PANA threat analysis and security requirements

draft-ietf-pana-threats-eval-00.txt

Mohan Parthasarathy

- Introduction
- PAA Discovery
- Authentication
- Leaving the network
- Attack on normal communication
- Miscellaneous attacks
- Issues discussed on the mailing list.

Assumptions

- Path between PAA and EP

  This can be secured by the network operators.
- Path between PAA and AAA backend

  This is secured in existing networks e.g. NAS and RADIUS
- Path between PaC and PAA

  Not secure. What are the threats involved in path ?

Factors affecting threats

- Link between PaC and PAA may not be a shared medium e.g. DSL Network
- Link between PaC and PAA may be a shared medium e.g. Ethernet
- PaCs are already authenticated at layer 2 to the Access Point/NAS e.g. CDMA2000

  NOTE: Not to each other.
- PaC and Access Point may share an SA at layer 2 that provides per-packet authentication and encryption.

PAA Discovery

- PaC’s first step on entering the network.
- Normally discovered by solicitations and advertisements.
- Attacker can pretend to be a PAA by sending spoofed advertisement.
- Common to have multiple authentication methods – implies that the attacker can use a less secure method to advertise.
- Send solicitations to learn more information about networks.

PAA discovery (contd..)

- Difficult to protect the discovery process because PaC and PAA don’t share a security association to begin with.
- Not a threat in existing dial-up networks because the link is not a shared medium.
- In shared links, this attack is easy to launch.
- Layer 2 authentication does not prevent a node from pretending to be a PAA.
- Requirement : PANA MUST not assume that the discovery process is protected.

Authentication

- THREAT: Identity protection.
- Hide the identity from the attacker.
- Identity of the AS itself may be learnt through other means and not interesting to the attacker.
- Need to protect the identity of the PaC.
- Learn identities by eavesdropping.
- Send falsified identity requests e.g. by initiating the authentication exchange with the PaC and

Authentication (contd..)

abort in the middle (polling attack).

- If the link is not shared, this threat is not present.
- Layer 2 encryption might prevent other nodes from learning the identity through eavesdropping.
- But the polling attack may be hard to avoid, even when layer 2 is secured.
- Requirements : PANA MUST protect the identity of the PaC against eavesdropping.

Authentication (contd..)

- THREAT: Falsified success or failure.
- Attacker can send false failure to prevent client from accessing the network.
- Attacker can send false success to fool the PaC that the access is granted.
- If the link is not shared, this attack is not possible.
- If the link is shared, attacker can easily spoof the success/failure packet.
- Layer 2 encryption can make it hard for the attacker but not impossible.

Authentication (contd..)

- Attack is possible whenever there is no mutual authentication and no per-packet protection for packets exchanged during the authentication process.
- Lack of mutual authentication can also lead to MiTM attacks like where the attacker pretends to be the real PaC to the PAA and pretends to be the PAA to the real PaC.
- Device identifier attack discussed in the mailing list (discuss at the end)

Authentication (contd..)

- Requirement : PANA MUST support mutual authentication (between PaC and AS/PAA) and be able to provide per-packet protection for success/failure and other authentication packets, when needed.
- THREAT: Replay attacks where old messages e.g. success/failure packets are replayed at a later time.
- If the link is not shared, then this threat is not present.

Authentication (contd..)

- If the link is shared, it is easy to replay packets.
- Layer 2 encryption can prevent the attacker from learning the original packet that needs to be replayed.
- Requirement : PANA MUST be resistant to replay attacks.

PaC leaving the network

- PaC leaving the network needs to inform the PAA before disconnecting from the network.
- Also, PAA may want to revoke the access.
- Attacker can pretend to be a real PaC and disconnect from the network.
- Attacker can pretend to be a real PAA and disconnect the PaC from the network.
- Once disconnected, the attacker can gain unauthorized access into the network.

PaC leaving the ..(contd..)

- Threat absent if the link is not shared.
- If the link is shared, then any node can spoof the disconnect.
- Layer 2 security does not help. The attacker can still spoof these messages e.g. pretend to be a PAA.
- Requirement : Disconnect and revocation messages MUST be authenticated when needed.

Normal Communication

- THREAT: Attacker can inject/modify data packets into any data stream by spoofing e.g. IP address and MAC address.
- THREAT: Attacker can eavesdrop to learn useful information.
- THREAT: Attacker can replay old data packets.
- If the link is not shared, this threat is absent.
- If the link is a shared medium, any node can inject, modify and eavesdrop.

Normal Comm.. (contd..)

- If layer 2 provides per-packet authentication and encryption, it will protect against eavesdropping and packet modification attacks.
- The attacker can still spoof IP addresses and inject false data.
- This threat is absent if the client is already using a secure VPN service e.g. IPsec.
- ISSUE : Will the clients trust the local network to provide this service or use VPN like service for this ?

Normal comm... (contd..)

- Requirement : PANA in combination with the underlying authentication protocol e.g., EAP MUST be able to derive keys in order to enable confidentiality, per-packet authentication and integrity.

Miscellaneous attacks.

- Attacker can bombard the PAA with lots of authentication requests. PAA need to create state before forwarding to the backend AS ?
- PANA requirements state that PaC should have an IP address.
- In IPv6, stateless auto-configuration can be used.
- In IPv4/IPv6, if DHCP is used, does it open the network to address depletion attack ?
- Should PANA care about this and not require an IP address ?

Mailing list Issue

- MItM attack /device identifier protection.
- Attacker can pretend to be PAA and blindly forward all the messages between PaC and the real PAA after modifying the source IP address.
- Attacker gains unauthorized access at the end.
- Clients packets from now on will just be dropped by the attacker.
- If keys were derived for per-packet protection of data packets by the real PaC, attacker cannot gain access.

Mailing list.. (contd..)

- EAP WG discussion on MITM attack pertains to the use of sequence of methods or when tunneling is used.