişimi değiştirilemez şekilde kayıt altına alındı

✓ Saldırı tespit edildi, önlandı ve kayıt altına alındı

Saldırı zamanı: 11:03:14 • Sistem güvenlik önlemlerini devreye aldı

Tekrar Test Et

Güvenlik Metrikleri

Her sayının ne anlama geldiğini aşağıda görebilirsiniz

1 TESPIT EDİLEN TEHDİT <small>Sistemin yakaladığı şüpheli aktivite sayısı</small>	1 YÜKSEK ÖNCELİKLİ <small>Acil müdahale gerektiren tehditler</small>	Aktif ML-IDS DURUMU <small>Yapay zeka tabanlı saldırı tespiti</small>	1 BLOCKCHAIN BLOK <small>Değiştirilemez güvenlik kaydı sayısı</small>
--	---	--	--

Tehdit: Sistemdeki anormal aktiviteler (saldırı girişimleri, şüpheli trafik) | **ML-IDS:** Makine öğrenmesi ile otomatik tehdit tespiti | **Blockchain:** Tüm olayın değiştirilemez güvenlik kaydı sayısı

Tespit Edilen Tehditler

Güvenlik sistemi tarafından yakalanan saldırı girişimleri

Kritik <small>Sistem çökmesine neden olabilir</small>	Yüksek <small>Ciddi güvenlik açığı</small>	Orta <small>Izlenmesi gereken durum</small>	Düşük <small>Bilgilendirme amaçlı</small>
---	--	---	---

MITM_OCPP_MANIPULATION

Man-in-the-Middle OCPP mesaj manipülasyonu: start_to_stop

İletişim araya girme - Verileriniz izleniyor olabilir

2025-12-25 11:03:14