

## Elektronik aldatma sanatı

Fatih Emiral

Deloitte

**S** standart bilgisayar kullanıcıları için bilgisayarlar çok karmaşık, nasıl çalıştıklarının anlaşılması zor sistemlerdir. Bu algılamanın sonucu olarak da bir bilgi bilgisayardan üretiliyor veya bilgisayar aracılığı ile iletiliyorsa, bu bilgiye olan güven son derece yüksektir. Bilgisayarların karmaşık oldukları, donanım, sistem yazılımı, bilgi ağı yazılımı ve uygulama yazılımlarının birbirleri ile uyum içinde ve hatasız çalışmalarının gerçekten son derece detaylı bir alt yapı sayesinde sağlandığı doğrudur. Ancak bilgisayarlar özellikle alt yapı (sistem yazılımları ve standart sistem uygulamaları) konusunda herkes için o kadar da karmaşık değildir. Bilgisayarların yeterli zamanı ve ilgisi olan kişiler için zannedildiği kadar karmaşık olmamasının nedeni, yüksek disiplin gerektiren alt yapı yazılım geliştirme çalışmalarının çoğunlukla hak ettiği disiplin içinde ve gerekli dokümantasyonu ile üretilmiş olmasıdır. Elbette üretici firmaların kendi standartlarını oluşturarak geliştirdikleri yazılım teknik dokümantasyonuna herkesin ulaşması söz konusu değildir. Ancak açık sistemler olarak tabir edilen ve TCP/IP bilgi ağı protokol setini kullanan sistem yazılımları ve bu setin parçaları için, bu dokümanlara herkesin erişimi doğal olarak mümkündür (bakınız <http://www.rfc-editor.org>). İşte bu nedenle, her detayı bilmeseye bile açık sistemlere çeşitli nedenlerle ilgi duyan kişiler açık sistem dokümantasyonlarına kolaylıkla ulaşabilir. Bu dokümanlara RFC (Yorum Talebi) adı verilir. TCP/IP olgunluk düzeyine ulaşmış bir protokol seti olduğundan, RFC yayınlanma veya değişiklik sıklığı yüksek değildir. Ancak yeni bir bilgi ağı hizmet uygulaması veya protokol türü için ilk olarak İnternet mühendislik çalışma grubu tarafından bilgisayar endüstrisinde bulunan firma temsilcilerinin, açık sistemlerin geliştirilmesine katkıda bulunan akademisyenlerin ve yine ilgililerin yorumları için Yorum Talebi üretilir. Nihayetinde son halini alan ve standart haline gelen Yorum Talepleri, geliştirilecek açık sistem yazılımları için temel oluşturur. Bu dokümanlarda sistem yazılımlarının nasıl davranacağı açık biçimde tanımlandığından, belli taleplere nasıl yanıt vereceklerini veya belli talepler durumunda nasıl davranacaklarını tahmin etmek mümkün olabilmektedir. Elbette buna ek olarak yazılım kodu incelemesi, deneme yanılma ve diğer pek çok yöntemle uygulamaya özel davranış şekilleri de tespit edilmektedir.

Yazılım güvenliği günümüzde son derece önemlidir, ancak bilgi teknolojilerinin ortaya çıkmaya başladığı dönemlerde yazılımın yerine getirdiği fonksiyon, güvenlik ihtiyaçlarını karşılamasından daha fazla önem taşımaktaydı. Güvenliğin önemi artmış olsa da günümüzde geliştirilen uygulamalarda da fonksiyonun önceliği, genellikle güvenlikten öndedir. Yukarıda belirtilen yöntemlerle ortaya çıkarılan güvenlik açıkları aracılığı ile kimlik gizleme, kimlik taklidi, hizmet uygulaması aracılığı ile yetkisiz kod çalıştırılması, hizmet veren sistemin yönetiminin ele geçirilmesi, hizmet sağlayan sistemin hizmet kesintisine uğratılması ve pek çok bilgi güvenliği tehdidinin gerçekleşmesi mümkün olmaktadır. Kısacası elektronik hizmetleri kötü amaçla kullanmak isteyenler için önemli olan, neyi nerede bulacağını bilmektir. Böylece sistemlerin karmaşıklığı azalmaktadır.

Sistem ve bilgi ağı uygulamalarına olan yüksek güvenin ne kadar hatalı olabileceğinin bir örneği olarak, her gün pek çok kişinin posta kutusuna gelen istenmeyen postalar verilebilir. Bu postalardaki gönderen adresleri uydurma adreslerdir. Hatta e-posta uygulamasında görülen alıcı adresi dahi bizim adresimiz olmayabilir. Bunun nedeni, "SMTP" olarak adlandırılan elektronik posta protokolünde (RFC821) güvenilir olmayan verilerin gönderici ve alıcı olarak kullanıcılara sunulmak üzere kullanılmasıdır. Elbette bu tür ve diğer pek çok bilgi güvenliği sorunları için güvenlik önlemleri mevcuttur, ancak standart uygulamada kullanıcının yanıltılması mümkündür.



Elektronik postanızın gönderici adres bilgisine de güvenemezseniz, 'e-posta ile onay alıyorum' sözünün ne anlamı kalır öyle değil mi?

FATİH EMİRAL

Deloitte Kurumsal Risk Hizmetleri

EYLUL 2004, ACTIVELINE