EVExchange – Tersine Şarj Etme Anomali Senaryosu

Ortam ve Önyargılar

Bir şehirde dağıtılmış şarj istasyonları (CS) var, hepsi ISO 15118 uyumlu ve V2G özelliğini destekliyor.

Kullanıcılar (araç sahipleri) şarj istasyonuna gidip aracını bağlıyor, protokol üzerinden kimlik doğrulaması, ödeme ve şarj parametreleri alışverişi yapılıyor.

Bazı şarj istasyonları ters akış (reverse charging / bidirectional flow) destekliyor: araçtan şebekeye enerji verilebiliyor.

Beklenen sistem davranışı: araç ile istasyon arasında güvenli, doğrulanmış iletişim kurulur; yalnızca araç sahibi öder; ters akış kullanılıyorsa bu ancak kullanıcının izniyle olur.

Saldırganın Amaçları

Saldırgan, başka bir kullanıcının araç şarjını kendi aracı için kullanmak istiyor — yani bir nevi "bedava enerji çalma".

Eğer ters akış aktifse, o aracın bataryasından enerji çekip satmak (veya başka bir araca aktarmak) amacında olabilir.

Amaç: ekonomik kazanç elde etmek, mağdurun bataryasını tüketmek veya bedava enerji almak.

Saldırı Aşamaları / Teknik Uygulama

Konum Yerleşimi / Relay Cihazı

Saldırgan, hedef aracın şarj ettiği CS noktasında sinyal iletimini yakalayabilecek bir "ortam cihazı" (relay cihazı) yerleştirir.

Bu cihaz, araç ile şarj istasyonu arasındaki iletişimi manipüle etmek üzere sinyal seviyesini artırıp iletir.

İletişim Araya Girme (Relay) / Zaman Kaydırma

Hedef araç, CS ile normal protokol mesajlarını gönderirken, bu mesajlar saldırgan cihaz aracılığıyla iletilir.

Saldırgan, istemci (araç) ile istasyon arasındaki mesafeyi (ve dolayısıyla zamansal gecikmeyi) manipüle etmeye çalışır (distance bounding saldırısı denen savunma mekanizmasını atlatmak üzere).

Enerji Yönlendirme

Saldırgan cihaz, mesajları değiştirir; örneğin istasyonla yaptığı "charge session"u, saldırganın aracıyla ilişkilendirilecek şekilde "müşteri kimliği"ni değiştirir.

Böylece istasyon, saldırgan aracı için enerji vermeye başlar; mağdurun aracı enerji almakta kalırken, enerji bedelini mağdur öder.

Ters Akış Durumu (Var ise)

Eğer ters akış aktifse, saldırgan cihaz, mağdur aracın bataryasından enerji çekilmesine izin veren komutları sokar.

Böylece mağdurun bataryası boşalır; saldırgan bu enerjiyi sisteme satabilir ya da kendi aracı için kullanabilir.

Ödeme Sapması

Ödeme ve ücretlendirme modülü, protokol mesajlarının değiştirilmesi sayesinde saldırgan “oturum”u kendine yönlendirir.

Mağdur, ödeme bildirimi alırken aslında saldırgan aracın enerji kullanımını öder.

Anomali / Beklenmeyen Davranış

Sistemde olması beklenen:

- Araç ile CS arasında doğrudan, doğrulanmış değişiklik yapılmayan mesajlar.
- Mesafe/zaman kontrollerinin (distance bounding) geçilmesi halinde iletişimin iptal edilmesi.
- Her şarj oturumunun araç kimliği ve ödeme kimliğiyle eşlenmiş olması.

Anormal durum (saldırı sonucu):

- Araç ile CS arasındaki kimlik eşlemesi tutarsızlığı: CS, ödeme ve oturum açısından saldırganın aracı ile ilişkili davranır, ama enerji çıkışı başka araçta gerçekleşiyordur.
- Mesafe / zaman kontrolü zayıf geçiliyor: geçici gecikmeler, beklenmeyen round-trip süreleri gözlenir.
- Enerji yöneliminde ters akışta ters yönde enerji akışı algısı: mağdurun bataryası boşalıyor, ama kullanıcı bunu beklemiyordur.
- Oturumda “fatura / kullanım detayları” ile enerji aktarımı tutarsızdır: kullanıcının faturasında belirtilenden daha fazla enerji aktarımı vardır, ya da araca gönderilen enerji ile faturadaki miktar uyuşmaz.

İzlenebilir Göstergeler / Algılama Kriterleri (İzlenmesi Gereken Anomali İşaretleri)

- Mesafe / zaman tutarsızlığı (örneğin protokol bazlı zaman gecikmesi sapmaları).
- Oturum kimliği değişimi veya oturum mesajlarının kimlik/sessyon tutarsızlığı.
- Enerji aktarım raporları ile ödeme raporlarının uyuşmazlığı.
- Ters akış komutlarının beklenmeyen zamanı, tutarsızlık.
- Loglar: iletişim kanalında gelen mesajların imzaları doğrulanamaması; oturum protokol mesajlarında beklenmeyen değerler ya da tekrarlar.

Kaynak Makale (Dayanak)

- Başlık: EVExchange: A Relay Attack on Electric Vehicle Charging System •
- Yazarlar: Mauro Conti, Denis Donadel, Radha Poovendran, Federico Turrin
- • Yayın Yılı: 2022 ArXiv
- • Linki: https://arxiv.org/abs/2203.0526