28.5.2019

Kablosuz Ağlarda Güvenlik Final Sınavı

Teslim Tarihi: 29.5.2019, saat 23:59

1. Büyük bir Toptan Satış Zincir mağazasından alışveriş yapacaksınız. Mağazada alışveriş söyle yapılmaktadır: Önce alacağınız ürünleri seçip kasaya gidiyorsunuz. Kasada ödeme yaptığınızda ürünler ayrı bir kanaldan çıkışa yönlendiriliyor. Siz ödeme yaptığınızı gösteren fişle çıkış kapısından fişinizi alınan malların üzerini bir memur kalemle işaretlemek suretiyle onaylattıktan sonra ürünlerinizi teslim alıyorsunuz.
2. (15 puan) Bu alışveriş yaklaşımında kullanılan iki güvenlik prensibini açıklayınız.
3. (10 puan) Onaylama işini yapan memurun hangi saldırıya karşı güvenlik oluşturduğunu açıklayınız. Saldırı tipini de tarif ediniz.
4. K uzunluğunda bir anahtar ve M uzunluğunda bir mesajın kullanıldığı AES-128 uygulayan şifreleme modunda, M mesajının I adet 128-bitlik bloktan oluştuğu bilinmektedir. Gönderici önce 128-bitlik bir string, C0 seçiyor ki bu ciphertext in ilk bloğunu oluşturuyor. Daha sonra i>0, her i blok için Ci=Ci-1 ⊕ AES-128K(Mi) formülü kullanılmaktadır. Ciphertext bu blokların birleşimi şeklinde oluşmaktadır: C = C0 || C1 || C2 || · · · || Cl .
5. (5 puan)C0 rastgele değerinin amacı nedir?
6. (10 puan) BU şifreleme modu güvenli midir? Öyle ise hangi özellikleri sağladığını ifade ediniz. Değil ise zafiyetlerini belirtiniz.
7. (10 puan) Ci hesaplamada kullanılan formülün yerine Ci = AES-128K(Ci−1 ⊕ Mi) kullanıldığını düşünelim. Bu şifreleme modunu daha güvenli yapar mı? Açıklayınız.
8. Twitter aracılığıyla bir botnet komut ve kontrıl yapısı kullandığını düşünelim. Basit bir Twitter yapısında: (1) kullanıcılar hesaba kaydolur (2) Kayıt tamamlandığında, bir çok kısa mesajı post edebilir, bunlara tweet adı veriliyor (3) A kullanıcısı B kullanıcısını takip eder ve A, B’nin tweet’lerinin birer kopyasını alır (4) B kullanıcısı ne zaman A kullanıcısının B kullanıcısını takip etmeye karar verdiğini söyleyebilir (5) Twitter home page üzerinden, en son tweet’lerin küçük bir örneğini (0.1%) kadar görebilir.
9. (15 puan) botmaster, bir botnet yapısını nasıl oluşturur ve Twitter için bunu kullanıma açar açıklayınız.
10. (10 puan) Twitter bunu nasıl kullanabilir.
11. (25) Bir Kahvede otururken yakındaki free WiFi servisinden faydalanmaya karar veriyorsunuz. Burada web ve tweet sistemlerini kullanıyorsunuz. Ağdaki mesajların şifresiz gittiğinden de haberdarsınız ve yanınızda oturan kişinin da kötü niyetli bir dinyeliyi olduğunun da farkındasınız.web bağlantınız için temel güvenlik özellikleri; confidentiality, integrity, and availability irdeleyiniz.