2010年9月合宿における DiameterとEAPによるWiFiアクセス制御の運用実験

wide-tr-aaa-experiment-201009-00.pdf

WIDE
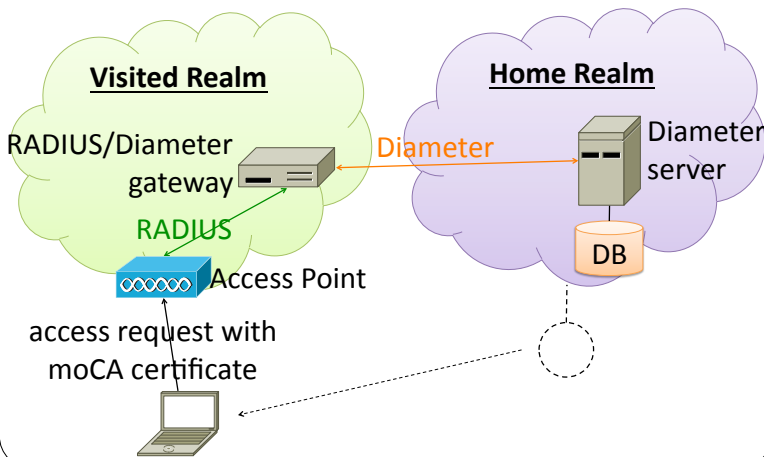
PROJECT

WIDE Project：http://www.wide.ad.jp/

Author(s): Sebastien Decugis (sdecugis@nict.go.jp), Souheil
Ben Ayed (souheil@tera.ics.keio.ac.jp), Ryo
Nakamura (nobushi@tera.ics.keio.ac.jp), Atsushi
Ishida (dolin@tera.ics.keio.ac.jp), Yuki Atsuya
(atie@tera.ics.keio.ac.jp), Fumio Teraoka (tera@ics.keio.ac.jp)

WiFi Access Control by Diameter and EAP

sdecugis@nict.go.jp, {souheil, nobushi, dolin, atie}@tera.ics.keio.ac.jp, tera@ics.keio.ac.jp

Basic System Structure

Visited Realm

RADIUS/Diameter gateway

Diameter

RADIUS

Access Point

access request with moCA certificate

Home Realm

Diameter server

DB

Advantages of Diameter over RADIUS

- multi-realm support
- message transport reliability (TCP/SCTP)
- message security (TLS)
- failover support
- extensibility
  - new applications / commands
- server initiated message
- introduction of agents
  - proxy agent, relay agent, redirect agent, translation agent

What is Diameter [RFC 3588]?

- A back-end protocol that carries AAA information between the AAA client and the AAA server.
  - AAA: Authentication, Authorization, Accounting
- Requests and answers are represented by AVPs (Attribute Value Pairs).
- The basic functions are capability negotiation and accounting.
- Extensible by adding new commands or AVPs
- There are several Diameter applications:
  - Network Access Server application [RFC 4005]
  - EAP application [RFC 4072]
  - SIP application [RFC 4740], etc.

What is Diameter EAP application [RFC 4072]?

- One of Diameter applications for user authentication and authorization
- used for network access control

What is EAP [RFC 3748]?

- EAP: Extensible Authentication Protocol
- Supports multiple authentication methods:
  - EAP-TLS [RFC 5216]
  - EAP-TTLSv0 [RFC 5281]
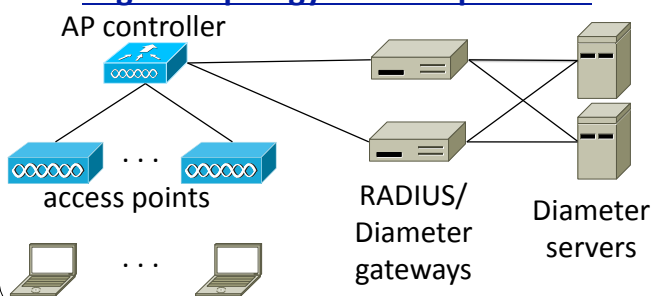 - EAP-GPSK [RFC 5433]
  - etc.

freeDiameter

- Open-source of Diameter Base Protocol developed by *sebastien@nict*.
- Comformance with RFC 3588 and 3588-bis
- Other Diameter applications can be implemented as extensions.
- http://www.freediameter.net/

DiamEAP

- Open-source of Diameter EAP application developed by *souheil@tera*.
- Includes codes of EAP-TLS and EAP-MD5.
- Other EAP methods can be implemented as plug-ins.
- http://diameap.yagami.freediameter.net/

Logical Topology of the Experiment

AP controller

access points

RADIUS/ Diameter gateways

Diameter servers

Experiment Items

- Basic performance (authentication time)
  - # of clients
  - local server@camp vs. remote server@tera-lab.
  - changing session lifetime (1 hour – 10 min)
- Failover transparency
  - intentional failure of a gateway or a server
- Statistics