# Hack'lenemeyen Cihazlar

80'li yıllarda tanıştığımız Görevimiz Tehlike dizisinin tutkunları şu sahneyi hemen hatırlayacaktır: Takım lideri Jim'e o yılların yeni teknoloji harikası CD ile yeni bir görev bildirimi yapıldıktan sonra dijital bir ses "Bu disk beş saniye içinde kendi kendini yok edecektir" uyarısını yapar ve beş saniye sonra disk arkasında dumanlar bıraka bıraka yok olur.

Geçenlerde Alman mühendisler tam da bu klasik sahneyi anımsatacak bir buluşa imza attılar. Mühendisler son derece güvenli yeni bir dijital zarf üretmeyi başardılar, öyle ki bu zarf içindeki veriye sızma ihtimali olduğunda veriyi yok ederek hack'lenmesini imkânsızlaştırıyor. Fraunhofer Uygulamalı ve Entegre Güvenlik Enstitüsü'nden (AISEC) Vincent Immler, Johannes Obermaier ve Jan Koenig'in de dahil olduğu ekip bu üstün güvenlikli veri saklama zarflarını Washington'da gerçekleşen Donanım Odaklı Güvenlik ve Güven Sempozyumu (IEEE-HOST)'nda tanıttı[1].

Bu cihazda modern kripto cihazlarında olduğu gibi şifreli anahtarlar depolanıyor ya da açılabiliyor, tek fark burada casus filmlerinde görülebilen o x-ışınları, milimetrik matkaplarla delme, elektromanyetik yöntemlerle hack'lemek gibi denemeler işe yaramıyor.

Donanım güvenlik modülü (HSM) olarak adlandırılan bu aygıt, içerisinde mikrometre boyutunda kablolarla döşeli gücü pilinden alan özel bir katman tarafından korunuyor. İçindeki şifreli veri, cihazın değişken hafızasında saklanıyor. Cihazın bu değişken hafızası üzerinde kırabilmek için 1 dakika bile uğraşılsa kendini hemen siliyor. Cihaz dışarıdan da koruma kaplaması ile güvenliği artırılmış fiziksel bir formda geliyor. Örneğin milimetrik matkaplarla en ufak delik açmak bile içeride kısa devreye sebep olurken elektromanyetik müdahaleler de sistem tarafından anında tespit ediliyor.

**Müdahale Anında Veri Yok Oluyor**

Daha önce birileri HSM'lerden birine sızabildi mi veya sistem hacklendi mi bunu bilmek güç çünkü böyle bir şey olduysa da firma muhtemelen bundan bahsetmek istemeyecektir. Fakat, Almanya Münih'ten üç mühendis, HSM'lerin daha iyilerini yapabileceklerini söylüyor. Bu geliştiriciler, mevcut sistemdeki pillere ve hafızaya mecbur olan düzenin potansiyel bazı problemler doğurduğunu düşünüyor.

AISEC Direktörü ve Münih Teknik Üniversitesi Bilgi Teknolojileri Güvenlik Başkanı Georg Sigl'e göre direnç değiştiren bir müdahale, cihazdaki gizli veriyi anında yok ediyor. Ancak HSM'nin bataryası

1 https://spectrum.ieee.org/tech-talk/computing/hardware/the-unhackable-envelope

burada kritik rol oynuyor. Eğer batarya biterse; geçmiş olsun. İçeride ne varsa yok oldu diyebiliriz. Bu durumda sistemin bilgileri saklama ömrü pilin ömrüyle kısıtlı olmuş oluyor. Bataryaya bu hayati bağlılık, sistemin çalışabileceği ortamları sınırlıyor. Pilin şarj olması için de güvenli bir bilgisayar merkezine gidilmeli. Cihazın merkeze yolculuğu esnasında çok soğuğa maruz kalırsa batarya ölebilir ya da içeride devreler istenmeyen bir işlem yapabilir. Böyle bir işlem olursa sistem şifreli anahtarları yok edebilir ki bunlar HSM'nin içine gömülü anahtarlardır ve silinirlerse geri dönüşü olmayan yola da girilmiş demektir. AISEC'in Fiziksel Güvenlik Başkanı Matthias Hiller'e göre, kararlı bir ortam arayışı bu cihazın kolayca transfer edilebilmesini zorlaştırıyor, mesela hareket halindeki araçlarda ya da insanın üzerinde taşınamıyor.

**Sistem Kapanınca Çalınabilecek Veri Olmuyor**

Bu sorunlara çözüm olarak B-Trepid ismi verilen bir katman geliştirildi. Burada B-Trepid, sistemin oluşturduğu şifreli anahtar ile zarfın kendi yapısının bizzat oluşturduğu şifreli anahtarı değiştiriyor. Artık zarfın ürettiği dirençler ile (batarya kullanarak) yaratılan şifre yerine B-Trepid, zarfın dıştan içe katmanları arasındaki direnç farklarını hesaplayarak ortaya yeni bir şifreli anahtar çıkarıyor. Bu femtofarad dirençler zarftan zarfa (incecik katmanlar olarak düşünülebilir) aktarılırken tahmin edilemez yollar kullanıyor ve her zarfın kopyası olmayan benzersiz bir imzası olmuş oluyor. Pratikte nasıl oluşturulduğu belirsiz olan bu imza klonlanamaz hale gelip bir kriptografik anahtar formunu alıyor.

B-Trepid bir bilgisayar ağına bağlanıp açıldığında sistem içinde görülebilir ne kadar veri varsa hepsini korumak için bu klonlanamayan anahtar şifreden oluşturuyor. Sistem kapalı olduğunda ise bir anahtar oluşturmuyor, dolayısıyla çalınabilecek bir veri de olmuyor. Böylece sistem sonraki ağ bağlantısı yapılana kadar kapalı kaldığı sürece hiç batarya harcamamış oluyor. Fiziksel bir müdahale yapıldığında ise (Sigl'in ekibi 0.3 mm'lik bir matkapla iç devrelere ulaşmak için cihazı delmeye çalıştı) dirençler ve kapasiteler anında değişiyor. Bu değişim ise içerideki herhangi bir veriyi otomatik olarak okunamaz hale getiriyor. Sigl şu an bu hack'lenemez veri saklama kutularının prototiplerini ürettiklerini ve konseptin düzgün çalıştığını söylüyor. Sırada zarfın seri üretimine geçmek ve bilişim sistemlerine entegrasyonunu sağlamak için geliştirmeye devam etmek var. Yakında daha zor kırılabilen, daha karmaşık devrelerin ve mühendisliklerin koruduğu güvenlik sistemlerine sahip olmamız mümkün görünüyor.

**Rübik Küp Gibi Çözülmesi Güç Bilgisayar**

Aslında hack'lenemeyen cihazlar fikri yeni değil. Pek çok alandan uzmanlar benzer cihazlar geliştirebilmek için uzun zamandır çalışmalar yapıyor. The Defense Advanced Research Projects Agency'nin (DARPA) 3.6 milyon dolarlık hibesi sayesinde Michigan Üniversitesi araştırmacıları, hack'lenmesi zor bir bilgisayar üzerinde çalışıyor örneğin[2]. 2018'in bahar aylarında DARPA, Sistem Güvenliği Entegre Donanım ve Yazılım (SSITH) programını duyurdu. Adından da anlaşılacağı gibi, programın misyonu, donanım düzeyinde uygulanan siber güvenlik çözümleri yaratmak. Michigan Üniversitesi'nin MORPHEUS projesi adındaki güçlendirilmiş bu bilgisayarı da, SSITH programında hibe almış dokuz fikirden biri.

Üniversite ekibi, bilgileri hızlı ve rastgele hareket ettirebilen ve imha edebilen bir bilgisayar yaratmayı planlıyor. Bu yöntem, hacker'lardan hayati verileri gizleyebilir ve siber saldırılarının başarısını azaltabilir.

ECNMag'de yer alan makalede, MORPHEUS Projesi lideri, Michigan Üniversitesi Bilgisayar Bilimi ve Mühendisliği Profesörü Todd Austin, "Bilgisayarı çözülemeyen bir bulmaca gibi tasarlıyoruz. Bir rübik

2 https://www.ecnmag.com/blog/2017/12/unhackable-computer-currently-under-development

küp çözmeye çalıştığınızı düşünün, gözünüzü her kırptığınızda tekrar karıştırıyoruz" diyor ve ekliyor: "Projeyle ilgili asıl heyecan verici olan şey, yarın karşılaşabileceğimiz zayıf, hassas noktaları şimdiden düzeltebilmesi."

**Apple, Hack'lenemeyen Telefon Üzerinde Çalışıyor**

Hack'lenemeyen cihaz üretimiyle ilgilenen bir başka kurum da Apple. Apple'a yakın bazı kaynaklar, 2016'da kendilerinin bile bilgilere ulaşamayacakları bir telefon üretmeyi hedeflediklerini açıklamıştı[3]. FBI, San Bernardino saldırganlarından Syed Farook'a ait olan iPhone'un bilgilerine ulaşmak için Apple'dan yardım istemiş, şirket ise bu talebi yerine getirmeyeceğini açıklamıştı. Bunun üzerine FBI, Apple'ın güvenlik önlemlerini geçmek için mahkeme emri çıkartmış, Apple ise bunun diğer müşterilerinin gizliliğini tehlikeye atacağı için emri uygulamayacağını açıklamıştı. *New York Times*'da yer alan habere göre ise Apple bugünlerde ülkede bazı güçleri karşısına alsa da iPhone'u hack'lenemeyecek bir forma getirmek için uğraşıyor. Firma bunun için hem yazılımsal hem donanımsal bir geliştirme içinde.

**Siber Güvenlik Şirketi Suçlularla İşbirliği Yaptı**

Bu arada Ekim 2017'de Kanada'da ilginç bir gelişme yaşandı. Siber güvenlik şirketi Phantom Secure'un CEO'su olan Vincent Ramos, suçlulara uyuşturucu kaçakçılarına hack'lenemeyen Blackberry telefonlar sattığı iddiasıyla gözaltına alındı[4]. Güvenlik seviyesi, fabrika çıkışlı bir Blackberry'den daha üst düzey olan bu akıllı telefonlar, suç örgütlerince güvenlik güçlerinin radarına girmeden işlerini yürütmek için kullanılıyor.

**Bitcoin İçin Hack'lenemeyen Telefon**

Öte yandan Dünya Mobil Cihazlar Konferansı 2018'de SIKURPhone markalı bir Android cihaz ilk "hacklenemeyen akıllı telefon" iddiasıyla tanıtıldı. Cihazı üreten firma SIKUR'un açıklamasına göre 800 dolara satılacak bu cihaz özellikle Bitcoin ve diğer kripto paralar için hack'lenemeyen cüzdanlar kullanacak[5]. Bitcoin ticaretinde henüz hiçbir akıllı cihazın iddia edemediği tamamen güvenli olma iddiasını taşıyan cihaz kripto borsalarında işlem yapanlar için fiyatı ile iPhone X'in rakibi olabileceğini gösteriyor.

**Temassız ATM, Hırsızlıkların Önüne Geçecek**

Güvenlik ve hızlı destek şüphesiz banka ATM'leri için en önemli kriterlerden. Bugün elektriğe erişimi olan hemen her yerleşim noktasında insanların en yoğun kullandığı ve aslında birer akıllı makine olan ATM'ler çeşitli güvenlik tehditleriyle mücadele ediyor. Kullanıcılarının varlıklarını korumak için PIN (şifre), biyometrik tarama gibi çeşitli önlemleri olan ATM'lerde en büyük güvenlik açığı kart kopyalanmasına çare bulamaması. En azından bazı ATM'lerde bu güvenlik açığı yüzünden yüzlerce müşterinin kredi kartları ATM'ye takıldığı an içindeki bilgiler ve şifreler başka bir karta dijital olarak kopyalanabiliyor. Bu soruna çözüm olarak biyometrik veri ve mobil cihaz birleşiminden doğacak yeni bir onay sistemi öne sürülüyor. Güvenlik şirketi Veridium'un internet sitesindeki habere göre, artık bankalar akıllı telefonumuzun bir QR kodu okuması ile çalışan, ATM'ye dokunmadan yüzümüzü tanıyacak sensörler ile güçlendirilmiş bir sistem ile para alışverişine imkân verecek[6]. ATM ekranında bir defaya mahsus görüntülenecek ve ekranda 10 saniye kalacak özel QR kodu, cep telefonumuzun kamerası tanıyacak ve sisteme giriş izni alabileceğiz. Ardından yine ATM'ye dokunmadan bankacılık işlemini mobil uygulama üzerinden gerçekleştirmek mümkün olacak. Bu sistemde kart olmadığı

3 https://www.techradar.com/news/phone-and-communications/mobile-phones/apple-is-reportedly-working-on-an-unhackable-iphone-1315728
4 https://www.theepochtimes.com/canadian-ceo-charged-with-conspiring-to-sell-unhackable-phones-to-criminals_2468716.html
5 http://www.trustedreviews.com/news/bitcoin-wallet-security-cryptocurrency-wallet-hacking-launch-mobile-world-congress-sikurphone-3406983
6 https://www.veridiumid.com/blog/creating-an-unhackable-atm/

için kopyalanacak bir şey de olmayacak ve en azından en yaygın ATM hack'leme yöntemi olan kart üzerinden dijital bilgi hırsızlığının önüne geçilmiş olunacak.

**Kuantum Cihazlar Daha Güvenli Bağlanacak**

*Physical Review Letters*'da yayımlanan bir makalede, bilim insanları, üç ya da daha fazla kuantum cihazın güvenli bir şekilde iletişim kurmalarının yeni yolunu anlatıyor. www.techexplorist.com sitesine konuşan makalenin başyazarı Dr. Ciarán Lee, "Kuantum bilgisayarlar tam olarak geliştirildiklerinde, güvenliği sadece matematiksel varsayımlara dayanan günümüz şifrelemelerinin çoğunu yıkacaklar" diyor[7]. Peki bu güvenli iletişim nasıl kuruluyor? Öncelikle kuantum cihazların güvenliği test ediliyor. Ardından da cihazlar arasındaki bağlantının kuantum olup olmadığına ve başka bir yöntemle bağlanamayacağına bakılıyor. Bu bağlantılar, yazışmaları karıştıracak anahtarları oluşturmak için kullanılıyor. Anahtarlar öyle güvenli ki hiçbir programcı içeriğe sızamıyor.

**Kırılamayan Bilgisayar Çipi**

2017'nin Ağustos ayında da New York Üniversitesi Abu Dhabi'den (NYU Abu Dhabi) araştırmacılar, bilgisayar donanımlarının savunmasını desteklemek için hack'lenemeyen bir bilgisayar çipi geliştirdiklerini duyurmuştu. NYU Abu Dhabi Mükemmelliyet Tasarımı Laboratuvarı Yöneticisi Özgür Sinanoğlu, Trojan olarak adlandırılan kötücül yazılımların bazen fabrikalarda ya da üretim laboratuvarlarında bilgisayarlara fiziksel olarak yüklenebildiğini ve bunun arka planda cihazlara serbest erişime olanak tanıdığını belirtiyor. Geliştirilen bu çip ise gizli bir anahtara sahip ve bu erişimi engelleyebiliyor ve sadece yetkilendirilmiş kullanıcılar için işlevsellik sağlıyor. Sinanoğlu, "Gizli anahtar olmadan çipler işlevsel hale gelmiyor" diyor[8].

7 https://www.techexplorist.com/step-forward-toward-secure-unhackable-quantum-network/10474/
8 https://www.thenational.ae/uae/science/new-york-university-abu-dhabi-researchers-develop-unhackable-computer-chip-1.621362