Bezpieczeństwo w sieciach bezprzewodowych standardu 802.11

KRZYSZTOF GIERŁOWSKI

WEP (Wired Equivalent Privacy)

Podstawowy protokół bezpieczeństwa zdefiniowany w standardzie IEEE 802.11b.

Podstawowe cele WEP:

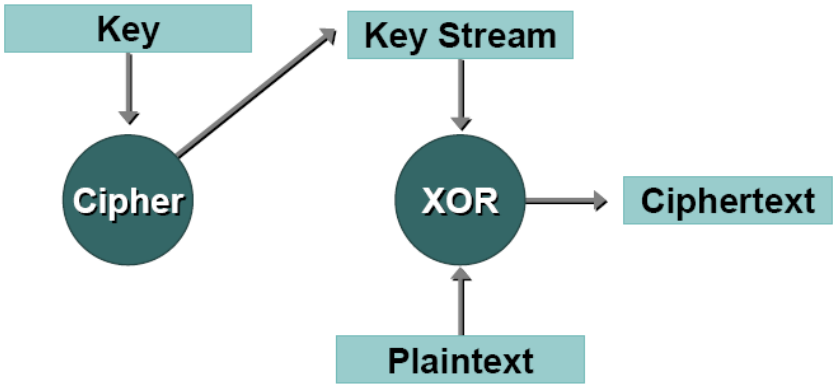
- ochrona informacji w warstwie łącza danych,
- zapewnienie bezpieczeństwa na poziomie co porównywalnym z bezpieczeństwem sieci przewodowych.

Elementy bezpieczeństwa:

- uwierzytelnienie,
- integralność,
- poufność,
- niezaprzeczalność.

Poufność – koder strumieniowy RC4

- XOR jawnej informacji ze strumieniem klucza
- strumień klucza generowany jest przez szyfr RC4
- koder strumieniowy RC4 jest niedostosowany do transmisji pakietowej
- nie można wygenerować dowolnego bitu klucza w czasie O(1)



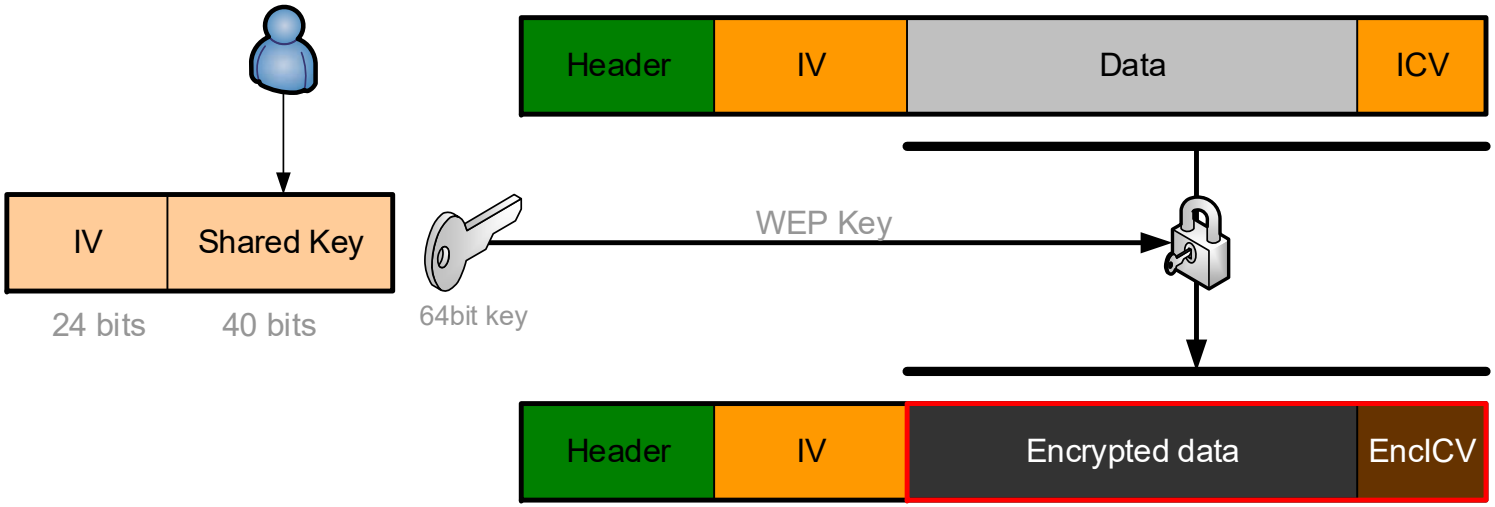
Wiadomość	0	1	1	0	1	0	0	1
	XOR							
Ciąg szyfrujący	1	1	1	0	1	1	0	1
W. zaszyfr.	1	0	0	0	0	1	0	0

W. zaszyfr.	1	0	0	0	0	1	0	0
	XOR							
Ciąg szyfrujący	1	1	1	0	1	1	0	1
Wiadomość	0	1	1	0	1	0	0	1

Generacja klucza szyfrującego

Dla każdej ramki należało generować strumień szyfrujący od nowa = takie same strumienie przy stałym kluczu.

Aby zróżnicować ciągi szyfrujące dodano do klucza IV, który następnie przesyła się wraz z zaszyfrowaną ramkę.



Koder strumieniowy RC4 + IV

Należy unikać ponownego użycia wektora IV

k – klucz tajny (stały), v – wektor inicjalizacyjny

Ramka 1:
$C1 = P1 \oplus RC4(v,k)$

Ramka 2:
$C2 = P2 \oplus RC4(v,k)$

$$C1 \oplus C2 =$$

$$=(P1 \oplus RC4(v,k)) \oplus (P2 \oplus RC4(v,k))=$$

$$= P1 \oplus P2$$

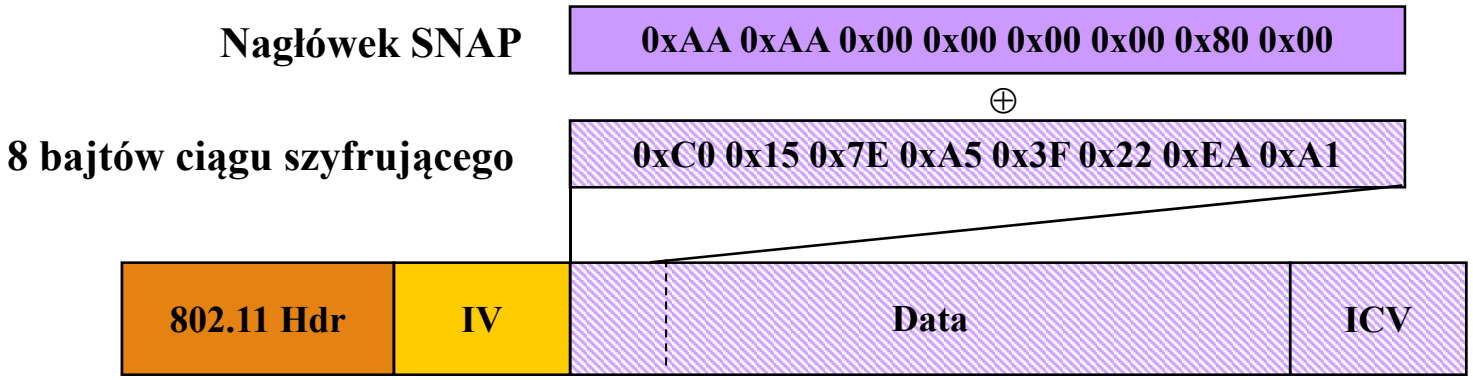
Wektor IV

Standard nie precyzuje sposobu wyboru IV

Różne implementacje:

- **stały IV** – wymaga zmiany tajnego klucza przy każdej ramce,
- **rosnący IV** – skutkuje ponownym użyciem klucza szyfrującego gdy dwie stacje wyślą po jednej ramce,
- **losowy IV** – po ~4800 ramkach, prawdopodobieństwo ponownego wystąpienia klucza wynosi 50%, czyli należy zmieniać tajny klucz co około 3 s.

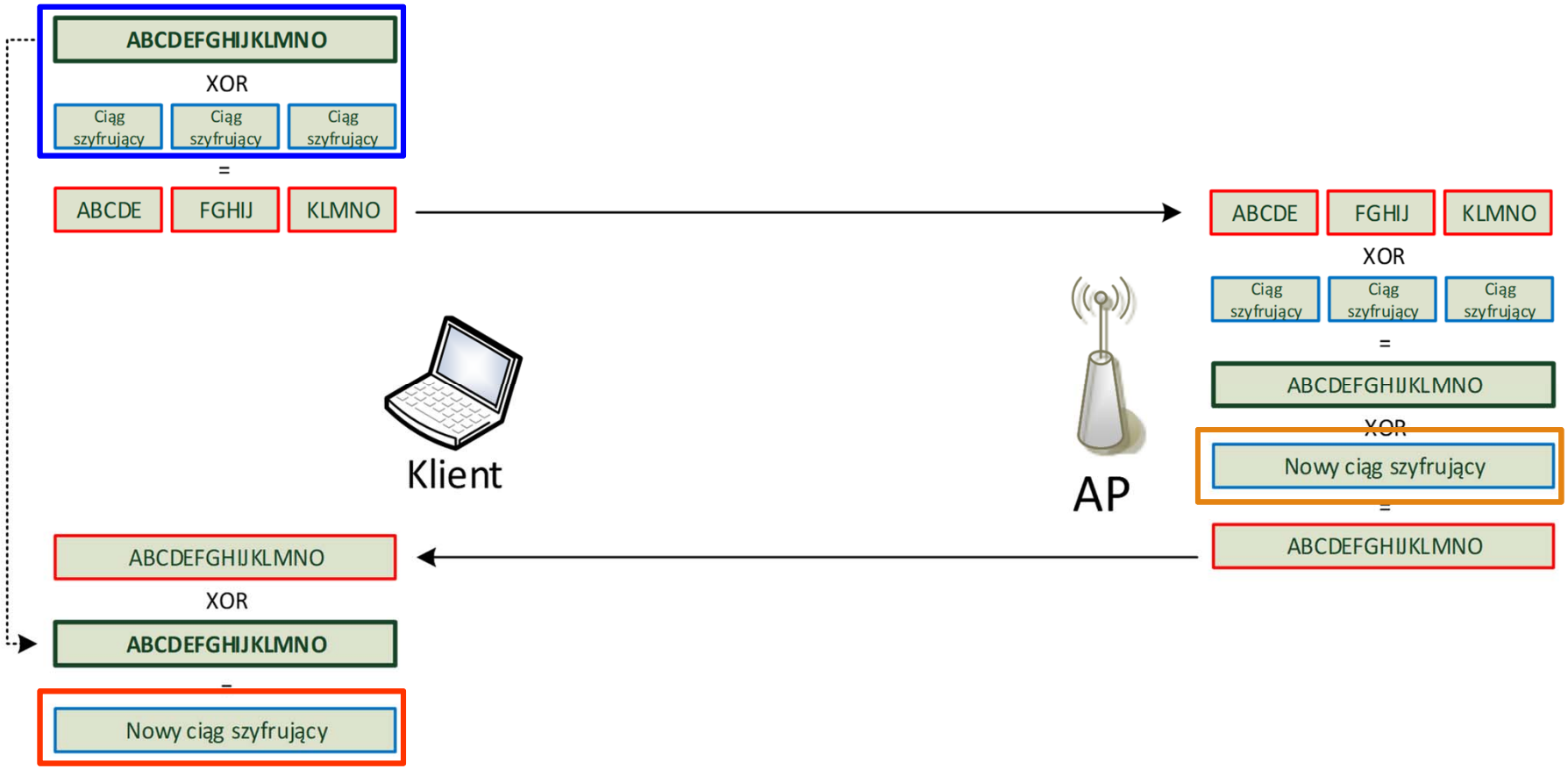
„Słabe” klucze WEP



- Wartość pierwszych bajtów pola danych ramki jest znana – nagłówek SNAP. Pozwala na ustalenie pierwszych bajtów ciągu szyfrującego.
- Umożliwia to zawężenie możliwych wartości klucza szyfrującego i/lub ustalenie wartości niektórych bitów.

- Ze względu na sposób tworzenia klucza szyfrującego, pojawiają się „słabe klucze” dla których układ bitów w pierwszych 3 bajtach klucza powoduje pojawianie się podobnych układów w pierwszych bajtach ciągu szyfrującego.
- Klucze te są rozpoznawalne po zawartości IV.

Fragmentation



Integralność

Do pakietów dołączana jest suma kontrolna ICV (32-bitowa funkcja kontroli CRC-32).

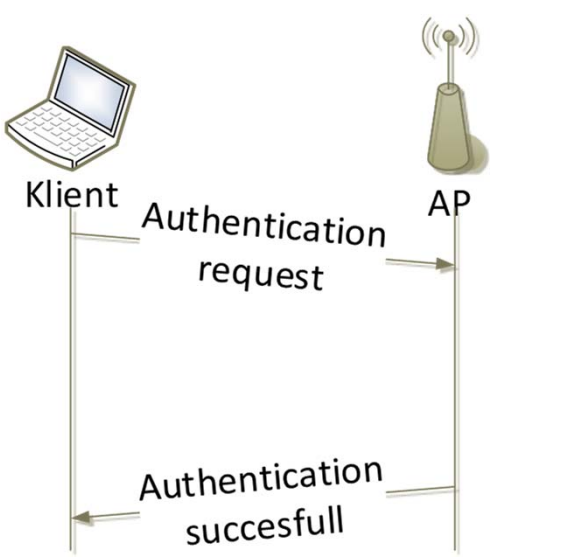
Nie jest to kryptograficzna metoda obliczania integralności danych.

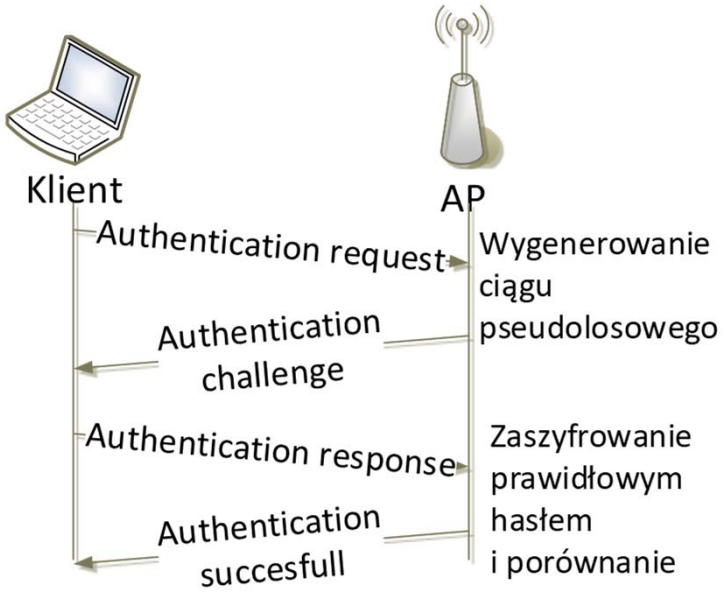
Nie obejmuje całej ramki (na przykład nagłówka).

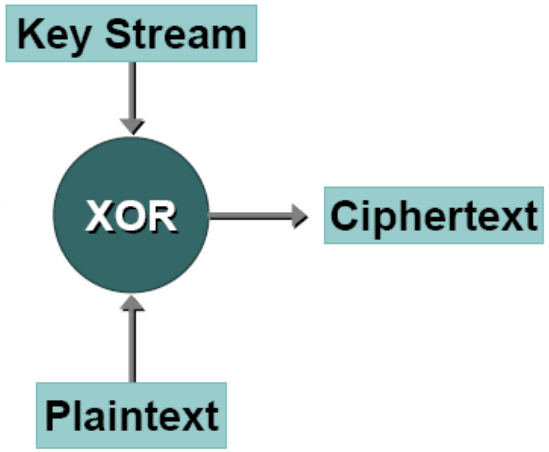
Słabości w tym elemencie protokołu pozwalają na:

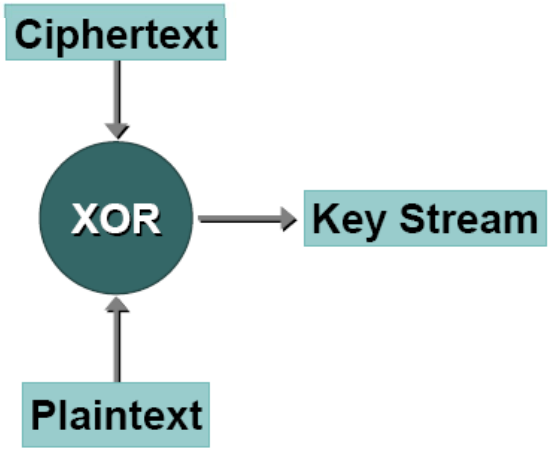
- łatwą modyfikację danych nagłówka,
- modyfikację danych bez rozszyfrowania,
- odtworzenie wcześniej zapisanego ruchu sieciowego.

WEP – Uwierzytelnianie









Wired Equivalent Privacy (WEP)

Nadawca wprowadza wspólny, stały klucz WEP (40 bitów) oraz dane do przesłania.

Nadawca oblicza ICV (CRC-32) obejmujące pole danych.

Nadawca tworzy klucz szyfrujący poprzez zestawienie wybranego wektora IV i wprowadzonego klucza sekretnego

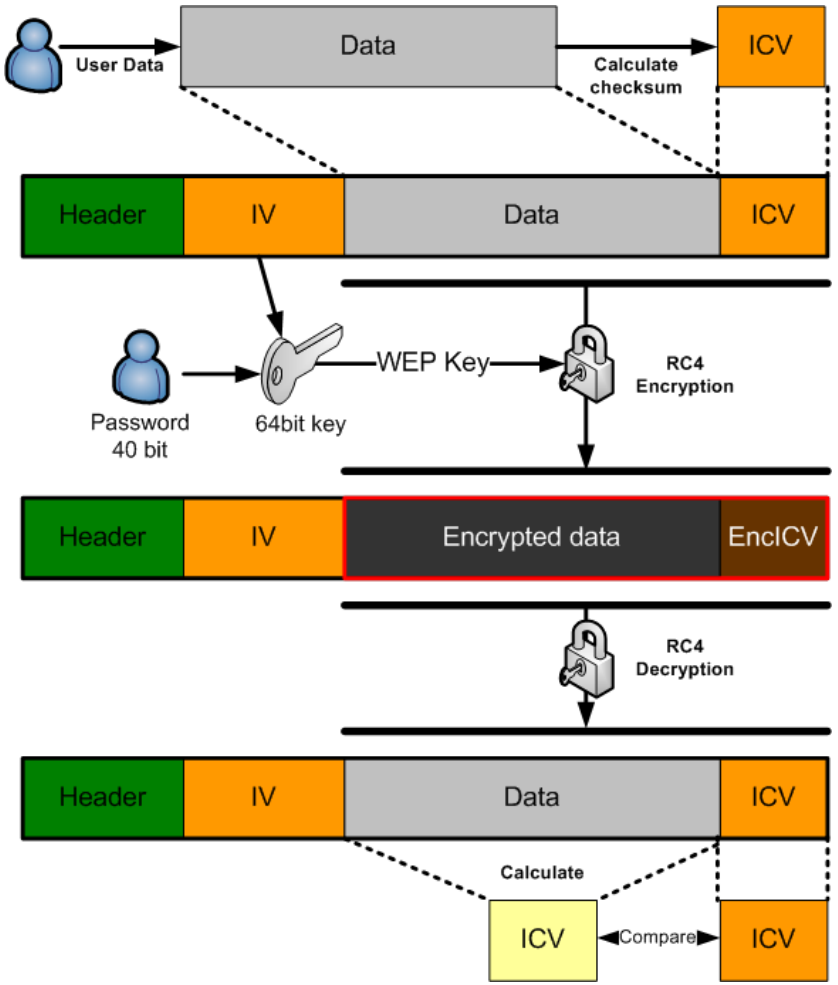
Pola danych i ICV są szyfrowane otrzymanym kluczem.

Nagłówek i IV są dołączane w postaci niezaszyfrowanej.

Odbiorca odczytuje IV z odebranej ramki i odtwarza klucz szyfrujący dzięki znajomości sekretnego klucza.

Pole danych i ICV jest odszyfrowywane, a następnie sprawdzana jest suma kontrolna.

Jeśli użyto właściwych kluczy i transmisja była bezbłędna, ramka jest przyjmowana jako prawidłowa



Ataki

Błędy w użyciu kodera RC4 powodują, że możliwe jest odczytanie sekretnego klucza po zebraniu od 20.000 (11s) do 1.000.000 ramek (10 min).

Możliwe jest odczytanie przesłanych danych bez odczytania klucza.

Ataki pasywne:

- FMS,
- SNAP header,
- IV reuse.

Active attacks:

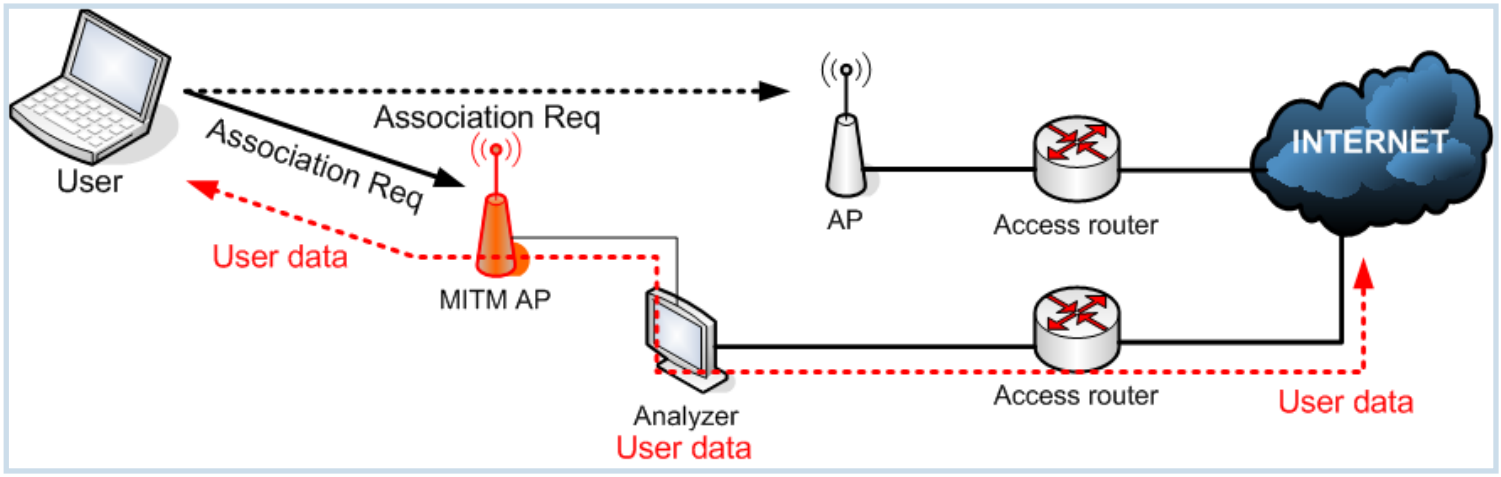
- Traffic replay,
- MAC address forging, identity hijacking,
- Man-in-the-middle,
- Bit-flipping,
- Header modification.

Man in the Middle

Klient nie jest w stanie potwierdzić tożsamości systemu bezprzewodowego.

Możliwe zastosowanie:

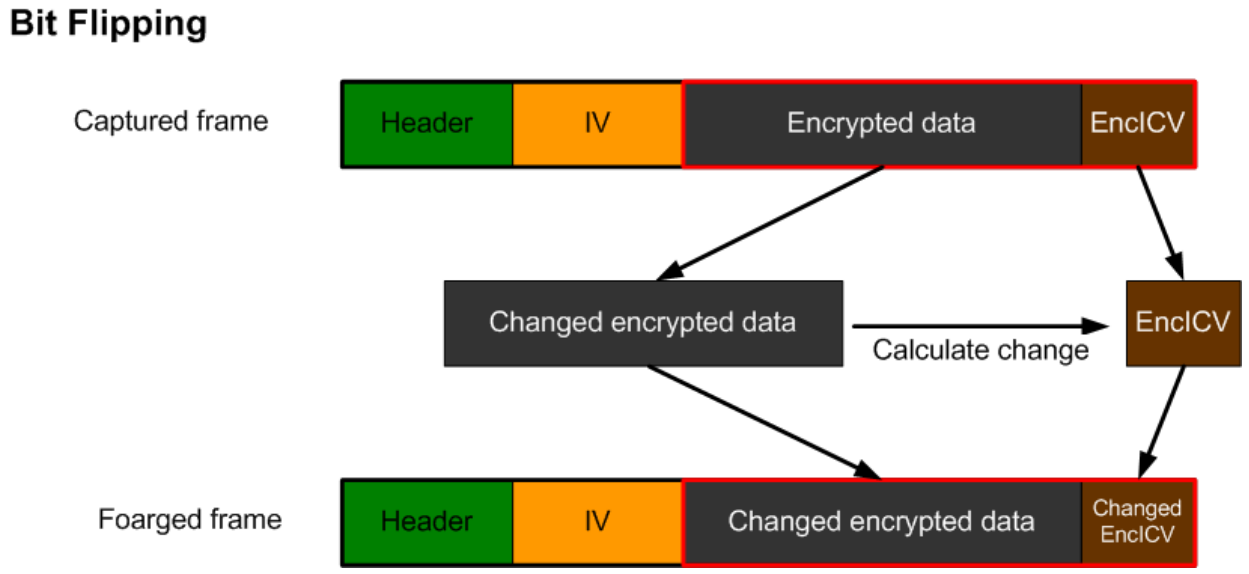
- atak Denial of Service,
- wykradzenie danych uwierzytelniających użytkownika,
- wykradzenie poufnych informacji przesyłanych przez użytkownika.



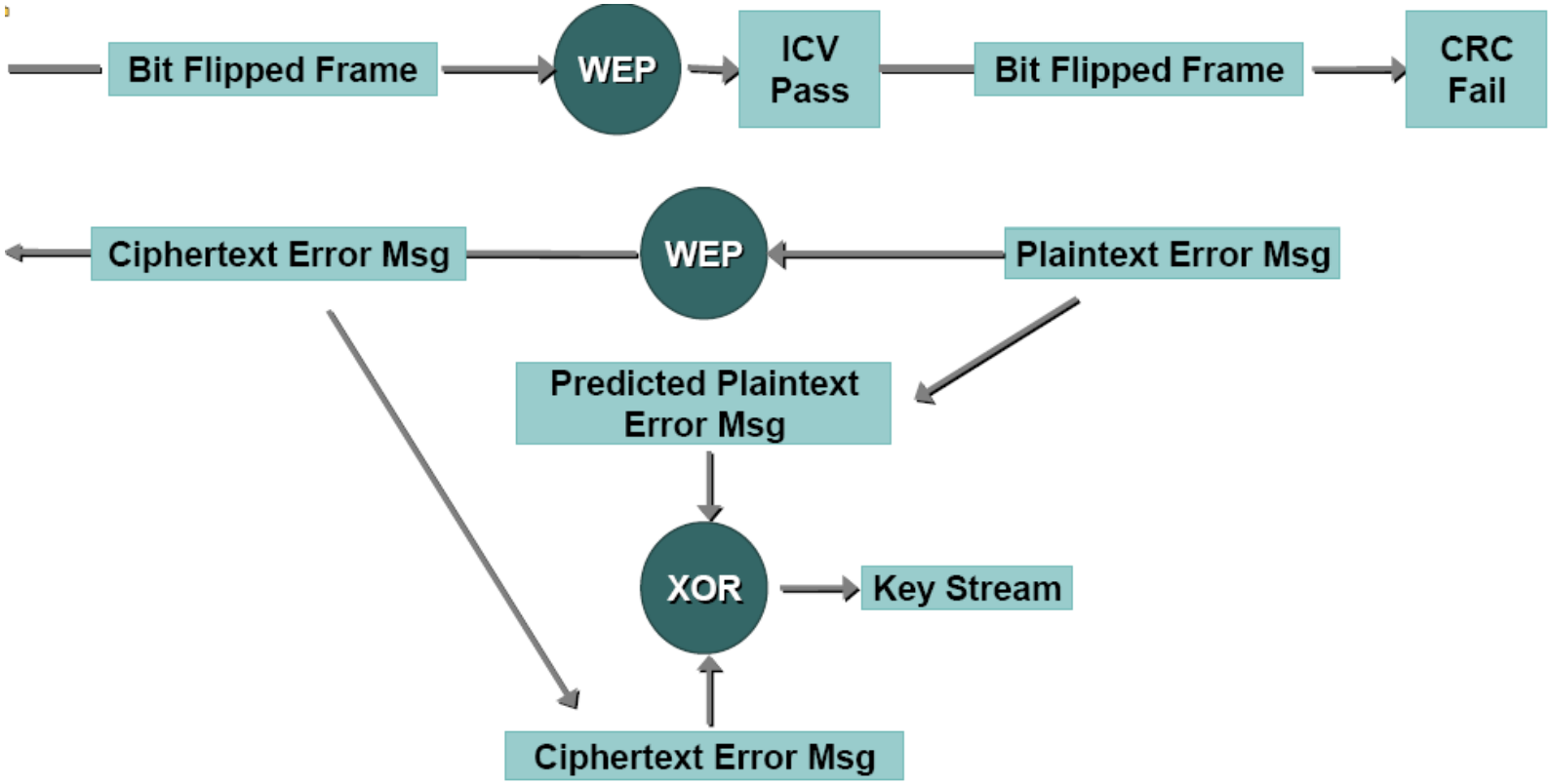
Bit Flipping

Możliwa jest modyfikacja danych bez ich rozszyfrowania.

Atak można wykorzystać jako część ataku ***Denial of Service*** lub w dla zwiększenia szans złamania klucza szyfrującego.



Bit Flipping – wykorzystanie

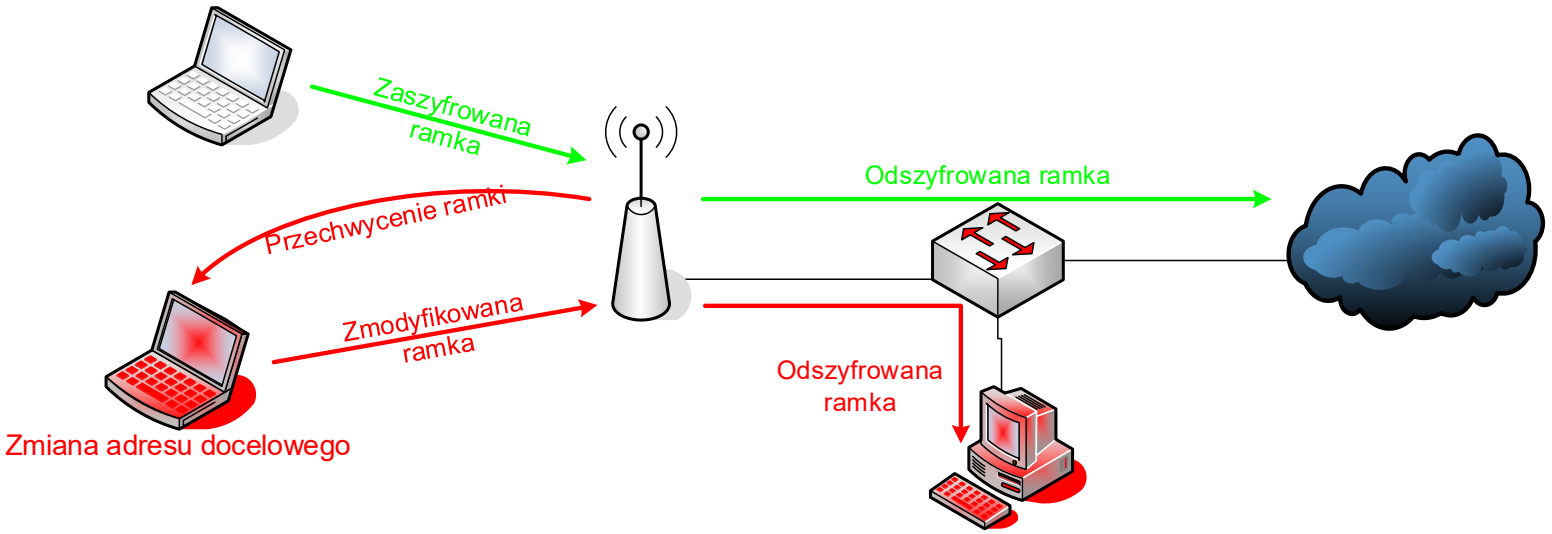


Modyfikacja nagłówka

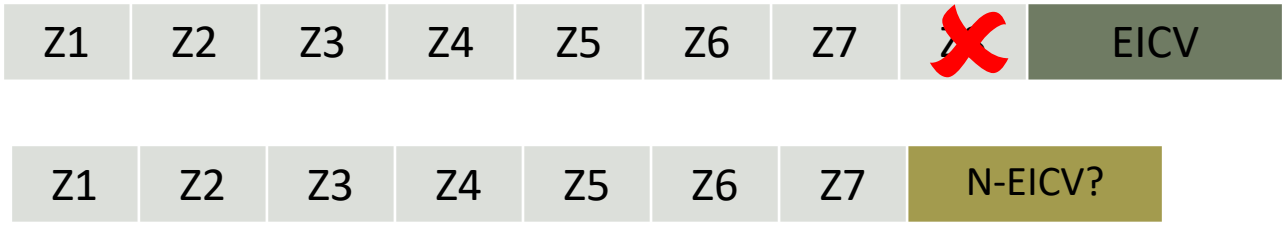
Brak ochrony nagłówka ramki umożliwia jej dowolne przekierowanie.

Brak ochrony przed retransmisją ruchu.

Można to wykorzystać, na przykład, w celu przechwycenia danych w części przewodowej.



ChopChop



Wysyłamy skróconą ramkę z różnymi N-EICV.

Jeśli trafimy na właściwe, to AP potwierdzi wysyłając ACK.

Ponieważ jedyną przyczyną zmiany jest usunięcie Z8, mając: stare EICV oraz nowe EICV, można wyliczyć D8.

Pozwalają na to słabości sumy kontrolnej – bazujemy na fakcie, że szyfrowanie zmienia wartość ICV na EICV, lecz ICV1 ⊕ ICV2 = EICV1 ⊕ EICV2

N-EICV	ACK	D8
N-EICV-0	-	00
N-EICV-1	-	01
N-EICV-...	-	...
N-EICV-3F	+	3F

Zx – zaszyfrowane bajty danych
Dx – odszyfrowane bajty danych
EICV – zaszyfrowana suma kontrolna oryginalnej ramki
N-EICV – zaszyfrowana suma kontrolna nowej ramki

Błędy projektowe WEP

Nieodpowiedni koder (strumieniowy).

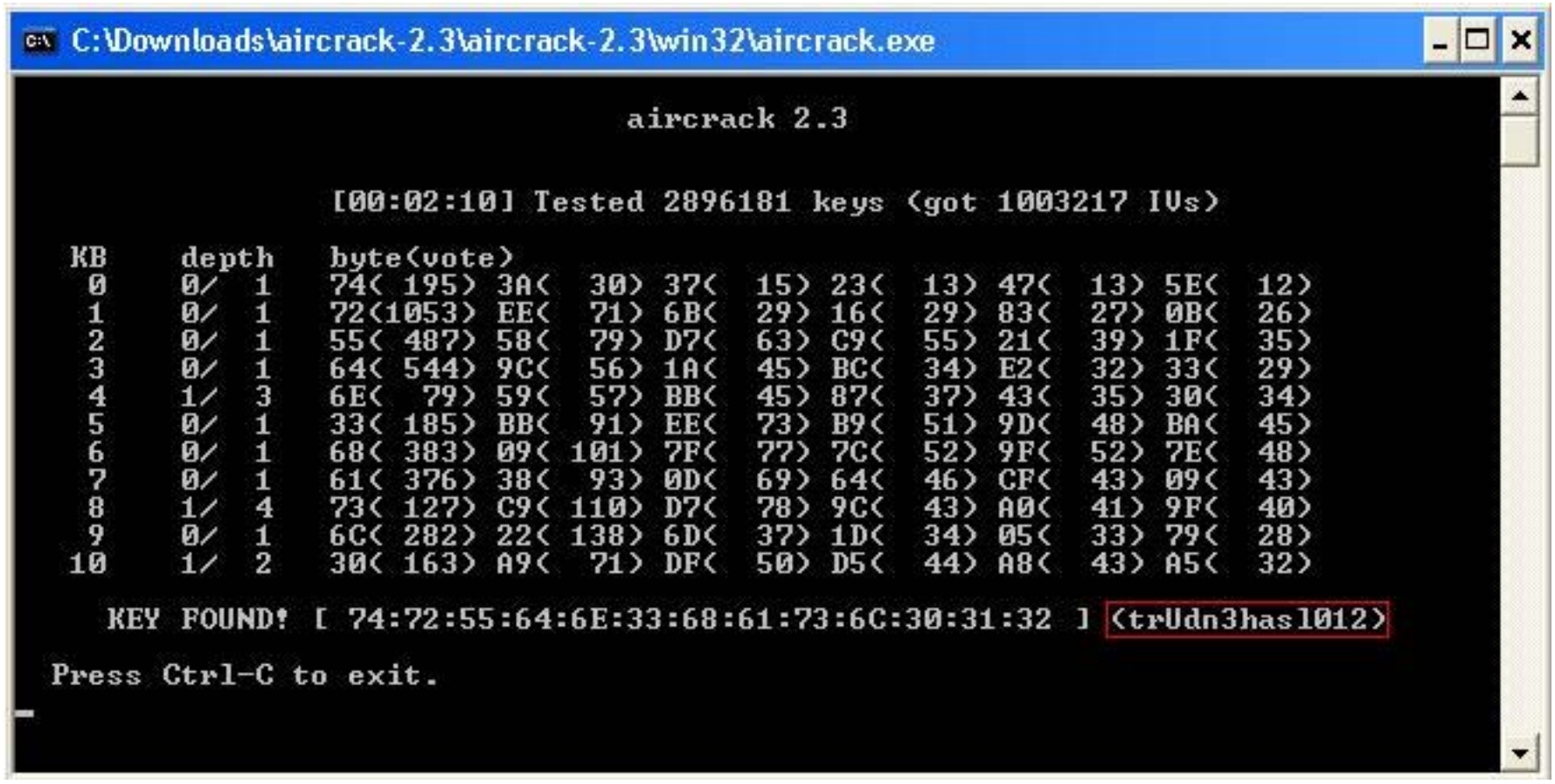
- Sposób tworzenia klucza szyfrującego.
- Długość i sposób generowania wektora IV.
- Obecność „słabych kluczy”.

Słabości mechanizmu weryfikacji integralności danych i nagłówka.

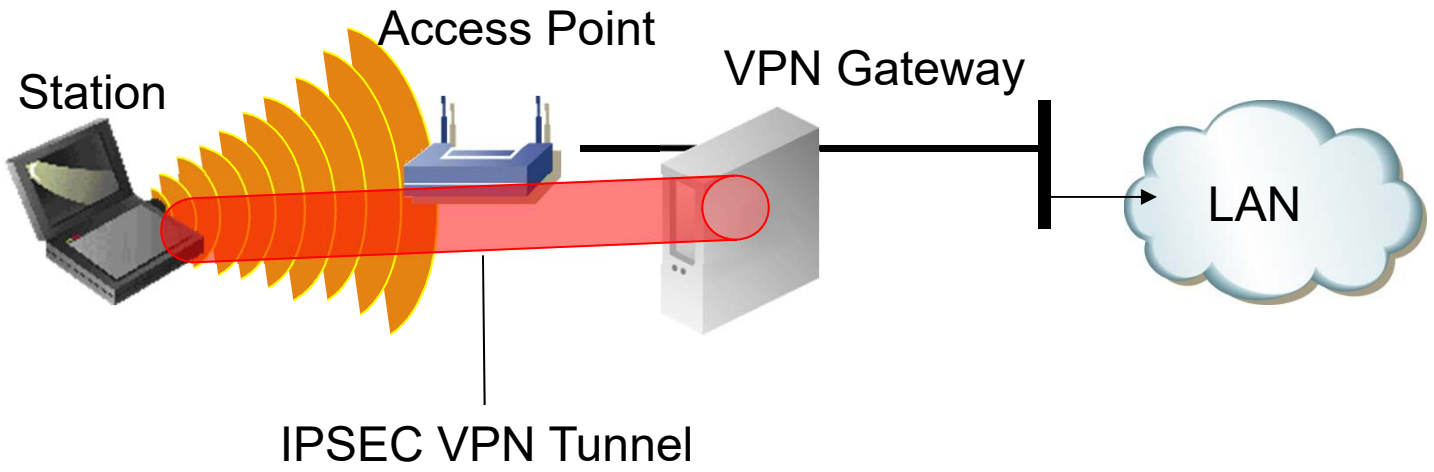
Brak wzajemnego uwierzytelniania.

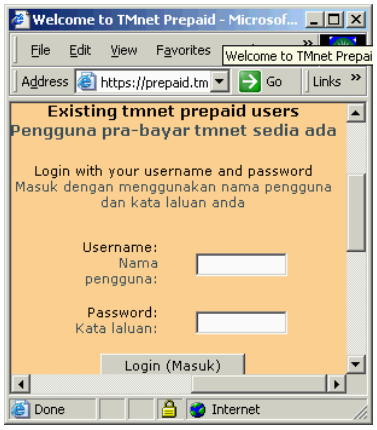
Brak zarządzania i dystrybucji kluczy.

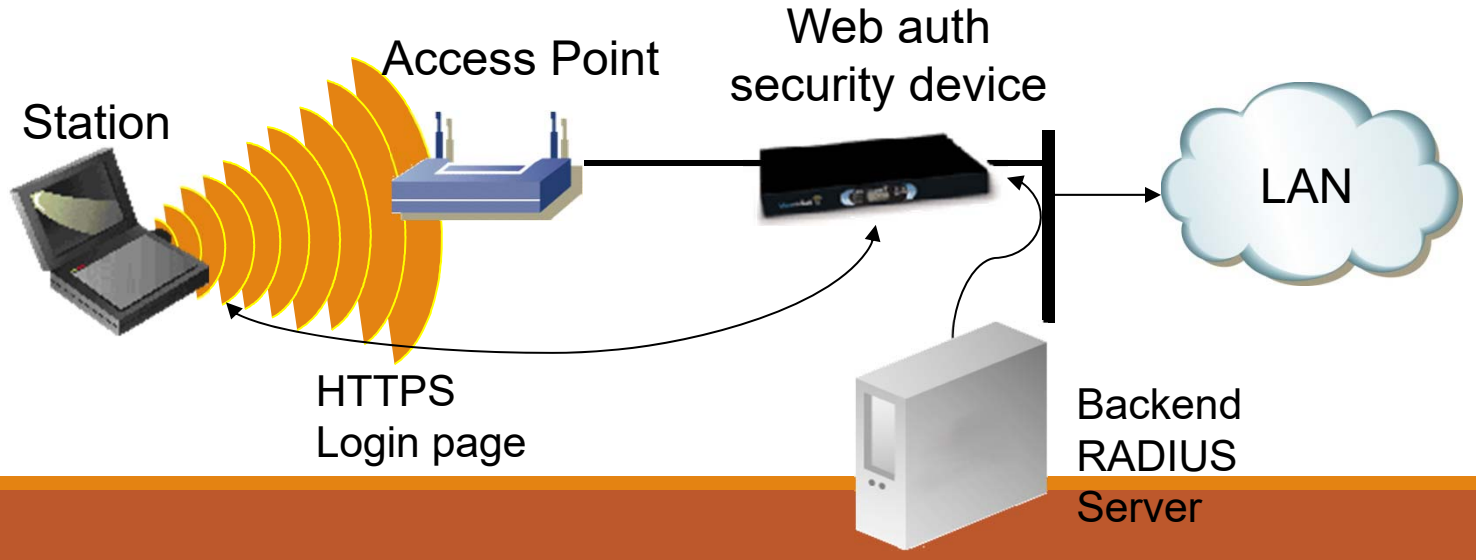
Narzędzia – program AirCrack



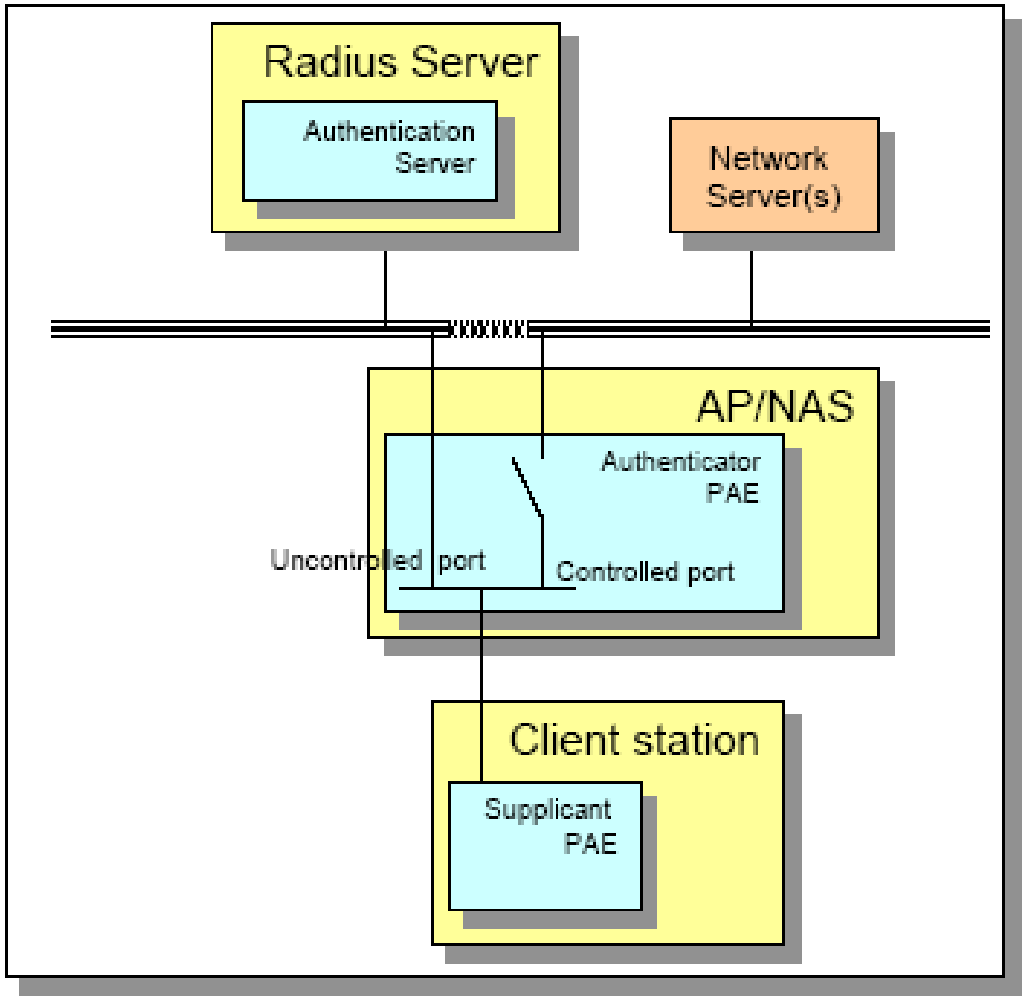
VPN Authentication and Encryption



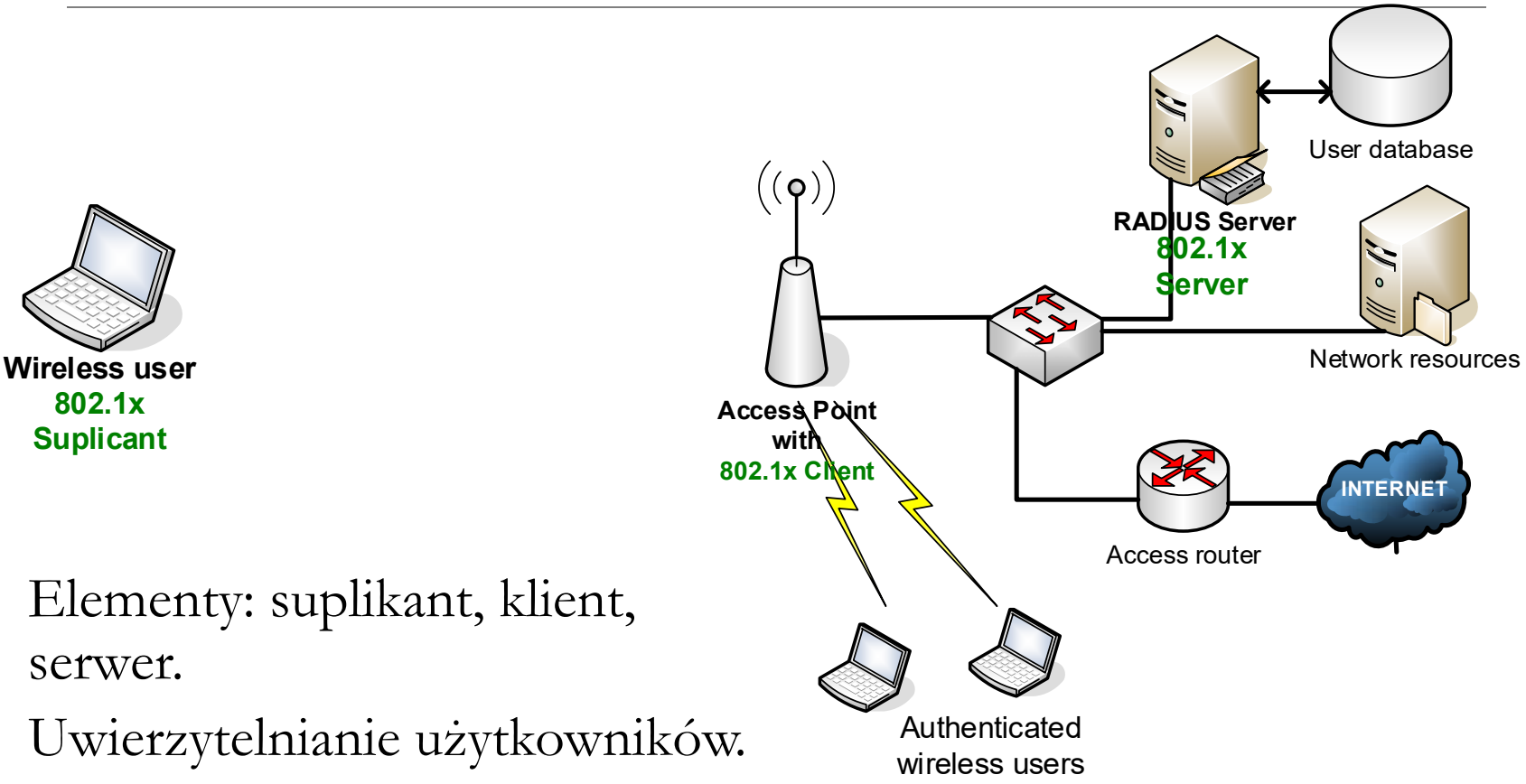




Kontrola dostępu 802.1x

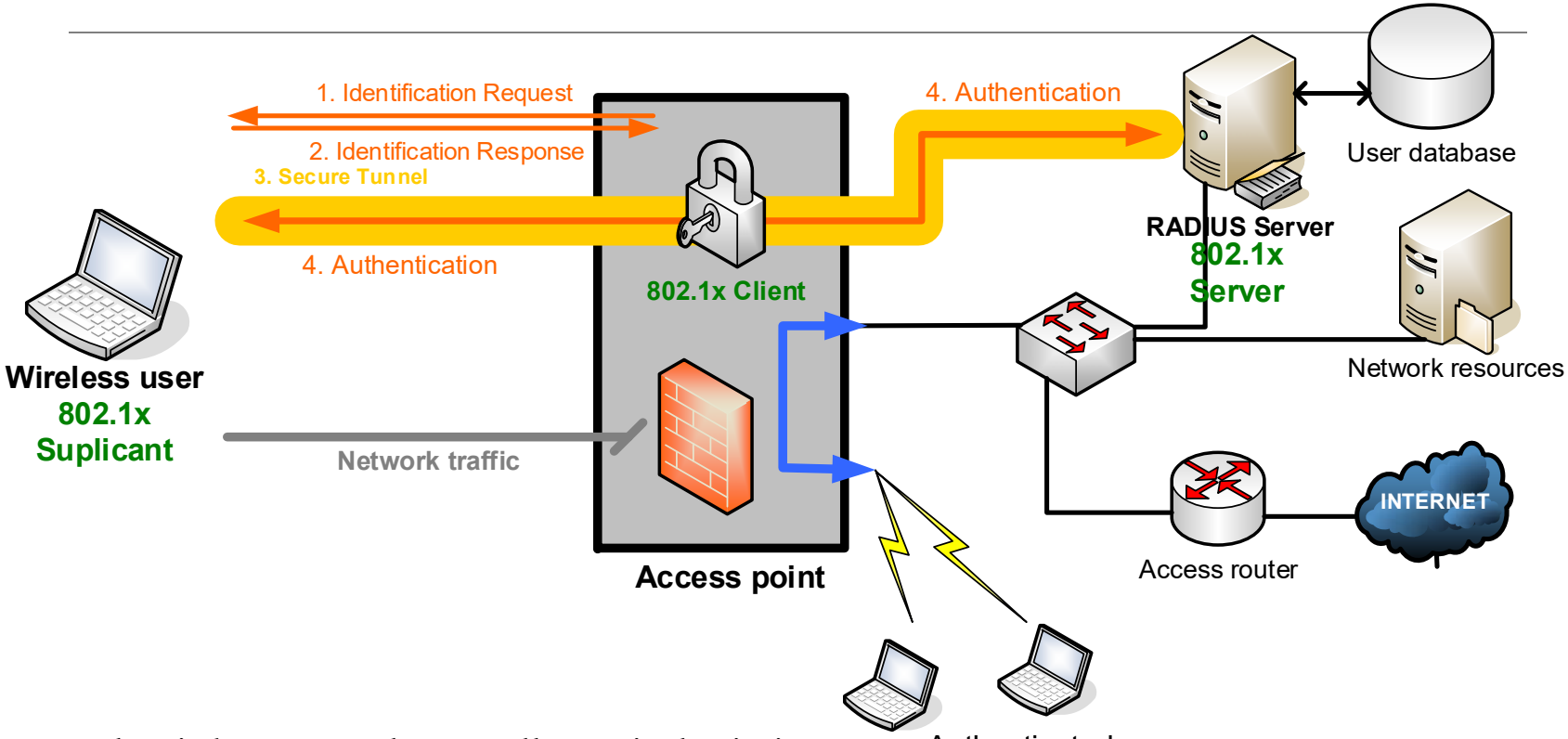


802.1x & RADIUS



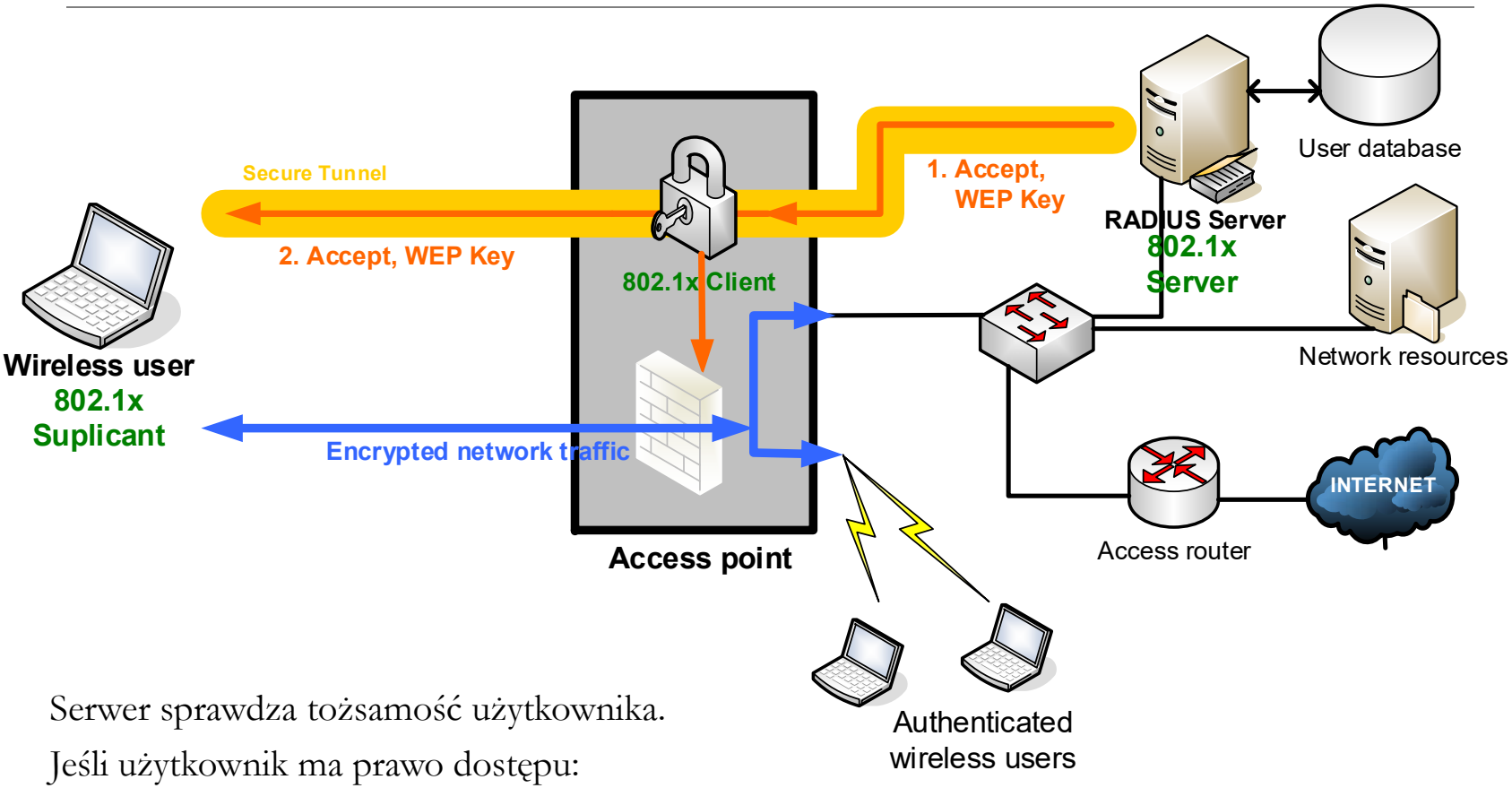
- Elementy: suplikant, klient, serwer.
- Uwierzytelnianie użytkowników.
- Wzajemne uwierzytelnianie systemu i użytkownika.
- Bezpieczna wymiana informacji.

802.1x & RADIUS



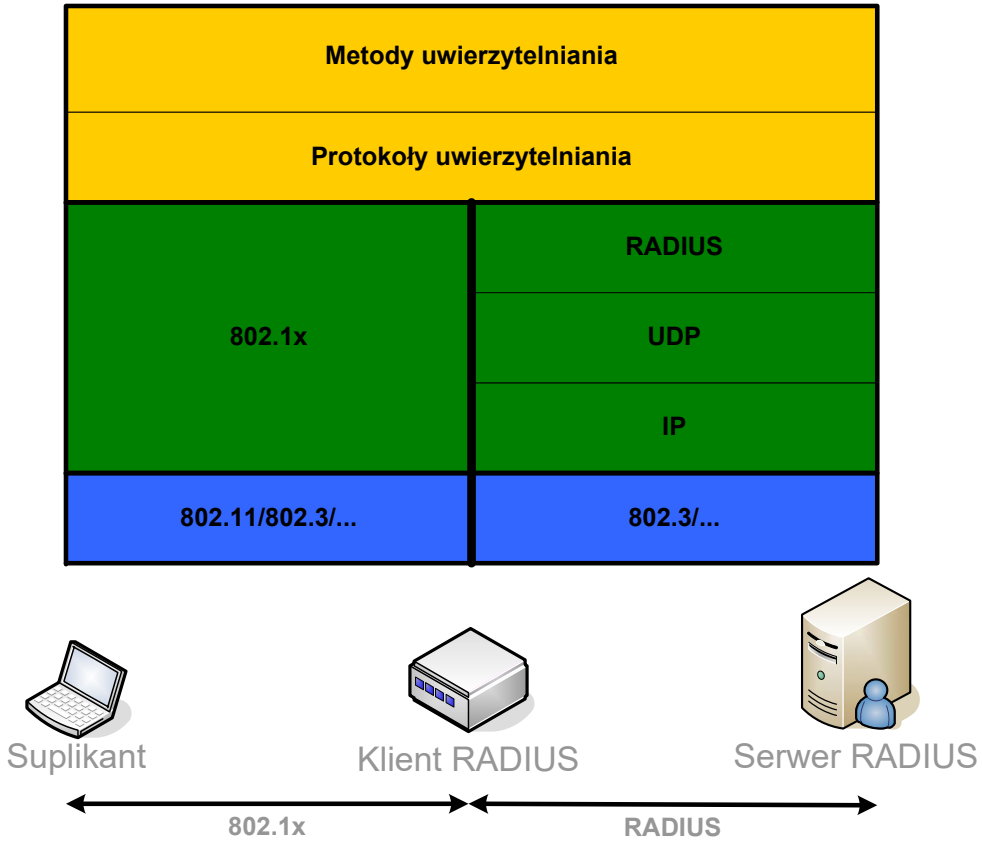
- Urządzenie bezprzewodowe podłącza się do sieci.
- AP blokuje ruch od urządzenia i (ocjonalnie) wysyła żądanie identyfikacji.
  Urządzenie odpowiada podając tzw. anonymous identity: _____@realm
- Ustanawiany jest zabezpieczony tunel pomiędzy urządzeniem, a serwerem.
- Serwer uwierzytelnia się, jeśli żąda tego urządzenie.
- Urządzenie przesyła informacje uwierzytelniające.

802.1x & RADIUS



- Serwer sprawdza tożsamość użytkownika.
- Jeśli użytkownik ma prawo dostępu:
  - serwer wysyła wiadomość informującą użytkownika i AP, że dostęp został przyznany,
  - AP zaczyna przekazywać ruch od użytkownika,
  - serwer generuje i wysyła AP klucz pozwalający na bezpieczne przekazanie użytkownikowi klucza WEP,
  - użytkownik podłącza się do sieci z użyciem otrzymanego klucza.

Architektura warstwowa 802.1x



802.1x & RADIUS

WEP jest w dalszym ciągu używany w sieci, ale:

- klucze WEP mogą różnić się u różnych użytkowników,
- jest możliwe automatyczne generowanie kluczy,
- klient nie jest uwierzytelniany z użyciem klucza WEP.

Uwierzytelnienie portów:

- Nie uwierzytelnieni użytkownicy nie mogą przesyłać danych, nawet jeśli posiadają prawidłowy klucz WEP.

Środowisko korporacyjne:

- wiele AP pracuje z użyciem tego samego serwera,
- serwer może korzystać z różnorakich baz danych.

Porównanie metod uwierzytelniania

Wireless Auth Type	Desktop Control Needed	Cost to Implement	Difficult to Manage	Vendor Support Problems	Vulnerable to Attack
Web Auth	low	low	medium	low	medium
VPN	high	high	medium	low	low
WEP	medium	low	high	low	high
802.1x EAP-TLS ceritficates	high	high	high	medium	low
802.1x PEAP	medium	medium	medium	medium	low

Wireless Protected Access

W pełni zgodne z WEP.

Może pracować na obecnym sprzęcie po dokonaniu uaktualnienia oprogramowania

Wykorzystuje RC4, z powodu ograniczonej mocy obliczeniowej sprzętu

Poprawiono najgorsze słabości WEP:

- obligatoryjny mechanizm uwierzytelniania,
- nowy sposób tworzenia wektora inicjalizującego,
- w miejsce ICV – Message Integrity Code (MIC): Michael,
- nowy sposób tworzenia klucza szyfrującego: funkcja mieszająca,
- mechanizmy zarządzania i dystrybucji kluczy.

WPA = 802.1x + EAP + TKIP

Uwierzytelnianie: 802.1x + EAP

Protokół 802.1x wraz z jednym z protokołów EAP (EAP-MD5, LEAP, EAP-TLS, PEAP).

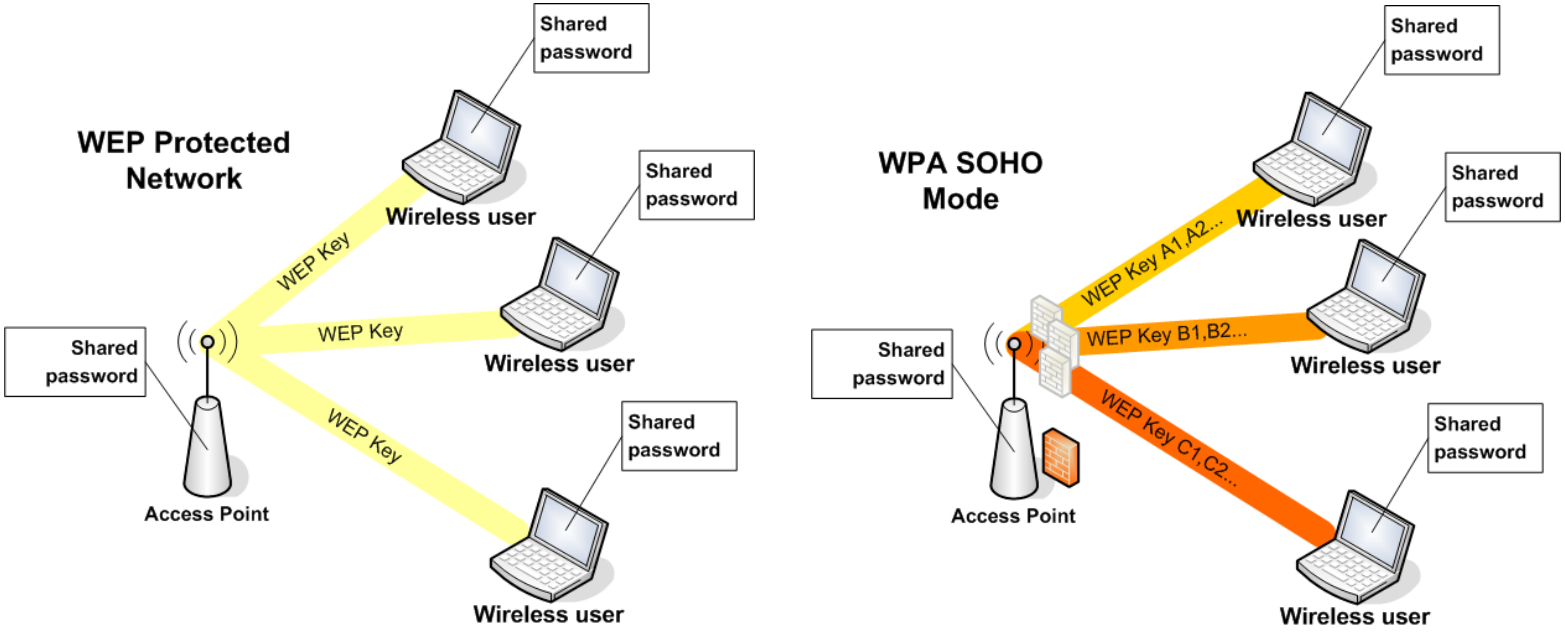
Bezwzględna konieczność potwierdzania tożsamości przed wysłaniem wiadomości w sieci (brak metody „open system”).

Wzajemne uwierzytelnianie użytkownika z serwerem dostępowym.

Możliwość wyboru dwóch trybów uwierzytelniania:

- za pomocą niezależnego serwera uwierzytelniającego RADIUS,
- przy wykorzystaniu współdzielonego klucza WPA-PSK (ang. WPA – Pre-Shared Key).

Wireless Protected Access – PSK



- WPA-PSK:
  - Wewnętrzny mechanizm zarządzania kluczami, wewnętrzny mechanizm uwierzytelniania.
- Możliwa jest też konfiguracja „korporacyjna”, korzystająca tu z poprawionych mechanizmów zarządzania kluczami:
  - RADIUS server, 802.1x klient, 802.1x suplikant

Hierarchia kluczy

Procesy kodowania i sprawdzania integralności wykorzystują klucze.

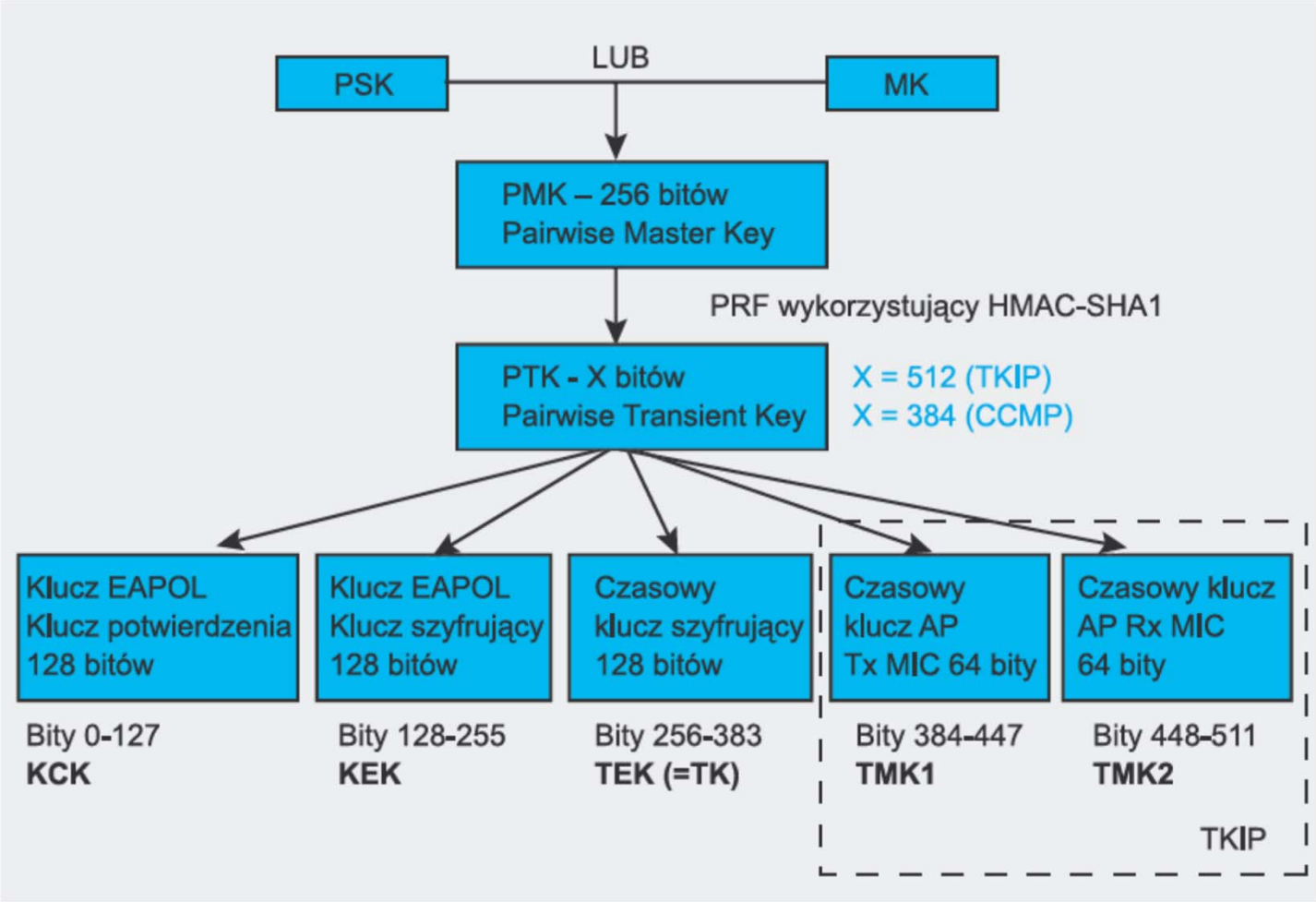
Rodzaje kluczy:

- klucz uniwersalny (Master Key) – przy wykorzystaniu serwera uwierzytelniania,
- parzysty klucz uniwersalny (Pair-wise Master Key)
- klucze tymczasowe (Temporal Keys).

Klucze czasowe (składają się na Parwise Transient Key):

- klucz szyfrowania danych (128 bitów) – TK,
- klucz integralności danych (2x64 bity) - TMK,
- klucz szyfrowania EAPOL-Key (128 bitów) - KEK,
- klucz integralności EAPOL-Key (128 bitów) - KCK.

Hierarchia kluczy



Nowy IV

Zabezpiecza przed atakami typu replay.

Nie współpracuje z mechanizmami QoS proponowanymi w 802.11e.

Nowy, 48 bitowy, IV pełni funkcję licznika ramek.

Po wprowadzeniu nowego klucza szyfrującego IV jest zerowany i rozpoczyna zliczanie ramek.

Jeśli licznik się przepełni, negocjowany jest nowy klucz.

Niemożliwe jest powtórzenie IV z tym samym tajnym kluczem.

Jeśli odbiornik wykryje ramkę z numerem mniejszym od już otrzymanej, jest ona odrzucana.

Message Integrity Code (MIC): Michael

Obejmuje całą ramkę: nagłówek i dane.

Chroni przez atakami typu bit-flipping.

64 bitowa wartość, obliczana na podstawie:

- nagłówka ramki,
- wektora IV,
- pola danych,
- z użyciem ***tymczasowego klucza integralności danych*** (64 bity).

Koszt obliczeniowy: ~5,5 c/bajt (3DES: 180 c/bajt).

Odporność: 1-2 minut.

Konieczne zastosowanie dodatkowego zabezpieczenia:

- Stacja odłącza się od sieci jeśli wykryje 2 nieudane próby fałszerstwa na sekundę. Obniża to prawdopodobieństwo udanej próby fałszerstwa do 1/stację/rok.

Key mixing

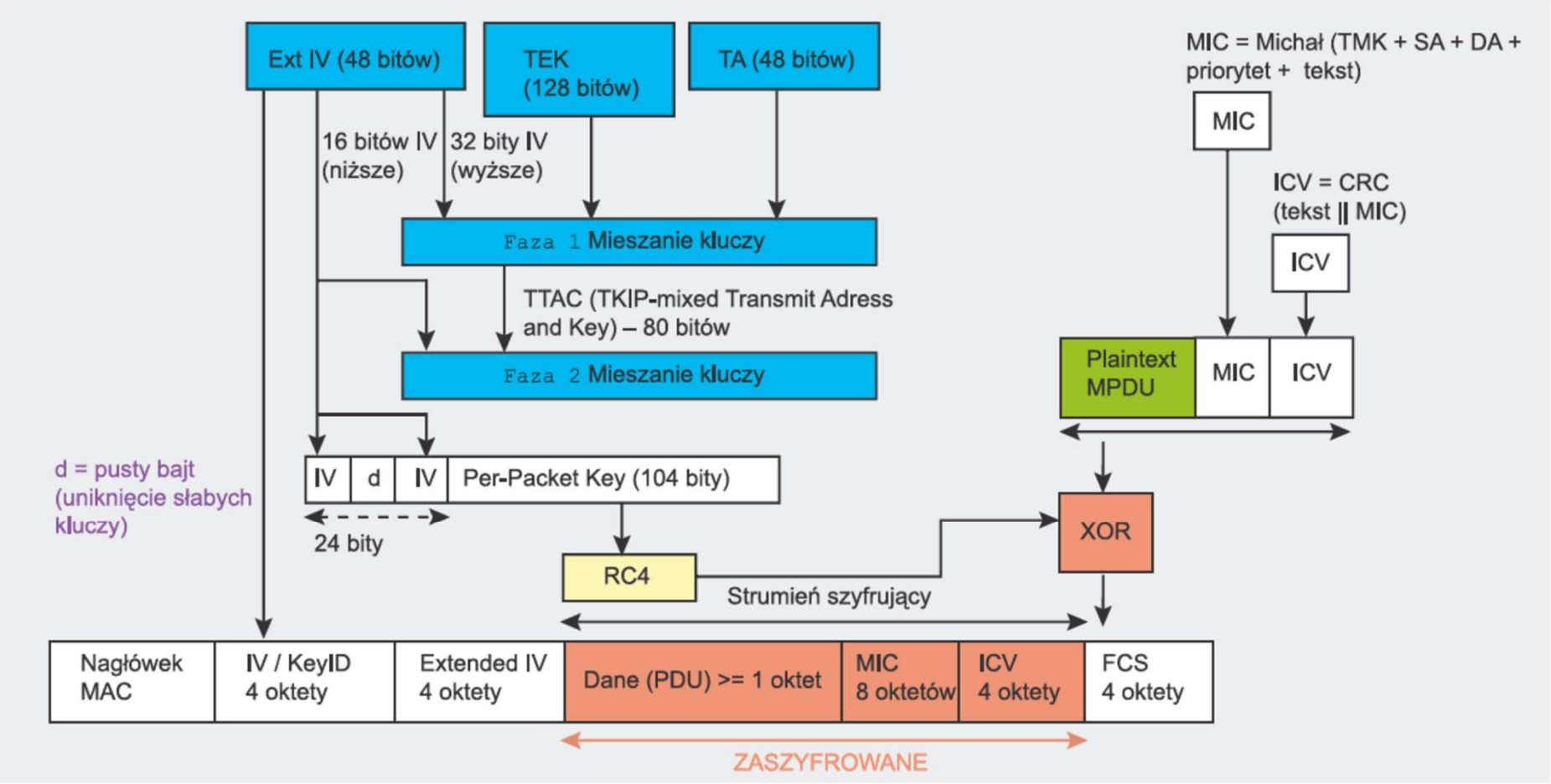
Nowa funkcja mieszająca, służąca tworzeniu klucza szyfrującego:

- klucz szyfrujący ustalany na podstawie ***tymczasowego klucza szyfrowania danych***,
- 1 faza: zróżnicowanie klucza szyfrującego pomiędzy stacjami,
- 2 faza: dekorelacja publicznego IV i klucza szyfrującego

Koszt obliczeniowy: ~150 c/ramkę.

Współpraca z protokołami 802.1X/EAP w celu generacji i wymiany kluczy.

WPA


Ext IV (48 bitów)
TEK (128 bitów)
TA (48 bitów)
16 bitów IV (niższe)
32 bity IV (wyższe)
Faza 1 Mieszanie kluczy
TTAC (TKIP-mixed Transmit Adress and Key) – 80 bitów
Faza 2 Mieszanie kluczy
d = pusty bajt (uniknięcie słabych kluczy)
IV
d
IV
Per-Packet Key (104 bity)
24 bity
RC4
Strumień szyfrujący
MIC = Michał (TMK + SA + DA + priorytet + tekst)
MIC
ICV = CRC (tekst || MIC)
ICV
Plaintext MPDU
MIC
ICV
XOR
Nagłówek MAC
IV / KeyID 4 oktety
Extended IV 4 oktety
Dane (PDU) >= 1 oktet
MIC 8 oktetów
ICV 4 oktety
FCS 4 oktety
ZASZYFROWANE

Wymagania dla mechanizmów bezpieczeństwa sieci bezprzewodowej

Wykorzystanie niezawodnej metody szyfrowania, w sposób zgodny z jej przeznaczeniem.

Ochrona przed fałszowaniem ruchu sieciowego. Bez tego wymogu atakujący może wykorzystać własne mechanizmy protokołu do złamania jego zabezpieczeń.

Uniemożliwienie ataków typu traffic replay (specjalny przypadek ataku polegającego na fałszowaniu ruchu – wymaga specyficznych środków obrony).

Uniknięcie możliwości powtórnego wykorzystania kluczy.

Uniknięcie możliwości powtórnego wykorzystania IV lub dowolnej innej informacji wykorzystywanej w procesie szyfrowania.

Ochrona zawartości nagłówka ramki, a w szczególności adresów źródłowych i docelowych. Ochrona adresu źródłowego pozwoli na uniknięcie ataków typu identity hijacking, a docelowego uniemożliwi przekierowanie ruchu do nieautoryzowanego odbiorcy (sieci miltihop ad-hoc).

Zastosowanie małej liczby mechanizmów kryptograficznych, w celu obniżenia kosztów sprzętu oraz wyeliminowania zbędnych możliwości konfiguracyjnych.

Minimalizacja wymagań obliczeniowych. AP pozostaną główną pozycją kosztów tworzenia sieci, a zatem należy się liczyć z ograniczeniem ich możliwości sprzętowych.

Zastosowanie nowoczesnych algorytmów kryptograficznych pozwoli na przedłużenie czasu życia produktu.

WPA2

Zgodne ze standardem 802.11i.

Jest, w przeciwieństwie do WPA, rozwiązaniem długoterminowym.

Powoduje konieczność wymiany obecnych urządzeń bezprzewodowych.

Umożliwia obsługę protokołu WPA.

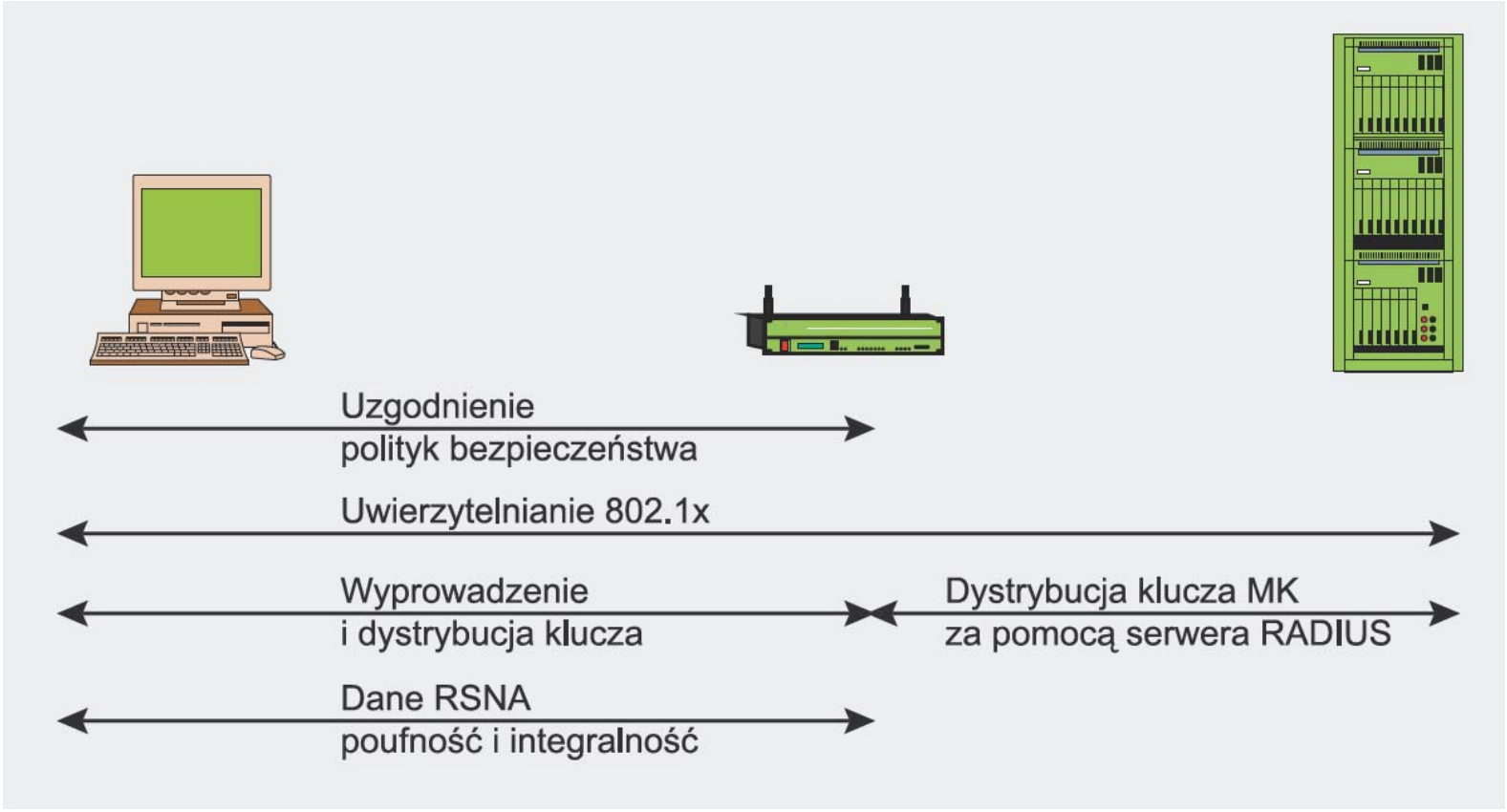
Podobieństwa z WPA:

- Uwierzytelnianie z użyciem serwera RADIUS lub WPA2-PSK.
- Hierarchia kluczy.

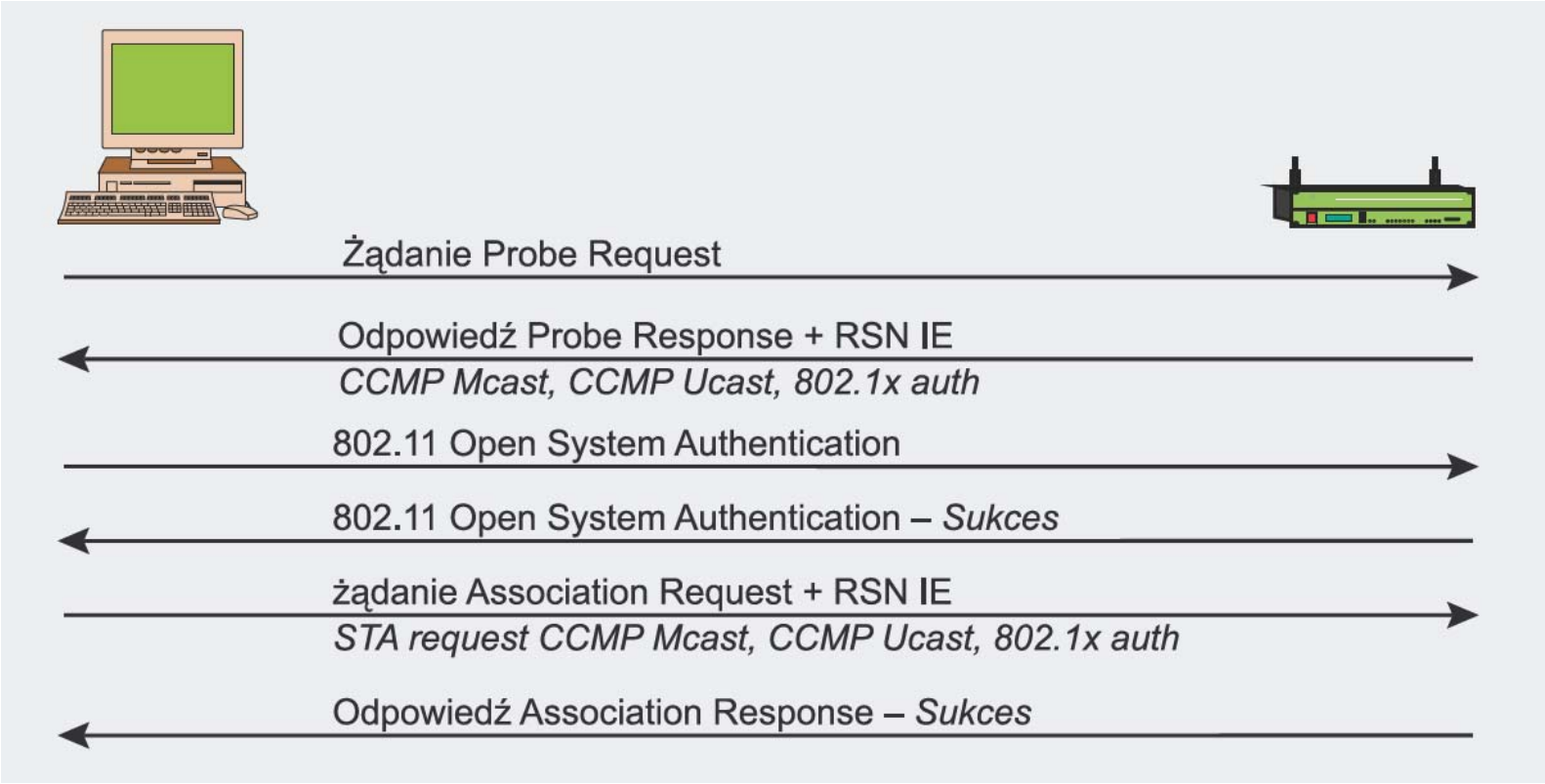
Fazy pracy 802.11i

- Uzgodnienie polityki bezpieczeństwa
- Uwierzytelnianie 802.1x
- Wygenerowanie i dystrybucja kluczy
- Zapewnienie poufności i integralności danych

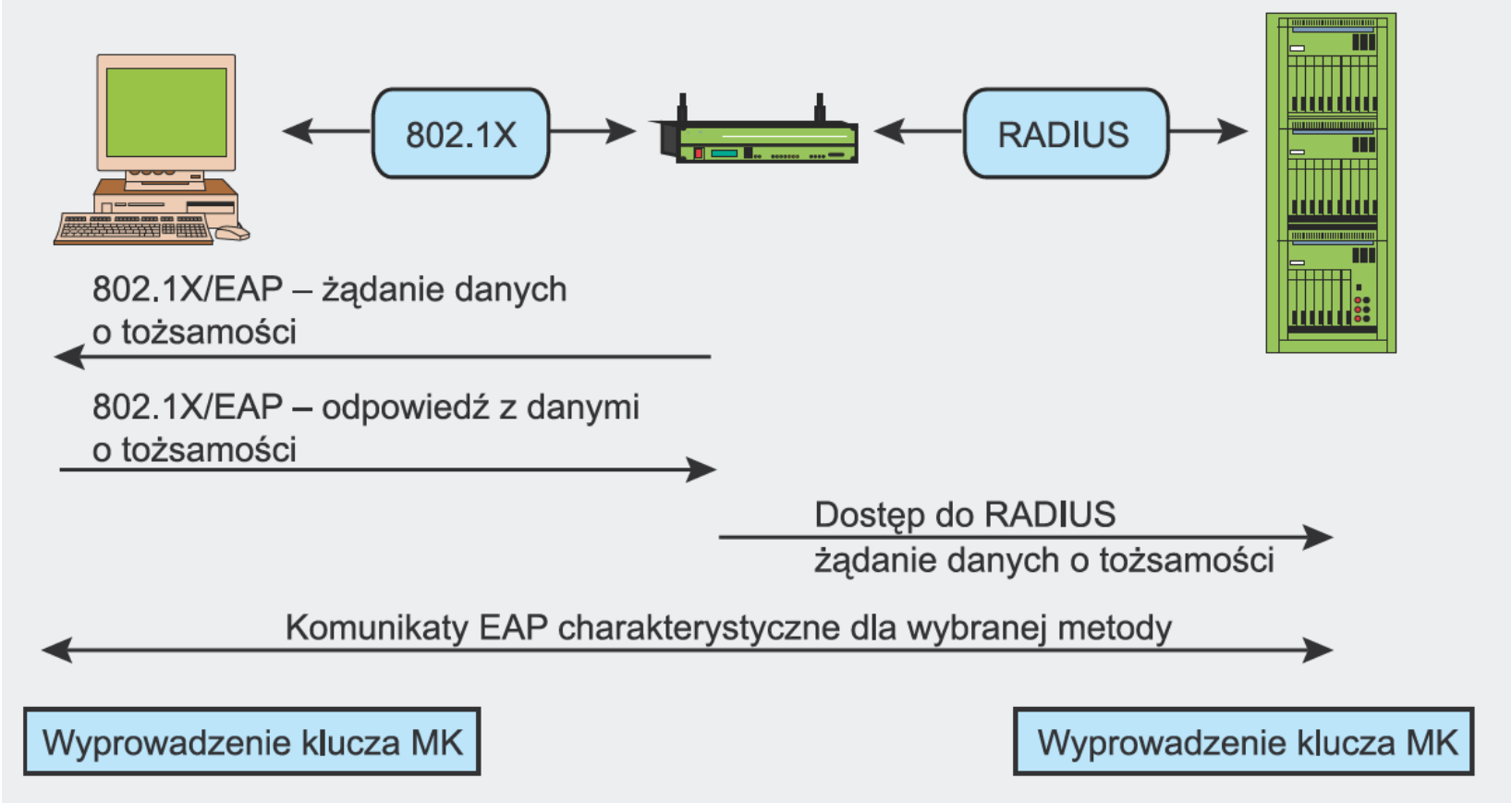
Fazy pracy 802.11i



Uzgodnienie polityki bezpieczeństwa



Uwierzytelnianie 802.1x - EAP



Wygenerowanie i dystrybucja kluczy

Klucz MK jest znany tylko suplikantowi i serwerowi uwierzytelniania.

Klucz PMK znany jest suplikantowi, serwerowi i klientowi (punkt dostępowy).

Potwierdzenie, że klient zna klucz PMK (Parwise Master Key).

Wygenerowanie klucza

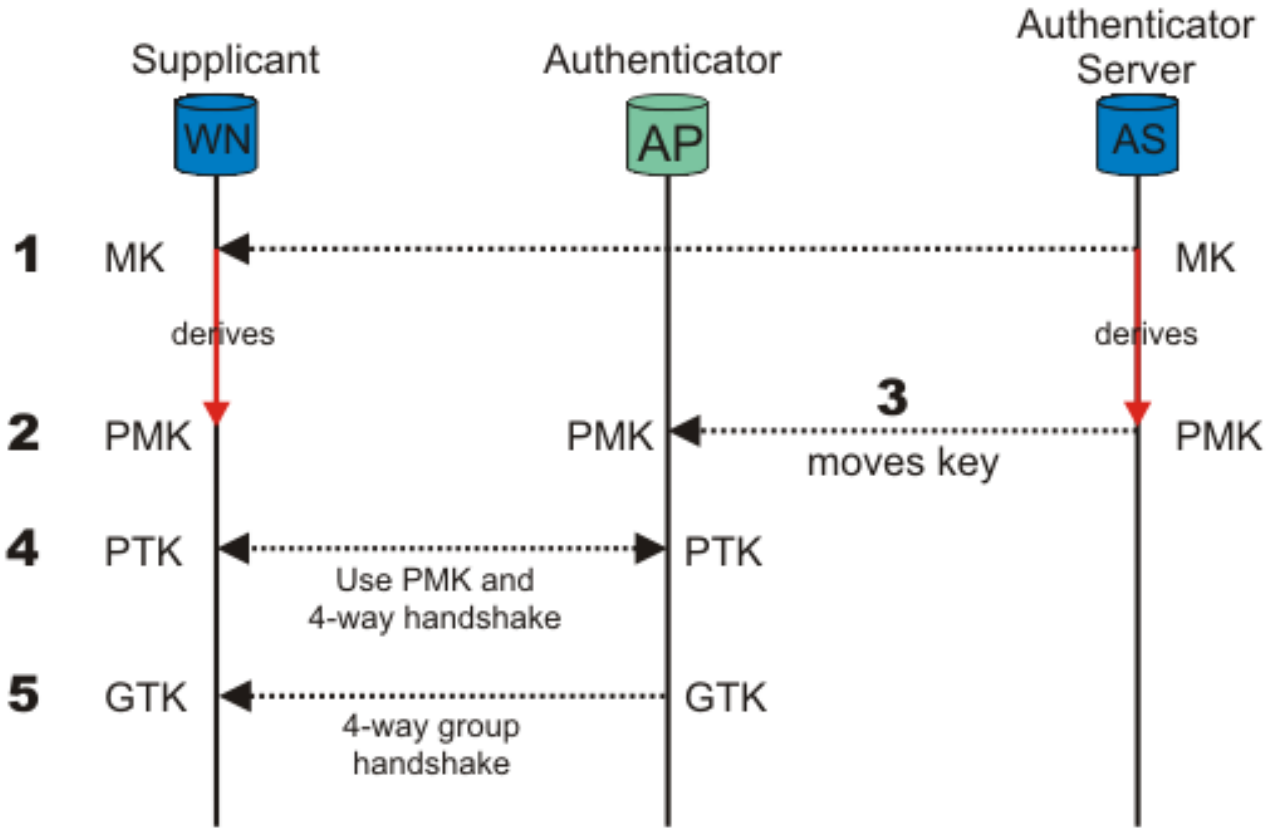
- PTK (Pairwise Transient Key) – na podstawie klucza PMK, ciągu znaków, adresów MAC AP i klienta, 2 losowych wartości.
- GTK (Group Transient Key).

Instalacja kluczy ochrony poufności i integralności.

Przesłanie klucza GTK.

Potwierdzenie wyboru zestawu mechanizmów kryptograficznych.

Wygenerowanie i dystrybucja kluczy



Poufność: AES

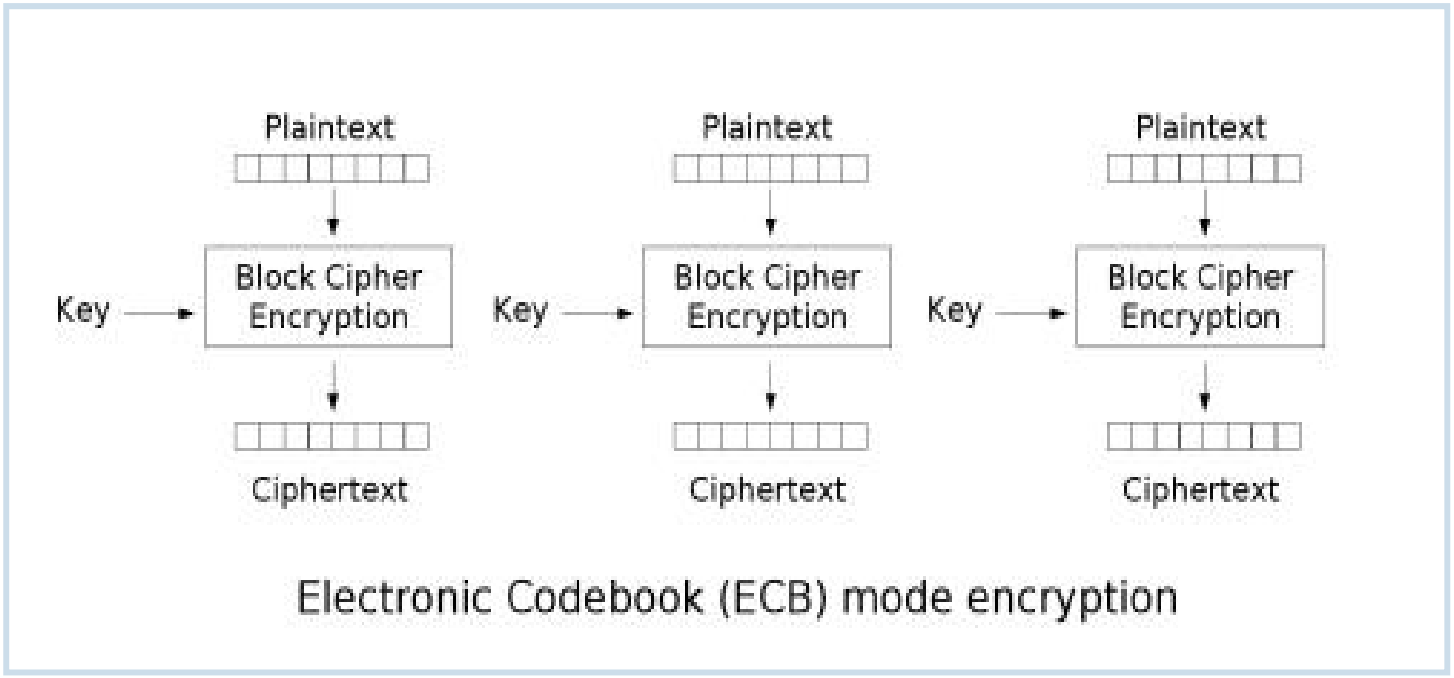
Szyfrowanie i kontrola integralności danych oparta na koderze AES (Advanced Encryption Standard) z kluczem 128 bitowym.

AES to szyfr blokowy, który wykorzystuje 128-bitowy blok danych i 128, 196 lub 256-bitowy klucz.

W przypadku WPA2 użyto protokołu Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP):

- szyfrowania AES w trybie Counter Mode,
- kontroli integralności z użyciem protokołu CBC-MAC.

Electronic Codebook (ECB)



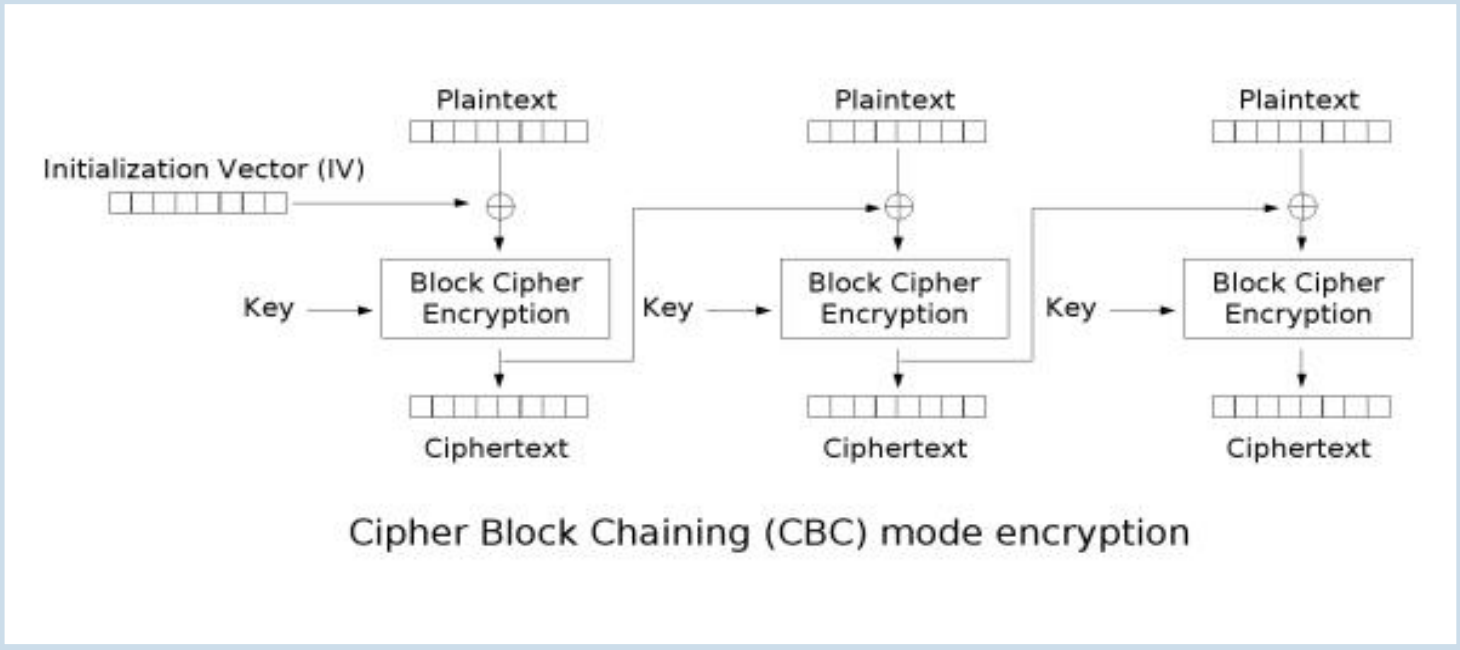
Electronic Codebook (ECB) mode encryption

No error propagation – errors are completely isolated

Least secure – identical input gives identical output

Patterns observable in video and image data

Cipher Block Chaining (CBC)

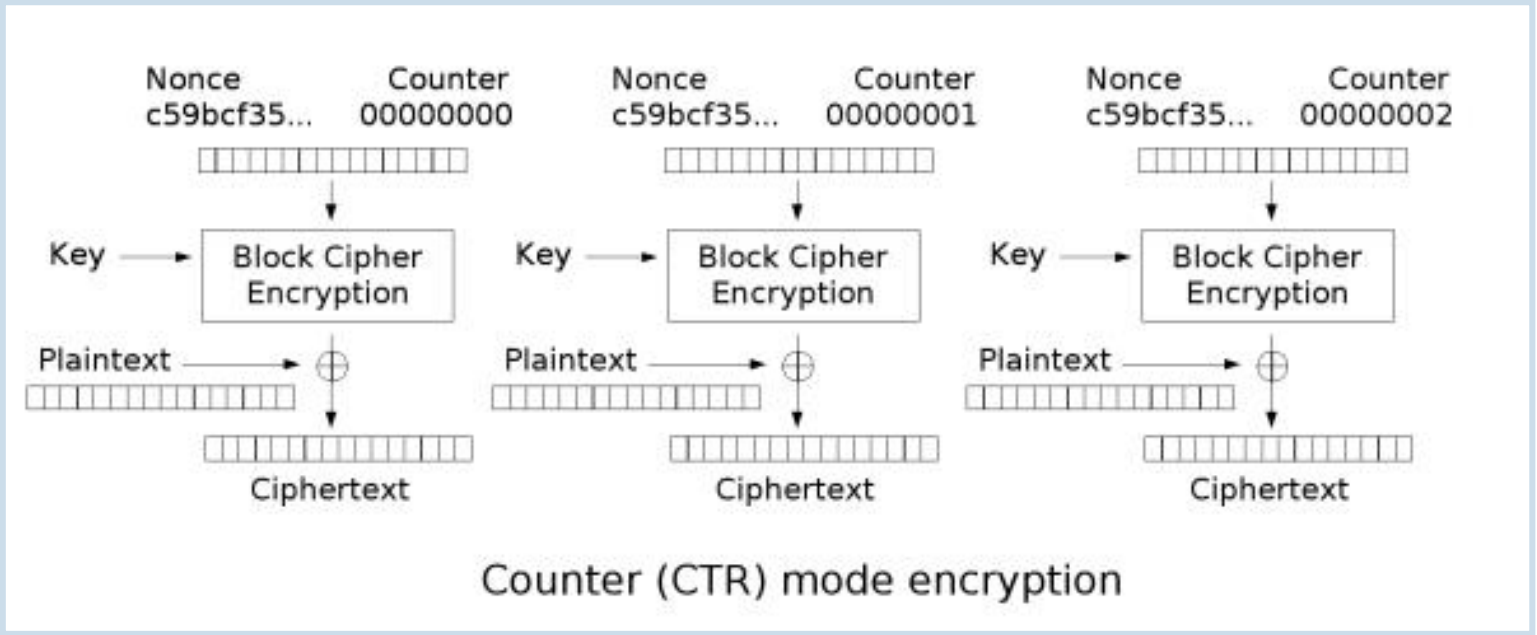


Cipher Block Chaining (CBC) mode encryption

Most secure – no patterns are observed

100% downstream corruption resulting from data loss or single-event upsets (SEUs) during encryption

Counter (CTR) Mode



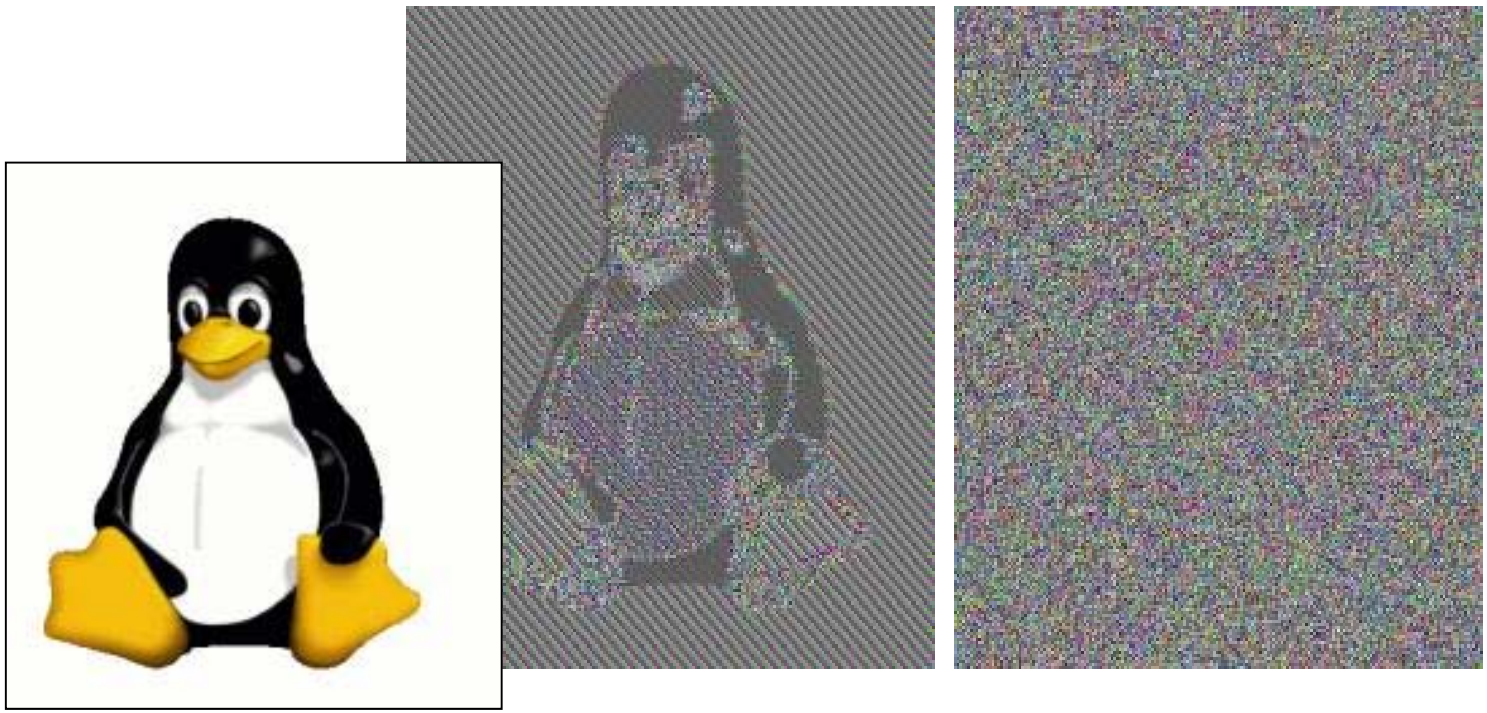
Counter (CTR) mode encryption

Effectively converts AES into a stream cipher

High security – similar to CBC

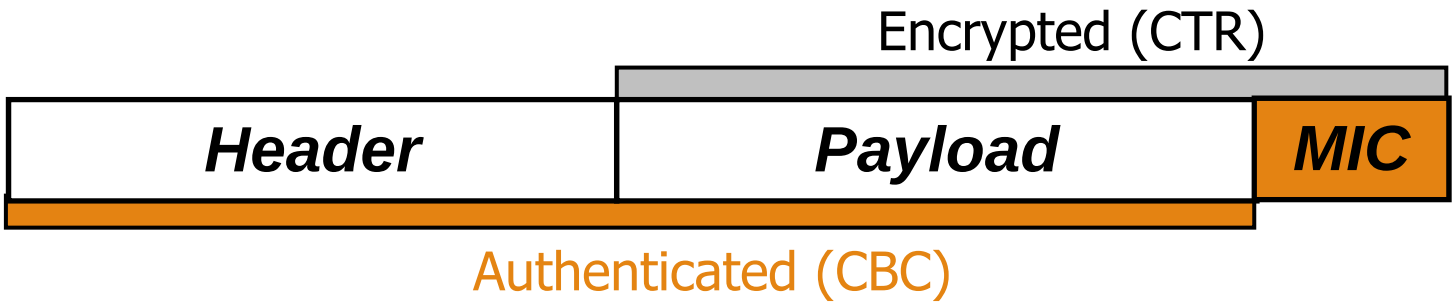
No error propagation – errors are completely isolated

Electronic Codebook (ECB)



- ECB-encrypted image has observable patterns
- CTR/CBC encryption looks like random noise

Integralność: CBC – MAC



Zasada działania:

- Pobierany jest pierwszy blok wiadomości i kodowany przy użyciu algorytmu AES
- Rezultat poddawany jest operacji XOR z kolejnym blokiem, a wynik znowu kodowany
- Operacja powtarzana jest z kolejnymi blokami, w wyniku czego otrzymuje się 128-bitowy blok MIC
- Całość (bez nagłówka) szyfrowana AES-CTR.

WiFi Protected Setup (WPS)

Rozwiązanie ułatwiające podłączanie urządzeń do sieci zabezpieczonej mechanizmami WPA/WPA2 – standaryzowane przez WiFi Alliance.

Możliwe tryby pracy – umożliwiają podłączenie urządzenia do sieci:

- PIN – poprzez wprowadzenie kodu PIN złożonego z 8 cyfr. Obligatoryjny dla wszystkich urządzeń.
- Push-button – po naciśnięciu przycisku (fizycznego lub wirtualnego) na urządzeniu dostępowym (punkt dostępowy) i urządzeniu podłączanym. Obligatoryjny dla punktów dostępowych i opcjonalny dla urządzeń klienckich.
- Near-field communication – dzięki komunikacji urządzenia dostępowego oraz podłączanego z użyciem NFC (zbliżeniowo). Opcjonalny.
- USB – dzięki przeniesieniu informacji dostępowej z urządzenia dostępowego do klienckiego z użyciem pamięci flash USB. Opcjonalny i rzadko stosowany w praktyce.

Późniejsza specyfikacja WiFi Direct wprowadza zmiany dotyczące wymaganej obsługi poniższych trybów:

- PIN – obligatoryjny dla urządzeń wyposażonych w klawiaturę i wyświetlacz,
- Push-button – obligatoryjny dla wszystkich urządzeń.

Podatności WPS PIN: online brute force

Tryb WPS PIN charakteryzuje się podatnością na atak brute-force.

PIN definiowany przez użytkownika składa się z 8 cyfr. PIN przypisany na stałe do urządzenia (sticker PIN), składa się z:

- 7 dowolnych cyfr,
- ostatniej cyfry będącej sumą kontrolną poprzedzających 7 cyfr.

Podczas uwierzytelniania PIN dzielony jest na 2 części po 4 cyfry, przetwarzane oddzielnie – po każdej części następuje potwierdzenie lub odrzucenie klienta.

Możliwe wartości dla liczby 8 cyfrowej: 10^8 = **100 000 000**

Możliwe wartości dla prekonfigurowanych (sticker) WPS PIN: 10^7 = 10 000 000

Wartości do sprawdzenia dla WPS sticker PIN:

$$10^4 + 10^3 = 10\,000 + 1000 = \mathbf{11\,000}$$

Wartości do sprawdzenia dla WPS PIN definiowanego przez użytkownika:

$$10^4 + 10^4 = 10\,000 + 10\,000 = \mathbf{20\,000}$$

Obrona możliwa dzięki specyficznej implementacji, np.: wprowadzeniu opóźnienia pomiędzy próbami.

Podatności WPS PIN: offline brute force

E ->R	**M1**	**N1 || Description || PKE**
R ->E	**M2**	**N1 || N2 || Description || PKR || Auth**
E ->R	**M3**	**E-Hash1 || E-Hash2**

N1 – 128 bitowa losowa wartość generowana przez E (Enrolee)

N2 – 128 bitowa losowa wartość generowana przez R (Registrar)

PKE – publiczny klucz E używany w DH, **PKR** – publiczny klucz R używany w DH

Auth = $\text{HMAC}_{\text{AuthKey}}$(M1 || M2)

E-Hash1 = $\text{HMAC}_{\text{AuthKey}}$(**E-S1** || **PSK1** || **PKE** || **PKR**)

E-Hash2 = $\text{HMAC}_{\text{AuthKey}}$(**E-S2** || **PSK2** || **PKE** || **PKR**)

PSK1 – pierwsze 4 cyfry PIN, **PSK2** – kolejne 4 cyfry PIN

Znając **E-S1** i **E-S2** możemy szybko wyznaczyć atakiem brute force w trybie offline (bez dostępu do atakowanego systemu) wartości **PSK1** i **PSK2**.

Podatności WPS PIN: offline brute force

Zgodnie z powyższym, odporność mechanizmu na atak zależy od jakości generowanych wartości losowych.

Jak, w praktyce, generowane są losowe wartości E-S1 i E-S2 ?
Różnie:

- Linux (hostapd) – nieźle, różne metody – /dev/random
- niektóre produkty Ralink: E-S1 = E-S2 = 0

W wielu wypadkach generatory liczb pseudolosowych (PRNGs) w urządzeniach przyjmują ten sam stan po restarcie.

Comparison

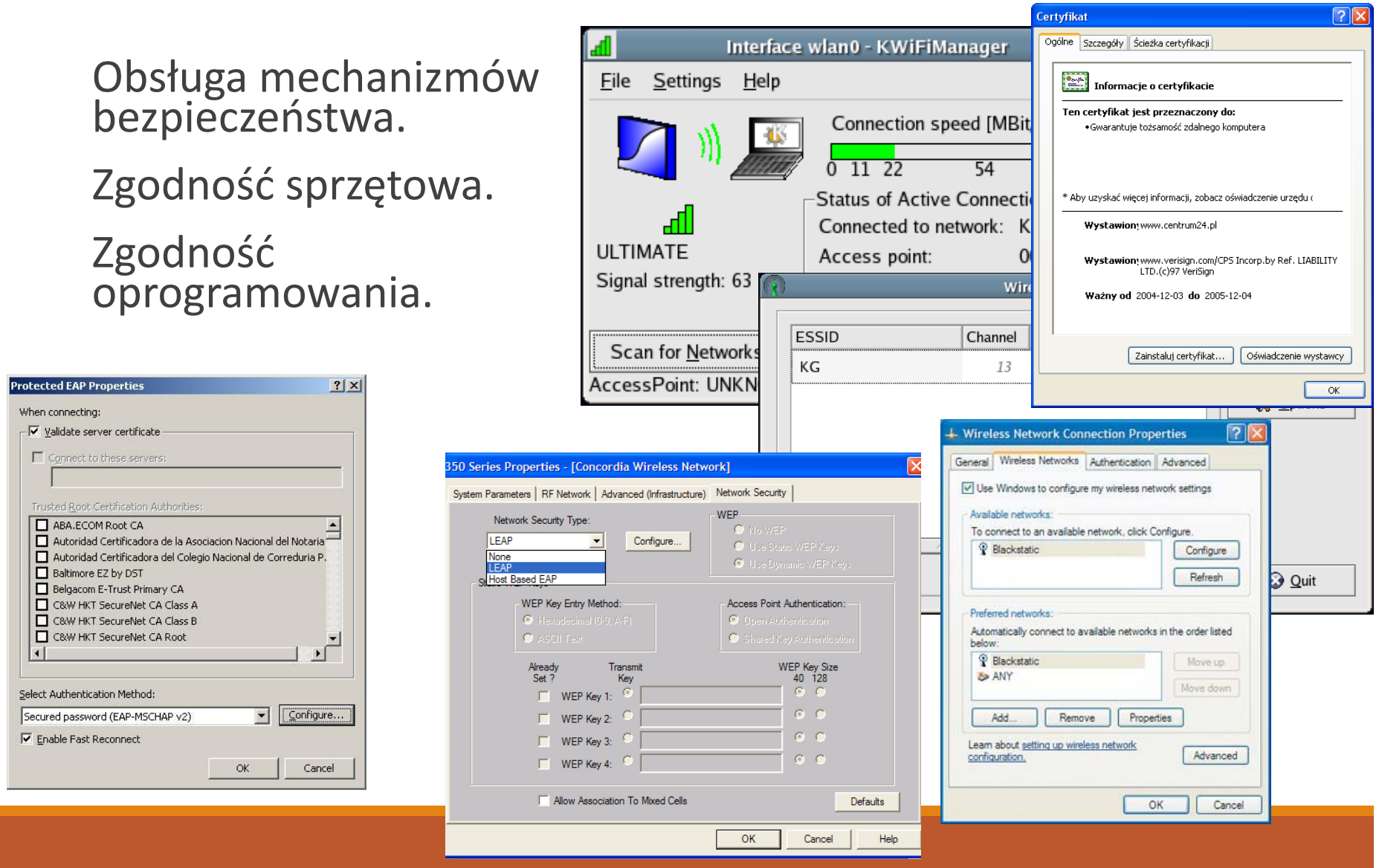
	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 encryption 64 authentication	128 bits
Key Life	24 bit IV	48 bit IV	48 bit IV
Packet Key	Concatenated	Mixing function	Not needed
Data Integrity	CRC32	Michael	CCMP
Header Integrity	None	Michael	CCMP
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-based

Klienci sieciowi

Obsługa mechanizmów bezpieczeństwa.

Zgodność sprzętowa.

Zgodność oprogramowania.

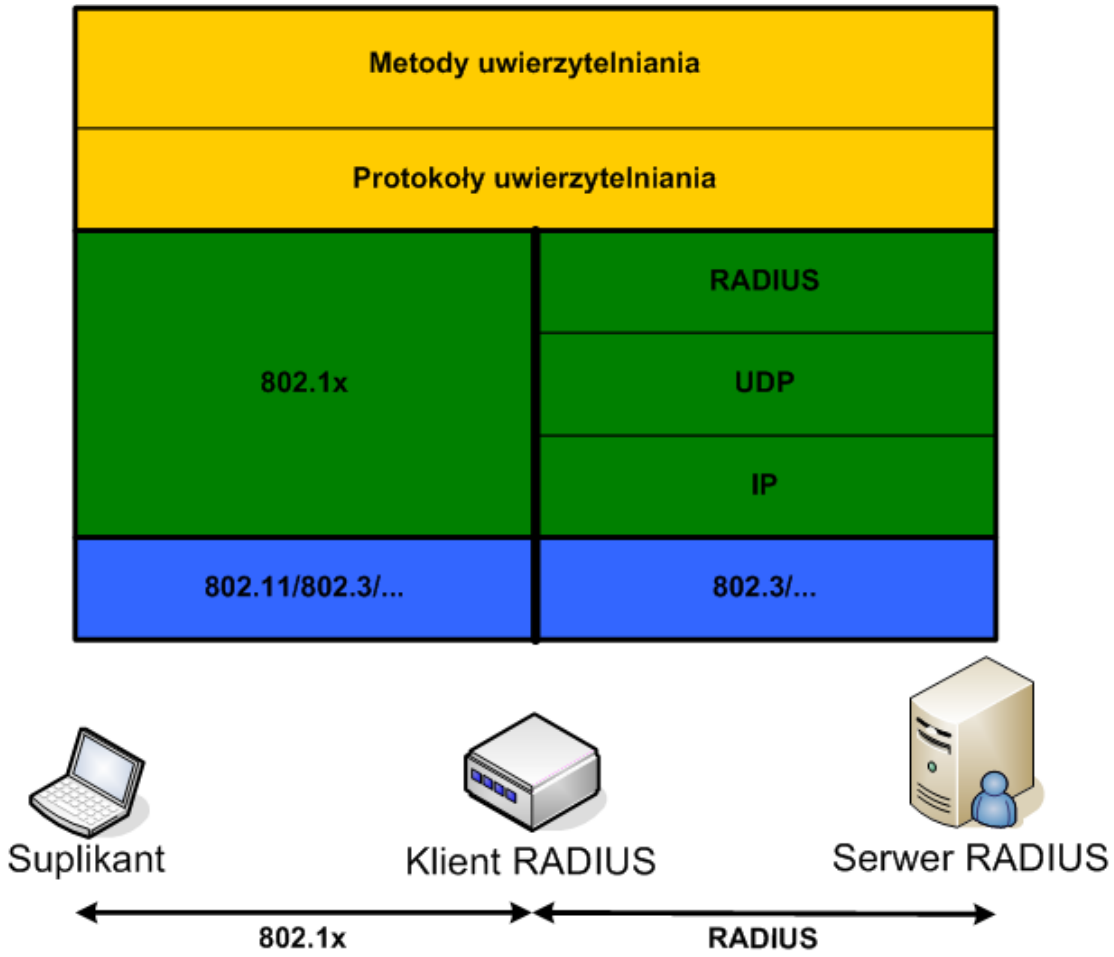


Extensible Authentication Protocol (EAP)

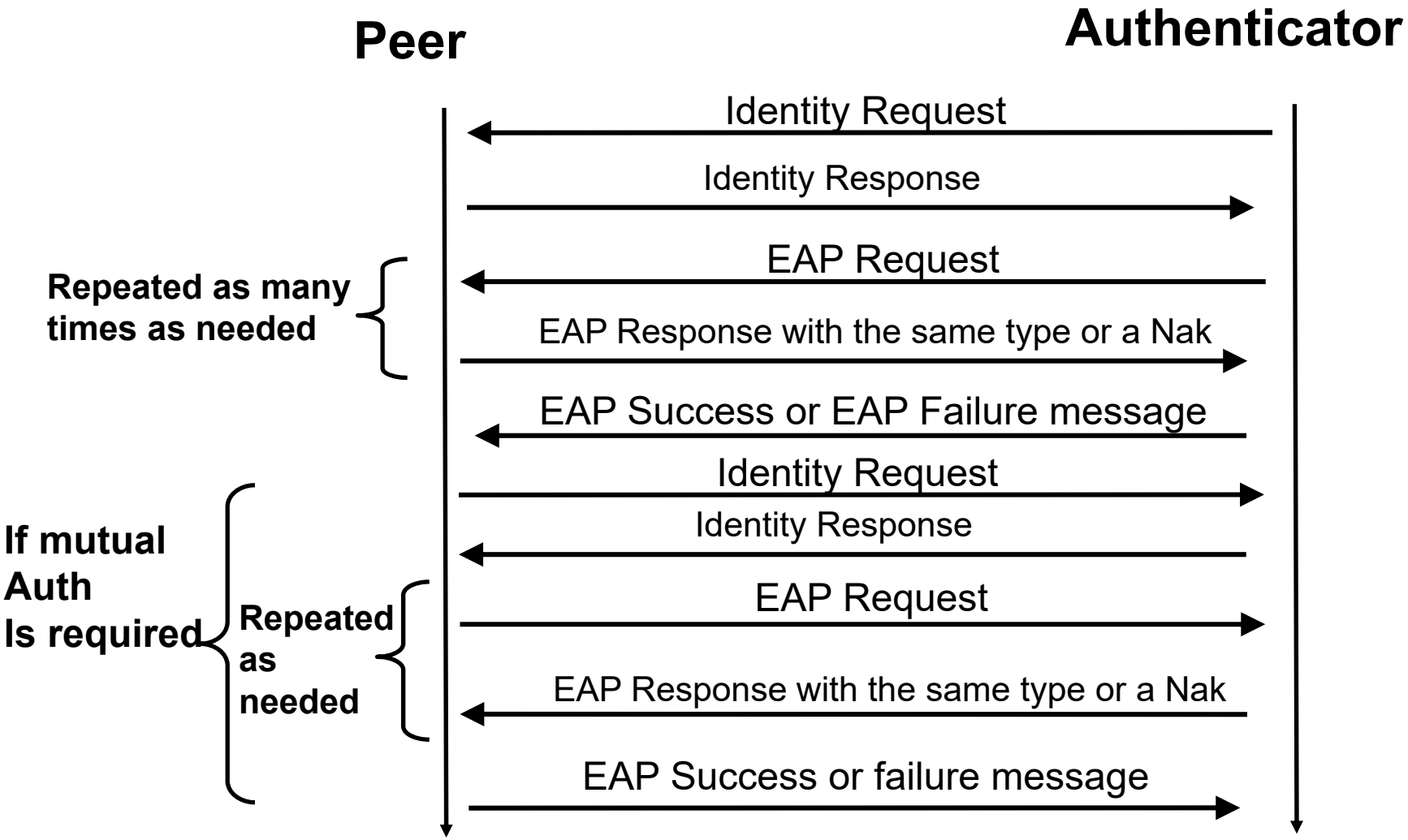
Jest to protokół transportowy, a nie metoda uwierzytelniania.

Istnieje wiele odmian stosujących różne mechanizmy komunikacji (EAP-TTLS, PEAP, ...).

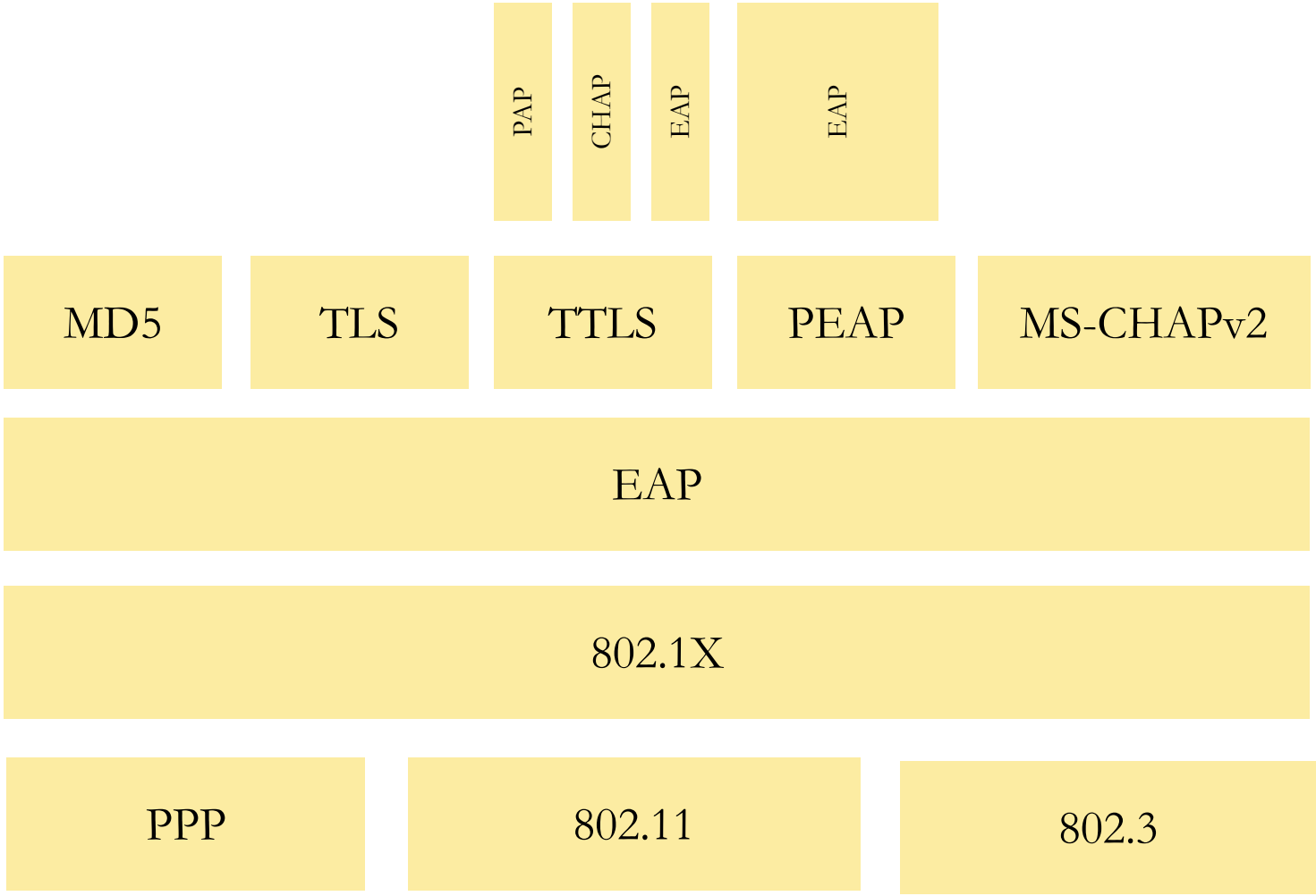
Wspiera różne metody uwierzytelniania, np.: PAP, CHAP, MSCHAP2, GTC...



Generic EAP Authentication Flow



Odmiany i metody EAP



Odmiany EAP

EAP – podstawowa wersja protokołu. Metody uwierzytelniania takie jak MD5 MS_CHAPv2 itp. wymieniają wiadomości bezpośrednio, korzystając z platformy komunikacyjnej udostępnionej przez protokół EAP.

Lightweight EAP (LEAP) – opracowana przez Cisco wersja EAP z wzajemnym uwierzytelnianiem przez funkcje skrótów z długimi kluczami;

EAP-TLS/EAP-TTLS – na platformie komunikacyjnej udostępnianej przez protokół EAP, zestawiany jest szyfrowany tunel TLS pomiędzy suplikantem i NAS. Metody uwierzytelniania wymieniają dane korzystając z tego tunelu.

PEAP (Protected EAP) – podobnie jak w TTLS, ale w zestawionym tunelu TLS uruchamiana jest kolejna warstwa protokołu EAP i to z jej pomocą komunikują się metody uwierzytelniania.

Metody EAP

MD5 – nazwa użytkownika i hasło szyfrowane funkcją skrótu MD5; nadaje się głównie do środowisk przewodowych - w warunkach sieci WLAN jest zbyt podatny na podsłuch i łamanie haseł offline oraz ataki typu man-in-the-middle.

TLS – metoda oparta na certyfikatach klientów i tunelowaniu TLS/SSL; daje wystarczający poziom bezpieczeństwa w sieciach WLAN i jest powszechnie wspierana przez producentów urządzeń

MS-CHAPv2 – technologia opracowana przez Microsoft zbliżona w ogólnych zarysach do MD5, lecz stosująca inną funkcję skrótu - MD4.

PAP – uwierzytelnianie z użyciem stałych haseł przesyłanych otwartym tekstem,

OTP (One-time Password) – uwierzytelnianie z użyciem haseł jednorazowych,

Metody EAP

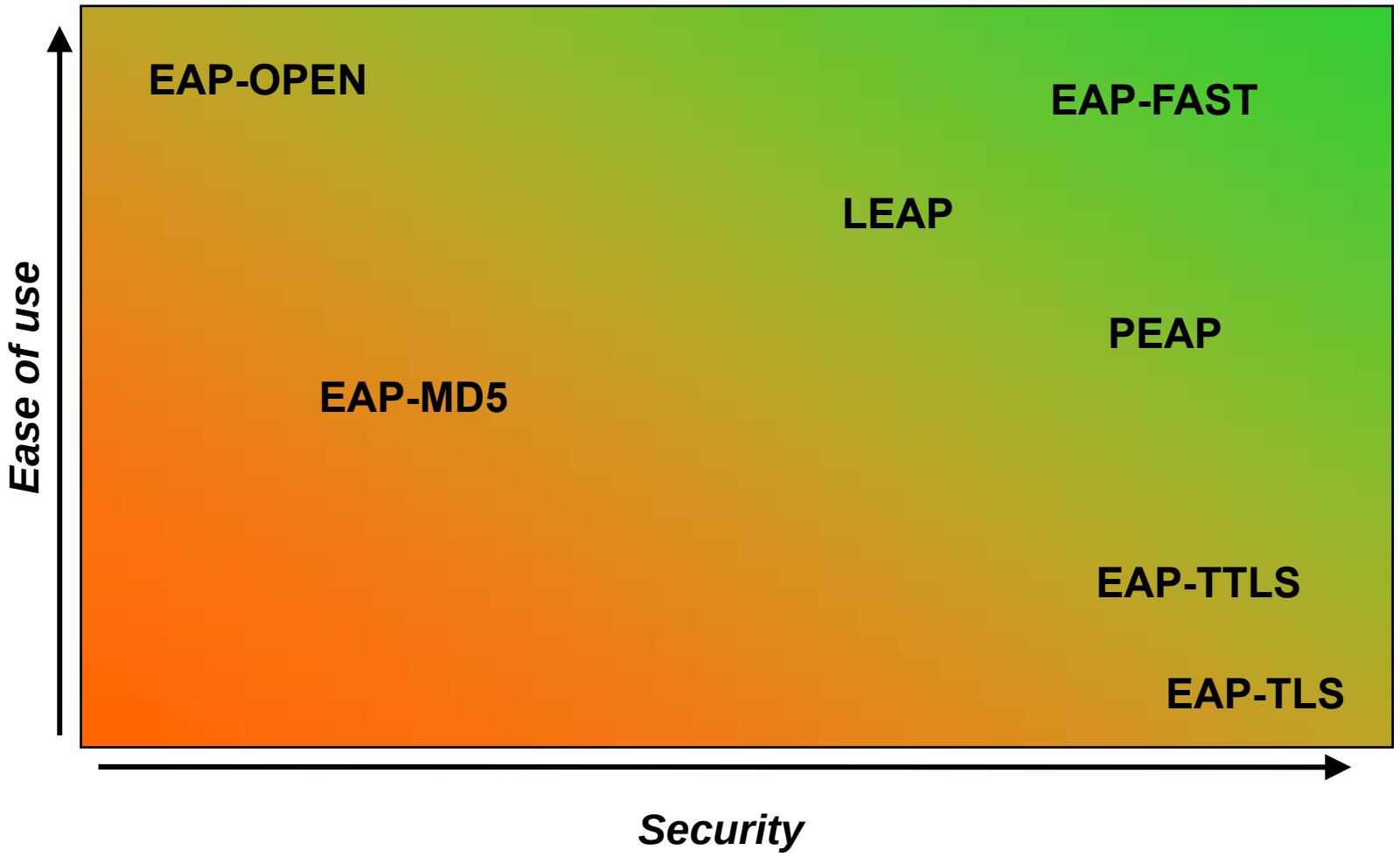
GTC (Generic Token Card) – uwierzytelnianie z użyciem kart chipowych,

SIM (Subscriber Identity Module)/AKA (UMTS Authentication and Key Agreement) – uwierzytelnianie z użyciem kart SIM i architektury uwierzytelniania właściwej dla sieci telefonii komórkowej.

SecurID – nie wymaga udostępniania danych uwierzytelniających suplikantowi.

SRP (Secure Remote Password) – nie wymaga przechowywania hasła na serwerze uwierzytelniającym.

EAP mechanisms

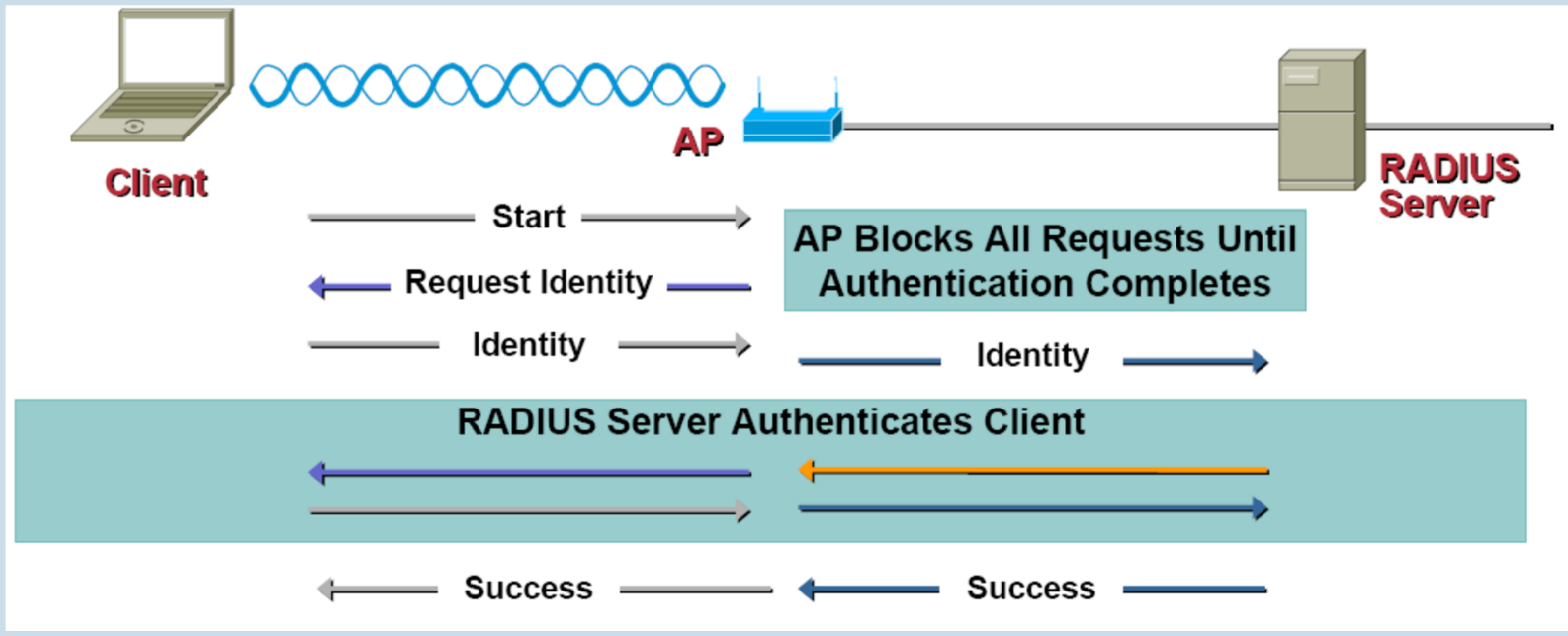


Method	Credential type	Authentication	Pros:	Cons:
EAP/MD5	• Fixed passwords	Challenge handshake authentication (similar to CHAP)	• Fairly easy to implement and deploy • Well supported	• Weak authentication mechanism • Does not provide mutual authentication
EAP/TLS (Transport Layer Security)	• Certificates	Mutual certificate authentication	• Strong authentication mechanism • Provides mutual authentication • Supports dynamic WEP key generation	• Difficult to implement and deploy • Requires public key infrastructure • Certificates required for both server and all client devices
EAP/TTLS (Tunneled TLS)	• Fixed passwords • One-time pass words (tokens) • Certificates	Sever-side authentication itself using a certificate while the client-side authentication occurs inside an encrypted tunnel	• Strong authentication mechanism • Provides mutual authentication • Supports dynamic WEP key generation	• More difficult to deploy than EAP/MD5 • Limited support in both hardware and software
Protected EAP (PEAP)	•Fixed passwords •One-time passwords (tokens) •Certificates	Similar to TTLS, except the inner authentication is another EAP method	• Strong authentication mechanism • Provides mutual authentication • Supports dynamic WEP key generation	• Emerging standard
EAP/Cisco (LEAP)	• Fixed passwords	Based around the MS-CHAP and MS-CHAPv2 authentication protocols	• Easy to implement and deploy • Provides mutual authentication • Supports dynamic WEP key generation	• Proprietary standard • Weak authentication mechanism if passwords are poorly chosen

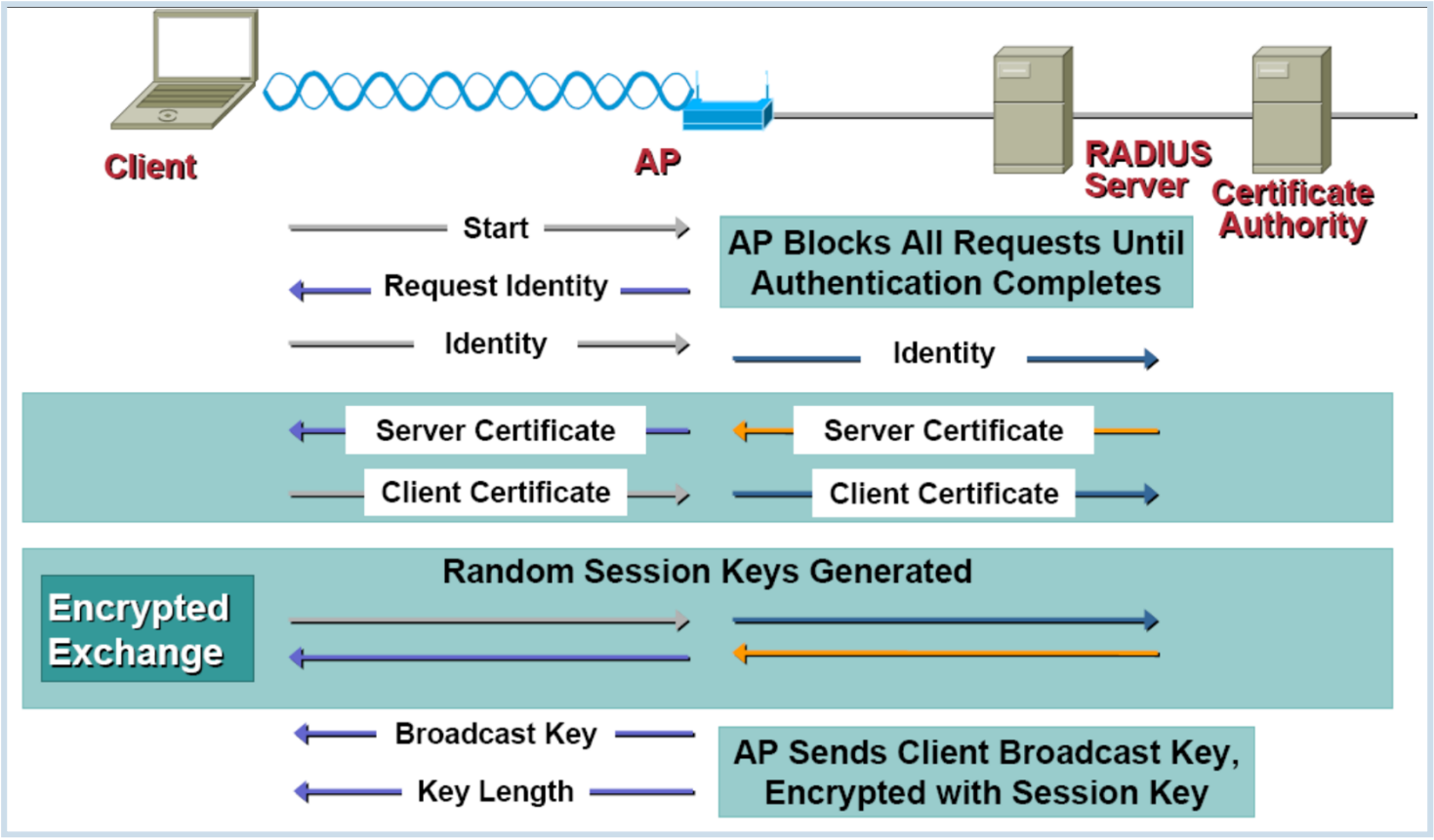
EAP TYPE	DYNAMIC RE-KEYING	MUTUAL AUTHENTI-CATION	USER ID & PASSWORD	ATTACK METHODS	COMMENTS
EAP-MD5	No	No	Yes	♦ Dictionary attack ♦ Man in the middle ♦ Session hijack	♦ Easy to implement ♦ Supported on many servers, but ♦ Insecure ♦ Requires cleartext databases
EAP-TLS	Yes	Yes	No	♦ Offers strong authentication security	♦ Requires client certificates ♦ Increases maintenance & token costs ♦ Two-factor authentication with smartcards
EAP-SRP	Yes	Yes	Yes	♦ Dictionary attack	♦ No certificates (server verifies secrets) ♦ Dictionary attack on credential store ♦ Intellectual property issues
EAP-LEAP	Yes	Yes	Yes	♦ Dictionary attack	♦ Proprietary solution ♦ AP must have LEAP support

EAP-SIM	Yes	Yes	No	◆ May be vulnerable to spoofing	◆ Leverages GSM roaming infrastructure ◆ Two-factor authentication
EAP-AKA	Yes	Yes	No	◆ Offers strong authentication security for cellular environment	◆ Leverages GSM roaming infrastructure ◆ Two-factor authentication
EAP-SecurID	No	No	No	◆ Man in the middle ◆ Session hijack	◆ Users PIN/One-time password ◆ Requires tunneled authentication ◆ Two-factor authentication
EAP-TTLS	Yes	Yes	No	◆ Offers strong authentication security	◆ Creation of secure TLS (SSL) tunnel ◆ Supports legacy authentication methods: PAP, CHAP, MS-CHAP, MS-CHAP V2 ◆ User identity is protected (encrypted)
EAP-PEAP	Yes	Yes	No	◆ Offers strong authentication security	◆ Similar to EAP-TTLS ◆ Creation of a secure TLS (SSL) tunnel ◆ User identity is protected (encrypted)

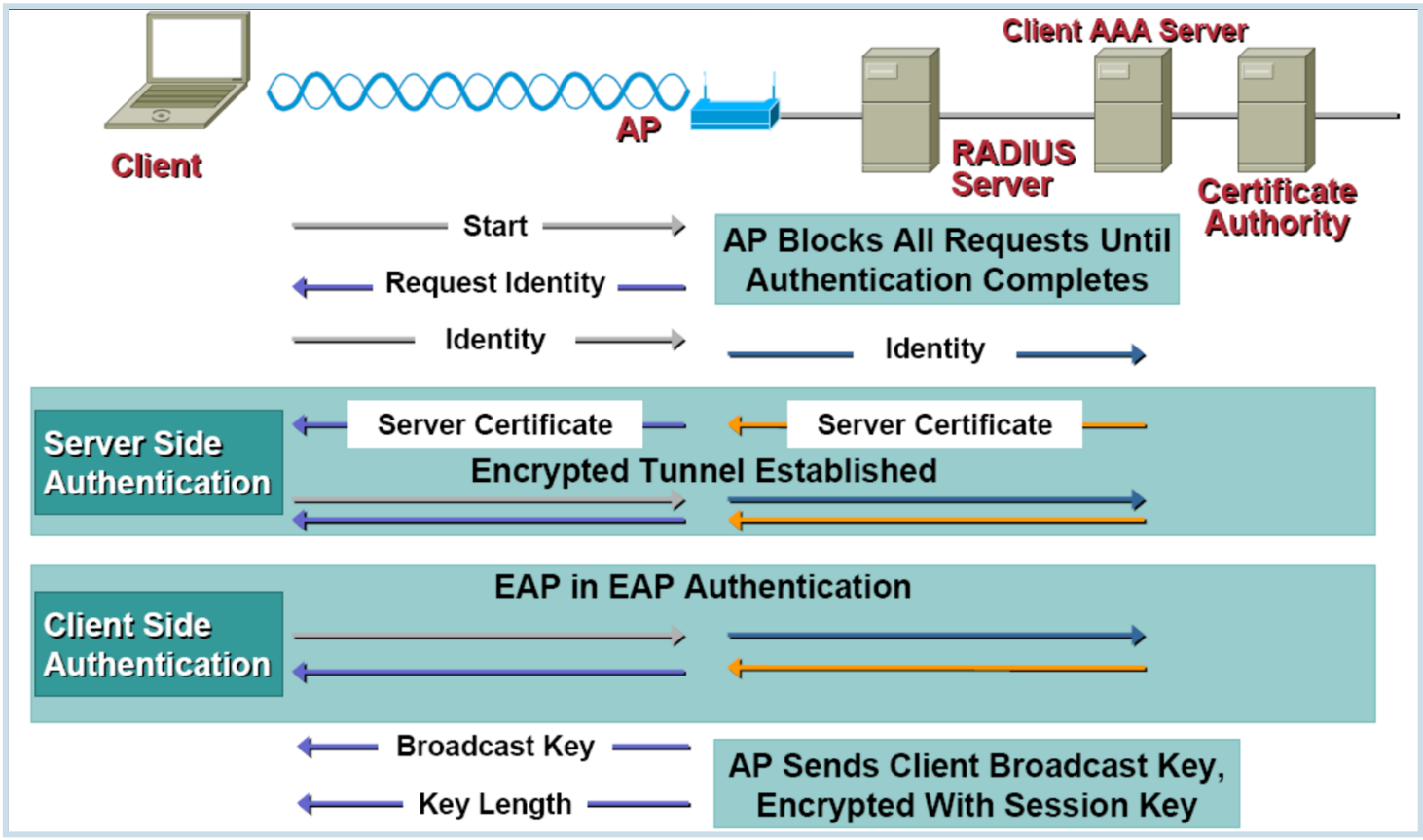
EAP-MD5


Client
AP
RADIUS Server
Start
Request Identity
Identity
AP Blocks All Requests Until Authentication Completes
Identity
RADIUS Server Authenticates Client
Success
Success

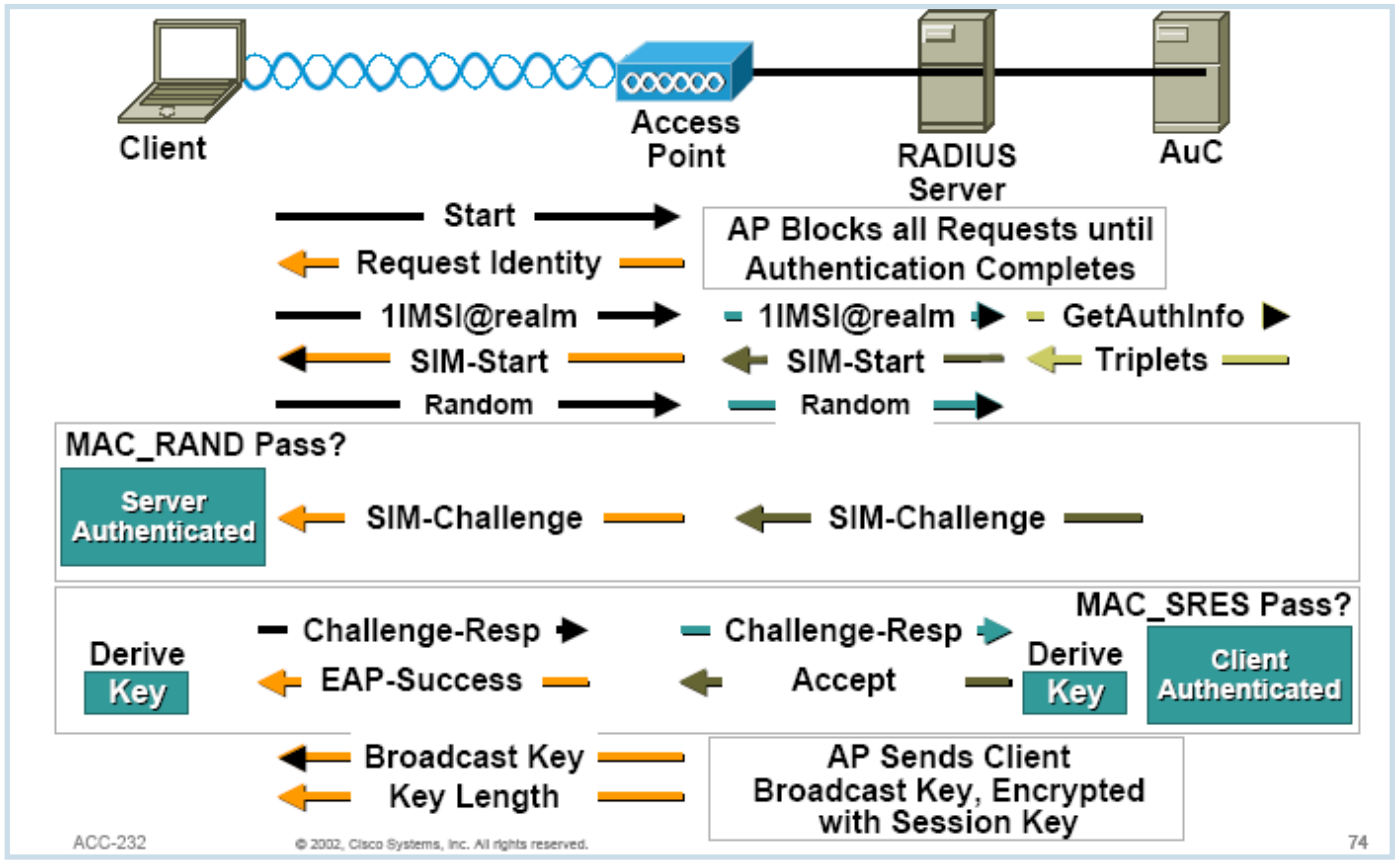
EAP-TLS


Client
AP
RADIUS Server
Certificate Authority
Start
Request Identity
Identity
AP Blocks All Requests Until Authentication Completes
Identity
Server Certificate
Server Certificate
Client Certificate
Client Certificate
Random Session Keys Generated
Encrypted Exchange
Broadcast Key
Key Length
AP Sends Client Broadcast Key, Encrypted with Session Key

Protected EAP



EAP-SIM


Client
Access Point
RADIUS Server
AuC
Start
AP Blocks all Requests until Authentication Completes
Request Identity
1IMSI@realm
1IMSI@realm
GetAuthInfo
SIM-Start
SIM-Start
Triplets
Random
Random
MAC_RAND Pass?
Server Authenticated
SIM-Challenge
SIM-Challenge
MAC_SRES Pass?
Derive Key
Challenge-Resp
Challenge-Resp
Derive Key
Client Authenticated
EAP-Success
Accept
Broadcast Key
Key Length
AP Sends Client Broadcast Key, Encrypted with Session Key
ACC-232
© 2002, Cisco Systems, Inc. All rights reserved.
74