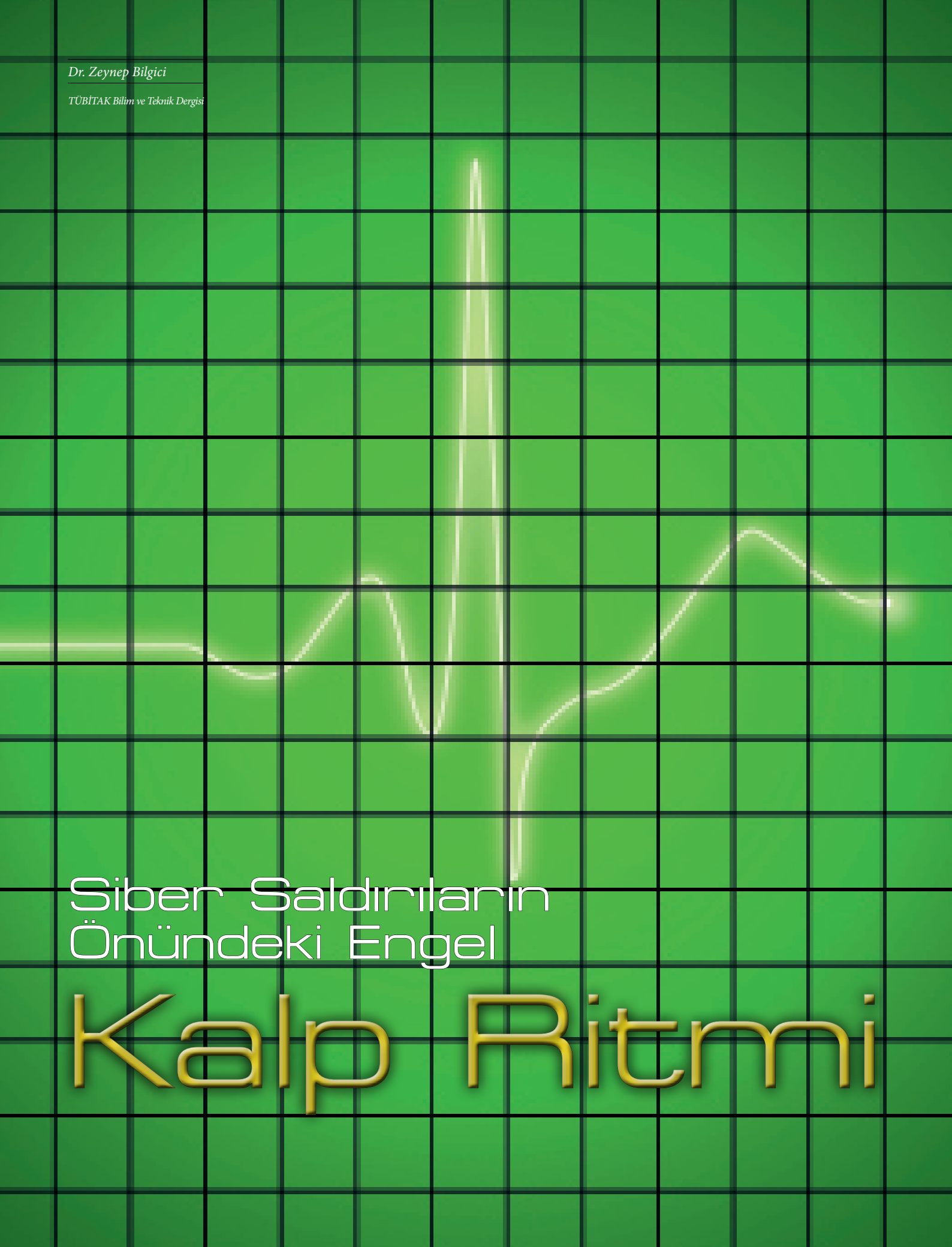
Dr. Zeynep Bilgici

TÜBİTAK Bilim ve Teknik Dergisi



Siber Saldırıların Önündeki Engel

Kalp Ritmi

>>>

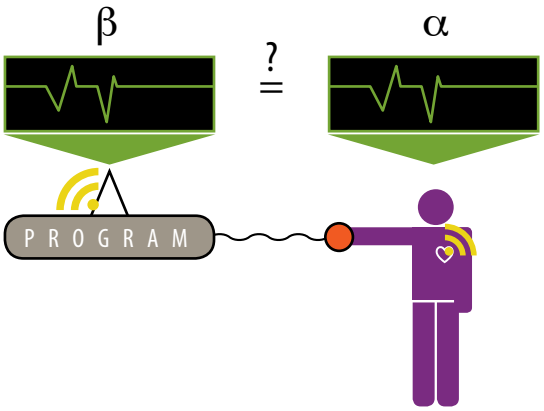
Bir bilgisayar korsanının bir adamın kalp piline saldırısı…

Homeland adlı TV dizisini izleyenler bu sahneyi hatırlayacaktır. Dizinin Aralık 2012'de yayımlanan bölümlerinden birinde yer bulan bu konu birçok izleyiciye "bu kadarı da olmaz" dedirtirken bir taraftan da "acaba olur mu" diye düşündürmüştü. İnsani değerlere akıl almaz derecede ters düşen bu durum sadece kurgu değil, hatta gerçek hayatta maalesef dizide olduğundan çok daha kolay yapılıyor. Çünkü dizide bu işlem için izinsiz müdahale edilen cihazın seri numarası kullanılıyor, hâlbuki gerçek hayatta tıbbi cihazın seri numarasına bile gerek yok.

Tehlike altında olan sadece kalp pili değil! Defibratörler hatta insülin pompaları bile izinsiz müdahaleye açık. Bu tür cihazlara yapılabilecek muhtemel bir korsan saldırının örneğini bir gösteriyle tüm dünyanın gözü önünde gerçekleştirmeyi planlayan ve güvenlik firması McAfee'de araştırmacı olarak çalışan, aynı zamanda ünlü bir bilgisayar korsanı olan Barnaby Jack, bu gösterisini gerçekleştiremeden aniden yaşamını yitirdi.

Aslında bu konu çok yeni sayılmaz, çünkü Massachusetts ve Washington üniversitelerinden bilim insanları 2008 yılında tıbbi cihazlarda güvenlik zafiyeti olduğunu gösteren bir çalışma yayımlamıştı. O dönemde de basında geniş yer bulan bu konu, bu TV dizisi ile birlikte yeniden birçok insanın ilgisini çekti.

Bilişim korsanlığı haberlerine her gün bir yenisi ekleniyor. Web sitesi çökertenler, resmi kurumların güvenlikli iç ağlarına girenler, kişisel bilgileri ve şifreleri ele geçirip banka hesaplarından para çalanlar, başkalarının bilgisayarlarındaki tüm verilere kolayca ulaşanlar ile ilgili sayısız haber okuyoruz. Bilişim korsanlarının ulaşabildiği cihazlar maalesef her geçen gün çeşitleniyor. Öyle ki artık bazı tıbbi cihazlar da bu listede yer alıyor.



Temel H2H işlemi:
Bilgisayar programcısının ve IMD'nin okuduğu değerlere β ve α denirse, ancak β≈ α olursa cihaza erişim sağlanıyor.

Bilgisayar korsanlarının tehdidi altındaki tıbbi cihazlar arasında kandaki insülin miktarını düzenlemek amacıyla şeker hastalarının kullandığı insülin pompaları, kalbin anormal hızda attığı durumlarda normal hızda atmasını sağlayan kardiyak defibrilatörler veya yine kalp atışlarını düzenleyen kalp pillerini sayabiliriz. Vücuda yerleştirilen cihazların ana bilgisayarla iletişimlerini sağlayan kablosuz bağlantıları vardır. Bu bağlantı özellikleri sayesinde, doktorlar tarafından düzenli olarak kontrol edilebilirler, program güncellemeleri yapılabilir ve acil durumlarda cerrahi operasyona gerek kalmadan cihazlara müdahale edilebilir.

Tüm insanlığın faydası için üretilen bu cihazlar kablosuz bağlantı özellikleri yüzünden üçüncü şahısların müdahalesine maruz kalabilir. Bu müdahalelerle kalbin atış ritmini veya kandaki şeker miktarını değiştirmek mümkün olduğu için bu tip siber saldırılar pek çok defa ölümcül sonuçlara yol açabilir.

Korsan saldırılara hedef olma riski taşıyan tıbbi cihazları sadece vücuda yerleştirilen tıbbi cihazlarla sınırlandırmak doğru değil. Çünkü hastanelerde kullanılan pek çok cihaz, örneğin izleme cihazları veya bilgisayarlar da hem korsanların kolay ulaşabileceği işletim sistemleri olduğu hem de ortak bir ağa bağlandıkları için bilgisayar korsanlarının saldırısına uğrayabilir.

Aslında tıbbi cihazlarda güvenliği sağlamak için genellikle şifre kullanılıyor. Fakat bu şifreler bilgisayar korsanları tarafından kolayca etkisiz hale getirilebildiği için kötü niyetli saldırılara engel olamayabiliyor. Nitekim Cylance isimli bir güvenlik firmasının yayımladığı rapor bunu açıkça gösteriyor. Bu raporda, üç yüz tıbbi cihazın şifresinin çözümlendiği belirtiliyor. Çalışmayı yapan araştırmacılar BillyRios ve Terry McCorkle sadece bu konuya dikkat çekmek istedikleri için şimdilik üç yüz şifre elde ettiklerini, aslında aynı yolla 1000 hatta 10.000 şifreye de kolaylıkla ulaşabileceklerini söylüyor.

Bildiğiniz Tüm Şifreleri Unutun!

Telefonumuz, bilgisayarımız ya da banka hesabımız için onlarca şifreyi aklımızda tutmaya çalışırız. Bu da yetmezmiş gibi evimizin ve otomobilimizin anahtarı, ofisimizin güvenlik kartı gibi çoğu zaman yanımızda bulundurmak zorunda olduğumuz eşyalarımız vardır. Biraz unutkan veya dalgın biriyseniz şifre hatırlamak veya anahtarlarınızı yanınıza almayı unutmamak sizin için tam bir sıkıntı olabilir.

Bionym isimli bir firma tarafından bütün bu sıkıntılara son verdireceği iddia edilen yeni bir bileklik tasarlandı. Nymi adı verilen bu bileklik aslında parmak izi veya yüz tanıma programları gibi kişiye özgü fiziksel karakterlerin şifre olarak kullanılması esasına dayanıyor.

Kullanan kişinin EKG verilerine ulaşan bu bileklik-yüklenecek özel bir uygulama sayesinde-erişmek istediği cihazla bir çeşit kablosuz bağlantı (Bluetooth) kullanarak iletişime geçer. Kalp ritmi sayesinde sahibini tanıyan ve çevresindeki dijital uygulamalarda gerekli olan şifre işlemlerini otomatik olarak gerçekleştiren bu bilekliklerde, bileği bükmek veya sallamak gibi bazı vücut hareketleri de komut olarak kullanılabilecek.

Fiziksel özellikleri kullanan sistemlerin zorbalıkla ele geçirilme ihtimali üzerindeki tartışmalar sürerken, internet üzerinden 100 $'ın altında bir fiyata ön siparişleri alınan bu bilekliklerin 2014 yılında piyasaya çıkması planlanıyor.

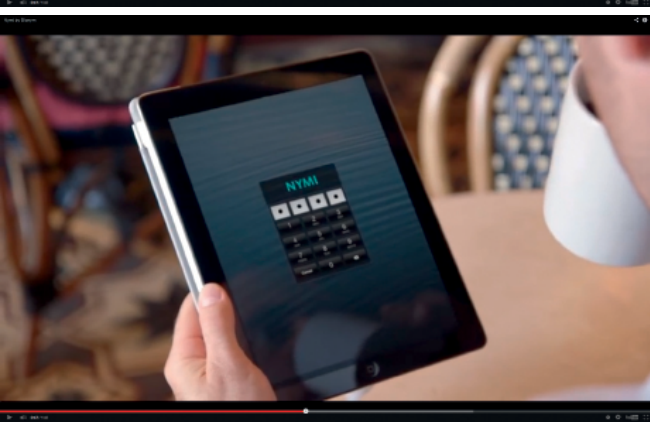
Artan riskler aslında pek çok çevrenin de harekete geçmesini sağladı. Bunlardan biri de geçtiğimiz Temmuz ayında bir belge yayımlayan ABD Gıda ve İlaç İdaresi (*American Food and Drug Administration*, FDA). FDA, bu belgeyle durumun ciddiyetine dikkat çekerek tıbbi cihaz üreticilerini, bu tip cihazları doğrudan etkileyebilecek olası saldırılara karşı uyararak bu konuda acil önlem alınması gerektiğini vurguluyor.

Kalp ritmi ya da kandaki şeker miktarı gibi hayati önem taşıyan faktörlerin bilgisayar korsanları tarafından değiştirilebilme ihtimaliyle yaşama korkusu, bir diğer deyişle kendini savunamadan, bilgisayar korsanlarının parmaklarının ucuna bağlı bir hayat yaşamaya çalışmak, bu tip cihaz kullanan birçok insanın kâbusu olmaya başladı. Bu korkular nedeniyle kullandıkları cihazların kablosuz iletişim özelliğini devre dışı bırakmak isteyenler var, ama bilgisayar korsanlarına göre bu bile kötü niyetli saldırıların önüne geçmek için yeterli olmayabilir.

Tıbbi cihazlardaki güvenlik boşluklarının kullanıcılarına yaşattığı kâbuslara son vermeyi hedefleyen çalışmalardan biri Rice Üniversitesi'nde yapıldı.

Bu çalışmada, tıbbi cihaz kontrollerinin ve programlarının kimlik doğrulamasını sağlayacak *Heart-to-Heart* (H2H) adı verilen yeni bir sistem geliştirildi. Bu sistemde vücuda cerrahi müdahale ile yerleştirilen cihazlar, örneğin kalp pilleri şifre olarak -yine aynı kişiye dışarıdan takılan küçük bir cihaz sayesinde-kalp atış çizelgesi (elektrokardiyogram, EKG) verilerini kullanıyor.

Bu çalışmayı yapan bilim insanları EKG'deki değişimleri, anlık olarak değişen borsa bilgilerine benzetiyor. Kalp atışlarının ritmini gösteren verilerdeki detaylara bakıldığında, verilerin mikrosaniyede bile değişebildiği görülüyor. EKG verileri her saniye değişiklik gösterdiği için şifrede sürekli yeniden tanımlanıyor, yani kullanılan bir şifre çok kısa sürede geçerliliğini kaybediyor.



Kişiye özel olarak üretilecek bu bileklikler sayesinde otomobil ve ev kapıları, hatta bilgisayarlar bile kolayca açılabilecek. Ödeme aracı veya uzaktan kumanda yerine bile kullanılabilecek bu cihazlar ileride günlük yaşamımızın ayrılmaz bir parçası olmaya aday.

Bu sistemde hastanın EKG verilerinin istatistiksel değerleri, hastaya temas eden şifreli (kriptolu) bir cihaz yardımıyla çözümleniyor. Bu veriler vücuda yerleştirilen cihazların okuduğu değerler ile karşılaştırılıyor. Eğer değerler birbiriyle uyum gösterirse kimlik doğrulama başlatılıyor ve programa erişim sağlanıyor.

H2H programı, aslında vücutta anlık olarak değişen başka bir fizyolojik değer üzerine de kurulabilirdi. Fakat bu çalışmayı yapan bilim insanları özellikle EKG verisi kullandıklarını, bu sayede en yaygın cihazlar olan kalp pilleri ve kardiyak defibrilatörler üzerinde tam bir başarı sağladıklarını, bu yöntemin vücudun herhangi bir yerine yerleştirilen ve EKG verisi okuyabilen herhangi bir cihazda da kullanılabileceğini savunuyor.

Kalp atış ritmine ait istatistiksel verileri kimlik doğrulamak için kullanarak, vücuda yerleştirilen tıbbi cihazların kötü niyetli saldırılara maruz kalmasını engelleyebilecek bu yöntemle birçok bilgisayar korsanının hain planları suya düşecek gibi görünüyor.

Vücuda yerleştirilen cihazların sadece sahiplerinin kullanabileceği kilidi olmaya aday kalp ritmi, bir bileklik sayesinde hayatımızın birçok alanında kullandığımız anahtarların ve şifrelerin yerini alacak gibi görünüyor.

Kaynaklar

- http://www.healthcareinfosecurity.com/medical-device-vulnerability-alert-issued-a-5847.
- http://www.secure-medicine.org/public/publications/icd-study.pdf.
- http://www.healthcareinfosecurity.com/fda-drafts-medical-device-security-guide-a-5835.
- http://www.aceslab.org/sites/default/files/H2H.pdf.
- http://www.getnymi.com/.
- http://www.newscientist.com/article/dn24141-wristband-unlocks-your-devices-with-your-heartbeat.html#.UoIaOjo5kpE.