Bina Otomasyonu ve Erişim Kontrol Sistemleri

Bülent ÖNEN
ODTU Elektronik Mühendisliği eğitimi sonrası,
1986 yılında Odeonist Elektronik San. ve Tic. Ltd. Şirketini kurarak
özel iş hayatına atıldı. Güvenlik Endüstrisi Sanayicileri ve
İşadamları Derneği (GESİDER) kurucu üyesi ve sektörün ülkemizde
önderlerinden biri olarak Güvenlik Elektroniği alanında bir çok büyük projeye imza attı.

Bina otomasyonunda önemli konulardan biri olan ve bina içinde personel dolaşımının kontrolü ile güvenliğin sağlanması fonksiyonlarını da sağlayan "Erişim Kontrol Sistemleri" (Access Control System) güvenlik sistemlerinin temelini oluşturmaktadır.

TARİHÇE: Erişim kontrol Sistemleri 70'li yılların ikinci yarısında kullanılmaya başlanılmıştır. Bu yıllarda kontrol ünitelerinin üzerinde bulunan anahtarlar ve çeşitli frekanslara ayarlanmış kristaller aracılığı ile yapılan ve şimdiki sistemlere göre çok daha sınırlı yeteneklere sahip olan ilk basit sistemler, 80'li yıllarda bilgisayar donanım ve yazılımlarının gelişmesi ile çok daha kullanışlı ve yetenekli hale dönüştürülmüştür. Bu gelişim erişim kontrol sistemlerinin yazılımlarının ayni zamanda "Güvenlik Yönetim Sistemleri"ne dönüşmesi ile sistemin, güvenlik sistemlerinin temel taşlarından ve vazgeçilmez elemanlarından biri olmasını sağlanmıştır.

Erişim Kontrol Nedir, Ne İşe Yarar?

Erişim Kontrol Sistemi, kart okuyucular aracılığı ile kendini sisteme tanıtan kişilerin, yazılımdaki tanımlamalara göre belli bina, bölge ya da odalara erişimini sağlayan sistemdir. Tanımlara uymayan kişilerin sistemi kullanımı bir uyarı sinyali yaratır bu da güvenlik elemanları için değerlendirilmesi ve raporlanması gereken bir durumdur. En basit anlatım ile sistem geçiş yapan kişilerin yetkili ve yetkisiz olarak ayrışmasını sağlayarak güvenlik görevlilerinin işlerini daha kolay ve verimli yapmalarını sağlar. Amaç yetkililerin geçişini kolaylaştırmak, yetkisizlerin geçişini kontrol altına almak ve böylece güvenliğin sınırlarını belirlemektir.

Bu aşamadan sonra olayı iki ayrı açıdan incelemek detaylara inme açısından yararlı olacaktır.

1-Sisteme tanımlı yetkili kullanıcılar

Sisteme tanımlı olan yetkili kullanıcılar, günlük iş hayatlarına , biraz da neden kullanıldığını anlayamadıkları hatta gereksiz gördükleri bir sistemin denetiminden geçerek başlarlar. Her birinin sahip olduğu özel kimlik kartını, sistemin kart okuyucularının birine okutarak çalışma alanlarına geçerler. Bu disiplini oluşturmak, doğru ve düzenli kullanımı sağlamak amacı ile kullanılan turnikelerden geçerken ister istemez oluşan gecikmelere, hele kart diğer ceket ya da çantada unutulmuşsa, istenilen ek uygulamalara kızarak içeri giren ve çıkış yapana kadar olayı unutan çalışanlar, sistemin yönetim için sağladığı faydaları göz ardı etmektedir. Binada çalışan kişinin kimliğini sisteme okutarak girişi ve sonra da çıkışı insan kaynakları departmanı için vazgeçilmez bir bilgidir. Bu bilgiler üzerinden personelin devam ve takibini sağlamakta, izinler, görevli çıkışlar ve benzeri olağan dışı kullanımları düzenlemekte ayrıca fazla mesailer de bu bilgiler ile düzenlenmektedir. Güvenlik departmanı yetkili girişleri denetlerken bir de yetkisiz girişlere de yoğunlaşmakta, ziyaretçileri kontrol ve elektronik ortamda kayıt işlerini yapmakta, bekçilerin turlarını düzenlemekte ve denetlemekte, yetkili personelin yetkileri doğrultusunda dolaşımlarını sağlayarak hem iç güvenliği sağlamakta hem de acil durumlarda can güvenliğinin sağlanması için gerekli acil durum planları üzerinde çalışmaktadır.

2-Yetkisiz kullanımların ve alarmların izlenmesi

Erişim kontrol sistemleri gerçekte "Erişim Kontrol ve Alarm İzleme Sistemi" olarak anılmaktadırlar. Yetkili personelin dolaşımının tanımı ve denetimi haricinde tanımların dışına çıkan tüm kullanımlar doğrudan güvenlikçilerin yoğunlaştığı konulardır. (Kartsız personel, personelin yetkisiz kart kullanımı, binaya gelen ziyaretçiler ve tüm alarmlar.)

Neyin alarm olduğunun tam olarak anlaşılması için şu basit örnek faydalı olacaktır. Bir kart okuyucu ve gerekli diğer donanım ile kontrol edilen bir kapıya personel kart göstererek girerse sistem tarih ve saat vererek içeri giren/çıkan kişinin kimliğini rapor edecektir. Bu yetkili kullanımdır. Kart sahibi diğer yerlere girme yetkisi olduğu halde bu özel odaya giriş yetkisi yoksa kart kullanıldığında sistem kart kullanımını alarm olarak raporlayacak ve geçiş engellenecektir. Kartı olmayan bir kişinin odaya giriş teşebbüsü ise doğrudan bir alarm olarak sisteme raporlanacaktır. Kart ile erişimin kontrol edildiği tüm kapıların dışında, güvenlik açısında önemli noktaların/alanların izlenmesi (yangın kapıları, çevre güvenlik gibi) ve bina ile ilgili tüm hayati fonksiyonların izlenmesi sistemin özellikleri içindedir. Bu izleme sadece kapılar ve diğer alarm algılayıcılar (Pasif ve Aktif Kızıl Ötesi Algılayıcılar, cam kırılma ve titreşim algılayıcılar ve tüm diğer kuru kontak veren cihazlar) için geçerli değildir, bina için hayati fonksiyonlar (UPS, havalandırma vb.) için de geçerlidir. Altı çizilmesi gerekli nokta tüm bu cihazların alarm için kuru kontak veriyor olması ve kontrollerinin sadece açık/kapalı olmasıdır. Mesela vananın yarı açılması gibi proses kontrol fonksiyonların denetimi ve kontrolü bu sistemin kapsamı dışındadır. Bu noktadan sonra bina yönetim sistemleri devreye girmektedir. Bizi ilgilendiren hayati fonksiyonların çalışıp çalışmadığı ya da güvenlik açısından önemli kapıların açık ya da kapalı olduğudur.

Konumuz olan erişim kontrol sisteminin kabaca ne olduğu ve ne işe yaradığını anladıktan sonra şimdi sistemi daha detaylı inceleyebiliriz.

Erişim Kontrol Sisteminin Elemanları ve Çeşitleri

1-Kart Okuyucular ve Kartlar

Yetkili personelin kendini sisteme tanıttığı kartlar ve kart okuyucular için çeşitli teknolojiler kullanılmaktadır. Artık geçerliliğini yitirmiş barcode, wiegand, magstripe okuyucuları geçerek en çok kullanılan kart ve kart okuyuculara bakalım. Proximity reader'ler günümüzde en çok kullanılan okuyucular dır. Kart aktif ya da pasif olarak kart okuyucu ile uzaktan iletişime girmekte ve kart okuyucu kartları okuduğu kod numarası ile ayırmaktadır. Bu kapsama Biometrik okuyucuları (Güvenlik seviyesi yüksek kullanımlarda kart sahibinin biometrik özellikleri ile tanımlanmasını sağlamaktadır. Parmak izi, El geometrisi ve iris okuyucular gibi) ve smart kartları ve kart okuyucuları da almak gerekmektedir. Smart kartlara yüklenen bilgiler kartların yukarıda anlatılan özellikler dışında başka amaçlar ile de kullanılmasını sağlamakta mesela üniversitelerde kayıt kabul, kütüphane, kafeterya, kahve makinaları ve fotokopi gibi ek fonksiyonların aynı kart üzerinden kontrol ya da yetkilendirilmesini sağlamaktadır.

2-Kontrol Ünitesi

Tüm kart okuyucuların bağlı olduğu bir mikro işlemci yazılım ve kart okuyucular arasındaki köprüyü oluşturmaktadır. Bu cihaz Server ile iletişimi sağlamakta, kendine bağlı tüm kart okuyucularla ilgili tüm tanımları belleğinde tutmakta, kendine bağlı alarm noktalarını izlemekte ve alarm anında sistemin tepkilerini verilen tanımlar doğrultusunda uygulamakta ve sisteme kayıtlı tüm kart kullanıcılarını tanımakta, iletişimin kesilmesi durumunda sistemi kesintisiz yönetmeye yönelik tüm bilgilere sahip bu cihaz bufferları ile kullanım bilgilerini de iletişim tekrar sağlanana kadar hafızasında tutabilmektedir. Böylece kart okuyucuya gösterilen bir kartın yetkili olup olmamasına göre kapının yada turnikenin açılıp açılmamasına karar vermekte, ilgili röleleri tetiklemekte ve ilgili bilgiyi servere göndermekte, alarm durumunda olayı raporlamakta ve isteniyorsa diğer sistemleri tetiklemektedir. (Olay yerini gören kamera görüntüsünün alarm monitoruna aktarılması gibi). Cihaz aynı zamanda tüm kendine bağlı diğer elemanları sürekli test etmekte ve devre dışına çıkanları rapor etmektedir.

3-Güvenlik Yönetim Sistem Yazılımı

Başlı başına bir konu olabilecek kadar detaylı olan bu bölümü yazılımın başlıca fonksiyonlarını anlatarak kısaca tanıtmaya çalışalım. Yazılımda ilk tanımlar sistemi sisteme tanımlayacak bilgilerin girilmesidir. Kart okuyucuların yerleri ve çalışma prensipleri, kontrol üniteleri ve iletişim protokolleri, alarm noktaları ve alarm kriterleri, her alarm için sistemin tepki tanımları ve tarih, saat ve yılın tatil günleri gibi. İkinci aşama kart sahiplerinin kimlik bilgileri ve sistemi kullanım

yetkilerinin sisteme tek tek girilmesidir. Her kullanıcının sistemde tanımlı her kart okuyucudan ne zaman ve ne şartlarla geçip geçemeyeceği tanımlanabilir. Mesela kişinin belli bir odaya çalışma saatlerinde, Cumartesi, Pazar ve tatillerde girip giremeyeceği ayrı ayrı tanımlanabilir. Oluşturulan bu veritabanı kişilerin fotoğraf bilgilerini de içerebilir. Bu bilgiler istenirse diğer sistemlere export (ihraç) edilebilir ya da diğer sistemlerde mevcut ise import (ithal) edilebilir. Oluşturulan veri tabanı diğer sistemlerle paylaşılabilir. Bu önemli bilgilerin güvenliğinin sağlanması ise, sistem yöneticilerinin ve operatörlerin sistemi kullanım yetkilerinin ve parolalarının oluşturulması ile mümkün olacaktır. Sistemin çalışması sağlayacak tanımların yapılmasından sonra kontrol üniteleri ile iletişimin kurulması ve bilgilerin ilgili kontrol ünitelerine yüklenmesi gereklidir. Bu aşamadan sonra sistem kullanıma hazırdır. Her sistemin kendine özgün farklılıklar içermesi ve tüm yukarıda basitçe anlatılan hazırlıkların bu özelliklere göre düzenlenmesi kaçınılmazdır. Örneğin:
1-Güvenlik Yönetim Sistemi tek bir (stand alone) üniteden oluşmayıp bir ağ altında çalışması gerekebilir. Bu ağ tek bir bina içinde değil değişik şehir hatta ülkelerde olması olasıdır. Bu durumda uygulayıcının "networking" bilgisine sahip olması ve tanımlarını bu doğrultuda yapması kaçınılmazdır. Ülkemizde bu tür uygulamalar mevcuttur.
2-Sistemin kendi içinde gizli ve kritik bilgiler içermesi sebebi ile "Redundant" olması yani veritabanını ikinci bir ikiz bilgisayara gerçek zamanda kopyalayarak olası bir arıza ya da bakım esnasında ana bilgisayarın yedeklenmesi ve kesintisiz kullanım istenebilir.
3-Veritabanının diğer sistemler ile paylaşılması olasılığına karşı işletim sisteminin "Open Source" ve "Open Architecture" olması gerekebilir. Bu durumda sistemin güvenliğinin sağlanması için gerekecek ek önlemlerin gündeme gelmesi söz konusu olacak ve ister istemez bilgi güvenliği konusu gündeme gelecek ve uygulamacı kuruluşun bu konu ile ilgili elemanları ile ortak çalışma yürütmesi gerekecektir.
4-Can ve mal güvenliği çelişen kavramlardır.Erişim kontrol sisteminin tasarım aşamasında özellikle yangın güvenliğini yapan tasarımcı ile ortak çalışılması çok önemlidir. Bu iki sistem farklıdır ve yazılım entegrasyonunun mahsurları vardır ama bir acil durumda hızla boşaltılması gereken bir binada iyi tasarlanmamış güvenlik buna engeldir. Bu ince çizgi, tesisin mimarisine, kullanılan sistemlerin özelliğine ve en önemlisi tasarımcıların bu detaylara verdiği öneme göre oluşmaktadır. Aslında istenen ve oluşturulması gereken normal şartlarda tam güvenli bir binada acil durum oluştuğunda insanların hiç bir elektronik sisteme bağlı kalmaksızın binayı hızlı ve hiç bir engele takılmaksızın terk edebilmesidir.

Güvenlik Yönetim Sistemi yazılımı ve uygulayıcı firmanın bu konuda bilgi ve tecrübesi erişim kontrol sistemleri uygulamalarında ve genel olarak bina otomasyonun oluşturulmasında önemli bir unsurdur. Bilgi ve tecrübe birikimi ile tasarlanmalı, diğer otomasyon sistemleri ile ilişkileri kurulmalı ve tanımlanmalı, eğitimli bir teknik kadro ile uygulaması yapılmalı ve en önemlisi bu bilgiler kullanıcıya, iyi bir eğitim programı çerçevesinde gerektiği kadar aktarılmalıdır. Güvenli ve huzurlu yaşamların her yeri sarması dileği ile...