Kriptanaliz ve Kriptosistemlere Saldırılar

Cipher-text only (Sadece Şifreli Metin) Saldırısı:

Bu saldırı tipinde, saldırıyı yapan kişi mesajın içeriği hakkında hiç bir şey bilmemektedir, ve sadece şifreli-metni kullanarak çalışmalıdır. Uygulamada düz metne (plain text) - pek çok mesaj türü sabit başlık formatlarına olduğundan - ilişkin tahminler yapmak genelde olasıdır. Sıradan mektuplar ve belgeler bile kestirilebilir bir şekilde başlamaktadır. Örneğin, pek çok klasik saldırıda ciphertext'in frekans analizi kullanılmaktadır, ancak modern cipherlara karşı bu yöntem iyi çalışmamaktadır. Buna rağmen mesajlar bazen istatistiksel bir yanlılık içermektedirler.

Bilinen Düz-Metin Saldırısı:

Saldırgan ciphertext'in bazı kısımlarından düz metni tahmin edebilir veya bölebilir. Geriye kalan iş bu bilgiyi kullanarak ciphertext bloklarını çözmektir. Bu işlem, veriyi şifrelemek için kullanılan anahtarın belirlenmesi ile yapılabilir. En sık kullanılan Bilinen Düz Metin Saldırısı, blok cipher'lara karşı lineer kriptanaliz saldırısıdır.

Seçilmiş Düz Metin Saldırısı:

Saldırgan bilinmeyen anahtar ile şifrelenmiş istediği her metni elde edebilmektedir. Buradaki iş, şifreleme için kullanılan anahtarı belirlemektir. Bu saldırı için iyi bir örnek, blok cipherlara karşı (ve bazı durumlarda hash fonksiyonlarına karşı) uygulanabilen diferensiyel kriptanalizdir. Bazı kriptosistemler, özellikle RSA, seçilmiş-düz metin saldırılarına karşı açıktır. Bu tip algoritmalar kullanıldığında, uygulama (veya protokol) öyle tasarlanmalıdır ki saldırgan istediği düz metni şifrelenmiş olarak elde etmeMElidir.

Ortadaki Adam Saldırısı:

Bu saldırı, kriptografik iletişim ve anahtar değişimi protokolleri ile ilgilidir. Fikir şudur; iki kişi güvenli iletişim için anahtarlarını değiş-tokuş ederken (örneğin Diffie-hellman kullanarak), bir düşman kendisini iletişim hattındaki iki kişi arasına yerleştirir. Sonra bu düşman her iki kişi ile ayrı bir anahtar değiş-tokuşu gerçekleştirir. Her iki kişi farklı bir anahtar kullanarak işlerini tamamlayacaklardır ki bu anahtarlar düşman tarafından bilinmektedirler. Bu noktadan sonra saldırgan uygun anahtar ile herhangi bir iletişimi deşifre edebilecek ve bunları diğer kişiye iletmek için diğer anahtar ile şifreleyecektir. Her iki tarafta güvenli bir şekilde konuştuklarını sanacaklardır, ancak gerçekte saldırgan konuşulan herşeyi duymaktadır.

Ortadaki-adam-saldırısını engellemenin bir yolu dijital imzaları kullanabilen bir açık anahtar kriptosistemi kullanmaktır. Kurulum için her iki tarafta karşı tarafın açık anahtarını bilmelidir (ki bu bazen açık anahtar kriptosisteminin esas avantajını baltalamaktadır). Paylaşılan gizlilik oluşturulduktan sonra, taraflarkendi dijital imzalarını karşı tarafa göndermelidir. Ortadaki-Adam bu imzaları taklit etmeye çalışacak, fakat imzaların sahtesini yapamayacağı için başarısız olacaktır.

Bu çözüm, açık anahtarların güvenli bir biçimde dağıtımı için bir yolun varlığı halinde yeterlidir. Böyle bir yol X.509 gibi bir sertifika hiyerarşisidir. Bu, örneğin, IPSec (Internet Protocol Security) 'de kullanılmaktadır.

Gizili anahtar ile kriptosistemin çıktısı arasındaki korelasyon kriptanaliz için ana bilgi kaynağıdır. En kolay durumda, gizli anahtar hakkkındaki bilgi direkt olarak kriptosistemden sızdırılır. Daha karmaşık durumlar, kriptosistem hakkında gözlenen (ölçülen) bilgi ile tahmin edilen anahtar bilgisi arasındaki korelasyon üzerinde çalışmayı gerektirir. Bu sıkça çok ileri düzey saldırı durumlarında kullanılır. Örneğin, blok cipherlara karşı lineer (ve diferansiyel) saldırılarda kriptanalist bilinen (seçilmiş) düz metin ve gözlenen şifreli-metin üzerinde çalışır.

1980 lerin sonuna doğru Adi Shamir ve Eli Biham tarafından tanıtılan direfansiyel kriptanaliz, blok cipherlara (özellikle DES 'e) karşı bu fikri (korelasyon fikrini) tam anlamıyla uygulayan ilk saldırıdır. Sonraları Mitsuru Matsui DES 'e karşı daha etkili olan lineer kriptanalizi ileri sürmüştür. Sonraqdan benzer fikirlere sahip saldırı çeşitleri geliştirilmiştir.

Bu konuya ilişkin belki de en iyi tanıtım EUROCRYPT ve CRYPTO 'nun 1990 lı yıllar boyuncaki sayılarında verilmiştir.Çalışmaya, Mitsuru Matsui'nin DES'in lineer kriptanalizi hakkındaki tartışması ile, veya Lars Knudsen 'in budanmış diferansiyeller fikri ile (örneğin, IDEA kriptanalizi) başlayabilirsiniz. Ayrıca Eli Biham ve Adi Shamir'in DES'İn kriptanalizi hakkındaki kitabı bu konu üzerine "klasik" bir çalışma olarak görülebilir.

Korelasyon fikri kriptografide temeldir ve pek çok araştırmacı bu tip saldırılar karşısında güvenliği sağlamaya çalışmışlardır. örneğin, Knoudsen ve Nyberg diferansiyel kriptanalize karşı güvenliği sağlamak üzerine çalışmışlardır.

Kaynak: science.ankara.edu.tr