IEEE802.1X 認証（利用者認証）

●有線や無線によって、LAN に接続を試みようとするノードを認証する仕組み

●サプリカント（PC 等）、オーセンティケータ（認証装置：L2SW や無線アクセスポイント等）、認証サーバ（IEEE802.1X/EAP に対応した RADIUS サーバを使用）で構成され、ベースプロトコルは EAP (Extensible Authentication Protocol：拡張認証プロトコル)

●EAP は PPP の認証機能を強化したものであり、データリンク層（PPP やイーサネット等）と認証層（TLS や MD5 等）を仲介する EAP 層に位置する。

●ベースは EAP であるが、サプリカントとオーセンティケータ間でイーサネット等（有線無線問わず）を使用している場合は、EAP を EAPOL（EAP over LAN）でカプセル化して、EAPOL を MAC でカプセル化する。

●ベースは EAP であるが、オーセンティケータと認証サーバとの間は RADIUS でカプセル化して、それを UDP、IP、MAC でカプセル化していく。そのため、認証サーバは RADIUS サーバ、オーセンティケータは RADIUS クライアントとなる。

●認証方法は EAP-PEAP、EAP-TLS、EAP-TTLS（Tunneled TLS）、EAP-MD5 等がある。

認証としての WEP（無線 LAN 専用）

●Wi- Fi 上で通信を暗号化して保護する技術規格として、WEP、 WPA、 WPA2、 WPA3 がある。

●WEP は、RC4（暗号アルゴリズム：疑似乱数系列を生成）を使用した暗号方式であり、WEP キー（アクセスポイント毎の事前共有鍵で最大 128bit、伝送フレームには現れない）と IV（Initial Vector：システムが自動生成するナンスであり 24bit、平文で伝送フレームに現れる）を連結したものに対して、RC4 を適用することによって、キーストリーム（疑似乱数系列による共通鍵）を次々と生成し、1bit ずつ平文と XOR を取ることで暗号化する。

●上記の暗号化は、パケット単位で行われるが、キーストリームが同じにならないように、変えるのに非常に面倒な WEP キーではなく、IV を変える。IV を変えたことを相手に伝えるために、IV は平文のまま送られる。

●IV は 24bit であり、一定周期で同じ IV が使用される。WEP キーは不変なので、その時の **RC4 で生成される**キーストリームは同じになるため、その時の暗号文をたくさん集めれば、平文が推測される可能性がある。

虎の巻に掲載されている情報は正確性に欠く部分及び誤字脱字等も多いと思います。そのため、虎の巻に起因した損害等については、管理人として責任を負いかねますので御了承ください。
© 2024 spine-team.com

WPA-TKIP（無線 LAN 専用）

●WEP の脆弱性は、長い周期であっても、同じキーストリームが出現することである。WPA-TKIP は、RC4 を適用する前に同じキーストリームが現れないように、TKIP というキーストリーム（正確には KS の元）の生成方法を規定する。

●アクセスポイント（AP）と端末は、WPA キーを共有している。WPA キーと ESSID から PSK（Pre – Shared Key）を生成し、PSK と ESSID から PMK（Pairwise Master Key）を生成する。これはパーソナルモードの手順であるが、エンタープライズモードは IEEE802.1X 認証後に配布されるセッション鍵が PMK となり、これ以降の処理である **4-way-handshake** は同じになる（←自信がない）。

●**4-way-handshake** は、AP と端末はナンスを交換し、PMK と 2 つのナンス及び両者の MAC アドレスから PTK（ペアー時鍵）を生成・共有する。ここで、**4-way-handshake** は完了する。

●その後、TK（一時鍵：PTK から一定の送受信回数毎に動的に生成）と送信側の MAC アドレスと IV（毎回変化の 48bit）からキーストリームを生成する。これで、接続毎及び端末毎にキーストリームは異なる値になるはずである。

●最終的にキーストリームは、WEP では WEP キーと IV、 WPA-TKIP では TK と MAC アドレスと IV となる。

WPA-AES と WPA2（無線 LAN 専用）

●WPA-AES の暗号アルゴリズムは、ブロック暗号である AES であり、CCMP なので CTR モードをとる。その際、使用する暗号鍵は、**4-way-handshake** で生成された PTK と送信側の MAC アドレスとカウンター値（毎回変化の 48bit）から生成する。これで、CTR モードにおけるキーストリームが生成されるため、あとは平文との XOR をとればいい。

●よって、WPA には、WPA-TKIP と WPA-AES がある。そして、TKIP を使用せず、AES-CCMP の使用を義務化したものが、WPA2 である。ただし、WPA2 と名乗っているだけで、TKIP は使用できるため、WPA=TKIP、WPA2=AES というわけではない。

WPA3（無線 LAN 専用）

●WPA2 を利用した通信を強制的に切断すると、**4-way-handshake** が再び行われ、この **4-way-handshake** の最中に攻撃者が割り込むことで、中間者攻撃、いわゆる鍵再インストール攻撃（KRACKs）ができる脆弱性が発見された。

●そこで新しい Handshake 方法として、DH 鍵交換のような SAE を導入したものが WPA 3 である。

●これまで **4-way-handshake** はパソモードとエンタモード共通の記載をしていたが、WPA3 の様々な資料を読んでいくうちに自信がなくなってきた。これについては、現時点でタイムアウトとする。

虎の巻に掲載されている情報は正確性に欠く部分及び誤字脱字等も多いと思います。そのため、虎の巻に起因した損害等については、管理人として責任を負いかねますので御了承ください。
© 2024 spine-team.com