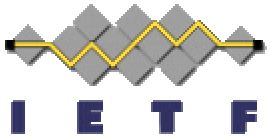

PANA Requirements and Terminology

Alper E. Yegin
Yoshihiro Ohba
Reinaldo Penno
George Tsirtsis
Cliff Wang

- IETF53 -

PANA

- WG's goal is to
  - Define (identify) a *carrier*
  - Identify at least one *payload* (authentication protocol)

  … to meet the *Requirements of Network Access Authentication*

Carrier vs. Payload

- PANA as a carrier (transport) of a security protocol
- Will *not invent:*
  - New security protocol
  - Authentication protocol
  - Key distribution, agreement, derivation
- But should *use* existing methods

Device Identifier

Device Identifier (DI)

The identifier used by the network as a *handle* to control and police the *network access* of a client. Depending on the access technology, identifier might contain any of *IP address, link-layer address, switch port number*, etc. of a device. PANA authentication agent keeps a table for *binding device identifiers to the PANA clients*. At most one PANA client should be associated with a DI on a PANA authentication agent.

Device Identifier

- More than one DI can be used by (bound to) a PaC?
  - Multiple IP addresses

Choice of Payload

- EAP as a candidate
  - Can be part of the *solution* as the “payload”
  - But we shouldn’t have it as a *requirement*

Security Requirements

- Mutual authentication
- Re-authentication
- Integrity protection for DI
- Must not assume secure channel
  - Protected against eavesdropping, spoofing, replay attacks.

Denial-of Service Attacks

Denial of Service Attacks

PANA MUST be robust against a class of DoS attacks such as blind masquerade attacks through IP spoofing that swamp the PAA in spending much resources and prevent legitimate clients' attempts of network access. *The required robustness is no worse than that for TCP SYN attack.*

Authorization

- Binary result supported (success/fail)
- Should PANA be designed *extendible* for finer granularity authorization?
  - Ability to carry a chain of extensions
- Should we have a requirement on extendibility?

Location of PAA

Location of PAA

PAA MAY be one or more hop away from the PaC. PANA MUST define a method used by PaCs for locating the PAAs in a network.

- No constraints on the location
- Also related to IP address configuration of PaC

IP Address Configuration

> It (PANA) MUST NOT make any assumptions on the protocols or mechanisms used for IP address configuration of the PaC.

- Should PANA work even before IP address configuration?

Comments/Issues?

Plans

- New editor
  - George Tsirtsis
- WG last call