# T-110.5110 Computer Networks II

# AAA

# 12.11.2007

Adj. Prof. Sasu Tarkoma

## Contents



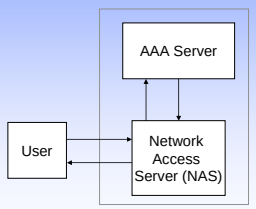
## AAA

- AAA
  - Authentication, Authorization, Accounting
  - RFC 2903 (Generic AAA Architecture)
  - RFC 2904 (AAA Authorization Framework)
- AAAA
  - AAA and Auditing
- Accounting and billing
  - Accounting is gathering information for billing, balancing, or other purposes
  - Billing is a process to generate a bill for customers based on gathered information

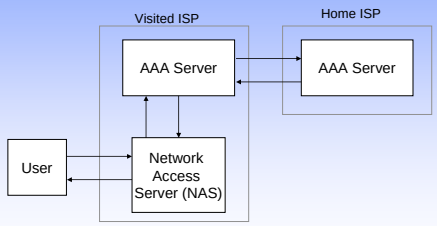
## Motivation for AAA

- Service organizations to host multiple organizations requiring dial-in facilities
- User organizations to outsourcing their dial-in service to one or more 3rd parties
- Agreements can be implemented using a standards based protocol (RADIUS)
- RADIUS allows User organizations or Agents to migrate to other Service Providers.
- An agent, using proxy AAA to change its service without affecting the agreement with its customers
- A service organization to have ultimate authority over its users

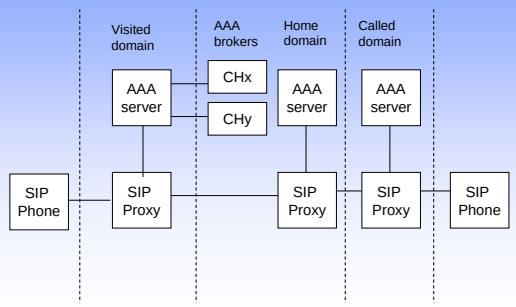
## Scenarios: Remote Dial-In

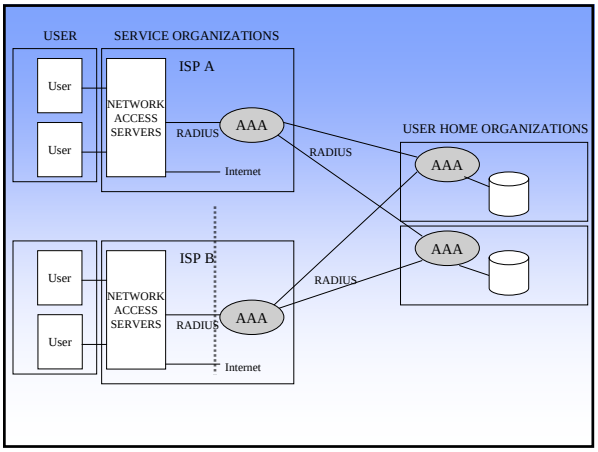



## Scenarios: Mobile Dial-In

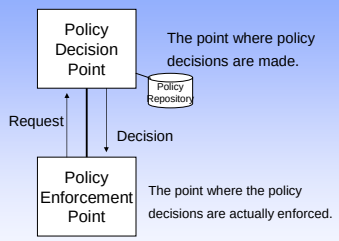


## Scenarios: IP-Telephony



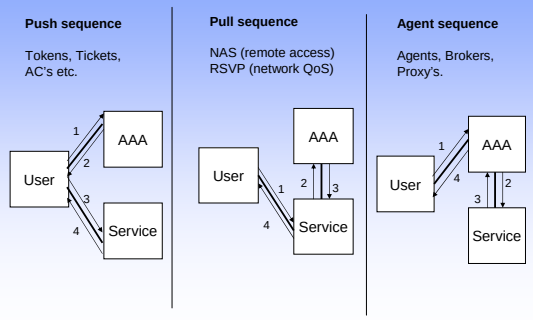




## Generic AAA Architecture (RFC2903)




GOAL: Allow policy decisions to be made by multiple PDP's belonging to different administrative domains.

## AAA Authorization Framework




## AAAA

- Authentication
  - Are you who you say you are?
- Authorization
  - Are you allowed to do what you want to do?
- Accounting
  - Keeping track of who is using how much of each resource
- Auditing/Accountability

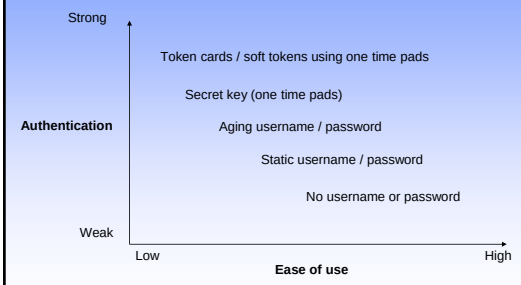
## Authentication

- Many authentication methods can be used
  - IP address
    - Easily forged
    - May change
    - Does not really identify a single end-host
  - User ID and password
    - Requires additional security measures to make it work
    - One-time pads support strong security

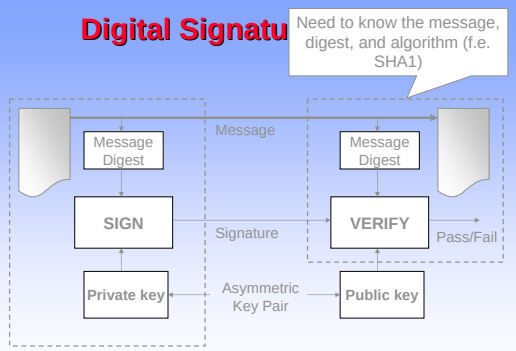
## Authentication II

- Challenge-response
  - Require proof of password, ownership, computational capability, perception, ..
- Shared secret
  - Symmetric key in cryptography
  - Never sent over the network
  - Requires a way to derive keys
    - Key negotiation protocols
      - Diffie-Hellman
- Asymmeric keying / public key cryptography
  - Can identify individuals
  - Encryption and signature
  - Hard to break without knowledge of the private key

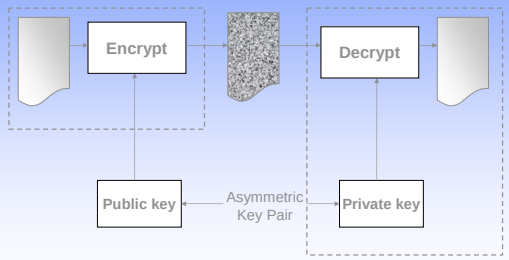
## Authentication III

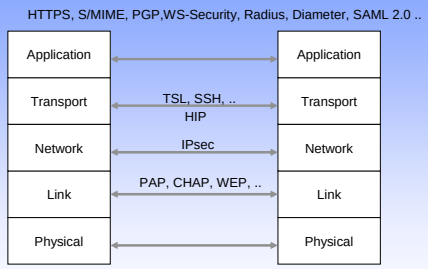



## Digital Signatu




## Encryption




## Attacks against authentication

- Eavesdropping passwords and credentials
- Password guessing / brute force (sniffing)
- Replaying credentials
- Man-in-the-Middle (MiTM)
  - Opportunistic protocols are prone
  - Solved using mutual authentication
    - Authenticated diffie-hellman
- Time synchronization based attacks (if timestamps are used)
- Resource exhaustion
  - Any exhaustion attack on resources
  - Signature checking, token creation
  - Entropy attacks

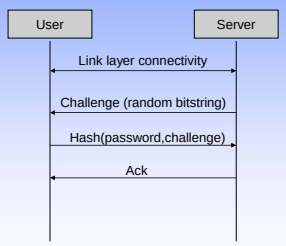
## Authorization

- After a user has been authenticated, authorization is used to grant privileges for performing certain actions
- Mapping from user identity and system state to authorized actions is needed
- Many techniques
  - Physical presence
  - Token-based authorization
  - PKI-based authorization
- Current systems rely on assertions
  - SAML 2.0

## PAP and CHAP

- Password Authentication Protocol (PAP)
  - Originally described in RFC 1334 for use with the Point-to-Point Protocol (PPP)
  - Username/passphrase challenge-response protocol
  - Authenticator sends a challenge to the client, and the response is validated by the authenticator
    - Authentication during initial connection attempt
- CHAP is detailed in RFC 1334 as a more secure alternative to PAP
  - Challenge Handshake Authentication Protocol
  - Periodic challenges during a session
  - Protection against replay attacks
  - Usernames as clear, passwords as hash values
- Microsoft CHAP version 2
  - Mutual authentication by piggybacking a second set of authentication handshakes over the original CHAP packets

## CHAP 3-way handhake




## EAP

- Extensible Authentication Protocol (EAP) is defined in RFC 3748
- Set of guidelines authentication message formats
  - Universal authentication framework
- EAP Transport Layer security (EAP-TLS)
  - Client-side certificates
  - Strong authentication methods through the use of PKI
  - Peers exchange certificates and use public key crypto to share keying material
- EAP Tunneled Transport Layer Security (EAP-TTLS)
  - Extends EAP-TLS
- EAP-TTLS provides mutual authentication
  - Server authenticated using certificate
  - Client is authenticated over secure tunnel

## EAP

- EAP parties: EAP peer, EAP server/AAA server, authenticator
- Basic scenarios
  - Peer and authenticator speak some other protocol, authenticator and AAA server speak AAA protocol
    - This is basic AAA usage (prior to EAP)
  - Peer and authenticator speak EAP; authenticator and EAP server/AAA server speak EAP over AAA
    - This is the basic EAP/AAA scenario (e.g. 802.11i)
  - Peer and authenticator speak some other protocol, but use keys derived from a previous EAP conversation between the same EAP peer and EAP server
    - This is a new application not yet defined.

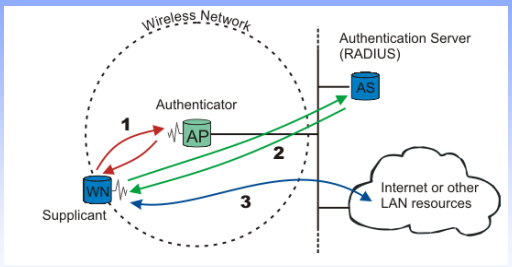
## PEAP

- Protected Extensible Authentication Protocol (PEAP)
- Similar to EAP-TTLS
- Strong mutual authentication
- Inner authentication protocol must be EAP variant
- PEAP is supported by Microsoft and Cisco systems

## IEEE 802.1X

- IEEE standard for port-based Network Access Control
- Authentication to devices attached to a LAN port
- Based on EAP
- Used in closed wireless access points
- Client-only authentication or mutual authentication with EAP-TLS/EAP-TTLS
- Blocking on data link layer, EAP traffic goes through (EAP-request, ..)

## 802.1X Security




Source: http://upload.wikimedia.org/wikipedia/commons/6/63/8021X-Overview.png

## RADIUS

## Radius

- Remote Authentication Dial In User Service (RADIUS) is defined in RFC 2865
- Designed to authenticate dial-in-access customers
  - Used for dial-in lines and 3G networks
- Idea to have a centralized user database for passwords and other user information
  - Cost efficient
  - Easy to configure
- Radius is used together with an authentication protocol such as PAP or CHAP

## Radius

- A client-server protocol
  - Network Access Server (NAS) is the client
  - Radius Server is a server
- Security based on previously shared secret
- More than one server can serve a single client
- A server can act as a proxy
- Based on UDP on efficiency reasons
- No keep-alive signaling

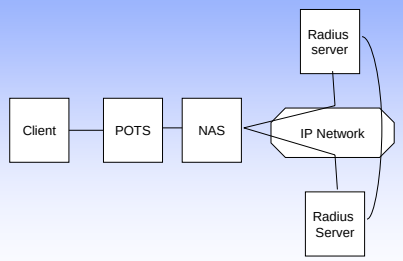
## Parameters for NAS

- The specific IP address to be assigned to the user
- The address pool from which the user's IP should be chosen
- The maximum length that the user may remain connected
- An access list, priority queue or other restrictions on a user's access
- Layer 2 Tunneling Protocol (L2TP) parameters (for VPNs.. )

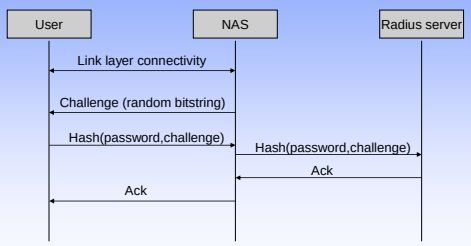
## Accounting

- NAS can use RADIUS accounting packets to ntify the RADIUS server of events such as
  - The user's session start
  - The user's session end
  - Total packets transferred during the session
  - Volume of data transferred during the session
  - Reason for session ending

## RADIUS




## Radius and CHAP




## Steps

- CHAP authentication challenge to the user
- User responds with a password using a one-way hash function
- NAS wraps the challenge and response in a RADIUS access-request
- RADIUS searches the password corresponding to the user ID and computes hash values corresponding to the password and the challenge
- If a hash value matches the user response, the RADIUS server returns an access-accept message to the NAS
- NAs sends a successful CHAP ack to the user

## Radius Signals

- The RFC defines the following signals:
  - 1 Access-Request
  - 2 Access-Accept
  - 3 Access-Reject
  - 4 Accounting-Request
  - 5 Accounting-Response
  - 11 Access-Challenge
  - 12 Status-Server
  - 13 Status-Client
  - 255 Reserved

## Radius Limitations

- Scalability
  - No explicit support for agents, proxies, ..
  - Manual configuration of shared secrets
- Reliability
  - UDP not reliable, accounting info may be lost
- Does not define failover mechanisms
  - Implementation specific
- Mobility support
- Security
  - Applied usually in trusted network segments or VPNs
  - Application layer authentication and integrity only for use with Response packets
  - No per packet confidentiality
- Diameter addresses some of the security issues

# DIAMETER

## Diameter

- A network protocol for providing AAA services to roaming users
  - Replacement for RADIUS, Kerberos, TACACS+
  - Open base protocol provides transport, message delivery, and error handling services
- Diameter Base Protocol is defined in RFC 3588
- Defines the following facilities
  - Delivery of AVPs (attribute value pairs)
  - Capabilities negotiation
  - Error notification
  - Extensibility through additional new commands and AVPs
  - Basic services necessary for applications
    - Handling of user sessions, Accounting, ..

## Diameter

- Uses TCP and SCTP for communications
- Can be secured using IPSEC and TLS
- End-to-end security is recommended but not mandatory
- Based on request-answer signal pairs
- In the Diameter network there can be
  - clients, relays, proxies, and redirect and translation agents

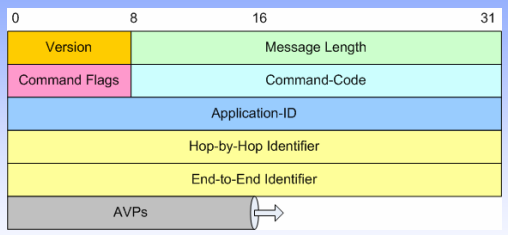
## Required Features

- Diameter protocol to support the following required features:
  - Transporting of user authentication information, for the purposes of enabling the Diameter server to authenticate the user.
  - Transporting of service specific authorization information, between client and servers, allowing the peers to decide whether a user's access request should be granted.
  - Exchanging resource usage information, which MAY be used for accounting purposes, capacity planning, etc.
  - Relaying, proxying and redirecting of Diameter messages through a server hierarchy.

## Features

- SCTP replaced UDP
  - Reliable transport, congestion avoidance, flow control
- Keep-alive messages implemented
  - Diameter can detect local failure of a peer
  - Failover
- Peer-to-peer replaces Client-server
  - Any node can initiate a request
  - Peer discovery and capabilities exchange
- Timestamp support
  - Prevents replay attacks
- Support for extensions
- IPsec and TLS support
- End-to-end security support

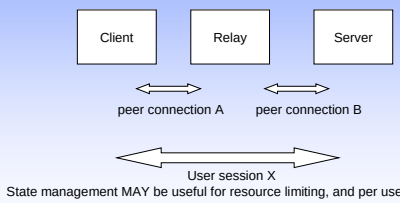
## Header



## Applications for Diameter

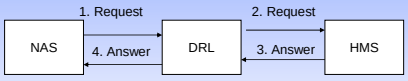
- NASREQ
  - Diameter Network Access Server Requirement
  - Remote dial-in support
  - RFC 2477, RFC 3169
  - EAP, PAP, CHAP
- Mobile IPv4
  - Diameter AAA servers act as Key Distribution Centers (KDC)
- EAP
  - EAP info in AVPs
- Various applications in 3GPP IP Multimedia Subsystem

## Diameter




State management MAY be useful for resource limiting, and per user auditing

## Diameter




Diameter Relay (DRL) can insert/remove information

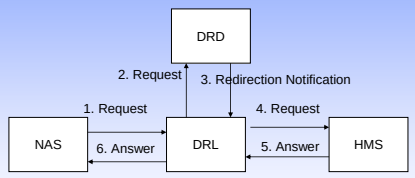
Home Diameter Server (HMS)

Forwarding based on realm

A relay or proxy MUST include Route-Record AVP to all requests forwarded

## Diameter

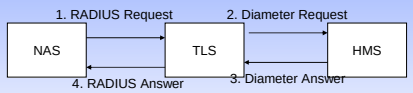
Redirect agent (DRD) returns HMS contact information




Diameter Relay (DRL) can insert/remove information

Home Diameter Server (HMS)

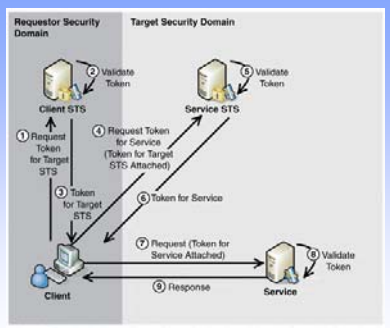
## Translation between RADIUS and Diameter




Translation Agent (TLS)

Must be stateful and must maintain transaction state

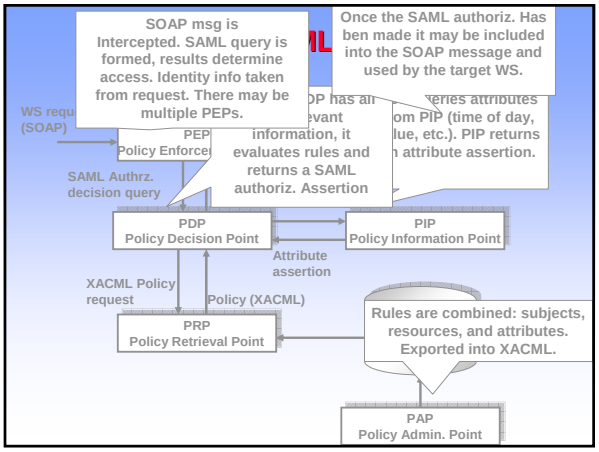
## Web services security




Source: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpag2/html/wssp.asp

## Who are specifying the standards?

- Joint IETF/W3C
  - XML Signature (www.w3.org/Signature)
- W3C
  - XML Encryption (www.w3.org/Encryption/2001)
  - XML Key Management (XKMS) (www.w3.org/2001/XKMS)
- OASIS
  - WS-Security
    - SOAP Message Security specification etc.
  - SAML: Security Assertion Markup Language
  - XACML: Extensible Access Control Markup language
  - Electronic Business XML (ebXML) (with UN/CEFACT)
- Web Services Interoperability Organization (WS-I)
  - Basic security




## Summary

- AAA and AAAA are integral parts of today's networks
- Policy Decision Points, Policy Enforcement Points
- RADIUS
- Diameter
- PAP, CHAP, EAP
- SAML 2.0

## Additional Slides

## Wireless Multi-domain Authentication

- Authentication of the end user or terminal by an AAA server in the network before access to the service is allowed each user is assigned a home area
  - its authentication credentials are established at a home AAA (H-AAAA) server
- Encryption of the data before it is transmitted on the air interface between the base station and the user terminal.
  - when the user roams, the authentication process involves a foreign AAA (F-AAA) server
  - to allow setup of roaming agreements, security associations must be maintained between F-AAAs in visited networks and the user's H-AAA.
- during the authentication process, it must be possible to derive cryptographically strong per-user per-session keys.