Denetci.org

REFERANS İLKELERİ

Mobil Uygulama Güvenliği İlkeleri

Rİ-YAZ-3

Sürüm 1.0 · 11.08.2026

www.denetci.org

Mobil Uygulama Güvenliği İlkeleri

Mobil uygulama güvenliği; uygulama, mobil cihaz, işletim sistemi, kullanıcı, arka uç hizmetleri ve cihaz üzerinde işlenen veriler arasındaki güven ilişkilerini ele alır. Amaç belirli bir mobil platform veya koruma teknolojisi belirlemek değil; cihazın kaybolabileceği, değiştirilebileceği, uygulama kodunun incelenebileceği ve istemcinin saldırganın kontrolüne girebileceği kabulü altında güvenilir bir uygulama tasarımı oluşturmaktır.

İlke 1: Mobil cihaz güvenilir bir sunucu ortamı gibi kabul edilmemelidir.

Uygulama, sahibinin veya saldırganın fiziksel ve teknik olarak önemli ölçüde kontrol edebildiği bir ortamda çalışır. Kritik güvenlik kararları, cihazın veya uygulamanın amaçlandığı biçimde çalışmaya devam edeceği varsayımına bırakılmamalıdır.

İlke 2: Uygulama kodunun ve çalışma mantığının gizli kalacağı varsayılmamalıdır.

Mobil uygulama paketleri edinilebilir, incelenebilir ve çalışma zamanında değiştirilebilir. Bir güvenlik özelliğinin değeri saldırganın onun nasıl çalıştığını öğrenememesine bağlı olmamalıdır.

İlke 3: Mobil istemcide uygulanan sınırlar tek başına gerçek güvenlik sınırı olmamalıdır.

Bir işlevin arayüzden kaldırılması, bir isteğin uygulama tarafından gönderilmemesi veya belirli bir kontrolün cihaz üzerinde yapılması saldırganın aynı işlemi başka biçimde gerçekleştiremeyeceğini göstermez. Kritik kararlar güvenilir tarafta bağımsız olarak korunmalıdır.

İlke 4: Kullanıcı, cihaz ve uygulama kimliği birbirinden ayrılmalıdır.

Resmî uygulamanın kullanılıyor olması kullanıcının yetkili olduğunu; doğrulanmış kullanıcı da cihazın veya çalışan uygulamanın güvenilir olduğunu tek başına göstermez. Bu unsurların her biri gerektiği ölçüde ayrı güven sinyalleri olarak değerlendirilebilmelidir.

İlke 5: Mobil istemciden gelen veri dış girdi olarak değerlendirilmelidir.

Uygulamanın normal arayüzü belirli değerler ve işlem sıraları üretse de saldırgan bu davranışı değiştirebilir. Arka uç güvenliği, istemcinin doğrulama yaptığı veya yalnızca izin verilen istekleri oluşturduğu varsayımına dayanmamalıdır.

İlke 6: Ağın güvenilirliği uygulamanın güvenliğinin ön koşulu olmamalıdır.

Mobil cihazlar kuruluşun kontrol etmediği ağlarda çalışabilir. Veri ve kimlik güveni, cihazın hangi kablosuz ağa veya operatör ağına bağlı olduğuna duyulan genel güvenden bağımsız kurulabilmelidir.

İlke 7: Uzak tarafın kimliği kullanılan iletişim kanalından bağımsız olarak anlamlı biçimde doğrulanmalıdır.

Bir bağlantının şifrelenmiş olması uygulamanın gerçekten amaçlanan hizmetle iletişim kurduğunu tek başına göstermez. Uygulamanın güven duyduğu uzak kimlik ve bu güvenin dayanağı açık olmalıdır.

İlke 8: İletişim güvenliği hata durumunda sessizce daha zayıf güvene dönüşmemelidir.

Bağlantı veya kimlik doğrulama mekanizması beklenen güveni sağlayamıyorsa yalnızca kullanılabilirliği sürdürmek için temel doğrulamanın etkisiz hale gelmesi olağan çalışma biçimi olmamalıdır. Daha zayıf güvene geçiş bilinçli bir tasarım kararı olmalıdır.

İlke 9: Mobil uygulamada bulunan sırlar cihazın ele geçirilemeyeceği varsayımına dayanmamalıdır.

Uygulama paketine veya cihaz üzerinde erişilebilir bir alana yerleştirilen sabit bir değer yeterli çabayla öğrenilebilir. İstemcide bulunan ortak sırlar çok sayıda kullanıcı veya sistem adına kalıcı ve geniş yetki sağlamamalıdır.

İlke 10: Oturum bilgileri kullanıcı parolası kadar gerçek erişim gücü taşıyabilir.

Geçerli bir oturum veya erişim belirteci, kullanıcı yeniden kimliğini doğrulamadan onun adına işlem yapılmasını sağlayabilir. Bu nedenle oturum güveni saklama, aktarım, süre ve sona erme bakımından bağımsız bir güven unsuru olarak ele alınmalıdır.

İlke 11: Cihazın kaybı erişimin ölçüsüz biçimde devam etmesine yol açmamalıdır.

Mobil cihazlar kaybolabilir, çalınabilir veya başka bir kişinin kontrolüne geçebilir. Cihaz üzerinde daha önce kurulmuş güven ilişkileri bu olasılık gerçekleştiğinde sınırsız süre ve etkiyle devam etmek zorunda olmamalıdır.

İlke 12: Yerel kimlik doğrulama ile uzak hizmetin kimlik kararı birbirine karıştırılmamalıdır.

Cihaz parolası, biyometri veya başka bir yerel mekanizma cihazı kullanan kişi hakkında belirli bir güven sağlayabilir. Bunun kapsamı, arka uç hizmetinin hangi kullanıcıya ve hangi yetkiye güveneceğine ilişkin kararın otomatik olarak yerine geçmemelidir.

İlke 13: Biyometrik doğrulama geri alınabilir bir sır gibi değerlendirilmemelidir.

Biyometrik özelliklerin parola gibi değiştirilmesi mümkün değildir ve uygulamanın biyometrik verinin kendisine çoğu zaman ihtiyacı yoktur. Biyometri, taşıdığı özelliklere uygun sınırlı bir güven rolünde kullanılmalı; gereksiz biyometrik veri maruziyeti oluşturmamalıdır.

İlke 14: Cihaz üzerinde hassas veri yalnızca gerçek bir ihtiyaç kadar bulunmalıdır.

Yerel olarak saklanan her hassas veri cihaz kaybı, yedekleme, kötü amaçlı yazılım veya cihazın ele geçirilmesi halinde yeni bir kayıp alanı oluşturur. Çevrimdışı kullanım veya başka anlamlı bir ihtiyaç bulunmadığında veri gereksiz biçimde istemciye taşınmamalıdır.

İlke 15: Yerel verinin yaşam döngüsü yalnızca ana uygulama depolamasıyla sınırlı değildir.

Önbellekler, geçici dosyalar, yedekler, ekran önizlemeleri, bildirimler, pano ve işletim sisteminin başka özellikleri uygulama verisinin yeni kopyalarını oluşturabilir. Geçici veya sistem tarafından oluşturulan kopyalar veri güvenliğinin dışında kabul edilmemelidir.

İlke 16: İşletim sisteminin sağladığı korumalar uygulamanın kendi güven sınırlarının yerine geçmemelidir.

Uygulama alanı ayrımı, güvenli saklama ve diğer platform özellikleri önemli savunmalar sağlayabilir; ancak yanlış yapılandırılabilir veya bazı saldırı koşullarında aşılabilir. Uygulama güvenliği tek bir platform varsayımının kusursuzluğuna bağlı olmamalıdır.

İlke 17: Uygulamalar arası etkileşim gerçek bir güven sınırı olarak görülmelidir.

Bağlantılar, dosya paylaşımı, mesajlaşma mekanizmaları ve dışarıdan çağrılabilen uygulama bileşenleri başka uygulamaların veri göndermesine veya işlem başlatmasına izin verebilir. Bu yollar, normal kullanıcı arayüzünün gizli uzantıları olarak değil bağımsız dış girişler olarak değerlendirilmelidir.

İlke 18: Web içeriği ile yerel uygulama yetkileri birbirine gereksiz biçimde aktarılmamalıdır.

Uygulama içinde gösterilen web içeriği dış kaynaklardan gelebilir ve web ortamının farklı güven özelliklerine sahiptir. Web içeriğinin yerel dosya, cihaz özelliği veya uygulama işlevlerine erişmesi gerekiyorsa bu ilişki gerekli işlev ve kapsamla sınırlı olmalıdır.

İlke 19: Mobil platform izinleri gerçek kullanım ihtiyacını aşmamalıdır.

Bir uygulamanın teknik olarak bir cihaz yeteneğine erişebilmesi o yeteneğin bütün kullanım süresi boyunca gerekli olduğu anlamına gelmez. Kullanıcıdan alınmış bir izin, verinin her amaçla ve sınırsız süreyle kullanılabileceği şeklinde yorumlanmamalıdır.

İlke 20: Cihaz bütünlüğüne ilişkin sinyaller mutlak güven kanıtı olarak görülmemelidir.

Cihazın değiştirilmiş olup olmadığı, uygulamanın beklenen kaynaktan gelip gelmediği veya çalışma ortamının bütünlüğü değerli güven sinyalleri sağlayabilir. Ancak bu sinyaller aşılabilir veya hatalı olabilir; tek başına kullanıcı yetkisinin ya da işlemin meşruluğunun yerine geçmemelidir.

İlke 21: Üçüncü taraf mobil bileşenleri uygulamanın gerçek güven sınırının parçasıdır.

SDK'lar, kütüphaneler ve dış hizmetler uygulama içinde kod çalıştırabilir, veri işleyebilir veya yeni ağ bağlantıları oluşturabilir. Üçüncü taraf tarafından sağlanmaları, uygulamanın veri ve güvenlik sonuçları üzerindeki etkilerini ortadan kaldırmaz.

İlke 22: Güncelleme yeteneği uygulamanın güvenlik yaşam döngüsünün parçası olmalıdır.

Bir mobil uygulamanın güvenliği yalnızca yayımlandığı andaki durumuna bağlı değildir. Eski sürümlerin ne ölçüde kullanılabildiği, yeni sürümün güvenilir biçimde edinilip edinilemediği ve güvenlik değişikliğinin kullanıcıya gerçekten ulaşabilmesi tasarımın parçasıdır.

İlke 23: Eski istemciler yeni güven sınırlarını süresiz biçimde aşmamalıdır.

Arka uç güvenliği zaman içinde değişebilir; eski uygulama sürümleri ise geçmiş davranışları taşımaya devam edebilir. Eski istemciler desteklenmeye devam ettiği ölçüde gerçek sistemin güvenlik düzeyinin bir parçası olarak değerlendirilmelidir.

İlke 24: Mobil uygulama güvencesi yalnızca uygulama paketinin incelenmesine dayanmamalıdır.

Uygulamanın gerçek güvenliği cihaz, işletim sistemi, arka uç, ağ, oturum, veri ve üçüncü taraf bileşenlerinin birlikte davranışından doğar. Güvence, değiştirilebilen bir istemci karşısında bu sınırların gerçekten korunup korunmadığı üzerinden doğrulanabilmelidir.