KARTLI VE ŞİFRELİ KAPI SISTEMLERINDE GÜVENLİK ZAFİYETLERİNİN TESPITI

Fatma DEMİREL





PROJENIN AMACI

Fakültemizin sekiz adet kartlı ve şifreli giriş kapısı bulunmaktadır. Proje amacı bu kapıların güvenlik zafiyetlerinin tespitidir.

DÜŞMANI TANIMAK ONU YENMENİN İLK ADIMIDIR.

Sun Tzu

Kartlı ve Şifreli Kapı Sistemlerinin Özellikleri

Fakültemiz de kullanılan kapı sistemleri hem şifreli geçişe hem de kart okutma yoluyla geçişe imkan tanıyor. İç ortam ile beraber dış ortamda da kullanımına olanak sağlayan IP65 özelliğine sahiptir. Aynı zamanda proximity kart okuma özelliğini barındırıyor.



Sistemin Kurulumu

Kartlı ya da şifreli giriş çıkış kontrol sistemi kurulumu yapılırken cihazın takılacağı kapıda elektrik kilit olması gerekir. Göstergeç sistemin çalışabilmesi için 12 volt adaptör kullanılır, bina giriş çıkışı için kullanılacak ise UPS özellikli bir sistem kurulması daha iyi olur, bu sayede elektrik kesintisinde kart okuyucu çalışmaya devam eder.



SISTEM ZAFİYETLERİ

- Kaba Kuvvet Saldırısı
 - Yan Kanal Saldırısı
 - Kart Kopyalanması
 - Donanımsal Erişim Zafiyeti
 - Resetleme ile Default Şifre Zafiyeti
 - Şifrenin Öğrenilme Kolaylığı

Kaba Kuvvet Saldırısı





Kaba kuvvet saldırısı, deneme yanılma yoluyla parola ve kullanıcı adlarını ele geçirme girişimidir. Bu saldırı türüyle şifrenin çözülmesi zor olsa da mümkündür. Bu yüzden sistem zafiyetleri arasındadır.

Yan kanal Saldırısı

Bilgisayar güvenliğinde yan kanal saldırısı bir bilgisayar sistemine gerçekleştirilirken şifreleme algoritmasının uygulanma şeklinin öğrenilmesinden ziyade uygulanan algoritmadaki zayıflıklara odaklanır. Fakültemizdeki kapı sistemlerinde şifreye ulaşmamızı sağlamasada yan kanal saldırısı şifredeki karakter sayısını bulmamızı sağlıyor. Bu sayede kaba kuvvet saldırısın yapılmasını kolaylaştırmış oluyoruz. Ayrıca rakamlar üzerindeki parmak izlerinden faydalanarak şifrede kullanılan rakamları belirleyebiliriz



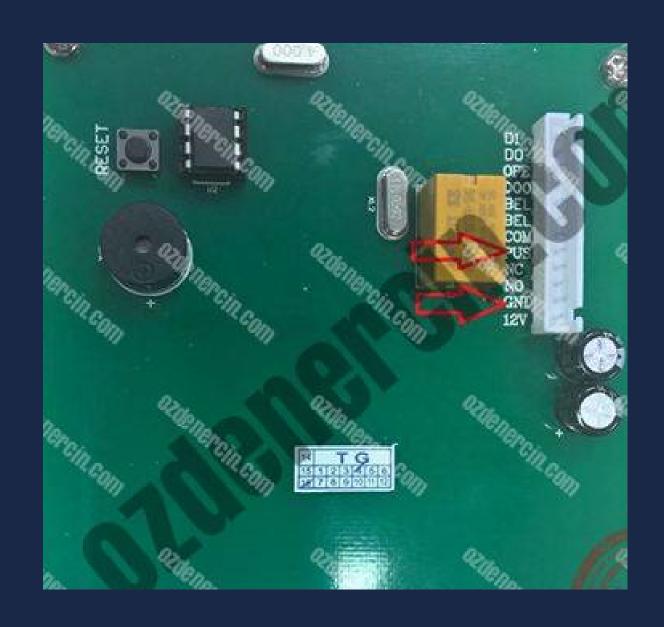
Kart Kopyalanması

Proximity ve Mifare kart okuma özelliğine sahip iki farklı tip cihaz bulur. Proximity kart okuma özelliğine sahip cihazlarda kartların kolay kopyalanabilir olmalarından kaynaklı güvenlik açığı oluşmaktadır



Donanimsal Erişim Zafiyeti

Kapı kilitlerinin ön panosunu bir vida
yardımıyla
açabiliyorsunuz ve birkaç saniye içerisinde
plakanın arkasına
ve bağlantı terminallerine erişebiliyorsunuz.
Arka bağlantı
terminallerini açtıktan sonra GND ve PUSH
bağlantılarına
kısa devre yapılırsa elektronik kilit açılır.



Resetleme ile default Şifre Zafiyeti

Kapı kilitlerinin ön panosu bir tornavidayla açıldığında plakanın arkasına, bağlantı terminallerine ve reset tuşuna erişebilir. Resetleme tuşuna baştıktan sonra keypad üzerinden "99019901" girildiğinde kapı kilidi açılır.

Şifrenin Öğrenilme Kolaylığı

Şifreyle giriş yapılırken birilerinin şifreyi görüp aklında tutması rahatlıkla giriş çıkış yapmasını sağlar. Bu da sistemdeki ciddi zafiyetlerdendir.

Ayrıca şifre girişine tanık olunamasa da şifreli geçiş sisteminin karşısına konulacak bir kamera sayesinde kolaylıkla şifre bilgisi elde edilebilir.



BENIM GÜVENLİ GEÇİŞ SİSTEMİM

Koku Ayırdediciliğiyle Çalışan Kapı Sistemi Ses Tanıma Sistemi Canlı Parmak İzi Okuyucu

Hareket Analizi Yapan Kapi Sistemiyle Yürüyüş Farklılıklarından Giriş Çıkış İzni Verilmesi