ASELSAN İLETİŞİM VE BİLGİ GÜVENLİĞİ YETENEKLERİ

Ali YAZICI, Hamdi ERKAN
ayazici@aselsan.com.tr, herkan@aselsan.com.tr
ASELSAN A.Ş.
Haberleşme ve Bilgi Teknolojileri Grubu
Kripto ve Bilgi Güvenliği Müdürlüğü
Tel: 0312 5921510
Faks: 0312 3541679

ÖZET

Günümüzde bilgi sistem ve iletişim teknolojilerinin gelişimiyle beraber bilgi ihtiyacı ve paylaşımı önem kazanmıştır. Bilgiye ulaşmak kolay hale gelmiş ve doğru bilgiye, güvenilir kaynaktan ve güvenilir bir biçimde nasıl ulaşırım kaygısı oluşmuştur. Bu kaygılar ancak gizlilik, veri bütünlüğü, kimlik doğrulama ve inkar edememe güvenlik ilkelerinin desteklendiği bilgi güvencesine uygun güvenlik mimarilerinin kullanılması ile giderilebilmektedir.

Bilgi güvencesinin temeli kriptografiye dayanmaktadır. Kriptografi ihtiyaç duyulan güvenlik ilkelerini sağlamak için gerekli matematiksel yöntemleri bir araya getirmektedir. Kriptografik ürünler, güvensiz yollarla yapılan iletişimin güvenliğini sağlamak amacıyla, kriptografik ilkeler çerçevesinde geliştirilmekte ve gerçek hayatta kullanılmaktadır. ASELSAN tarafından anayurt güvenliği ve siber güvenlik amacıyla geliştirilen kriptografik ürünler sahip olduğu simetrik, asimetrik ve özet algoritmaları, özgün kriptografik protokolleri, TEMPEST ve kırmızı-siyah fiziksel ayrımına uyumlu donanımsal tasarımları, yetkisiz kurcalanmaya karşı korunmuş yapıları ve sunmuş olduğu milli çözümler ile güvenlik mimarilerinin vazgeçilemez bir parçası olarak yer almaktadır.

ANAHTAR KELİMELER:
Kriptoloji, Kripto Algoritması, Ağ Destekli Yetenek, IP Kripto, IPSec

1. ASELSAN'DA KRİPTOLOJİ

1980'li yıllarda sadece telsiz ortamından yapılan ses haberleşmesinin kriptolanması amacıyla kripto cihazı geliştirme faaliyetlerine başlayan ASELSAN, 1990'lı yıllarda telli ve telsiz hatlar üzerinden yapılan her türlü ses, veri ve video haberleşmelerinin kriptolu olarak yapılabilmesi için gerekli olan dahili ve harici muhtelif kripto cihazlarını geliştirerek TSK'nin kullanımına sunmuştur. 2000'li yıllarda ise ASELSAN, kripto ve bilgi güvenliği konusunda ulaşmış olduğu üstün yetenek sayesinde günümüz teknolojisine uygun, yüksek güvenlik seviyesine sahip yeni nesil kripto cihazlarını tasarımlama yeteneğine sahip olmuş ve sadece yurt içi değil, yurt dışı pazarlara da yönelmiştir. Başta ABD, Uruguay, Pakistan, Mısır, Bosna ve Azerbaycan olmak üzere bir çok ülkeye kripto cihazı ihraç eder duruma gelmiştir. Ayrıca ASELSAN tarafından geliştirilen kriptografik ürünlerin NATO ve NATO üyesi ülkeler tarafından da

kullanılabilmesi amacıyla ihtiyaç duyulan NATO SECAN sertifikasyonu için gerekli çalışmalar da yapılmaktadır.

ASELSAN tarafından geliştirilen tüm kriptografik ürünlerde özgün milli kripto algoritmaları kullanılmaktadır. Kriptoloji alanındaki teknolojik gelişmelere paralel, kriptografideki son saldırı yöntemlerine dayanıklı ve istenilen güvenlik seviyesine uygun anahtar boylarında milli kripto algoritmaları özgün olarak tasarlanmaktadır. Milli algoritmaların dışında yurt dışına ihraç edilen Aselsan kriptografik ürünlerinde kullanılmak üzere güvenlik gereksinimlerine uygun olarak yurt dışı algoritmalarının da tasarımı gerçekleştirilmektedir.

Geliştirilen kripto algoritmaları literatürde bulunan testlerin yanı sıra Aselsan tarafından geliştirilmiş istatistiksel ve yapısal testler ile test edilmektedir.

ASELSAN tarafından geliştirilmiş ve milli olarak onaylanmış on adet milli kripto algoritması, NATO SECAN tarafından onaylanmış bir adet NATO algoritması ve 25'den fazla yurtdışı kripto algoritması bulunmaktadır. Üç adet yurtdışı kripto algoritmasının yurt dışına teknoloji transferi başarıyla gerçekleştirilmiştir.

Teknolojideki gelişmelere bağlı olarak gizlilik dışı servislerde kullanılan açık anahtarlı algoritmalara (RSA) ait anahtar uzunluklarının 2048 veya 4096 bit olması gerekmektedir. Taktik sistemlerde band genişliği ve işlem gücü sınırlamaları nedeniyle daha düşük anahtar uzunluklarına gereksinim duyulmaktadır. Eliptik eğriler sayesinde en yüksek güvenlik seviyeleri, RSA tabanlı algoritmalara nazaran çok daha kısa anahtar boyları (onda bir) kullanılarak ve çok daha az işlem gücü (beşte bir) harcanarak elde edilmektedir. ASELSAN tarafından mobil sistemlerde kullanılmak üzere geliştirilen yeni nesil kriptografik ürünlerde RSA tabanlı algoritmaların yerine ASELSAN tarafından tasarlanan özgün eliptik eğriler kullanılmaktadır.

Aselsan kriptografik algoritma tasarım yetenekleri aşağıda özetlenmiştir:

- Simetrik Algoritma Tasarımı (Comsec/Transec)
    - Dizi Tipi Simetrik Algoritmalar
    - Blok Tipi Simetrik Algoritmalar
- Asimetrik Algoritma Tasarımı
    - RSA Tabanlı Algoritmalar
    - Eliptik Eğri Tabanlı Algoritmalar
- Açık Anahtar Altyapısı (PKI)
- Özet Algoritma Tasarımı (HASH)
- Kripto Analiz
    - İstatistiksel Testler
    - Yapısal Testler

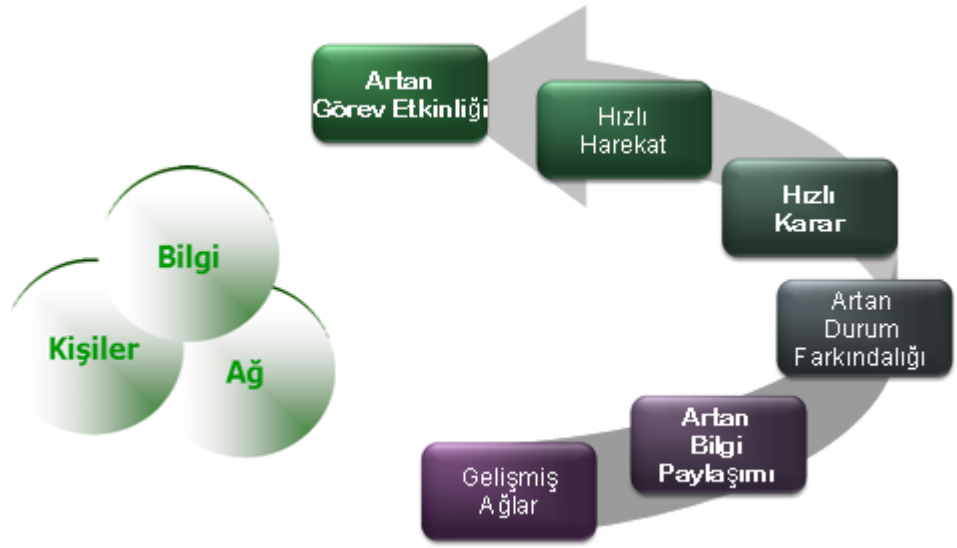
2. ASELSAN'DA AĞ DESTEKLİ YETENEK ÇALIŞMALARI

Ağ Destekli Yetenek, 2000'li yılların başında ABD savunma Bakanlığı tarafından askeri ve sivil kurumlar arasında bilgi değişiminde eşgüdümün sağlanması amacıyla

geliştirilen servis odaklı mimariye sahip IP tabanlı gelişmiş ağlardan oluşan Küresel Bilgi Şebekesii (Global Information Grid) kavramının NATO'ya bir yansımasıdır.

Temel olarak insan, bilgi ve ağ teknolojileri bileşenlerinden oluşan Ağ Destekli Yetenek, stratejik seviyeden taktik seviyeye kadar, bir bilgi sistemi ve IP ağ altyapısı kullanılarak, muharebe (operasyon) ortamının etkin olarak yönetilmesidir. Kısaca, Ağ Destekli Yetenek, bilgi çağına özgü olarak edinilen bilgi üstünlüğünün muharebe gücüne yansıtılması olarak da tanımlanabilir. NATO tarafından yayınlanan Ağ destekli yetenek kavramı, temel olarak siber saldırılara karşı dirençli, güvenli ve geniş alana yayılmış farklı ülkeler ve/veya kurumlar tarafından çalıştırılan federe bir IP haberleşme ağı üzerinden bilgi üstünlüğü temeline dayalı olarak güvenli bilgi paylaşımından oluşmaktadır. Bilgi paylaşımında en önemli husus harekat etkinliği açısından doğru bilgiye, doğru yer ve zamanda ulaşılmasıdır.

Ağ Destekli Yetenekte, sağlam, güvenli ve daha geniş bir coğrafi alana yayılmış servis odaklı mimari yapıya sahip IP tabanlı ağlar üzerinde gerçek zamanlı bilgi paylaşımı ile doğru karar verme süreçlerini hızlandırmak suretiyle komuta hızının ve harekat üstünlüğünün arttırılması hedeflenmektedir. Ağ destekli yetenek gelişim halkası Şekil 1'de gösterilmiştir.



Şekil-1: Ağ Destekli Yetenek Gelişim Halkası

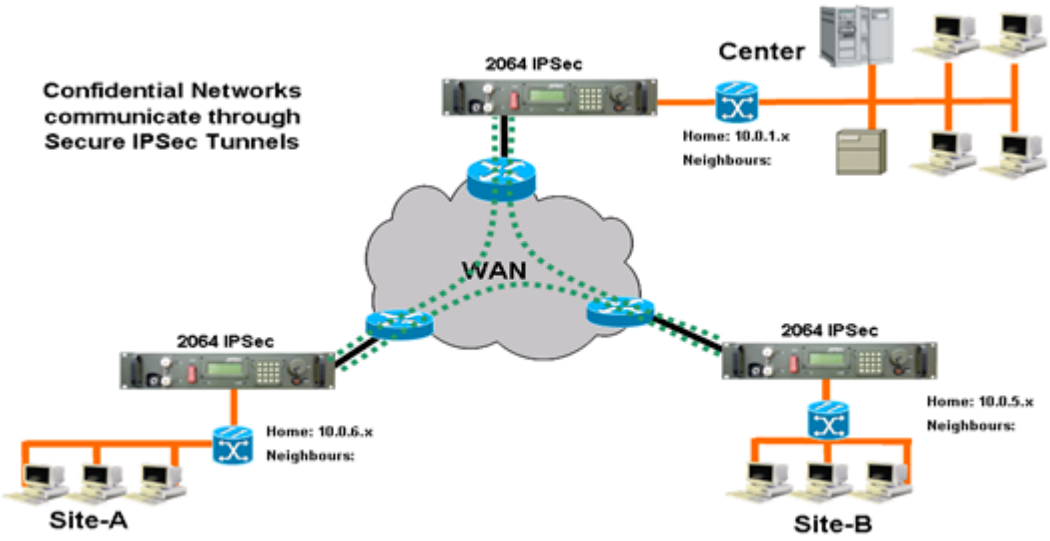
ASELSAN, stratejik ve taktik haberleşme sistemlerinde kullanılmak üzere geliştirmekte olduğu NATO NINE (Network Enabled Capability Network and Information Infrastructure IP network encryption) standartlarına uyumlu yeni nesil IP Kripto Cihazı, Sanal Hava Boşluğu sistemi, hem NINE hem de SCIP (Secure Communications Interoperability Protocol) uyumlu VoIP terminal ve Yazılım Tabanlı Telsiz (SDR) Ailesi ile yüksek güvenliğe sahip ağ destekli yetenek çözümleri oluşturarak doğru bilgiye, doğru yer ve zamanda ulaşılmasına olanak sağlamaktadır.

Şekil-2: Aselsan Ağ Destekli Yeteneği

3. YENİ NESİL IP KRİPTO CİHAZI

Aselsan 2064E IP Kripto Cihazı Yerel Alan Ağları (YAA) ve Geniş Alan Ağları (GAA) üzerinde IP paketlerini her iki yönde aynı anda şifreleyerek güvenli iletişim sağlayan yeni nesil bir IP ağ kripto cihazıdır.

Emniyetli Ağ Yönetim Sistemi ile uzaktan 2064E cihazlarının konfigürasyon, alarm ve emniyet yönetimi SNMP protokolü aracılığıyla yapılabilmekte ve ağ üzerinden anahtar yükleme işlemi gerçekleştirilebilmektedir.



Şekil-3: 2064E Cihazları ile Kurulan Güvenli Tüneller

2064E Cihazı, RFC 4301, 2402 ve 2406 IPSEC standartlarının yanı sıra NATO NINE standartlarına da uygun bir yapıya sahiptir. IPSEC Tünel (Tunnel) ve Aktarma (Transport) çalışma modlarında çalışabilen 2064E Cihazı üzerinde iki adet farklı gizlilik seviyesine sahip kripto algoritması bulunmaktadır. Bu sayede farklı gizlilik dereceli ağlar ile gerçek zamanda bağlantı sağlayarak güvenli bilgi paylaşımına olanak sağlamaktadır.

IP kripto cihazları tarafından güvenli tünellerin oluşturulabilmesi için güvenlik politikalarının tünel kurulacak IP adresleri ile birlikte kripto cihazlarına yüklenmesi gereklidir. Eski nesil IP Kripto cihazlarında bu işlemler statik olarak sistem yöneticisi tarafından manuel yöntemler ile cihazlara yüklenmektedir. Hareket gereksinimi olmayan, göreceli olarak sabit yapıda bulunan IP ağlarında uygulanabilir olan bu yöntem, taşınabilir, hareketli veya genişleyebilen IP ağlarında kullanıma uygun değildir; çünkü her değişiklik sonrasında, sistem yöneticisi tarafından ağ üzerinde bulunan tüm IP Kripto Cihazlarının manuel olarak konfigürasyonlarının yenilenmesi gereklidir.

Mobil sistemler olan Taktik Saha Muhabere Sistemlerinde ise IP şebekesini oluşturan alt birimler hareketli ve birbirlerine radyo linklerle bağlı bulunmaktadırlar. IP ağında zamana göre genişlemeler, değişiklikler, eklemeler ve çıkarmalar olabilmektedir. Bu nedenle IP ağının topolojisi sürekli olarak değişmektedir. IP ağ yapısına uyum sağlamak için sistem yöneticisinin müdahalesine gerek olmaksızın IP Kripto Cihazlarının birbirlerini otomatik olarak keşfetmeleri ve güvenli IP tünellerini kurabilmeleri için IP ağ topolojisini dinamik olarak elde edebilmeleri gerekmektedir.

Mobil IP desteğine sahip olan 2064E cihazları, dinamik keşif yeteneği ile kırmızı (güvenli) ağ topolojisini (OSPF ve BGP gibi mesajlarla) kriptolayarak siyah ağ üzerinden diğer 2064E cihazlarına güvenli olarak dağıtırlar. 2064E cihazları siyah ağ üzerinde herhangi bir konfigürasyona ve/veya operatöre ihtiyaç duymaksızın birbirlerini Tünel Keşif Protokolü (TED, Tunnel Endpoint Discovery Protocol) ile otomatik olarak keşfeder ve kriptografik olarak doğrulama işlemini gerçekleştirirler.

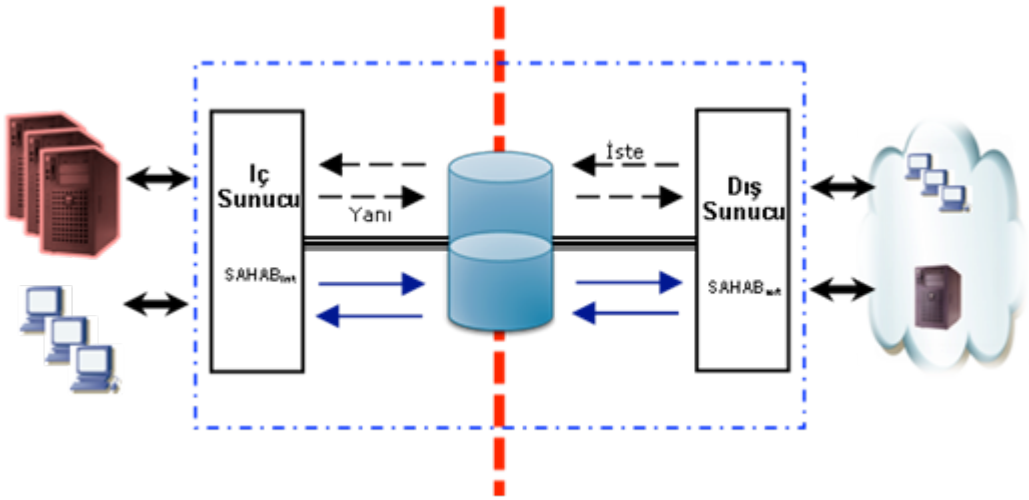
2064E cihazları sahip oldukları tünel keşif protokolü sayesinde, kripto cihazlarının IP adreslerini dinamik olarak dağıtabilmekte ve güncelleyebilmektedir. IP ağı üzerinde aktif olan kripto cihazları için bir veri tabanı tutulmaktadır. Bu veri tabanında sistem yöneticisi tarafından atanmış bir adet Master 2064E cihazı ve birden fazla yedek Master 2064E cihazı bulunmaktadır. Bu veri tabanının bir kopyası Master 2064E cihazında, diğer kopyaları ise yedek Master 2064E cihazlarında bulunmaktadır. Master ve Yedek Master 2064E cihazlarının listesi tüm 2064E cihazlarına sistem yöneticisi tarafından manuel ve/veya ağ üzerinden elektronik olarak yüklenebilmektedir.

2064E cihazları tünel modda Güvenlik İlişkisi Veritabanı (SAD, Security Associations Database) ve Güvenlik Politikaları Veritabanında (SPD, Security Policy Database) tanımlı olan bağlantılar için IP Ağı üzerinde IPSec standartlarında uygun ESP tünelleri kurarak, IP trafiğini bu güvenli tüneller içinden noktadan noktaya kriptolu olarak aktarırlar.

2064E cihazı sabit ve mobil IP uygulamalarında özgün olarak sahip olduğu üstün teknik özellikleri, yüksek işlem hızı ve askeri koşullara uygun mekanik yapısı ile ağ destekli yeteneğin vazgeçilmez bir parçasını oluşturmaktadır.

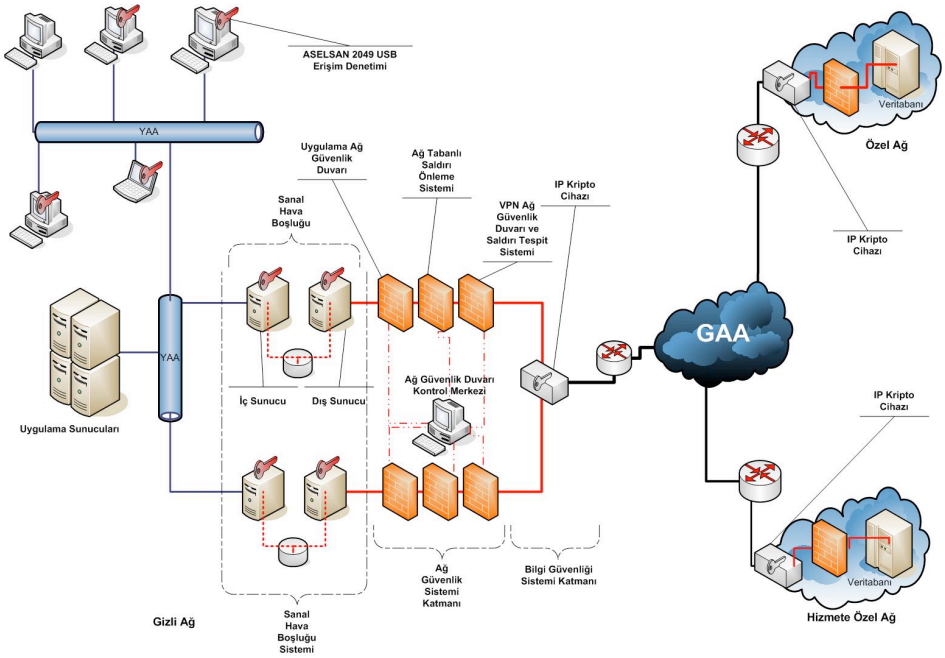
4. SANAL HAVA BOŞLUĞU SİSTEMİ

Aselsan 2180 Sanal Hava Boşluğu (SAHAB), farklı güvenlik seviyesine sahip ağların (Cross Domain Networks) yüksek güvenlik seviyesine sahip ağın güvenlik seviyesini ihlal etmeden birbirleriyle güvenli bilgi alış verişini sağlayan bir sistem çözümüdür.
Sanal Hava Boşluğu sistemi, gerçek zamanlı hizmet alan/veren kuruluşlar için gündemde olan güvenlik tehditlerine karşı durmak ve onları ortadan kaldırmak amacıyla tasarlanmıştır. Dış ağ (Internet) ile kurum ağı (iç ağ) arasında konuşlandırılan sistem, kendi içinde IP tabanlı iletişim kullanmamakta ve böylece iki ağ arasında yüksek düzeyde güvenlik sağlayan bir "sanal hava boşluğu" (virtual air gap) sınırı oluşturmaktadır. Sistemin bu özelliği güvenlik düzeyi yüksek (kritik) görev yapan kurumsal ağlar için düşük güvenlik seviyesine sahip ağlara güvenli olarak bağlanma konusunda arzu edilen bir güvenlik çözümü sağlamaktadır.
2180 Sanal Hava Boşluğu yönlendirilebilir bir protokolün doğrudan yüksek güvenlik seviyesine sahip ağa erişmesini engellemektedir. 2180 Sanal Hava Boşluğu, üzerlerinde özelleştirilmiş bir işletim sistemi bulunan iç ve dış iki sunucudan ve ortaklaşa kullanılan disk ünitesinden oluşmaktadır. Veri akışı ortak disk ünitesi üzerine okuma/yazma şeklinde gerçekleşmektedir. 2180 SAHAB iletişim modeli Şekil 4'de gösterilmiştir.



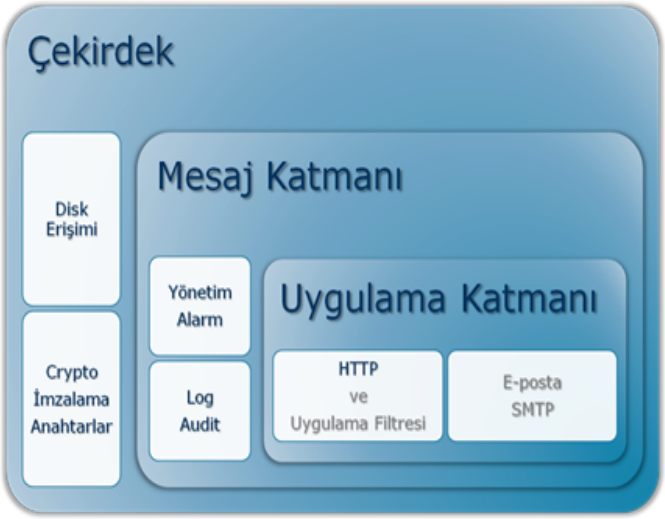
Şekil 4: 2180 SAHAB İletişim Modeli

İlgili kurum/kuruluş tarafından alınacak diğer güvenlik önlemleri gereğince, SAHAB sistemin dışında ve ona ek olarak çeşitli diğer güvenlik teknolojilerin dış ve iç ağ üzerinde barındırılması da mümkündür. Bu durum tasarlanmış sistemin çalışmasına engel olmadığı gibi, sistemin kurumsal ağ üzerinde konuşlandırılması da, kurumun aldığı diğer güvenlik önlemleri açısından bir sorun teşkil etmemektedir. 2180 SAHAB genel sistem mimari yapısı Şekil 5'de gösterilmiştir.



Şekil 5: 2180 SAHAB Mimari Yapısı

2180 Sanal Hava Boşluğu sistemi Şekil 6'de gösterildiği üzere üç katmanlı bir yapıya sahiptir. En alta disk erişim, kriptolama ve sayısal imza işlemlerinin yapıldığı çekirdek katmanı yer almaktadır. Ortada yer alan mesaj katmanında ise mesajlaşma paketlerinin içinden verinin çıkarılması ve/veya yeniden mesajlaşma paketlerinin yaratılması ile yönetim işlevleri, alarm ve log kayıtlarının tutulması gerçekleştirilir. En üstte birden fazla protokolün desteklendiği uygulama katmanı yer almaktadır.



Şekil 6: 2180 SAHAB Yapısı

2180 Sanal Hava Boşluğu sisteminin sunduğı güvenlik servisleri aşağıda özetlenmiştir;

- İç ve Dış sunucularda çalışan, özelleştirilmiş ve güvenliği arttırılmış bir 'Linux' işletim sistemi çekirdeği yer almaktadır.
- İç ve Dış sunucular arasında paket alış verişi paylaşılan disk üzerinden sadece iki sunucunun bildiği özgün bir veri alış veriş protokolü ile gerçekleştirilmektedir.

- İç ve dış sunucuların paylaştığı disk ünitesi özgün bir yöntemle biçimlendirilmektedir. Ayrıca disk üzerine bilgiler anlık ve şifreli olarak yazılmaktadır.
- Sistemin iç ve dış ağ arayüzleri üzerinden IP protokolü kullanılarak gelebilecek zararlı ve/veya gereksiz tüm trafiğin denetlenmesi, filtrelenmesi ve kayıt altına alınması amacıyla sistemde iç ve dış güvenlik duvarı özelliği bulunmaktadır.
- Saldırı Tespit: Güvenlik duvarından geçen ve sisteme erişen ağ trafiğinde barınabilecek muhtemel saldırıları önlemek ve kayıt altına almak amacıyla iç ve dış sistemde ağ ve sistem tabanlı saldırı tespit özelliği bulunmaktadır.
- İç ve dış sistemlerdeki tüm kritik dosya ve dizinlerde yetki dışı değişiklikleri denetleyen bir bütünlük denetleyicisi bulunmaktadır.
- İç ve dış güvenlik bileşeninde yapılan şifreleme işlemleri için gerekli olan anahtar bilgilerinin depolandığı bir donanım güvenlik bileşeni bulunmaktadır.
- Dış ve İç güvenlik bileşenleri arasında paylaşılan bellek üzerinden iletilen kimlik denetleme (authentication) ve canlılık (heartbeat) mesajlaşması özelliği bulunmaktadır.
- Dış ve İç güvenlik bileşenleri üzerinde anlaşılmazlık/şaşırtma (obfuscation) işlemleri gerçekleştirilmektedir.
- Dış ve İç güvenlik bileşenleri üzerine yerleştirilmiş orijinallik (authenticity) bilgisi bulunmaktadır.
- Dış ve iş güvenlik bileşeni arasında özel mesaj sıralama protokolü bulunmaktadır.
- İzleme/Günlükleme ile ilgili kayıtlar tutulmaktadır.
- Sistem Bütünlüğü'nü denetleme mekanizmaları bulunmaktadır.

Ağ destekli yetenek, farklı ülkeler ve/veya kurumlar tarafından çalıştırılan federe bir IP haberleşme ağı üzerinden bilgi üstünlüğü temeline dayalı olarak güvenli bilgi paylaşımını gerektirmektedir. Ağ destekli yetenekte ağ kavramı genişleyerek iç ağ veya dış ağ ayrımı yapılmaksızın, federe ağda yer alan herhangi bir bilgi sistemi ile bilgi paylaşımını zorunlu kılmaktadır. Ağ yapısnın gelişmesi ile, ağlar siber saldırılara karşı daha açık hale gelmekte; bunun sonucu olarakda daha komplike güvenlik politikalarının uygulaması ihtiyacı ortaya çıkmaktadır.

Bilgi paylaşımım güvenli ve sağlıklı olarak gerçekleştirilmesinde, İyi tasarlanmış bir bilgi ağı mimarisinin yanı sıra uygun iletişim protokolleri ve şifreleme yöntemlerinin kullanımı, bilgi ağı cihazlarının seçim ve konfigürasyonu, güvenlik duvarı, anti-virüs yazılımları ve saldırı tespit sistemi gibi bilinen kontrol araçlarına ilave olarak ASELSAN 2180 Sanal Hava Boşluğu sistemi, ağ güvenlik ve erişim denetimi alanında bünyesinde barındırdığı özellikler ile yeni bir sayfa açmaktadır.

5. SONUÇ

Yeni nesil IP Kripto Cihazı, Emniyetli IP Telefon, Emniyetli Yazılım Tabanlı Telsizler, Sanal Hava Boşluğu Sistemi ve Milli Güvenlik Duvarı çözümleri yanı sıra ASELSAN,

bilginin kendisini korumaya yönelik çevrim içi ve çevrim dışı kripto özelliklerine sahip milli olarak geliştirilmiş geniş bir kriptografik ürün yelpazesine sahiptir.

Kripto ve bilgi güvenliği çözümlerinin milli olarak karşılanması önem arzetmektedir ASELSAN 35 yıllık deneyimi, bilgi güvenliği ve kriptoloji alanında ulaşmış olduğu olgunluk seviyesiyle bilgi teknolojileri ve bilgi güvencesi konularında her türlü hizmeti sağlama ve bilgi güvenliği ürününü geliştirme yeteneğine sahiptir.