**Makale Terimleri Sözlüğü**

**Protokol ve Mimarî Terimleri**

* **OCPP (Open Charge Point Protocol - Açık Şarj Noktası Protokolü):** Şarj İstasyonları (CS) ile bu istasyonları yöneten Merkezi Yönetim Sistemi (CSMS) arasındaki iletişimi kuran standart bir uygulama protokolüdür.
* **CS (Charging Station - Şarj İstasyonu):** Elektrikli araçların (EV) şarj edildiği fiziksel istasyonlar.
* **CSMS (Charging Station Management System - Şarj İstasyonu Yönetim Sistemi):** Genellikle halka açık yerlerde bulunan tüm şarj istasyonlarındaki işlemleri ve kullanıcı taleplerini verimli bir şekilde yönetmekten sorumlu merkezi sistemdir.
* **EVSE (Electric Vehicle Supply Equipment - Elektrikli Araç Besleme Ekipmanı):** Şarj istasyonunun (CS) içinde bulunan ve elektrikli araçla (EV) fiziksel bağlantıyı ve iletişimi başlatan/durduran parçalardır.
* **ISO 15118:** Elektrikli araç (EV) ile şarj istasyonu (CS) arasındaki çift yönlü iletişimi (V2G - Araçtan Şebekeye) destekleyen uluslararası bir standarttır.

**Risk Analiz Yöntemleri**

* **STRIDE (Tehdit Modelleme Metodolojisi):** Olası siber güvenlik tehditlerini 6 ana kategoriye ayırarak tanımlamak ve sınıflandırmak için kullanılan bir yöntemdir. Bu 6 kategori şunlardır:
  + **S - Spoofing (Kimlik Sahtekarlığı):** Başka bir kullanıcının kimlik doğrulama bilgilerini yasa dışı olarak elde etme ve kullanma.
  + **T - Tampering (Kurcalama / Veri Bozma):** Verilerin, yapılandırmaların veya kaynak kodlarının kasıtlı olarak değiştirilmesi.
  + **R - Repudiation (İnkar Etme):** Bir eylemi gerçekleştirdikten sonra (örneğin bir ödeme emri) bunu yaptığını inkar etme.
  + **I - Information Disclosure (Bilgi İfşası):** Gizli bilgilerin, görmeye yetkisi olmayan kişilere sızdırılması.
  + **D - Denial of Service (DoS - Hizmet Reddi):** Bir sistemin (örn. şarj istasyonunun) çalışmasını engelleyerek veya yavaşlatarak meşru kullanıcıların hizmet almasını engelleme.
  + **E - Elevation of Privilege (Yetki Yükseltme):** Normal bir kullanıcının, sistemde daha yüksek yetkilere (örn. yönetici) sahip olmak için yetkilerini artırması.
* **DREAD (Risk Değerlendirme Modeli):** STRIDE ile belirlenen tehditlerin ciddiyetini ve önceliğini belirlemek için kullanılan bir risk puanlama modelidir. Puanlama şu 5 kritere göre yapılır:
  + **D - Damage (Hasar):** Bu saldırı başarılı olursa ne kadar büyük bir hasar verir?.
  + **R - Reproducibility (Tekrarlanabilirlik):** Bu saldırıyı tekrarlamak ne kadar kolay?.
  + **E - Exploitability (Sömürülebilirlik):** Bu güvenlik açığını kullanmak (sömürmek) ne kadar kolay? Ne kadar uzmanlık gerektiriyor?.
  + **A - Affected users (Etkilenen Kullanıcılar):** Saldırıdan kaç kullanıcı etkilenir?.
  + **D - Discoverability (Keşfedilebilirlik):** Saldırganın bu güvenlik açığını bulması ne kadar kolay?.

**Enerji ve Şebeke Terimleri**

* **Microgrid (MG - Mikro Şebeke):** Güç sistemini daha basit ve daha sağlam hale getirmek için tasarlanmış, Dağıtılmış Enerji Kaynaklarından (DERs) oluşan küçük, yerel ve birbirine bağlı güç birimleridir.
* **EMS (Energy Management System - Enerji Yönetim Sistemi):** Mikro şebekenin performansını (enerji üretimi, dağıtımı ve tüketimini) izleyen, kontrol eden ve optimize eden sistemdir.
* **DERs (Distributed Energy Resources - Dağıtılmış Enerji Kaynakları):** Bir mikro şebekeyi oluşturan yerel enerji kaynaklarıdır (örneğin güneş panelleri, rüzgar türbinleri veya depolama sistemleri).
* **CPS (Cyber-Physical System - Siber-Fiziksel Sistem):** Bu makalede mikro şebekeler (MGs) için kullanılan bir terimdir. Hem fiziksel (enerji) hem de siber (kontrol, iletişim) bileşenlerin sıkı bir şekilde birbirine bağlı olduğu sistemleri tanımlar. Bu sistemler siber saldırılara karşı savunmasızdır.

**Siber Güvenlik ve İletişim Terimleri**

* **CV (Configuration Variables - Yapılandırma Değişkenleri):** Şarj istasyonunun nasıl çalışacağını belirleyen ayar parametreleridir. Makale, bu değişkenlerin (CVs) saldırganlar tarafından değiştirilmeye (tampering) açık olduğunu belirtiyor.
* **MitM (Man-in-the-Middle - Araya Girme Saldırısı):** Bir saldırganın, iki taraf (örneğin Şarj İstasyonu ve Merkezi Sistem) arasındaki iletişimin ortasına gizlice girerek verileri dinlemesi veya değiştirmesidir.
* **TLS (Transport Layer Security - Taşıma Katmanı Güvenliği):** İletişim kanallarını şifrelemek için kullanılan bir güvenlik protokolüdür.
* **Firmware (Donanım Yazılımı):** Bir cihazın (örneğin şarj istasyonunun) çalışması için gereken temel yazılımdır ve cihazın donanımına gömülüdür.
* **Malware (Kötü Amaçlı Yazılım):** Bir sisteme zarar vermek, veri çalmak veya sistemi bozmak için tasarlanmış genel bir yazılım terimidir.
* **Backdoor (Arka Kapı):** Bir saldırganın, normal kimlik doğrulama adımlarını atlayarak bir sisteme gizlice yeniden erişmesini sağlayan gizli bir yoldur.
* **Spyware (Casus Yazılım):** Kullanıcının haberi olmadan sisteme sızan ve kullanıcının aktivitelerini veya sistem bilgilerini gizlice toplayıp saldırgana gönderen yazılımdır.
* **Ransomware (Fidye Yazılımı):** Bir sistemin verilerini şifreleyerek erişilemez hale getiren ve verilerin geri verilmesi karşılığında fidye talep eden kötü amaçlı yazılımdır.
* **Rootkit:** Bir sisteme sızdıktan sonra saldırganın varlığını ve gerçekleştirdiği kötü amaçlı faaliyetleri gizlemek için tasarlanmış yazılım araçları bütünüdür.
* **Jamming (Sinyal Bozma):** Kablosuz iletişimi (Wi-Fi, Bluetooth vb.) engellemek için radyo frekanslarını kasıtlı olarak bozma veya parazit yapma eylemidir.
* **Flooding (Taşkın Saldırısı):** Bir sisteme veya ağa, kaldırabileceğinden çok daha fazla istek veya veri paketi göndererek sistemi meşgul etme ve çökertme yöntemidir. DoS saldırılarının bir türüdür.
* **Replay Attack (Yeniden Oynatma Saldırısı):** Bir saldırganın, iki taraf arasındaki meşru bir iletişim verisini (örneğin bir giriş şifresi paketi) yakalayıp, daha sonra bu veriyi sanki kendisi meşru kullanıcıymış gibi sisteme tekrar göndermesidir.
* **Heartbeat (Kalp Atışı Mesajı):** Bir cihazın (CS) merkezi sisteme (CSMS) hala "hayatta" ve "bağlı" olduğunu bildirmek için belirli aralıklarla gönderdiği küçük sinyal mesajıdır. Saldırganlar bu mesajların sıklığını değiştirerek DoS saldırısı yapabilir.
* **RFID (Radyo Freansı ile Tanımlama):** Kullanıcıların şarj işlemini başlatmak için kartlarını okuttukları temassız bir kimlik doğrulama teknolojisidir.
* **BLE (Bluetooth Low Energy - Düşük Enerjili Bluetooth):** Kullanıcıların telefonlarıyla şarj istasyonuna yakın mesafeden bağlanması için kullanılabilen bir kablosuz iletişim teknolojisidir.
* **NFC (Near-Field Communication - Yakın Alan İletişimi):** Kullanıcıların telefonlarını veya kartlarını istasyonuna çok yakın (birkaç cm) bir mesafeye dokundurarak iletişim kurmasını sağlayan teknolojidir.
* **VPN (Virtual Private Network - Sanal Özel Ağ):** Güvenli olmayan bir ağ (internet gibi) üzerinden güvenli, şifreli bir iletişim tüneli oluşturan teknolojidir.
* **Digital Signature (Dijital İmza):** Bir verinin bütünlüğünü (değişmediğini) ve kaynağını (kimden geldiğini) doğrulayan kriptografik bir yöntemdir.
* **Certificate (Dijital Sertifika):** Bir cihazın veya sunucunun kimliğini dijital olarak kanıtlayan bir belgedir.
* **CA (Certificate Authority - Sertifika Otoritesi):** Bu dijital sertifikaları üreten ve kimliklerini doğrulayan güvenilir üçüncü taraf kurumlardır.
* **SIEM (Security Information and Event Management - Güvenlik Bilgisi ve Olay Yönetimi):** Bir sistemdeki tüm güvenlik uyarılarını ve günlük kayıtlarını (logları) tek bir yerde toplayan, analiz eden ve anormallikleri tespit eden merkezi güvenlik izleme sistemidir.
* **Hash Function (Karma Fonksiyonu):** Herhangi bir boyuttaki veriyi (örneğin bir parola veya dosya) sabit uzunlukta benzersiz bir karaktere (hash) dönüştüren matematiksel bir fonksiyondur. Verinin değiştirilip değiştirilmediğini kontrol etmek (bütünlük) için kullanılır.
* **V2G (Vehicle-to-Grid - Araçtan Şebekeye):** Elektrikli aracın sadece şebekeden enerji almasını (şarj) değil, aynı zamanda ihtiyaç anında aracın bataryasındaki enerjiyi şebekeye geri satmasını (deşarj) sağlayan çift yönlü teknolojidir.
* **Telemetry (Telemetri / Uzaktan Ölçüm):** Şarj istasyonundan veya mikro şebekeden uzaktaki bir merkeze (CSMS veya EMS gibi) durum verilerinin (voltaj, tüketim, sıcaklık vb.) otomatik olarak toplanıp gönderilmesi işlemidir.
* **Smart Meter (Akıllı Sayaç):** Elektrik tüketimini anlık olarak ölçen, kaydeden ve bu bilgiyi otomatik olarak merkezi sistemlere ileten gelişmiş elektronik sayaçlardır.

**Siber Güvenliğin Temel Kavramları**

* **Authentication (Kimlik Doğrulama):** Bir kullanıcının veya cihazın, iddia ettiği kişi veya cihaz olduğunu doğrulama işlemidir.
* **Authorization (Yetkilendirme):** Kimliği doğrulanmış bir kullanıcının veya cihazın hangi kaynaklara (veriler, ayarlar vb.) erişebileceğini ve hangi işlemleri (okuma, yazma, silme) yapabileceğini belirleme kuralıdır.
* **Integrity (Bütünlük):** Verilerin, iletim sırasında veya saklanırken yetkisiz kişilerce değiştirilmediğini, bozulmadığını veya kurcalanmadığını garanti etme durumudur.
* **Confidentiality (Gizlilik):** Bilginin sadece yetkili kişiler tarafından erişilebilir olmasını sağlama durumudur.
* **Availability (Erişilebilirlik / Kullanılabilirlik):** Bir sistemin veya hizmetin (örneğin şarj istasyonunun), ihtiyaç duyulduğu anda meşru kullanıcılar tarafından erişilebilir ve çalışır durumda olmasını garanti etme durumudur.
* **Non-repudiation (İnkar Edilemezlik):** Bir işlemi gerçekleştiren tarafın, bu işlemi yaptığını sonradan inkar edememesini sağlayan güvenlik özelliğidir.