Computer Networks II, advanced networking

AAA II
What is AAA

Harri Toivanen
11.11.2004

AAA

- What today?
  - Authentication methods
  - Weak Authentication
  - Radius
  - Diameter

Authentication methods

- Authentication methods with some properties
  - IP-address
    - Can be easily forged
  - User ID and password
    - Without encryption under can be easily stolen
    - The people willingly choose easy to remember passwords and so easy to guess passwords
    - One time passwords will make much stronger

Authentication methods

- Authentication methods with some properties (cont.)
  - Challenge – response
    - In general case can be used to prove some characteristic like humanity
  - Shared secret (cryptographic: symmetric key)
    - Cannot prove individual user
    - Proves to be a member of a certain group

Authentication methods

- Authentication methods with some properties (cont.)
  - Asymmetric keying / public key cryptocraphy
    - An individual player can be identified
    - The methods are assumed to be hard to solve without actual private key
    - New mathematic methods can be found to break the used methods

Weak Authentication

- Weak Authentication: How to Authenticate Unknown Principals without Trusted Parties
  - J. Arkko and P. Nikander
  - Proceedings of Security Protocols Workshop 2002, Cambridge, UK, April 16-19, 2002
  - http://www.tml.hut.fi/~pnr/publications/cam2002b.pdf

Weak Authentication

- **Abstract**
  - This paper discusses "weak authentication" techniques to provide cryptographically strong authentication between previously unknown parties without relying on trusted third parties.
- There is already in use several technques using 'Weak Authentication'

Weak Authentication

- Categories of techniques
  - Spatial Separation
    - Ability of a node to ensure that its peer is on a specific communications path
  - Temporal Separation
    - The general ability of the peers to relate communications at time t_1 to some earlier communications at time t_0

Weak Authentication

- Categories of techniques (cont.)
  - Asymmetric Costs
    - Usually it is easier for the attacker to find a single security hole than for the defender to block all holes
    - Fortunately, this asymmetric situation can sometimes be reversed and used to the defenders' advantage
  - Application Semantics
    - Certain applications may offer particular semantics that can be employed to produce weak forms of authentication

Weak Authentication

- Categories of techniques (cont.)
  - Combined and Transitive Techniques
    - The techniques presented above can be combined
    - Web-of-trust models and information from neighbours could potentially be used together

Weak Authentication

- Some Concrete Techniques
  - Anonymous Encryption
    - unauthenticated Diffie-Hellman key exchange
  - Challenge-Response
    - Challenge-response techniques can be used to ensure freshness and, under certain assumptions, that the peer is on a specific path towards the given address
    - It is therefore typically used to ensure spatial separation.

Weak Authentication

- Some Concrete Techniques
  - Leap-of-Faith
    - Leap-of-faith is another method based on temporal separation, but it also encompasses aspects from spatial separation and asymmetric cost war
    - It has been successfully employed, e.g., in the SSH protocol

Radius

- Remote Authentication Dial In User Service (RADIUS) is defined in RFC 2865
- It is intented to authenticate dial-in-access customers
- It is a client server protocol, where a Network Access Server (NAS) is a client and Radius Server is a server
- The security of Radius is based on pre-shared secret

Radius

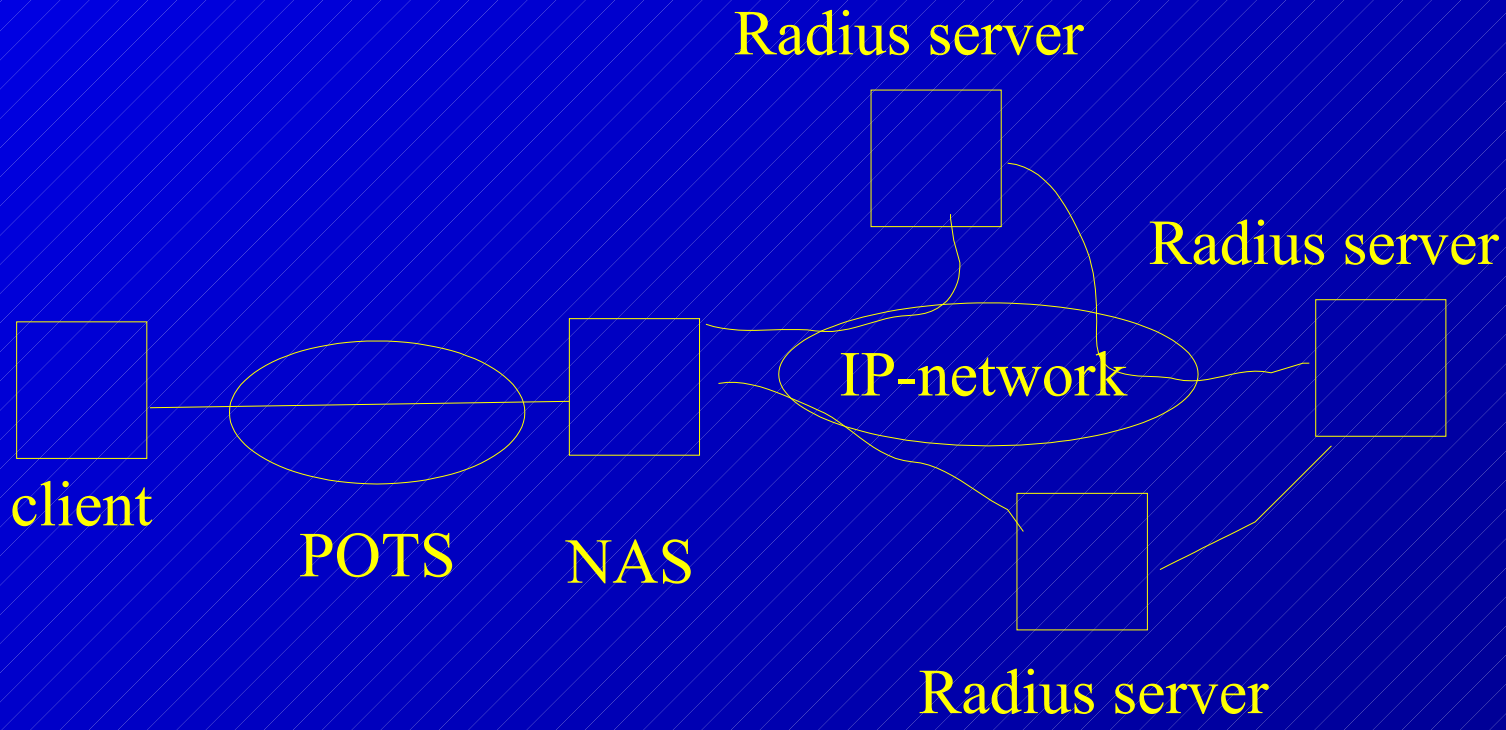
- There can be more than one server serving one client
- A server can act as a proxy
- Technically Radius is based on UDP messages because of effeciency reasons
- No keep-alive signalling is desirable

Radius

- It has the following signals defined:

1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Radius



Diameter

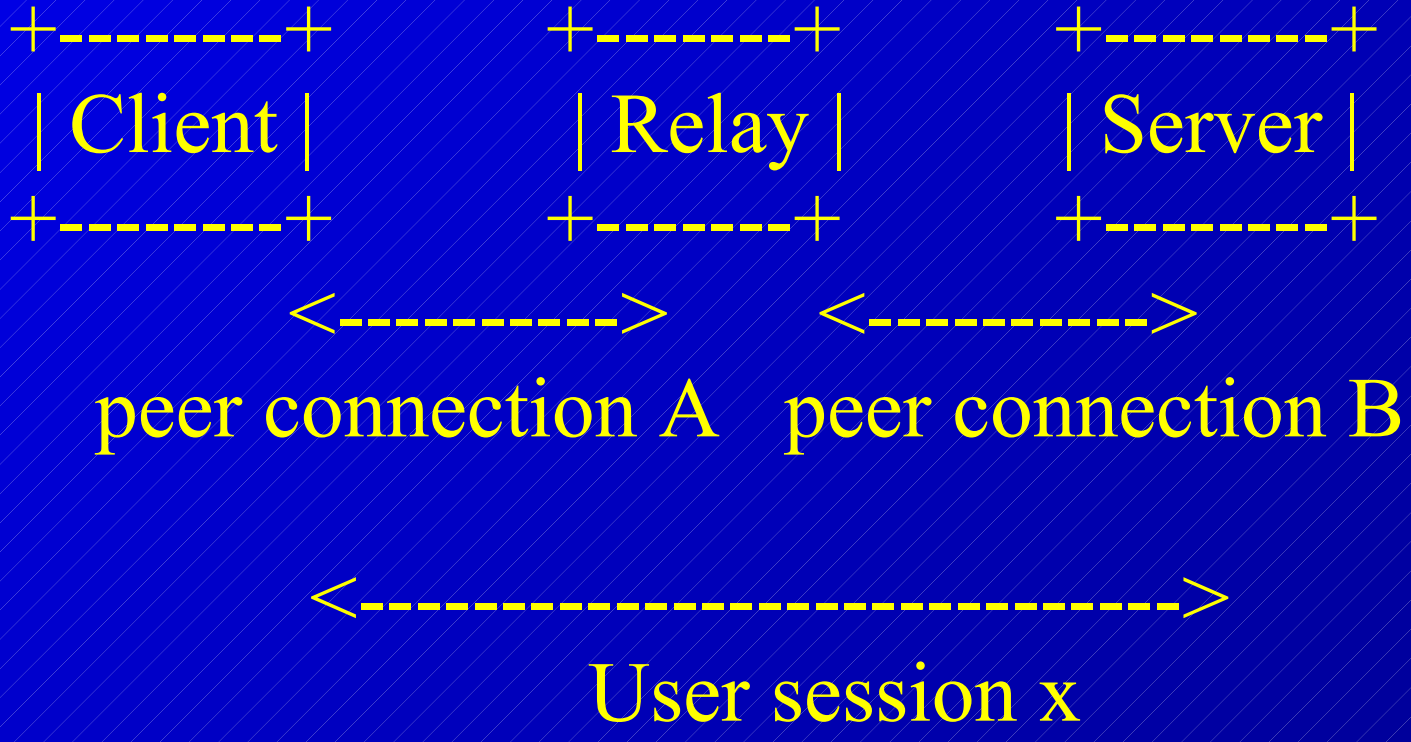
- Diameter Base Protocol is defined in RFC 3588
- It provides the following facilities:
  - Delivery of AVPs (attribute value pairs)
  - Capabilities negotiation
  - Error notification
  - Extensibility, through addition of new commands and AVPs
  - Basic services necessary for applications, such as handling of user sessions or accounting

Diameter

- It is using TCP and SCTP for transportation
- It can be secured with IPSEC and TLS
- End-to-end security is strongly recommended, but not requested
- It is based on request – answer signal pairs
- In the Diameter network there can be Clients, Relays and Servers and relay, proxy, redirect, and translation agents

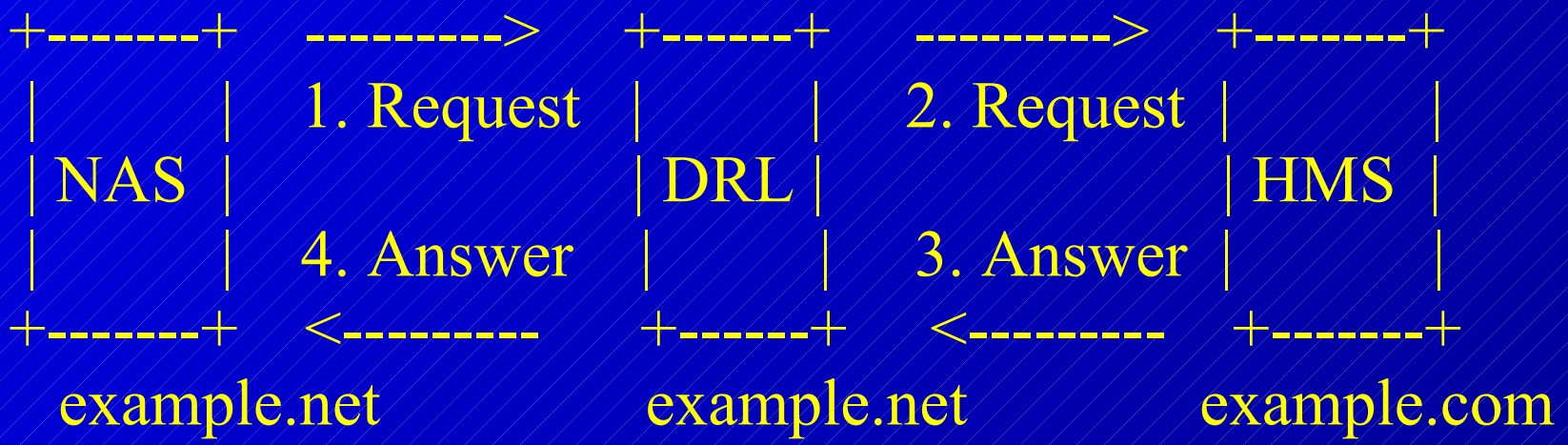
Diameter

- Connections vs. Sessions



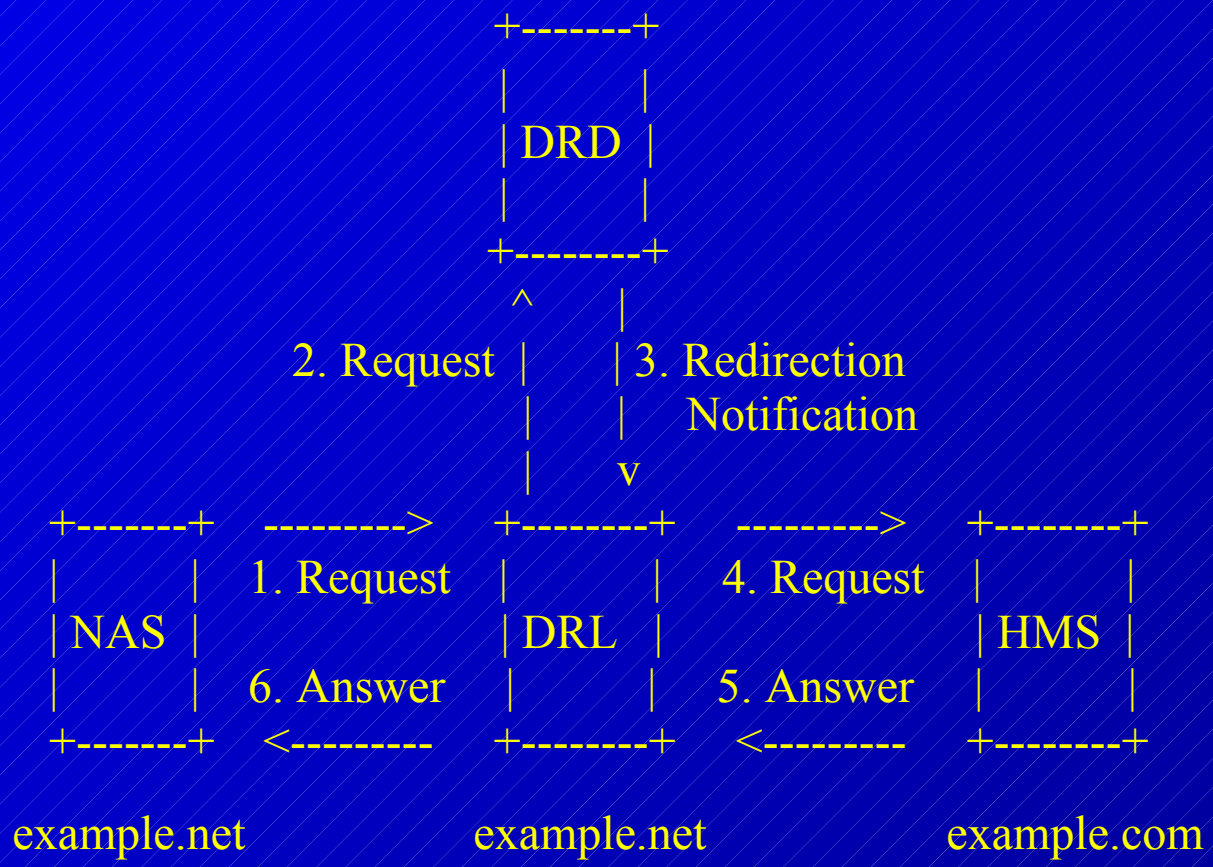
Diameter

- Relaying of Diameter messages



Diameter

- Redirecting a Diameter Message



Diameter

- Translation of RADIUS to Diameter