VoIPSec sorunları ve çözümler

ÇETİN KAYA
KOÇ

VoIP, küçük boyutlu paketleri çok hızlı gönderme eğiliminde olan bir protokol.

VoIP paketlerinin servis kalitesi sorunları, özellikle paket gecikmesi ve kaybı, bu paketlerin etkili biçimde şifrelenmesine engel oluyor. Yapılan araştırmalar bize kriptografik algoritmaların performans sorunlarının VoIP servis kalitesini çok ciddi bir şekilde etkilediğini öğretiyor. Şifreleme ve deşifre etme algoritmalarının harcadıkları zaman, paketlerin tesliminde gecikmelere neden oluyor. NIST (National Institute of Standards and Technology) tarafından 100 Mbps hızındaki bir ağ üzerinde yapılan deneyler, hafif ve çok hızlı algoritmaların daha başarılı sonuçlar verdiğini gösteriyor. Bu deneylerde DES, 3DES, Şifrelemesiz SHA-1, ve 3DES artı SHA-1 kullanılmış, beklenildiği gibi hızlı ve az yer kaplayan algoritmaların daha hızlı şifreli ve kimlik doğrulamalı VoIP iletişimi sağladığı tespit edilmiş. Bu sayede biz de kriptografik algoritmaların performans faktörlerinin ne kadar önemli olduğunu bir kere daha öğrenmiş olduk.

VoIP, küçük boyutlu paketleri çok hızlı gönderme eğiliminde olan bir protokol. Ayrıca paket kaybına hiç tolerans yok. Diğer taraftan, en hızlı ve en basit şifreleme algoritmaları aynı zamanda kırılması en kolay algoritmalar oluyor, ne yazık ki. Bütün bunlar VOIP'da servis kalitesi ve güvenlik amaçlarının birbirleri ile çeliştiğini ve bu sorunun tek çözümünün ancak çok hızlı ama aynı zamanda çok güvenli kriptografik algoritmalar tasarımıyla mümkün olacağını gösteriyor. Bu çözüm, şimdilik çok uzakta gözüküyor. Çünkü elimizdeki kriptografik tasarım araçları böyle algoritmalar bulmak için yeterli değil.

koc@krip.to