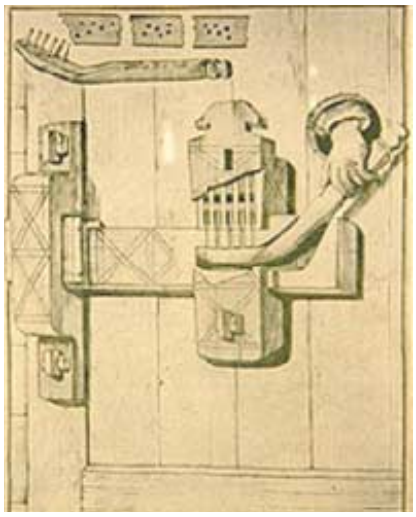
GÜVENLİĞİN ÇAĞLAR BOYU DEĞİŞMEYEN ADI

KİLİTLER VE ANAHTARLAR

Özel mülkiyet, başka bir deyişle mülk sahibinin yalnızca kendisinin ya da izin verdiği sınırlı sayıdaki kişinin kullanabileceği mallar çok eskiden beri var. Yaşadığımız evler de, belki neolitik çağın başlangıcından beri özel mülkiyet konumunda. Böyle olunca kendimize ait olanı korumak istiyoruz. Korumak istediğimiz evimiz, eşyalarımız ya da arabamız olabilir. Bankadaki paraların, devlet sırları gibi özel bilgilerin de korunması gerekir. Yüzyıllar boyunca biçim değiştirse de, insanın özel mülkiyetini koruyan tek bir şey var: Kilitler ve anahtarlar.



İlk kez Mezopotamya, eski Mısır ve eski Yunan uygarlıklarında kilit olarak adlandırılabilecek basit sürgüler kullanıldığı biliniyor. Ne var ki, bunlar çok basit bir mekanizmaya sahip oldukları için zorlanmadan açılıyorlardı. Metal kilit, anahtar ve kilit tırnağıyla sağlanan güvenlik sistemi, bize Romalılardan miras kaldı. Yüzlerce yıl, bir kilidin anahtar deliğinde yalnızca o kilide uyan anahtarın dönmesini sağlayan tek yöntem olarak kalan bir sistemdi bu. Bu sistemde temel olan şey, kilit tırnağı. Kilidin içinde, anahtar deliğinin çevresinde bulunan çıkıntılara kilit tırnağı adı verilir. Bu çıkıntılar, düz bir anahtarın kilit içinde dönmesini engeller. Yalnızca bu çıkıntılara uygun dişleri olan anahtarlar kilidin içinde döner. Yüzyıllar boyunca kilitlerin güvenilirliği, kilit dillerine bağlı kaldı. Yakındoğu ve Uzakdoğu'da yapılan kazılarda çok miktarda bulunan asma kilitlerin, Doğu'da Çin'de geliştirilmiş olduğu düşünülüyor.

Kilit sistemleri Roma İmparatorluğu'yla ve Çin'le sınırlı değildi elbette. Ortaçağda, özellikle Almanya'nın Nürnberg kentinde son derece usta işi metal kilitler geliştirilmişti. Kilidin hareketli parçaları incelikle işlenerek birbiri üzerine yerleştiriliyor, böylece kilidin boyutları küçülüyordu. Kilidin içindeki kılavuz adı verilen diller de özenle işleniyordu. Anahtarlar bu dönemde sanat eseri gibi hazırlanıyordu. Bununla birlikte, bu anahtarların kılavuz sistemlerini açmanın çok zor olduğu söylenemez. Çok şık olmalarına karşılık, bu anahtarların kilit mekanizmaları çok güvenilir değildi. Bu nedenle kilit ustaları anahtar deliğini gizler, sahte anahtar delikleri sayesinde kötü niyetli birini yanıltmayı hedeflerlerdi. Bu, çilingirlerin kilit yapımında ne denli yüksek bir hayal gücüyle çalıştıklarını gösteriyor. Yüzyıllar boyunca çilingirler, kilit tırnaklarının yapılması konusunda büyük yaratıcılık gösterdiler. Birçok başarılı kilit sistemi geliştirildi. Ne var ki, asıl anahtarı olmadan da kilidi açabilen ve "maymuncuk" adı verilen aletler de yapıldı.

Kilitlerin Gelişimi

Kilitlerin güvenilirliğinin artırılması yolundaki ilk önemli adımı 1778'de İngiliz buluşçu Robert Barron attı. Barron'un bu tarihte patentini aldığı kilit, çift etkili mandallı sistemle çalışıyordu. Manivela işlevi gören mandal, normal konumdayken sürgüye açılmış bir yuvaya oturuyor ve sürgünün hareket etmesini önlüyordu. Sürgü, ancak anahtarın mandalı kaldırması ve böylece mandalın ucundaki çıkıntıların yuvanın girintilerinden kurtarılmasıyla hareket edebiliyordu. Barron kilidi, günümüzde de kullanılan manivelalı kilitlerin atası olarak görülebilir. Ne var ki Barron kilidi de azimli hırsızlara dayanamadı. 1818 yılında Jeremiah Chub, kilide, zorlanma sırasında mandalı yakalayarak tutan bir yay ekleyerek manivelalı kilit türünü biraz daha geliştirdi. Bu düzenek hem sürgünün geri çekilmesini önlüyor, hem de kilitle oynandığını gösteriyordu.

O dönemde bir başka kilit türünü de1784'te İngiliz Joseph Bramah geliştirdi. Çalışma ilkesi tümüyle farklı olan ve çok küçük, hafif bir anahtarla açılan bu kilit, kendinden öncekilerden çok daha güvenliydi. Bu kilitler çok karmaşık, aynı zamanda pahalıydı. Bramah kilidinin anahtarı, ucuna uzunlamasına ince oluklar açılmış metal bir boru biçimindeydi. Anahtar kilide sokulduğunda üzerindeki oluklar kilitteki bir dizi sürgüye oturuyordu ve bu sürgüler oluğun uzunluğuna bağlı olarak aşağı itiliyordu. Anahtar, ancak bütün sürgülerin gerekli uzunluğa kadar itilmesi durumunda döndürülebiliyor; böylece asıl sürgü hareketlendirilebiliyordu. Bramah, yaptığı bu kilide çok güveniyordu. Öyle ki, 1801'de Londra'daki dükkanında sergilediği kilitlerden birini ilk açabilene 200 sterlin ödül vereceğini açıklamıştı. Ödülü elli yıl sonra, 1851'de ABD'li bir çilingir olan Hobbs alacaktı. Bramah kilitleri bu tarihe kadar yaygın olarak kullanıldı.

Kilit ve anahtar mekanizmasının 19. yüzyıla kadar fazla değişikliğe uğramadan kaldığını söyleyebiliriz. Bunun bir nedeni

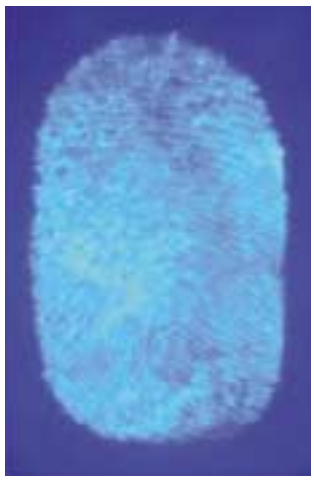
de, insanların güvenlik gereksinimlerinin bu yüzyıla kadar yaklaşık aynı kalması denebilir. Oysa, sanayi devriminden sonra sosyal ve ekonomik yaşamın hareketliliği, yeni kilit ve anahtar sistemleri gerektiriyordu. Bu yüzyılda değişen yaşama alışkanlıkları yeni güvenlik gereksinimleri öne sürüyordu. Bunun da bir sonucu olarak anahtar ve kilit yapımında bir dizi gelişme oldu. Bu dönemde geliştirilen kilitlerin bir kısmı Bramah kilidinin çalışma ilkesine dayanan geliştirilmiş modellerdi. Bunlardan biri, Robert Newell'in tasarladığı kilitti. Bu kilidin özelliği birbiri üzerinde çalışan iki mandalın ve anahtarla birlikte dönerek kilit deliğinin öteki tarafının gözlenmesini önleyen levhanın bulunmasıydı. Böylece, hırsızların önce içeride kimsenin bulunup bulunmadığını kontrol etmesi güçleştiriliyordu. Ayrıca anahtarın dili değiştirilebilir türdendi. Böylece anahtar değiştirmek kolaylaşıyordu.

Anahtar ve kilitlerde en büyük yenilik Yale kilidiyle ortaya çıktı. 1848'de Linus Yale, çok eskiden Mısır'da kullanılan kilitlerden yola çıkarak pim mandallı bir kilit geliştirmişti. Silindir göbekli Yale kilidinin binlerce değişik biçimde yapılabilen ince, kullanışlı anahtarınıysa oğul Yale 1860'lı yıllarda yaptı. Bu kilidin anahtarı, yalnızca belirli bir anahtar deliğine uymasını sağlayan birkaç değişik kesite sahip. Dolayısıyla kesitin kendisi de bir tür kilit tırnağı olur. Yuvaya sokulan anahtarın dişleri, kenetleyici yaylı pimleri iter ve böylece kilit göbeğinin dönerek kilit dilini itmesini sağlar. Bu kilitlerin maymuncukla açılmaları olanaksız değilse de yine de oldukça kullanışlı ve güvenlidirler. Öyle ki Yale sistemi 20. yüzyılda dünyanın her yerinde benimsendi ve dış kapıları kilitlemekte en çok kullanılan anahtar çeşidi oldu.

Anahtarsız Kilitler

En yaygın kilitler, anahtar kullanılarak açılanları. Öte yandan, anahtarsız, şifreli kilitler de kullanılıyor. Anahtarsız şifreli kilit türü, 17. yüzyılın başlarında İngiltere'de kullanılan "harfli kilit" düzeneği temel alınarak geliştirildi. Bu kilitte üzerinde harfler ya da sayılar bulunan bir dizi bilezik, bir mile geçirilmişti. Bilezikler, şifre sözcüğü ya da sayıyı oluşturacak biçimde sırayla döndürüldüğünde, bileziklerin içine açılmış yuvalar aynı hizaya geliyor, böylece mil dışarı çekilebiliyordu. Harfli kilitler önceleri yalnızca asma kilitlerde ve oyuncaklarda kullanıldı. 19. yüzyılın ikinci yarısında son derece güvenli oldukları düşünülen bu tür kilitler kasalarda ve çelik odaların kapılarında kullanılmaya başladı. Bu kilitlerde neredeyse sonsuz sayıda şifre kurmak mümkündü. İçine anahtar sokmak gerekmediğinden, bir deliği yoktu; böylece içine patlayıcı maddeler yerleştirilip parçalanarak açılması da söz konusu değildi. 20. yüzyılın ikinci yarısında bilgisayarların ve elektronik sistemlerin gelişmesiyle birlikte şifreli kilitlerin elektronik olanları da yapıldı. Bu sistemler birkaç değişik biçimde çalışıyordu. Kapıyı açmak için gerekli şifreyi yazacağınız kilitler, bir anlamda bilezikleri çevirmekle aynı işi yapar. Bir başka yöntemse, üzerinde güvenlik çipi bulunan bir kartı kilide "tanıtmaktan" geçer. Elektronik

kilidin anahtarı, bu manyetik karttır. Ne var ki kartın çalınması ya da kopyalanması durumunda kilitler kolayca açılabilir. Tasarımcılar bu durumu aşmak için "melez" denebilecek bir sistem geliştirdiler: Buna göre şifre anahtar olarak kullanılan kartların üzerine tuşlanabilir. Üzerinde rakamlar bulunan elektronik anahtarınızı, şifrenizi girdikten sonra kilit yuvasına yerleştirirseniz kapı açılır. Bu sistemle elektronik kilitler biraz daha güvenli oluyordu. Ne var ki şifrenin unutulması ya da kartları kaybetme gibi riskler hâlâ vardı. Asla kaybolmayacak, ya da unutulmayacak şifreler yapmak gerekiyordu.



Şifre girilerekya da mantetik bir kart okutarak açılan kilitlerde sorun kartın kaybedilmesi ya da şifrenin unutulmasıydı. Parmak izine duyarlı kilitlerle bu sorunlar aşıldı.

Anahtar Olarak İnsan

Henüz evlerimizde kullanacağımız kadar yaygınlaşmadı; ama artık bedensel özelliklerimiz de anahtar olarak kullanılıyor. Uzmanlar yalnızca tek bir kişiye ait olan bir şey düşündüklerinde akıllarına gelen, her insanda yine tek ve diğer insanlardan farklı olan özellikler. Bu tür güvenliğin bir adı var: Biyometri. Şimdiye kadar kullanılan yöntemler ya bir güvenlik kartı ya da güvenlik koduna bağımlı yöntemlerdi. Oysa, bunlar kolaylıkla kaybolabilir ya da unutulabilir. Kötü amaçlı kişilerce kolaylıkla kopyalanabilen ve çoğaltılabilen bu yöntemler yerine fizyolojiden yararlanmak güvenlik açısından birçok sorunu ortadan kaldıracak gibi görünüyor. Uzmanlar, yalnızca size özel bir şeyin ancak yalnızca size özgü başka bir şey yardımıyla korunabileceğini söylüyorlar. Bunlar da elbette sizin fizyolojik özellikleriniz. Gözün bir bölümü olan iris, parmak iziniz, yüzünüz ya da sesiniz hep sizinle. Bunları unutmanız ya da kaybetmeniz söz konusu değil. Vücudunuzun bu bölümleri yalnızca size özel olduğu için, çalınması mümkün olmadığı gibi, sizin de hata yapmanız mümkün değil. Uzmanlara göre iki farklı iris tabakasının aynı desende olması 10^{52}'de bir olasılık. Birbirinin aynı parmak izi bulunma olasılığıysa hiç yok.

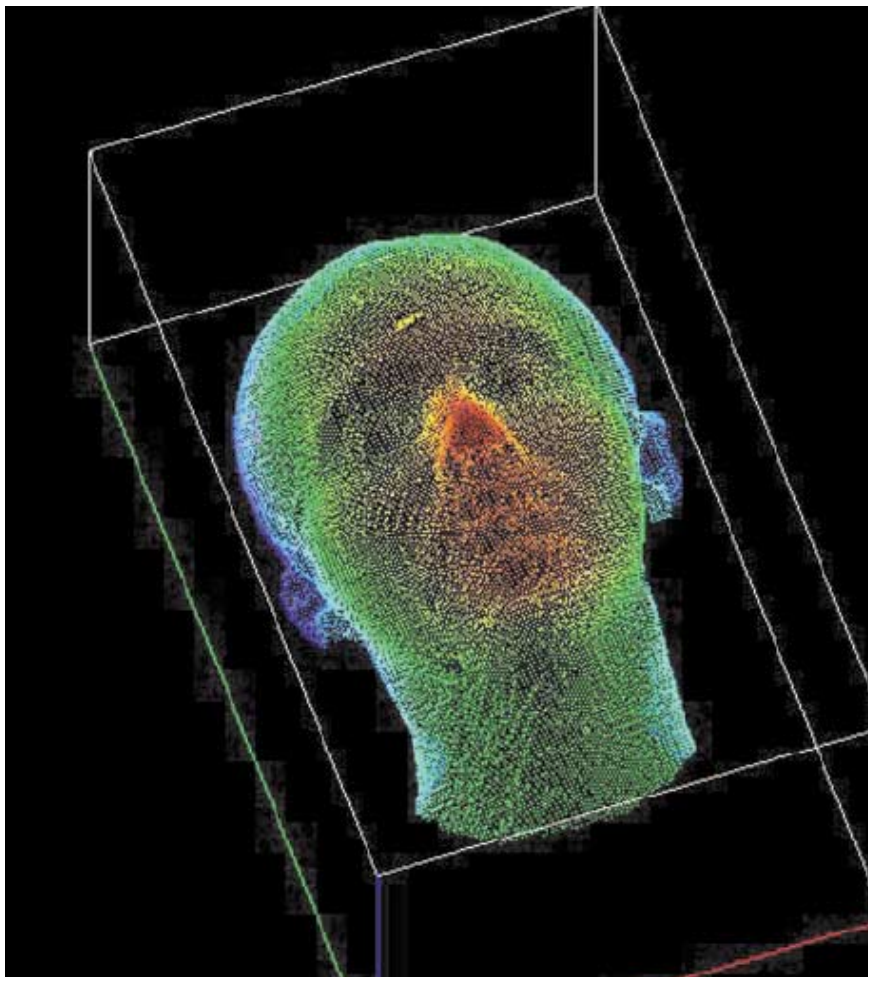
Şifreli kilitler anahtar gerektirmiyor. Yapılması gereken tek şey, halkaları doğru hizaya getirmek.

Bütün biyometrik sistemler aynı prensibe göre çalışıyor: Örneklem, sayısal olarak taranıyor ve karakteristik özellikler kaydedilip bir veri bankasına yükleniyor. Sözgelimi, bankadan para çekmeye gittiğinizde veri bankasında bulunan kayıtlarınızla, o sırada alınan örnek karşılaştırılır. İki örneğin birbirini tutması durumunda para çekmeniz için onay verilir ve paranızı alırsınız. Aynı şekilde, kilitlerin açılması için yapılacak bir göz taraması ya da sesli bir komutla veri bankasının kayıtları birbirine uyduğunda onay verilir ve kapılar açılır. Bu yöntem hırsızlara karşı oldukça iyi bir önlem olarak düşünülüyor. Uzmanlar benzer sistemlerin çoğaltılabileceğini söylüyor. DNA koduna göre, bedeninizden yayılan kokunun kimyasal analizine göre sizi tanıyıp onay verecek güvenlik sistemleri de yolda.

Peki varolan biyometrik kilit sistemlerinin hangisi daha güvenilir, hangi sistemi seçersek bizim için daha iyi olur? Elbette her sistemin iyi yanları olduğu gibi kötü yanları da var. Sözgelimi, parmak izi tanıyan kilitlerin fiyatları, diğerlerine göre daha ucuz ve parmak izi tanıyıp onay verme süresi oldukça kısa. Bununla birlikte, eğer parmağınızda yaralanmadan kaynaklanan bozukluklar olmuşsa elbette ki onay alamayacaksınız. Parmağınızdaki minik bir kesik bile, veri bankasındaki kayıtlarınızla parmağınızın eşleşmesini önleyecektir. Yine de uzmanlar parmak izi yönteminin güvenlik notunu "iyi" olarak veriyor. Parmak izi yerine, elin geometrik yapısını tanıyan güvenlik sistemleri de var. Hatta bunlar 1996 yılında Atlanta'da yapılan Olimpiyatlarda kullanılmış ve başarılı olmuştu. Ne var ki parmak iziyle ilgili sorunlar bu sistemde de geçerli. Ayrıca, çok büyük ya da çok küçük elleri olan kişiler için sistem sağlıklı çalışmıyor. Bu sistemde birbirine benzer el yapıları bulma olasılığı bulunduğu için güvenlik notu "orta". Bir diğer yöntem, yüz şeklinizin analizi yoluyla gerçekleşiyor. Yüzünüzün geometrik yapısı, gözlerinizin konumu, burnunuzun biçimi incelenerek kullanılıyor. Herhangi bir yere

dokunmak gerekmediği için daha hijyenik. Ne var ki, insanların yüz yapılarının zamanla değiştiği düşünülürse, uzun dönemde çok pratik sayılmıyor. Estetik ameliyatlarla yapılan yüz değişiklikleri, yaşlanmanın etkileri bu sistemi güvenilir olmaktan çıkarıyor. Son günlerde en yaygın gündeme gelen biyometrik güvenlik sistemi iris taraması. Bu yöntemin güvenlik notu hayli yüksek. Bunun yanında maliyeti en yüksek olan sistem de bu. En bilindik yöntemlerden biri de sese duyarlı güvenlik sistemleri. Görece ucuz olan bu sistemde, telefon aracılığıyla da onay verebiliyorsunuz. Ne var ki yaşlandıkça ya da hastalandığınızda sesin değiştiği düşünülürse güvenlik açısından bunun da notu yüksek değil. Eğer çok bağırmaktan sesiniz kısılmışsa ya da gripten dolayı sesiniz kalınlaşmışsa evinize girememek oldukça sinir bozucu olabilir.

Bunlar pratikte yaşanan sorunlar. Bir diğer önemli problem de işlem zamanı. Kişisel konutlarda kullanılan güvenlik sistemlerinde bunun o kadar da önemi yok. Ne var ki sözgelimi bankada para otomatından para çekeceğiniz sırada veri işlemenin uzun sürmesinden dolayı yığılmalar yaşanabilir. Biyometrik veri bankaları yoluyla sağlanan güvenlik sistemlerinin sıkıntı yaratan bir başka yanı da insanların fizyolojik özelliklerinin sürekli kontrol edilme ve kişilerin bireysel özgürlüklerinin bu yolla kısıtlanabileceği korkusu. George Orwell'in 1984 romanında yarattığı "Büyük Birader" karakteri yerine geçebilecek veri bankalarını kimse istemiyor. Parmak izlerinizle açılan kapılar, sesinize ya da iris tabakanıza duyarlı tarayıcılarla her yaptığı izlenen insanlar haline dönüşme tehlikesiyle karşı karşıyayız. Biyometrik sistemlere yöneltilen eleştiriler, yalnızca bu kadar değil. Günümüzde kapınızın kilidini ya da şifrenizi değiştirebilirsiniz. Ne var ki parmak iziniz ya da iris, retina gibi organlarınız değiştirilemez. Bir şekilde parmak izinizin ya da biyometrik özelliklerinizin kopyalanarak güvenlik sisteminize sızılması durumunda bunları değiştiremezsiniz.



Biyometrik güvenlik sistemlerinden biri de yüzün yapısını tanıyarak onay vermek prensibiyle çalışıyor. Ne var ki yaşlandıkça yüzümüzün yapısının değiştiğini düşünürsek, bu sistem çok da güvenli değil.

Biyometrik sistemler içinde en güvenli olanı iris taraması. Bu sistem görece pahalı olmasına karşın gittikçe yaygınlaşıyor.

Biyometrik sistemler oldukça güvenli olabilir, ancak maliyetlerinin yüksek oluşu şimdilik yaygınlaşmalarını önlüyor. Kolayca edinebileceğimiz, bozulduğunda kolayca değiştirebileceğimiz kilitler ve anahtarlar hâlâ en çok tercih edilen güvenlik sistemleri. Yalnızca fiyat değil, kullanım kolaylığı sağladığından yüzyıllardır kullandığımız yöntemleri kullanmaya devam ediyoruz. Kişisel yaşamın özelliği, özel mülkiyet gibi kavramlar olduğu sürece kilitler ve anahtarlar da var olmayı sürdürecek. Öte yandan, hırsızlığın da insanla birlikte var olmayı sürdüreceğini söyleyebiliriz. Güvenlik sistemleri geliştikçe bunları aşmanın yolları da gelişecek. En güvenliye ulaşıncaya kadar kilitler ve anahtarlar gelişimini sürdürecek.

Gökhan Tok

Kaynaklar:
Der Mensch als Passwort, Bild der Wissenschaft, ss:80-85, no:10, 1999
Security Engineering Applications Manual, AM4, CIBSE, 1991
http://www.biometrics.org
http://www.queensnewyork.com/history/locks.htm
http://www.accesexcellence.org/WN/SU/SU102001/irisscan.html