rovenma Smart Technology

L1 Link, L2 Ethernet ve L3 IP Kripto Cihazları

Kripto Sistemleri Kökeni

Şadi Çağatay Öztürk

Rovenma CTO

Kripto (crypto) kelimesi Fransızca'dan dilimize geçmiş "cryptogramme" kelimesinin kısaltmasıdır. Bu kelime ise eski Yunanca kryptós (gizli) ve grámma (yazı) kelimelerinin birleşimi olarak Fransızca'ya geçmiştir.

Kripto, yani gizli yazı, neredeyse yazının icadı kadar eskidir. Bulunabilen en eski kripto örneği yaklaşık 4000 yıl öncesinde Mısır'da Menet Khufu kentinde Khnumhotep II'nin mezarı üstündeki yazılardır. Bu yazılar klasik hiyerogliflerden farklıdır ve gizli anlamlara sahiptir.

Antik zamanlardan beri çeşitli medeniyetler farklı şifreleme teknolojileri geliştirmiş ve rakiplerinin şifreleme teknolojilerini kırmaya çalışmıştır. Orduların konumlarından merkezi yönetimlerin emirlerine kadar birçok veri hedeflere korunaklı ve gizli olarak gitmek zorundadır.

Müslüman matematikçi Kindi 9. yüzyılda frekans analizi tekniğini bularak sistematik biçimde şifre çözme tekniklerini ortaya çıkarmış ve bunları Risalah fi Istikhraj al-Mu'amma (Kripto Mesajların Çözülmesi Kitabı) kitabında dokümante etmiştir. Bu tarihten sonra 2. Dünya Savaşına kadar bu boyutta sistematik bir şifre çözme teknolojisi ortaya çıkarılamamıştır.

2. Dünya Savaşı ile beraber ilk bilgisayarların şifreleme ve şifre çözme amaçlı kullanılmaya başlamasıyla şifreleme teknolojilerinde gizli tutulan birçok ilerleme kaydedilmiş ve birçok şifreleme ve analiz tekniği ortaya çıkarılmıştır. Almanların "Enigma" kripto cihazı İngiliz "Bletchhley Park" kripto analizcileri tarafından kırılmış, Japonların "Purple" kripto cihazı ise Amerikalıların "SIS" (Signal Intelligence Service) tarafından kırılmıştır. Savaşı kazanan tarafın şifreleri bilindiği kadarıyla savaş zamanında kırılamamıştır, bu bağlamda şifrelemenin önemi net bir şekilde ortaya çıkmaktadır.

1945 yılında Bell Labs çalışanı Claude Shnnon'un yazdığı "A Mathematical Theory of Cryptography" (Kriptografinin Matematiksel Teorisi) modern matematiksel şifrelemenin temelidir. Bu çalışma sayesinde kriptografi alanı gerçek manada bir bilime dönüşmüş ve ölçülebilir/tariflenebilir hale getirilmiştir.

1970'li yıllara doğru bir şifreleme tekniğinin bu sayede ne kadar kuvvetli olduğu, kırılıp kırılamayacağı ya da kırılma zorluğu bilimsel olarak tariflenebilir hale gelmiştir. 1970'li yıllarda ise ilk standartlaşma çalışmaları başlamış ve önce DES, sonra da AES gibi şifreleme algoritmaları ortaya çıkarılmış ve matematiksel olarak tariflenmiştir. Aynı tarihlerde mikro elektronik teknolojinin gelişmesiyle bu algoritmalar elektronik modern kripto cihazları ile yapılabilir hale gelmiş ve günümüz kripto cihazlarına evrilmiştir.

Kripto Cihazları

Modern kripto cihazları bu bağlamda matematiksel temellere oturan, güvenlik seviyeleri ölçülebilir ve genel olarak standart algoritmalar kullanan cihazlardır.

Kripto cihazları temel olarak iki türdür:

- Veri iletiminde kullanılan kripto cihazları
- Veri saklamada kullanılan kripto cihazları

Bu yazıda daha çok veri iletiminde kullanılan kripto cihazlarına yönelik bilgiler verilecektir. Bu bağlamda veri iletiminde kullanılan kripto cihazları için temel kriterler:

1. **Veriyi güvenli transfer etmek**
2. **Veriyi güvenilir olarak transfer etmek**
3. **Veriyi düşük gecikmeyle ve hızlı transfer etmek şeklindedir.**

1-) Güvenli Transfer

Veri iletiminde güvenlik, temelde şifreleme algoritması, anahtar değişim yöntemleri ve genel sistem bilişim güvenliği ile sağlanmaktadır.

Öncelikle güvenli bir şifreleme algoritması tercih edilmelidir. Örneğin günümüz hesaplama kabiliyetleri göz önünde bulundurularak simetrik şifrelemede 100 bitten daha kısa anahtarlar kesinlikle kullanılmamalıdır. AES 128bit algoritması düşük öneme sahip verilerin güvenliğini sağlamada "kabul edilebilir" seviyede görülmekte fakat kullanımı 2024 yılından sonra önerilmemektedir. Günümüzde uzun vadeli şifreleme (~2068 yılı) için önerilen anahtar genişliğine sahip algoritma 256bit genişlikle AES 256bit'dir. Bu bağlamda matematiksel modellemesi bilinmeyen, doğrulanmamış ve bilimsel olarak sınanmamış algoritmaların kullanılması uygunsuz ve güvensizdir.

Kullanılan algoritmanın matematiksel güvenlik seviyesi önemlidir ve göz ardı edilmemelidir. Fakat algoritmadan daha önemlisi anahtar ve anahtarın güvenliğidir. Düzgün üretilmemiş zayıf anahtarlar en güvenli algoritmaları güvensiz hale getirebilmektedir. Buna ek olarak doğru transfer yöntemleriyle iletilmeyen anahtarlar saldırganlar tarafından tespit edilerek bütün sistemin güvenliği bertaraf edilebilmektedir. Bu bağlamda kullanılan kripto cihazlarının anahtar aktarım ve anahtar değişim algoritmaları büyük önem arz etmektedir.

Genel sistem bilişim güvenliği ise sektörde "tamper-resistant / kurcalamaya dayanıklı" cihazlar üretilerek sağlanmaktadır. Cihazlara yapılan fiziksel ve yazılımsal izinsiz erişimlerde anahtarların ve algoritmaların silinmesi gibi tedbirler bu bağlamda kritiktir. Cihazların bulunduğu yerden hareket ettirilmesi, cihazların delinerek veri yollarının okunması, entegre devrelerin soyularak bellekte tutulan verilerin okunması, güç tüketiminin ölçülmesiyle anahtarların ortaya çıkarılması ve elektromanyetik yayılımın tespit edilmesiyle veri elde edilmesi gibi güvenlik zafiyetleri tamper-resistant sistemler ile ortadan kaldırılmaktadır. Bu bağlamda donanımsal şifreleme sistemleri öne çıkmaktadır.

2-) Güvenilir Transfer

Verinin güvenli transferi kadar verinin transferinin güvenilirliği de önemlidir. Kritik anlarda kesintiler nedeniyle veri kaybı yaşanması, düşük SLA değerlerinin sunulması veya cihazlara saldırılar yapılarak DoS (Denial of Service / Hizmet Reddi) veri transferinin güvenilirliği aksayabilir. Genel olarak donanımsal kripto cihazları uygulamaya özel cihazlar olduğundan bu alanlarda da ön plana çıkmaktadır.

Güvenilirliğin sunulabilmesi için öncelikli gereksinim sistemin modüler ve yedekli olmasıdır. Örneğin güç modülleri (PSU) bulunan sunucular ilgili PSU'larda oluşabilecek sıkıntılarda kapanmak zorunda kalmayarak çalışmalarına devam edebilmektedir. Benzer şekilde kripto cihazlarında da PSU, şifreleme, yönetim ve benzeri birimlerin yedekli ve modüler olması 7/24 çalışma için olmazsa olmazdır.

3-) Düşük Gecikmeyle ve Hızlı Transfer

Veri iletiminde az gecikmeyle veri transferi çok yüksek hızlarda özelleşmiş donanımlarla hesaplamalar yaparak sağlanabilmektedir. Bir şifreleme döngüsü kabaca:

1. Ham veri cihaza girer.
2. Ham veri cihazda bir miktar depolanır.
3. Ham veri şifrelenir.
4. Şifreli veri cihazda bir miktar depolanır.
5. Şifreli veri cihazdan çıkarılır şekildedir ve her aşamada belirli bir zaman kaybı yaşanmaktadır.

Yazılımsal kripto sistemleri her aşamada bellek işlemleri gibi işlemler nedeniyle zaman kaybetmektedir, donanımsal sistemler ise daha verimli biçimde düşük gecikme ve yüksek hızla bu döngüleri sonlandırabilmektedir.

Bu bağlamda 1Gbps ve altı hızlarda simetrik şifreleme yazılımsal sistemlerle yapılabilirken, 10Gbps ve üstü hızlar için özel donanımsal şifreleme cihazlarının kullanılması gerekmektedir.

Kripto Cihazları İletim Ortamı Desteği

Veri iletiminde kullanılan kripto cihazlarında önem arz eden bir başka özellik ise cihazın destek verdiği iletim ortamıdır. İletim ortamı cihazın kullanılabildiği yeri ve iletim güvenliği seviyesini tanımlamaktadır.

Bu bağlamda sektörde:

- L1 (Link) kripto cihazları
- L2 (Ethernet) kripto cihazları
- L3 (IP) kripto cihazları bulunmaktadır.

L1 (Link) ve L2 (Ethernet) kripto cihazları TRANSEC (transmission security / iletim güvenliği) cihazları olarak anılırken L3 (IP) kripto cihazları COMSEC (communication security / iletişim güvenliği) cihazları olarak anılmaktadır. İletim hattı üzerinden aktarılan verinin güvenliği ise INFOSEC (information security / bilgi güvenliği) olarak ifade edilmektedir. Bilgi güvenliği ile L1, L2 ve L3 kripto cihazları doğrudan ilintili değildir.

OSİ MODELİ KATMANLARI

Uygulama Katmanı (L7)	Birimi: Veriler (Data) Görevi: Uygulama programlarının çalıştığı çerçeveyi (ağa erişmek için kullanacağı protokolleri) sağlamaktadır. Protokol: HTTP, SMTP, DNS vb.. Kullanan: Yazılımlar
Sunum Katmanı (L6)	Birimi: Veriler (Data) Görevi: En önemli görevi, gönderilen verinin alıcı tarafından anlaşılabilir halde olmasını sağlamaktadır. Protokol: JPG, SSL, SSH vb.. Kullanan: Yazılımlar
Oturum Katmanı (L5)	Birimi: Veriler (Data) Görevi: Gönderici ve alıcı arasında bir oturum kurulmasını, bu oturumun sürdürülebilmesini ve sonlandırılabilmesini sağlamaktadır. Protokol: NetBIOS, PPTP vb.. Kullanan: Yazılımlar
Taşıma Katmanı (L4)	Birimi: Bölütler (Segments) Görevi: Veriyi parçalara ayırıp segment haline getirir ve daha sonra alıcıya doğru bir şekilde iletilmesini sağlamaktadır. Protokol: TCP, UDP vb.. Kullanan: Yazılımlar
Ağ Katmanı (L3)	Birimi: Paketler (Packets) Görevi: İletilecek veri paketini bir noktadan bir noktaya taşımak amacıyla yönlendiricilerin kullanacağı bilginin eklendiği katmandır. Protokol: IP, IPSec, ARP vb.. Kullanan: Routerlar, L3 Switchler
Bağlantı Katmanı (L2)	Birimi: Çerçeveler (Frames) Görevi: Bu katmanın temel görevi verinin gönderileceği bilgisayarı tanımlaması, kablonun kullanılıp kullanılmadığının belirlenmesi ve fiziksel katmandan gelen verinin kontrol işlemlerini gerçekleştirmesidir. Protokol: Ethernet, PPP vb.. Kullanan: Switchler
Fiziksel Katman (L1)	Birimi: İkili Simgeler (Bits) Görevi: Üst katmandan iletilen sayısal verinin fiziksel iletim ortamına (elektrik radyo dalgası) taşınması ile ilgili yapıyı tanımlamaktadır. Protokol: Fiber, Coax vb.. Kullanan: Operatör

Buradaki L1, L2 ve L3 ibareleri doğrudan güvenlik seviyesi veya benzeri bir başarım kriteri göstermekten ziyade veri iletiminde desteklenen iletim altyapısı tipini tarif etmek için kullanılmaktadır. Daha detaylı olarak L1, L2 ve L3 kripto cihazlarının farklarını belirtmeden önce OSI'nin 7 katmanına kısaca bakmak gerekmektedir.

OSI 7 Katman

OSI (Open Systems Interconnection) ISO tarafından 1980'lerde standartlaştırılmış ve bilgisayarlar arası iletişimin seviyelerini katman katman ayıran bir modeldir. Bu modelde temel 7 katman bulunmakta ve her katman iletişim alt yapısına farklı bir soyutlama seviyesinden bakmaktadır.

En alttaki katman olan L1 katmanı temel olarak bitlerin iletimi ile ilgilenmektedir. İletim hattı üstünde verinin modülasyonu, kontrolü ve çözümlenmesinden sorumludur. L1 katmanında bitlerin bir anlamı yoktur, sadece taşınan bitler vardır.

L2 katmanı, L1 katmanındaki bitleri gruplu bir şekilde belirli bir hedefe göndermekten sorumlu katmandır. Bu katmandaki bu bit grupları "çerçeve" olarak adlandırılmaktadır. Çerçevelerin kendi

başlarına anlamları olabileceği gibi anlamları olmayabilir de. Bilgisayarların Ethernet kartları işletim sistemlerine bu çerçeveleri iletmekten sorumludur. İşletim sistemleri bu çerçeveleri genel olarak doğrudan yazılımlara iletmez.

L3 katmanı ise paket seviyesinde protokolleri yürütmekten sorumlu daha soyut bir yapıdır. Yazılım seviyesindeki paketler gerçekte iletim hattı üzerinden L2 çerçevelerine işletim sistemi tarafından konarak veya işletim sistemi tarafından birden fazla L2 çerçevesine bölünerek uygun olarak Ethernet kartı üzerinden aktarılmaktadır.

L1, L2 ve L3 IP Kripto Cihaz Farkları

Genel OSI modeli akılda tutularak sektörde çokça karıştırılan L1 (Link), L2 (Ethernet) ve L3 (IP) kripto cihazı farklarını örneklendirelim.

Kripto Cihazı Olmayan Durum

Veri yolumuzu aşağıdaki şekilde olduğu gibi çift yönlü bir otoban olarak düşünelim. Bu otobanda giden araçlar çeşitli çerçeveleri göstermektedir. Taşıtlar içerisindeki insanlar ise paketleri ifade etmektedir.

Herhangi bir kripto cihazı kullanılmadığı durumda ağda:

- İletilen veriler
- Kullanılan protokoller
- Paketler
- Paketlerin özellikleri
- Paketlerin hedefleri
- Çerçeveler
- Çerçevelerin özellikleri
- Çerçevelerin hedefleri açık olarak iletilmektedir. İletim hattınızı dinleyen herhangi bir saldırgan ağdaki bütün bilgiye sınırsızca erişebilir durumdadır.

L3 (IP) Kripto Cihazlı Durum

L3 (IP) kripto cihazları ile sadece belirli paketler şifrelenir. Örneğimizle ifade edersek bu durum temelde araçlar içerisindeki bazı insanların gizlenmesi anlamına gelmektedir.

Otobanda hangi araçların olduğu, kaç kişinin taşındığı, trafiğin durumu, trafiğin yönelimi ve kişilerin nerelere gittiklerini görebilirsiniz.

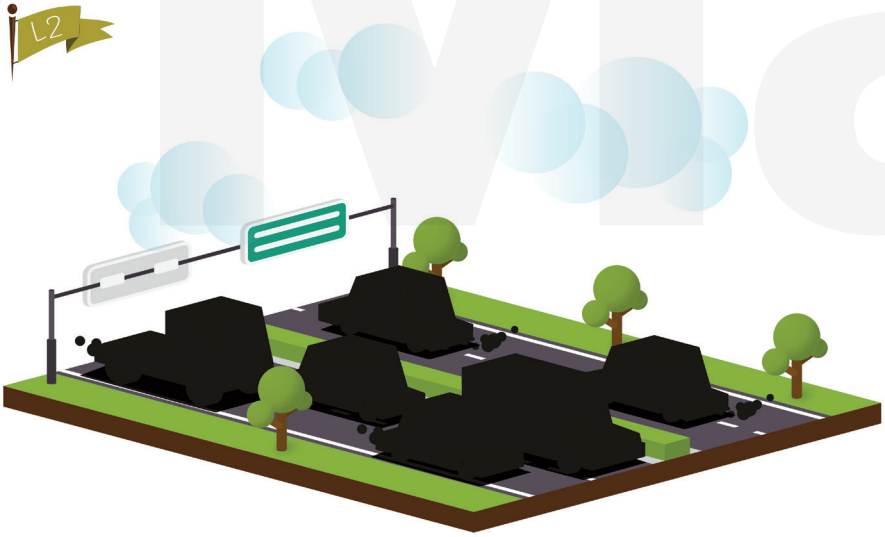
Bu bağlamda L3 (IP) kripto cihazı kullanıldığı durumda:

- İletilen veriler
- Paketler
- Paketlerin özellikleri saklanırken;
- Kullanılan protokoller
- Paketlerin hedefleri
- Çerçeveler
- Çerçevelerin özellikleri
- Çerçevelerin hedefleri açık ve erişilebilir olarak iletilir.

Açık ve erişilebilir olan bu bilgiler kurum ağları içerisinde çok büyük güvenlik zafiyetleri oluşturmazken, kurum dışı ağlara çıkıldığında ciddi bilgi sızıntılarına neden olmaktadır. Bu nedenle L3 (IP) cihazları daha çok güvenilir kurum iç ağlarında veya TRANSEC güvenliği farklı yöntemler (örneğin L2 kripto cihazları) ile sağlanmış dış ağlarda kullanılmaya uygundur.

L2 (Ethernet) Kripto Cihazlı Durum

L2 (Ethernet) kripto cihazları kullanıldığı durumda çerçeveler tamamen şifrelidir. Yani otoyolda belirli makinelerin hareket ettiğini anlayabilirsiniz fakat bu makinelerin ne olduğu, ne taşıdığı, kaç kişi taşıdığı gibi kritik bilgileri elde etmeniz mümkün değildir.



> Veri iletiminde kullanılan kripto cihazlarında önem arz eden bir başka özellik ise cihazın destek verdiği iletim ortamıdır. İletim ortamı cihazın kullanılabildiği yeri ve iletim güvenliği seviyesini tanımlamaktadır.

Bu bağlamda L2 (Ethernet) kripto cihazı kullanıldığı durumda:

- İletilen veriler
- Kullanılan protokoller
- Paketler
- Paketlerin hedefleri
- Paketlerin özellikleri
- Çerçeveler
- Çerçevelerin özellikleri saklanırken; sadece çerçevelerin hedefleri açık ve erişilebilir olarak iletilir.

Bu bilginin açık olarak iletilmesi ağ üstündeki hub/switch/router gibi cihazların çalışabilmesi için gerektiğinden açık olarak sunulmaktadır. Bu bağlamda neredeyse L1 (Link) şifreleme seviyesinde ağ üstündeki bilgiyi gizlemektedir.

L2 (Ethernet) kripto cihazlarının genel olarak L1 (Link) kripto cihazlar yerine tercih edilmesinin nedeni L2 (Ethernet) kripto cihazlarının ağlarda kullanımı mümkünken, L1 cihazların sadece noktadan noktaya özel kablolu uygulamalarında kullanılabilir olmasıdır.

Bu bağlamda L2 (Ethernet) cihazları kurumların iç ve dış ağların işlevselliğini etkilemeden TRANSEC seviyesinde iletim güvenliğine sahip olmalarını sağlamaktadır.

L1 (Link) Kripto Cihazlı Durum

L1 (Link) şifreleme cihazları yolu tamamen şifreler. Trafik olup olmadığı görülemez. Kaç kişi taşındığı, kaç taşıt bulunduğu ve benzeri bütün bilgiler tamamen gizlenmektedir.

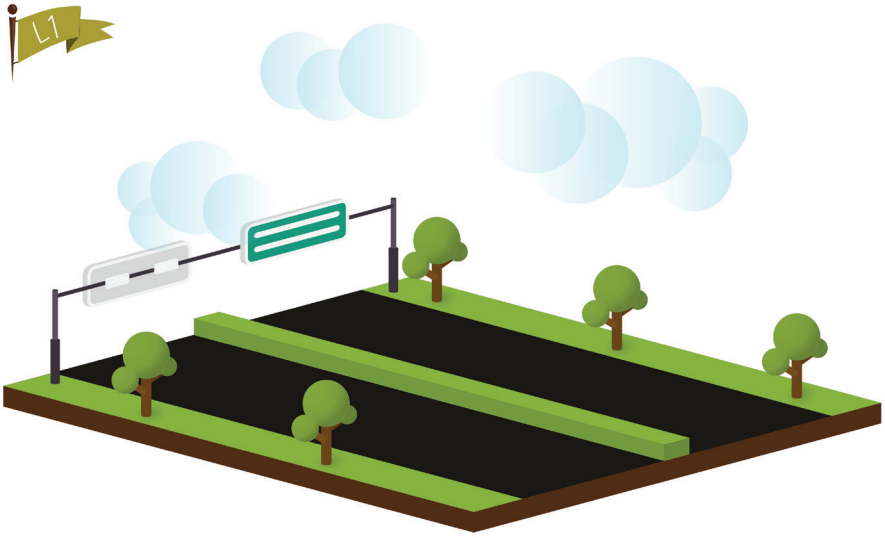
Bu bağlamda en çok bilgi saklaması L1 (Link) şifreleme cihazları ile sağlanırken en büyük dezavantajı sadece noktadan noktaya özel hatta sahip uygulamalarda kullanmaya uygun olması ve çalıştığı hat üstünde başka bir network cihazının bulunmasına izin vermemesidir.

Kindi Kripto Cihazları

Rovenma olarak Kindi markası altında ülkemizde tamamen yerli ve milli olarak geliştirdiğimiz, yazılımlarından entegre devre tasarımlarına kadar bünyemizde tasarlanan teknolojilerimizle:

- Link Crypto (L1)
- Ethernet Crypto (L2)
- IP Crypto (L3)

ürünlerimiz ile her 3 katmanda ürünler sunmaktayız.

Ürünlerimiz 10Gbps ve üstü hızlarda, 2uS'den düşük gecikmelerle çalışmakta ve tamamen modüler/yedekli yapıdadır.

> Modern kripto cihazları bu bağlamda matematiksel temellere oturan, güvenlik seviyeleri ölçülebilir ve genel olarak standart algoritmalar kullanan cihazlardır.