TÜRKİYE BÜYÜK MİLLET MECLİSİ

YASAMA DÖNEMİ	YASAMA YILI
24	3

HABERLEŞME ÖZGÜRLÜĞÜNE VE ÖZEL HAYATIN GİZLİLİĞİNE YÖNELİK İHLALLERİN TESPİTİ VE ÖNLENMESİNE İLİŞKİN TEDBİRLERİN BELİRLENMESİ AMACIYLA KURULAN MECLİS ARAŞTIRMASI KOMİSYONU

TUTANAK DERGİSİ

3 Nisan 2013 Çarşamba

HABERLEŞME ÖZGÜRLÜĞÜNE VE ÖZEL HAYATIN GİZLİLİĞİNE YÖNELİK İHLALLERİN TESPİTİ VE ÖNLENMESİNE İLİŞKİN TEDBİRLERİN BELİRLENMESİ AMACIYLA KURULAN MECLİS ARAŞTIRMASI KOMİSYONU

GÖRÜŞME TUTANAKLARI

3 Nisan 2013 Çarşamba

----0----

K O N U

İ Ç İ N D E K İ L E R

Açılma Saati: **11.02**
Kapanma Saati: **12.25**

BİRİNCİ OTURUM

3 Nisan 2013 Çarşamba

Açılma Saati: 11.02
BAŞKAN: Mihrimah Belma SATIR (İstanbul)
_____0_____

BAŞKAN – Hoş geldiniz. Herkese güzel bir gün diliyorum.

Bugün, Alt Komisyonumuzun dinleme anlamında ilk toplantısını gerçekleştireceğiz. Tartışarak, görüşerek belirlediğiniz listelerdeki ilgilileri bugün dinlemeye devam edeceğiz inşallah.

İlk dinleyeceğimiz kurum TÜRKTRUST. Buna ortak karar verdik. Daha doğrusu, bu işin ilk önerisini Erdal Bey bize yapmıştı. "Bu arkadaşlarımızı, bu yetkilileri dinleyelim ve bize bilgi versinler." dedi. Kendilerini davet ettik. Sağ olsunlar, davetimize icabet ettiler.

Bir sunum hazırlamışlar galiba. Uygulamamız şöyle: Önce sizin sunumunuzu dinliyoruz, ondan sonra biz ve arkadaşlarımız soracaklarımızı soruyoruz, soru-cevap şeklinde devam ediyoruz ve bitiriyoruz.

Buyurun efendim.

TÜRKTRUST AŞ YAZILIM GELİŞTİRME VE AR-GE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Efendim, sunumum, hem birkaç slaytla şirketimiz hakkında bilgi vermek, yaptığı faaliyetler hakkında bilgi vermek hem de şirketimizin faaliyet göstermekte olduğu elektronik sertifika ve elektronik imza konularında kısa, küçük teknik detaylar vermek.

Şöyle başlayayım: TÜRKTRUST, Türk Silahlı Kuvvetleri Elele Vakfının bir iştiraki olarak kurulmuştur. 2004 yılının Temmuz ayında, o zaman için ciddi bir sermaye ile kurulmuş ve elektronik sertifika hizmet sağlayıcılığı görevi yapmak amacıyla kurulmuş bir şirkettir. Burada amaç, dediğim gibi, 5070 sayılı Elektronik İmza Kanunu kapsamında hizmet vermek; bunun yanında, bilgi güvenliğinin diğer alanlarında, yazılım geliştirme ve diğer faaliyetleri, ürün ve hizmet faaliyetlerini sürdürmektir. Bu, kuruluşundan yaklaşık bir sene sonra kendi altyapısına ilişkin faaliyetleri tamamlamış ve o zamanki Telekomünikasyon Kurumu, şimdiki BTK, Bilgi Teknolojileri ve İletişim Kurumundan yetki belgesini alarak 2005 yılının Temmuz ayında faaliyetine başlamıştır.

Genel Müdürlüğümüz Ankara'dadır. Ankara Yıldız'da, fotoğrafta gördüğünüz binamızda hizmet vermekteyiz. Buradaki altyapımızla uluslararası ölçekte bir ESHS'nin, Elektronik Sertifika Hizmet Sağlayıcı'nın verebileceği bütün faaliyetleri sürdürebilmekteyiz. Bunun yanında, bu teknik çalışmalarımızı da -kendi bir ekibimiz var, yazılım ekibimiz var- ODTÜ Teknokent'te ve Bilkent Cyberpark'taki ofislerimizde bulunan teknik arkadaşlarla sürdürüyoruz, devam ettiriyoruz. Bunun

dışında da Türkiye'nin çeşitli yerlerinde, özellikle son kullanıcıya yönelik nitelikli elektronik sertifika satış hizmeti veren birtakım satış ofislerimiz bulunmaktadır.

TÜRKTRUST, şu anki elimizdeki bilgiler ve rakamlarla Türkiye'deki mevcut nitelikte elektronik sertifika pazarında lider kuruluştur. Türkiye'de özel sektörde TÜRKTRUST gibi iki tane ve ayrıca TÜBİTAK, kamu tarafından yetkilendirilmiş olarak diğer ESHS'ler olarak Türkiye'de hizmet vermekte olan kuruluşlardır. TÜRKTRUST'ı diğerlerinden ayrı kılan, özel sektördeki ESHS'lerden ayrı kılan en önemli özelliklerden bir tanesi, ilk kuruluşu itibarıyla kendi altyapısında çalışan bütün yazılımları kendisi geliştirmiş, bütün teknolojiyi ve oradaki know-how'u elinde bulunduran, hiçbir dış bağımlılığı olmayan, yazılım anlamında ve altındaki teknolojiler anlamında bir kuruluş olmasıdır. Bunun yanında, hemen kuruluşunun arkasından itibaren, hemen ilk yılındaki faaliyetleriyle, özellikle SSL pazarında da -o detaya gireceğim, SSL sertifikaları sunucular içindir, nitelikli elektronik sertifikalar kişiler için verilen sertifikalardır- faaliyet gösterebilmek için Microsoft, Mozilla, Apple gibi değişik Browser üreticileriyle iletişime geçerek onların "store"larına girmek amacıyla çalışmalar yürütmüş ve bunları başarıyla tamamlamış bir firmadır. Bu yazılım ürünlerimizle de hem yurt içinde hem yurt dışında, hem ürün satışı gerçekleştirmiş hem de çok çeşitli bilgi güvenliği projeleri yapmış bulunmaktayız. Birkaç belge… Bunların bazıları zaten ESHS olabilmek için olmazsa olmaz belgelerdir. Örneğin, 27001: Bilgi Güvenliği Yönetim Sistemleri Standardı. Buna sahibiz, bu olmadan zaten ESHS faaliyetinizi sürdüremiyorsunuz. Bunun yanında 9001 yazılım kalitesi belgelerine, Millî ve NATO Tesis Güvenlik Belgeleri'ne sahip bir firmayız. Özel güvenlik birimi istihdam edebiliyoruz, öyle bir yetkimiz var ve ayrıca en önemlisi olarak da, en alta gördüğünüz, Türkiye'deki ETSI TS 102 042 ESHS Yönetim Sistemi Standardı'nı almış tek firmayız, tek sertifika sağlayıcıyız. Bu belge sayesinde -yine belki birazdan teknik olarak bahsedeceğim- sunucu sertifikalarındaki özel birtakım sertifikaları da, EV SSL denilen sertifikaları da verebilme yetkisi kazanıyoruz.

ERDAL AKSÜNGER (İzmir) – Pardon, araya girebilir miyim?

BAŞKAN – Tabii.

ERDAL AKSÜNGER (İzmir) – Şimdi şöyle: Teknik çok anlattığınız için biraz da arkadaşlar anlamıyorlar bence konuyu, öyle hissediyorum çünkü. Yani, bu nedir, ne değildir…

BAŞKAN – Anlıyoruz, anlıyoruz.

ERDAL AKSÜNGER (İzmir) – Sen anlarsın da yani SSL Sertifika ne demek, bilmem öbürü ne demek…

ALİ ERCOŞKUN (Bolu) – Anlıyoruz.

ENVER ERDEM (Elâzığ) – Teknik olanları anlamıyoruz tabii canım.

ERDAL AKSÜNGER (İzmir) – Anlıyorsanız tamam, o zaman problem yok. anlıyorlarsa problem yok, o zaman yanlış söylüyorum.

BAŞKAN – Dinleyelim.

ERDAL AKSÜNGER (İzmir) – Hayır, hayır, şunu demek istiyorum ben, şunu: Şimdi, normalde, biraz daha halk diline indirgerseniz konuyu… Ben çünkü teknik terimleri soracağım size zaten, bazı konuları. Yani, mesela, bu nedir? Dijital noterdir. Anlatabiliyor muyum? Yani, sonuçta…

ENVER ERDEM (Elâzığ) – Sizin anlattığınız boyutuyla da ilgili…

ERDAL AKSÜNGER (İzmir) – Ya, onu, tekniği ben soracağım zaten sana, o ayrı bir konu ama yani bu bir dijital noter sonuçta yani devlet adına noterlik yapıyor veya dijital platformda. "store" dediğiniz de işte, o, gidip Google'da veya Microsoft'ta… "Browser" dediniz. Biraz bunları açıklarsanız yani o zaman anlamı daha rahatlar diye düşünüyorum, ondan söz ediyorum yoksa teknik şeyleri, biraz zor onları anlamak.

TÜRKTRUST AŞ YAZILIM GELİŞTİRME VE AR-GE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Haklısınız efendim. Aslında şöyle: Hemen arkasındaki sunumlarda şeyden bahsetmiştim. Hani, bu kavramları zaten basitçe açıklamaya çalışacaktım, sadece burada tanıtım olduğu için öncelikle geldi, o yüzden şey olmuştu. Hemen arkasında, şurada zaten anlatmaya başlıyorum. ESHS nedir? Elektronik Sertifika nedir? SSL nedir? Bunlar hakkında kısa kısa bilgiler vereceğim. Hemen de zaten yeri gelmişken oraya geçeyim.

TÜRKTRUST, bir elektronik sertifika hizmet sağlayıcıdır Türkiye'de. Bu elektronik sertifika hizmet sağlayıcılar ne yapar? Türkiye'deki 5070 sayılı Elektronik İmza Kanunu'na göre "Elektronik sertifika hizmet sağlayıcı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan gerçek veya tüzel kişilerdir." diye geçer bu maddede. Bu kapsamda, son kullanıcıları veya elektronik sertifika hizmetleri yasa kapsamındaki kısmı nitelikli elektronik sertifikaları ilgilendirir. Nitelikli elektronik sertifikalar da kişilere verilen sertifikalardır. Yani, biz mesela, bu yasa kapsamında şu yetkiyi yapıyoruz ve şöyle çalışıyor hizmetlerimiz: Siz bir şahıs olarak elektronik sertifika almak için başvuruda bulunuyorsunuz. Bu alacağınız elektronik sertifika sizin elektronik imza atabilmenizi sağlayan bir araç. Bu sertifika, bir akıllı kartta, özel birtakım donanımlarda veriliyor, belli güvenlik standartları sağlaması lazım. Böyle bir donanım üzerinde size kendi adınıza çıkarılmış olarak -bir kimlik belgesi gibi düşünebilirsiniz, elektronik kimlik belgesi gibi düşünebilirsiniz- teslim ediliyor. Buradaki en önemli özellik, en önemli detay, gerçekten o kişiye verdiğinize emin olmanız lazım. Yani, nitelikli kılan, yasa karşısında geçerli bir elektronik imza atmanız, nitelikli elektronik imza atmanız. Onun için, nitelikli elektronik sertifika sahibi olmanız lazım. Nitelikli elektronik sertifikayla ESHS'ler gerçek kişilere gerçekten onlar olduğunu bilerek vermekle yükümlü. Yoksa zaten oradaki zincir hiçbir şekilde işlemez, güven zinciri hiçbir şekilde işlemez.

Bu elektronik imza mevzuatı, Türkiye'de, hem 5070 sayılı Elektronik İmza Kanunu hem de ona bağlı olarak BTK'nın çıkardığı yönetmelikler, Başbakanlık genelgesi, birtakım teknik tebliğler, bunların eklerinde bulunan teknik tebliğler ve zorunlu mali sigorta düzenlemeleri gibi birtakım mevzuatı içeriyor. Hem teknik hem idari olarak bu mevzuatın hepsini sağlamakla yükümlü buradaki ESHS'ler.

Nitelikli elektronik sertifika da -biraz önce ifade etmeye çalıştım- yine, 5070 sayılı Elektronik İmza Kanunu'nda "Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur." ibaresi var. Yani, sizin, nitelikli elektronik sertifikanızla yaptığınız elektronik imzalama işlemi elle attığınız imzayla aynı eş değerlikte. Bu yasa çıktığında birtakım kapsam dışında tutulan yerleri vardı. Bunlar nedir? Özel merasime tabi olan işlemlerdir. Örneğin, elektronik imzayla evlenemezsiniz veya tapu işlemleri yapamazsınız. O tarz yani özel birtakım merasime tabi olan şeyler ama onun dışındaki bütün işlemlerde nitelikli elektronik imza, elle attığınız imzayla aynı hukuki sonucu doğurur.

Nitelikli elektronik sertifikaların en önemli özellikleri, o imzayı kimin attığını birebir tespit etmenize imkân sağlar. Yani, aslında, elektronik sertifika işlemi kriptografik matematiksel bir işlemdir, imzalama işlemi. Bu imzalama işleminde, böyle, elle attığımız imzalarda nasıl o imzanın size ait olduğunu tespit etmeyi sağlayan birtakım kriminal yöntemler varsa burada da daha matematiksel ve algoritmik yöntemlerle bunun gerçekten o kişi tarafından atılıp atılmadığı tespit edilebilir.

Sadece -biraz önce anlattığım gibi- gerçek kişiler nitelikli elektronik sertifika sahibi olabilirler, tüzel kişiler nitelikli elektronik sertifika sahibi olamazlar ve bu nitelikli elektronik sertifikanın içerisinde de kimlik bilgileri yer alır. Bu, yine, mevzuatta bulunan birtakım teknik dokümanlarda belirlenen, işte, belli şeyler var. Örneğin, sertifikanın içerisinde TC kimlik numarası yazmalıdır, adı soyadı yazmalıdır, vesaire gibi birtakım kriterler var, onlar kapsamında sertifikalar dağıtılır. Şu görsellerden şeyi anlayabilirsiniz, bunlar böyle birtakım cihazlar, bilgisayarınıza USB portundan takabildiğiniz, memory, flash disk'ler şeklinde olabilir ya da akıllı kartlar, okuyucular şeklinde olabilir. Bu sertifikaları alıp bunlarla elektronik imza işlemi gerçekleştirebilirsiniz. Şurada da zaten şeklin üzerinde görebiliyorsunuz, bir nitelikli elektronik sertifikanın -5070 sayılı Elektronik İmza Kanunu madde 9'a göre- içerisinde nelerin olması gerektiği belirtilmiş durumda. Bu sertifikaların kimin adına verildiği, -biraz önce bahsettiğim gibi- geçerlilik süresinin ne olduğu -o da olması gereken bir bilgidir- ve diğer ilgili alanların neler olması gerektiği yasada belirtilmiştir.

Bunun dışında, biraz önce sizin de bahsettiğiniz gibi, daha çok, noterlik tarafı diyebileceğimiz... Hani, bu taraf sanki birazcık nüfus işi gibi. Yani, geliyorsunuz o kişiye, gerçekten o olduğunu bilerek bir kimlik belgesi veriyorsunuz, bir imza atabilecek nitelikli elektronik sertifika veriyorsunuz. Bir de işin zaman damgası tarafı var. Yine yasayla belirlenen, 5070 sayılı Elektronik İmza Kanunu. Zaman damgası da şöyle bir şeydir, o birazcık daha noterliğe daha yakın sanki: Bir belgenin -yasada geçen tabiriyle- o an itibarıyla mevcut olup olmadığını belirlemeye yarayan bir bilgidir zaman damgası. Bu şöyle çalışır kabaca: Elektronik ortamda bir belge oluşturdunuz.

ERDAL AKSÜNGER (İzmir) – Doğru olup olmadığını...

TÜRKTRUST AŞ YAZILIM GELİŞTİRME VE AR-GE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Mevcut olup olmadığını belirtir, zaman vardır çünkü.

Bu şöyle çalışır kabaca: Bir belgeniz var elektronik ortamda, Word veya başka bir formatta hazırladığınız bir belge. Bu belgeyi -özellikle telif haklarında çok yaşanan şeydir- hani, ben yazmışımdır fakat oldu ya çaldırmışımdır bir şekilde diskimden veya işte laptop'ımdan, bunu başka birisi kullanmıştır. "Bu benim." diyemezsiniz. Hani, burada şey var: Elle yazdığınızda belki imzalarınız var, notere onaylatıyorsunuz, vesaire ama burada elektronik bir belgede birtakım sorunlar çıkabilir. Bu durumlarda biz zaman damgası hizmeti vermekle de yükümlüyüz, 5070 sayılı Elektronik İmza Kanunu'na göre. Siz bu belgenin bir özetini -bir HS özetini, teknik tabiriyle, eşsiz bir özettir o, hiçbir belgenin özeti birbiriyle eşleşmez, öyle söyleyeyim- zaman damgası hizmet sağlayıcıya gönderiyorsunuz -belgenin kendisini değil, özetini- zaman damgası hizmet sağlayıcı ona zaman bilgisini ekliyor -o anki zaman bilgisini, gerçek zaman bilgisini ekliyor- ve üzerine kendi elektronik imzasıyla imzalıyor bu hizmet sağlayıcı -örneğin, TÜRKTRUST- ve size geri gönderiyor. Siz bu zaman damgası bilgisiyle o dokümanı birebir şekilde kriptografik olarak doğrulayabilirsiniz, ona ait olduğundan emin olabilirsiniz. O dokümanın üzerinden en ufak bir değişiklik o zaman damgasını da geçersiz kılacaktır, aynı elektronik imzada olduğu gibi, elektronik imzada da aynı şey söz konusudur. Böyle olunca, o belgenin gerçekten, o tarih itibarıyla sizde olduğunu, o zaman damgası dosyasıyla size ait olduğunu doğrulayabilirsiniz. Böyle bir mekanizmadır. Biz bunu vermekle de yükümlüyüz, zaman damgası hizmetlerini. Bunlar yasal yükümlülüklerimiz yani nitelikli elektronik sertifika ve zaman damgası yasa kapsamında vermekle yükümlü olduğumuz hizmetler. Bunun dışında da diğer sertifikalar var. Biraz önce bahsi geçen SSL sertifikaları, sunucu sertifikaları, basit elektronik sertifikalar ya da nesne imzalama sertifikalar gibi. Bunlar nereden kullanılır? SSL sertifikaları sunuculara kullanılır. Örneğin, hepimiz banka işlemleri yapıyoruz. Bankalarda, o aramızdaki İnternet üzerindeki trafiğin güvenli bir şekilde oluşabilmesi için, aradaki trafiğin izlenememesi, takip edilememesi için bir SSL sertifikası kullanılır. O sertifikalardır burada kastettiğim sertifikalar. Böylece, sizin İnternet tarayıcınızla karşı taraftaki sunucu arasındaki trafik güvenli bir şekilde bu sertifika vasıtasıyla işletilmiş olur.

Bunun yanında, örneğin, nesne imzalama sertifikaları şeydir, bir kod yazmışsınızdır, yazılım firmasısınızdır; yazdığınız kodların gerçekten size ait olduğunu -dağıtıyorsunuz çünkü bunları, başka insanlar kullanıyor- belirlemek için "Bu ürün gerçekten bana aittir." diye o kodları imzalarsınız ve onlar, kurulum yapılırken kurulum ekranlarında sizin imzanızla gözükür. Bu tarz, birtakım başka sertifikaları da sağlıyoruz, bunların hizmetlerini de veriyoruz ve bunları tabii mevzuatın dışında olan diğer hizmetlerimiz.

Biraz önce açıklamaya çalıştım: Bu SSL ve EV SSL sertifikaları… EV SSL'de SSL'in bir üst seviyesi sertifikadır, güvenlik seviyesi biraz daha artırılmış bir sertifikadır. Aslında teknik olarak bir farkı yoktur, teknik, güvenlik açısından altyapısında bir fark yoktur, sadece idari birtakım şeyleri kapsar. Mesela, siz bir SSL sertifikasını sunucuya… Aynı, kişilerde nasıl şey vardır, görmediğiniz birisine vermemeniz gerekiyor sertifikayı. SSL sertifikalarında, size belgelerini göndermişse, noter onaylı veya

kendisi hazırlayıp istediğiniz belgeleri göndermişse -mevzuata dâhil değil çünkü bu- siz ona sertifika verebilirsiniz ama EV SSL sertifikası verebilmeniz için gerçekten o kurumun orada olup olmadığını bilmeniz lazım. Örneğin, gidip görmeniz lazım. Birtakım idari tedbirler var, bunları kayıt altına almanız lazım. Türkiye'de şu an EV SSL sertifikası verebilen bir ESHS yok. Biz bunun çalışmalarını yaptık geçen sene içerisinde. Yıl başında talihsiz bir şey yaşadığımız için bir süredir askıda ama sanırım bu sene sonunda tekrar her şey yolunda gidecek ve zaten süreç de ilerliyor. Tekrar biz bu süreci ESHS olarak vermeye başlayacağız, EV SSL sertifikalarımızı ama SSL sertifikası hizmetlerimiz zaten devam ediyor, bu hiçbir kesintiye uğramadı.

Benim TÜRKTRUST hakkında ve bu teknik konular hakkında aktaracaklarım bunlar. Sorularınıza cevap vermeye çalışalım.

BAŞKAN – Teşekkür ediyoruz.

Arkadaşların varsa soruları, başlayalım sorularımıza.

Ali Bey…

ALİ ERCOŞKUN (Bolu) – Evet, öncelikle sunum için teşekkür ediyoruz, sağ olun.

Burada, tabii, bu sertifikalandırma işlemini yaparken kullandığınız algoritmalar yani kendi içinizdeki şeyler, bunlar millî mi yani tamamen siz mi ürettiniz veya dışarıdan gelen, dışarıdan sağlanan şeyler mi? Bu algoritmalarınızın kripto analiz değerlendirmelerini nasıl yapıyorsunuz? Bunları sizin dışınızda yapan herhangi bir kurum, kuruluş var mı? Yani, burada gördüğümüz kadarıyla, lider, tek… Ama sizin dışınızda kimse var mı?

Bu, gazetelere konu olan problemi, uluslararası camiada ve akademik çevrelerde özel olarak hani, sanki özel olarak böyle bir şey yapıldığına dair şeyler çıktı, bundan dolayı test ve kriptoloji yani o süreçlerde bir değişiklik yaptınız mı? Yani bu, herhâlde en fazla merak edilen konu, sizin de "Talihsiz olay." dediğiniz konu.

Tabii, bunların üretilmesi için çok ciddi bir AR-GE desteğinin olması lazım. Şimdi, 2004'de kurdunuz, 2005'te hemen yani bir yıl sonra yetkiyi aldınız, çalışmaya başladınız. Yani, burada tüm detaylara hakim olabilmek için aslında ciddi bir altyapı lazım. Yani, bu altyapıyı sağlama noktasında geçmişten tecrübeler mi vardı? Yani, o da önemli bence. Dolayısıyla, bu konuda üniversitelerle veya başka kurumlarla iş birliğiniz oldu mu? Veya, -nasıl diyelim- çalışan kişiler yani sizdeki personelin ulusal, uluslararası düzeylerde yayınları, bu konularda deneyimleri var mı? Dolayısıyla, nerelerde var, nerede bu deneyimleri görebiliriz?

ISO standardı var, gördük ama bu NIST, FIPS gibi, dünyada hani şöyle baktığımız zaman bu standartları almak tabii gerekmiyordur anladığımız kadarıyla belki ama böyle bir çalışma var mı?

Kripto altyapıları yani sizin ürettiğiniz kripto altyapılarının analiz raporları var mı yani bu tür bir raporlama çalışması var mı? Eğer varsa bunları paylaşma şansınız var mı bizimle?

Teşekkür ederim.

BAŞKAN – Bir şey söylemek istiyorum.

Öner Bey, arzu ederseniz sorulara cevap verebilirsiniz, arzu ederseniz zabıtlar size gönderilir, yazılı olarak da cevap verebilirsiniz. Şu anda, kısa, aklınızda olanları yani cevap vermek istediklerinizin hepsini dinleyelim biz. Çünkü, vereceğiniz cevaplara göre yeni sorular da gelebilir, böyle bir imkân da var, onu söylemek istedim.

Teşekkür ederim.

TÜRKTRUST AŞ YAZILIM GELİŞTİRME VE AR-GE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Anladım.

ERDAL AKSÜNGER (İzmir) – Soralım mı, cevap mı verecek?

BAŞKAN – İsterseniz hepsini soralım.

ERDAL AKSÜNGER (İzmir) – Tamam, soralım bence.

BAŞKAN – Erdal Bey, buyurun.

ERDAL AKSÜNGER (İzmir) – Ben de hoş geldiniz diyorum her şeyden önce, sunumunuzdan dolayı da teşekkür ediyorum.

Şimdi, birincisi, tabii, geçmiş dönemde, bu, "dijital noterlik" derken, eser konusunda söyledim bir vesileyle. Şimdi, Türkiye'de insanların bilgileri, zaten bu elektronik imza ve güvenlik ölçeğiyle karşılıklı altyapıda birbirini test eden, arka tarafta iki tane programın birbirine okey vermesiyle sağlanıyor. Yani, siz de aslında bu tarafındasınız işin bir tarafından baktığınızda. Hani bunu Türkçe mealiyle söylüyorum yani daha teknik söylemeyeyim: Yani, birisi geliyor, bir yere girdiği zaman altta çalışan program karşı taraftaki sertifikaya bakıyor. O baktığı zaman, bu sertifika yetkili kurumlar tarafından yapılmış güvenli bir şey ise bütün bilgileri oraya rahatça girebilir şekilde izin veriyor, orası da açılıyor browser'la. Siz de giriyorsunuz, her türlü bilginizi orada yapabiliyorsunuz. Bankadır, özel bilgilerinizdir, hepsini orada güvenli bir şekilde yapmak kaydındayız.

Doğru mu? Aslında özeti bu hikâyenin.

TÜRKTRUST AŞ YAZILIM GELİŞTİRME VE AR-GE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Doğrudur, doğrudur.

ERDAL AKSÜNGER (İzmir) – Şimdi, geçen yıl yaşanan olayda özellikle şunu merak ediyorum, birincisi: Mesela, iki tane kuruma bununla ilgili sehven olduğunu söylediğiniz. Sizin, hani, basına düşen açıklamalarda öyle, "Bu yetkiler sehven verilmiştir." diye. Yani şunu verdiniz orada, yanlışlıkla veya sehven ne ise: Bu iki kuruma da sertifika verme yetkisi verdiniz. Yani, bunlar da dediler ki: "Bizden gelen bütün elektronik sertifikaların hepsi de doğrudur."u siz teyit etmiş oldunuz sehven veya yanlışlıkla. Bu iki kurumdan bir tanesi Kuzey Kıbrıs'ta, bir tanesi de Ankara'da, Ankara Büyükşehir EGO. Şimdi, Kuzey Kıbrıs hiç kullanmamış bunların hiçbirisini, EGO kullanmış mesela. Ne yapabilir mesela bunlarla ilgili? Ve, bu dağıtılmış olan veya onların verdiği bu elektronik imzalar veya sertifikalarla bugüne kadar tespit ettiğiniz nedir? Nasıl önüne geçilebilme operasyonu yaptınız? Bir

kere, bu verdikleri sertifika ve elektronik imzalarla neler yapılabilir? Yani, Komisyona anlatmanız benim açımdan önemli. Çünkü, bunu Google Chrome ortaya çıkarttı. Dedi ki:"Sitede bütün herkesin bilgilerini alırlar karşı tarafa da ulaşırlar." Bunu söyleyen Google, kendi rakiplerinin hepsine de gitti, Microsoft'a da, diğer, işte bütün... Aslında rakipleri olanların hepsine de aynı şeyi söyledi. Onlar da ortak bir açıklama yaptılar, "Bunların hepsi sahtedir ve insanların bilgileri toplanabilir, toplanma ihtimali de olmuştur." dedi. Onunla ilgili ne diyorsunuz? Bunun çok önemli bir şey olduğunu düşünüyorum ben zaten.

Kuzey Kıbrıs bunu iade ettikten sonra siz bunu diğer Ankara Büyükşehirden ya da EGO'dan talep ettiniz mi, etmediniz mi, en başta yani konu ilk gündeme geldiğinde?

Bir de şunu söylemek istiyorum: Şimdi, bizim Komisyonun genelde ana işi, özel hayatın gizliliği konusu var zaten veya işte, oraya yapılan müdahaleler. Haberleşme özgürlüğüne bir vesileyle olabilecek kasıtlar konusunda çalışma yapıyoruz. Sizce, sonuçta, bu siteler konusunda birinin özel mahremiyetini bu yapılan işlemle birlikte gerçekten oraya müdahale edilebilir mi yani böyle sahte bir elektronik imzayla haberleşme özgürlüğüne darbe vurulabilir mi bununla ilgili?

Anlatabildim mi bilmiyorum ama herhâlde teknik anlatmamaya çalıştım, gerçi, herkes de anlasın diye anlatmaya çalışıyorum genelde. Anladınız değil mi?

TÜRKTRUST AŞ YAZILIM GELİŞTİRME VE AR-GE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Anladım, eğer tam açıklayamazsam...

ERDAL AKSÜNGER (İzmir) – Tamam, peki. Bende sorular var, açıklamanıza göre tekrar devam edeceğim.

Teşekkür ederim.

BAŞKAN – Var mı başka sorusu olan arkadaşımız Enver Bey.

ENVER ERDEM (Elâzığ) – Yok.

BAŞKAN – Ben de bir iki şey sorabilir miyim, biraz daha şirketinizle ilgili?

TÜRKTRUST AŞ YAZILIM GELİŞTİRME VE AR-GE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Tabii.

BAŞKAN – Şirketin kuruluşunda veya daha sonrasında görev alan malikler hakkında, hissedarlar hakkında bize bir bilgi verebilir misiniz? Birincisi bu.

İkincisi, sunumunuzda "Özel güvenlik birimi istihdam ediyoruz." dediniz. Doğru mu?

TÜRKTRUST AŞ YAZILIM GELİŞTİRME VE AR-GE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Doğrudur.

BAŞKAN – Oradaki kişilerle ilgili kafanızda soru işareti veya uygulamada sıkıntı yaşadığınız şeyler oldu mu? Onu öğrenmek istiyorum?

Biraz evvelki sohbetimizde barolar birliğiyle anlaşma yaptığınızı, -büyük bir güç barolar birliği ve üye sayısı fazla olan bir birimdir biliyorsunuz- avukatların elektronik imzasını sizin

üzerinizden aldığını öğrendik. Ben de bir avukatım. Avukatlarla ilgili herhangi bir şey yaşadınız mı? Onu öğrenmek istiyorum.

Teşekkür ederim.

Bir soru daha var, Sayın Vekilimiz de sorsun.

ŞİRİN ÜNAL (İstanbul) – Hoş geldiniz. Verdiğiniz bilgiler için teşekkür ediyorum.

Biliyorsunuz, RSA anahtarlarının boyu gittikçe büyümektedir. Bu da şifreleme ve imzalama süreçlerinin uzamasına, bundan dolayı da sistemin yavaşlamasına sebep olmaktadır. Bunun yanında piyasada olan RSA sertifika anahtarlarının pek çoğunun gerçekte güvensiz olduğu ortaya çıkmıştır. Sertifikalarınız çok daha hızlı ve çok daha güvenli olarak bilinen eliptik eğri yöntemlerini kullanıyor mu? Bu yapıların AR-GE desteğini ve güvenliğini, güvenilirliğini ve doğruluğunu nasıl sağlıyorsunuz?

Ürettiğiniz anahtarları saklıyor musunuz? Saklamıyorsanız bunu denetleyen bir kurum, kuruluş var mı? Saklıyorsanız ne tür bilgiler bulunduruyorsunuz? Sisteminizde ve veri tabanlarınızda sakladığınız bilgiler nelerdir? Kişisel bilgiler ile ilgili neler saklıyorsunuz?

İstihdam ettiğiniz personeli hangi kaynaktan alıyorsunuz, seçmek için özel bir kriteriniz var mı? Siz olsanız, yasa dışı dinleme ve izlemeleri ve özel hayatın güvenliği konusundaki problemleri nasıl çözersiniz?

Teşekkür ederim.

BAŞKAN – Öner Bey, buyurun.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Teşekkür ederim.

Aldığım notlara istinaden sırayla cevap vermeye çalışayım.

Şimdi, ilk olarak bu algoritmalarla ilgili bir konu vardı. Bizim faaliyet gösterdiğimiz sektörde elektronik sertifika hizmet sağlayıcılarının mevzuattaki belirlenen altyapıdaki bütün algoritmalar açıktır. Yani kamuya açık algoritmalardır, tüm dünya tarafından kabul görmüş ve tüm dünya tarafından aynı şekilde kullanılan algoritmalardır. Yani burada millî, gizli, dışarıya bilinmemesi gereken bir algoritma kullanılmamaktadır. Bu algoritmaların gücü algoritmanın herkes tarafından bilinmesi fakat o algoritmayla üretilmiş anahtarların çözülmesindeki güçlükten gelmektedir. Bu en son sorudaki RAS anahtarıyla ilgili kısım da orasıdır ve burada -bahsettiğim gibi- millî, gizli bir algoritma kullanılmamaktadır.

Şimdi, yaşanmış şeyle gideyim, hemen arkasından ISO'yla bağlayayım aslında: ISO 27001 Sertifikası -dediğiniz gibi, benim de biraz önce belirtmeye çalıştığım gibi- mevzuat gereği olmazsa olmaz bir şey zaten. Bizim bunu mutlaka işletmemiz gerekiyor ama mevzuat zaten onun dışında başka bir sertifika sahibi olmamızı zorunlu tutmuyor fakat biz buna rağmen özellikle şu en son problemlere dolaylı olarak sebep olan -aslında sebep o değildir, orada o hazırlık sırasında yapılmış olan bir hatadır- konuda olduğu gibi biz kendi inisiyatifimizle hiçbir şey olmadan, birtakım dışarıdan yani Türkiye'de

bunu vermeye yetkili kuruluş BTK'dır; bunun dışındaki dünya tarafından kabul görmüş kurumlara denetimler yaptırarak birtakım başka sertifikalar, başka güvenlik şartlarını sağlamaya çalışıyoruz. Burada dediğiniz gibi NIST'in veya FIPS'in özel olarak bir şeyini kullanmıyoruz, sertifikasına sahip değiliz ama mevzuat gereği kullanmak zorunda olduğumuz donanımlar bu sertifikalara sahip olmak zorunda ki, biz de o donanımları kullanıyoruz yani size verdiğimiz bir akıllı kartın, örneğin içerisinde sertifika olan akıllı kartın bu standartları sağlaması zaten mevzuat gereğince zorunlu. O yüzden onlar da sağlıyorlar o belgelerle. Zaten biz Türkiye'de TÜBİTAK'ın üretmekte olduğu, çeşitli şeyleri de kullandık geçmişte ama özellikle son dönemde TÜBİTAK tarafından üretilmekte olan ve bütün bu standartları sağlayan akıllı kart işletim sistemi var biliyorsunuz -AKİS, duymuşsunuzdur- hatta yeni elektronik kimlik kartlarımızda da kullanılacak olan o kartları kullanıyoruz, AKİS kartlarını kullanıyoruz; bunlar da bu standartları sağlayan ürünlerdir.

Kripto altyapılarının analiziyle ilgili olarak şöyle: Buradaki algoritmaların hepsi -dediğim gibi- açık algoritmalar. Bu açık algoritmalar tarafımızdan implemente edilmiş algoritmalar yani burada algoritmayı biz yeniden yaratmadık ama o bilinen algoritmalar üzerinde bütün yazılımlarını kendimiz yaparak alt tarafında bunları kullandık.

Bu algoritmaların tabii ki birtakım testleri vardır. Yine bir şeyi yazdığınızda onun testlerini de yazarsınız ve testlerini de yaparsınız. Bu testleri yapıyoruz zaten, yaptık ve bu algoritmalarımızın güvenilirliğini tespit ettikten sonra bu algoritmaları kullanıyoruz. Ayrıca sadece yazılım değil, mesela yine mevzuat gereği, biraz önceki o akıllı kartlarda olduğu birtakım ESHS'lerin kullandığı özel donanımlar da vardır. Bunu şey gibi düşünebilirsiniz, kişilere akıllı kart da verilir, onun işlem gücü sınırlıdır, zayıftır, birkaç işlem yapabilirsiniz üzerinde, imzalama işlemleri yavaş olur ama bunun daha büyüğünü -belki işte şöyle cihazlar düşünün- masaüstü kullanabildiğiniz daha büyük cihazlar, bunlara HSM denilir, hardware security module'dür "Güvenlik Donanım Modülü"dür adı teknik tabiriyle, o cihazlar da aslında akıllı kartların -basitçe bakarsanız- daha büyüğüdür, işlem gücü daha yüksek olanıdır ve ama aynı güvenlik standartları sağlayanıdır hatta daha fazlasını sağlayanıdır. Biz o HSM'leri kullanıyoruz, kullanmazsak zaten hani mümkün değil böyle bir şeyi yapabiliriz, tüm EV SSL'ler kullanıyor, tüm EV SSL'lerde de HSM'ler vardır ve gizli anahtarları EV SSL'lerin gizli anahtarları o HSM'lerde saklanır. O HSM'ler de yine benzer şekilde bu kripto anahtar üretme işlemleri, imzalama işlemleri vesaireler için hepsinin sertifikalarına ve belgelerine sahip cihazlardır. O yüzden de hani bunların hem kendi tarafımızdaki yazılımsal olarak hem de donanımların bir testleri yapılmış durumdadır; öyle diyebilirim.

İlk başta not almayı kaçırdığım için, yaşanmış problemle ilgili sorularınız vardı, arzu ederseniz ikisini bir arada birleştirerek ben konuyla ilgili biraz bilgi vermeye çalışayım, çok kısa tarihçesini anlatayım yaşanan problemin.

BAŞKAN – Çok iyi olur.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Problem, yılbaşında başımıza gelen konu, medyada da çeşitli şekillerde çıktı açıkçası; bunun medyada çıkmasının sebebi de işte Google'ın ilk el olarak saptadığı ve daha sonrasında diğer browser'ların da güvenlik açıklamaları yaparak bildirdiği konudur. Konu şöyle bir konu: Biz Ağustos 2011'de bu bahsettiğim EV SSL verebilmek için, gerekli sertifikayı alabilmek için dışarıdan bir denetim geçirmek durumundaydık. Bu denetim tabii çok ciddi bir denetim yani bizim mevzuatımızdakilerden farklı şeyler de isteniyor bu hizmeti verebilmeniz için, bu yüzde altyapımızda ciddi bir yenileme faaliyeti gerekti yani kendi yazılımlarımızı da kendimiz yazdığımız için -biraz sonra o insan kaynağıyla ilgili şeye de geleceğim- oradaki bütün esnekliğe sahibiz. Bu altyapımızda kendimiz bir yenileme faaliyeti başlattık hem veri tabanlarımızda hem yazılımlarımızda vesaire vesaire… Bu sırada birtakım test platformlarımız var -hepsi production ürünün çalıştığı gerçek platform, bir de test platformlarımız var tabii ki bu yazılımları test ettiğimiz- orada basın açıklamalarımızda da anlattığımız şekilde Ağustos 2011'de test sisteminde kullanılmış olan iki tane üretim şablonu yani bu şablonu şöyle anlatabilirim: Siz sertifikalarınızın ne tip çıkmasını istiyorsanız, işte son kullanıcısı sertifikası mı olacak, yoksa aradaki bir -burada olduğu gibi- alt kök sertifika mı olacak? Bunların bir şablonları vardır. Her sertifika için bir şey yapmazsınız, aynı şablonları kullanırsınız. Buradaki iki hatalı şablon gerçek sisteme yanlışlıkla aktarılmıştır, buradaki geçiş çalışmaları sırasında, bunun farkına da varılamamıştır, buradaki en büyük problem budur. Biz zaten bunu da açıklamalarımızda olduğu üzere kabul ettik yani burada bir hata yapılmış ve bu farkına varılamamıştır o anki güncelleme çalışmasında. Ağustosun 8'inde bize iki tane kurumdan SSL başvurusu yapılmış o tarihte -aslında daha iki gün önce yapılmış fakat biz bu geçişi tamamladıktan sonra ilk sertifika üretilen kurumlar onlardır- Kuzey Kıbrıs Türk Cumhuriyeti Merkez Bankasıdır bir tanesi, diğeri de EGO Genel Müdürlüğüdür Ankara'daki. Bu iki kurumun sertifikası o hatalı şablonlarla üretilmiştir. O hatalı şablonlar da aslında SSL sertifikası olması gerekirken o sertifikaların bir alt kök yani bizim hiyerarşik olarak… Şöyle düşünebilirsiniz, size çizerek karşıdan aktırmaya çalışayım: En üstte bir kök sertifika vardır, bu TÜRKTRUST'un köküdür, bunun altında birtakım alt kök sertifikalar vardır; örneğin -biraz önce bahsettiğim- nitelikli elektronik sertifika, kişilere verdiğimiz ya da bir SSL verdiğimiz sertifikalar. Bunların altından biz sertifikaları veririz, bunlar alt kök sertifikalarımızdır. Hiyerarşik ve kriptografik olarak bakarsanız da bunlar zincir hâlinde çalışırlar, birbirlerini tamamlarlar. Şuradan altında vermemiz gereken SSL sertifikası, SSL kökünün, alt kökünün altında EGO'ya ve KKTC Merkez Bankasına vermemiz gereken sertifikalar bu hatadan dolayı bunlarla aynı seviyede gibi düşünebilirsiniz -tam altında değildir ama mantık olarak öyle düşünebilirsiniz- özellikleri aynıdır yani şu kökümüze bağlı değildir fakat özellik olarak şunlarla içerisindeki özellikleri taşımaktadır. İki tane hatalı sertifika verilmiştir.

Şimdi, buradaki en büyük problem şuydu bizim açımızdan ve özellikle bizim bu ilişkide olduğumuz Mikrosoft, Mozilla, Apple gibi diğer browser üreticileri bu sorunun kaynağını tam olarak

tespit edebilmekti. Mesela, bunu vermişiz ama sadece bu iki sertifikada mı vermişiz? En büyük problem odur. Hani başkalarına da vermiş misiniz? İlk gelen sorudur zaten bize. Veri tabanımızda yaptığımız bütün kontrollerde başka hiçbir sertifikaya rastlamadık bu ikisi dışında. Niye bu ikisinde var, daha sonra niye olmadı peki? Onu da tespit ettik, bununla ilgili çok ciddi çalışma yaptık biz. Bütün kayıtları da elimizdedir. Bu çalışma sonucunda şunu tespit ettik: O 8'inde sertifikalar üretildikten sonra -bunlar süre olarak üç yıllık sertifikalardır- bir sonra gelen sertifika yani bundan sonra üretilmesi gereken, bir sonra gelen sertifika başka bir sertifikadır, bir özel şirkete ait sertifikadır. Şablon uymadığı için sistem hata vermiştir, üç yıllık değil, iki yıllık gelmiştir oradaki. İki yıllık şablonda hata fark edilince orada bir yanlışlık olduğu anlaşılmıştır fakat şablonların yanlış üretildiği anlaşılmamıştır, bir sistem hatası olarak düşünülmüş, "O şablonu biz taşımamış." diye düşünmüşüz ve test sisteminden değil de bu sefer gerçekten olması gereken şablonları geri koymuşuz üzerine, her şey normal çalışmaya başlamış. Yani o iki sertifikadan sonraki sertifikada problem tespit edilmiş, sorunun ondan kaynakladığı anlaşılamamış fakat bir sorun olduğu anlaşılmış "Herhâlde biz bu şablonları eksik taşıdık." denilip, bu sefer hatalı olmayan, doğru olan yerden taşınmış ve her şey yoluna girmiştir. Yalnız biz en çok zorluğu burada taşıdık. Niye? Çünkü sonrasında bu problem devam etmedi. Orada birtakım şeylerimiz var mesela, en büyük kendi içimizdeki, iç denetimlerimizde ve kendi içimizde yaptığımız eleştirilerde de o oldu: Buradaki değişikliği tespit edememiş olmak, daha doğrusu teknik tabirle change management yani yaptığınız birtakım değişikliklerin yönetimine ilişkin süreçleri iyi takip edememiş olmak zaten bizim bu hatayı sebep olmuştur orada ve ondan sonra her şey normal yürümüştür. Fakat biz bundan haberdar olamadık, tabii o sertifikaları hatalı ürettiğimizi de fark etmedik. Açıkçası o tarih itibarıyla sistemimizde hani veri tabanımızın tamamını tarayıp da, geçmişe doğru tarayıp "Hatalı ürettiğimiz bir sertifika var mıydı?" diye inceleyen bir altyapımız da yoktu yani üretilmeyeceğini varsayıyordu aslında oradaki.

ERDAL AKSÜNGER (İzmir) – Bir süre onlar kök sertifika verebilme yetkisine sahip olmuşlar.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Sahip olmuşlardır.

ERDAL AKSÜNGER (İzmir) – Onu anlatırken şunu demek istiyor insan yani alttaki kökle sertifikaları da verebilme yetkisine sahip olmuş bunlar.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Tabii doğrudur.

ERDAL AKSÜNGER (İzmir) – Bayağı bir zaman sürecinde…

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Doğrudur.

ERDAL AKSÜNGER (İzmir) – Farkındalar mı?

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Hemen oraya geleyim efendim?

KKTC Merkez Bankası bu sertifikayı kullanamamış, sistemlerinde anahtarlarını değiştirmişler, başka sertifika kullanmışlar, zaten onu iptal etmişler, hiç kullanmadan başka sertifika almışlar tekrar ve o sertifikayı kullanmışlar.

EGO'daki problem ise: EGO bunu kendi sunucularına yüklemiş, web sunucularına yüklemiş, o anda herhangi bir problem yok web sunucularında. İşin enteresanı mesela, oradaki ürün özelinde web sunucunun yazılımı da mesela, bu sertifikaya "hatalı sertifika" dememiş, ona hizmet vermeye devam etmiş, bu bir webmail'dir yani kendi çalışanlarının webmail SLL sertifikasıyla bağlanıp maillerine ulaştıkları bir sitede kullanılmıştır. Burada herhangi bir sıkıntı yoktur. Bu ana kadar da sertifikanın bu şekilde kullanılmasında bir güvenlik açığı da yoktur aslında. Sunucu izin verse SSL işlevini yapmıştır. Ne zamanki kurum altyapısında birtakım değişikler yapmış… Biz bununla ilgili tabii EGO'yla aynı şeyi tespit edebilmek için bir çalışma yaptık yani biz de anlamaya çalıştık orada nasıl buna sebep olabildiğine bu problemin, anlamaya çalıştık. Bizim elimizdeki bilgiler şunu gösteriyor: Aradan bir buçuk yıl geçtikten sonra -Ağustos ayından Aralık 2012'ye geliyoruz- Aralık 2012'nin 21'inde EGO'da bir güvenlik duvarı çalışması yapılmış, bu çalışma sırasında güvenlik duvarlarında… Şimdi, Komisyonunuzun da şey yaptığı gibi birtakım güvenlik kuralları alınabilir, güvenlik duvarları üzerinde uygulanabilir. Şirketlerde, kamu kurumlarında, özelde ya da kamu kurumlarında kullanılabilen birtakım yöntemler vardır. Buradaki güvenlik duvarı üzerinde "SLL Inspection" denilen bu güvenli kanalın içerisinden geçen trafiği anlamaya yönelik, daha doğrusu o trafiği yönetmeye yönelik bir cihazların yetenekleri vardır. bu yeteneği devreye almak istemiştir EGO kendi kapsamında. Burada da bir sertifika kullanılması gerekir çünkü sertifika şöyledir: Sizi browser'ınızdan tarayıcınızdan siz İnternet'e bağlanmak istediniz; örneğin, Facebook'a bağlanmak istediğinizde güvenli bir şekilde Facebook'a bağlantı kurarsınız. Burada eğer o trafiği denetlemek isterseniz arada bu trafiği kesmeniz, sertifikayla kendi üzerinizde kullandığınız sertifikayla -teknik tabiri man in the middle'dır "ortadaki adam" diye düşünülebilir- bir işlem yaparsınız; bu, bilinen bir işlemdir yani bir yöntemdir bu işi yapabilmek için. EGO da bunu yapmak istemiştir. Birçok şeyde kendi tasarruflarıdır, kendi inisiyatiflerindedir fakat burada ellerinde TÜRKTRUS'tan verilmiş bir SLL sertifikası var -onlar hâlâ SLL sertifikası olduğunu düşünmektedirler bu arada, bize aktardıkları ve bizim en azından süreçten de gördüğümüz odur- "SLL sertifikamız var, tekrar biz yeni sertifika üretmeyelim, nasıl olsa orada kullanıyoruz sunucuda ve firewall'a da bunu yükleyelim." diye düşünmüşlerdir. Firewall'a yükledikleri anda bu sertifika olmasından fazla yetkili olduğu için yani normalde standart bir SLL sertifikası olsaydı hiçbir problem yoktu bizim gerçekten vermemiz gereken ama biz yanlış bir sertifika verdiğimiz ve olmasından fazla yetkilerle olduğu için bu işlem sırasında aradaki sertifika Google'ın tespit ettiği

birtakım sertifikaları üretmiştir, Google'ın bir… Çünkü o SLL Inspection işlemi zaten birtakım fake sertifikalar üretmektir teknik tabiriyle.

ERDAL AKSÜNGER (İzmir) – Öyle tabi.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – O sertifikaları da Google kendi tarafındaki bir yöntemle -biz gene teknik açıklamalarımızda Google'daki bütün teknik yetkililerle de iletişim içerisindeydik- tespit etmiştir, public key pinning denilen teknik tabiriyle, Google'ın bir güvenlik algoritmasıdır, bununla onlara uyarı vermiştir. Bize de 21 Aralıkta bu çalışma yapıldıktan sonra 26 Aralık günü Google'dan bir e-posta ile bildirim geldi, dediler ki: "Böyle bir sertifikası var, bu sertifikanın üretilmesini biz sizden talep etmedik ama böyle bir konu tespit edildi, nedir?" diye bizim araştırmamız için şey yapıldı. Bunun üzerine biz aynı gün konu üzerinde bütün teknik çalışmaları yaptık ilgili sertifikaları iptal ettik hemen ve konuyla ilgili çalışmaya başladık. Bu arada biraz önce bahsettiğiniz gibi arka tarafta aslında bu browser'lar, İnternet güvenliğini ilgilendiren bir konu olduğu için rakip de olsalar aslında olması gerektiği gibi bir birliktelik vardır orada hatta browser'lar ve ESHS'ler arası bir forum da söz konusudur, bizim de üye olduğumuz bir forum vardır orada. Burada bilgi alışverişi ve teknik bilgi alışverişi yapılır zaten bu forumda. Orada duyurulmuş ve diğer browser'lar da bununla ilgili tedbirleri almışlardır. Yapılan şey şudur: TÜRKTRUST'ın hiçbir kök sertifikası iptal edilmemiştir, hiçbir kök sertifikası browser'lardan dışarı çıkarılmamıştır çünkü biz bütün teknik çalışmamızı gayet açıklıkla yaptık, bütün objektifliğimizle yaptık, elimizdeki bütün bilgileri paylaştık. Bu sertifikaların içerisinde birtakım şeyler vardır; yine teknik tabirler ama şöyle ifade etmeye çalışayım: Mesela, siz o sertifika kullanıldığında tarayıcı şeye sorar -bu, kişilere verilen sertifikada da öyledir aynı kredi kartı provizyonu gibi düşünebilirsiniz- "Bu sertifika geçerli mi?" diye, aynı kredi kartını geçirdiğinizde bankalar arası kart merkezine nasıl soruyorsa onu veren ESHS'ye "Bu sertifika geçerli mi?" diye sorulur. Bu soru sırasında kimler için sorulduğu, hangi zamanlarda geldiği bu sorguların falan tespit edilmişti bizim tarafımızdan. Hiçbir anomali aslında görülmemiştir burada. Bunların hepsi karşı taraflarla paylaşılmış ve karşı taraftan Google tarafından da örneğin, bunu kullanarak herhangi bir sahteciliğin yapıldığına ilişkin bir kanıt olmadığı da Google tarafından da açıklanmıştır. Bu Mozilla'daki herkese açık forumlarda görülebilir. Bu konuyu bildiren, ilk olarak duyuran Google yetkilisinin kendi açıklamaları da vardır. Bununla ilgili herhangi bir şey tespit edilemedi ama bu hatanın ne olduğunu tespit etmek çok önemliydi bizim için. Bir kere, bir daha olmayacağını tespit etmek de çok önemliydi. Bunların hepsi açık şeffaf bir şekilde hem kamuoyuyla hem ilgili bu tarayıcı firmalarla paylaşılmıştır. Bizim çıkarılan sertifikalarımız daha doğrusu iptal edilen sertifikalarımız sadece bu verilmiş olan iki hatalı sertifikadır. Bu iki hatalı sertifikayı iptal etmişler, kendi listelerine almışlar, onun dışındaki…

BAŞKAN – Sanıyorum yeterli açıklama oldu bununla ilgili.

ENVER ERDEM (Elâzığ) – Şimdi, bunlara dayanarak başka sertifika verilmemiş mi?

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Hatalı sertifika verilmemiş durumdadır.

Hemen orayı da tamamlayayım efendim.

Biz bu konu ortaya çıktıktan sonra hemen ocak ayının başında sistemimizde güvenlik tedbirleri aldık, bu nedir? Zaten var olan ama bunu öngörmediğimiz, geçmişe doğru olmayan birtakım başka tedbirler ekledik, bunları da web sitemizde açıkladık, kamuoyuyla da paylaştık. Dedik ki: "Hem anlık olarak, o an için hem de daha sonra geriye dönük olarak bütün sertifikalarımızı biz düzenli olarak kontrol eden birtakım proseslerden geçiriyoruz ve böyle bir şeyin hem olmasına izin vermiyoruz hem böyle bir şey olduğunda da anında haberimiz olacak şekilde mekanizmaları kurduk." birincisi budur.

İkincisi, özellikle bizim bu change management -hani biraz önce bahsettiğim- idari bir şeydir o, iyi yönetememizden kaynaklanan, prosedürlerimizin hepsini güncelledik, o prosedürleri yeniledik ve ocak ayının sonunda bu prosedürlerimizdeki yeniliğe ilişkin yine yurt dışındaki İngiliz Standartları Enstitüsü ona yetkili sertifikayı vermeye, bir de denetçi kuruluş gelerek tekrar bizi denetledi ve buradaki değişikliklerimizle ilgili şeyleri onayladı ve oradaki süreçlerimiz de değişti. O yüzden şimdi o tarih itibarıyla, o tarihten öncekinden çok daha güvenilir bir haldeyiz, tedbirlerimizi almış durumdayız.

BAŞKAN – Teşekkür ederiz.

Erdal Bey…

ERDAL AKSÜNGER (İzmir) – Birincisi zaten şöyle düşünmek lazım: Mesela "Hiç üretilmedi." diyorsunuz yani sahte sayılan elektronik imza. EGO tarafından hiç üretilmedi mi diyorsunuz?

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Şöyle, biraz önce bahsetmeye çalıştım, o cihazın üzerine koyduğunuzda o cihazın kendisi biraz önce bahsettiğim sertifikaları üretir.

İLHAN CİHANER (Denizli) – Otomatik mi üretiyor?

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Otomatik üretir, otomatiktir yani kimse oraya elle müdahale etmez.

ERDAL AKSÜNGER (İzmir) – İçerideki yazılımı nasıl yönlendirdiğin de önemli orada. Mail trafiğini bir vesileyle… Şunu da sordum size: "Bunları yapan birisi neler yapabilir?" mesela diye. Mail trafiklerini, Twitter'ı, Facebook'u veya diğer bilgilerin hepsini, trafiği yönetebilir; doğru mu? Bütün bilgilere ulaşabilir mi? Ulaşabilir. O mailden üretilmiş bütün sertifikaları karşıda herhangi bir mail adresleri veya başka bir konu mesela, Twitter, Facebook diğer şeylerin hepsini üretmişse bunların hepsini tekrar oraya yönlendirebilir komple, o bilgilere sahip olabilir komple. Yani buna benzer bilgileri istiyorum sizden.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Tabii.

Efendim, bunu net olarak şöyle ifade edeyim: Bu sertifikanın özel yetkili sertifika olmasının bu konuyla herhangi bir ilgisi yoktur. Yani siz standart TÜRKTRUST'ı hiç düşünmeyin, TÜRKTRUST veya herhangi bir ESHS olmasına da gerek yok. Bu yazılımların hepsinde, güvenlik duvarı yazılımının hepsinde kendi içinde gelen bir ESHS yazılımı vardır yani kendi iç kullanımı için kullanılan bir ESHS yazılımı vardır. Bu işi yapabilmeniz için zaten bu ESHS yazılımından kendi tanıdığı bir tane sertifika üretip o cihaza yüklersiniz yani TÜRKTRUST'tan, herhangi bir yerden aldığınız bir SLL sertifikasına ihtiyacınız yoktur, dediğiniz anlamda SLL Inspection işlemini yapabilmek için yani bu çok bilinen, her yerde bilinen, sektörün kendinde olan, oradaki güvenlik duvarlarının bir özelliği olan bir şeydir. Bu niye vardır? Bu teknoloji niye geliştirilmiş bir teknolojidir? Takdir ederseniz aynen burada tabii işin kişisel güvenlikle, kişisel bilgilerin gizliliğiyle ilgili olduğu gibi şeyleri de var; örneğin, sizin içerinizden, iç trafikten dışarıya giden bir özel trafik söz konusu takip edemediğiniz. İşe diğer tarafından bakın, belki 5651 Yasa'sı kapsamında illegal bir trafik söz konusu olabilir veya -atıyorum- içeride bir virüs veya başka bir backdoor facility'siyle bir şey yapılmıştır, oradan giden trafiği de izleyemiyorsunuzdur. O yüzden bunları engellemek amaçlı SLL Inspection özelliği firewall'lardır, tüm dünyada yapılan eklenmiş bir özelliktir. Bu özelliği kullanmak için -biraz önce bahsettiğim gibi- böyle özel yetkili bir sertifikaya vesaireye ihtiyacınız yoktur, kendi içinden üretilmiş bir sertifikayla da bunu kullanabilirsiniz. Zaten kurum bunu kullansaydı herhangi bir problem yoktu veya kullansaydı, kullanmasaydı ama bizim verdiğimiz sertifikayı oraya yüklemeyi düşündüklerinde "Nasıl olsa var bir daha üretmeyelim onu kullanalım." dediğinde -buradaki basittir yaklaşım- bizim verdiğimiz sertifika da hatalı olduğu için böyle bir şeye sebep olmuştur.

ERDAL AKSÜNGER (İzmir) – Şimdi, bu mail server'a kurulmuş bir şey ama normalde bir İnternet sitesi de oluşturabilir böyle bir sertifikayla diyelim, karşıda Facebook veya Twitter veya herhangi birisi yani oradan kendisine, account sahibi olan herhangi bir kişi kişisel güvenliğini karşı taraftaki sitenin altındaki aslında güvenlik sertifikası onaylayacak yani mesela, Twitter'dan Fecebook'tan veya Google'dan bir yerden o siteye girdiğinizde o datanın, o karşı taraftaki sitenin güvenliğini onaylayan verdiğiniz kök sertifikaları verebilir.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Şöyle: Normal şartlarda bu sertifikalar her hâlükârda oluşturulur biraz önce bahsettiğim gibi.

ERDAL AKSÜNGER (İzmir) – Şimdi bakın, "Oluşturur" ayrı bir şey. Sizin verdiğiniz tek bir tanesinde aşağıda noter yetkisi vermiş oldunuz normalde birisine öyle değil mi? Yani kaba tabiri bu aslında.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Evet.

ERDAL AKSÜNGER (İzmir) – Kaba tabirle ona bir noter yetkisi verdiniz, bir tane kuruma. Bu kurum, bunu suistimal etmiş mi etmemiş mi?

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Bizim tespitlerimize göre ortada şeye ilişkin bir kanıt biz bulamadık açıkçası yani bunun kullanıldığına ilişkin bir kanıt bizim elimizde yoktur.

BAŞKAN – Tamam.

İLHAN CİHANER (Denizli) – O zaman niye iptal edildi yetkisi?

ERDAL AKSÜNGER (İzmir) – Yani Kuzey Kıbrıs kullanmadı zaten Merkez Bankası, onlar kendileri…

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Evet, onlar kullanmadı.

ERDAL AKSÜNGER (İzmir) – Şimdi sorun da şu: Bir yıl öncesinden onlar zaten bu konuyu görüyorlar -bir sürü şeyi- kullanmıyorlar başka bir yerden alıyorlar. Burada kullanılan bir konu var anlatabiliyor muyum? Sorun burada çelişki yaratıyor bir taraftan da. Onlar iade ediyorlar size değil mi?

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Efendim bizden alıyorlar gene, yine bizden alıyorlar.

ERDAL AKSÜNGER (İzmir) – Başka bir sertifika alıyorlar.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Başka bir sertifika alıyorlar yani kullanmayıp da başka bir şey değil, yine bizden alıyorlar ama başka bir sertifika alıyorlar, yeniden anahtar üretiyorlar. Kendi taraflarındaki teknik bir şey olabilir onu bilmiyorum.

ERDAL AKSÜNGER (İzmir) – Bu sehven yapılmış da, bu bir cinayet aslına bakarsan yani öldü birisi "Kusura bakmayın yanlışlıkla öldü." gibi de olabilecek yani tabiri caizse bu böyle…

ALİ ERCOŞKUN (Bolu) – O kadar da değil.

ERDAL AKSÜNGER (İzmir) – Öyle öyle yani bu sertifikayı bana ver, ben sana binlerce adamın bütün verisini toparlayabilecek kabiliyete sahip olurum yani çünkü bütün mail trafiğini yönlendirebiliyor.

ALİ ERCOŞKUN (Bolu) – Zaten onu söylüyorlar.

BAŞKAN – Söylüyorlar.

ERDAL AKSÜNGER (İzmir) – Google veya browser'ların hepsi demiş ki: "TÜRKTRUST'un verdiği sertifikalar hepsi güvenlidir." Doğru mu?

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Tabii, doğrudur.

ERDAL AKSÜNGER (İzmir) – Şimdi, aynı yetkiyi bana verdiğiniz zaman ben de bütün ne kadar Google, Facebook bilmem kim varsa, eğer niyetimde bir şey varsa, bütün bu adamların kişisel bilgilerini toparlayabilir miyim?

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Elinizde böyle bir sertifika varsa tabii ki toparlayabilirsiniz.

ERDAL AKSÜNGER (İzmir) – Verdiniz sertifika, ben de alıp toparlayabilir miyim?

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Tabii ki toparlayabilirsiniz.

ERDAL AKSÜNGER (İzmir) – Konu bu.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Problem şu…

ERDAL AKSÜNGER (İzmir) – Yani teknik anlatmak istemiyorum sen teknik anlatıyorsun. Ben anlatırken farklı şekilde anlatmaya çalışıyorum anlatmak istediğim tehlike bu yani böyle bir tehlike verilmiş, "Bu suistimal edilmiş mi edilmemiş mi?" başka bir konu. Siz şu an onların bilgilerine dayanarak bunu söylüyorsunuz.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Efendim, kendimizdeki bilgilerle de teyit ediyoruz. Yani biraz önce bahsettim o sertifikalar kullanıldığında -aynı o provizyon işleminden bahsettim biraz önce- o sertifikaların geçerliliğiyle ilgili bizim sunucularımızda da sorgular yapılıyor. Bu sorguların yapılıp yapılmadığı, ne kadar kullanıldığına ilişkin de bizim elimizde de birtakım istatistiki bilgiler var yani bu kayıtlara göre biz Google'la da bunları paylaştık, açık açık hepsini gönderdik, aynı şekilde onlardan da karşılıklı bir teyitleşme oldu yani bunun kullanıldığına ilişkin bununla ilgili bir sahtecilik yapıldığına ilişkin bizim elimizde bir kanıt yok.

ERDAL AKSÜNGER (İzmir) – Google sahte olarak tanımladı zaten bütün üretilmişleri.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Köklerimizi çıkarmadılar, sadece "O iki sertifika hatalı üretilmiştir." diyerek çıkardılar; iki sertifika.

BAŞKAN – Sadece o iki sertifika.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Evet. Mesela böyle bir şey olsaydı köklerimizi de çıkarırlardı, daha büyük bir problem olsaydı.

ERDAL AKSÜNGER (İzmir) – Ama bu büyük bir tehlike ya. Yani biz bunu çok anlatamıyoruz gerçi de bu tehlike şu: Herkes için tehlike yani senin mail adresinden birisi istediği zaman yönlendirebilir, mail bilgilerini de alabilir.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Efendim, böyle bir sertifikaya veri artık verilmeyeceğine ilişkin…

ERDAL AKSÜNGER (İzmir) – İşte "sehven yapıp" dediğim cinayet buydu onu demek istiyorum yani ben de merak ediyorum, siz dediniz ki: "Biz onlara sorduk, onlar bu işin suistimal edilmediğine dair bize teminat verdiler." ve EGO için…

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Hayır öyle bir… Yani şöyle: Teminat vermeleri veya şey gibi değil, biz sadece teknik çalışma yaptık, bunun nasıl olabileceğine yönelik bir çalışma yaptık orada çünkü konuyu anlamamız gerekiyordu, biz de anlamaya çalışıyorduk nasıl olduğunu. Hem kendi tarafımızda teknik çalışma yaptık hem de EGO'daki yetkililerle çalıştık karşılıklı olarak, onların yaptıkları hangi işlemin buna sebep olduğunu anlamaya çalıştık çünkü o kaynağın şey olması lazım. Mesela, onların söylediği, bize verdiği bilgilerle her şey burada yanlışlıkla yapılmış bir işlem olduğunu teyit ediyor açıkçası ama hani "Biz bunu böyle yaptık." diye bir teyit vermedikleri gibi biz de bir şeyi teyit etmedik açıkçası. Bizim elimizdeki bilgiler ışığında söylediğimiz şeydir sadece bu.

BAŞKAN – Öner Bey, çok teşekkür ediyoruz açıklamalarınız için.

Diğer sorular eksik kaldı, onları yazılı olarak cevap verirseniz memnun oluruz.

TÜRKTRUST AŞ. YAZILIM GELİŞTİRME VE ARGE MÜDÜRÜ MUSA ÖNER DEMİRKOL – Peki efendim.

BAŞKAN – Arkadaşlar size zabıtları bir şekilde ulaştıracaktır, onlara cevap verirseniz çok memnun oluruz.

Çok teşekkür ediyoruz katkınız için, sağ olun.

Arkadaşlar, ara verelim mi yoksa devam edelim mi, hocalarımızı dinleyelim mi?

ENVER ERDEM (Elâzığ) – Devam edelim.

BAŞKAN – Devam edelim, peki. Şimdi gündemimizdeki ikinci konuya geçiyoruz. Şu anda Bilkent Üniversitesinden iki hocamız var bizimle beraberler. Onlar da bir sunum yapacaklar.

Hocam, hoş geldiniz.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Teşekkür ederiz, sağ olun.

BAŞKAN – Vereceğiniz destek için şimdiden teşekkür ediyoruz.

Çalışma usulümüzü biraz evvel gördünüz. Sizin sunumunuzu izleyeceğiz, ondan sonra sorularımızı soracağız. Kendinizi de tanıtarak başlarsanız çok memnun oluruz.

Buyurun efendim.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Ben Bilkent Üniversitesi Elektrik Elektronik Mühendisliği Bölümünde ses, görüntü, video işleme konusunda bir uzmanım. Bu ses sinyalleri ya da başka sinyallerden anlamlı bilgiler çıkarma konusunda çalışmalar yapıyorum.

Profesör Ayhan Altıntaş da…

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Evet, ben de Bilkent Üniversitesi Elektrik Elektronik Mühendisliği Bölümünde öğretim üyesiyim. Benim çalışma alanlarım da daha çok elektromanyetik alanlar, radarlar gibi konular. Ayrıca, İSYAM adı verilen İletişim ve Spektrum Yönetimi Araştırma Merkezinin direktörlüğünü de yapıyorum.

BAŞKAN – Buyurun Hocam.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Ben kısaca bu modern ses ve konuşma, işleme sistemleri hakkında bilgi vermek istiyorum. Günümüzde bu tür sistemler artık sayısal ortamda çalışmaktadır ya da -halk dilindeki şeyle- dijital işlemler yapılmaktadır. Bu ses modellemesi ve ses sentezlemesi konusunda bir bilgi vereceğim. Daha sonra görüntü işleme ve kameralar hakkında bilgi vereceğim. Rakamlarla resim, görüntü işleme ve sayısal video… Orada da her şey rakamlarla ifade ediliyor ve birtakım sunuşlarım var.

Şimdi, daha önce de belirttiğim gibi ses sinyalleri rakamlarla ifade edilebilir ya da konuşmalar rakamlarla ifade edilebilir. Telefonda konuştuğumuzda saniyede 8 bin rakam üretiriz standart telefonlarda. Daha sonra, şu yan taraftaki grafiklerde mesela "fa" sesinin grafiği var -yani bir fonksiyon gibi çizebiliriz- diğeri de "sa" sesinin grafiği var, birisi "fa" ve "sa" demiş. Cep telefonlarında ise her konuşanın 20-30 milisaniye içinde gırtlak modeli çıkarılır. Daha sonra bu gırtlak modeli 10 rakam olarak şebeke üzerinden diğer telefona gönderilir. Orada da yine saniyede 8 bin tane rakam örneklenir ve o rakamlardan her konuşanın gırtlak modeli üretilir. GSM şebekesinde havada giderken bu rakamlar şifreli olarak GSM'in standardının belirlediği rakamlar şifrelenir. Dinleyen taraf da yani diğer, konuşmanın öbür tarafında ses, yazılım aracılığıyla yarı yapay olarak sentezlenir. Gırtlak modeliniz karşı tarafa gittiği için -aynen fiziksel olarak ses ürettiğimiz gibi, gırtlağımıza ciğerlerimizden hava basarak ve ses tellerimizi titreştirerek ürettiğimiz gibi- bilgisayar ortamında ses sentezlenir. Bunun amacı, havada daha az bilgi taşımaktır ve elektromanyetik spektrumu daha etkili kullanmaktır. Bu, aslında sayısal ses sentezleme işini de gündeme getiriyor. Metinden ses sentezleme bilgisayar ortamında yapılabilir ve bu problem aslında tamamıyla çözülmüş bir problemdir diyebiliriz. Yani, bu kes-yapıştır yöntemiyle herkese her şey söyletilebilir yeterince kayıt varsa, bu bütün kelimeleri de söylemesi gerekmiyor o kişinin. Bizim hani ilkokulda öğrendiğimiz gibi hece tabanlı sistemler vardır, yeterince böyle bir iki sayfa bir okuma, metin varsa o kişiye her şey söylettirilebilir. Hatta İnternet'te şeyler de

var… Ben burada birtakım sentez şeyleri de getirdim yani kendim, dün akşam sentezlediğim şeyler var. Onlar bu sunumda yok da şu Amerikan Telefon ve Telgraf Şirketinin yazılımıyla yaptığımız şeyler var, burada örnekler vereyim şimdi.

İLHAN CİHANER (Denizli) - Bu yazılıma herkes ulaşabiliyor mu kolaylıkla?

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Tabii, tabii, İnternet'te var. Bu, İnternet'teki biraz böyle sekiz on senelik hatta belki de on beş senelik bir şey ancak daha yenileri çok daha güzel. Şurada şimdi…

(Profesör Doktor Enis Çetin tarafından ses kaydı dinletildi)

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Mesela bu tamamen yapay bir şey, o AT&T Şirketinin sayfasından aldığım şey.

(Profesör Doktor Enis Çetin tarafından ses kaydı dinletildi)

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Bu, birine Ahmet Enis dedirttim, Amerikalı birine.

(Profesör Doktor Enis Çetin tarafından ses kaydı dinletildi)

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Bu, İngiliz birine…

(Profesör Doktor Enis Çetin tarafından ses kaydı dinletildi)

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Bu da Alman, falan…

(Profesör Doktor Enis Çetin tarafından ses kaydı dinletildi)

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Böyle gidiyor. Hatta şu anda İnternet'e de bağlıyız,oradan gösterebilirim de yani şeyleri.

Yani, kes-yapıştır yöntemiyle heceleme, ilkokullarda okuma-yazma öğretirken heceler vardı. Heceleri uygun bir şekilde kes-yapıştır yaparsanız, uygun rakam dizisini de üretirseniz -rakam dizisi üretmek- daha sonra sesi rakamlardan sentezliyoruz.

Şimdi, görüntü ve resimler… Aslında cep telefonlarında, kameralarda, görüntüler de yine rakamlarla ifade ediliyor. Renkli resimler mesela kırmızı, yeşil ve mavi rakam matrislerinden oluşuyor. Mesela, şu gördüğünüz renk, kırmızı 187, yeşil 224, mavi 224 dediğiniz zaman bilgisayar ekranında o renk oluşuyor. Büyük bir resim oluşunca da bunlardan arka arkaya bir sürüsünü koyuyorsunuz ve resim oluşuyor. Yine, dijital resimlerle de kolayca kes ve yapıştır yapılabilir. Zaten fotomontaj, hepimiz biliyoruz, eskiden beri var. Orada da yine… Mesela yine son zamanlarda Angela Merkel'in resmi çıktı. Bu gerçek midir, fotomontaj mıdır bilmek mümkün değil aslında. Yani, yine uzmanlar araştırıp birtakım

raporlar üretebilir, bir uzman gerçek diyebilir, diğeri sahte diyebilir vesaire. Mesela, şu ikinci sırada bir aslan yürüyor, o aslanı oradan yok etmişler. Aşağıda iki tane kız çocuğu var, çok güzel bir şekilde montajlanmış resimler. Bu konuda da araştırma şeyleri var, kameranın karakteristiğine göre ayrıştırmaya çalışılıyor falan ama yüzde yüz bu resim gerçektir ya da bu resim -İngilizce tabiriyle- "doktor" edilmiştir ya da işte, montajlanmıştır demek yine mümkün değil çünkü rakam dizileri var. Ancak her şey gittiğinde yine bir rapor üretilecek, bir uzman sahtedir diyebilir, başka bir uzman gerçektir diyebilir.

Sayısal videoya gelince, sayısal, dijital video arka arkaya gelen sayısal resimlerden oluşmaktadır. O da yine rakam dizilerinden oluşuyor. Rakamlar, saniyede 25 tane rakam, resim gelince video oluyor. Yine, videoya da obje montajı yapılabilir ya da objeler silinebilir.

Şimdi, bu güvenilir ses, görüntü ve video aktarımı için bunlar şifrelenmiş olarak telefon hatlarından, İnternet ya da haberleşme hatlarından, İnternet üzerinden gönderilebilir. Deminki arkadaşımız bu RSA şifreleme algoritmasından bahsetti. Mesela o kullanılabilir ya da işte, TÜBİTAK-MAM'ın geliştirdiği algoritmalar var, onlar kullanılabilir. Aynı şekilde, açık olarak da bunlar yine gönderilebilir güvenilir olarak. Bu durumda sinyalin bu rakamlarının içine filigran rakamları dizisi gömerek otantik olduğu ya da oynanmış olduğu belirlenebilir ama bu durumda her resmi çektikten sonra kendinizin onu bu sertifika gibi şey yapmanız lazım. Başkası oynadığı zaman o rakam dizisi kırılır ve sahte olduğu bulunabilir.

Sonuç olarak İnternet'e bağlı iseniz dokümanlarınıza, resimlerinize, görüntülerinize, ses dosyalarınıza başkaları ulaşabilir. Yani, Çin devleti bildiğiniz gibi Microsoft işletim sistemi kullanmıyor çünkü Microsoft işletim sistemi olduğu zaman bu bilgisayarın ya da bu bilgisayarın ne yaptığını bilmemiz mümkün değil. Arada birtakım güvenlik duvarları falan koyabilirsiniz ama yani esas ruhu Microsoft'tan gelince yani ruh gibi oluyor, ruh Microsoft'tan gelince bilemeyiz.

Telefon şebekeleri daha güvenilirdir çünkü devletler güvenliğimizi sağlamaya çalışırlar. Ancak bunlarda da mesela Amerika'da Huawei şirketinden -Çin şirketi bu- kritik yerlere donanım alınmıyor, bu yazılmamış bir kuraldır. Çünkü bir kere donanım olunca donanımın da ruhu var yani işletim sistemi var, uzaktan girilebilir, ulaşılabilir. Bizim şeyimiz böyle.

İnternet arama motorları da hareketlerimizi izleyebilir, her girdiğiniz şeyi takip edebilirler ve olabilir. Ülkemizde de aslında bir anti-virüs yazılımı yok kendimizin. Böyle bir yazılımımız olsa iyi olur esas itibarıyla. Yani, bu şeylerde tamamen güvenli olabilmek ancak İnternet kablonuzu söktüğünüz zaman mümkün olabilir.

BAŞKAN - Çok teşekkür ediyoruz.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Ben teşekkür ederim.

BAŞKAN - Teknolojinin "faydalarını" kısa ve net olarak bize anlattınız. Bir de bunun içine kötü niyet eklenirse… Bizim jenerasyonda -yarım asrı deviren birisiyim- sosyal olaylarda "İki kere iki dört etmez." denirdi hep ama siz bu sunumunuzda mesela "Kes-yapıştırı hem seste hem görüntüde tespit edemeyebiliriz." diyorsunuz. Onu ben anlamakta biraz zorluk çekiyorum. Yani, bu teknik bir konu değil midir nasıl tespit edilemez? Seste veya görüntüde kes-yapıştırı "Bir bilirkişi öyle der veya bir teknik insan öyle der, öteki böyle der." diyorsunuz. Bu…

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Şimdi mesela şu grafiğe dönersek burada mesela "fa" var üst tarafta, "fa" denmiş. Aynı kişiye "fa" dedirtirseniz aynısı olmuyor, rakamlar değişebiliyor. Yani, biz bir kere "fa" derken bu gırtlak yapımızı, kaslarımızı kullanarak gırtlağımızı ve burnumuzu bir şekillendiriyoruz farkında olmadan ve aşağıdan hava basıyoruz. Bu havayı basarken kiminde belki daha çok hava basıyoruz, kimisinde daha az basıyoruz. Onun için, hep bu "fa"lar farklı olabiliyor. O yüzden de rakam dizileri hep aynı olmuyor, aynı olmayınca da kes-yapıştırla yapılmışla orijinal olanı ayırmamız çok zor.

BAŞKAN - Teknik olarak mümkün değil diyorsunuz.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Yani, bunlar yine mümkün, bir uzman alıp baştan sona uğraşabilir. İşte, diyebilir ki yüzde 90 ihtimalle ya da büyük olasılıkla kes-yapıştırdır, değildir.

HAMZA DAĞ (İzmir) – Yani, bilgisayar üzerinde yapılmıyor mu yine?

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Tabii bilgisayar üzerinde yapılıyor.

HAMZA DAĞ (İzmir) – Yani, bilgisayar üzerinden İnternet kullanılarak yapılıyor.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Tabii, tabii.

HAMZA DAĞ (İzmir) – Şimdi, bilgisayar üzerinden onun yapıldığına dair bunun İnternet'te yapıldığı biliniyor. Yani, şimdi İnternet'teki her şey, mesela Google "Bir kelimeyi bile boşa harcamayız." diyor.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – İnternet'e bağlamadan da yapabilir şeyini.

HAMZA DAĞ (İzmir) – Yani, indirmesi lazım bilgisayarına.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Hayır, yazılım kendisi geliştirmiş olabilir o kes-yapıştır yapanı.

HAMZA DAĞ (İzmir) – İşte, her şey için yazılım hazırlıyorsak bunun karşı noktası, bunun tespiti için bir yazılım bulamıyor muyuz?

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Yok bulunmaz. Siz kendiniz oluşturabilirsiniz. Hazır böyle, mesela MATLAB diye bizim kullandığımız bir şey var, matematik "library"in herhâlde kısaltılmışı. Onu satın alırsınız, o genel bir program, ondan sonra onun üzerinde siz kes-yapıştır yapabilirsiniz...

HAMZA DAĞ (İzmir) – Ya, şimdi anlamadığım şu...

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – ...ve bilgisayarı da sökersiniz İnternet'ten, olur size ses dosyası. Sonra kaydedersiniz, bu şunu söyledi dersiniz, olur.

BAŞKAN – Bitti.

HAMZA DAĞ (İzmir) – Yani, İnternet'teki her şey girdiğimizde, bir şey yaptığımızda güven noktasında sıkıntı yaşayabiliyoruz ama bu güveni ortadan kaldıracak -kripto falan bu tarzda şeyler var ama- bu güveni sağlayacak bir sistemi ise ortaya koyamıyoruz. Öyle mi yani? Teknolojik olarak her şey yapılabiliyor, güven noktasında sıkıntı yaşayabiliyoruz ama bu güvenle alakalı tesis edilecek bir sistemi koyamıyoruz? Şöyle söyleyeyim yani daha açık bir şekilde: Yani, eve giren bir hırsız...

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Evet, Türkiye'de koyamayız.

HAMZA DAĞ (İzmir) – ... eve girebiliyor ama eve girmeyi engelleyecek bir sistemi veyahut da eve girdikten sonra nasıl girdiğini anlayabilecek sistemi ortaya koyamıyoruz, çok açık bir şey yani.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Çok özel durumlar için yapabilirsiniz ama tüm kullanıcılar için yapmıyoruz.

HAMZA DAĞ (İzmir) – Hayır, hayır şimdi özel şeylerde zaten... Mesela, elimize bir dosya geldi. Bu dosyada iddia var, diyorlar ki: "Benim normalde böyle bir konuşmam yok, benim böyle bir söylediğim söz yok, benim böyle bir ifadem yok. Burada birbiriyle karışmış ifadeler var." ve bunu siz inceliyorsunuz bir öğretim üyesi olarak veyahut da başka bir kurumumuz inceliyor. Yani, burada hecelerin bir araya getirildiği, rakamların bir araya getirildiğini anlayamayacak mıyız?

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Yüzde yüz anlayamayız, bu DNA şeyi gibi değil. Diyebiliriz ki büyük ihtimalle kes-yapıştır yapılmış ama büyük ihtimalle denilebilir.

BAŞKAN – Peki, Türkiye'yle dünya arasındaki fark nedir? "Türkiye'de yapamayız." dediniz, dünyada yapılabiliyor mu bu?

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Şimdi, -mesela şu şeye gelirsek- telefon şebekelerimiz daha güvenilirdir, devlet güvenliğimizi sağlamaya çalışır. Amerikan telefon şebekeleri bizden daha güvenlidir.

BAŞKAN - O anlamda söylüyorsunuz.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Ya da Çin telefon şebekeleri bizden daha güvenlidir. Yani, onlar çünkü hem donanımı üretiyorlar hem yazılımı kendi yazılımları. Biz şu anda donanımı da dışarıdan alıyoruz, yazılımı da dışarıdan alıyoruz, virüs programını da dışarıdan alıyoruz, işletim sistemini de dışarıdan alıyoruz, bilgisayarı da dışarıdan alıyoruz. Bilgisayar devresinin içine de şey konulabilir…

BAŞKAN - Zaafın oradan olduğunu söylüyorsunuz.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Yani, bilgisayarda bu devrelerin içine de virüsler konulabilir. Sadece virüsler "soft" ya da yumuşak değil, "hard" olarak da var. Yani, devrenin içinde gömülü olarak duruyor, vakti geldiğinde aktive edilebilir, sizin şeyiniz yanabilir ya da ne bileyim, uçaksavarınız başka tarafa doğru dönüp atış yapabilir ya da işte, yap dersiniz yapmaz. Normalde yap dediğinizi yapmayabilir. Yani, "hard" olarak, donanım olarak da…

ERDAL AKSÜNGER (İzmir) - İşletim sistemi koymadan da onu zaten içerisinde gelen herhangi bir epromun üzerine de koyabilir yani.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Evet, sadece eprom üzerinde değil, yani devre…

ERDAL AKSÜNGER (İzmir) - Devrenin üzerinde…

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Devrede yani kartın üzerinde şey olabilir.

BAŞKAN – Sorulara geçmeden önce Ayhan Hocam, siz İSYAM'la ilgili bilgi verebilirseniz kısa bir şey.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Ben İSYAM hakkında kısa bir bilgi vereyim.

BAŞKAN - Buyurun.

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – İSYAM, uzun adı İletişim ve Spektrum Yönetimi Araştırma Merkezi. Bu Bilkent Üniversitesinin bir birimi, kuruluşu 1994 yılında. Kuruluşu aslında Radyo Televizyon Üst Kurulunun kurulmasıyla ilişkili çünkü Radyo Televizyon Üst Kurulu 1994 yılında kurulunca yasaya göre frekans planlaması yaptırması gerekiyordu. O görevi de Bilkent

Üniversitesine verdi ve biz ilk frekans planını 1994 yılında yapmaya başladık, 1995 yılında da RTÜK'e teslim ettik. O plan bir türlü uygulanamadı, gerekçeleri teknik değil, başka nedenlerle uygulanamadı.

İLHAN CİHANER (Denizli) - Hangi gerekçelerle?

BİLKENT ÜNİVERSİTESİ ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – İdari nedenlerle. İki kere ihaleye çıkıldı, ikisinde de iptal edildi. Birisinde Danıştay durdurdu, birisinde Başbakanlıktan yazı geldi, durduruldu. Hatta RTÜK Başkanı Orhan Oğuz istifa etti, RTÜK üyeliğinden de istifa etti bu olay üzerine filan yani geçmişte bu oldu tabii ama…

Daha sonra biz 1998-2002 yıllarında ASELSAN'la ortak olarak Millî Monitör Sistemi kurduk. Millî Monitör Sistemi şu: Türkiye'de havadan yapılan yayınların izlenmesi, monitör edilmesi amacını taşıyor. Bunun için işte Ankara'da bir merkez var, değişik bölgelerde Diyarbakır, Trabzon, Mersin, İstanbul, İzmir gibi merkezlerde de bölgeler var. O bölgelerde cihazlar kuruldu, bu cihazlar yayınları tespit ediyor fakat yayın içeriğiyle ilgili değil bunlar. Yayının varlığı, yokluğu veya yayının lisans aldığı teknik parametrelere uygun yapılıp yapılmadığıyla ilgili. Örneğin. bir radyo yayıncısı bir yayın yapıyor, lisans aldıysa eğer yayın yapıyor ama mesela yayınında belirtilen gücün çok üstünde bir yayın yapıyor, bunu tespit etmek amaçlı. Veyahut yayının olmaması gereken yerde bir yayın varsa bu da izinsiz bir yayın anlamına geliyor, bunu tespit etmek amaçlı içeriğiyle ilgili değil, sadece Millî Monitör Sistemi'nin amacı bu tür şeyleri izlemek. Bu, şu anda BTK'nın elinde bu sistem, Bilgi Teknolojileri ve İleşitim Kurumu. O zaman, ilk ihaleye çıkıldığında Telsiz İşleri Genel Müdürlüğüydü, daha sonra Telekomünikasyon Kurumu oldu, daha sonra BTK oldu, şu anda öyle. Onun dışında, Enis Bey'le beraber ASELSAN'a yaptığımız bir işte ses kodlayıcı modeli var, INBE, telsiz sistemleri için. Yine - geçenlerde yeni bitirdik- Radyo Televizyon Üst Kuruluna sayısal televizyon planı, ulusal planı ortaya çıktı. 16 Nisanda da bildiğim kadarıyla RTÜK ihaleye çıkıyor, sayısal yayıncılık için ihale başlayacak, 16 Nisan günü ihale olacak. Dolayısıyla, biz kamu kurumlarıyla bu tür konularda çalışıyoruz.

Esas çalışma alanımız frekans planlaması. Frekans planlaması derken bu aslında vericilerin birbirlerini çok kötü etkilemeden, uyum içerisinde değişik vericilerden, değişik yayınların ülke kaynaklarını da maksimize edecek şekilde yapılmasını sağlamak. Çünkü frekans aslında bir kaynak ülke için. Kullanmazsanız tabii o kaynağı kullanmamış oluyorsunuz, kullanırsanız ve doğru kullanırsanız da tabii maksimum faydayı sağlamış oluyorsunuz. Örneğin, Ankara'da bir televizyon yayını yapacaksınız, 3-4 yerden aydınlatabilirsiniz Ankara'yı veya 15 yerden aydınlatabilirsiniz, her tarafı kirletirsiniz. Dolayısıyla, bunun bir bedeli olması lazım, bu kirletmeyi önlemek lazım, devletin bunu düzenlemesi lazım. Bu işi de işte, Radyo Televizyon Üst Kurulu yapıyor şu anda. Yani, elektromanyetik açıdan bakarsak -bir de şey eklemek istiyorum Enis Bey'in söylediğine- tabii her şeyi telli yaparsanız yine tellerden de havaya yayın çıkabilir veya birileri o tellerin etrafından o yayını alma imkânına sahip olabilir, öyle cihazlar da var.

BAŞKAN - Teşekkür ederiz, sağ olun.

Sorularımız var herhâlde.

Ali Bey, buyurun.

ALİ ERCOŞKUN (Bolu) – Hocam teşekkür ederiz.

Hangi frekans aralıklarında ortamda verici olabilir? Yani, böcek denilen vericiler hangi frekansları kullanabilir? Bu böcek tabir ettiğimiz alıcıların veya vericilerin tespitine yönelik frekans planlaması açısından ne gibi tedbirler alınabilir? GSM, wifi, bluetooth gibi standart frekans ve protokolleri kullanan bir böceğin salt, sadece frekans spektrumuna bakılarak tespiti mümkün olabilir mi? Uydudan yapılan GSM haberleşmesinin dinlenmesinin mümkün olduğunu düşünüyor musunuz? Frekans tahsislerine yardımcı girişim analizlerinde hangi anten parametlerini kullanabiliyoruz? Yani, buradan şunu anlamak istiyorum: Bu gibi analizlerin yardımıyla olmaması gereken bir verici -çünkü daha önceki oturumlarımıza da konu olan bir yalancı baz istasyonu yani baz istasyonlarının yalancıları olabilir gibi şeyler geçmişti- bunların tespiti mümkün mü, pratikte böyle bir tespit yapabilme şansımız var mı? Bu böceklerin, böcek tabir ettiğimiz alıcı vericilerin frekanslar arasında gizlendikleriyle alakalı gene teknik sunumlarda bazı şeylerden bahsedildi. Bunların spektrum içinde saklanma imkânı var mı? Dolayısıyla, kendini saklamayı becerebilecek bu tür alıcı vericilerin, böceklerin yakalanma imkânı var mı? Bir de gene -aslında genel olarak bir soruda da geçti ama- sizce GSM gibi bir kablosuz haberleşme sistemlerinin TİB veya operatörler dışında başka herhangi bir yapı tarafından tespit edilmesi, dolayısıyla havada bunun yakalanması ve çözülmesi mümkün mü, bilginiz dâhilinde böyle bir sistem var mı?

BAŞKAN - Diğer soruları da alalım.

İlhan Bey, buyurun.

İLHAN CİHANER (Denizli) – Evet, teşekkür ediyorum sunum için.

Şimdi, bizde, bizim sistemimizde yasal olarak dinleme yapabilen üç kurum var: Emniyet var, MİT var, Jandarma var ve bunların hepsi de TİB üzerinden yapıyorlar bu dinlemeyi. TİB kendi yaptığı ses kayıtlarında bu ses kaydına ilişkin bir dijital veri olduğunu, onda hem zaman hem de sese dair bir veri -sizin dediğiniz gibi belki filigran olarak adlandırabileceğimiz- gömülü olduğunu, onun üzerinden bir şeyler yapılabileceğini yani kendilerine ait olup olmadığının tespitini yapılabileceğini söyledi. Tabii, bir de ortam dinlemesi işte, teknik araçlarla takip yöntemiyle yapılıyor. İşte, hassas mikrofonlarla veya ortama birtakım cihazlar yerleştirecekken TİB üzerinden yapılmayan ses ve görüntü kayıtları da var. Bunların güvenliğini sağlamak için şüpheye yer bırakmayacak şekilde o kayıtların kim tarafından, hangi tarihte yapıldığı, bütünlüğünün bozulup bozulmadığını sağlayacak bir yazılım, bir damga geliştirilebilir mi? Birinci sorum bu.

Bu şeylerde, mesela renkli fotokopi makinelerinde ya da dijital fotoğraflarda falan var bu. İşte, oraya sıradan kullanıcının göremeyeceği birtakım bilgiler yerleştirilebiliyor. Bu tarz bir yazılım

aracılığıyla veya kim tarafından kaydedilmiş, bütünlüğü bozulmuş mu gibi bilgilere yani güvenliğini artırabilir miyiz? Bir bunu sormak istiyorum.

Bir de bu Millî Monitör Sistemi'nin -gerçi biraz benzer bir soru geldi ama- hassasiyeti nedir yani ne kadar hassas yayınları ayırt edebiliyor? Bu, şunun için önemli: Dinlediğimiz görevlilerden birisi, uzmanlardan birisi bir baz istasyonunun herhangi bir yerde kurulmasının kendilerine ihbar gelmedikten sonra, kendilerine bildirilmedikten sonra işte, başka kurumlar tarafından fark edilemeyeceğini söylediler. Oysa orada oldukça güçlü bir elektromanyetik yayılım var. Bu Millî Monitör Sistemi'nin hassasiyeti nedir? Mesela bu tarz bir baz istasyonunu ayırt edebilir mi?

BAŞKAN - Evet, Hamza Bey, buyurun.

HAMZA DAĞ (İzmir) – Teşekkür ediyorum ben de sunum için.

Şimdi, Ayhan Bey ve Enis Bey diye ayırmıştık ama ben hepsini birden sorayım, artık aranızda ona göre tayin edersiniz.

Sizce GSM baz istasyonlarına veya telefon santrallerine operatör şirketinin haberi olmaksızın dışarıdan müdahale mümkün müdür? Bu tür altyapıların Alcatel, Sıemens, Huawei, Erıcsson gibi şirketlerden temin edildiği bilinmektedir. Bu şirketlerin yerli üretimleri var mıdır? Bu şirketlerin kendi mal imal ettikleri bu santrallere sızmaları imkânsız mıdır? Çeşitli istihbarat servislerinin kolaylık sağlamaları imkânı sizce var mıdır? Bu türden sistemlerin millî olarak üretilmesi konusunda çalışmalar bilginiz dâhilinde mevcut mudur? Bu konuda atılması gereken adımlar sizce nelerdir? Ekonomi sistemi hakkında görüşleriniz nelerdir? Sizce teknik imkânlar ne ölçüde olabilir? Tüm dünyanın dinlenebilmesi mümkün müdür?

BTK'nın görevini hakkıyla yapabildiğini düşünüyor musunuz? Bu konudaki eksikleri nelerdir? GSM'in dinlenmemesi için GSM kripto algoritmalarının dışında alınan ekstra tedbirler de mevcut mudur? Türkiye'de tüm illerde spektrum takibi yapılabiliyor mu? Bir telefon şirketinin bütün telefon görüşmelerinin kayıtlarını tutabilmesi teknik olarak mümkün müdür? Bir saatlik bir telefon görüşmesi bilgisayarda ne kadar yer kaplar? Yüz tanımanın geldiği son nokta nedir? İstihbarat örgütlerinin bu teknolojilere ilgisi ne ölçüdedir? Berrak bir ses iletimi için saniyede ne kadar örnekleme yapmak yeterlidir? Küçük ve ucuz bir böcek bu konuda yeterli olur mu? Aynı şekilde, görüntü ve ses aktarımı birlikte düşünüldüğünde minimum ne kadar veri aktarımı yeterli olur? Ses ve kelimeye odaklı bir dinleme cihazı geliştirilmesi sizce mümkün müdür? Mesela, ortamda yalnızca belli bir kişi konuştuğunda veya belli kelimeler geçtiğinde aktivite olan böcekler mevcut mudur?

Şimdi, biraz önceki şeyi belki tam kayda girmedi tekrar daha açık bir şekilde sormak istiyorum: Biraz önce bize gösterdiğiniz ses kaydının yazılımla, rakamlarla yapıldığının tespiti mümkün değil midir, yani -bahsettiğim husus- başka bir yazılımla hecelerin bir araya getirildiğinin tespiti mümkün değil midir?

Biraz önce yine söylediğiniz bilgilerden yola çıkarak yazılım ve donanımın ve bütün teçhizatın yurt dışından alındığını söylediniz. Bu konuda, yeni yazılım ve donanım üretme konusunda akademik birikimimiz mevcut mudur?

Teşekkürler.

BAŞKAN – Buyurun.

ŞUAY ALPAY (Elâzığ) – Teşekkür ederim Sayın Başkanım.

Ben de değerli sunumlarınız için teşekkür ediyorum değerli hocalarım.

Şimdi, biz, tabii, özel hayatın gizliliği ve haberleşme hürriyetine yapılan ihlallerin tespiti amacıyla kurulmuş bir Komisyonuz ve şu ana kadar, tabii, çeşitli kurumlar dinlendi, şahsi olarak benim öğrendiğim kadarıyla da zaten bu ihlallerin, özellikle haberleşme hürriyetine yönelik ihlallerin bu frekans tahsisi ve kontrolüyle ilgili birimler aracılığıyla yapılması gerektiği hususunda bir değerlendirme. Bunu defaaten de gündeme getirdim ben Komisyonda. Yani, özellikle BTK'nın bu frekans tahsis eden biriminin 27 civarında seyyar araç, 8-9 sabit merkezle bunu yapması gerektiği ve yasal görevin de bunlarda olduğunu duymuştuk. Bu, görevin ne kadar yapılıp yapılmadığıyla alakalı.

Yine bununla ilgili, sizin "millî monitör sistemi" dediğiniz sistemin aslında bu mu olduğu, yoksa bunun dışında bir sistem mi olduğu; bu sistemin şu anda ne kadar çalışıp çalışmadığı? Yani, frekanslar nihayetinde devletin yetkili bir kurumu tarafından tahsis edildiğine göre, bu frekanslara yapılacak yasa dışı müdahaleler ve nihayetinde, haberleşmenin birtakım frekanslar üzerinden yapılacağı da düşünüldüğünde, bunların tespit edilip edilemeyeceğini, geçmişte yapılmış olan bu özel hayatın gizliliği veya haberleşme hürriyetine yönelik bu ihlallerin de yine bu millî monitör sistemi tarafından tespit edilmiş olup olmadığını ben öğrenmek istiyorum.

Teşekkür ediyorum.

BAŞKAN – Buyurun.

ŞİRİN ÜNAL (İstanbul) – Çetin Hocam, verdiğiniz bilgiler için teşekkür ediyorum. Müsaade ederseniz size beş sorum var.

Görüntü sistemleri hakkında özellikle de ülkemizin seviyesi konusunda bizi biraz aydınlatabilir misiniz? Sizce, MOBESE'ler, mahremiyet odaklı teknolojiler ve uygulamalar nasıl oluyor? Masum insanları bertaraf ederek sadece şüpheli olan ve mahkeme kararıyla aranan yüzler aranabilir mi?

İkinci sorum: MOBESE kayıtları sizce nasıl saklanmalıdır, hangi süreyle saklanmalıdır, veri büyüklükleri ne kadardır; sistemin arka tarafında çalışan herhangi biri bu kayıtlara ulaşabilir mi, ne tür kripto altyapısı kullanılmaktadır?

Üçüncü sorum: MOBESE kayıtları hangi durumlarda silinmelidir? Örneğin, MOBESE'nin çektiği ortamda bir emniyet veya jandarmayı ilgilendiren olay olmadıysa hemen silinmeli mi?

Dördüncü sorum: Görüntüyle ilgili yasal bir boşluk olduğunu düşünüyor musunuz? Sizce mevcut sistemler kişisel mahremiyet ve güvenlik için yeterli mi?

Beşinci sorum: Siz tam yetkili olsanız Sayın Hocam, bu yasa dışı dinlemeyi nasıl ortadan kaldırırsınız?

Altıntaş Hocam, size de çok teşekkür ediyoruz.

Tabii, verdiğiniz bilgiler bizi azıcık da ürküttü. Ben 1988 yılından 2010 yılına, emekli olana kadar F-16 uçaklarında uçtum. F-16 uçaklarının radarı yazılımla çalışıyor biliyorsunuz, havadan havaya attığımız füzeler yazılımla çalışıyor, havadan yere attığımız bombaları yazılım sistemleriyle, atış... Onların hepsi yazılımla ilgili. Motorunu üç-dört tane bilgisayar kontrol altında bulunduruyor, uçuş kumandalarını dört değişik çeşit bilgisayar kontrol altında... Eğer hakikaten bunların içerisine bir şey konulabiliyorsa ciddi sıkıntımız var demektir. Ülke olarak, tabii, yazılım konusunu stratejik bir ihtiyaç olarak değerlendiriyorum ben emekli bir asker olarak.

Birinci sorum: Sizce, Türkiye'deki spektrum denetleme ve ihlalleri tespit altyapısı yeterli midir?

İkinci sorum: İzinsiz yayın yapan bir vericinin kapsama alanı en az kadar olursa tespiti mümkün olur?

Üçüncü sorum: Yetkisiz bir kullanıcı spektrum takibi veya kaydı yapabilir mi, bu yasal mıdır? Bu konuda herhangi bir yasal eksiklik olduğunu düşünüyor musunuz?

Dördüncü sorum: Uydulardan karasal spektrumun tespiti sizce mümkün müdür? Mümkün olduğunu düşünüyorsanız bunun bölgesel olarak yapılması mümkün müdür?

Beşinci sorum: Tahsisli bantlar, mesela GSM içerisindeki frekans kullanımı da düzenleniyor olsa onlara tahsis edilen banttaki planlamayı kendileri mi yapıyorlar?

Altıncı sorum: "Jammer" kullanılarak her türlü böceği saf dışı etmek mümkün müdür?

Yedinci sorum bir önceki soruyla, bölümle aynı şekilde: Yasa dışı dinleme ve izlemeleri siz tam yetkili olsanız ortadan kaldırabilir misiniz, nasıl kaldırabilirsiniz Hocam?

BAŞKAN – Buyurun efendim.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – İsterseniz, ilk sorular frekansla ilgiliydi, onlara ben kısaca cevap vermeye çalışayım. Şimdi, "Böcekler hangi frekansta veya bunlar frekanslar arasına saklanabilir mi?" diye bir sorumuz vardı. Tabii, böcek aktif veya pasif olabilir. Eğer pasifse her frekansta olabilir yani onu "her frekansı dinleyebilir" anlamında söylüyorum. Yalnız, aktifse o zaman bir yayın yapıyor demektir. Bu sefer, çoğu zaman bu tür cihazlar "halka açık frekanslar" dediğimiz frekanslarda çalışıyorlar. Bunlar genellikle ASM bandında veya GSM bandında filan gibi bantlar da olabilirler. Çok geniş bantla da çalışanlar olabilir. Dolayısıyla, frekanslar arasında saklanma da söz konusu olabilir. Yani, öyle bir spektrum dediğimiz bir iletişim sistemi var. Burada siz gücünüzü çok

geniş bir frekansa yayıp gürültü seviyesine indiriyorsunuz, dolayısıyla karşı taraf sizin konuşmanızı anlamakta güçlük çekiyor. Askerî sistemlerin çoğu böyledir yani spektrum kullanıyorlar.

Şimdi, yalancı baz istasyonu tespiti aslında şöyle: Telekomünikasyon Kurumu baz istasyonlarının yerlerini kendisi tespit etmiyor, bunu operatörlere bırakıyor, operatörler yapıyor o işi; operatörler kendileri tespit edebilirler, bence edebilirler, yalancı baz istasyonunu kolaylıkla bulabilirler. Bu benim görüşüm. Çünkü onların zaten bir baz istasyonunun da merkezle konuşması lazım. Dolayısıyla, baz istasyonunun kendisini başka bir baz istasyonu olarak tanımlaması lazım. Yazılımlarla onlar tespit edebilirler. Havadan yayınlarla bunu tespit etmek zor çünkü baz istasyonu da yayın yapacak, gerçeği de, sahtesi de. Dolayısıyla, o havadan yayına bakarak baz istasyonunun sahte olup olmadığını tespit etmek oldukça zor. Dolayısıyla da o açıdan yakalanma ihtimali yok. Fakat GSM operatörleri bunu yazılımla, kendi sistemlerinin işletimleriyle tespit edebilirler.

Yayının, tabii, TİB'in -siz sormuştunuz galiba- kendilerine ait olup olmadığını, bu izlemenin kendilerine ait olup olmadığını, otantik olup olmadığını tespit etmek mümkün mü? Enis Bey daha iyi cevap verir. Herhâlde mümkün demin bahsettiği yöntemlerle, yani filigram konabilir veyahut ona benzer birtakım "authentication" şeyler konabilir.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Onu başa koyuyorlar, yani her konuşmanın başına konuluyor, bütünlük şeyi yok. Bütünleme şeyi de var ama o her şebekeye, bunu bütün şebekeye yaymak, herkese yaymak mümkün değil, yani büyük masraf gerektirir. Herkes için böyle her metnin içine tamamen filigram gömmek falan, bu bayağı zor.

İLHAN CİHANER (Denizli) – Yok, benimki daha çok MİT'in ve Jandarmanın yaptığı dinlemelerle ilgili.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – O normal telefon şebekesinde de var başına şey konuluyor ama sadece başına konuluyor.

İLHAN CİHANER (Denizli) – TİB'inki de öyle mi, bilginiz var mı?

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Hepsi öyledir yani.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – "GSM baz istasyonu operatörlerine müdahale var mı? Cihaz veren şirketler bir şekilde müdahale edebiliyorlar mı? Millî üretim olmadığı için hepsini dışarıdan alıyoruz." diye bir soru vardı. Tabii, onu çok bilemiyorum çünkü GSM şirketlerinin nasıl çalıştığını tam bilmiyorum. Onlar tabii ki cihazları satın alıyorlar. Millî üretim, bildiğim kadarıyla, pek yok şu ana kadar, hepsi dışarıdan geliyor. Dolayısıyla, BTK açısından da GSM operatörlerine karışmıyor. Frekans planlamalarını da kendileri yapıyorlar, baz istasyonlarının yerlerini kendileri tespit

ediyorlar, sadece bunu BTK'ya bildiriyorlar. Fakat, Türkiye'de, biliyorsunuz, binlerce, on binlerce baz istasyonu var, bunların iyi bir veri tabanı da yok BTK'nın içindeki veri tabanında. Tabii, birtakım kapatılmış baz istasyonları olabiliyor, yeri değiştirilmiş baz istasyonu olabiliyor. Bunları sürekli güncel tutmak bütün operatörler için çok kolay bir işlem değil. Hepsinin yerlerini çok iyi bilemiyor olabiliyorsunuz.

Bu Echelon sistemini sordunuz galiba. O sistem, Amerikalıların kurduğu bir sistem bildiğim kadarıyla. Tüm dünyadaki şeyleri dinliyor, özellikle İnternet haberleşmesini. Bildiğim kadarıyla, anahtar kelime "keyword" bazında dinliyor. Sizin yazdığınız e-mail mesajında geçen kelimelerin içinden hassas kelimeleri buluyor, tespit ediyor, eğer onlar varsa bu sefer onları izliyor, yani sistem öyle çalışıyor. Türkiye'ye en yakın Kıbrıs'ta var galiba, Güney Kıbrıs'ta, Echelon sistemi.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Konuşma içinde de yine bu tür anahtar kelimeler geçtiği zaman şey yapıyor.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Avustralya'da, Amerika'da, dünyada…

ENVER ERDEM (Elâzığ) – Bütün uydulardaki konuşmaların tamamını bu yöntemle…

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Sadece uydu olması şart değil, yerdekiler de var.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Yerdekiler de var. Bütün sistemi, İnternet trafiğini izliyorlar diye biliyorum.

HAMZA DAĞ (İzmir) – "İnternet" diyorsunuz ama, ortam değil.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – İnternet ve… İnternetlerin bazıları uyduya da çıktığı için uydu şeyleri de var. İnternet, ortam değil.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Şimdi, zaten, Amerika'da telefon şebekeleri de yavaş yavaş ortadan kalkıyor, her şey İnternet yapısına dönüyor.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Millî monitör sisteminin amacı, tabii, bu tür şeyleri takip etmek değil, yani yayın, izinsiz dinlemeler filan gibi şeyler amaçlı değil. Millî monitör sistemi, aslında BTK'nın görevi olan ülkedeki frekansların verimli kullanımını sağlamak. Tabii, BTK'nın görevini yasa da tespit ediyordur. Ben BTK görevlisi değilim, onlar adına konuşamam tabii ama onlar kendi görevleri açısından bakıyorlar buna. Onların içinde böyle yayın içeriği tespiti konusu

yoktu, en azından biz proje yaparken. Dolayısıyla onu bilemeyeceğim yani. Böyle bir amacı yok yani millî monitör sistemi projesinin.

ENVER ERDEM (Elâzığ) – Denetim, kontrol görevi yok, sadece verimli kullanımıyla alakalı.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Şöyle: Onların üç kontrolü var:

Bir: İzinsiz yayın ve yayıncıların tespiti,

İkincisi: Yayınların teknik parametrelerine uygun yapılıp yapılmadığı,

Üçüncü görevleri de: Spektrum doluluğu.

Yani, belli bölgelerde spektrum ne kadar kullanılıyor, ne kadar kargaşa var? Tabii, bunların amacı şu: Başka bir frekans talebi olduğu zaman kendilerine gelen, o talebe ne tür cevap verecekleri. Fakat, BTK, bildiğimiz kadarıyla, bizim yazılımlarımızı kullanıyor, bizim yazılımlarımız da "spektrum mühendisliği yazılımları" dediğimiz yazılımlar. Onları on yıldır da çok yenilemediler, yani o bakımdan belki yenilemeye ihtiyaçları olabilir. Yaklaşık on yıldır, on-on bir yıldır yazılımlarını yenilememiş durumdalar.

BAŞKAN – Yazılı da cevap verebilirsiniz Hocam sonra.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Evet, aşağı yukarı benim... BTK açısından çok fazla bir şey söyleyemeyeceğim.

ENVER ERDEM (Elâzığ) – Cevap vermeyebilirsiniz yani.

BAŞKAN – Hocam gayet güzel cevap veriyor.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Türkiye'nin her tarafında ne kadar verimli kullanılıyor? Tabii, onu ben bilemeyeceğim, BTK'nın kendi işleyişiyle ilgili bir konu. Biz onlara yazılımları verdik, eğitimleri yaptık, proje tamamlanmış durumda. Ondan sonra, tabii, on yıl geçti, şu anki durumu çok bilmiyorum.

BAŞKAN – Enis Hocam, buyurun.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Ben şu ses tanımayla ilgili, hani "Kesyapıştır yapılmış mı?" konusunda bir örnek vermek istiyorum da analog, analoji yaparak. El yazısı tanımayla eş değer durumda. "El yazısı benimdi." diyebilir, "Benim değildi." diyebilir, öyle bir şeyi var. Görüntülerde de kesyapıştır, el yazısı tanıma gibi, yani DNA şeyi gibi değil. Şurada ortam dinleme konusunda bir soru vardı, tam şeyi hatırlayamıyorum ama. Mesela, biz konuşunca ses dalgaları gidiyor, pencereye çarpıyor, pencere titremeye başlıyor. Karşıda da birisi varsa ve o da pencereye bir lazer tutmuş olabilir, ondan sonra o lazerdeki oynamalarla bizim konuşmamız orantılı oluyor, oradan konuşmayı çıkarıyor. O

zaman, işte, pencereyi kapatmanız, perdeyi çekmeniz lazım. Askerî şeydeki gibi "measure" var, "counter measure" var. Bu işin sonu yok; siz daha iyi bilirsiniz, bu işin sonu yok maalesef.

"Görüntü sistemleri hakkında biraz bilgilendirme, ülke olarak hangi seviyedeyiz?" Ülkemizde de yine bu MOBESE sistemleri üretilmiyor, yani biz aslında teknolojik olarak geri bir memleketiz açıkçası.

BAŞKAN – ARGE yatırımlarını desteklemediğimiz için zamanında…

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – O açıdan, durum böyle maalesef. Yani biz Çin'in ve Amerika'nın çok gerisindeyiz ya da Japonya'nın ya da işte, ciddi bir Avrupa devletinin.

"Örneğin, sizce, MOBESE'ler mahremiyet odaklı teknolojiler ve uygulamalar kullanabilir mi?" Evet, kullanıyorlar. Avrupa Birliğinin çeşitli standartları var. Mesela, bir yere kamera koyarsanız, karşıda da bir ev varsa o evi bloke etmek zorundasınız. Bu tür şeyler biliyorum ama hukuki şeylerini tam bilmiyorum.

"Masum insanları bertaraf ederek sadece şüpheli olan ve mahkeme kararıyla aranan yüzler aranabilir mi?" Bu çok zor çünkü bu yüz tanımada büyük bir başarı sağlanamadı. Amerikalılar bunu herkes uçağa binerken falan yapmaya çalıştılar fakat başarılı olamadı. Mesela, yüzde 98 falan oranla tanıma yapılıyor ama 100 kişide 2 kişi hata yapsanız, uçakta da 300 kişi olsa hemen hemen neredeyse her uçağı durdurmak zorunda kalacaksınız ve o yüzden mümkün değil.

"MOBESE kayıtları sizce nasıl saklanmalıdır?" Bunu bilemiyorum, hukuki bir şey yani.

"Hangi süreyle saklanmalıdır?" O da yine değişiyor.

"Veri büyüklükleri ne kadardır?" Şöyle diyebiliriz: Sekiz kanallı bir videoyu sıradan bir bilgisayarda birkaç hafta saklayabilirsiniz.

"Sistemin arka tarafında çalışan herhangi biri bu kayıtlara ulaşabilir mi?" Evet, ulaşabilir.

"Ne tür kripto altyapısı kullanılmaktadır?" O da yine MOBESE üreticisinin kullandığı kripto şeyi oluyor. Onu da bilemeyiz. Hangisini kullanıyorsa. Bazıları hiç kullanmıyor, bazıları da güvenli olanları kullanıyor.

"MOBESE kayıtları hangi durumda silinmelidir?" O da hukuki bir şey, ben cevaplayamam.

"Örneğin, MOBESE'nin çektiği ortamda emniyeti veya jandarmayı ilgilendiren bir olay olmadıysa hemen silinmeli mi?" Zaten üstte yazıyorlar, orada bir süre var, süre geçince üzerine yazarak devam ediyor. Bu süreyi baştan siz belirliyorsunuz çoğunda. Bu emniyet veya jandarma o şeyi aldıktan ve bunu bir şekilde otantike ettikten sonra silinebilir. Yani, herhâlde, avukatın da onayını almak lazım, emniyet ve jandarmanın bunu şeyden silmesi için şüphelinin avukatının da onayını alması lazım diye düşünüyorum.

"Görüntüyle ilgili yasal bir boşluk olduğunu düşünüyor musunuz? Sizce mevcut sistemler kişisel mahremiyet ve güvenlik için yeterli mi?" Avrupa Birliğinin standartlarının Türkiye'ye de uyarlanması ve getirilmesi lazım diye düşünüyorum.

"Siz tam yetkili olsanız yasa dışı dinleme ve izlemeleri nasıl ortamdan kaldırabilirsiniz? " Çok zor, yani "measure", "counter measure" var. Siz alsanız…

ŞİRİN ÜNAL (İstanbul) – Komisyon kendini fazla hırpalamasın.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. ENİS ÇETİN – Evet. Çok zor ama bilgisayarınızı şey yapmak istiyorsanız İnternet kablosunu çekebilirsiniz, o zaman bir güvenliğiniz oluyor.

Teşekkür ederim.

BAŞKAN – Çok teşekkür ederiz.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Ben bu konuda bir şey söylemek istiyorum.

BAŞKAN – Buyurun.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Tabii, bunu kaldırmak mümkün. "Her şeyi kaldırdık." demek mümkün değil ama yasal bir cezası olması lazım. Yani, nasıl okullarda cam kırmanın önüne geçemezsiniz çünkü…

ŞİRİN ÜNAL (İstanbul) – Adam öldürmeyi ortadan kaldıramazsınız.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Evet, yani… Ama mutlaka çocuk onun suç olduğunu bilecek ve dolayısıyla ona göre davranacak. Fakat, hani, böcekler falan… Yasa dışı izleme konusunda en kritik şeyler elektriğin olduğu yerler. Dolayısıyla, avizelerin içi, prizlerin için gibi yerler her odada var. Ayrıca da elektrik var. GSM, cep telefonlarının içi... Eğer ortamda başka bir şey yoksa, eğer boşaltabiliyorsanız o alanı, böcek de yaptığı bu kayıtları bir şekilde nakliyorsa bunu frekanstan tespit etmeniz mümkün olabilir ama dediğim gibi, çok zor. Bir kere, her şeyi temizleyeceksiniz, boşaltacaksınız, etraftaki yayınların girmesini önleyeceksiniz… O oldukça zor bir işlem.

BAŞKAN – Evet Hocam, bitirdik ama Erdal Bey'in herhâlde son bir sorusu var.

ERDAL AKSÜNGER (İzmir) – Yani, soru değil de şey için söyleyeceğim. Tabii, hocalarım da bilirler, biz de hemen hemen aynı şeyleri yapıyoruz, birbirimizi de tanıyoruz, bizim hoca. Teknolojinin böyle bir şeyine hâkim olmak mümkün değil, bunu zaten ilk günden beri de söylüyoruz. Bizim meselemiz de bence o olmalı zaten. Efendim, bunu nasıl önleyebiliriz? Önleyemeyiz yani. Öyle bir… Dünyanın hiçbir yerinde kamunun kendisi de -ben bunu her zaman söyledim- sektörel bazda hiçbir zaman, hiçbir şeyin önünde değil zaten. Üniversiteler veya özel sektör her zaman kamunun önünde ama şu var:

Bir: Müeyyidelerin düzgün bir şekilde… Bence temel amaç o olmalı. Bizim müeyyideleri artırmamız lazım, birincisi o.

Denetimlerin gerçekten nasıl yapılabilmesi gerektiğini ortaya koymamız lazım. İlk günden beri de söylüyorum, yasamanın üyesi olarak birtakım vesayetleri neredeyse aşamıyoruz. Bu ciddi bir sorundur Türkiye'de. Hukuki altyapısının doğru bir şekilde ortaya koyulması ihtiyacı var, bu kesin yani.

Önleyici tedbirler kesinlikle şart.

Yapanların cezalandırılması… En yüksek düzeyde yapılması lazım çünkü bununla ilgili olarak.

Ama ortada da bir facia var, yani gerçekten bir terör var ortada, özel hayatın ihlali terörü var. Onu da biliyorsunuz ki her türlü… Bunu sizler de çok rahatlıkla anlayan bir insan olarak söylüyorum, ilk geldiğimiz günden beri de söylüyoruz, bu konu sayısallaşıp dijitalleştikten sonra bir vesileyle, sizin kendinizi koruyabilecek alabileceğiniz asgari tedbirleriniz… İşletim sistemleriniz konusu, işte, açık kaynak kodlu yazılımlar, işte, virüslerdir, diğer şeylerdir, bunlar bir vesileyle bir tedbir ama her şeyi de getirmez. Bence biz ana arterden uzaklaşmadan, yani özellikle bunun üzerine…

Bir kere "Kim yaptı?"yı tespit etmekle ilgili bir görevimiz var.

İki: Bence, müeyyideleri artırmak, denetim.

Şunu soracağım size denetimle ilgili: Dünyanın her yerinde yeni denetim mekanizmaları kurulmaya çalışılıyor, siz de biliyorsunuzdur bunları. Avrupa çok çalışıyor buna, Amerika'da oldu. En son bir form konusu oldu, ben çok uğraştım onunla ilgili, fişlenme konusunda. Yarı resmî bir denetimin yapılması konusu. Yani, bu hep tartışılıyor, Avrupa'da da çok tartışılıyor. Bununla ilgili nasıl bir kurum olmalı sizce, yani denetimi ortaya koyabilecek bir kurum yapısal olarak nasıl olmalı? Ne düşünüyorsunuz?

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – Vallahi, o konuda çok hazırlıklı değilim ben ama BTK…

BAŞKAN – Hocam, bu soruyu düşünerek daha sonra da yazılı bilgi verebilirsiniz. Zaten başka sorular da var.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – BTK aslında bu türden çok, düzenleyici bir kurum, yani kuralları belirleyici bir kurum ama denetleyici bir kurum anlamında değil.

ERDAL AKSÜNGER (İzmir) – BTK zaten denetleyici bir kurum değil, ben de onu söylemeye çalıştım işte. Zaten BTK değil, denetim yapan bir kurum değil.

BİLKENT ÜNİVERSİTESİ ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ BÖLÜMÜ ÖĞRETİM ÜYESİ PROF. DR. AYHAN ALTINTAŞ – O daha çok regülasyon yapıyor, regülasyonun olup olmadığını belki kontrol…

ERDAL AKSÜNGER (İzmir) – Belki en büyük dertlerimizden birisi, denetim mekanizmasındaki açıklar, gedikler.

BAŞKAN – Tekrar teşekkür ediyoruz size ve sabah sunum yapan arkadaşlara, ellerinize sağlık.

Eksik kalan bölümlerde arkadaşlarımız da size yardımcı olacaklar, bu sorulara da cevap verirseniz memnun oluruz.

Bugünkü çalışmamız burada bitiyor arkadaşlar. Yarının programı da belli, sizlere gönderildi. Önümüzdeki hafta İstanbul'u öngörüyoruz ama henüz bir netlik oluşmadı. Gelişmeleri sizinle paylaşacağız. Yarına kadar bir gelişme olursa yarın onu…

ŞİRİN ÜNAL (İstanbul) – "Bizi izlemeye devam edin." diyoruz.

BAŞKAN – Evet.

Teşekkür ederiz.

Toplantıyı kapatıyorum.

Kapanma Saati. 12.25