RADIUS Client Kickstart

draft-moskowitz-radius-client-kickstart-02.txt

Robert Moskowitz
ICSAlabs
Alan DeKok
IDT Canada Inc.

RADIUS Client Kickstart

- The problem
- SSPP
- RADIUS Client Registration
- RADIUS Server Response
- Security Considerations

The Problem

- RADIUS requires a fixed client IP, and fixed shared secret
- IEEE 802.1x Access Points may obtain addresses through DHCP
- AP autoconfiguration becomes impossible
- Shared secrets are difficult to manage
- Solution:
  - add indirection to RADIUS client secret
  - add registration of client IP

SSPP

- **Shared Secret Provisioning Protocol (SSPP)**
- **Theory:**

`draft-moscowitz-shared-secret-provprotocol-02.txt`

- **SSPP over SNMP**

`draft-moscowitz-sspp-snmp-01.txt`

- **Master secret bootstrap, SSPP over SNMP**
- **Master secret change, SSPP over SNMP**

RADIUS Client Registration

- **Access-Boot packet, similar to Access-Request**

```
Access-Boot packet from 192.168.0.1:3456 ...

 NAS-IP-Address = 192.168.0.1,
   NAS-Port = 3456,
   NAS-Identifier = "AP 1234",
   Calling-Station-Id = "00:01:02:03:04:05",
   Called-Station-Id = "My RADIUS server",
   Event-Timestamp = "2003-11-14 09:00:00",
   Boot-Number = "5",
   State = "1234567890abcdef...
   Message-Authenticator = 0x0001020304...
```

RADIUS Server Response

- **Access-Booted packet, similar to Access-Accept**

```
Access-Booted packet to 192.168.0.1:3456 ...

   Event-Timestamp = "2003-11-14 09:00:00",
   Boot-Number = "5",
   State = "1234567890abcdef...,
 Encrypted-Data = 0xfedcba0987654321...
   Session-Timeout = 7200,
   Message-Authenticator = 0x0001020304...
```

Security Considerations

- MITM attacks are bad.
- Operator validates the fingerprint of the Client's public Diffie-Hellman value [SSPP over SNMP]
- Replays are prevented through nonces, timestamps, and boot sequence numbers.
- Spoofing is prevented through signatures.
- Packet modifications are prevented through signatures.