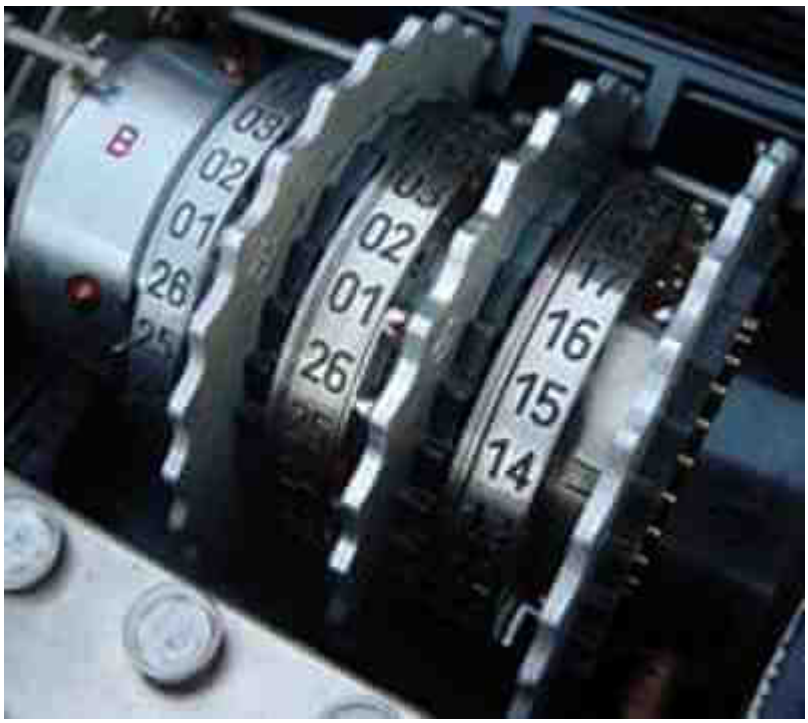
canyoupwn.me

TR | Kriptografiye Giriş – 1

Furkan BUYRUKOĞLU

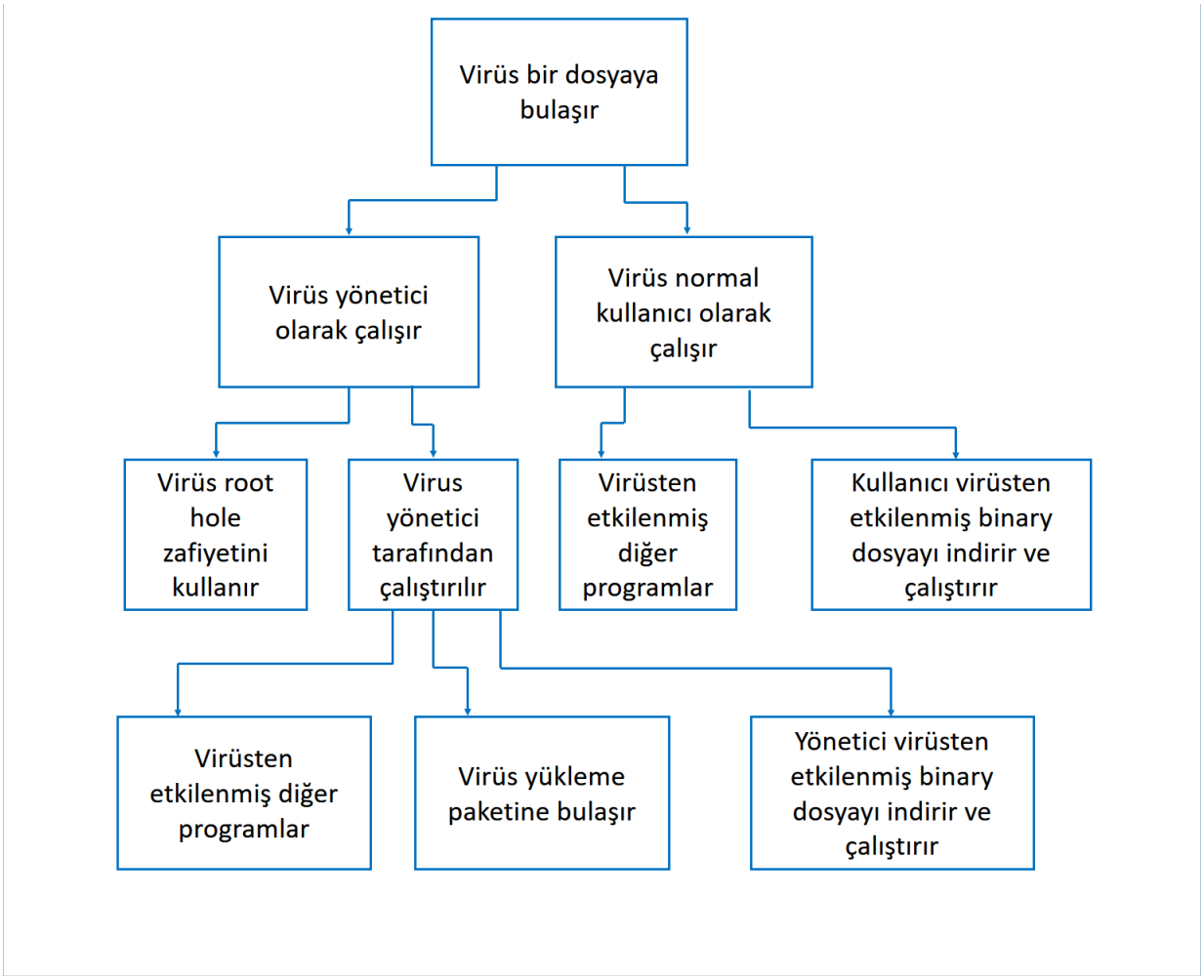


Kriptografi şifreleme bilimi ve sanatıdır. Günümüz dünyasında yetkilendirme, dijital imzalar ve daha birçok temel güvenlik fonksiyonlarının temelini oluşturur. Ayrıca kriptografi hayatın birbirinden farklı yüzlerinde karşılaşabileceğimiz bir alandır. Mesela kriptografi konulu bir konferansta, bilgisayar güvenliği, cebir, iktisat, adli suçlar, istatistik, çip dizaynı, yazılım optimizasyonları gibi konularla karşılaşmanız muhtemeldir.
Bahsedilen alanlardaki çeşitlilik kriptografiyi, bir çalışma konusu olmak için ziyadesiyle cazip hale getirdiğinin kanısındayım.

Tek başına kriptografinin rolünden bahsetmek gereksiz ve anlamı olmayan bir harekettir. Kriptografi daha büyük bir sistemin parçası olmak zorundadır. Bunu daha iyi anlamak için kriptografiyi günlük hayatta kullandığımız kilitlere benzetebiliriz. Bir kilit ancak koruduğu binayla ya da kafesle bir anlam ifade eder. Aksi halde, tek başına bir kilidin kullanışlı olduğundan bahsetmemiz mümkün değildir. Bina örneğinden devam edersek, bu binada oturan insanların kapılarını kilitlemeyi unutmaması ve anahtarı güvenli bir şekilde saklayarak hırsızlardan uzak tutması gerekir. Aynı şekilde kriptografi de, içinde bulunduğu güvenlik sisteminin ya da protokolünün küçük bir kısmını oluşturur.
Kriptografi içinde bulunduğu sistemin küçük bir parçası olsa bile, sistemin en kritik kısımlarından

biridir. Kriptografi, bazı insanlara erişim vermek zorunda olduğu gibi istenmeyen insanları da bu erişimden uzak tutmak zorundadır. “İyi” ve “kötü” arasında ayrım yapmak zorundadır. İşte bu kısım kriptografi biliminin ince noktalarından birisini oluşturur. Güvenlik sistemlerinin büyük çoğunluğunu oluşturan kısımlar, tüm insanları dışarısında tutabileceğimiz duvarlara benzer. Kriptografi ise “iyi” ve “kötü” insanları ayırmak zorundadır. Görüldüğü üzere bu işlem, herkesi dışarıda tutmaktan daha zahmetli bir iştir. İşte bu yüzden kriptografi ve kullandığı diğer etmenler, bir sisteme yapılacak olan saldırının en doğal noktası konumundadır.
Ama bu durum kriptografinin, bir sistemin her zaman en zayıf noktası olduğu anlamına gelmez. Bazı durumlarda kötü bir kriptografi yaklaşımı bile bir güvenlik sisteminin diğer parçalarından daha iyi olabilir. Hepimiz filmlerde, banka kasalarını koruyan birkaç metre kalınlığında etkileyici çelik kapıları görmüşüzdür. Dijital dünyada ise bunun gibi bir kapının basit bir çadırı korumak için kullanıldığını görebiliriz. İnsanlar ise çadırın basitliğine bakmak yerine, kapının kalınlığının ne kadar olması üzerinde tartışarak vakit harcıyorlar. Siber dünyadan daha somut bir örnek vermek gerekirse herhangi bir web uygulamasındaki şifreleme anahtarının uzunluğunu tartışarak, o uygulamadaki buffer overflow zafiyetini göremeyebiliyoruz. Sonuç ise saldırgan kriptografi sistemine saldırmakla uğraşmayıp buffer overflow zafiyetini kullanarak amacına ulaşıyor. Sonuç olarak sistemin diğer parçalarının “yeterli” seviyede güvenli olması şartıyla kriptografinin asıl yararına ulaşılabilir.
Bir sistemdeki farklı zafiyetler, farklı saldırganlar için farklı yollarla yararlı olabilir. Mesela, kriptografi kısmını atlayabilen bir saldırganın tespit edilme olasılığı düşüktür. Çünkü saldırganın sisteme erişimi “iyi” ya da “muhtemel” bir erişim olarak görülecektir. Bu ayrıca saldırganın takip edilmesini de zorlaştıracaktır. Yine gündelik hayattan bir örnek vermek gerekirse, levye kullanarak eve giren bir hırsız, kapıda görülebilen bir hasar bırakırken, maymuncuk kullanan bir hırsız da bu durum söz konusu olmayacaktır. Maymuncuk kullanılan bir hırsızlığın tespit edilmesi çok daha zordur.

“Bir sistem en zayıf halkası kadar güçlüdür.” Büyük puntolarla yazıp bilgisayarımıza, ofise, panolara yapıştırılabilecek bir ifade değil mi sizce de?
Bu ilke, güvenli bir sistem oluşturmanın ne kadar zahmetli olduğunu gösteren ana sebeplerden birisidir. Bir zincirin diğer kısımları ne kadar sağlam olursa olsun, en zayıf halkası, kopacak olan ilk kısımdır. Bir plazadaki her ofis kapısının geceleyin kilitlendiğini düşünelim. Kulağa gayet makul ve güvenli geliyor değil mi? Ama bir problem var ki, plazada asma tavan kullanılmış. Asma tavan parçalarından birisi kaldırıldığında kilitli kapının üzerinden tırmanılıp kapı çok kolay bir şekilde aşılabilir. Başka bir açıdan düşünürsek, kilitli kapılar elbette hırsızların işini zorlaştıracaktır fakat güvenlik görevlisinin ofisleri kontrol etmesini de zorlaştıracaktır. Bu örnekte “en zayıf halka ilkesi”, kapıların kilitlenmesinin sağlayacağı etkiyi azaltmıştır. Evet, kapılar kilitlenerek aşılması zor hale getirilmiştir fakat hala tedbir almamız gereken asma tavan problemi devam etmektedir. Bu durumda “en zayıf halka” asma tavan problemidir.
Bir sistemin güvenliğini artırmak için, en zayıf halkasının güçlendirilmesi gerekir. Bunu başarabilmek içinse halkaların hepsinin bilinmesi ve hangilerinin en zayıf olduğunun tespit edilmesi gerekir. Bu tespitleri, saldırı ağacı(attack tree) kullanarak yapabiliriz.



Saldırı ağaçları, muhtemel atakları önceden görebilmek için değerli bir bakış açısı sağladığından dolayı önemlidir. Bir sistemi güvenli hale getirmek için yapılan çalışmaların ilk adımı, bu yapının ortaya çıkarılmasıdır. Aksi halde vakit ve efor kaybı kaçınılmazdır.
“En zayıf halka ilkesi” kriptografi çalışmalarını çeşitli yollardan etkiler. Mesela, kullanıcıların güçlü parolalara sahip olduğunu varsaymak her ne kadar cazip gelse de, günlük hayatta maalesef bu gerçekleşen bir durum değildir. Genelde kısa parolalar kullanılmaktadır. Parolaların ekrana yapıştırılması verilebilecek en bariz örneklerden birisidir. Böyle bir durum sistem tasarımcıları tarafından göz ardı edilemez. Bir sistem tasarımcısı olarak kullanıcılara her hafta 13 haneli rastgele oluşturulmuş parola verseniz bile, bu parolaların ekrana yapıştırılacağından emin olabilirsiniz. Bu zafiyet en zayıf halka olan kullanıcıyı daha da zayıf hale getirmektedir. Kısaca zayıf halka dışındaki diğer halkaların güçlendirilmesinin hiçbir yararı olmayacaktır.
Sistemin zayıf halkası saldırgana ve kullandığı araçlara göre de değişkenlik gösterebilir. Bunun için kriptografi bilimi, bu alanda uğraşan insanlara profesyonel paranoyaya sahip olmaya zorlayabilir.

Kriptografi, güvenlik problemlerine bir çözüm değildir. Çözümün bir parçası olabileceği gibi problemin de bir parçası olabilir. Bazı durumlarda kriptografi, bir problemi daha da zor hale getirerek, kriptografi kullanmanın avantajı ortadan kalkabilir.

Kimse tarafından okunmasını istemediğiniz bir dosyanız olduğunu varsayalım. Bu dosyayı basit bir şekilde istenmeyen erişimlerden koruyabilirsiniz. Diğer bir seçenek ise dosya içeriğini şifreleyip rastgele oluşturulan anahtarı koruyabilirsiniz. Dosyanızı şifreledikten sonra USB'de sakladığınızı varsayalım. USB kaybolsa bile okumak için hala anahtara ihtiyaç var. Peki anahtarı nerede saklayabiliriz? İyi bir anahtar, hatırlanmayacak kadar uzun bir anahtardır. Bazı programlar bu anahtarları diskte depolarlar. Dosyanızı sabit diskten ya da USB'den ele geçirebilen bir saldırıyı göz önüne alırsak, artık anahtarınız da tehlike altındadır. Bu saldırı anahtarınızı ve şifrelenmiş dosyanızı ele geçirerek dosyanızı okuyabilir. Artık yeni bir zafiyet noktamız var: Eğer şifrelerin rastgele oluşturma oranı düşükse ya da şifreleme işlemi güvensizse, saldırgan şifreleme işlemini kırabilir.
Kriptografi uygun yollarla sağlanmazsa sistemi güvenli hale getirmek yerine daha büyük bir problemlere yol açabilir. Yukarıdaki örnekte de bu görülebilir.

———

Bu gerçeklemesini istediğim Kriptoloji yazı dizisinin ilk parçası… Bu ve olası diğer yazılar için yapıcı olduğunu düşündüğünüz her türlü eleştiriyi ve fikri paylaşırsanız hem keyifli hem de öğretici bir yolculukta beraber olabiliriz.