

Kablosuz Ağlarda EAP Tabanlı Güvenlik Metotları

TANER KOÇ/ İTÜ'BiDB 2010

EAP(Extensible Authentication Protocol), birçok kablosuz ağ güvenliği metodunun temelini oluşturan protokoldür. EAP protokolü üzerinden geliştirilen PEAP, LEAP, EAP-TLS, EAP-FAST metotları bunlara örnek olarak gösterilebilir. Bunlardan her biri EAP'i temel alır, fakat kimlik denetimi için farklı referanslar kullanırlar. Bazılarında ek güvenlik özellikleri mevcuttur.

LEAP(Lightweight EAP)

Cisco tarafından geliştirilmiş bir protokol olan LEAP'te AP'ler kullanıcıların kimlik denetimlerini bir RADIUS(Remote Authentication In User Server/Service) üzerinden gerçekleştirirler. Kimlik denetimi için kullanıcı adı ve şifre kullanılır.

LEAP ayrıca WEP'i kullanarak veri güvenliğini de sağlar. Her kablosuz ağ kullanıcısı için dinamik olarak RADIUS sunucu tarafından bir WPA anahtarı üretilir. Böylece kullanıcı bazlı veri güvenliği sağlanmış olur.

EAP-TLS

EAP-TLS metodu, güvenli kimlik denetimi için TLS(Transport Layer Security) protokolünü kullanır. TLS'in temeli güvenli web oturumları sağlamak için kullanılan SSL(Security Socket Layer) protokolüne dayanır. EAP-TLS kimlik denetimi için dijital sertifikaları kullanır. Bu yüzden her AP'nin ve her kullanıcının sertifika otoritesi tarafından üretilmiş bir sertifikaya ihtiyacı vardır.

EAP-TLS; sunucu, kullanıcıyı her yeniden kimlik denetiminden geçmeye zorladığında otomatik olarak WEP anahtarı üreterek veri güvenliğini de sağlar. Kimlik denetiminden geçen her kullanıcı için TLS oturum anahtarı, WEP anahtarını üretmek için kullanılır ve veri güvenliği sağlanır.

PEAP(Protected EAP)

PEAP'te de EAP-TLS'te olduğu gibi kimlik denetimi için TLS oturumu temel alınır. Fakat PEAP'te dijital sertifikaya sadece kimlik denetimi sunucusunda gerek duyulur. Kullanıcılar kimlik denetiminden geçmek için MSCHAPv2'yi(Microsoft Challenge Handshake Authentication Protocol version 2) kullanırlar.

EAP-FAST(EAP Flexible Authentication via Secure Tunneling)

EAP-FAST Cisco tarafından geliştirilmiş bir protokoldür. Yönetimsel karışıklıkları azalttığı için esnek bir protokoldür. Kullanıcıların dijital sertifikalar kullanmasına ve güçlü şifre kurallarına gerek yoktur.

EAP-FAST ile kimlik denetim sunucusu ve kullanıcı arasında güvenli bir tünel oluşturulur. Tüneli oluşturmak için PAC(Protected Access Credential) adında bir referansa ihtiyaç duyulur. PAC bir PAC sunucusu vasıtasıyla veya EAP-FAST fazlarında dinamik olarak

oluřturulabilir. Tünel bir kez kurulduğunda, kullanıcılar kullanıcı adı ve řifreleriyle kimlik denetiminden geçerler.

Ayrıca PEAP'te WEP sayesinde veri güvenliđi de garanti altına alınabilir.