RADIUS

Protokoll + Erweiterungen

Universität Hamburg
Seminar: Internet-Sicherheit

Claas Altschaffel
Sommersemester 2005

Inhalt

- Einleitung
- Paketaufbau
- Ablauf
  - Protokoll-Support
- RADIUS Proxy
- Erweiterungen
  - Accounting
  - Protokoll-Support

Einleitung

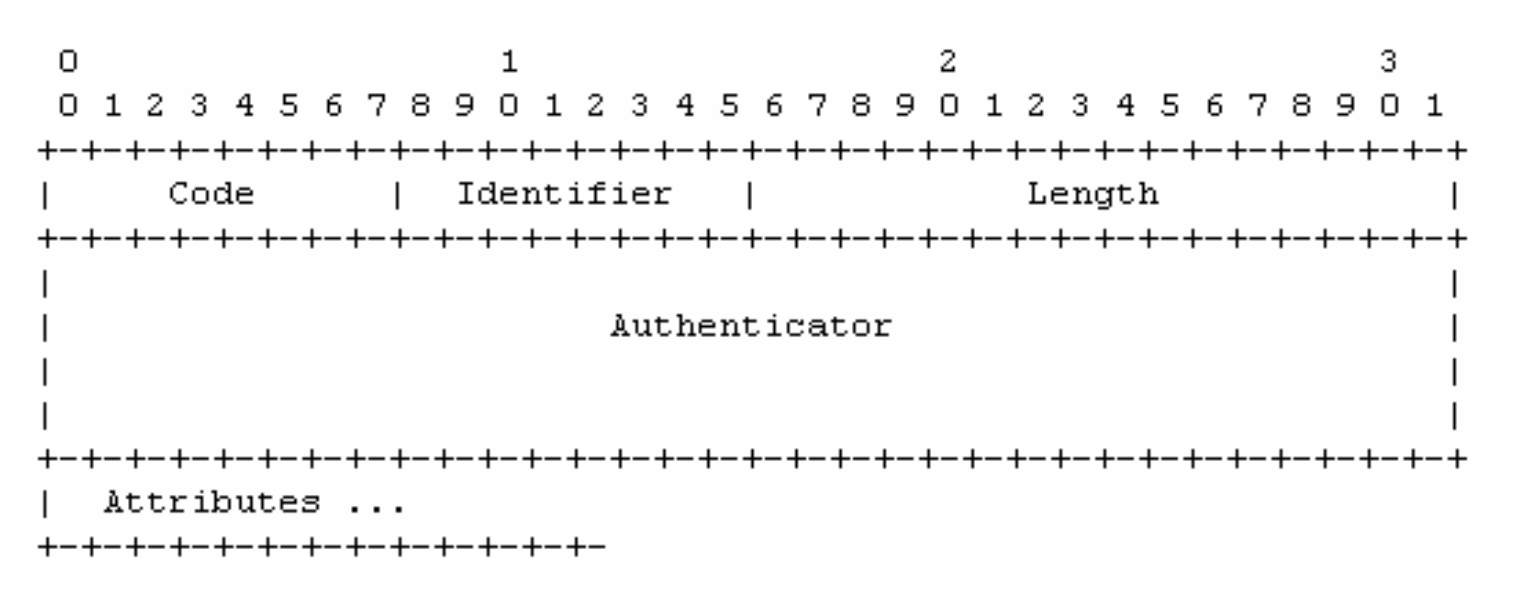
- Remote Authentication Dial In User Service
- Basiert auf UPD
- Client/Server
- Zentralisierung von
  - Authentifikation
  - Autorisation
  - Konfiguration
- Flexibel und erweiterbar
- „shared secret“ zur Authentifizierung der Pakete

Aufgabenverteilung

- Network Access Server (NAS) als Client
  - Sendet Zugangsanfragen an den RADIUS Server
  - Ermöglicht Zugang anhand der Antwort des Servers
- RADIUS Server
  - Empfängt Zugangsanfragen des NAS
  - Authentifiziert Benutzer
  - Sendet alle notwendigen Zugangsinformationen an den NAS
- RADIUS Server als Proxy
  - Für weitere RADIUS Server
  - Für andere Authentifikations-Server

RADIUS Paket

- Genau ein RADIUS Paket in einem UPD Paket
- UPD Destination Port: 1812



Code

- 1 Byte
- Bestimmt Typ des RADIUS Paketes
- Pakete mit einem ungültigen Code werden verworfen
- Dezimal spezifiziert

- RADIUS Codes:
  - 1 Access-Request
  - 2 Access-Accept
  - 3 Access-Reject
  - 11 Access-Challenge
  - 12 Status-Server (exp.)
  - 13 Status-Client (exp.)
  - 255 Reserved

Identifier

- 1 Byte
- Identifiziert eine Anfrage
- Ist in Anfrage und Antwort gleich
  - Ermöglicht die Zuordnung von zusammengehörigen Anfrage/Antwort Paaren
- Mehrfach gesendete Pakete können vom RADIUS Server erkannt werden, wenn sie innerhalb kurzer Zeit ankommen und:
  - Von der gleichen IP sind
  - Den gleichen Source-Port verwenden
  - Den gleichen Identifier besitzen

Length

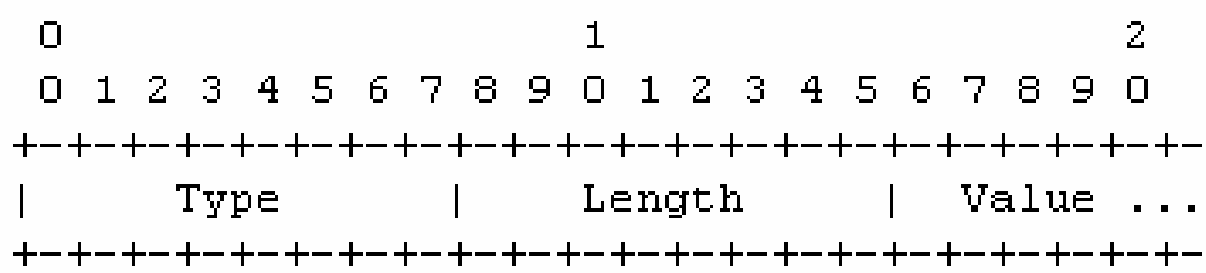
- 2 Byte
- Länge des Paketes in Byte gebildet über:
  - Code
  - Identifier
  - Length
  - Authenticator
  - Attribute
- Bytes außerhalb der Länge müssen ignoriert werden
- Pakete die kleiner sind als die Länge müssen verworfen werden

Authenticator

- Request Authenticator
  - 16 Byte Zufallszahl
  - Global und temporal eindeutig innerhalb der zeitlichen Verwendung eines „shared secret“
  - Wird beim Verschlüsseln des User-Password Attributes verwendet
- Response Authenticator
  - 16 Byte
  - MD5 Hash über:
    - Code
    - Identifier
    - Length
    - Request Authenticator
    - Attribute
    - shared secret

Attribute

- Tripel aus Typ, Länge und Wert
- Enthalten spezifische
  - Authentifikations- und Autorisationsinformationen
  - Konfigurationsdetails
- Ende der Attributliste definiert durch das „Length“ Feld des RADIUS Paketes



Attribut-Vorkommen

- Attribut eines Typs kann mehrfach in einem RADIUS Paket vorkommen
  - Reihenfolge der Attribute relevant
  - Sind nicht zusammenhängend
  - Für jedes Attribut extra spezifiziert
  - Auswirkung sind attributspezifisch
- Attributspezifikation kann definieren in welchen Paket-Typen es vorkommen kann / muss
- Spezifizierte Vorkommen betreffen nur das spezifizierende Dokument

Attribut-Deskriptoren

- Type
  - 1 Byte, interpretiert als dezimaler Wert
  - 1-63 RADIUS + RADIUS Accounting
  - 64-191 für weitere Spezifizierungen
  - 192-223 für experimentelle verwendung
  - 224-240 für implementierungs-abhängige Verwendung
  - 241-255 vorbehaltlich reserviert
- Length
  - 1 Byte
  - Länge des Attributs in Byte über Type, Length und Value

Attribut-Werte

- Text
  - 1-253 Byte, UTF-8 kodierte Zeichen
- String
  - 1-253 Byte, Binärdaten
- Address
  - 32bit, höchstwertiges Byte zuerst
- Integer
  - 32bit unsigned, höchstwertiges Byte zuerst
- Time
  - 32bit unsigned, höchstwertiges Byte zuerst
  - Sekunden seit 01.01.1970 UTC

User-Password Attribut

- Type: 2
- Wert: String
- Länge:
  - Minimal 18 Byte
  - Maximal 130 Byte
- Wird verschlüsselt übertragen
- Maximal 128 Byte für das Passwort

- Verschlüsselung:
  - 1. padding password:
    → L(pw) % 16 = 0
  - 2. b1 = MD5(S + RA)
  - 3. c(1) = b1 XOR p(1)
  - 4. b2 = MD5(S + c(1))
  - 5. c(2) = b2 XOR p(2)
  - 6. …….
  - 7. bi = MD5(S + c(i-1))
  - 8. c(i) = b(i) XOR p(i)
  - 9. c(1)+c(2)+…+c(i)

Protokoll-Ablauf 1

- Client sendet „Access-Request“ an den Server
  - Kann mehrfach und an verschiedene RADIUS Server versendet werden, wenn keine Antwort erhalten wird
  - Eventuell neuer Authenticator und ID notwendig, wenn ein anderes „shared secret“ verwendet wird
- „Access-Request“ enthält die Attribute:
  - User-Name
  - User-Password (verschlüsselt)
  - NAS-Identifier oder NAS-IP-Address
  - NAS-Port oder NAS-Port-Type
  - Eventuell weitere Attribute

Protokoll-Ablauf 2

- Server antwortet mit
  - „Access-Accept“
    - Enthält alle notwendigen Zugangsinformationen
  - „Access-Reject“
    - Enthält eventuell einen Text als Fehlernachricht
  - „Access-Challenge“
    - Enthält typischerweise eine „challenge“ als Text
    - Enthält eventuell ein „State“ Attribut
- Server verwirft den „Access-Request“
  - Wenn der Server kein „shared secret“ mit dem NAS hat
  - Wenn die Anfrage ungültig ist (z.B. falsche Länge)

Protokoll-Ablauf 3

- Client verarbeitet die Antwort
  - „Access-Accept“
    - Ermöglicht Zugang mit den enthaltenen Informationen
  - „Access-Challenge“
    - Challenge wird dem Benutzer (der Benutzersoftware) übergeben
    - Ursprünglicher „Access-Request“ wird an den Server gesendet mit:
      - Einem neuen Identifier
      - Challenge-Response als Attribut „User-Password“ (verschlüsselt)
      - Dem „State“ Attribut der „Access-Challenge“, wenn vorhanden
  - „Access-Reject“
    - Zugang wird verweigert

PAP und CHAP Support

- PAP
  - Attribute:
    - User-Name = PAP ID
    - User-Password = Password
  - Optionale Attribute:
    - Service-Type = Framed-User
    - Framed-Protocol = PPP
- CHAP
  - Attribute:
    - User-Name = CHAP username
    - CHAP-Password = CHAP ID + CHAP response
    - CHAP-Challenge (RA) = 16 Byte Challenge
  - Optionale Attribute wie bei PAP

RADIUS Proxy

- Arbeitet als „Forwarding Server“
  - Nimmt Anfrage vom RADIUS Server/NAS entgegen
  - Leitet Anfrage an „Remote Server“ weiter
  - Empfängt Antwort vom „Remote Server“
  - Leitet Antwort an RADIUS Server/NAS weiter
    - Eventuell angepasst an lokale Policies
- RADIUS Server kann sowohl „Forwarding Server“ als auch „Remote Server“ sein
  - Typisches Beispiel: Roaming
- „Ketten“ von Proxies möglich

Proxy-State Attribut

- Enthält implementierungs-abhängige Informationen vom Proxy
- Nur für den RADIUS Server von Interesse der es hinzugefügt hat
- Vorhandene „Proxy-State“ Attribute
  - Dürfen nicht interpretiert werden
  - Können 1 zu 1 in eine Anfrage übernommen werden
  - Müssen der Antwort wieder hinzugefügt werden
  - Müssen in derselben Reihenfolge erhalten bleiben
- Eigenes „Proxy-State“ Attribut wird vor dem Senden der Antwort entfernt

RADIUS Accounting

- Berechnen des durch den NAS erbrachten Service
- 2 RADIUS Codes
  - 4 Accounting-Request
  - 5 Accounting-Response
- 11 Attribute (40-51), z.B. „Account-Status-Type“
- Start „Accounting-Request“
  - Welcher Service wird erbracht
  - An welchen Benutzer wird der Service erbracht
- Stop „Accounting-Request“
  - Welcher Service wurde erbracht
  - Optional: Zeitangabe, Input/Output

RADIUS Tunnel-Support

- Viele Tunnel-Protokolle verwenden Dial-Up-Mechanismen zur Authentifikation
  - PPTP, IPSec …
- Werte für das Attribut „Acct-Status-Type“
  - 6 Werte (Tunnel-Start/Stop …)
- RADIUS Attribute
  - Tunnel-Konfiguration
  - Schlüssel/Passwort-Übertragung

RADIUS Extensions

- Erweitert das RADIUS Protokoll um
  - Interim Accounting
    - Attribute:
      - Acct-Input/Output-Gigawords
        (wie oft 2^32 Bytes erreicht wurden)
      - Event-Timestamp
  - Support für
    - ARAP (Apple Remote Access Protocol)
    - EAP (Extensible Authentication Protocol)

EAP Support

- Ermöglicht die Verwendung verschiedener Authentifizierungs-Mechanismen in PPP
  - Smart-Cards, Kerberos, Public Key, One Time Passwords, etc …
- RADIUS nur Transportprotokoll für EAP
  - Attribute:
    - EAP-Message
    - Message-Authenticator
- Protokoll zwischen RADIUS Server und Authorisierungs Server proprietär

Message-Authenticator Attribut

- 16 Byte Checksumme
- Sicherstellung der Authentizität des NAS
- In Antworten wird der Request Authenticator der Anfrage für den Hash verwendet
- HMAC-MD5 mit „shared secret“ als Schlüssel über:
  - Type
  - Identifier
  - Length
  - Request Authenticator
  - Attribute

Literaturverzeichnis

[Rig00] C. Rigney: *RADIUS Accounting – RFC 2866*, 2000

[RWC00] C. Rigney, W. Willats, P. Calhoun: *RADIUS Extensions – RFC 2869*, 2000

[RWR+00] C. Rigney, S. Willens, A. Rubens et. Al.: *Remote Authentication Dial In User Service (RADIUS) – RFC 2865*, 2000

[ZAM00] G. Zorn, B. Aboba, D. Mitton: *RADIUS Accounting Modifications for Tunnel Protocol Support – RFC 2867*, 2000

[ZLR+00] G. Zorn, D. Leifer, A. Rubens et. Al.: *RADIUS Attributes for Tunnel Protocol Support – RFC 2868*, 2000