

OPC UA güvenliği: modlar, sertifikalar ve güven listeleri

OPC UA bağlantısını “çalışıyor” diye bırakmayın. Güvenlik modunu, sertifika güvenliğini ve kullanıcı kimlik doğrulamasını ayrı kararlar olarak alın.

Kısaca

- Bir OPC UA bağlantısı şifreli olsa bile anonim bir kullanıcıyla açılabilir, bu yüzden güvenlik modu ve kullanıcı doğrulaması ayrı kontrol edilmelidir.
- Güvenlik modu “hiçbiri” olduğunda üretim ağında mesajlar okunabilir ve değiştirilebilir kalır, kullanılan güvenlik ilkesi ise sunucu ve istemcide desteklenmelidir.
- Bir sertifikayı güven listesine eklemek o uygulamaya erişim vermek demektir, bu yüzden sahibi doğrulanmadan otomatik kabul edilmemelidir.

01 / Üç ayrı karar

OPC UA’da iletişim güvenliği (kanalın imzalanması ve şifrelenmesi), uygulama kimliği (sertifikalar) ve kullanıcı kimlik doğrulaması ayrı kavramlardır. Bir bağlantı şifreli olabilir ve yine de anonim kullanıcıyla açılmış olabilir. Her birini kendi kontrol listesiyle ele alın.

02 / Güvenlik modu

Güvenlik modu üç değer alır: hiçbiri, yalnızca imza, imza ve şifreleme. “Hiçbiri” modu laboratuvar denemesinde işe yarar, ancak üretim ağında mesajları okunabilir ve değiştirilebilir bırakır. Kullandığınız güvenlik ilkesinin (algoritma seti) sunucu ve istemci tarafından desteklendiğini, eski ve zayıf ilkelerin kapatıldığını belgeleyin.

03 / Sertifikaları yönetin

Her uygulama örneği bir sertifika taşır. Bir sertifikayı güven listesine eklemek, o uygulamaya erişim vermek demektir. Sertifikayı sahibini doğrulamadan otomatik kabul etmeyin. Son kullanma tarihlerini izleyin; süresi dolan bir sertifika üretim hattında beklenmedik bir veri kesintisine dönüşebilir.

04 / Yapay zekâ için okuma hesabı

Veri bilimi ekibi için ayrı, salt okunur bir kullanıcı ve mümkünse ayrı bir uygulama sertifikası kullanın. Yazma yetkisi olmayan bir okuma hesabı, hatalı bir modelin sahadaki bir ayarı değiştirmesini engeller. Bu rehber, önerilen bir güvenlik çalışma biçimidir ve bir sertifikasyon ya da uygunluk iddiası içermez.

Uygulayın

Kendi OPC UA sunucunuzdaki uç noktaları listeleyin ve her birinin güvenlik modunu ile kabul ettiği kullanıcı türlerini tabloya yazın.

Kaynaklar ve çevrimiçi rehber

Güncel çevrimiçi rehberi açın

OPC Foundation: OPC UA

Önerilen pilot adımları saha doğruluk iddiası içermez. Sentetik örnekler gerçek tesis ölçümü değildir.