T26: 間違いだらけの無線LANセキュリティー

進藤　資訓
ファイブ・フロント(株)
Chief Technology Officer
mshindo@fivefront.com

ある先生の採点方法

- もちろん正解は “加点”
- もちろん不正解は “加点なし”
  - しかし、あまりに大きな誤解を含んだ答えや、あまりにあてずっぽの答え(too wildly guessed answer)は **“減点”！**
- 「自分が理解していない事」を理解することも大切！！

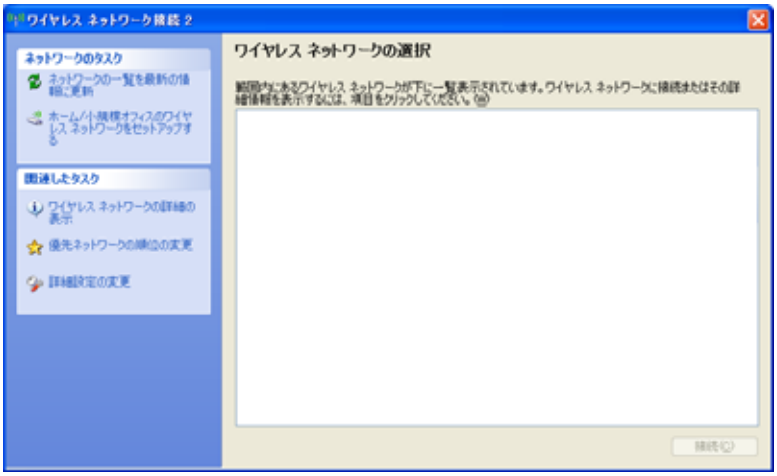
無線LANのセキュリティー

- SSIDの秘匿
- MACアドレスの制限
- WEP
- 802.1X
- WPA
- WPA2 / 802.11i
- …

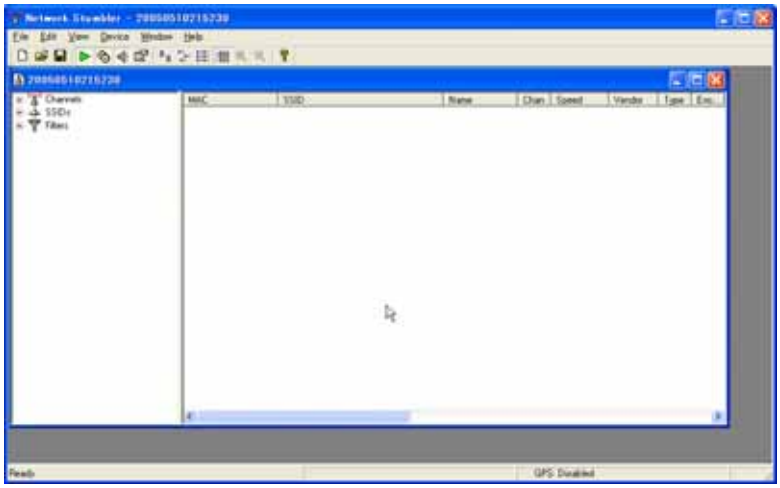
SSIDを隠す！？

- 何をしているか？
  - 802.11 のビーコンを止める
  - プローブリクエストに対して、
    - 応答しない
    - 応答はするが、レスポンスに SSID は入れない
    - 自分の SSID に合致する場合のみ応答
- 呼び名もいろいろ
  - ステルス機能、SSID ブロードキャストの無効化、Any 拒否、Closed System or Network、等々

確かにWindowsからは見えない



NetStumblerでも見えない



でも Kismet なら見える！！

秘匿された SSID

なぜ見える？

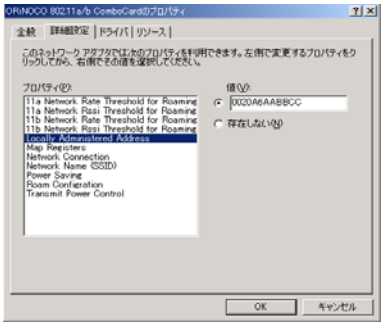
- 802.11では、SSIDを完全に隠すのは不可能
  - アソシエーションする際に必ず SSID は必要！
- 無線LANを “モニタ” すれば見えてしまう

MAC アドレス認証

- 何をしている？
  - クライアントが接続してくるときのMACアドレスを調べ、許可されていないものなら受け付けないようにする
- 実現方法
  - AP に静的に設定する
  - RADIUS 等のサーバーに設定する

「固有」じゃないのよ、MACアドレスは

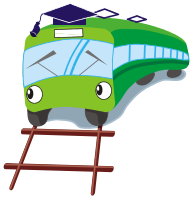
- MAC アドレスの詐称は簡単！
- 正規のMAC アドレスはワイヤレス上で簡単に見つけることができる！




```
# ifconfig eth1 down
# ifconfig eth1 hw ether 12:34:56:aa:bb:cc
# ifconfig eth1 up
```

無線LANキセル乗車

- どうってことない？
  - 自宅のブロードバンドはすかすかだから、少しくらい使われたからって・・・・・



ついに起きたか・・・

他人の無線LAN盗用…不正アクセスで逮捕の大学職員

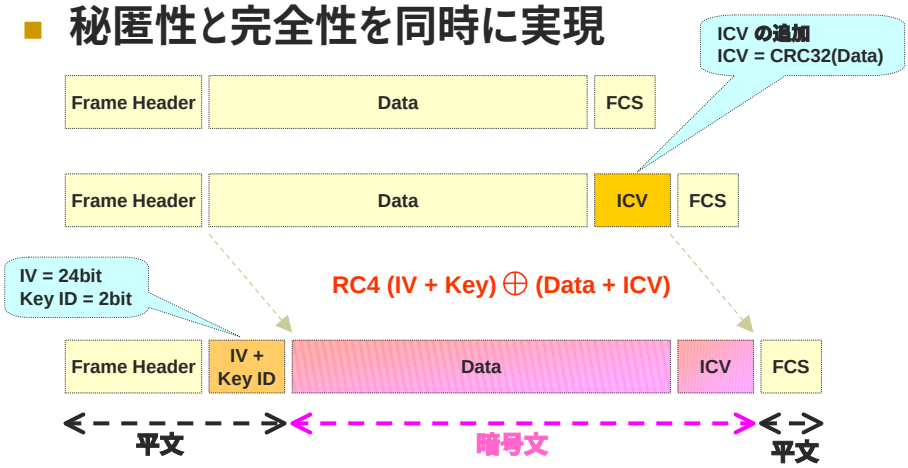
（読売新聞：04/06/09より）
高千穂大学（東京都杉並区）のコンピューターシステムへの不正アクセス事件で逮捕された大職員が、調布市内の会社役員（33）が家庭で使っている無線LAN（構内情報通信網）に"ただ乗り"して、不正アクセスしていたことが9日、警視庁の調べでわかった。
パソコン通信で使われる無線LANは、第三者に電波を"盗用"される恐れがあると指摘されていたが、実際に不正アクセスへの悪用が表面化するのは異例。事態を重視した警視庁は、無線LANの危険性について注意を呼びかける。
調べによると、不正アクセス禁止法違反容疑で逮捕された同大職員中山良一容疑者（47）は昨年11月下旬、車に積んだパソコンを使って、無断使用防止対策が講じられていない無線LAN用電波を物色。
東京・調布市の住宅街で、会社役員宅の電波が無断で使えるのを発見した中山容疑者は、近くに車を止め、会社役員の無線LANに"ただ乗り"してインターネットに接続。他人のIDとパスワードを使い、同大のコンピューターシステムにアクセスしたという。
（以下略）

WEP (Wired Equivalent Privacy)

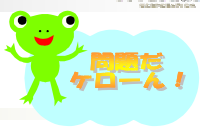
- **何をしている？**
  - **秘匿性** (Confidentiality)
  - **完全性** (Integrity)
  - **認証** (Authentication)
- **実際は？**
  - What on Earth does this Protect?

WEP **処理**

- **秘匿性と完全性を同時に実現**



これ、ほんと？？



WEPには、同じIVで暗号化したフレームを幾つか集めると暗号鍵を解読できるという弱点がある。

（A誌、2003年9月）

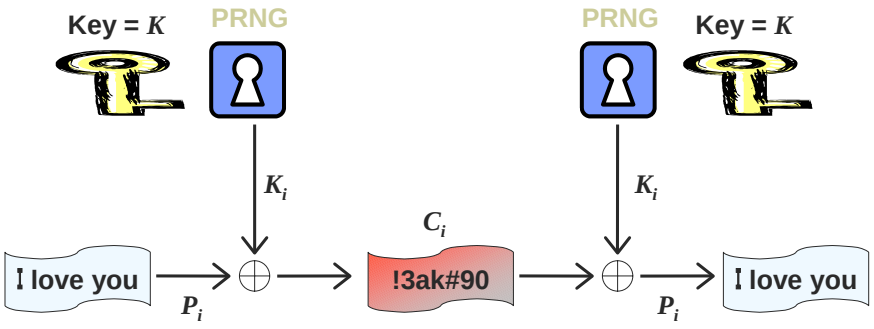
ところが、ここに落とし穴があった。IVは24ビットしかなく、連続して通信を行っていると早くて数時間で1巡してしまう。また、無線LANで送信されるパケットの最初の部分はつねに同じパターンが使われているのである。つまり、IVが何巡かするまでパケットを監視しつづけていれば、暗号鍵が解読できてしまうのだ。

（C誌、2004年9月）

誤解と現実

- いわゆるIVの衝突（コリジョン）に関する誤解
- ストーリーとしては分かりやすい
  - i.e.「24ビットは短すぎたので、WPAでは48ビットにしたのさ！　だからWPAは安全なのよ。」
- 実際は、
  - IVが衝突しても壊滅的（e.g. WEP鍵を解き明かす）なことが起こるわけではない
  - ただ、衝突はできる限り起こらないほうが望ましい

Stream Cipher



Property 1: If $C_i = P_i \oplus K_i$ Then $P_i \oplus C_i = K_i$

Property 2: If $C_1 = P_1 \oplus K_a$ and $C_2 = P_2 \oplus K_a$
Then $C_1 \oplus C_2 = (P_1 \oplus K_a) \oplus (P_2 \oplus K_a) = P_1 \oplus P_2$

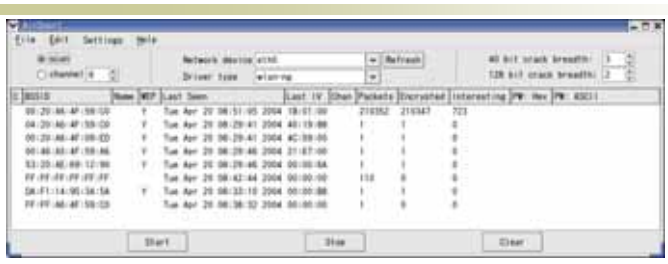
同じIVを使うと何が起こるか？

- WEP鍵は変わらない（前提）
- 同じIVを使うと、同じキーストリーム(KS)が生成される
- $(M_1 \oplus KS) \oplus (M_2 \oplus KS) = M_1 \oplus M_2$
  - M_1 がわかるわけでもなければM_2 がわかるわけでもない
  - ましてやWEPキーがわかるわけではない
  - 多少、M_1やM_2に関する情報は得られる

本当の脅威 ～ FMS 攻撃 ～

- S. Fluhrer, I. Mantin, A. Shamir, *Aug. 2001*
- Key Recovery 攻撃
- 条件
  - 生成される RC4 stream の最初のバイトが判っていて、
  - IV がある種の条件を満たす場合、Key Byte を5%の確率でguessできる
    - 代表的 Weak IV: (*B*+3, 0xff, *N*)
- key の長さに比例しかしない！
- 4,000,000 ～ 6,000,000 パケットで 40bit WEP を解読できる
- 更なる最適化で 1,000,000 パケット程度で解読可能
  - 5Mbps, 200 bytes/packet で、3125 秒

WEP Cracking Tools



AirSnort
http://airsnort.shmoo.com

bsd-airtools (dwepcrack)
http://dachb0den.com/projects/bsd-airtools.html

多くの人は・・・

- 多くの人は、以下の二つの問題：
  - IVが比較的簡単に一巡してしまう
  - Weak IVを使って暗号化されたフレームを沢山集めるとWEP鍵をリカバーできてしまう
- をゴッチャに理解している！

ほんと？？

さらに、WEPが利用しているRC4と呼ぶ関数では256バイトごとにRC4ストリームが初期化される。つまり、一つの電文内でN + (256 × c) バイト目（ただし c ≧ 0）は同じ値のキーストリームで暗号化されているのだ。従って、これらの内の1バイトでも分かれば他のバイトもすべて割り出せてしまう。

（D誌、2003年4月）

もちろん

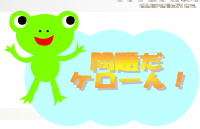
- そんなことはない！
  - もし、そんなことになっていたら怖くてインターネットショッピングなんてできない

SSL 保護つき (128ビット)

RC4 は脆弱か？

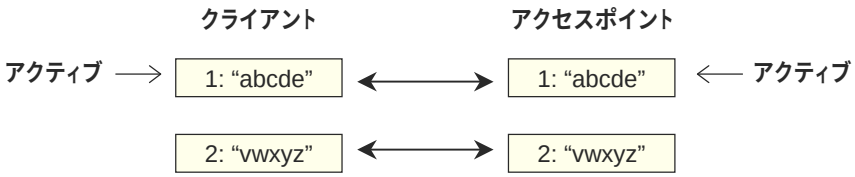
- 若干の脆弱性はあるが、一般的にはほとんど問題ない
- WEP が脆弱なのは RC4 の使い方を少々間違えたからである
- RC4 を正しく使えば安全
  - セッション毎に (相関関係の無いように) キーを変える
    - 例) SSL / TLS
  - 最初の数百バイト (例えば 256 バイト) を捨てる
    - 例) GTK over EAPOL

なぜ WEP 鍵は4つあるの？



- 多くのアクセスポイントは WEP 鍵を4つ設定することができる
  - 1つでも動くの？
  - 4つ設定したほうがより安全？

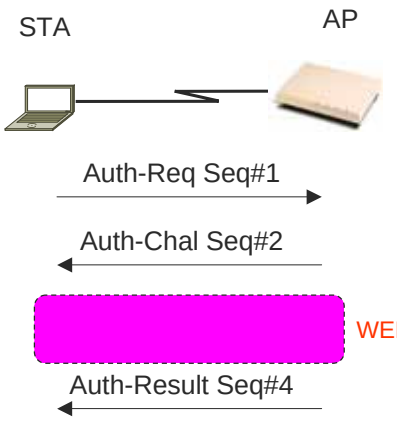
答： 鍵の変更をしやすくするため



1) クライアント、アクセスポイント共に 1: “abcde” で通信している。
2) アクセスポイントに 2: “vwxyz” を追加（ただし、まだ、アクティブな鍵は 1: のまま）。
3) クライアントに 2: “vwxyz” を追加し、アクティブな鍵を 2: に変更。
4) 全てのクライアントで 3) までの設定が終了したら、アクセスポイントのアクティブな鍵を 2: に変更。
5) アクセスポイント＆全てのクライアントが 2: “vwxyz” で通信しているので、鍵 1: “abcde” を削除（この時点で鍵 1: “abcde” から鍵 2: “vwxyz” への変更が完了！

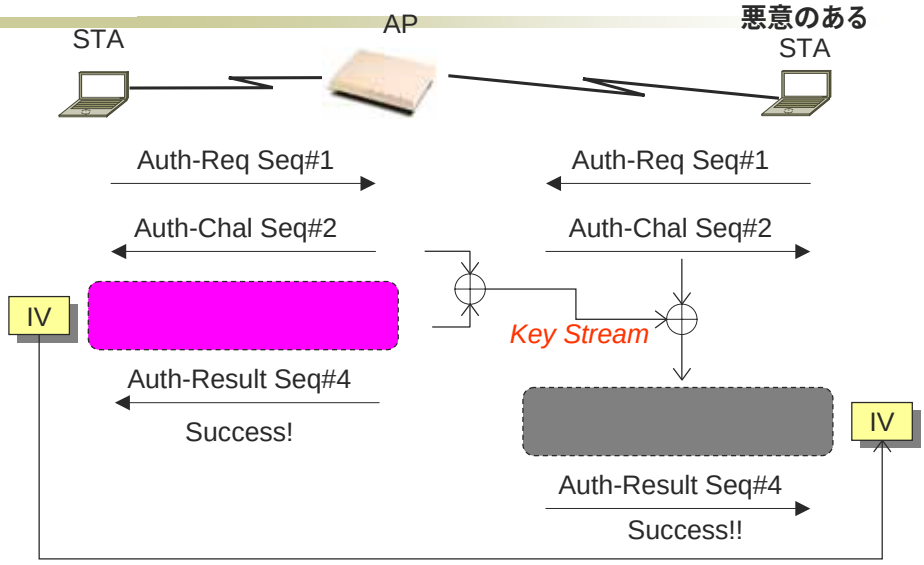
アクセスポイントでの認証

802.11 の認証



- WEP を使う！
  - AP は Challenge (128bytes) を送出
  - STA はそれを WEP で暗号化して AP へ送る
  - AP はそのフレームの整合性をチェック

こらあかん・・・



結論

- “する (シェアードキー認証) ” より “しない (オープン認証) ” ほうが安全！
- WPA / 802.11i ではオープン認証を使うことになっている

WEP おさらい

- 何をしていた？
  - 秘匿性 (Confidentiality)
  - 完全性 (Integrity)
  - 認証 (Authentication)
- 実際に
  - What on Earth does this Protect?

WPA の目標

- 暗号的脆弱性の排除
- ユーザーベースの認証
- 鍵の配布をサポートすること
- 動的なユーザー･セッション･パケット毎の鍵を使用
- 認証サーバーを強要しないこと
- 2003年中に利用可能になること
- ソフトウェアアップグレード可能

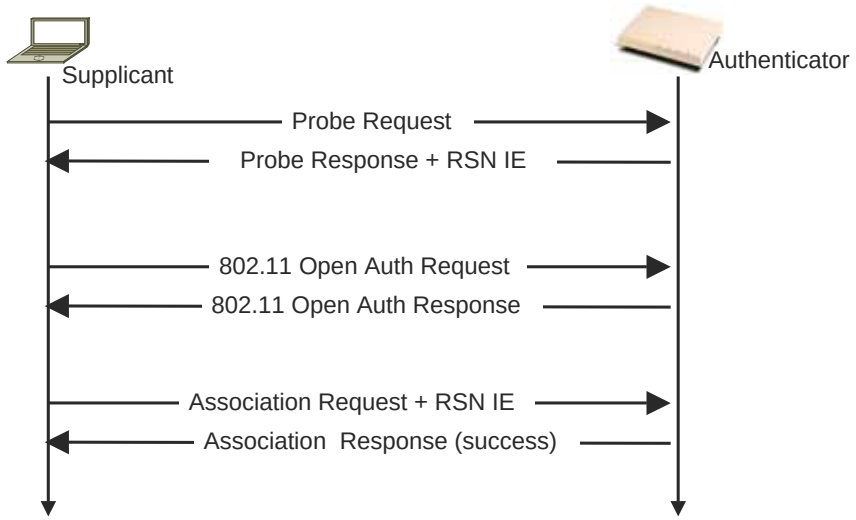
WPA (Wi-Fi Protected Access)

- 802.11i のサブセット
- 認証
  - 802.1X + EAP
- 秘匿性 (暗号化)
  - 802.1X 動的鍵配布
  - TKIP
- 完全性
  - Message Integrity Check (MIC) “Michael”

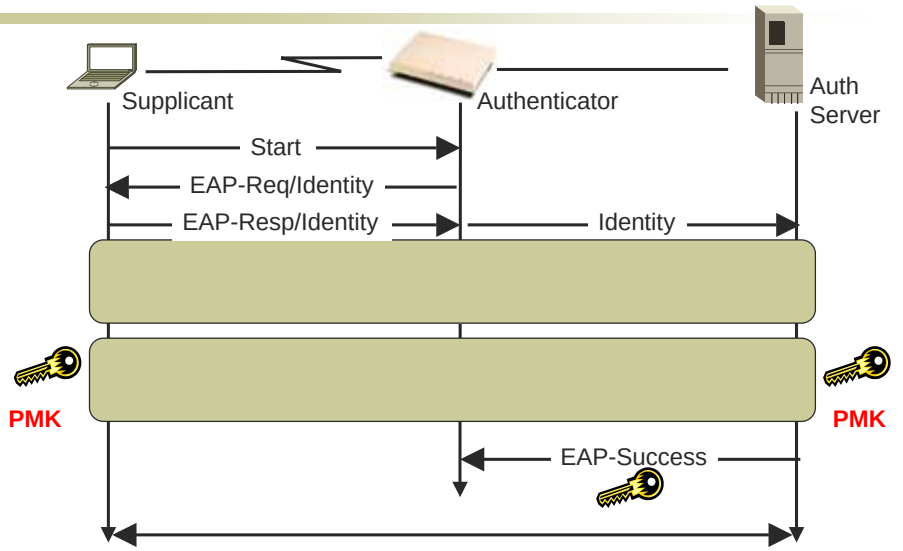
WPA ステップ

- アソシエーションとケーパビリティーの確認
- 802.1X 認証と PMK (Pairwise Master Key) の配布
- TK (Temporal Key) の導出
- GK (Group Key) の導出
- 暗号化および整合性チェック

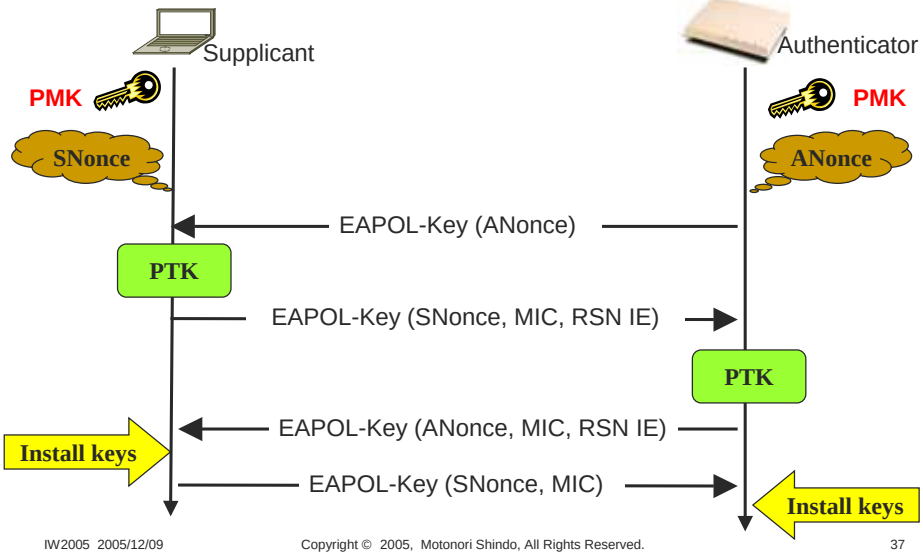
アソシエーションとケーパビリティーの確認



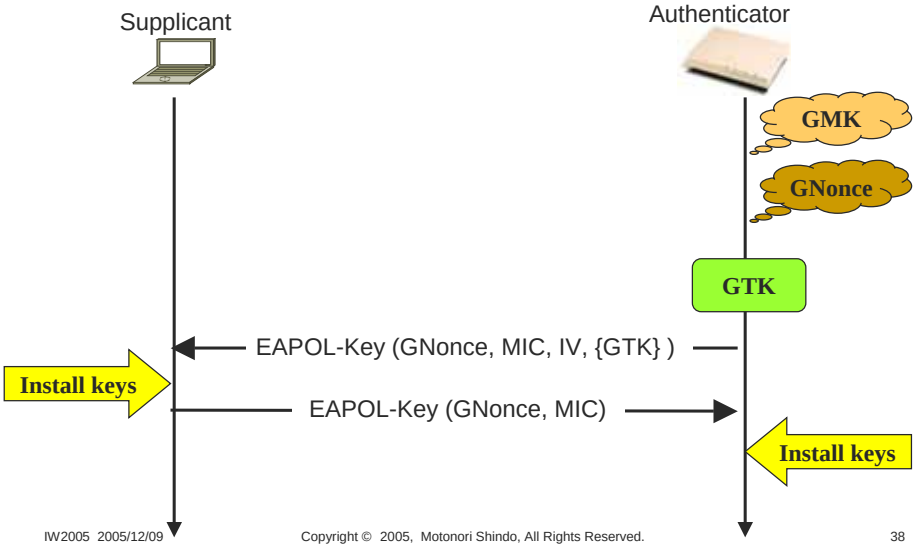
802.1X 認証と PMK の配布



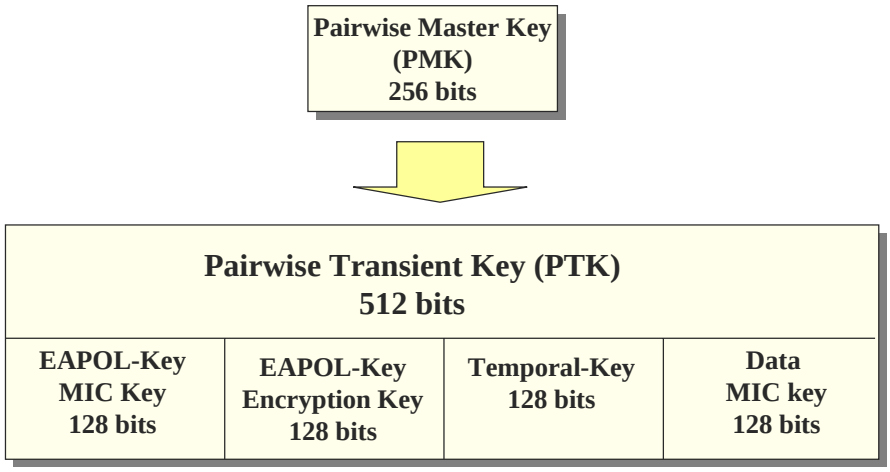
Temporal Key の導出 ～ 4 way handshake ～



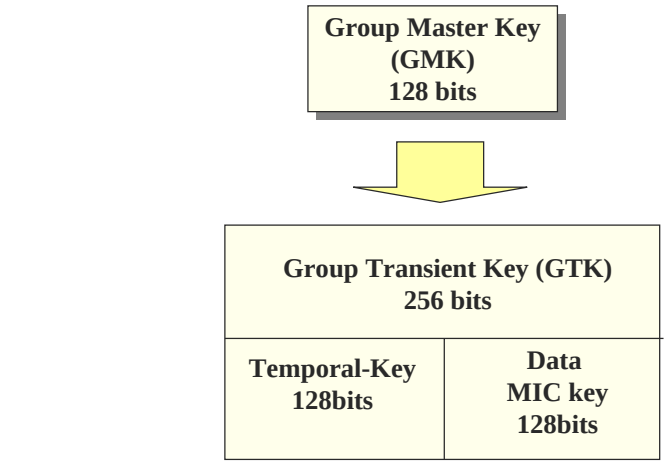
Group Key の導出 ～ 2 way handshake ～



Pairwise Key Hierarchy (for TKIP)



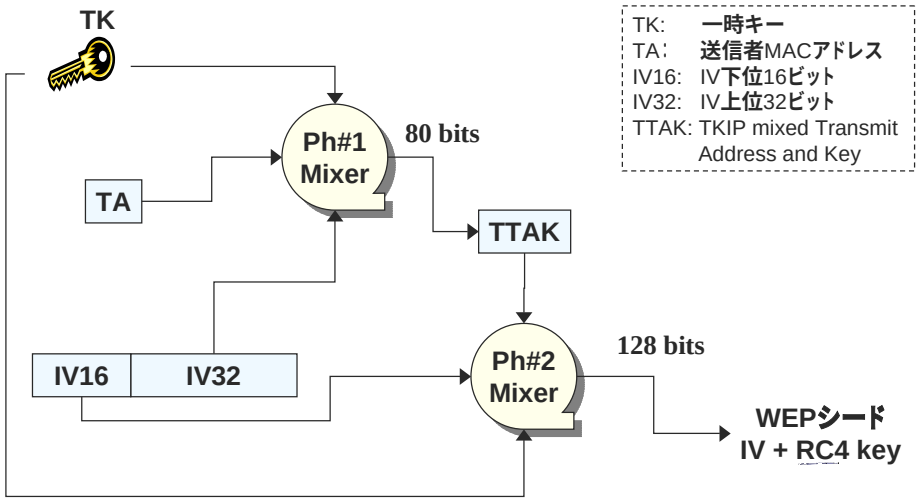
Group Key Hierarchy (for TKIP)



TKIP (Temporal Key Integrity Protocol)

- IV **空間の拡張** (24 -> 48 bits)
- IV **シーケンス処理の規定**
- Per-packet-mixing Function
- Michael MIC (Message Integrity Code)

Per-packet-mixing function



PreShared Key (PSK) Mode

- RADIUS を使用しない（用意できない）場合を想定
  - ホームユース
- 802.1X で実現していた部分を手動設定で代替
  - 認証
  - PMK の配布
  - 802.1X 以降の動き(4 and 2 way handshake, 鍵の導出、TKIP、等) は non-PSK 時と同様
- PMK (256bits) を AP, STA 双方に設定

典型的WPA(TKIP) の説明

TKIPはWEPの暗号化技術をより発展させ、一定時間ごとに自動的に暗号キーが変更されるしくみを持つ。

（B誌、2004年9月）

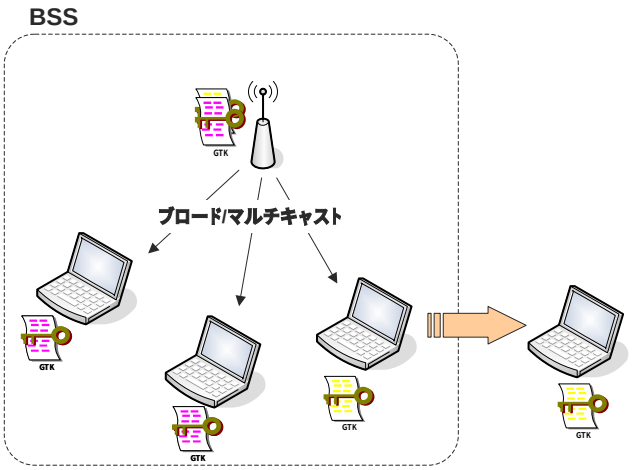
TKIPの設定画面

確かにWPA(TKIP)には鍵の更新間隔に関するパラメータが追加されている！

鍵の更新

- 鍵を更新するって、どの鍵よ？？
  - PMK?
    - **多くの人はこれであると思っているのでは！？**
    - でも、PSKの時だって鍵の更新はできるでしょ！
  - PTK?
    - 4-Wayハンドシェークからやり直しても、変わるのはNonceだけだし。。
  - TK?
    - PTKから計算で導出されるので、更新するタイミングないし。。
  - …

更新の必要があるのはGroup Key！



Group Key 更新のタイミング

- 本来はクライアントがBSSから去ったらGroup Key を更新すべき！
- しかし、それではオーバーヘッドが大きいので、
  - 一定時間経ったら更新する
  - 一定のパケット数そのGTKを使ったら更新する

というのもアリ

鍵更新に関する誤解

- 多くの人は（鍵の安全性劣化を防ぐために）一定時間ごとに鍵（のおおもと=PMK）を更新すると思っている（ハズ）
  - 説明としては分かりやすい
    - FMS攻撃は沢山パケットを集めなければいけない
    - 沢山パケットを集められる前に鍵を変えてしまえ！
    - WPA（TKIP）は一定時間で鍵を更新するので安全
  - しかし、これは802.1Xで既にやっていた（できていた）ことである！

ほんとのところは

- WPA（TKIP）の鍵の更新は、鍵の劣化を防ぐためではなく、本質的に必要だから存在する！
- しかも、マルチ/ブロードキャストの通信に関連するもので、ユニキャストには無関係。

これも・・・

そして、その後はTKIP (Temporal Key Integrity Protocol) という暗号化方式でやり取りする。これは先ほどのWEPとは違い、一定時間ごとに暗号化のための鍵を変更する。

(A誌2004年9月)

これはぎりぎり合格点？

TKIP

Temporalの名の通り、一定時間ごとに暗号鍵を変更するプロトコルです。パケットごとの鍵更新、IV鍵の48bit化などにより、従来のWEPが持っていた脆弱性を克服しています。

(ベンダーAのホームページ)

かなりの混乱が・・・

- WPAの特徴
  - ユーザーパスワード WPA-PSK (Pre-Shared Key) を128bitとする
  - IV を24bitから48bitとする
  - 暗号鍵は WPA-PSK と IV、MAC アドレスからハッシュ値を持って生成する
  - 1万パケット毎に暗号鍵の更新を行う

(Web上の記事A)

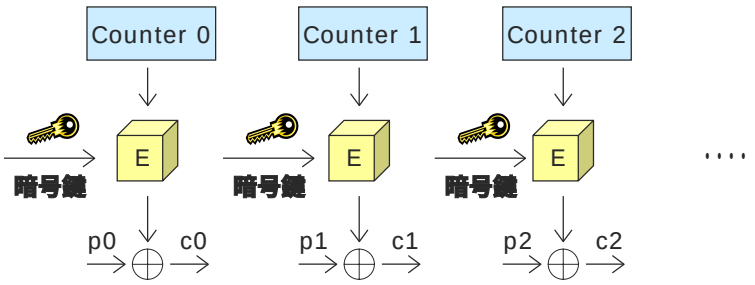
IEEE 802.11i

- 802.11iは2004年6月に正式規格として成立
- CCMP (Counter-mode with CBC MAC Protocol)
  - AES が前提
  - TKIP はオプション扱い
- その他の部分はほぼ WPA と同様だが、若干の機能追加あり
  - PMK caching
  - Pre-authentication

CCMP

- Counter-mode CBC-MAC Protocol
  - AES を “Counter mode” で使用
  - AES で “CBC-MAC” も計算
- **暗号化と整合性検証を同時に実現する！**
- RFC 3610

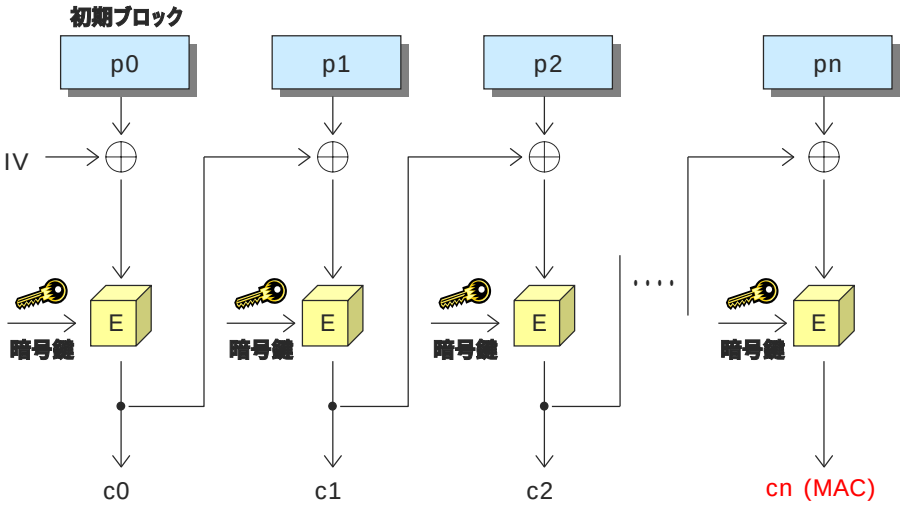
Counter-Mode



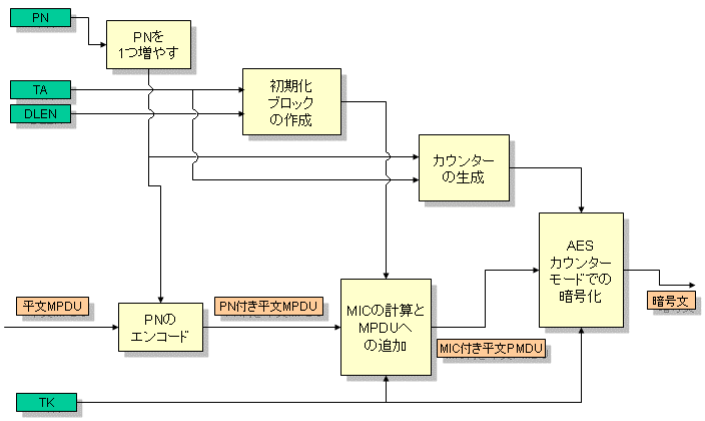
- 復号化も全く同じプロセスで良い
- 並列化可能
- ランダムアクセス
- 事前に計算しておける
- メッセージはブロックサイズに依存しない

- 暗号化だけあればよい
  - AESは暗号化と復号化は異なる

CBC-MAC



CCMP Encapsulation 処理の流れ



WPA2

- WPA2 は 802.11i の相互接続性を WiFi Alliance が具体化し、認定するもの
  - WPA2 で認定されているものは 802.11i に準拠したものとなる
- 2004年9月から認定作業を開始
  - 現在、約50数社が認定をパスしている (Personal & Enterprise)
    - 昨年の同時期は10社程度だった
  - ほとんどの “新” 製品はサポート

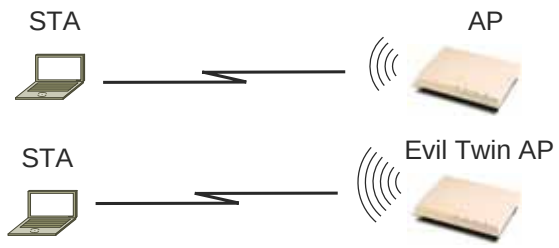
WEP, TKIP and CCMP

	WEP	TKIP	CCMP
暗号化アルゴリズム	RC4	RC4	AES
暗号鍵の長さ(bits)	40 / 104 / 128	104	128
認証鍵の長さ(bits)	N / A	64	64
IV の長さ(bits)	24	48	48
データ部の完全性	CRC32	Michael	CCM
ヘッダ部の完全性	なし	Michael	CCM
Anti-Replay-Attack	なし	あり	あり

不正アクセスポイント (Rogue Access Point)

- 2つのタイプ
  - きちんと設定されずにネットワーク管理者に無断で設置したアクセスポイント
    - 踏み台になる可能性
  - 正当なアクセスポイントにみせかけ、クライアントを接続させ、情報を入手したり悪意のある行為をおこなう
    - 通称 “Evil Twin” (悪魔の双子)

Evil Twin



- より強い電波を出すAPを設置
  - 新しいクライアントはそちらに associate する

逆 war driving

- Evil Twin を搭載した車で、クライアントを “釣りに” 行く

何が恐怖か？

- 通信を傍受されることが恐怖ではない
- 多くの公衆無線LANサービスでは、接続時に強制ポータルで、ユーザーID / パスワードを求められる
  - ユーザーは他でも同じユーザーID / パスワードを使う傾向にある
- さらに積極的な攻撃の可能性も
  - 悪意のあるコードをダウンロードさせる、etc.

お手軽キットも存在する

- Airsnarf
- **構成要素**
  - Linux, httpd, dhcp, sendmail, iptables, Perl DNS module
- **どのように動いているか？**
  - **自分自身** or **自分配下の** AP **に** associate **させて、**
  - dhcp **で** IP **アドレス、**DNS **サーバー、デフォルト･ゲートウェイを割り当て、**
  - **どの** URL **も自分に** resolve **するようにし、**
  - **自分の** httpd **(強制ポータルページ) に接続させ、ユーザー** ID / **パスワードを入れさせ、**
  - **それをメールで管理者に通知する！**

Evil Twin **攻撃をどのように防ぐか**

- 802.1X **で、きちんとした認証を行う**
  - **ほんとうに十分だろうか?**
- **それが出来ない場合は、ユーザーが最大限の注意を払う**
  - **前回のログイン日時に注意する**
  - **接続されたAPのMACアドレスを確認**
  - **見覚えの無いポータル画面に注意する**
- **もう少しクライアント側に工夫があってもよいのではないか？**
  - **接続** AP **の** MAC **アドレスのホワイトリスト**
  - SSID **の変化**
  - AP **の** MAC **アドレスの変化**
  - **デフォルトゲートウェイの** MAC **アドレスの変化**
  - **急激な電波強度の変化**

さて、

- みなさんは100点取れましたか?
- 80点以上なら合格です！
- 60点以下の場合は補習です！ (ウソ)
- 正しく理解することは、そう難しい事ではない
- “知らない/理解していない” ことを知ることが大切！
  - 伝える側の責任＆伝えられる側の好奇心

略語一覧

AES	Advanced Encryption Standard
AP	Access Point
CBC	Cipher Block Chaining
CCMP	Counter-mode CBC MAC Protocol
CFB	Cipher Feedback
CRC32	Cyclic Redundancy Check 32bits
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
ECB	Electronic Code Book
ESS	Extended Service Set
FCS	Frame Check Sum
GK	Group Key
GMK	Group Master Key
ICV	Integrity Check Value
IE	Information Element
IV	Initialization Vector
LCG	Linear Congruential Generator
LEAP	Lightweight EAP
MAC	Message Authentication Code
MD5	Message Digest 5
MIC	Message Integrity Code
OFB	Output Feedback
PAE	Port Authentication Entity
PBKDF	Password-Based Key Derivation Function
PEAP	Protected EAP
PKCS	Public Key Cryptographic Standard
PMK	Pairwise Master Key
PPP	Point-to-Point Protocol
PRF	Pseudo Random Function
PRNG	Pseudo Random Number Generator
PSK	PreShared Key
PTK	Pairwise Transient Key
RADIUS	Remote Access Dial-Up System
RC4	Rivest Code (or Cipher) 4
RSN	Remote Secure Network
SHA1	Secure Hash Algorithm 1
SSID	Service Set Identifier
STA	Station (client)
TA	Transmit (MAC) Address
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTAK	TKIP-mixed Transmit Address and Key
TTLS	Tunneled TLS
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WRAP	Wireless Robust Authenticated Protocol
XOR	Exclusive OR