IT-Sicherheit:

Drahtlose Sicherheit

(unter Benutzung von Material von Brian Lee und Takehiro Takahashi)

Sicherung des Zugangsnetzes

Network access security

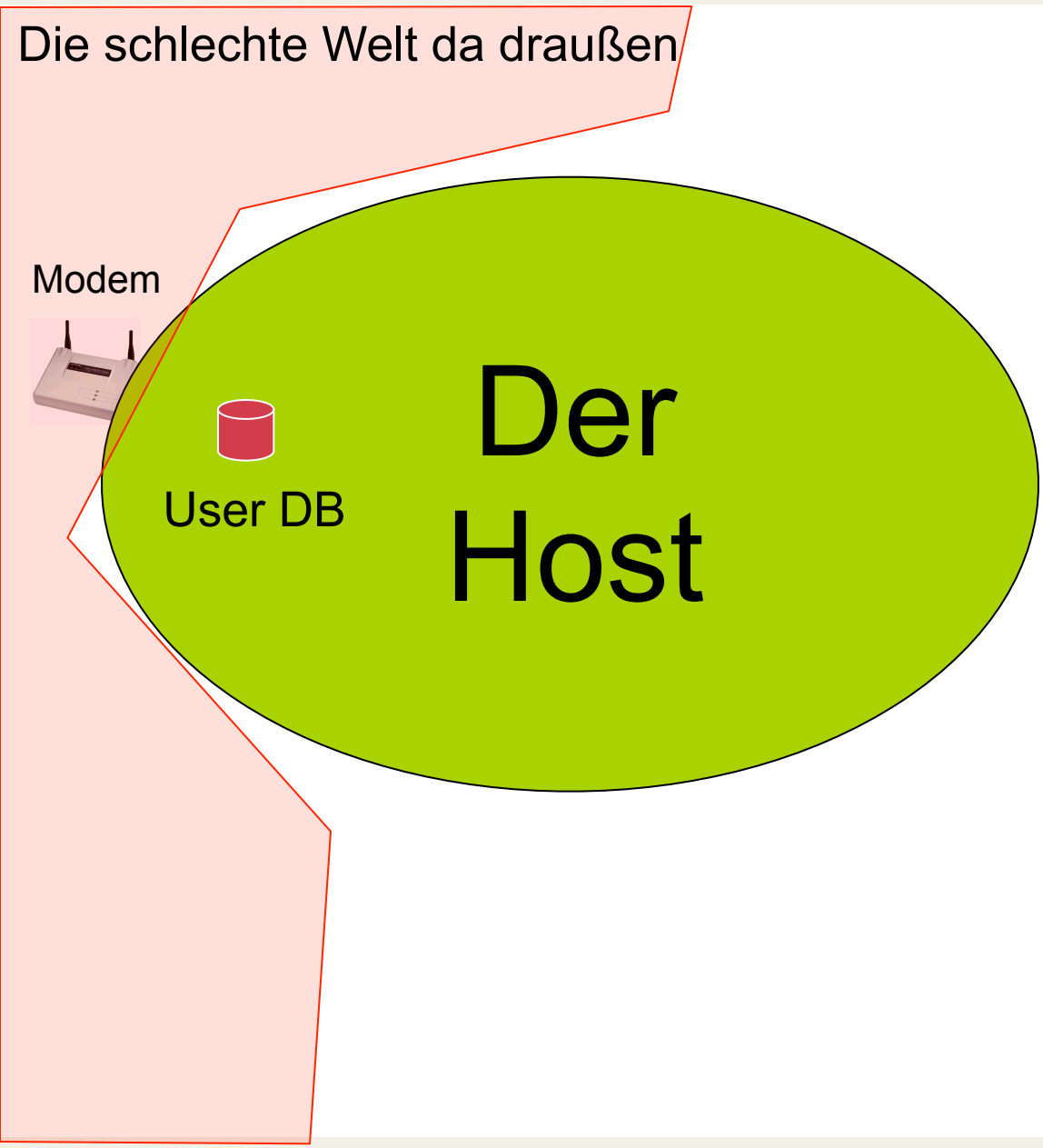
Überblick

- Traditionelle Sicherung des Zugangsnetzes
- WLAN-Sicherheit
- WLAN Roaming (nicht hier)

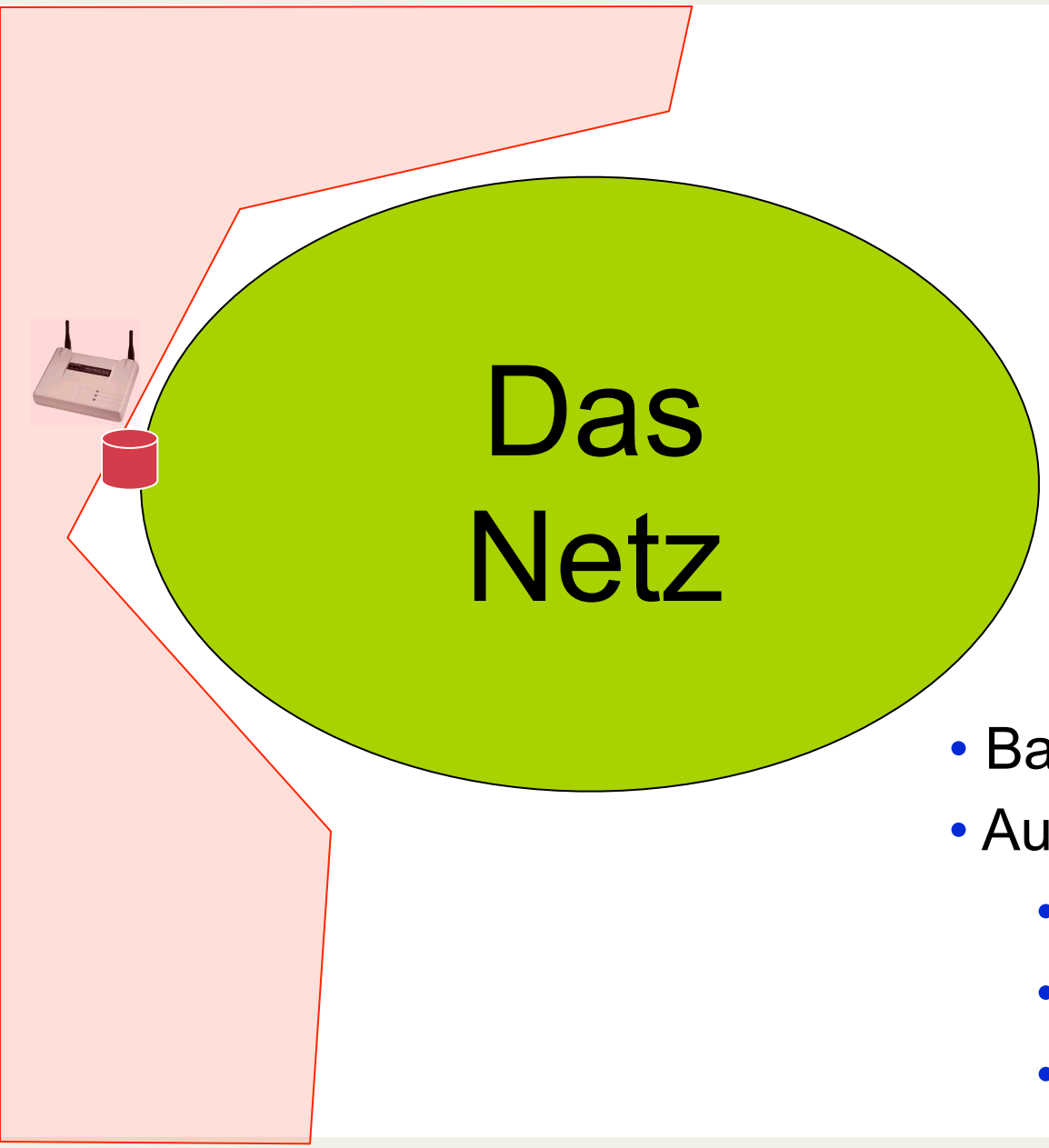
Überblick

- Traditionelle Sicherung des Zugangsnetzes
- WLAN-Sicherheit
- WLAN Roaming

Die alte Welt

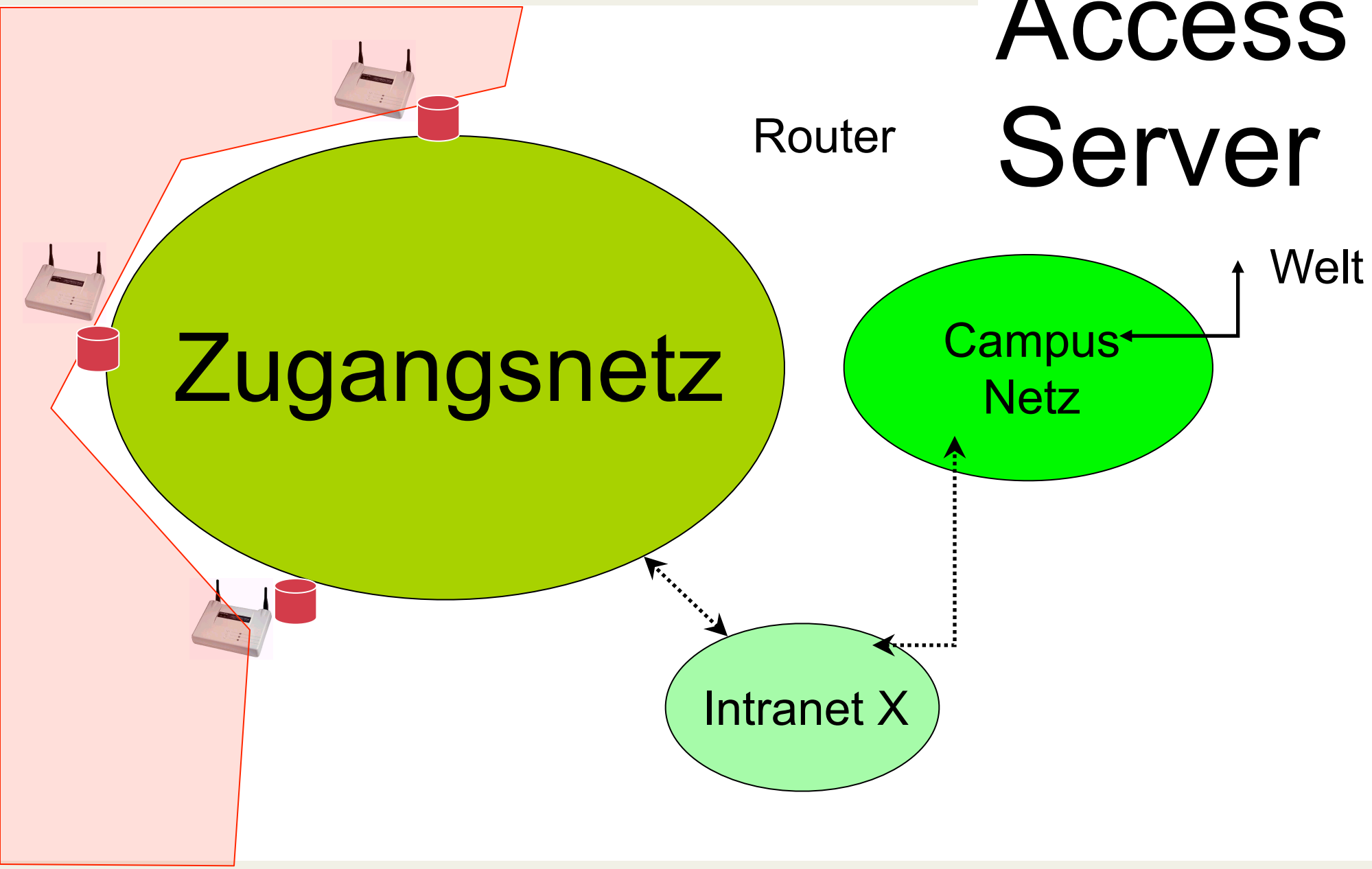


Access Server

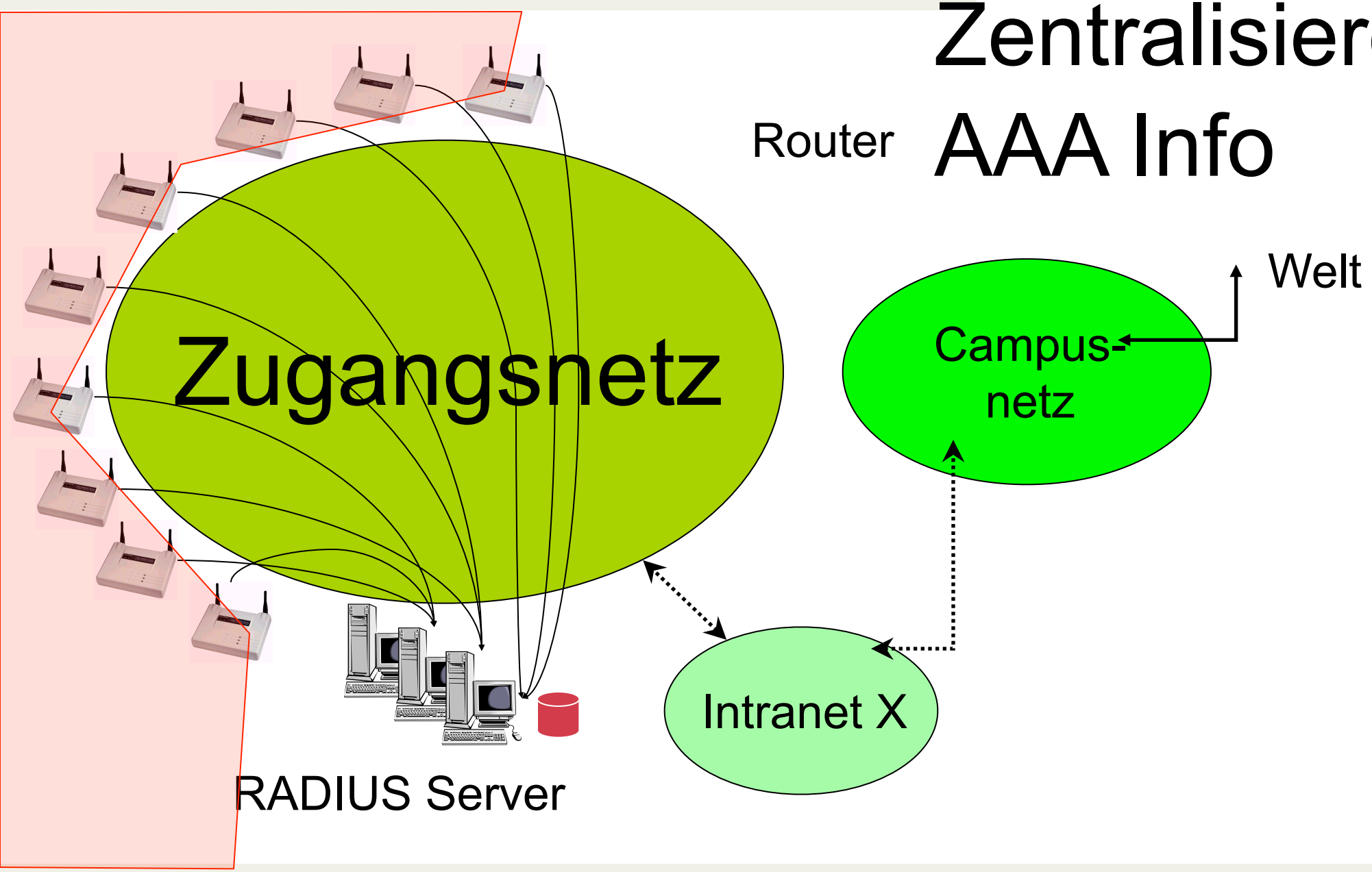


- Basisprotokoll: PPP
- Authentisierungsprotokolle:
  - PAP (Passwörter)
  - CHAP (Challenge/Response)
  - EAP (Plugin-fähig)

Access Server



Zentralisiere AAA Info



Elemente der traditionellen Sicherheit für den Netzzugang

- Behandle die Sicherung des Zugangsnetzes in Schicht 2
  - PPP und die dazugehörigen Authentisierungsprotokolle (PAP, CHAP, EAP)
  - Hauptsächlich Benutzer-/Passwort-basiert
- RADIUS als “Backend Protokoll”
  - Access Devices (PEPs, Policy Enforcement Points) bleiben “dumm”
  - RADIUS-Server ist der PDP (Policy Decision Point)
- NAIs und RADIUS Proxying
  - Network Access Identifier: cabo@tzi.de
  - Verwende den Teil hinter @, um den Home RADIUS Server zu identifizieren

802.1X: Sicherung des Zugangsnetzes im Ethernet

- Vor 802.1X:
  Jeder konnte sich an einen Switch „hängen“ und auf diese Weise Zugang zum Netz erhalten
- 802.1X: EAP over LAN
  - Supplicant: Client-Gerät, das versucht, Zugang zum Netz zu erhalten
  - Authenticator (PEP): Switch
  - Authentication Server (PDP): RADIUS Server
- Switch kann Entscheidungen treffen, die auf Informationen beruhen, die vom RADIUS Server zurückgeliefert werden

  (wie z.B. die VLAN-Zuordnung)

Was ist zu schützen?

- Knappe Netzressourcen
  - Dial-in Pool etc.
- Netzsicherheit
  - Häufig war die Sicherung des Zugangsnetzes die einzige Sicherheit für das gesamte Netz!
    - Heutzutage wegen des Internets keine Option mehr
  - Privilegierte IP-Adressen
  - Zugriff hinter dem Firewall

Übersicht

- Traditionelle Sicherung des Zugangsnetzes
- WLAN-Sicherheit
- WLAN Roaming

WLANs sind anders

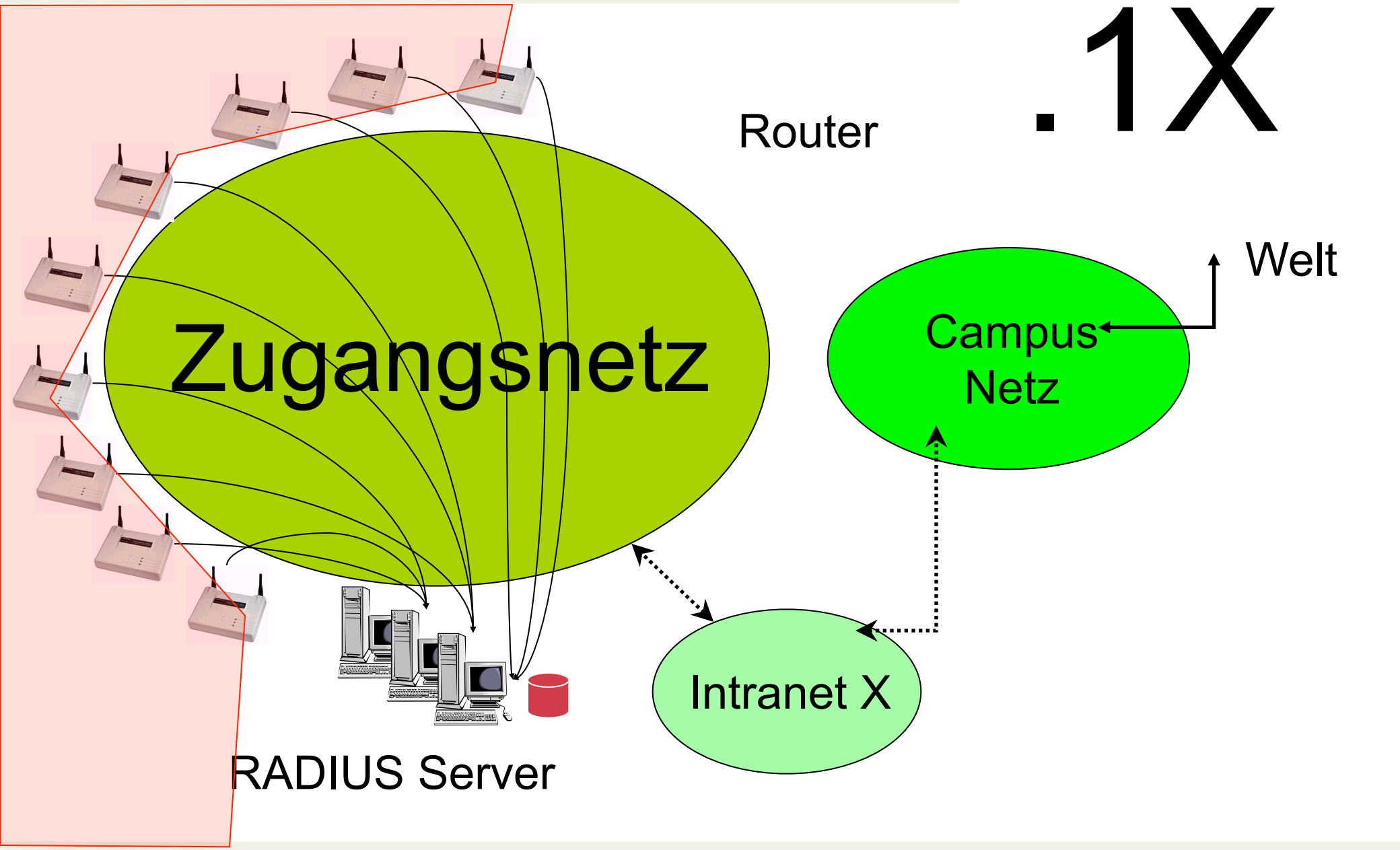
- WLANs sind funk-basiert
  - Jeder kann alles hören
  - Vertraulichkeitsanforderungen
- Keine „Leitungen“ mehr
  - Unerwünschte Access-Points können Informationen hinzufügen oder manipulieren
- Keine hohen Ressourcenanforderungen
  - WLAN ist „schnell“
  - ISM-Band Funk kann sowieso nicht geschützt werden

WLAN-Sicherheit: Anforderungen (Sicht Universität)

- Vertraulichkeit (Privacy):
  - Fremder Datenverkehr kann nicht verstanden werden
  - Angriffe von Insidern genauso wahrscheinlich wie Angriffe von außen
- Accountability:
  - Möglichkeit, herauszufinden, wer was getan hat
  - Voraussetzung: Authentisierung

WLAN-Sicherheit: Ansätze

- **AP-basierte Sicherheit**: AP ist die Grenze des Netzes
  - WEP (gebrochen), WEP Fixes
  - 802.1X (EAP-Varianten + RADIUS) + 802.11i (“WPA Enterprise”)
- **Netzbasierte Sicherheit**: starke Sicherheit
  - VPNs werden von mobilen Benutzern sowieso verwendet
    - SSH, PPTP, IPsec
  - Alternative: Web Diverter (temporäres Filtern von MAC-/IP-Adressen)
    - Allerdings keine Vertraulichkeit

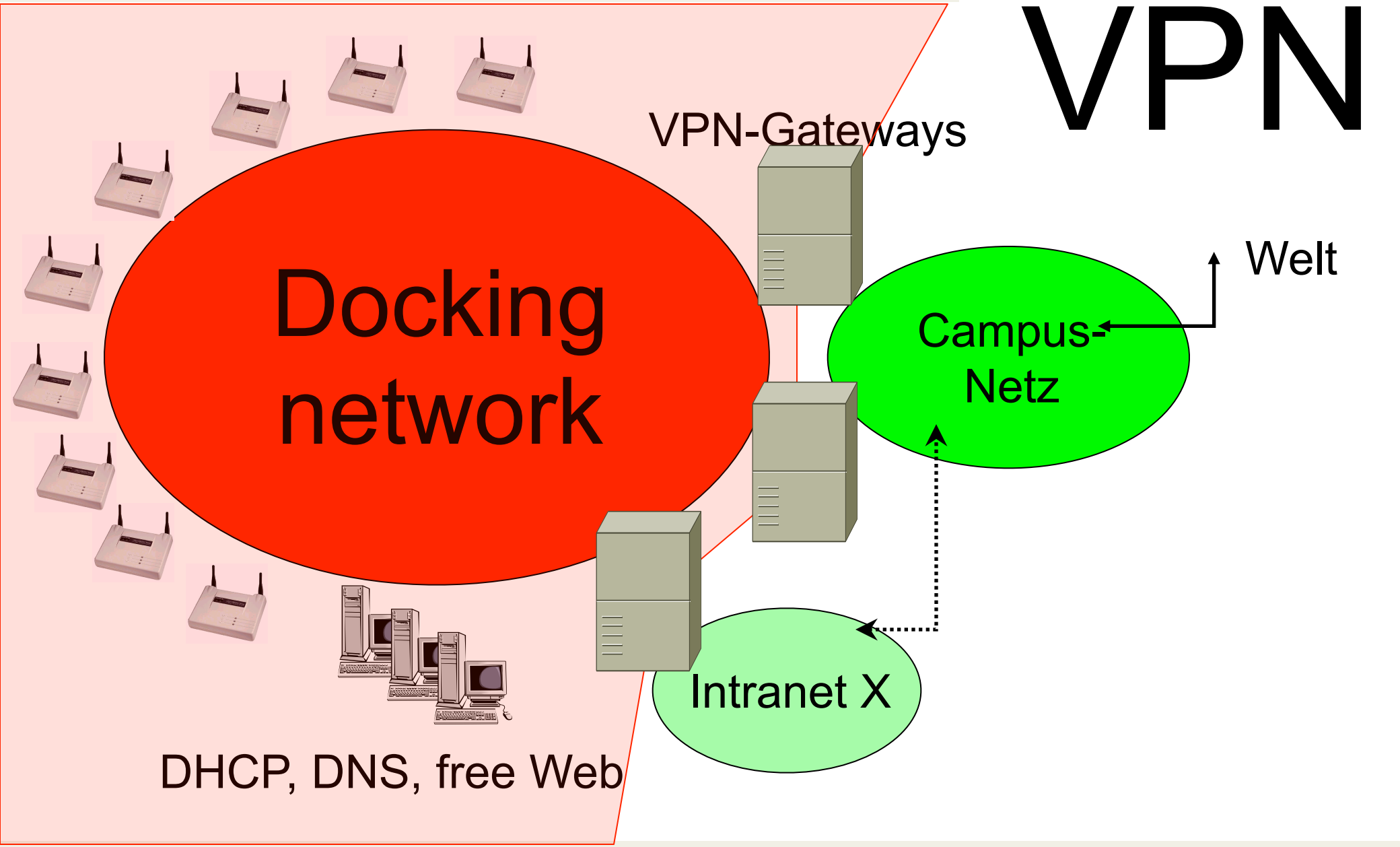

.1X
Router
Zugangsnetz
Welt
Campus
Netz
Intranet X
RADIUS Server

WLAN-Zugangskontrolle: Warum 802.1X besser ist

- 802.1X hat sich weitgehend durchgesetzt
- Mehrere EAP/XYZ-Varianten sind inzwischen weit verbreitet
- Wird von immer mehr Systemen unterstützt (Windows 2000 aufwärts)
- Aufwendige Kryptographie wird auf viele APs verteilt
- Angreifer werden so früh wie möglich abgewehrt
  - Roaming: mehr Kontrolle durch Administratoren der Gastgeber-Sites

- Vor allem aber: It just works™

VPN

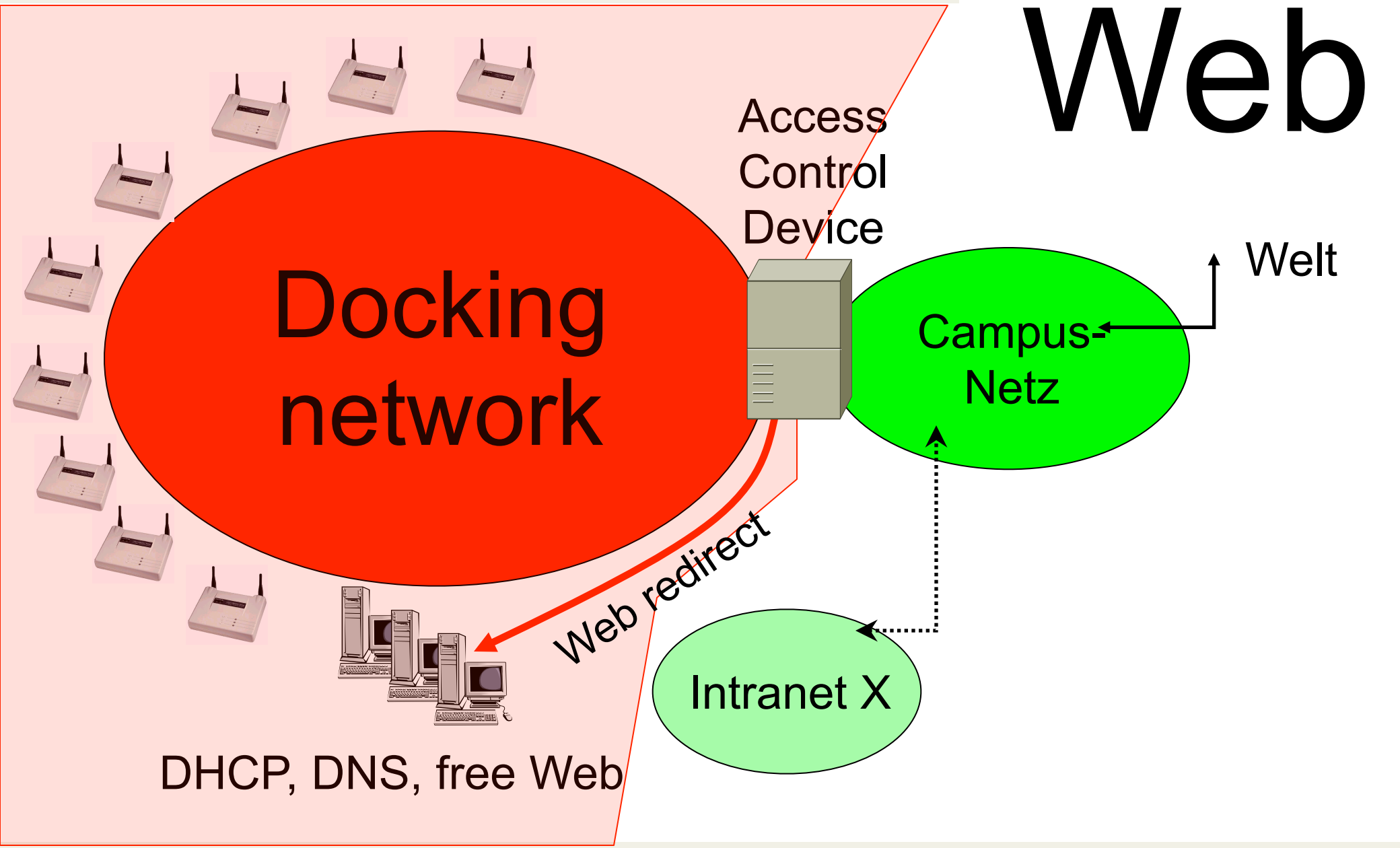

VPN-Gateways
Docking network
Welt
Campus-Netz
Intranet X
DHCP, DNS, free Web

WLAN-Zugangskontrolle: Warum ein VPN besser ist

- Aus historischen Gründen sollte man der Sicherheit in Schicht 3 mehr als der Sicherheit in Schicht 2 trauen:
  - IPsec ist eingehend auf Sicherheitsprobleme hin analysiert worden
- Man kann billige/„dumme“/nicht vertrauenswürdige APs nutzen

- Auf fast *allen* Systemen (Windows 98, PDA etc.) verfügbar
- Leicht für mehrere Sicherheitskontexte anzupassen
  - Sogar mit einer Infrastruktur „von vor 2003“
  - Die Daten sind nun auf der Luftschnittstelle und bis zum VPN Gateway gesichert

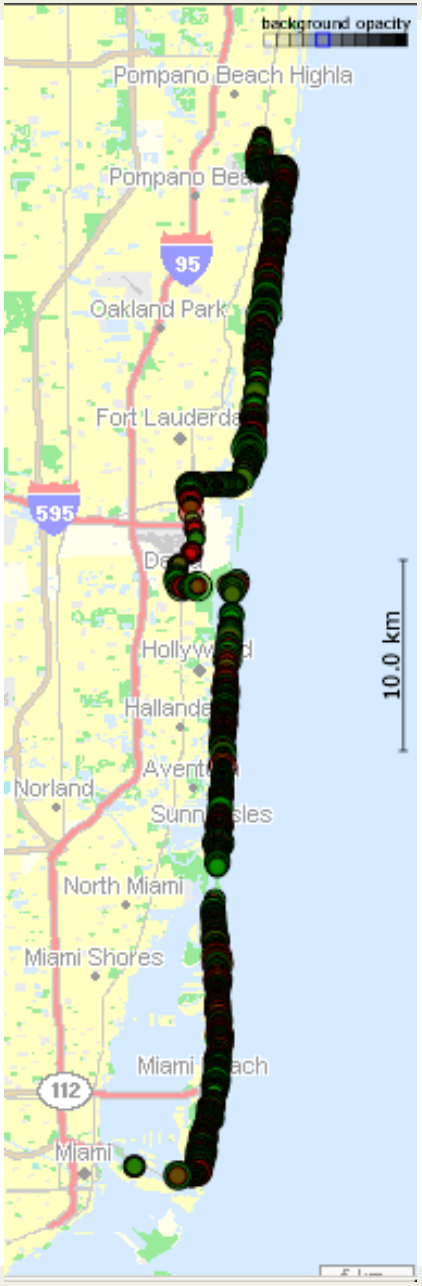
- Aber vor allem: It just works™


Web
Access
Control
Device
Docking
network
Welt
Campus-
Netz
Web redirect
Intranet X
DHCP, DNS, free Web

WLAN-Zugangskontrolle: Warum Web-basiertes Filtern besser ist

- Keine Software auf dem Client benötigt (jeder hat ja einen Browser)
- Passt gut zu den bereits existierenden Benutzer/Passwort-Schemata
- Kann einfach für Gastbenutzer eingerichtet werden
  - Die Hotspots benutzen Web-basiertes Filtern, so dass Gastbenutzer dies schon kennen
  - Passt auch gut zu Hotspot-Föderationen
- Privacy ist hier nicht sicherzustellen (verwende TLS und SSH)
- Accountability ist kaum herzustellen.

- Aber vor allem: It just works™



2561
Access Points!

Eingebaute Sicherheitsmechanismen

- Service Set Identifier (SSID)
- Wird zur Unterscheidung von APs verwendet
- SSID wird alle paar Sekunden in *Beacon Frames* per Broadcast versendet.
- Beacon Frames werden im Klartext verschickt!
- Erste Sicherheitsschicht
- Stealth Mode – Testanfrage (*probe request*)

Was man in Bezug auf SSIDs tun und was man nicht tun sollte

- Default SSIDs sind weit verbreitet (Linksys AP Default ist `linksys`, Cisco Default ist `tsunami` etc.): Verwirrung

  ➔ Default-SSIDs ändern!

- ? Ändere die Einstellungen im AP, so dass dieser nicht mehr die SSID in einem Beacon Frame per Broadcast versendet

- Warum?

Verbergen der SSID

- Wie bereits erwähnt, wird die SSID standardmäßig alle paar Sekunden per Broadcast versendet
- + Wenn man dieses Feature abschaltet, dann kann man schwerer herausfinden, dass man es überhaupt mit einer drahtlosen Verbindung zu tun hat
- – Lesen von Rohpaketen (*raw packets*) offenbart die SSID
  - Selbst wenn WEP verwendet wird, ist die SSID im Klartext
- – Schwieriger in Betrieb zu nehmen
  - Windows scheint hier durcheinander zu kommen

Filtern von MAC-Adressen

- Durch Filtern von MAC-Adressen dürfen sich nur bestimmte Geräte mit einem AP assoziieren
- – Management in großen Netzen undurchführbar
- – Selbst bei Verschlüsselung der Daten kann man mit Hilfe eines Paket-Sniffers sehr leicht eine gültige MAC-Adresse finden und dann über das Betriebssystem die eigene so abändern, dass diese verwendet wird
- ➔ Micky-Maus-„Sicherheit“ für sehr kleine Netze, die sich nur vor zufälligen Angriffen schützen müssen

Verbinden mit dem AP

- Access Points haben zwei Möglichkeiten, eine Verbindung mit einem Client zu initiieren:
  - Shared Key- oder Open Key-Authentisierung
- Open Key-Authentisierung erlaubt jedem Client, eine Verbindung mit dem AP aufzubauen
- Shared Key-Authentisierung soll zusätzliche Sicherheit bringen, indem sie Ausweisinformationen (*credentials*) erfordert, wenn man sich verbindet

Wie die Shared Key-Authentisierung funktioniert

- Challenge Response:
  - Client sendet eine Anforderung für eine Verbindung an den AP
  - AP antwortet mit einer unverschlüsselten Challenge
  - Client verschlüsselt die Challenge mit Hilfe eines korrekten WEP-Schlüssels und sendet diese zum AP zurück
  - Wenn die Challenge korrekt verschlüsselt worden ist, dann erlaubt der AP die Kommunikation mit dem Client

Ist die Open Key- oder Shared Key-Authentisierung sicherer?

- Merkwürdigerweise ist die Open Key-Authentisierung sicherer!

- Mit Hilfe von passivem Sniffen kann man zwei der drei Parameter abfangen, die für die Shared Key-Authentisierung benötigt werden, nämlich:

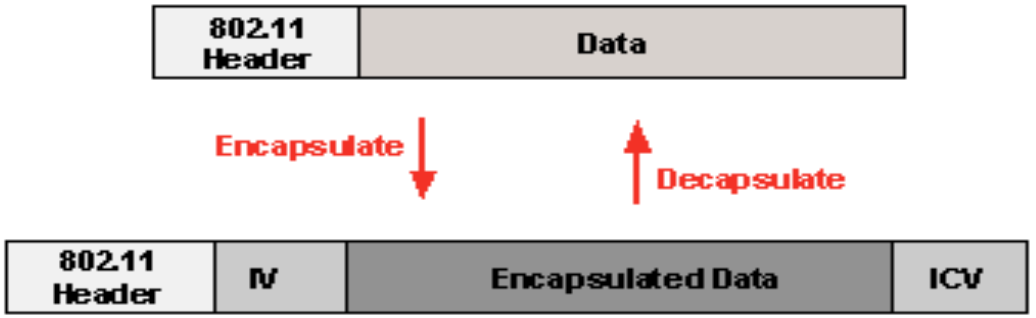
  Challenge und die verschlüsselte Challenge

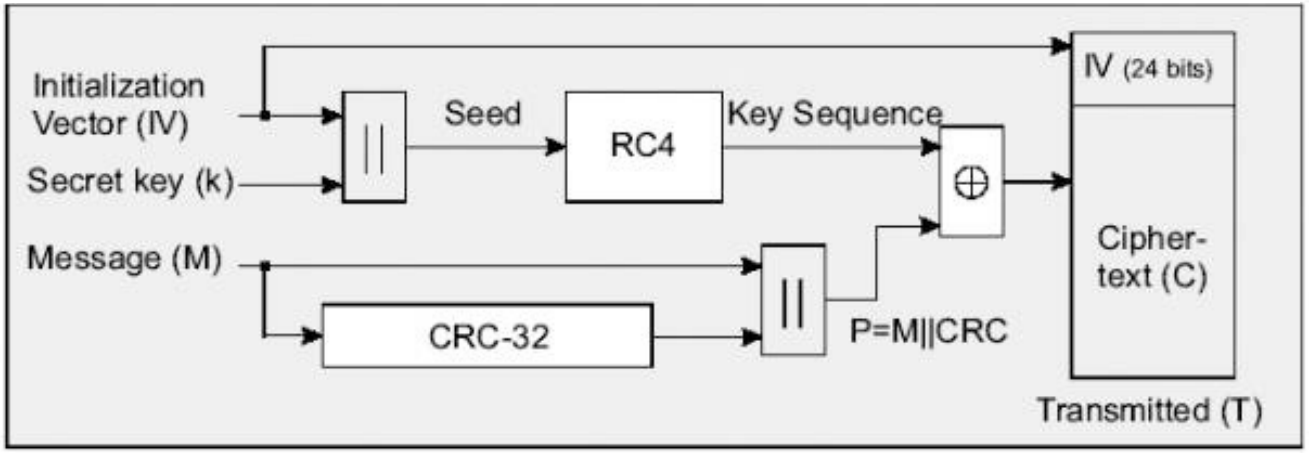
  - Kann man durch einen Dis-Assoziierungsangriff (***disassociation attack***) erhalten

Wired Equivalent Privacy (WEP)

- Ursprüngliche Sicherheit für das 802.11-Protokoll
- Sollte drahtlose Netze genauso sicher machen wie das herkömmliche Netz
- Sollte „Vertraulichkeit“, „Integrität“ und „Authentisierung“ sicherstellen
- Verwendet 40-Bit-RC4-Verschlüsselung
- Leider hat sich diese Art, RC4 zu verwenden, seit der Annahme des 802.11-Standards als unsicher erwiesen:
  - Das 802.11 Protokoll ist verwundbar gegenüber unterschiedlichsten Arten von Angriffen

WEP-Verschlüsselung





Probleme mit WEP (1)

- Schlüssellänge ist zu kurz (40 Bits!)
  - Brute Force-Angriff ist möglich
- Keine Spezifikation für die Schlüsselverteilung
  - Keine Skalierbarkeit
- ➔ Ein statischer Schlüssel!
  - Keine noch so gute Verschlüsselung ist stark, wenn ein Schlüssel für immer verwendet wird

Probleme mit WEP (2)

- Verwenden von CRC32 als ICV (*integrity check value*)
  - Bit flipping-Angriff:
    `CRC(msg XOR delta) = CRC(msg) XOR CRC(delta)`
  - Bits können zwar nicht gezielt gesetzt oder gelöscht, dafür aber umgedreht werden
- Kein Schutz vor Replay-Angriffen
- Falsche Anwendung von RC4
  - Protokoll spezifiziert nicht, wie IVs verwendet werden sollen
  - Es existieren zwei Angriffe

Angriff auf die Länge des IVs

- IVs sind nur 24 Bit lang und somit gibt es nur 16 777 216 mögliche Werte für die IVs
- Ein Netz mit viel Datenverkehr wird die IVs also oft wiederholen
- Indem der verschlüsselte Verkehr mitgeschnitten wird und Duplikate der IVs eingesammelt werden, kann man den Klartext wiedergewinnen

FMS-Angriff (Weak IV-Angriff)

- Manche IVs sind für RC4 unbrauchbar!
- Wenn man eine Formel nutzt, kann man diese IVs verwenden, um Teile des WEP-Schlüssels abzuleiten
  - 5 % Wahrscheinlichkeit, richtig zu raten
- Es gilt wieder: Eine passive Überwachung des Netzes ein paar Stunden lang kann bereits ausreichen, genug schwache IVs einzusammeln, um den WEP-Schlüssel zu ermitteln
- 4M ~ 6M Pakete, um einen 40-Bit-WEP-Schlüssel zu ermitteln
- Die Zeit, die man zur Durchführung des Angriffs benötigt, ist **proportional** zur Schlüssellänge
  - 104-Bit-Schlüssel sind nur 2.6 mal sicherer als 40-Bit-Schlüssel
- Fluhrer, Mantin, Shamir: Weaknesses in the key scheduling algorithm of RC4. In *8th Annual Workshop on Selected Areas of Cryptography*, 2001

Zusammenfassung: WEP

- Vertraulichkeit
  - FMS-Angriff
- Integrität
  - Bit-flipping-Angriff
- Authentisierung
  - Nicht wirklich

- WEP ist gebrochen, und es gibt keine einfache Möglichkeit, WEP zu reparieren
- Angriffe auf WEP sind passiv möglich und extrem schwer zu erkennen

WEP NICHT MEHR VERWENDEN!

Übersicht

- Traditionelle Sicherung des Zugangsnetzes
- WLAN-Sicherheit
- WLAN Roaming

Virtual Private Networks (VPN)

- Ein sicheres VPN über ein drahtloses Netz kann die Sicherheit der Daten substantiell erhöhen
- Die Idee ist hier, dass ein drahtloses Netz genauso wie ein unsicheres Netz (das Internet) behandelt wird
- Das „docking network“ führt nur zu den VPN-Gateways

Probleme des VPN-Ansatzes

- Erheblicher Aufwand bei der Inbetriebnahme
- Performance skaliert nicht mit der Anzahl der eingerichteten APs
  - PC: Krypto-Geschwindigkeiten liegen bei ungefähr 500 Mbit/s, stark parallelisierbar
- Anfällig für DoS-Angriffe
  - Zum Beispiel gegen DHCP/DNS im Docking Netz
- PCs im Docking-Netz sind verwundbar
- Anfällig für Angriffe auf das jeweils gewählte VPN
  - Begründete Annahme: Kann schnell in Ordnung gebracht werden (VPNs haben eine Schnittstelle zum Internet!)
  - (aber PPTP mit MSCHAPv2 ist ziemlich anfällig für Wörterbuch-Angriffe)

Zurück zu Lösungen auf der Schicht 2 (Netzgrenze)

- 802.1x
  - Authentisierung für jeden einzelnen Nutzer
  - Mechanismus für die Schlüsselverteilung
- 802.11i „RSN“ (Robust Security Network)
  - 802.1x mit EAP + AES + CCM
- WPA
  - Teilmenge von 802.11i
  - Zwei Arten
    - Enterprise mode: 802.1x mit EAP + TKIP (enthält MIC)
    - Personal mode: Pre-shared Schlüssel + TKIP (enthält MIC)

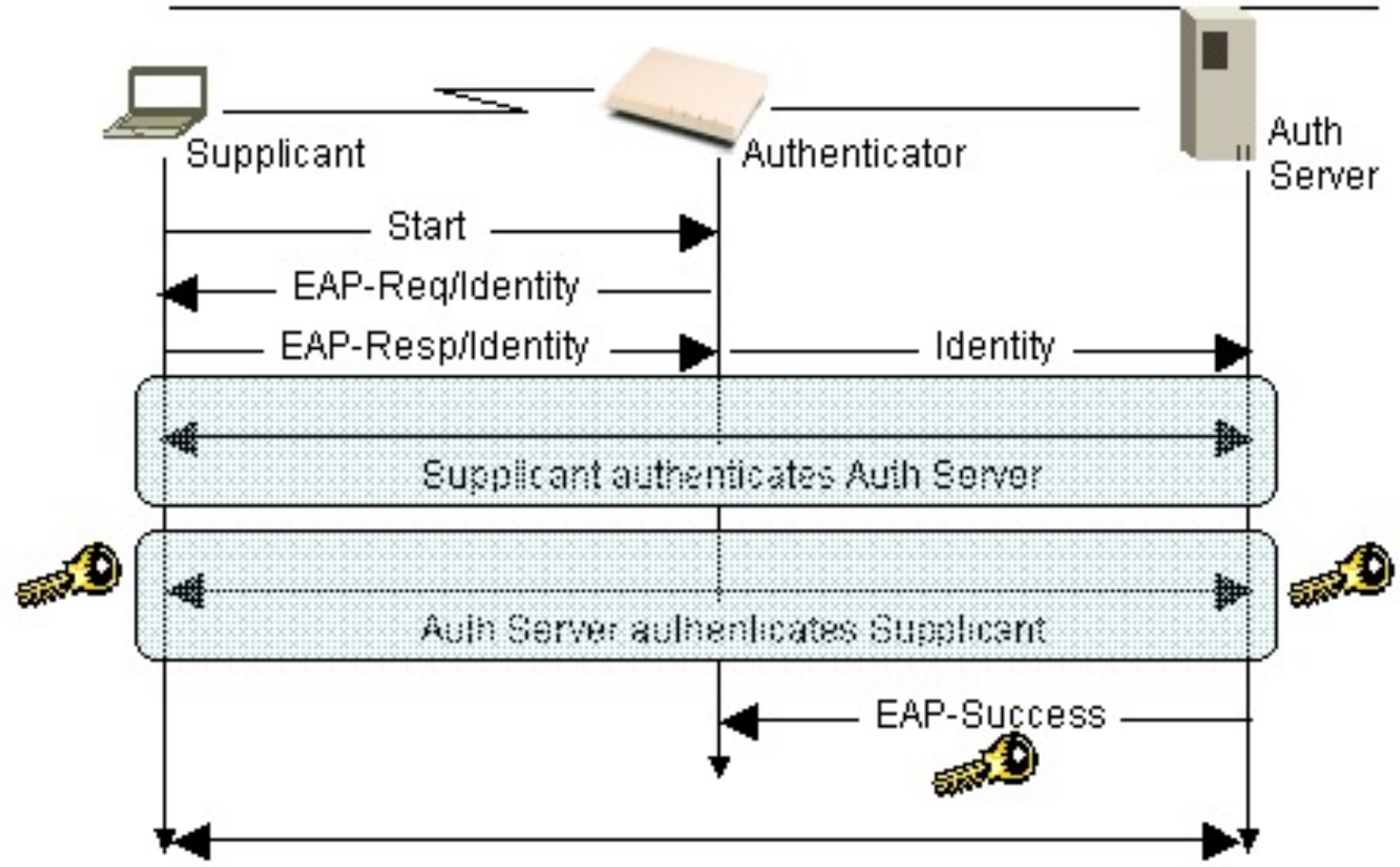
802.1X-Authentisierung

- 802.1X ist port-basiert, Rahmenwerk zur Authentisierung in IEEE 802-Netzen auf Schicht 2 (MAC-Adressen-Schicht)
- Nicht nur anwendbar in 802.11-Netzen
- Verwendet EAP für die Implementierung
- 802.1X ist keine Alternative zu WEP: Es arbeitet mit dem 802.11-Protokoll zusammen, um die **Authentisierung** von WLAN Clients zu regeln
  - Erzeugt auch temporäre Schlüssel für die Verschlüsselung und zur Sicherstellung der Datenintegrität

Wie die Authentisierung durchgeführt wird

- Ein Client verlangt Zugriff auf den AP
- Der AP fragt nach einer Menge von Ausweisinformationen (***credentials***)
- Der Client schickt die Ausweisinformationen an den AP, der seinerseits die Ausweisinformationen an den Authentisierungsserver weiterleitet
- Das genaue Verfahren, um die Ausweisinformationen zu verteilen, wird in 802.1X selbst nicht festgelegt
  - Verwendet EAP über LAN (EAPOL)

802.1x-Authentisierung



Extensible Authentication Protocol (EAP)

- 802.1X verwendet EAP für sein Rahmenwerk zur Authentisierung
- Flexibel: Einmalpasswörter, Zertifikate, Chipkarten, eigene EAP-Protokolle etc.
-
- Kosteneffizient
  - 802.1X passt gut zu anderen offenen Standards wie RADIUS
  - RADIUS ist der De-facto Standard für ein Backend-Protokoll zur Authentisierung an einem Network Access Server

EAP-MD5

- EAP-MD5 ist ein einfaches EAP-Protokoll (ähnlich CHAP)
- Verwendet einen MD5-Hash des Benutzernamens, eine Challenge für den Server und ein Passwort, das zum RADIUS-Server gesendet wird
  - Verwundbar gegen Wörterbuch-Angriffe
- Authentisiert nur in einer Richtung
  - Middle-Person-Angriff
- Keine Schlüsselerzeugung

LEAP (Cisco Wireless)

- Wie MD5 verwendet LEAP ein Login-/Password-Schema, welches an den RADIUS-Server gesendet wird
- Jeder Nutzer erhält einen dynamisch erzeugten Einmalschlüssel beim Login
- Authentisiert Client am AP und vice versa
- Kann auch mit RADIUS Session Time Out Feature verwendet werden, um Schlüssel an dynamisch festgelegten Intervallen zu erzeugen
- Funktioniert nur mit Cisco Wireless Clients
- Gebrochen – ASLEAP von Joshua Wright
  - Wörterbuch-Angriffe zu leicht durchzuführen

EAP-TLS

- Anstelle eines Benutzername-/Passwort-Schemas verwendet EAP-TLS eine auf Zertifikaten beruhende Authentisierung
- Dynamische Erzeugung von Einmalschlüsseln
- Zwei-Wege-Authentisierung
- Verwendet TLS (Transport Layer Security), um die PKI-Information an den RADIUS Server weiterzureichen
- Mit vielen Betriebssystemen kompatibel
- Schwerer zu implementieren und „auszurollen“, weil Schlüssel/Zertifikate für Clients erzeugt werden müssen

EAP-TTLS (Bob Funk)
PEAP von Microsoft und Cisco

- Sehr ähnlich zu EAP-TLS; allerdings brauchen die Clients sich nicht selbst mit einem Zertifikat beim Server zu authentisieren
  - Phase 1: Es kann eine gefälschte Identität (*bogus identity*) vom Client verwendet werden (muss aber gut genug sein, um den Authentisierungsserver zu finden); nur der Server authentisiert sich in dieser Phase
  - Phase 2: Der durch TLS geschützte Kanal kann für ein einfaches Login-/Passwort-Schema vewendet werden (z.B. MSCHAPv2 verwenden)
- Leichter einzurichten, erfordert nicht notwendigerweise eine PKI
- PEAPv0 arbeitet ursprünglich mit Windows XP SP1, aber andere Plattformen beginnen es nun auch zu unterstützen; EAP-TTLS wird immer mehr von Open Source Software unterstützt

EAP-Arten

	Offen / Proprietär	Gegen-seitige Auth.	Auth. Client	Auth. Server	Nutzername im Klartext
MD5	Offen	Nein	Ben./ Pass.	Kein	Ja
TLS	Offen	Ja	Zertifikat	Zertifikat	Ja
TTLS	Offen	Ja	Ben./ Pass.	Zertifikat	Nein
PEAP	Offen	Ja	Ben./ Pass.	Zertifikat	Nein
LEAP	Proprietär	Ja	Ben./ Pass.	Kein	Ja

WPA-Schritte (Enterprise)

- 802.1x Authentisierung und Erzeugung von PMK
- 4-Way-Handshake und PTK-Installation
- Installation von Gruppenschlüsseln (GTK)
- Verschlüsselung mit TKIP (WPA) oder AES/CCM (WPA2)

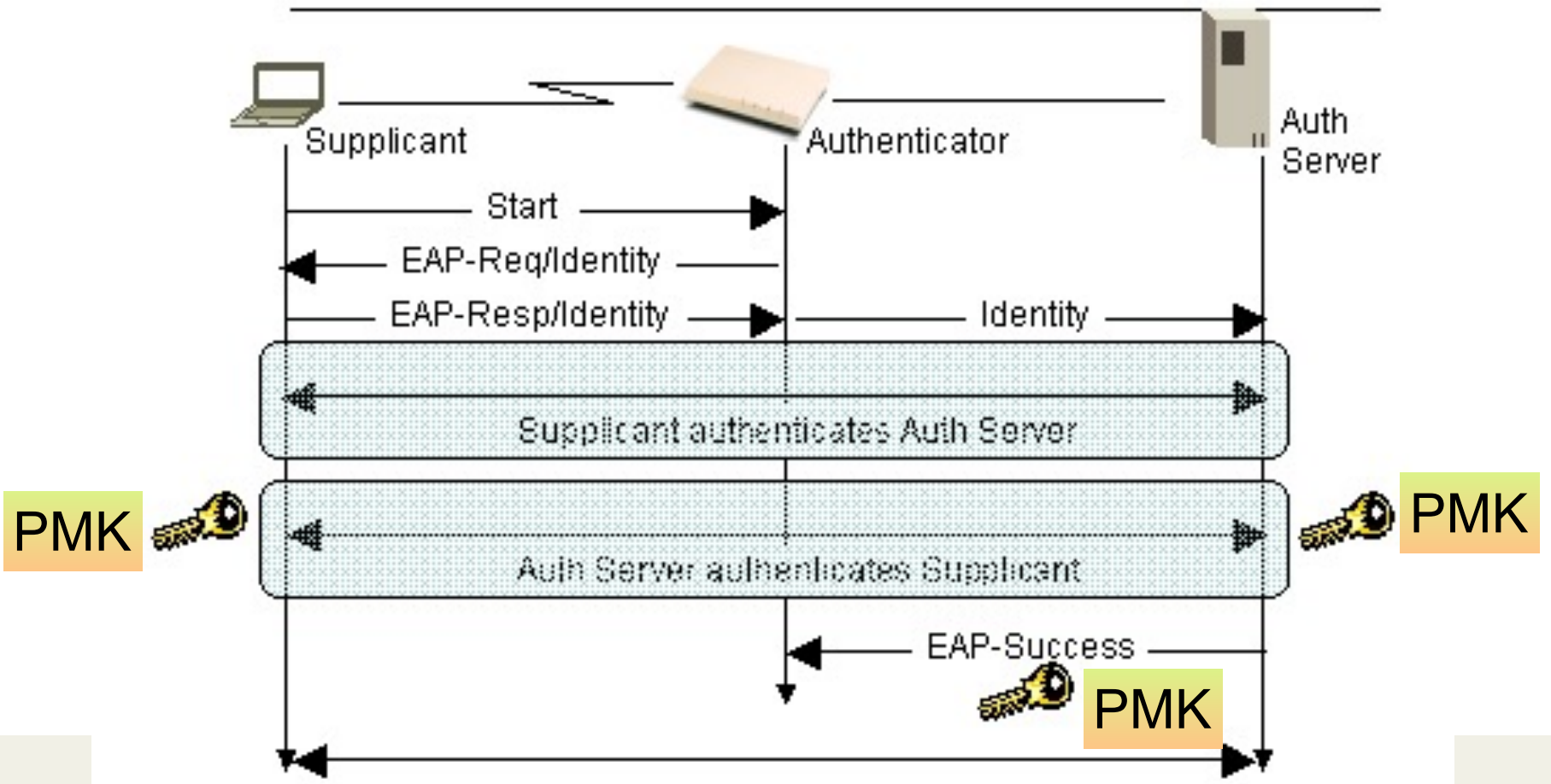
802.1x Authentisierung + PMK

Pairwise Master Key (PMK):

- Authentisierungsprozess nutzt einen sicheren Kanal
- Dieser kann auch für die Erzeugung des PMKs verwendet werden

- PMK ist die Basis für die Erzeugung eines temporären WEP-Schlüssels in der nächsten Phase
- PMK wird erzeugt, indem das Ergebnis der Authentisierung des Benutzers zugrundegelegt wird

802.1x Authentisierung + PMK

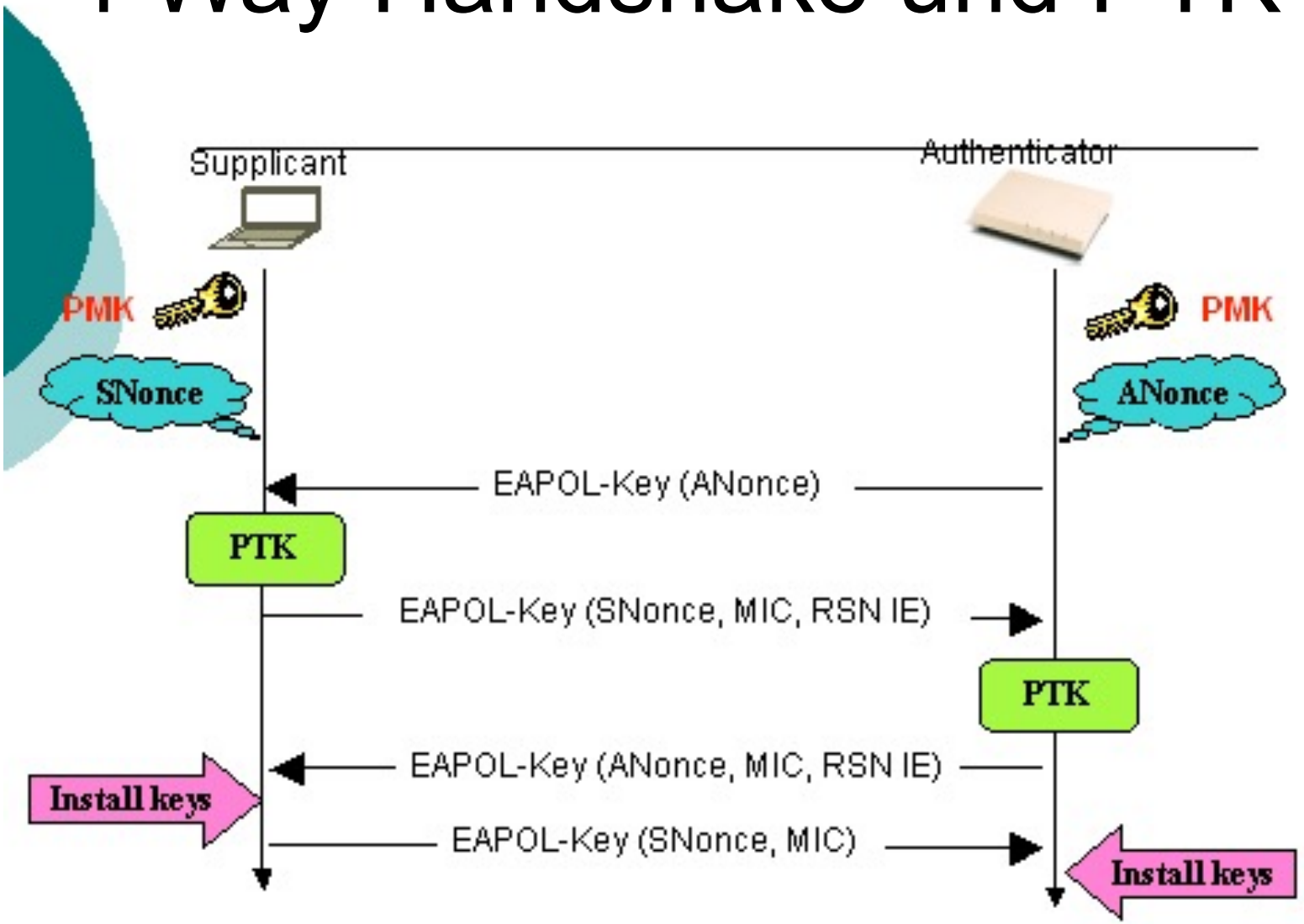


Situation nach erfolgreicher Durchführung von EAP

- Supplicant (Station) und Authentisierungsserver haben sich gegenseitig authentisiert, sie kennen beide den PMK
- Authentisierungsserver sendet dem AP (Authentikator) den PMK

- Die Station und der AP müssen sich nun gegenseitig beweisen, dass sie den PMK kennen
  - Dieses Handshake erzeugt auch den PTK;
    ANonce (*authenticator nonce*) und SNonce (*supplicant nonce*) stellen sicher, dass der PTK frisch ist

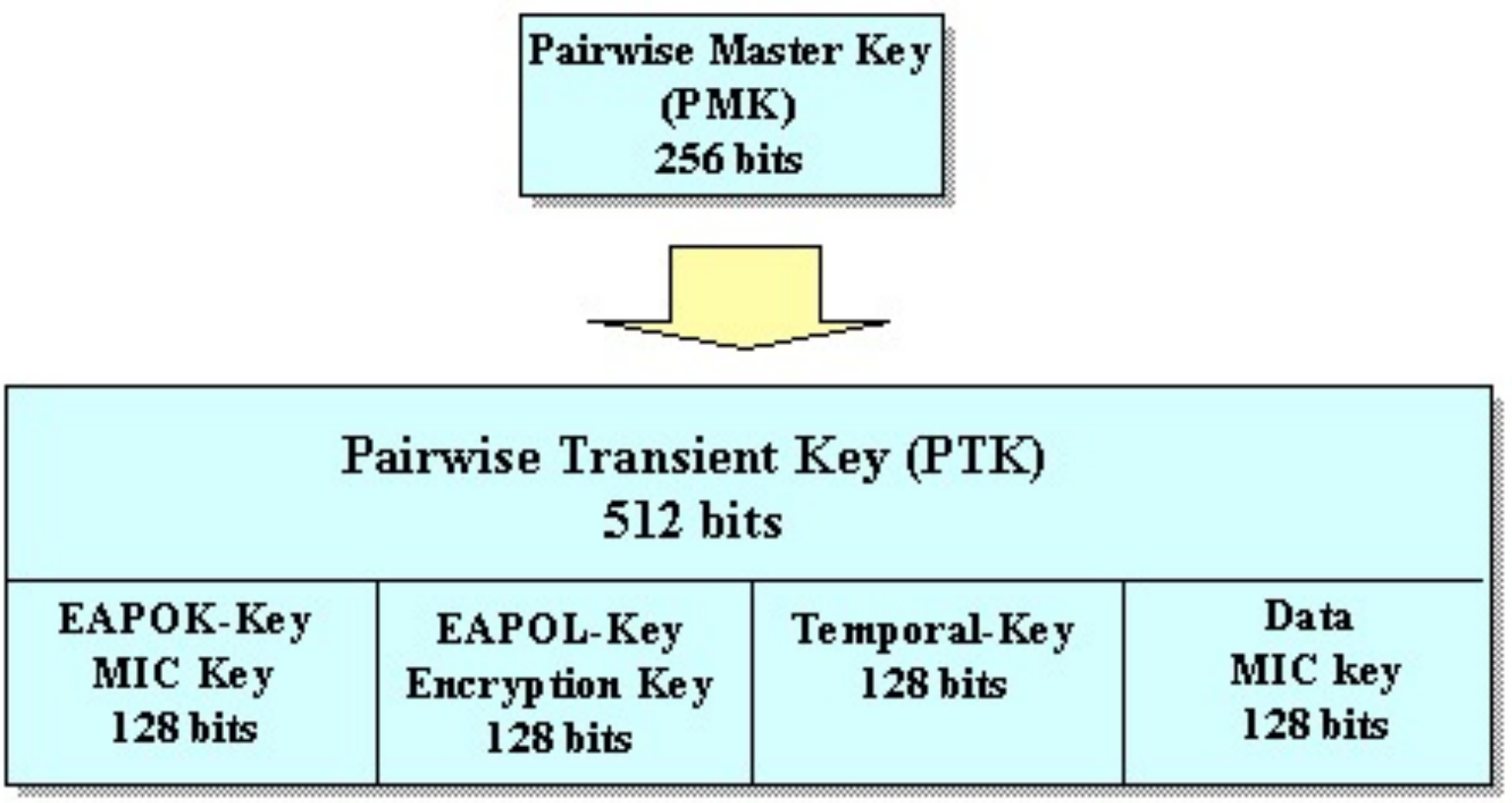
4 Way Handshake und PTK



4-Way-Handshake und PTK

- Verwende PMK nicht direkt für die Krypto
- Erzeuge Pairwise Transient Key PTK (512 bits) aus dem PMK und Nonces
- Aufgeteilt in 4 Teile, jeder einzelne ist 128 bit lang:
  - Verschlüsselung der Daten, Datenintegrität, EAPOL-Key Verschlüsselung, EAPOL-Key Integrität
- Ein Teil des PTKs wird verwendet, um den Schlüssel für die Verschlüsselung (äquivalent zu WEP) in der nächsten Phase zu erzeugen

4 Way Handshake und PTK



KRACK: Key Re-installment AttaCKs

- IV is vorhersagbar ➔ wiederholte Benutzung eines Schlüssels deckt Nutzdaten auf
- KRACK: Client dazu überlisten, einen (korrekt ausgehandelten!) Schlüssel zweimal zu installieren (und damit beim IV wieder vorne anzufangen)
- N.B.: Das 4-way-handshake-Protokoll ist “formal verifiziert”!

Gruppenschlüssel

- Problem: Broadcasts (AP zu Stationen) können keine paarweisen Schlüssel verwenden
  - Broadcast-Pakete von den Stationen werden hingegen zu den APs zunächst per Unicast verschickt –für diesen Teil des Weges wird der PTK genutzt
- Separater Group Transient Key (GTK)
- Wird gesendet, nachdem paarweise sichere Verbindungen eingerichtet worden sind
- Muss nach jeder Dis-Assoziierung neu erzeugt werden!
  - WEP Key-ID Feld wird wiederverwendet, um einen nahtlosen Übergang (transition) zu gewährleisten

Hole 196

- S. 196: GTK ist allen Stationen bekannt, also kein Schutz gegen Einspielung von Broadcast/Multicast

NOTE—Pairwise key support with TKIP or CCMP allows a receiving STA to detect MAC address spoofing and data forgery. The RSNA architecture binds the transmit and receive addresses to the pairwise key. If an attacker creates an MPDU with the spoofed TA, then the decapsulation procedure at the receiver will generate an error. GTKs do not have this property.

- Ethernet-Modell: jeder kann Broadcast senden
- Entwicklungen bei Basisstationen: proprietäre Hacks (gegen ARP-poisoning, ra-guard etc.) unterdrücken BC/MC
- Veränderte Sicherheitsanforderungen ➜
  S. 196 ist plötzlich eine Sicherheitslücke

TKIP (Temporal Key Integrity Protocol)

- Problem: Alte Hardware ist nicht leistungsfähig genug, um AES-CCMP zu unterstützen; RC4 wird also weiter verwendet

TKIP:

- Vergrößert IV-Raum (24 → 48 Bits)
- IV-Sequenz wird festgelegt
  - TSC (TKIP sequence counter) bietet Schutz vor Replay-Angriffen
- Mixing Function erzeugt für jedes Paket den 40-Bit- (104-Bit-) Anteil
  - Man kann auch mit Legacy Hardware arbeiten, die eine 24+40-Struktur erwartet
  - Auch MAC-Adresse beim Mischen berücksichtigen, um die Wiederwendung des IV zwischen Systemen zu vermeiden
- MIC (*message integrity code*): Michael
  - Sehr billige Integritätsprüfung für MAC-Adressen und Daten

Der MIC-Tradeoff

- Die meisten guten Verfahren zur Überprüfung der Integrität von Nachrichten sind zu teuer
- Michael ist schnell und billig
  - Aber nur begrenzte Widerstandsfähigkeit
  - Wird zum WEP ICV (CRC) hinzugefügt, der immer noch auf der MPDU-Ebene angewendet wird
  - Michael wird auf der MSDU-Ebene angewendet
- Angriffe würden Millionen von Paketen benötigen
  - “Gegenmaßnahmen” (60-Sekunden-Blackout), wenn ein Angriff entdeckt wird
- Erzeugt das altbekannte DoS-Problem
  - Es gibt allerdings einfachere Möglichkeiten für DoS-Angriffe in drahtlosen Netzen

WPA-PSK

- Geeignet für zuhause / Einsatz im Bereich Small Office bzw. Home Office (SOHO)
- Entfernt 802.1X-Authentisierung
  - Pre-shared Key („PSK“) wird aus einer Passphrase via Password-based Key Derivation Function PBKDF2 (RFC2898) erzeugt
  - Verwende diesen als PMK
- WPA-PSK = Pre-shared Key + TKIP
- Verwundbar gegenüber passivem Wörterbuchangriff
  - Wähle lange, komplexe PSKs
- Immer noch viel, viel besser als WEP

WPA3

Fixes für WPA2:

- “Simultaneous Authentication of Equals” (RFC 7664)
- Offline-Angriffe auf Passwort schwerer
- Forward secrecy
- Opportunistic Wireless Encryption (RFC 8110)
  - ➔ WiFi Enhanced Open
- WiFi Protected Setup ➔ WiFi Easy Connect
- Protection of management frames (802.11w) erforderlich
  - Verhindert disassociation attack

Was ist beim Ausrollen eines WLANs zu berücksichtigen?

- Verstecke SSID (???)
- Verwende ***nicht*** WEP
- Verwende WPA mit 802.1x, falls möglich
- Oder verwende WPA wenigstens mit einem sehr komplexen Pre-shared Key

- Und/oder verwende VPNs

Was lernen wir also?

- “If you **compromise** on security, your security will be compromised”
- Führe ein Review der Sicherheit schon **früh** während des Entwicklungsprozesses durch
- Verteilen von sicherheitskritischen Funktionen in Millionen von nicht-änderbaren Hardwaregeräten **wird** früher oder später zu einem Problem führen
- *With sufficient thrust, pigs fly just fine*
  - *However, this is not necessarily a good idea. It is hard to be sure where they are going to land, and it could be dangerous sitting under them as they fly overhead.*
    [RFC 1925: Fundamental truths of networking, 1. April 1996]