Rovenma CTO'su Şadi Çağatay Öztürk

Rovenma'dan, Yüksek Hızlı ve Donanım Tabanlı Kripto Çözümü: Kindi Ethernet Crypto

Elektronik alanında inovatif çözümler sunan Rovenma, Mayıs ayında düzenlenen IDEF 2019 fuarında ilk kez sergilediği donanım tabanlı kripto cihazı Kindi Ethernet Crypto ile savunma sektörüne de giriş yaptı. Cumhurbaşkanlığı tarafından 6 Temmuz'da yayınlanan Bilgi ve İletişim Güvenliği Tedbirleri konulu genelgenin, kamu kurumları için milli kripto çözümlerinin kullanımını zorunlu kılması, bu tip donanımların gündemin üst sıralarına taşınmasında da etkili oldu. Bu gelişme ile birlikte, Kindi Ethernet Crypto'ya yönelik faaliyetlerine ağırlık veren Rovenma'nın kripto sistemleri alanındaki çalışmalarını, Rovenma CTO'su Şadi Çağatay Öztürk'ten dinledik.

Şebnem ASİL / s.asil@savunmahaber.com
Alper ÇALIK / a.calik@savunmahaber.com

MSI Dergisi: Şadi Bey, öncelikle benzeri çözümler arasında hangi özellikleri ile öne çıktığına da değinerek bize Kindi Ethernet Crypto'yu anlatır mısınız?

Şadi Çağatay ÖZTÜRK: Kindi Ethernet Crypto, Türkiye'de geliştirilen; L2 seviyesinde kriptolama yapabilen, yüksek hızlı ve donanım tabanlı olarak çalışan çok az sayıdaki kripto çözümünden biri. Kindi Ethernet Crypto için mevcut durumda "EAL 4+ Sertifikasyonu" süreçleri devam ediyor. Böylelikle Kindi Ethernet Crypto, az önce saydıklarıma ilave olarak, uluslararası sertifikasyona sahip, tek yerli kripto çözümü olacak. Öncelikle en çok öne çıkan özellikleri bunlar. Bunun haricinde ürünümüz, tasarladığımız sayısal devreler sayesinde, veriyi kriptolama görevini 32 Gbps gibi çok yüksek hızlarda gerçekleştirebiliyor. Rakibimiz sayılabilecek ürünlerin ulaşabildiği azami hızlar ise 8-9 Gbps seviyelerinde.

Ayrıca Kindi Ethernet Crypto, şeffaf ve açık bir tasarıma sahip. Yani tasarımı ile ilgili gizli bir şey yok. Bu yaklaşım zaten, kripto alanındaki en önemli uluslararası standartlardan birisi olan EAL Sertifikasyonu'nu alabilmek için de ön şart. Çünkü bu sertifikayı alabilmek için, ürününüzün kripto algoritmasının açık olması; ürününüzde herhangi bir arka kapının bulunmadığının kanıtlanabilmesi ve tüm bunların, kullanıcı tarafından test edilerek doğrulanabilmesi gerekiyor. Sonuçta algoritmanız güvenliyse ve kripto analize dayanıklıysa sadece anahtarlarınızı koruyarak sisteminizin güvenliğini sağlayabiliyorsunuz. Bu, tüm dünyada kabul gören bir yöntem. Bununla birlikte, pazarda algoritması gizli olan çeşitli kripto çözümleri mevcut. Bunun ilk başta çok güvenli

bir yaklaşım olduğu düşünülebilir. Ancak, algoritmanın çalışma prensibi kadar, aslında zafiyetleri de gizli. Dolayısıyla ne zaman kırılabileceği belli değil. Kötü niyetli kişilerin bu algoritmaları çözebilecek bir yöntem geliştirmeleri durumunda, kullanıcının tüm veri akışı, uzun bir süre kimsenin haberi bile olmadan izlenebilir. Bu cihazları kullanan kurumlar farkına bile varmadan, yıllarca verileri çalınabilir. Biz de bu nedenle Kindi ürünümüzde, kripto analize karşı dayanıklı olduğu dünyaca kabul edilen AES algoritmasını ve ilintili teknikleri kullanıyoruz. Bu alandaki uzman ve akademisyenler, bilgisayar teknolojilerindeki gelişim mevcut trendi ile devam ettiği takdirde, 256 bit anahtar kullanan bir AES algoritmasının, ancak 2063 yılında geliştirilecek bilgisayarların sahip olacağı işlem güçleri ile kırılabileceğini hesaplıyorlar. Hatta AES, kuantum dayanıklı ya da post-quantum bir algoritma olduğu için, geliştirilecek ilk kuantum bilgisayarlar tarafından dahi kırılamayacak.
Kindi Ethernet Crypto'nun bir özelliği de sabit bir anahtarla da uzun süreler boyunca güvenli şekilde kullanılabilmesi. Cihaz, CTR/GCM Modu olarak adlandırılan bu modda çalıştığında, iletimini yapacağı verileri şifrelemenin yanı sıra verilerin sırasını da sürekli değiştirerek, kripto analiz ile çözülmesini neredeyse imkânsız hâle getirebiliyor. CTR/GCM Modu sayesinde Kindi, tek bir anahtarla bile uzun süre emniyetli şekilde kullanılabiliyor. Dilenirse tabii ki anahtarlar periyodik olarak kullanıcı tarafından veya otomatik olarak değiştirilebiliyor da.

Anahtarlar için Fiziksel Erişim Şart

MSI Dergisi: Kindi Ethernet Crypto'nun donanım tabanlı olmasının avantajları neler?

Şadi Çağatay ÖZTÜRK: Aslında donanım tabanlı olmasının pek çok avantajı var; ancak en önemlisi güvenlik. Yazılım bazlı kripto sistemlerinde, kötü niyetli kişiler sisteme bir kez erişmeyi başarırlarsa sistemdeki tüm anahtarları çalabilirler. Anahtarlarınızın çalınması ise algoritmanız ne kadar güçlü olursa olsun işlevini yitirmesi demek. Ayrıca benzer şekilde, yazılım

© Rovenma

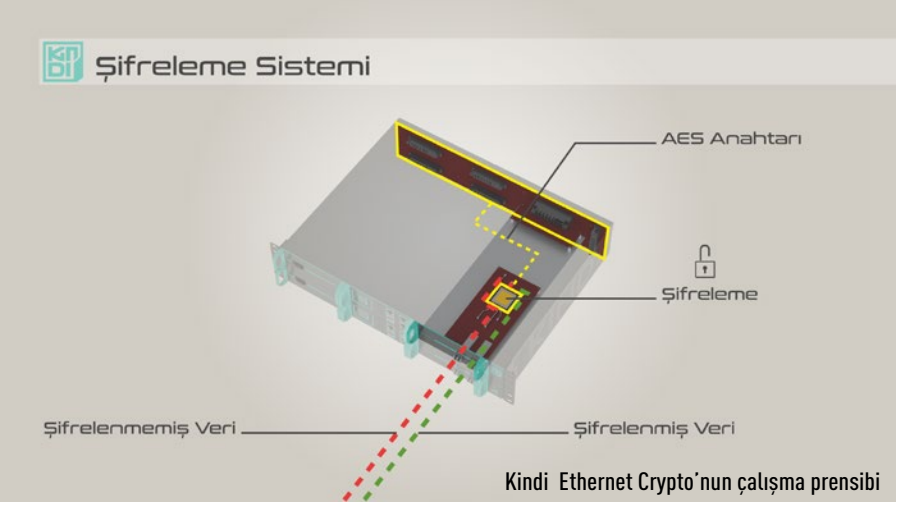
Kindi Ethernet Crypto

tabanlı çözümlerde anahtarlarınızın çalındığını fark etmeniz de çok güç. Bu ise başlı başına bir tehdit. Üstelik bu tip durumlar ağdaki bilinçsiz kullanıcılardan da kaynaklanabilir. Örneğin, zararlı yazılımlar taşıdığı bilinmeyen bir USB bellek, ağ cihazlarından herhangi birine takıldığında, ağ içerisindeki anahtarlara erişip, bunlara ilişkin verilerin, kriptolanmamış şekilde dışarı aktarılmasını sağlayabilir. Bununla birlikte donanım bazlı sistemler insan hatasına yer vermediğinden ya da bunu en aza indirgediğinden daha güvenli.
Kindi Ethernet Crypto'nun donanım tabanlı olmasının bir başka avantajı ise anahtarları ele geçirmek isteyen kişilere karşı da sistemin kendisini, yaklaşık 40 farklı yöntemle kademeli olarak koruyabilmesi. Bunların bazılarından bahsetmek gerekirse öncelikle kötü niyetli kişilerin cihaza fiziksel olarak erişmeleri gerekiyor ki; güvenli tesisler söz konusu olduğunda, sadece bu bile oldukça zor bir şey. Diyelim ki kişi, cihazın bulunduğu sunucu dolabına erişti. Gerekli prosedürleri izleyerek cihazı bakım moduna almadan dolap kapağını açtığı anda, Kindi Ethernet Crypto, üzerindeki tüm anahtarları siliyor. Bunu da bir şekilde aştı diyelim, anahtarlara erişebilmek için cihazı dolaptan çıkarması lazım. Cihaz, titreşimde, nemde veya sıcaklıkta bir fark hissedince de anahtarları siliyor. Diyelim ki bunu da aştı ve cihazı dolaptan çıkardı, cihazın kapaklarını sökmesi gerekiyor, bu durumda anahtarlar yine siliniyor. Tüm bunların da bir şekilde aşıldığını varsayalım. Artık cihazın kapakları da açıldı ve kişi modüllere erişti. Bu durumda da Kindi Ethernet Crypto, bileşenlerindeki elektrik akımında meydana gelen anormallikleri algılayarak anahtarları siliyor. Bunun üstüne de birçok mekanik, elektronik ve yazılım önlemimiz var, bunların da tek tek aşılması lazım. Kısacası cihazdaki anahtarları ele geçirmek isteyen birinin, ortaya sınırsız kaynak koyması gerekiyor.

Saniyede 32 Gibabit Veri Şifreliyor

MSI Dergisi: Kindi Ethernet Crypto'nun muadillerine göre daha hızlı çalıştığını söylediniz. Bu özelliği biraz daha detaylı anlatabilir misiniz?

Şadi Çağatay ÖZTÜRK: Kindi Ethernet Crypto'nun üzerinde tasarımını şirketimizin yaptığı ve paralel hesaplamaya yarayan sayısal devreler var. Bu nedenle ürünümüzün iletişimde yarattığı



© Rovenma

Kindi Ethernet Crypto'nun çalışma prensibi

gecikme 1 mikrosaniyeden daha düşük seviyelerde. Yazılım tabanlı kripto sistemlerinin ise en hızlısı, üzerinde bulunduğu donanıma da bağlı olarak, 2-3 milisaniye civarında bir gecikme ile veri gönderiyor. Bu da çok hızlı iletişim kurması gereken, örneğin hava savunma komuta kontrol sistemleri için kabul edilemez bir gecikme süresi. Sivil sektör açısından bakıldığında ise alım satım emirlerinin anlık olarak verildiği finans sektöründe, geç iletilecek emirlerden dolayı, maddi kayıplar yaşanabiliyor. Ya da mobil iletişim alanındaki uygulamalarda, kullanıcının ses iletimindeki gecikmeyi hissetmesi demek. Milisaniye mertebesindeki gecikmeler küçük görünse bile milyarlarca sorgunun aktığı sistemler üstünde toplamda ciddi gecikmelere ve performans düşüşlerine sebep olabiliyor.

Özgün Tasarım

MSI Dergisi: Kindi Ethernet Crypto'yu, hazır bileşenler kullanarak mı geliştirdiniz?

Şadi Çağatay ÖZTÜRK: Ürünümüzde yer alan temel elektronik komponentlerin haricindeki her şeyi kendimiz ürettik. Bu süreçte de ürünün tüm yazılım ve donanım tasarımını biz gerçekleştirdik. Bu nedenle kullanıcıların, Kindi Ethernet Crypto'ya farklı yetenekler kazandırılması konusundaki taleplerine çok hızlı cevap verebilecek konumdayız. Hatta kullanıcı istekleri doğrultusunda, Kindi Ethernet Crypto'ya farklı şifreleme algoritmaları bile yükleyebiliyoruz.

MSI Dergisi: Cumhurbaşkanlığının, 6 Temmuz'da yayınladığı, Bilgi ve İletişim Güvenliği Tedbirleri konulu genelge ile ilgili neler söylemek istersiniz?

Şadi Çağatay ÖZTÜRK: Bu genelge, kamu kurumları için uluslararası standartlardaki yerli ve milli kripto çözümlerinin kullanımını zorunlu hale getiriyor. Bütün devlet kurumları ile özel işletmelere yol gösterir nitelikte tehditlerden ve alınması gereken önlemlerden bahsediyor. Burada, "uluslararası standartlardaki" ifadesi bizim için çok önemli; çünkü bilimsel yaklaşım ile doğrudan uyumlu. Mevcut durumda pazardaki pek çok çözüm, nasıl çalıştığı belli olmayan gizli algoritmalar kullanmakta ve bu nedenlerden ötürü uluslararası sertifikasyonlara girememekte. Biz yaklaşık 1 yıl kadar önce, Kindi için EAL Sertifikası almak üzere başvurularımızı yaptık ve sürecimiz pürüzsüz şekilde ilerliyor. Tahminen 4 ay içerisinde de EAL 4+ sertifikamızı almış olacağız. Bu nedenle genelge çerçevesinde oldukça umutluyuz, şimdiden bize bu yönde talepler gelmeye başladı bile.

© MSI Dergisi

Rovenma CTO'su Şadi Çağatay Öztürk, MSI Dergisi İş Geliştirme Koordinatörü Şebnem Asil ve Rovenma Genel Müdürü Fatih Mutlu

Siparişler Kapıda

MSI Dergisi: Kindi Ethernet Crypto için şu ana kadar bir sipariş aldınız mı?

Şadi Çağatay ÖZTÜRK: Yurt içindeki potansiyel kullanıcılara ürünümüzü tanıttık; birçoğunun da ilgisini çekmeyi başardık ve detaylı görüşmelerimizi sürdürüyoruz. Takdir edersiniz ki bu tarz projeler kapsamlı projeler, o nedenle süreçler devam ediyor. Türkiye'de bu alanda EAL4+ sertifikasyonu dahil çeşitli standartlara uygunluk sağlayan ilk ürünle piyasada olduğumuz için satış konusunda kendimize güvenimiz tam. Bu nedenle seri üretim çalışmalarımıza başladık ve cihazlarımızı siparişler için hazır etmeye son hızla devam ediyoruz. Ayrıca Kindi Ethernet Crypto, gerçekten çok başarılı bir ürün olduğu için, ihracat potansiyeli de çok yüksek. Biz de daha en baştan hedefimizi bu şekilde belirledik ve ürünün sertifikasyonuna yönelik tüm bilgi ve belgeleri İngilizce olarak hazırladık. Türk Cumhuriyetlerinden bazıları ve çeşitli Orta Doğu ülkeleri ile zaten görüşme halindeyiz. Yurt içindeki ilk satışlarımızın hemen

Her İhtiyaca Bir Kindi

Kindi ürün ailesi, farklı noktalar arasında, kriptolu ve güvenli iletişim kurulabilmesine imkân tanıyan donanım tabanlı çözümlerden oluşuyor. Bu ürünler, bir kurum veya kuruluşun mevcut bilişim alt yapısına, Ethernet gibi evrensel arayüzler vasıtasıyla kolaylıkla bağlanarak kullanılabiliyor ve bu ağın belirli noktaları arasındaki veriyi, matematiksel bir yöntem kullanarak şifreliyor. İletişim, örneğin iki nokta arasında yapılacaksa her iki noktada da bu cihazlardan bulunuyor. Bir cihaz veriyi şifreleyerek gönderiyor; karşı taraftaki benzer cihaz ise şifreli veriyi normal hâle getiriyor.Kindi ürün ailesi ve işlevleri ise kısaca şöyle:

- **Kindi Line Crypto:** Bir noktadan bir noktaya güvenli iletişim için kullanılıyor. Veri merkezi ve kabiniçi ağlar, SSL / TLS'nin sunuculardan boşaltılmasını mümkün kılmak için Kindi Line Crypto ile de güvence altına alınır.
- **Kindi Ethernet Crypto:** Noktadan noktaya, noktadan çoklu noktaya gibi birçok nokta arasında 10 Gbps'e kadar olan hızlarda veri şifreleme / şifre çözme ve aktarma sağlanır.
- **Kindi IP Crypto:** İnternet Protokolü (IP) üzerinden yapılacak iletişimlerde, sadece istenilen veri paketlerini şifreler.
- **Kindi Diode Crypto:** Güvenlik kameraları gibi tek yönlü olarak iletişim sağlayan sistemlerde kullanılıyor.

ardından da ihracat çalışmalarımızı hızlandıracağız.

Kullanıcılar Arasında Savunma Sanayisi de Olabilir

MSI Dergisi: Ürünün potansiyel kullanıcıları arasında kimler yer alıyor?

Şadi Çağatay ÖZTÜRK: Kamu kurumlarının bu tip ürünleri kullanımı, zaten yayınlanan genelge ile bir anlamda zorunlu hâle geldi. Bunun haricinde, farklı konumlardaki tesisleri arasında güvenli iletişim tesis etmesi gereken herkesin, bu tip bir ürün kullanması gerekiyor. Bunlar arasında da savunma sanayi firmalarının yanı sıra finans, bankacılık, telekomünikasyon, sağlık ve iletişim sektöründe faaliyet gösteren kurum ve kuruluşlar yer alıyor. Bu sektörlerden talepler almaya başladık, görüşmelerimiz devam ediyor.

Askeri Gemilerden İHA'lara

MSI Dergisi: Kindi Ethernet Crypto'nun türevlerinin, savunma ve havacılık sanayisi açısından farklı uygulamaları da olabilir mi peki?

Şadi Çağatay ÖZTÜRK: Aslında Kindi, savaş gemisi gibi büyük platformlarda doğrudan kullanılabilir. Bu gemilerin, kurdukları her türlü iletişimi kriptolu hâle getirebilir. Bunun için tek yapılması gereken de aslında, geminin ana sunucuları ile iletişim cihazlarının arasına Kindi Ethernet Crypto'nun entegre edilmesi. Bu iletişim cihazları, telsizler de olabilir, uydu alıcı vericileri de. Benzer şekilde, Kindi Ethernet Crypto'nun daha küçük boyutlu versiyonları da örneğin İHA'ların kriptolu iletişimi için kullanılabilir.

© Rovenma

Kindi Ethernet Crypto, testler sırasında görülüyor.

MSI Dergisi: Nispeten genç bir firma olan Rovenma, nasıl böyle bir ürün geliştirmeyi başardı?

Şadi Çağatay ÖZTÜRK: Rovenma, belirttiğiniz gibi nispeten genç bir firma; ancak kurucu ortaklarımız ve çalışanlarımız; elektronik, yazılım, siber güvenlik ve mekanik imalat gibi sektörlerde, uzun yıllar tecrübe edinmiş insanlar. Ayrıca, Rovenma kurulduğu daha ilk günden itibaren, kurumsal bir firma olarak yola çıktı. Bu nedenle sahip olduğumuz kurumsal hafızanın, bizden birkaç kat daha büyük ve 10'larca yıl daha yaşlı firmalardan iyi olduğunu iddia edebilirim.

MSI Dergisi: Kindi Ethernet Crypto'yu gelecekte neler bekliyor?

Şadi Çağatay ÖZTÜRK: Günümüzde teknoloji, çok hızlı şekilde gelişiyor ve ilerliyor. Bu alanda ise kendinizi geliştirmeniz, tercih meselesinden ziyade bir zorunluluk. Kindi ürün ailesinin yeni sürümlerini geliştirmeye yönelik çalışmalara şimdiden başladık. İlk ürünümüz için sertifika alır almaz da yeni sürümleri için sertifika süreçlerini başlatacağız. EAL 4+ Sertifikası'nın bir avantajı da daha önceden sertifika almış bir ürün üzerinden geliştirilen yeni sürümlerde, sertifikasyon süreçlerinin daha kısa sürüyor olması. Bu nedenle Kindi Ethernet Crypto'nun yeni sürümlerinde, bu süreçlerin 1,5 yıl değil de 3-4 ay kadar süreceğini tahmin ediyoruz. Böylece, sektöre, sürekli daha gelişmiş ve sertifikasyona sahip ürünler sunabileceğiz.

Rovenma CTO'su Şadi Çağatay Öztürk'e, zaman ayırıp sorularımızı cevaplandırdığı ve verdiği bilgiler için, okuyucularımız adına teşekkür ediyoruz.

Rovenma Hakkında

Elektronik alanında inovatif çözümler sunan Rovenma, 2016 yılında Ankara'da kuruldu. Firma, 90 kişilik bir ekip ile 4.000 metrekarelik iki ayrı tesiste faaliyet gösteriyor. Rovenma'nın güvenlik güçlerine yönelik ürünleri arasında, Akıllı Mühimmat Takip Otomatı bulunuyor. Bu otomat, ilgili personelin kedisine verilen bir şifre ile sadece kendi yetkisine tanımlı silah, tabanca, şarjör, mühimmat ve fünye gibi hassas ekipmanlarını, emniyetli şekilde saklayabilmesini ve gerektiğinde bu ekipmana hızlıca erişebilmesini sağlıyor. Bu ürünün bir benzeri olan ve Rovenma'nın PTT için 400 adet ürettiği KARGOMAT cihazları ise hâlihazırda 5 farklı ilde kullanılıyor.