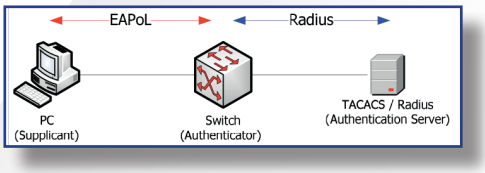
EAP-TLS

AP-TLS setzt für die Authentifizierung auf Client- und Serverseite zwingend ein Zertifikat voraus. Bei einer Anmeldung am Switch werden die Zertifikate ausgetauscht und überprüft. Der Vorteil besteht darin, dass ein Angreifer aufgrund eines fehlenden oder ungültigen Zertifikates keine Verbindung erhält, obwohl er eventuell ein gültiges Passwort besitzt.



Funktion

EAP mit Transport Layer Security

Gegenseitige Authentifizierung von Peer und Authenticator mit digitalen Zertifikaten und Schlüsselmanagement bringt die EAP-Erweiterung TLS (RFC 5246). TLS nutzt ein asymmetrisches Chiffrierverfahren zum Ermitteln der Sitzungsschlüssel. Zu Beginn schickt der Authenticator sein Zertifikat zusammen mit seinem öffentlichen Schlüssel (Public Key) und fordert den Peer auf, das gleiche zu tun. Der Peer antwortet entsprechend und generiert anschließend ein Premaster Secret, das er mit dem Public Key des Authenticators verschlüsselt und abschickt. Aus dem Premaster Secret leitet der Authenticator dann ein Master Secret ab, mit dem er neue Schlüssel erzeugt, die beispielsweise als dynamische Sitzungsschlüssel dienen können.

Hat der Peer das Zertifikat des Authenticators über einen sicheren Kanal erhalten oder kann er dessen Gültigkeit über ein Stammzertifikat einer Certification Authority (CA) überprüfen, dann ist diese EAP-Variante die sicherste von allen. EAP-TLS wird in RFC 5216 beschrieben.

Protokoll	PEAP	EAP-TLS	EAP-TTLS	EAP-MD5	LEAP
Standards	Ja	**Ja**	IEFT Draft	Ja	Nein (Cisco)
Sicherheitslevel	Hoch	**Sehr Hoch**	Hoch	Sehr Schwach	Schwach
Server Zertifikat erforderlich	Ja	**Ja**	Ja	Nein	Nein
Client Zertifikat erforderlich	Nein	**Ja**	Optional	Nein	Nein
Geräteauthentifizerung	Unterstützt	**Unterstützt**	Unterstützt	Nein	Nein
Implementierungs-aufwand	Mittel	**Hoch**	Mittel	Sehr gering	Gering, nur Cisco

CISCO

IEEE 802.1x

Zufriedenheit | Unabhängigkeit | Sicherheit

K5 Netzwerksysteme GmbH · Am Giener 23 A · 55268 Nieder-Olm · Tel.: 0 61 31 / 97 155 - 0 · Fax: 0 61 31 / 97 155 - 94 · info@k5-netzwerk.de