Güvenli Bir akıllı kartta bulunması gereken güvenlik önlemleri

Anomali sensörleri

Akıllı kartlarda anormal durumları sezmek için çok sayıda donanımsal anomali sensörü yer almaktadır. Bu sensörler karta uygulanan gerilim, saat işareti, sıcaklık, ışık gibi etmenlerin tanımlı alt ve üst limitlerin dışında olduğu anormal bir durum sezdiğinde, kart yongası bu durum ortadan kalkana kadar çalışmasını keserek kendini güvenli duruma alır (reset durumu). Bu sensörler sayesinde UV ışığı kullanarak EEPROM'un silinmesi, saat işaretinin kesilmesi gibi saldırılara karşı koruma sağlanmış olur.

Akıllı kart yongasının güvenlik önlemleri

Akıllı kart yongalarında yonganın yüzeyinin kazılarak analiz edilmesini önlemek için değişik yöntemler uygulanmaktadır. İlk olarak önemli bloklar yongaya rasgele yerleştirilirler. Bir başka yöntemde mikroişlemcinin lazerle kesilmesi saldırısına karşı yonganın üzerine ikinci bir metal tabaka konarak yonganın özelliklerinin ortaya çıkması engellenir. Güçlü akıllı kart yongalarında, yonga yüzeyinden değerli verileri okumayı engellemek için etkin kalkan (active shield) olarak adlandırılan bir mekanizma kullanılmaktadır. Bu mekanizmada yonga yüzeyinde gelişigüzel dizilmiş ve rasgele sayı üretecinden elde edilen verilerle beslenen çok ince veri yolları bulunmaktadır. Etkin kalkan mekanizması bu veri yollarındaki değişken verilerin doğruluğunun denetlenmesi prensibine göre çalışmaktadır. Eğer bu yüzey aşındırılacak olursa veri yollarındaki veriler hatalı olacağından yonga kendisini güvenli konuma sokar.

Akıllı kart işletim sisteminin güvenlik önlemleri

• Algoritmaların işlem süreleri sabitlenerek yan kanal analizleri ve zamanlama analizleri ile gizli bilginin açığa çıkarılması önlenir. Eğer herhangi bir işlemin gerçekleşme süresi gizli bilginin içeriğine bağlı olarak değişiyorsa, bu bilgi güç analizi ile ortaya çıkabilir. Bu nedenle giriş değerleri ne olursa olsun işlem süreleri sabit tutulmalıdır. Bunun için gerekiyorsa algoritmanın değişik noktalarına rasgele gecikmeler eklenir.

• Güvenlik açısından önemli olan verilere (anahtarlar, PIN, PUK, vs) toplama sınaması konularak verinin bütünlüğü denetlenir. Herhangi bir nedenle bütünlük bozulduğunda kart kendini korumaya alır.

• Algoritmalarda gerçeklenen işlemlerin işleyiş sırası değiştirilerek algoritmanın ne yaptığının saptanması güçleştirilir.

• Algoritmalarda gerçekleştirilen karşılaştırma işlemleri gibi kritik işlemlere çift kontrol konulup sonuçlar karşılaştırılarak hata enjeksiyonunun önüne geçilebilir.

• Güvenlik açısından önemli verilerin birden fazla kopyası birden fazla formda tutularak (verinin üssü, vs) verinin değiştirilmesi durumu sezilebilir.

• Yan kanal analizlerinde yanlış PIN girilmesi sonucu PIN hata sayacının azaltılma işlemi tespit edilip o sırada güç kesilerek hata sayacının azaltılması engellenebilmektedir. PIN doğrulaması yapılırken PIN'in doğruluğuna bakılmadan sayaç azaltılıp PIN doğru girilirse eski değerine çekilerek bu saldırı önlenebilir