802.1Xを使った無線LANのセキュリティと相互接続実験

関義和(株式会社ディアイティ)
相互接続WG

2003 年　6月　4日

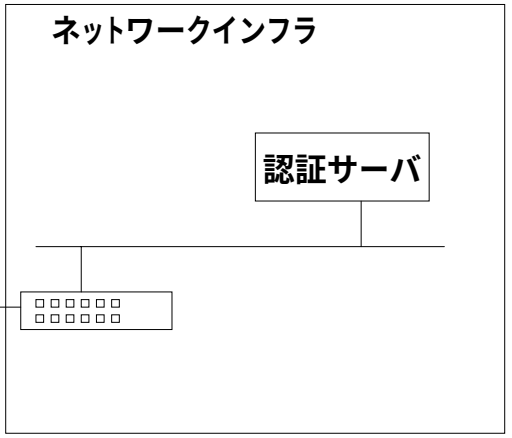
無線LANのセキュリティ問題

JNSA

- WEPが抱える問題
  鍵の入力方法
  鍵の更新
- IEEE802.1Xで解決を図る

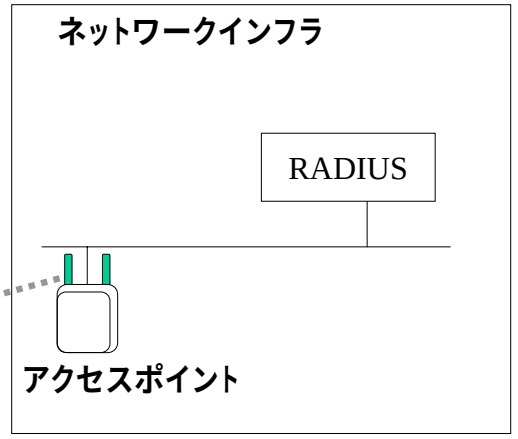
IEEE802.1X

クライアントの識別
認証機能
暗号処理の環境



無線LANでの構成要素

クライアントの識別
認証機能
WEP鍵の運搬
WEP鍵

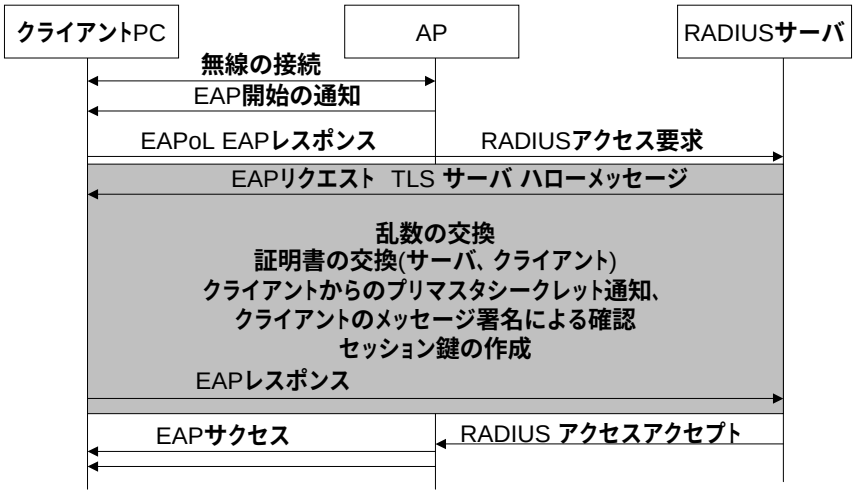


基本形となるEAP-TLS

- サーバは証明書を使って暗号化する
- クライアントは証明書を使って認証を受ける

- TLSの暗号と鍵材料を使って
  WEP鍵を安全に配布する
  WEP鍵を生成する
  (TLSはSSLの後継技術)

EAP-TLSのシーケンス



APの作業

- EAPoLとRADIUSプロトコルを相互に変換
  無線側：EAPoL：レイヤー2のプロトコル
  有線側：RADIUS：UDPのデータグラム
- RADIUSのアクセスアクセプトを
  EAPサクセスに変換
- WEP鍵の処理を行う

TLSからWEPへ鍵の変換

- TLSのマスターセッションキーの作成
  クライアント、サーバランダム
  プリマスタシークレット
- マスターセッションキーの通知
  RADIUSアクセスアクセプト パケット
  　MS-MPPE属性の値
- EAPoL Keyによる通知
  Unicast Keyと Broadcast Key

WEP鍵の取り扱い

- EAPoL Key
  Key：WEP鍵
  Key IV：Initial vector
  Key Index：鍵の番号(1~4)
  - Unicast Key
    デフォルトのWEP Keyに指定される
  - Broadcast Key
    デフォルトに指定されないWEP Key

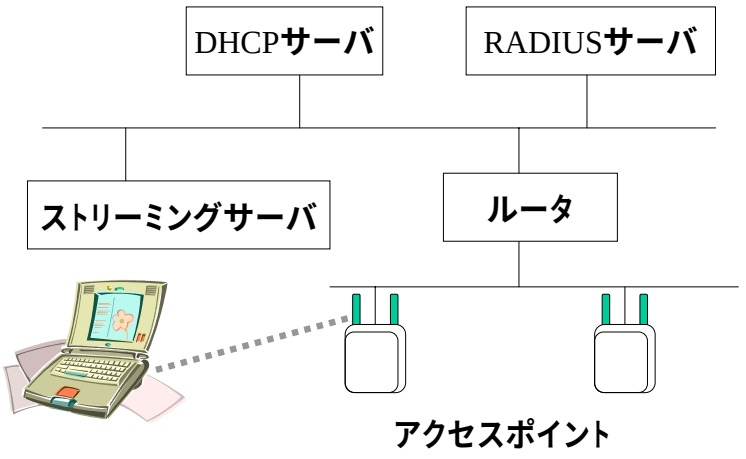
なぜ相互接続が必要か

- 様様な機器
  スイッチ、PC、サーバ、デバイス
- 全ての機器を一斉に
  入れ替えることが難しい
- 混在するネットワーク

実験の目的

- 現状の相互接続性を検証する
- 関係するネットワークの仕組みで問題が出ないかどうかを確認する

実験環境



実験前に想定した問題

- 認証に使う証明書のプロファイル内容
- 認証の失敗
  認証のパラメータが異なるなど
- アプリケーションとの相互干渉
- ローミングによる問題

実験前にわかった問題

プロトコルの実装状況

- 無線に適応すべきプロトコル
  EAP-TLS、
  EAP-TTLS、PEAP
- その他のプロトコル
  EAP-MD5

実験を開始してわかったこと

- APは相互接続性に影響力をもたない
  APは通信プロトコルの変換のみ行う
- APはパフォーマンスが運用の安定性に影響する可能性がある
- サプリカントはRADIUSとAPからの指示に従うのみ

相互接続性の問題

- 802.11のパラメータ
- 認証パケットのパディング

実験の障害

- 操作方法が不明
- 動作が不安定
  APが不安定
  認証の手順がパニックに

ストリーミングデータ

- REALサーバを用意してマルチメディアデータを受信
- UDPのとき
  パケットロストの期間は表示に乱れ
- TCPのとき
  表示の乱れを長く引きずる

結論:相互接続性

- EAP-TLSについては良好であった
- 実験開始の時点では相互接続実験にならない条件もあった

予想するシナリオと異なる動作

- EAP-OL Key
  - 空のUnicast Key
  - 値のあるUnicast Key
- EAP-OL Keyデータグラムの個数
- EAP-OL Keyの送信タイミング

→これらは相互接続性に影響しない

不安な要因

- APとRADIUSサーバの間の通信
  WEP鍵を保護するための暗号鍵
  WEP鍵の材料

  強固な暗号処理を行っていない

- APとRADIUSサーバの通信は安全でなければならない

導入本格化前に望む解決

- プロトコルの統一
  フェーズ1、フェーズ2
- ID(証明書、パスワード)の管理
- APとRADIUSサーバの通信セキュリティ

- 認証SWなどとの連携
- 他のPKIアプリケーションとの連携

直近の展開

- WPA、IEEE802.11iのリリース
  相互接続実験の計画
- LANレベルのセキュリティの実現に向けて
  構築に必要な知識と技術の確立