ANOMALİ SENARYO RAPORU — ADAPTİF ÖRNEKLEME MANİPÜLASYONU (Sampling Manipulation)

Ders: Bilgi Sistemleri Güvenliği
Proje: Şarj İstasyonlarının Güvenliği
Tarih: 09.11.2025
Hazırlayan: İbrahim Kerem Güven (Takım 10)

RAPOR ve GEREKSİNİMLER (Requirements-focused)

Bu doküman, adaptif örnekleme manipülasyonu anomalisini test etmek, tespit etmek ve azaltmak için gerekli **işlevsel** ve **işlevsel olmayan** gereksinimleri (requirements) açık, ölçümlenebilir ve uygulanabilir biçimde listeler. Her gereksinim için kabul kriterleri, veri gereksinimleri, telemetri isteği, log formatı ve test senaryosu eşleştirmeleri verildi.

---

1) Yük Kapsamı & Hedef

- **Amaç:** CP/gateway kaynaklı örnekleme manipülasyonlarını tespit edebilmek için CSMS, CP ve araç/BMS tarafında hangi gereksinimlerin yerine getirilmesi gerektiğini belirlemek.
- **Hedef kitle:** Sistem mühendisleri, güvenlik ekipleri, test mühendisleri, SIEM yöneticileri.

---

2) Özet (Kısa)

- Sistemin başarısı, manipülasyonlu oturumların %95 ve üzeri tespit edilmesine; yanlış alarm oranının %3 altında tutulmasına; ve alarm latency'sinin 10 saniyeyi aşmamasına bağlıdır. Bu hedefler gereksinimlerin uygulanmasıyla sağlanır.

---

3) İşlevsel Gereksinimler (Functional Requirements)

Her gereksinim `R-Fx` şeklinde numaralandırıldı. Kabul Kriterleri (AK) ve Test Senaryosu (TS) ile birlikte verilmiştir.

R-F1 — Örnekleme Telemetri Raporlama

Açıklama: CP her 1 dakika içinde `raw_sample_count` ve `sent_sample_count` telemetri alanlarını CSMS'e göndermelidir.

- **AK:** CSMS, her 5dk içinde her CP için `samples_per_minute` hesaplayabilmelidir. (>=95% doğruluk)
- **TS:** S1 (sampling düşürme) ile doğrula.

R-F2 — Minimum Örnekleme Politikası

Açıklama: Her CP firmware'inde `min_sampling_rate` parametresi bulunmalı; bu parametre CA tarafından imzalanmış olmalı ve CP bu alt sınırın altına inememelidir.

- **AK:** Denemede CP, imzalı min_sampling_rate altına düştüğünde CSMS alarm üretir ve CP forced_offline moduna gider.
- **TS:** Firmware parametre bypass denemesi.

R-F3 — Rolling Variance & Percentile Hesabı

Açıklama: CSMS, her aktif seans için `rolling_variance(N=60)` ve `P95/P99` hesaplayabilmelidir.

- **AK:** Geçmiş bazlı `historical_variance` ile kıyaslama yapılabilmeli; %30 azalma tespitinde alarm tetiklenmeli.
- **TS:** S2 (peak smoothing) ile doğrula.

R-F4 — Raw vs Sent Tutarlılık Kontrolü

Açıklama: CSMS, CP'den gelen `raw_sample_count` ile alınan `sent_sample_count` arasındaki farkı sürekli izlemelidir.

- **AK:** `raw_sample_count - sent_sample_count > RAW_DIFF_THRESHOLD` durumunda otomatik alarm ve evidence snapshot alınmalı.
- **TS:** S3 (buffer manipülasyonu) ile doğrula.

R-F5 — Çapraz Doğrulama (Araç/BMS)

Açıklama: Sistem, mümkünse araç/BMS kaynaklı enerji raporlarını kabul edip CSMS verileriyle otomatik karşılaştırma yapabilmelidir.

- **AK:** Enerji farkı `> ENERGY_DIFF_THRESHOLD` ise alarm.
- **TS:** S4 (araç/BMS karşılaştırması).

R-F6 — Forensic Artefakt Toplama

Açıklama: Her alarmda otomatik olarak pcap, signed-log, cp-config snapshot ve firmware hash toplanmalı.

- **AK:** Forensic artefakt seti 1 saat içinde erişilebilir depoda arşivlenmiş olmalı.
- **TS:** Her senaryo çalıştırıldığında artefakt setinin varlığı kontrol edilir.

---

4) İşlevsel Olmayan Gereksinimler (Non-functional Requirements)

Her gereksinim `R-NFx` ile numaralandırıldı.

R-NF1 — Performans

- **Açıklama:** SIEM/CSMS, 1000 eşzamanlı CP'den gelen telemetriyi işleyebilmelidir.
- **AK:** Telemetri işleme latency'si < 2s (ön işleme), alarm latency ≤10s.

R-NF2 — Güvenlik

- **Açıklama:** Telemetri ve veriler WSS+mTLS ile taşınmalı; tüm loglar imzalanmış (HMAC/ECDSA) olarak saklanmalıdır.
- **AK:** Geçersiz imza ile gelen telemetri reddedilmeli ve alarm üretmeli.

R-NF3 — Güvenilirlik ve Dayanıklılık

- **Açıklama:** Forensic artefaktları WORM storage veya write-once mekanizma ile saklanmalı.
- **AK:** 90 gün içindeki olayların tamamında artefaktlar doğrulanabilmeli.

R-NF4 — Ölçeklenebilirlik

- **Açıklama:** System, artan CP sayısına yatay olarak ölçeklenebilmeli (kubernetes/eks gibi).
- **AK:** Her 10K CP artışında ek node ile otomatik scaling gösterilmesi.

---

5) Veri Gereksinimleri & Telemetri Şeması

Açık ve indekslenebilir alanlar tanımlandı — SIEM sorguları için zorunludur.

`telemetry_sample` JSON şeması (zorunlu alanlar):

```
{
  "timestamp":"<ISO8601>",
  "cp_id":"<CP-xx>",
  "session_id":"<sess-...>",
  "raw_sample_count":<int>,
  "sent_sample_count":<int>,
  "samples_per_minute":<int>,
  "power_sample_stats":{
    "mean":<float>,
```

```
    "variance":<float>,
    "p95":<float>,
    "p99":<float>
  },
  "fw_hash":"<sha256:...>",
  "telemetry_sig":"<hmac/ecc_sig>"
}
```

İndekslenebilir alanlar: `cp_id`, `session_id`, `samples_per_minute`, `variance`, `raw_sample_count`, `sent_sample_count`, `anomaly_flags`.

---

6) Güvenlik Gereksinimleri (Security Requirements)

- **R-S1:** mTLS zorunlu; client cert revocation (CRL/OCSP) kontrolü aktif.
- **R-S2:** Telemetri ve loglar HSM/KMS tarafından imzalanmalı.
- **R-S3:** Firmware signing + Secure Boot zorunlu.
- **R-S4:** SIEM erişimi RBAC ile sınırlandırılmalı; forensics artefaktlarına erişim logging'e tabi olmalı.

---

7) Kabul Kriterleri & Test Matriksi

Kısa bir tabloyla gereksinimler ve eşleşen test senaryoları:

- R-F1 → TS: S1
- R-F2 → TS: Firmware bypass testi
- R-F3 → TS: S2
- R-F4 → TS: S3
- R-F5 → TS: S4
- R-F6 → TS: Her senaryo

Kabul kriterleri özet: Tespit ≥ %95, False Positive ≤ %3, Alarm latency ≤10s, Artefakt seti mevcut.

---

8) Uygulama Adımları (Requirements-First Yaklaşımı)

1. **Telemetri şemasını canlıya al:** CP firmware/agent telemetri alanlarını etkinleştir. (R-F1)
2. **Minimum sampling parametresini imzala ve zorunlu kıl:** İç CA ile imzalanmış parametreyi dağıt. (R-F2, R-S2)
3. **CSMS ölçüm modüllerini aktive et:** rolling_variance, percentile hesapları. (R-F3)
4. **SIEM kural setini yükle:** K1-K3 tabanlı ve samples_per_minute uyarıları. (R-F4)
5. **Forensic pipeline:** pcap ve signed-log otomasyonu sağla. (R-F6)
6. **Baseline topla:** 24–72 saat normal trafik. (Kabul testi için).
7. **Senaryoları yürüt ve K-FR gereksinimlerini doğrula:** S1–S4.

---

9) Test Senaryoları (Kısaca)

- **S1:** Sampling düşürme → R-F1,R-F2 doğrulaması.
- **S2:** Peak smoothing → R-F3 doğrulaması.
- **S3:** Buffer manipulation → R-F4 doğrulaması.
- **S4:** Araç/BMS karşılaştırması → R-F5 doğrulaması.

Her test sonrası SIEM sorguları, pcap ve signed-log toplanmalı; test raporu üretilecek.

---

10) Raporlama ve İzleme Gereksinimleri

- **R-R1:** Dashboard: samples_per_minute, variance, anomaly score, alarms per CP.
- **R-R2:** Haftalık özet rapor: tespit oranı, yanlış alarm oranı, ortalama alarm latency.
- **R-R3:** Olay sonrası (post-incident) rapor şablonu ve şüpheli CP takibi.

---

11) Forensic & Kanıt Gereksinimleri

- **F-1:** Her alarm için pcap + signed-log + fw_hash + cp-config snapshot.
- **F-2:** Artefaktların korunması: WORM veya imzalı arşiv.

---

12) Kabul Testleri & Başarı Ölçütleri (Tekrar)

- Manipülasyonlu senaryoların ≥ %95 tespiti.
- Yanlış alarm ≤ %3.
- Alma → alarm latency ≤ 10s.

---

13) Ekler / Kaynaklar

- Farokhi, F. (2020). Review of results on smart-meter privacy by data manipulation, demand shaping, and load scheduling. IET Smart Grid.
- Giaconi, Gunduz, Poor (2018). Privacy-Aware Smart Metering: Progress and Challenges. IEEE Signal Processing Magazine.
