Prof. Dr. Çetin Kaya KOÇ

Bilgi Teknolojileri ve Güvenlik Problemleri

Bilgi güvenliği teknolojileri ticaret hayatını bir çok noktadan kucaklayarak, hukuki ve gerçek anlamda gereken güvenlik mekanizmalarını işletir ve yapılan işlemlerin doğru, eksiksiz, güvenilir ve denetlenebilir olmasını sağlar. Örneğin, Türkiye'nin dört bir tarafına dağılmış bürolarınız, fabrikalarınız ve tasarım merkezleriniz varsa, bunları birbirlerine VPN (virtual private network) denilen yazılım ve donanım elemanlarından oluşmuş sistemlerle İnternet üzerinden bağlarsınız ve bütün bürolar sanki fiziksel güvenliğe sahip bir bina içindeymiş gibi çalışmalarına devam eder.

Bilgi sistemleri geliştikçe ve bizim onlara olan ihtiyacımız arttıkça, bilginin ve üzerinde aktığı veya beklediği bilgi sistemlerinin güvenliği de üzerinde düşünülmesi gereken bir konu haline geliyor. Bu ne çok abartılacak, ne de hiç önemsenmeyecek bir konu. Bilgi güvenliği firma yöneticileri, mühendisleri ve uzmanları, "bilgi güvenliği problemi" ile içinde timsahların yüzdüğü bir nehirde sörf yapmak arasında bir benzerlik kurarlar.

Dışarıda timsahlar var ve firmanızın değerlerine saldırıyor, bundan dolayı bizim ürettiğimiz güvenlik ürünlerine ihtiyacınız var! Bu analoji aslında ulaşmak istediğimiz amaca, yani güvenli veya güvenilir bilgisayar ve ağ sistemleri kurmamıza pek yardımcı olmuyor. Gereksiz bir korku yaratıp, potansiyel kullanıcıları bilgi teknolojilerinden uzak tutuyor. Sonuçta en güvenli bilgisayar, kapalı bir bilgisayar veya hiç satın alınmamış bir bilgisayar değil midir?

Bilgi güvenliği üzerinde elektronik ticaretin aktığı bilgi teknolojisi sistemlerinin ve yaratılan sanal ortamların hukuki geçerliğe sahip olmasını sağlayarak, katılımcıların mahremiyet, kimlik, eser sahipliğini ve tüketici haklarını korur. Benim faydalı bulduğum analoji işte bu ana temanın üzerine kurulu. Bilgi güvenliği ile yaptığımız şey aslında sanal bir ortama hukuki bir elbise giydirmek ve fiziksel bir ortam gibi çalışmasını sağlamak. Fiziksel bir mağazadan içeri giren müşteri ödemeyi yaptığı zaman malı alacağını ve onunla çıkabileceğini bilir. Ödemeyi nakit veya kredi kartı ile yaptığı zaman, firma çalışanları gereken noktalarda "fiziksel bütünlük" veya kimlik doğrulaması yaparak ödemenin hukuki olmasını sağlar. Ürünlerin tesliminden envanter kontrolüne, satın almadan ödemeye kadar yürüyen prosedürler, bu ortamı bütün katılımcılar için hukuki olarak güvenilir bir hale getirmiştir. Bütün hayatımız boyunca alışık olduğumuz bu fiziksel süreçler şimdi sanal ortamlar için kurulmalıdır.

Bilgi güvenliği firma yöneticileri, mühendisleri, ve uzmanları, "bilgi güvenliği problemi" ile içinde timsahların yüzdüğü bir nehirde sörf yapmak arasında bir benzerlik kurarlar. Dışarıda timsahlar vardır ve firmanızın değerlerine saldırmaktadırlar.

Örneğin fiziksel bir tatlıcı mağazasının sahte olmadığını, yıllardır aynı noktada var olmaya devam etmesi yüzünden ve bizim de un kurabiyelerimizi oradan aldığımız için "fiziksel bütünlük" nedeni ile biliriz. Sanal mağaza ise "gerçekliğini" bize Elektronik Sertifika Servis Sağlayıcısından aldığı sayısal sertifikasının bizim bilgisayarımızda kimlik doğrulanması ile ispatlamak zorundadır. Örnekler çoğaltılabilir. Hırsızlığa veya vandalizme karşı koruma da da-

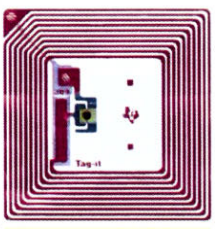
MÜSİAD

hil olmak üzere, bir çok bilgi güvenliği kavram ve tekniklerini bu analoji yardımı ile anlamak ve üzerlerinde yorum yapmak mümkündür.

Bilgi güvenliği teknolojileri, ticaret hayatını bir çok noktadan kucaklayarak, hukuki ve gerçek anlamda gereken güvenlik mekanizmalarını işletir ve yapılan işlemlerin doğru, eksiksiz, güvenilir ve denetlenebilir olmasını sağlar. Örneğin, Türkiye'nin dört bir tarafına dağılmış bürolarınız, fabrikalarınız ve tasarım merkezleriniz varsa, bunları birbirlerine VPN (virtual private network) denilen yazılım ve donanım elemanlarından oluşmuş sistemlerle internet üzerinden bağlarsınız ve bütün bürolar sanki fiziksel güvenliğe sahip bir bina içindeymiş gibi çalışmalarınıza devam ederseniz. İnternet üzerinde akan bilgilerinizin rakip firmalar veya başka nedenlerle istismarcı kişi veya kurumlar tarafından görülmesi veya değiştirilmesi derdiniz olmaz. Diğer bilgi güvenliği ürünleri, örneğin güvenli e-posta yazılımları, noktadan noktaya şifreleme sistemleri bize farklı tehditlere karşı farklı çözümler sunar ve onların yardımıyla işlerimiz güvenli yürür.

Sanki bütün bilgi güvenliği problemleri çözülmüştür veya çözülebilir türdendir diye bir izlenim vermem doğru olmaz. Bilgi güvenliği, problemlerin ve çözümlerin sürekli bir şekilde dinamik bir etkileşme için olduğu bir bilimsel alan. Güvenli sistemler tasarlanır, üretilir ve uygulamaya konulur, ama bir süre bunların açıklarını keşfederiz ve tamir etmeye çalışırız. Ancak çok da arkadaşça bir çalışma değil bu, çünkü sistem tasarlayıcıları ve uygulayıcıları ile bu sistemlere saldıran kişiler hem aynı kişiler değil ve hemde dost değiller! Çünkü saldırı amaçları farklı olabilir. Rakibiniz yerli veya yabancı firma sizin yeni tasarladığınız mutfak robotunun tasarım dokümanlarını elde etmeye veya iyi eğitilmiş bir "hacker" sizin İnternet bankacılığı şifrenizi öğrenip hesabınızdan para çalmaya veya 15 yaşında bir çocuk birtakım yanlış yönlendirmeler ile sadece arkadaşlarına böbürlenebilmek için web sitenizi göçertmeye çalışıyor olabilir. Tek bir saldırgan profili olmadığı gibi tek bir saldırı yöntemi de yoktur. Bu da bilgi güvenliği probleminin teorik olarak "kolay" bir problem olsa da uygulama da çok zor bir problem olmasına neden oluyor. Bütün bu çalışmaları bir örnek üzerinde anlatıp, hem problemlerin ne kadar çeşitli ve karmaşık ve hemde çözümlerin henüz mükemmellikten ne kadar uzak olduğu size anlatmak isterim. Seçtiğim örnek teknoloji RFID dediğimiz ve bu gün çok kullandığımız barkod teknolojisinin yerini almak üzere tasarımlanmış ve yavaş yavaş uygulamaya giren bir teknoloji.

RFID Teknolojileri

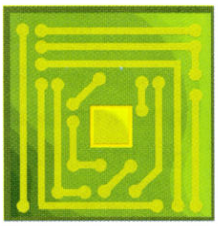


RFID Yongası ve Anteni

RFID (Radio Frequency Identification) etiketi bir anten ve içerisinde birazcık hafıza ve basit bir işlemcinin bulunduğu bir yongadan ibaret. Perakende satış dünyası için dizayn edilenlerde işlemci bile yok, sadece bir kaç yüz bitlik hafıza var. Birim maliyetinin bir kaç kuruş (5 sent'den daha az) olması gerektiği için, pilleri de yok. Etiket üzerine doğru tutulan okuyucudan gelen elektromagnetik dalgadan gelen enerjiyi kullanıp, hafızasında tuttuğu ürün numarasını anteni vasıtası ile zayıf bir elektromagnetik dalga olarak yayıyor ve okuyucuda bu dalgayı algılayıp, ürünü tanıyor. Aynı anda birden fazla ürün aynı frekans üzerinden yayın yaptığı için, okuyucu bunları ayırtedebilmeli tabii. Mobil telefonlarda da kullanılan benzer bir algoritma ile bu çakışmalar önleniyor.

RFID etiketleri ve arka plandaki enterprise bilgisayar sunucu sistemleri ile birlikte bu modern etiketleme sistemi önümüzdeki yıllarda tüketiciye dönük çok önemli gelişmeler olacak. Bir çok RFID etiketleme sistemi üretim, depolama ve dağıtımda kullanılıyor zaten. Market içi sistemler ise pilot projeler halinde devam etmekte. Maliyet ve güvenlik problemlerinin aşılması ile birlikte RFID etiketleri günlük hayatımıza girecekler. RFID etiketleri artık "elektronik ürün kodu" denilen ve ürünleri kategorik olarak değil, her bir ürünü ayrı bir şekilde seri numarası vererek barkodlardan çok daha ileri ve faydalı bir ürün tanıma sistemi oluşturacaklar.

Barkod



RFID Etiketi ve Elekronik Ürün Kodu

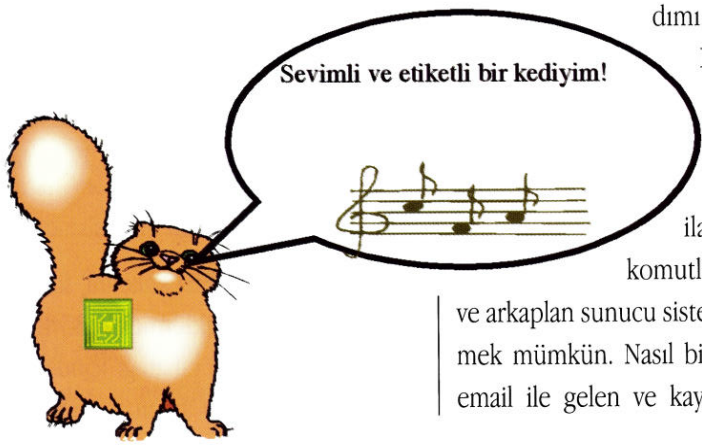
Şimdi size RFID güvenlik sorunlarından biraz bahsetmek istiyorum. Birinci güvenlik problemi tüketiciyi ilgilendiriyor: mahremiyet. RFID etiketi bir mal satıl

MÜSİAD

RFID Etiketli Evcil Hayvanlarımız

dıktan, tüketicinin sepetinde marketi terketten sonra da yaşamına devam ediyor. Bir okuyucuyu elde eden herhangi bir üçüncü şahıs, kolaylıkla sizin hangi ürünleri aldığınızı öğrenebilir, dolayısıyla eğilimleriniz, yaşam tarzınız hakkında bilgiler elde edebilir. Bu sorun dikkatli bir şekilde adreslenmeden ve tatmin edici çözümler bulunmadan RFID etiketlerinin yaygınlaşması söz konusu olamaz.

İkinci güvenlik problemi ise market sahibi olan firmayı ilgilendiriyor: sistem. Örneğin RFID etiketleri üzerinde ürün numaralari başkaları tarafından değiştirilebilmesi durumunda, firmanın zarara uğraması söz konusu. Eğer RFID yongaları kolaylıkla klonlanabilirse, perakende satış sistemlerinde kaos yaşanır. Klonlama dışında başka sistemik problemleri de var, örneğin RFID virusleri! Bu kadar küçük bir cihazın virüsü de olurmuymuş demeyin. Bir RFID etiketi sadece hafızadan ibaret, yani virusun bulaşacağı bir (işletim) sistemi yok; peki nasıl oluyorda virus dağıtımında rol alabilir? Bilimsel çalışmalar bize bunun mümkün olabileceğini gösteriyor. RFID etiketleri evcil hayvanları tanımak ve bulmak amacı ile kullanıldığından, kediniz için kullandığınız RFID etiketine virus bulaşması, daha doğrusu bu etiketin taşıyıcı olarak kullanılması mümkün! Bu durumda kedinizin bir bilgisayar virusu taşıyıcısı olduğunu düşünmeniz gerekecek. Zaten kedinin biyolojik virusleri ve diğer iç hastalıkları (detaylarını verip, iştahınızı kaçırmak istemiyorum) yetmezmiş gibi şimdi birde onun bilgisayar virusünü tedavi ettirmek zorundasınız. Semtimize artık bir "bilgisayar veterineri" gerekiyor galiba.



Virus aslında RFID etiketinde değil arkaplan enterprise sistemine bulaşmış ve başka bir arkaplan sistemine RFID etiketini kullanarak bulaşıyor. Örneğin bir arkaplan yazılımı bir veritabanına istekleri ni RFID etiketinden okuduğu veri yardımı iletiyor olsun. Eğer sistem veri formatını kontrol etmiyorsa, RFID etiketine ilave veritabanı komutları yerleştirmek ve arkaplan sunucu sistemini istismar etmek mümkün. Nasıl bir işletim sistemi email ile gelen ve kaynağı belirsiz bir programı koşturmamalı ise aynı şekilde bir RFID arkaplan sistemi de kaynağı belirsiz bir RFID etiketinden aldığı veri ile bir veritabanı isteği oluşturmamalı. RFID arkaplan sistemi aldığı verinin formatının doğru olduğunu da kontrol etmeli. Yani problem ve çözümü RFID etiketinde değil, arkaplan sisteminde. Ancak RFID etiketleri çok hızlı yerdeğiştirebildiği için (özellikle RFID etiketli kedinizi komşunun zalim köpeği kovalıyorsa!) bunları kullanarak virus bulaştırmak kolay bir hale geliyor.

RFID Klonlama Problemi

RFID etiketlerinin güvenlik problemlerinden bir tanesi de klonlama. Basit bir RFID etiketi, prensip olarak hafızasında tuttuğu kimlik belirleyici sayıyı yaymaktan başka bir iş yapmadığı için, onun bir kopyasını yapmak çok kolay. Başka bir RFID etiketine bu bu sayıyı yazmamız yeterli. RFID etiketlerinin erişim kontrolu uygulamalarında, özellikle tek adım kimlik doğrulama metodu kullanılıyorsa, klonlama olasılığı bir güvenlik tehlikesi arzediyor. Klon etiket aslı sanılacağı için, kapıdan içeri girecektir. Evcil hayvanları ve hatta insanları etiketlemek için RFID kullanılacağı için, otomatik kontrollu kapıdan sizin kedinizin yerine bir hırsız bir kedinin girmesi söz konusu!

Peki bunu nasıl önleyeceğiz. Bir fikir klonlamayı zorlaştırmak. Örneğin, karmaşık bir protokol yardımıyla, RFID cihazı, içindeki gizli bilgiyi vermeden o bilgiye sahip olduğunu ispat edebilir. Ancak böyle protokoller açık-anahtarlı şifreleme sistemlerine, sayılar ve karmaşıklık teorilerine dayanıyor. Bunları RFID yon-

MÜSİAD

galarına sığdırmak, RFID etiket teknolojisinin prensiplerine, yani ucuz ve küçük olma ve az enerji kullanma özelliklerine aykırı. Üstelik klonlamanın zorlaştırılması saldırganın fiziksel olarak RFID etiketini ele geçirmesine engel değil. Yani kedinizi ele geçirip, boynundan RFID etiketini alabilirler. RFID etiketinin deri altına implantasyonu durumunda ise daha vahim sonuçlar çıkabilir. Biyometrik sistemlere yapılan fiziksel saldırılar gibi (örneğin, saldırganın kullanıcının parmağını kesip kullanması gibi), implantasyon halindeki RFID etiketini almak için kedinizi yaralamaları ve hatta öldürmeleri söz konusu.

Başka bir çözüm var mı, diye soracaksınız. Öyle gözüküyor ki en iyi çözüm klonlamaya izin vermek. Yani klonlamayı zorlaştırmayacaksınız. RFID etiketi kimlik belirleyici sayıyı tutacak ve arzu eden herkes bu etiketin klonunu kolaylıkla elde edebilecek. Ancak arkaplandaki protokol, iki adımlı bir kimlik doğrulama metodu yardımıyla sizin kedinizin kapıdan girmek istediğini anlayacak.

RFID Mahremiyet Problemleri

Bir RFID etiketini sadece konuşlandırıldığı yerde, mesela market içindeki rafında değil, başka yerlerde de okumak mümkün. Bu problem bir mahremiyet sorunu demek ve bunu iyi bir şekilde halletmeden RFID etiketlerinin tüketiciye veya çok sayıda kullanıcıya dönük uygulamaları pek olası görülmüyor. Bu sadece benim şahsi görüşüm değil; bir çok mühendis, sosyal bilimci, ekonomist ve tüketici hakları uzmanıda aynı görüşde.

Problemi açıklayabilmek için tipik senaryo ortaya koyalım: Market içinde RFID etiketlenmiş bir ürün (daha önce arka planda yürüyen çok karmaşık envanter kontrol sistemleri ve süreçleri yardımıyla) şimdi usluca rafında müşteriyi (adına Ali diyelim) bekliyor. Ali gelip ürünü sepetine koyuyor ve diğer ürünlerinde yer aldığı sepeti ile kasiyer noktasına ilerliyor. Elektronik kasiyer, sepetteki ürünlerin RFID etiketlerini gönderdiği elektromagnetik dalgalarla enerjileyerek, her birisinin içindeki ürün kodunu okuyor ve çıkış ve ödeme işlemini tamamlıyor.

Ali şimdi otoparkdaki arabasına veya sokağın köşesindeki otobüsüne doğru yürürken, alışverişini etmiş olmanın gönül rahatlığı içinde.

Ancak evine varana kadar ve hatta evinde bile, Ali'yi bir takım hoş olmayan durumlar bekliyor. Ne yazık ki kötü kalpli "Hacker", elektronik kasanın benzeri bir okuyucu ile Ali'nin sepetindeki, alışveriş çantasındaki, arabasının arkasındaki ve hatta evinin içindeki RFID etiketleri kolaylıkla okuyabilir. Etiketi okumak için onun bir kaç metre yakınına kadar sokulmak yeterli. Fazla kalın olmayan duvarların arkasından Hacker sinsice Ali'nin alışveriş alışkanlıkları ve aldığı ürünler hakkında bilgiler topluyor. Yediği bisküviler, kullandığı ilaçlar, ve daha neler. Bu bilgilerin başkalarının eline geçmesi, mahremiyet ihlali demek.

Üstelik bu sorun "dokunma istemeyen" türünden kredi kartları içinde geçerli (mesela KGS kartları). Zarfın içinde evinize gelen bu tip kartlar, eğer içlerinde bilgiler tamamı ile şifrelenmemiş ise, posta dağıtım merkezlerinde ve hatta apartman girişlerinde kolaylıkla (zarfı açmadan) okunabilir ve bizim haberimiz bile olmadan, bazı şahsi bilgiler Hacker çetelerinin eline geçebilir.

Çözümler Hakkında

RFID etiketlerinin mahremiyet sorunlarına önerilen çözümleri anlatmaya başlayalım ama gerçekten de çözümlerin çok yetersiz. Mahremiyet problemi tüketici haklarını savunanlar tarafından çok iyi dile getiriliyor ve hatta RFID etiketlerini ürünlerinde kullanan firmalara karşı boykotlar bile başlatılmış (örneğin, Spychips.com, BoycottGillette.com, BoycottBenetton.com). Problem iyi dile getirildiği halde çözümün henüz uzakta durduğu ender durumlardan birisiyle karşı karşıyayız.

İlk akla gelen fikir RFID etiketini, satışın yapıldığı noktada "öldürmek". Böylece müşteri evine gönül rahatlığı içinde gidebilir. RFID etiketi hayatta olmadığı

için, bundan sonra herhangi bir okuma işlemine de cevap vermez. Müşteri açısında çözüm olarak gözükse bile, aslında öldürmek iyi bir fikir değil. Ürün geri verilmek istenirse ve değiştirilmek istenirse, referans noktası yani ürün kodu kaybedilmiş olduğundan zorluklar çıkar.

Ayrıca RFID etiketini öldürmek onun market dışındaki kullanımlarına da engel olur. Bizim amacımız RFID etiketli süt şişesinin buzdolabı ile konuşması ve buzdolabının ise sütün satın alındığı gün ve son kullanma tarihi gibi bilgilerini kullanarak ev sahibine yardımcı olması idi.

Bu işleri ölü bir RFID etiketi ile nasıl yapacağız? Özet olarak RFID etiketi içindeki bir sürü faydalı bilgi ve fonksiyonlar yüzünden öldürülmemesi, tam tersi hayatta tutulması gereken bir araç.

İkinci fikir RFID etiketini gölgelemek. Yani etiketi koruyucu bir tabaka içinde tutarak genel ortamlarda okunmasına engel olmak. Ancak bu çözüm de hareket kısıtlaması getirdiği için iyi bir çözüm değil.

Ayrıca marketler, hırsızların bu kapıyı istismar etmesinden endişe ettiklerinden, bu çözümü pek beğenmediler. Başka bir fikir ise çok iyi yazılmış kanun ve kurallarla kanun dışı okumaları cezalandırmak. Ancak bunun etiketlerin yasadışı okunmalarına engel olacağını beklemek hayal olur.

RFID etiketlerinin yaygın kullanılması önündeki temel engel sadece mahremiyet problemi değil. Etiketlerin maliyetleri çok düşük olmalı. Bu yüzden minimalist bir yaklaşımla dizayn edilmeleri ve üretilmeleri gerekir. İçinde kuvvetli şifrelemenin olduğu bir RFID etiketi, mahremiyet sorunlarını ileri düzey protokollerle çözebilir, ancak maliyeti etiket başına 40 dolar ise, proje laboratuarda hapis kalmaya devam edecek demektir.

RFID etiketlerinin üretilmesi ve kullanılması ile birlikte hayatımızda bazı değişiklikler olması kaçınılmaz. Mahremiyet problemlerinden kirliliğe kadar bazı sorunlarımız olabileceği gibi, RFID etiketleri mağaza hırsızlıklarına da yeni boyutlar getirecek, üstelik dikkatle planlanmış RFID saldırıları zaman ve para kayıplarına neden olacak. Eğer bir RFID etiketli DVD diski cebinize koyup çıkarsanız, çıkışa kurulmus Elektronik Eşya Gözetim Sistemi (EEGS) uyarı verecektir. EEGS sistemini devreden çıkarmak için 50 kuruş verip bir RFID etiketi satın alın. Sonra DVD üzerindeki RFID etikeni okuyup, ürün kodunu bu ucuz RFID etiketinize aktarın.

Sonra bu etiketi gidip çıkış kapısında fazla gözle görülmeyen bir yere yapıştırın. EEGS sistemi alarm verecek ve bu alarmları belli aralıklarla vermeye devam edecektir. Bilin bakalım, bir süre sonra mağaza çalışanı ne yapacak? Tabi EEGS sistemini devre dışı bırakmak zorunda kalacaktır!

Bilgi teknolojileri bir yandan hayatımıza çok büyük kolaylıklar getirip, işimizin kapasite ve yayılım alanını genişletirken, diğer yandan bu yeni dünya içinde daha önce hayal etmediğimiz riskler ve tehlikeleri de beraberinde getirir.

Son Sözler

Barkodların mağaza işleyişine ve getirdiği kolaylıkları saymakla bitiremeyiz. Barkodları elektronik, dinamik ve kablosuz hale getirelim ve onları daha faydalı hale getirelim derken, bir pandora kutusu açtık galiba. Amacımız bir örnek üzerinde bilgi teknolojisi ürününün, tasarımdan uygulamaya ve oradanda günlük hayatımıza girerken ne kadar karmaşık bilgi güvenliği problemleri yaratabileceğini anlatmaktı. Amacımıza ulaştık galiba.

Bir kaç adım daha atıp, RFID gibi henüz hayatımıza tam girmemiş bir bilgi teknolojisi ürünü yerine, hayatımıza girmiş ve bir çoğumuzun endişe ile dokunmakta kararsız kaldığı İnternet bankacılığını ele alalım. Burada potansiyel kayıplarımız çok daha yüksek ve farklılar, örneğin bakınız: www.sanalbankamagdurlari.com. Hem saldırgan ve hemde bizim için risklerin çok yüksek olduğu bir ortam söz konusu.

Önerilen sistemler ve onların güvenlik dereceleri bizi çok yakında ilgilendiriyor. Bilgi teknolojileri bir yandan hayatımıza çok büyük kolaylıklar getirip, işimizin kapasite ve yayılım alanını genişletirken, diğer yandan bu yeni dünya içinde daha önce hayal etmediğimiz riskler ve tehlikeler var. Bilgi güvenliği mühendislerine ne kadar ihtiyacımız olduğunu takdir edersiniz artık.