ANOMALİ SENARYOSU RAPORU

Hazırlayan: Betül ALTUNYUVA

Senaryo Adı

Anahtar Yeniden Kullanımı ve Zayıf KDF ile Telemetri Çözülmesi (Key Reuse → Telemetry Decryption & Falsification)

Özeti

Sistem, CP'lerden CSMS'e giden hassas telemetri ve durum mesajlarını simetrik şifreleme (ör. AES-CBC) ile koruduğunu iddia etmekte; fakat cihazlarda ve CSMS'de aynı simetrik anahtarların tekrar kullanılması, zayıf/tek adımlı KDF (key derivation) ve sabit IV/nonce kullanımı nedeniyle bir saldırgan, şifreli trafiğin istatistiksel analizinden anahtar türetme, telemetri içeriğini çözme ve sonrasında sahte/bozulmuş telemetri göndererek sistem davranışını manipüle etme imkânı bulur.

Amaç

- Zayıf anahtar yönetiminin (key reuse) ve yetersiz anahtar türetme fonksiyonlarının (zayıf KDF/PBKDF) telemetri gizliliğini ve bütünlüğünü nasıl tehlikeye atabileceğini göstermek.
- Telemetri doğruluğunun ve merkezi karar mekanizmalarının (faturalama, alarm, yük yönetimi) zafiyetten nasıl etkilendiğini ortaya koymak.
- Güçlü anahtar yönetimi, nonce kullanım politikası ve uygun KDF uygulamalarının önemini öğretmek.

Kapsam

- **Dahil:** Cihaz içi simetrik şifreleme (firmware'de gömülü anahtar), CSMS'de saklanan simetrik anahtar/kopyaları, telemetri mesaj formatı (sampledValue payload), anahtar türetme yöntemi, IV/nonce kullanımı.
- **Hariç:** Asıl fiziksel sayaç donanımı kırılması, tedarikçi sunucu güvenliği (yalnızca şifreleme kullanım modeli incelenir).

Hedefler ve Tehdit Modeli

- **Hedef Varlıklar:** Şifreli telemetri paketi akışı; anahtar depolama/şifre çözme modülü; telemetri işleyen faturalama/otomasyon pipeline'ı.
- **Saldırgan Yetkinliği:** Orta. Ağ pozisyonu (MitM veya trafik yakalama) ve kriptanaliz / istatistiksel analiz bilgisi; ayrıca cihazın firmware binary'sinden anahtar doğrultusunda ipucu çıkarabilme (side-info) mümkünse avantajlı.
- **Ön-koşullar / Zayıflıklar:**
    - Cihazlarda ve CSMS'de **aynı** veya deterministik şekilde türetilmiş simetrik anahtar kullanımı (key reuse across sessions/devices).
    - Zayıf KDF (örn. tek-round hash veya salt yok), PBKDF veya HKDF yerine direkt parola → anahtar dönüşümü.
    - IV/nonce'in sabit veya tekrarlanan kullanımı (ör. tüm mesajlar için IV=0 veya nonce counter kötü yönetimi).
    - Mesajlara ek bir HMAC/signature konmaması (sadece şifreleme ile bütünlük bekleniyor).

Adım Adım Saldırı Akışı

1. **Keşif:** Saldırgan CP ↔ CSMS trafiğini pasif olarak yakalar (pcap). Firmanın dokümantasyonu veya firmware örnekleri üzerinden şifreleme parametrelerini (algoritma, IV davranışı, anahtar kökeni) belirler.
2. **Analiz:** Yakalanmış çok sayıda şifreli paket üzerinde istatistiksel analiz yapar — aynı IV'ler, blok tekrarları, ciphertext-tekrar desenleri ve known-plaintext şablonları tespit eder.
3. **Anahtar Tahmini / Kırma:** IV/nonce tekrarları ve key reuse durumunda, XOR/crib-dragging, blok-tekrar atacığı veya basit KDF zayıflığı kullanılarak simetrik anahtarın veya kısmi anahtar bilginin türetilmesi denenir. (Laboratuvarda örnek veri ile anahtar kurtarma mümkündür.)
4. **Telemetri Çözme:** Elde edilen anahtar ile şifreli telemetri çözülür; idTag, transactionId, sample değerleri okunur.
5. **Manipülasyon:** Aynı anahtarla veya anahtarı yeniden türeterek sahte telemetri paketleri oluşturulur (ör. gerçek sample'ları düşürme/çoğaltma, cihazı offline gösterme). Bu paketler CSMS'e gönderilip sistemin faturalama/alarmlarını yanıltır.
6. **Kalıcılık:** Eğer anahtar firmware'e gömülü ise veya deterministik türetme sürüyor ise saldırgan aynı yöntemi tekrar kullanarak uzun süre etkili olabilir.

Beklenen Etkiler

- **Bütünlük/Doğruluk Bozulması:** Faturalama ve raporlama sistemleri yanlış telemetriye göre karar alır — gelir kaybı veya yanlış operasyonel kararlar.
- **Gizlilik İhlali:** Token/kimlik/veri sızması ile müşteri gizliliği ihlali.
- **Süregelen Erişim:** Anahtar kurtarıldıysa saldırgan sistemde kalıcı manipülasyon yapabilir (ör. faturalama periyotlarında düzenli düşük bildirim).
- **Güven ve Uyum:** Regülatif yükümlülüklerin (doğru ölçüm ve faturalama) ihlali, itibar kaybı.

Tespit Metodları

1. **Ciphertext Analizi & Repetition Detection:** SIEM/flow-collector üzerinde aynı IV veya aynı ciphertext-blok tekrarlarını algılama; yüksek tekrarlama olması key reuse/IV reuse için IOC'dur.
2. **Entropy ve Block Correlation Testleri:** Her blokun entropi dağılımı ve bit korelasyon testi; sabit IV/nonce ile CBC bloklarında belirli korelasyonlar ortaya çıkar.
3. **Message Frequency / Pattern Monitoring:** Aynı tip mesajların (ör. heartbeat, meter sample) ciphertext boyut/structure'unda anormal sabitlik (normalde random-like olmalı).
4. **Known-Plaintext Probing:** Test cihazları kullanarak known-plaintext'ler gönderip ciphertext çıktısını toplayarak deterministik davranışı test etme (laboratuvar).
5. **Key Management Audit:** Anahtar rollover sıklığı, KDF parametreleri (salt, iterations) ve storage (secure element, HSM) kontrolleri ile doğrudan yönetim zafiyeti tespiti.
6. **Anomali Korelasyonu:** Telemetri ile fiziksel sayaç/cross-check (gateway raw data) uyuşmazlıkları; ör. cihazın fiziksel logları ile CSMS raporları uyumsuzsa uyar.

Önleme Yöntemleri

Anahtar & KDF Politikaları

- **Her session/cihaz için benzersiz anahtar** (no key reuse): Anahtarlar asla global veya deterministik olarak yeniden kullanılmamalı. Cihaz başlatma sırasında

cihaz-unique secret ile HSM destekli KDF (HKDF veya PBKDF2/Argon2 with high iterations + unique salt) kullanılmalı.

- **Güçlü KDF kullanımı:** PBKDF2/Argon2/HKDF gibi modern, parametrelenebilir KDF'ler; yeterli iteration ve per-device salt zorunlu.
- **Secure Key Storage:** Anahtarlar secure element / TPM / HSM içinde saklanmalı; firmware'e gömülü düz metin anahtar kesinlikle yasak.
- **Nonce/IV Yönetimi:** Her mesaj için **unique, unpredictable IV/nonce** kullanılmalı; CBC ise IV rastgele, GCM ise nonce uniqueness garanti edilmeli. Asla sabit IV kullanmayın.
- **Authenticated Encryption:** Sadece şifreleme değil, **AEAD** (AES-GCM, ChaCha20-Poly1305) kullanın — hem gizlilik hem bütünlük sağlar.
- **Key Rotation & Revocation:** Anahtarların düzenli rotasyonu, hızlı revocation mekanizması ve CSMS/cihaz senkronizasyonu.
- **Telemetry Cross-Validation:** Telemetry ile gateway raw verisini düzenli olarak karşılaştıran otomatik korelasyon; sapma olduğunda anahtar/şifreleme kontrolü tetiklensin.
- **Code/Firmware Denetimi:** Firmware'lerde gömülü anahtar veya deterministik KDF uygulamalarını tespit eden statik analiz süreçleri.
- **Logging & Forensics:** Encryption-related metadata (IV, cipher, KDF params hash) merkezi loglanmalı; WORM saklama ile adli inceleme imkanı.