Secure Network Access

Alper E. YEĞİN
DoCoMo USA Labs

March 6th, 2002

Network Access

- Components of connectivity
  - Link-layer connectivity
  - IP address configuration
  - On-link forwarding
    - ARP
    - Neighbor Discovery
  - Off-link forwarding
    - Gateway
      - Router discovery (stateless)
      - DHCP (stateful)
      - Manual configuration

Secure Network Access

- Only authenticated and authorized clients gets access
  - Important for enterprise networks
  - Definitely for public access networks
- Public access networks:
  - More challenging
    - Network also has to prove its identity to clients
    - Wireless technologies, possible malicious nodes/networks everywhere
- Authentication (not privacy)

Current Technologies

- Door locks
- HTTP-based schemes
  - Mobilestar
- PPP with EAP
- 802.1x (EAP)

Current Technologies - Issues

- Door locks
  - Wireless network leaks
  - No doors on street!
- HTTP-based schemes
  - Requires user intervention
- PPP
  - Works only on point-to-point links
  - Additional encapsulation
- 802.1x
  - Only works for 802 family links
  - Not general deployment yet

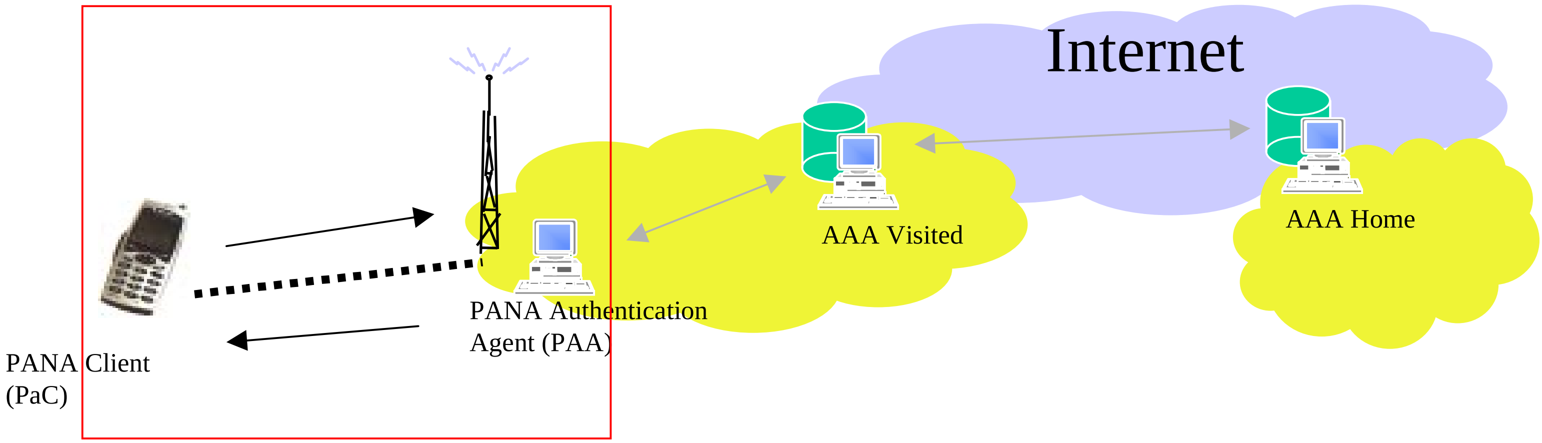
PANA

- Protocol for Carrying ***Authentication for Network Access***
- To define a network-layer carrier for authentication and basic authorization process
  - Link-layer independent
- Part of ALL-IP architecture

PANA

- Define the carrier, pick the payload
  - Like Mobile IPv4 registration request carries MN-FA authentication extension
  - Possible payloads
    - EAP
    - MN-AAA authentication extension of Mobile IPv4
- Like a front-end to AAA

PANA


Internet
AAA Visited
AAA Home
PANA Authentication
Agent (PAA)
PANA Client
(PaC)

PANA WG Plan

- *Requirements and terminology*
- *Usage scenarios*
- Framework
- Interactions with PPP and 802.1x
- Protocol design
- MIB definitions

Requirements Highlights

- *draft-ietf-pana-requirements-01*
- Authentication and (simple) authorization
- Mutual authentication
- Authentication backend
- Just the carrier, pick an already defined payload (security mechanism/protocol)
- Accounting, access control, mobility management outside the scope
- Multi-access links, clients
- Efficiency

Link Security

- PANA likely to do key distribution
- Data traffic can be authenticated and encrypted by using these keys with
  - IPsec
  - Link-layer protocols

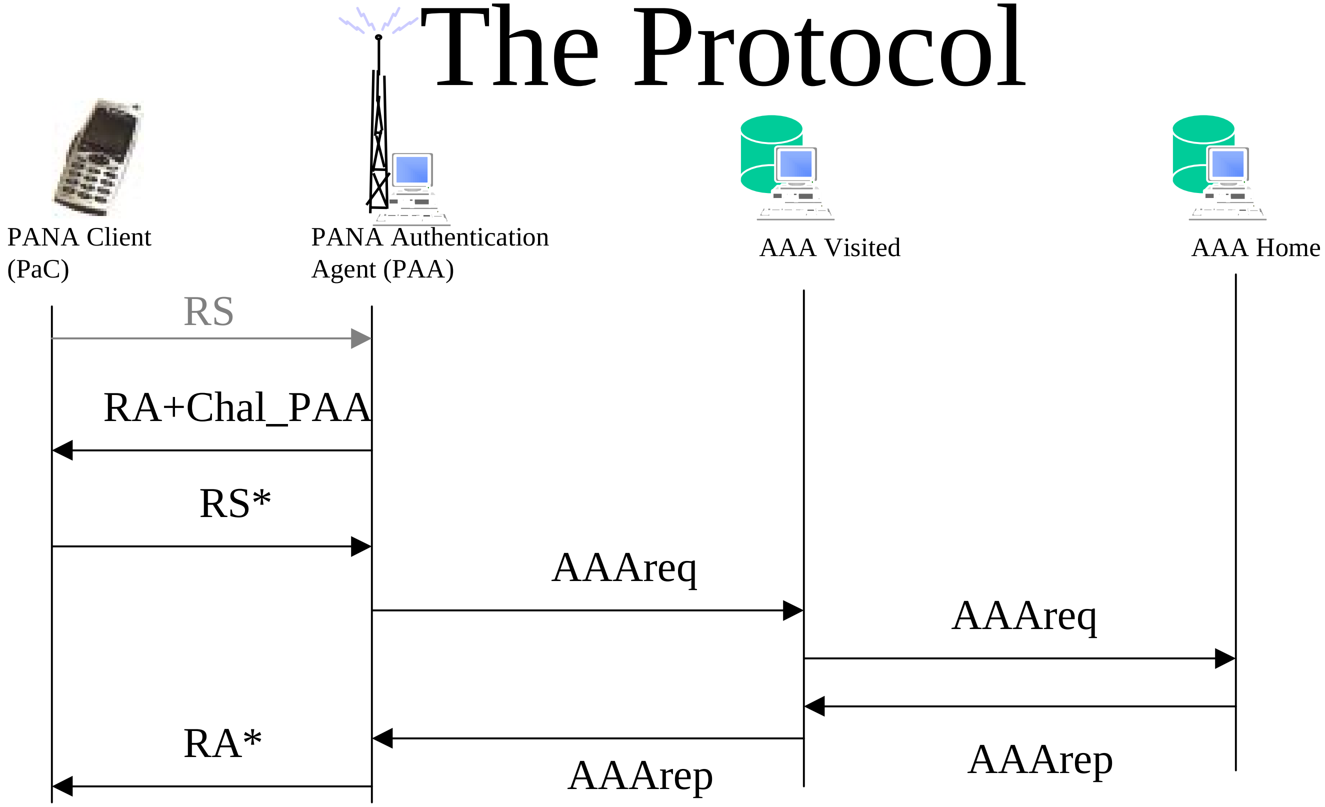
Solutions

- Too soon to discuss at IETF, but:
  - SNARD: Alper E. Yegin, Xiaoning He, Carl Williams, Lisa Yiqun Lin, Satomi Okazaki
  - EAP over ICMP: George Tsirtsis
  - EAP over UDP: Paal Engelstad

SNARD

- Secure network access using router discovery and AAA: draft-yegin-unap-snard-00
- Carrier:
  - Router discovery
    - Router solicitations from PaC
    - Router advertisements from PAA
    - PAA located on the access router
- Payload:
  - MN-AAA authentication extension (RFC3012)
  - AAA registration keys for Mobile IP: draft-ietf-mobileip-aaa-key-08
  - Generalized key distribution extensions for Mobile IP: draft-ietf-mobileip-gen-key-01

The Protocol



PANA Client (PaC)

PANA Authentication Agent (PAA)

AAA Visited

AAA Home

RS

RA+Chal_PAA

RS*

AAAreq

AAAreq

AAArep

RA*

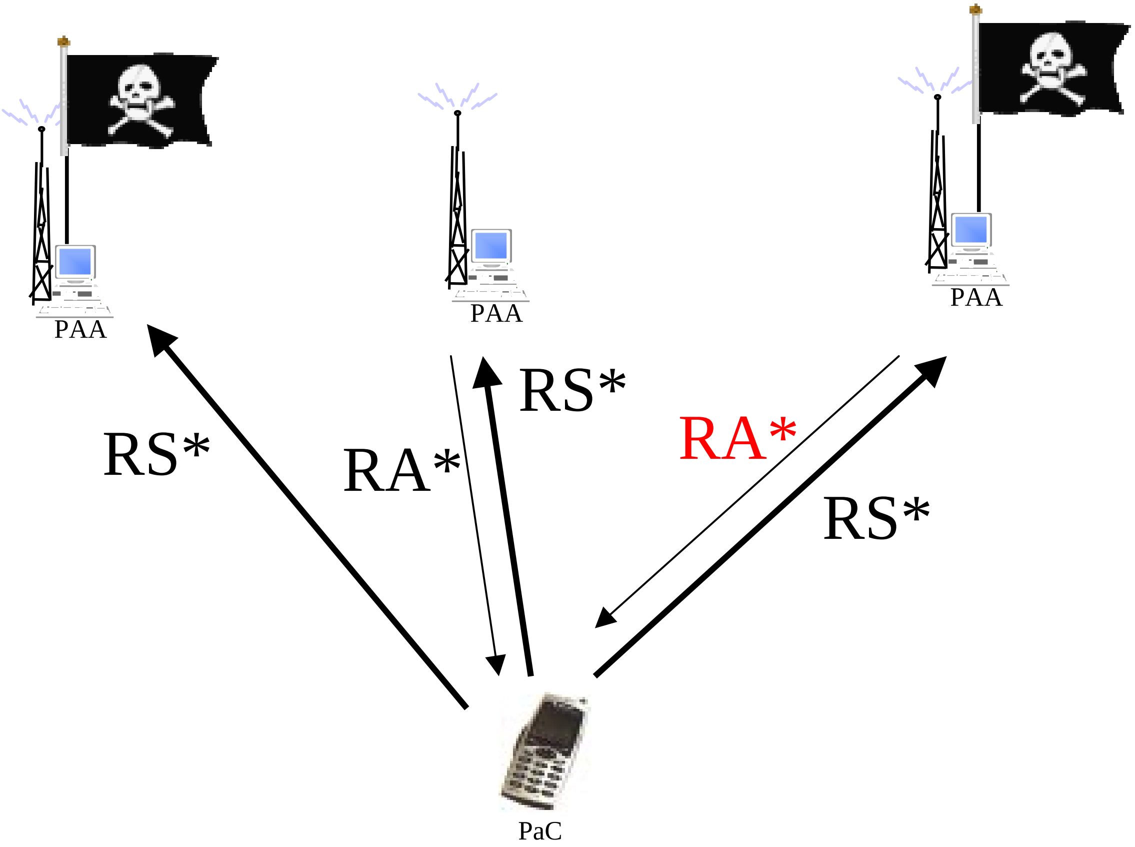
AAArep

- **RS*: RS + PaC_id + MN-FA_key_request + Chal_PAA + Chal_PaC + MN-AAA_auth_ext**
- **RA*: RA + PAA_id + MN-FA_key_reply + Chal_PaC + Chal_PAA + MN-FA_auth_ext**

Async Re-authentication

- At any time PaC can challenge the PAA by sending a RS*
- PAA can kick start this challenge process by sending a RA* with 0 or low lifetime

Malicious Networks



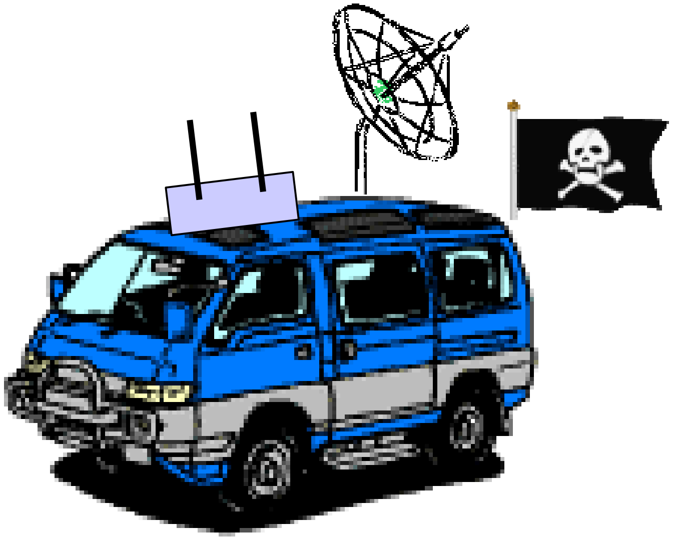
Advantages

- A natural extension to existing protocols
  - Semantically fit
- A device goes through router discovery anyways (efficieny)
- A generic IP solution
  - Can be used for IPv4, IPv6, Mobile IPv4, Mobile IPv6
- Optimizations by creating local security associations

PANA+

- Enhanced authorization
  - Network access parameters
- Go beyond initial client authentication for network access
  - Secure neighbor discovery, ARP
    - SNARD will deal with this using key distribution
  - Secure router discovery
    - SNARD already takes care of this!

Modern Pirates



Questions/comments