

TÜRKİYE'DEKİ KRİPTOLOJİ UYGULAMALARININ TARİHÇESİ

Olay SALCAN

Uzun yıllar TSK'de bulunduğum görevlerin ağırlığı, haberleşmenin sağlanması ile ilgili idi. Bu haberleşmenin sağlanmasındaki en önemli unsur ise güvenliktir. TSK ulusal güvenliği ilgilendiren her konunun iletilmesinde güvenliğe büyük önem vermiş ve çok büyük bir titizlik göstermiştir. Bu titizlik ve hassasiyet bu gün de artarak devam etmektedir. Kripto ise bu güvenliğin sağlanmasında uygulanan ilk ve önemli güvenlik unsurlarından birisidir.

Ancak bu güvenliğin ulusal kaynaklardan elde edilen kripto cihazları ile değil dış kaynaklardan temin edilen kripto cihazları ile yapıldığı da bir gerçektir. Bilinen bir şey vardı; o da ulusal olmayan kripto cihazları ile güvenliğin yeteri kadar sağlanamayacağı idi. Bu konu, daha sonraları TSK'de bir prensip haline gelerek yapılan çalışmalara ışık tutmuştur. Türkiye'deki bilgi güvenliği alanındaki gelişmelere, TSK ile TÜBİTAK'ın yürüttüğü müşterek çalışmaların olumlu katkıları olmuştur.

Türkiye'de, bir kripto cihazı üretilmesi konusunda bilgi, beceri ve altyapı da yoktu. TSK'nin kullandığı kripto cihazları dış kaynaklıydı. TSK, bu cihazları dışarıdan alıyor ve karşılığında büyük paralar ödüyordu. Yalnızca parasını ödemek yetmiyor, bir cihazı alabilmek için aylar hatta bir yıl kadar uzun bir süreyi beklemek gerekiyor, acil ihtiyaçların karşılanmasında büyük sıkıntı çekiliyordu. Bunun da nedeni, kripto cihazlarını almak istediğiniz ülkelerin kanunlarına göre resmi makamlarının onayı gerekiyor ve bu da uzun bir süre alıyordu. Cihazların bakım ve onarım ücretleri için dışarıya ödenen para da, oldukça büyük bir yekun tutuyordu.

Haberleşme ve bilgi teknolojilerindeki gelişmelere uyum sağlamak için gerekli güvenlik tedbirlerinin alınmasında; yeni teknolojiye uyumlu kripto cihazlarının yurt dışından temin edilme zorlukları ve maliyetlerinin yüksekliği nedeni ile, büyük sorunlar yaşanıyordu. Yaşanan bu zorluklara ilave olarak aynı zamanda TSK içerisinde, ulusal olmayan kripto cihazları ile güvenliğin sağlanamayacağı gerçekleri görülmüş ve ulusal kripto cihazının Türkiye'de gerçekleştirilmesinin gerekliliği konusunda fikirler oluşmaya başlamıştı.

İlk ulusal kriptoloji cihazı üretilmesi çalışmaları, 1974 yılı içerisinde yeni adı ile GEBZE'deki Marmara Araştırma Merkezi, eski adıyla Marmara Araştırma Enstitüsü'nün bünyesinde bulunan Elektronik Araştırma Ünitesi'nde başlatılmıştır. EAÜ, bu gün faaliyetlerini Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) adı altında yürüten Enstitü'nün başlangıç noktasıdır. Türkiye'nin bilgi güvenliği tarihinde önemli bir yeri işgal etmesi nedeniyle, bu Ünite'nin tarihçesine burada kısaca değinmenin faydalı olacağını değerlendirmekteyim.

EAÜ, ilk defa 1968 yılında, Ankara'da bulunan Ortadoğu Teknik Üniversitesi Mühendislik Fakültesi binasında, 5 kişilik bir araştırmacı grubu ile kurulmuştur.

1972 yılında, Ankara'dan Gebze-Kocaeli'deki MAE yerleşkesine taşınarak bundan sonraki faaliyetlerini MAE'ye bağlı bir birim olarak yürütmeye başlamıştır. Bu ünitenin kriptoloji cihazı yapılması ile ilgili üç kişiden oluşan araştırmacı ekibi, bundan sonra çalışmalarına GEBZE'de devam etmiştir. Halen bu çalışmalar bu yerleşkede sürdürülmektedir.

TSK, resmi olarak ilk defa 1975 yılında EAÜ'den ulusal bir kriptoloji cihazının yapılıp yapılamayacağını araştırılmasını talep etmiştir. Verilen cevapta bunun mümkün olduğu belirtilmiştir. Ayrıca, araştırmaların TSK tarafından desteklenmesi halinde, bir proje olarak kendileri tarafından çalışmalara başlanabileceği ifade edilmiştir. Bu rapor doğrultusunda, TSK da bu güne kadar EAÜ tarafından yürütülen çalışmaları uygun gördüğünü ve EAÜ bünyesinde bir ulusal on-line kriptoloji cihazının yapılabileceğine kanaat getirdiğini belirterek, yürütülen çalışmaları destekleyeceğini bildirmiştir.

05 Mayıs 1976 tarihinde de ulusal on-line kriptoloji cihazı çalışmalarının TSK'nın projesi olarak uygun görüldüğü belirtilerek 4 adet prototip üretilmesi çalışmalarına başlatılması istenmiştir.

23 Kasım 1976 tarihinde Türkiye'de ilk defa ulusal on-line kriptoloji cihazının prototipinin üretilmesine başlanmıştır. Bu arada proje grubunda çalışanların sayısı da on ikiye yükselmiştir.

İlk prototipin üretimi, 1978 yılı Şubat ayının ilk haftasında, yani başlangıcından on beş ay gibi bir süre sonra gerçekleştirilmiştir. Böylece Türkiye'de ilk defa Türk

tasarımcı, mühendisi ve teknisyeni tarafından, o günün şartlarına uygun olarak TSK'nın ihtiyaçlarını karşılayabilecek bir ulusal on-line kriptoloji cihazı yaratılmıştır.

Yeni ulusal on-line kriptoloji cihazının ismi de MİLON-I, açık adıyla; "Milli On-Line Kriptoloji Cihazı-I" olarak belirlenmiştir. Bundan sonra da bu cihaz, TSK'nın kriptoloji envanterine bu adla girecek ve ulusal on-line kriptoloji cihazlarının atası olarak tarihteki önemli yerini alacaktır. O tarihte üretilen ve TSK'da kullanılan MİLON-I On-Line Kriptoloji cihazlarının serisi, teknolojik gelişmeler ve TSK'nın ihtiyaçlarına paralel olarak bu gün MİLON-VII'ye kadar ulaşmıştır.

28 Mart 1978 tarihinde Genelkurmay Başkanlığında yapılan toplantı sonu alınan kararda; "Yurt içinde kriptoloji cihazı tedarikini sağlayarak, hem kriptoloji güvenliğini daha sağlam temellere oturtmak ve hem de döviz kaynaklarımızı daha ekonomik olarak kullanmak için, öncelikle yurt içindeki mevcut imkanlardan yararlanılması konusunda iki yıl önce TÜBİTAK'ta başlatılmış olan ulusal on-line kriptoloji cihazı projesi üzerine hızla gidildiği ve kısa zamanda yapılan çalışmalar sonucunda cihazın bir laboratuvar prototipinin meydana getirilmiş olduğunun memnuniyetle görüldüğü belirtilmiştir. Buna ilaveten de, ancak yurt dışından cihaz tedarikine devam edildiği, hatta az bir miktar dahi olsa yeniden cihaz alındığı takdirde, yurt içinde uzun süre kriptoloji cihazı üretiminin gerçekleşmeyeceği, hatta bu projenin terk edilmek zorunda kalacağı; halbuki TÜBİTAK tarafından ortaya çıkarılan, cihazların gözle görülür bir duruma geldiği bir sırada da projenin devamını tehlikeye düşürebilecek atılımlara girişilemeyeceği" beyan edilmiştir.

Böylece, dışarıdan hiç bir kriptoloji cihazı teminine gidilmeden yürütülen projenin sonuna kadar desteklenmesine karar verilmiştir.

Bu arada TSK, MİLON-I cihazlarının NATO TEMPEST Standartlarına göre test edilmesinin uygun olacağı şeklinde bir talepte bulunmuştur.

O günkü şartlarda, bu imkan ve kabiliyetlere sahip olunmaması nedeni ile, bu testlerin yapılamayacağı beyan edilmiştir.

Bu durumda, TEMPEST Laboratuvarı'nın en kısa zamanda kurulması, bilgi, yetenek ve yetişmiş elemana sahip olunması ve sonuçta kriptoloji cihazlarının TEMPEST testlerinin yapılabilmesi gerekliliği ortaya çıkmıştır. Bu ihtiyaç doğrultusunda, daha sonra da bahsedeceğimiz üzere, yapılan çalışmalar neticesinde, Türkiye, bugün akredite olmuş bir TEMPEST laboratuvarına, onu

işletecek bilgiye ve yetişmiş personele sahiptir. O kadar ki 10-14 Mayıs 2005 tarihleri arasında, UEKAE’de bulunan bu TEMPEST laboratuvarında, 12 NATO ülkesinden 26 personelin katılımı ile bir TEMPEST Work-shope düzenlenmiştir.

Üretilen ilk MİLON-I kriptu cihazları, 04 Temmuz 1984 tarihinde TSK’ya teslim edilmiştir. TSK’nın zaman içerisinde artan iletişim kabiliyetlerine paralel olarak çoğalan güvenlik taleplerinin karşılanması amacıyla, yeni teknolojiyi kapsayan on-line kriptu cihazlarının üretilmesine ihtiyaç duyulmaya başlanmıştır.

Yeni nesil MİLON-II 23 Mayıs 1990, MİLON-III 15 Aralık 1995 tarihinde hizmete girmiş ve bunları diğer cihazlar takip etmiştir.

1991 yılı içerisinde EAÜ, bağlantı değişikliği yapılmadan Elektronik ve Yarı İletkenler Teknolojisi Bölümün’e (EYİTB) dönüştürülmüştür.

22 Ocak 1991 tarihinde Genelkurmay Başkanlığına gönderilen yazıda; TÜBİTAK-MAM’ın 1991 yılında yeniden bir yapılanmaya gideceği, kurulacak bu yeni yapıda kriptu biriminin kriptu-analiz yetenekleri kazandırılarak daha da büyütülmesinin planlandığı belirtilmiştir. Ancak bu planlamanın başarılı olabilmesinin, TSK’nın desteği ile mümkün olabileceği vurgulanmıştır. Sonuç olarak ta, kriptu cihazlarının güvenilirlik derecelerini kriptolojik yönden tayin edebilme yeteneğine sahip, ulusal kriptu algoritmaları ve cihazlarını bir aile olarak tasarımlayan, geliştiren, üreten bir “Kriptoloji Merkezi”nin Genelkurmay Başkanlığı yönetim ve denetiminde MAM bünyesinde kurulması teklif edilmiştir.

09 Kasım 1992 tarihinde Genelkurmay Başkanlığı buna cevabında,; TEMPEST, EMP (Electromagnetic Pulse) koruması ve elektronik harbe (EH) dayanıklılık gibi özelliklerin; muhabere, elektronik ve bilgisayar sistemlerinde aranan özellikler olduklarını belirtmiştir. Bunların teknik şartnamelere dahil edilmesine rağmen, test ve ölçümlerinin mevcut imkanlarla yeteri kadar yapılamadığı, bu nedenle bir “TEMPEST Test Laboratuvar”ına ihtiyaç duyulduğu vurgulanmıştır.

Ayrıca, aynı cevapta, yurtiçi ve yurtdışı kaynaklardan tedarik edilen haberleşme emniyet cihazlarının, hizmet süreleri boyunca kriptu analizlerinin yapılması, sağladıkları emniyet düzeylerinin kontrolü, modifikasyon ihtiyaçlarının tespiti, ihlale uğrayan veya yeni nesil ulusal cihazlar için algoritma geliştirilmesi gibi hassas hizmetlerin yapılabilmesi için bir “Kriptu Analiz Merkezi” kurulmasının gerekliliği önemle belirtilmiştir.

Sonuç olarak ta; her iki tesisin kurulabilmesi maksadıyla MAM'daki mevcut imkanların değerlendirilmesi konusunda bir inceleme yapılması talep edilmiştir.

Burada bir "TEMPEST Test Laboratuvarı" ve "Kriptoloji Merkezi" ifadesi kullanılmakla beraber, gerçekte ileride teşkil edilecek ve Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü-UEKAE adını alacak bir enstitünün kurulmasının ana fikri oluşmakta ve temelleri atılmaktadır.

Halen Enstitü Müdürü olarak görevini sürdüren Önder Yetiş ve beraberinde çalıştığı ekibinin bu teşkilata katılımı 15 Ekim 1993 yılında olmuştur. TELETAS AR-GE direktörlüğünden ayrılan Önder Yetiş, Yarı İletken Teknolojileri Araştırma Bölüm Başkanı olarak TÜBİTAK'a girmiştir. Çalışanların sayısı da 20'ye ulaşmıştır.

Yeni katılımcıların gizlilik kleranslarının ellerine geçmesi ile bölümde bulunan bir kasa açılmış ve içerisinde MAM bünyesinde bir kripto analiz merkezinin kurulması ile ilgili bir andıç bulunmuştur. Bu andıca paralel olarak Genelkurmay Başkanlığı ile yapılan müşterek çalışmalar neticesinde; MAM'da "Kriptografik Test ve Tasarım Merkezi"nin kurulması ile ilgili sözleşme, 1994 tarihinde MAM ve MSB arasında imzalanmış ve tesis de 1997 yılında tamamlanarak hizmete açılmıştır.

Yapılan çalışmalar sonunda, 1995 yılında "EMC/TEMPEST Test Merkezi"nin kurulması ile ilgili sözleşme MSB ile imzalanmıştır. 1999 yılında ise bu Merkez'in kurulması işlemleri tamamlanarak faaliyete geçirilmiştir.

Buraya kadar, Türkiye'de bir ulusal kripto cihazının Türk mühendis ve tasarımcısı tarafından, TSK'nin büyük desteği ile nasıl meydana getirildiğinin ve ondan sonraki gelişmeleri kısa bir tarihçesini, olayların akışı içerisinde anlatmaya çalıştım. Mühim olan bu işe başlayabilmek ve belirli bir yere gelebilmek idi. İhtiyaç duyulan bilgi, deneyim, beceri, altyapı ve insan gücü sağlandıktan sonra, teknolojik ilerlemeler yakından takip edilerek bu alandaki süratli gelişme temposu kendiliğinden yakalanmıştır.

Bundan sonraki gelişmeleri çok kısa olarak özetlemeye çalışacağım:

Tüm bu gelişmelerin mevcut yapı ile devamının mümkün olmadığı görülerek, yeniden bir yapılanmaya gidilmesinin gerekliliği hissedilmeye başlanmıştır.

Bu nedenle de, yukarıda da belirttiğimiz üzere, Elektronik ve Yarı İletkenler Teknoloji Bölümü, 1995 yılında bir enstitüye dönüştürülerek MAM'a bağlı olarak

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü-UEKAE adı altında, bundan sonraki faaliyetlerini yürütmeye başlamıştır.

1998 yılında ise Enstitü MAM'dan ayrılarak doğrudan TÜBİTAK'a bağlanmıştır. Halihazırda bu statüsü devam etmektedir.

Bir kriptoloji cihaz ya da algoritmasının NATO üyesi ülkelerde kullanılabilmesi için NATO'nun onayı alınması gerekmektedir. Bu konuda yapılan çalışmalar neticesinde bir kısım cihaz ve algoritmaların NATO onayı da alınmıştır. Türkiye de, NATO tarafından onaylanan kriptoloji cihaz, algoritma ve sistemleri ile; A.B.D., İngiltere, İtalya, Norveç ve Fransa gibi bu konuda söz sahibi birkaç NATO ülkesinden biri olarak ve her yıl yenilenerek yayınlanan NATO ülkelerinde kullanılacak NATO Kriptoloji Cihazları Listesine girmiş bulunmaktadır. UEKAE, NATO'nun INFOSEC Alt Komite ve çalışma gruplarının tüm çalışmalarına katılmakta ve Türkiye'nin NATO'da INFOSEC alanında etkin bir rol oynamasına katkı sağlamaktadır.

Enstitüde Yarı İletken Teknolojisi Araştırma Laboratuvarı, EMC/TEMPEST Test Merkezi ile Kriptografik Test ve Tasarım Laboratuvarı'nın yanında daha sonraları; Tam Yansız Oda, Ağ Güvenliği Laboratuvarı, Akustik Test Laboratuvarı da tesis edilip farklı zamanlarda faaliyete geçirilerek güvenlik konusunda verilen hizmet çok yönlülüğe kaydırılmıştır.

1968 senesinde ODTÜ'de temelleri atılan ve 1974'de GEBZE'de çalışmalarına üç kişi ile Elektronik Araştırma Ünitesi adı altında devam eden bu ünite, bu gün 500'ü aşan çalışanı ile büyük bir enstitü haline gelmiştir. Çalışanlarının %91'i araştırmacı personeldir.

Birkaç kelime ile UEKAE'den de bahsetmek isterim.

Enstitünün Vizyonu

Bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak.

Enstitünün Misyonu

Bilgi güvenliği, haberleşme ve ileri elektronik alanlarında, Türkiye'nin teknolojik bağımsızlığını sağlamak, sürdürmek ve rekabet gücünü artırmak için, nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile, bilimsel ve teknolojik çözümler üretmek ve uygulamaktır.

Enstitünün çalışma alanları; Bilgi güvenliđi, Mikroelektronik, Mikrooptik ve Elektronik Harp'tir.

Enstitünün Kuruluşu

Ürün Geliştirme Bölümü

1978 yılında üretilen ilk milli kriptu cihazı prototipinden sonra günün artan ihtiyaçlarını karşılamak maksadıyla gelişen teknolojik imkanlar kullanılarak çeşitli kriptu cihazlarının tasarımı yapılmıştır.

Kullanıcıya tek bir cihazla güvenli ses, veri ve faks gibi haberleşme imkanı yaratılarak çok maksatlı bir ortam tesis edilmiştir.

Kriptu Analiz Bölümü

Bu bölümde milli kriptu algoritmaları ve protokollerinin test ve tasarımları gerçekleştirilmektedir. Ayrıca, diğer tasarımcılar tarafından gönderilen kriptu algoritmalarının deđerlendirmeleri yapılmaktadır.

Mikroelektronik Bölümü

Bu bölümde, Yarı İletken Araştırma Laboratuvarında yonga (chip) üretilmekte ve üretilen bu yongalar tamamen Enstitü tarafından tasarlanan kriptu cihazlarında kullanılmaktadır.

TEMPEST Bölümü

Bu bölümde, gizlilik dereceli bilgilerin korunması ve bu bilgileri işleyen elektromanyetik özellikteki sistem ve cihazların bilgi güvenliđi açısından ne kadar güvenli olduklarının belirli ölçümlerle test edilmesi, bu testler ile ilgili yöntemleri, bilgi emniyetini zedeleyebilecek istenmeyen elektromanyetik sızıntıların kontrol altına alınması ile ilgili önlem ve uygulamaların tümünü kapsayan faaliyetler yürütülmektedir.

Ađ Güvenliđi Bölümü

Bir kısmı Ankara'da konuşlanmış bölüm bünyesinde, kurulan bilgi sistemleri güvenlik laboratuvarı ile milli ITSEC kriterlerine göre sistemlerin güvenlik test ve deđerlendirme işlemleri yürütülmekte, korunması bulunmayan sistemler korunur hale getirilmekte, ađ ortamında işleyen mevcut bilgi sistemlerinin açıklıkları saptanmakta ve gerekli önlemler alınmaktadır.

İLTAREN Bölümü :

Ankara'da konuşlanmış bu bölüm TSK'nin ileri teknoloji ile ilgili ihtiyaçlarını karşılamak ve bu konuda yeterli seviyeye gelmesini sağlamak maksadıyla faaliyetlerini sürdürmektedir.

Arz ederim.