PANA Working Group
Internet Draft
Document: draft-ietf-pana-threats-eval-00.txt
Expires:April 2003

Mohan
Parthasarathy
Tahoe Networks
October 2002

PANA Threat Analysis and security requirements

Status of this Memo

Abstract

The PANA (Protocol for carrying authentication for Network Access) working group is developing a layer 3 authentication method for authenticating clients to the access network. This document discusses the various trust models, threats present in these models and requirements out of these threats.

Table of Contents

1.0 Introduction

The PANA (Public Access and Network Authentication) working group is developing a layer 3 authentication method for authenticating to the access network. Any client wishing to get access to the network needs to discover the IP address of the PANA authentication agent (PAA) and then authenticate itself to the network. This document discusses the threats involved in PAA discovery and authenticating the client to the access network and the resulting security requirements out of the threats.

The requirements specified in this document are yet to be discussed in the working group and hence subject to change.

2.0 Keywords

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [KEYWORDS].

3.0 Terminology and Definitions

Device

A network element (namely notebook computers, PDAs, etc.) that requires access to a provider's network.

Device Identifier (DI)

The identifier used by the network as a handle to control and police the network access of a PANA 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.

Identity

The information used to identify the user. It is used for authenticating the PaC. Identity could be e.g, NAI [NAI]

Edge Subnet or link

The immediate IP subnet that is available to an interface of the device for network access.

Access/Edge Router

A router that is present in the edge subnet.

Enforcement Point (EP)

A node that is capable of filtering packets sent by the PaC to the Access/edge router using the DI information authorized by PAA.

PANA Client (PaC)

An entity in the edge subnet who is wishing to obtain network access from a PANA authentication agent within a network. A PANA client is associated with a device and a set of credentials to prove its identity within the scope of PANA.

PANA Authentication Agent (PAA)

An entity in the edge subnet whose responsibility is to authenticate the PANA client (PaC) and grant network access service to the device.

Authentication Server (AS)

An entity that authenticates the PaC which may be co-located with PAA or part of the back-end infrastructure.

Local Security Association (LSA)

A temporary security association between a PaC and a PAA, which is derived from credentials of the PaC during initial authentication.

Initial Authentication

Authentication performed when a device enters into the edge subnet and provides the credentials to be authorized for network access without having any a priori authorization information. This will require a PAA to verify the credentials either locally or by using a authentication server.

Re-authentication

Authentication that occurs when a device needs to extend the authorization lifetime, changes attributes such as IP address and/or MAC address, etc., for the same network access after successful initial authentication. This may require a PAA to verify the credentials (used for initial authentication) either locally or by using a AS.

Local re-authentication

A type of re-authentication that occurs locally between a PaC and a PAA by using the LSA established between them. In this type of re-authentication, the PaC does not use the same credentials as used for initial authentication.

4.0 Usage Scenarios

PANA is mostly expected to be used in environments where the nodes trust the operator of the network to provide the service but do not trust the other nodes in the network e.g., Public access networks, Hotel, Airport. In these environments, one may observe the following.

o The link between PaC and PAA may not a shared medium e.g. PPP over wireline.

o The link between PaC and PAA may be a shared medium e.g., Ethernet.

o All the PaCs may be authenticated to the access network at layer 2 already e.g., PPP, 802.11.

o PaCs may already share a security association with layer 2 authentication agent e.g., Access Point in 802.11, that provides per-packet authentication and encryption.

These factors affect the threat model of PANA. This document discusses the various threats in the context of the above attributes.

5.0 Assumptions

The communication paths involved in the discovery and authentication are as follows.

1) The path between PaC and PAA
2) The path between PAA and EP
3) The path between PAA and AS

If PAA and EP are co-located, the path is already secured. Even when they are not co-located, the network operators can setup a security association between PAA and EP to secure the traffic between PAA and EP. Hence it is assumed that path (2) is secure.

The authentication server could be co-located in the same network as PAA or with the back-end system. In either case, this document assumes that there exists a security association between PAA and back-end system. Without this, it is not possible to authenticate users securely. In the current deployment e.g. NAS and RADIUS, path (3) is secured.

Thus, this document considers threats only for path (1).

6.0 Types of Attacks

The PANA authentication client (PaC) needs to discover the PAA first. This involves either sending solicitations or waiting for advertisements. Once it has discovered the PAA, it will lead to authentication exchange with PAA. Once the access is granted, PaC will most likely exchange data with other nodes in the Internet. All these packets are vulnerable to attack. Attacker in the path between PaC and PAA can launch the following attacks.

1) Denial of Service (DoS) attacks, in which a malicious node (PaC) prevents communication between other PaCs and PAA. This includes resource exhaustion attacks etc.

2) Man In The Middle (MITM) attack include interception, insertion, deletion, modification, replaying, reflection back at the sender and redirecting messages.

3) Service theft, Stealing the service intended for someone else

7.0 Threat Scenarios

7.1 PAA Discovery

PaC is in the process of discovering the PAA. Agents are normally discovered by sending solicitations or receiving advertisements. Following are the possible threats.

T7.1.1: A malicious node can pretend to be a PAA by sending a spoofed advertisement.

T7.1.2: A malicious node can send a spoofed advertisement with capabilities that indicate less secure authentication methods than what the real PAA supports, thereby fooling the PaC into negotiating a less secure authentication method than what would otherwise be available. This is a bidding down attack.

T7.1.3: A malicious node can send solicitations to learn more information about networks which might help the attacker to launch some known attacks e.g., PAA supports weak authentication suite.

It may not be possible protect the discovery process because the security association between PaC and PAA does not exist prior to authentication and hence there is no way of protecting the discovery.

If mutual authentication is performed i.e., client to AS and AS to client, via the PAA, the successful authentication response from the AS can be used to validate the authenticity of the PAA. This works because of the assumption that PAA and the AS share a security association. In such cases, a node pretending to be a PAA can be detected at the end. Note that this does not prevent DoS attacks where the rogue PAA does not send any responses back to the client.

In existing dial-up networks, the clients authenticate to the network but generally do not verify the authenticity of the messages coming from NAS. This mostly works because the link between the device and the NAS is not shared with other nodes (assuming that nobody tampers with the physical link) and clients trust the NAS to provide the service, without which the network operator will not make any profit. As the nodes in the network cannot directly communicate with other nodes, spoofing is avoided. In this environment, as the PaC may

assume that the other end of the point-to-point link is the PAA, spoofing attacks are not present.

In environments where the link is shared, any node can pretend to be a PAA. Even the nodes that are authenticated at layer 2, can pretend to be a PAA and hence the threat is still present in such networks.

Requirement 1:

PANA MUST not assume that the discovery process is protected.

7.2 Authentication

PaC is in the process of authenticating to the PAA.

7.2.1 Identity Protection

Identity protection is a feature where the identities are not sent in clear. PaC and the AS exchange identities during the authentication process via the PAA. The identity of the AS itself may not be interesting to the attacker. But the attacker may be able to learn some partial information about the PaC using the identity of the AS in some cases e.g., when NAI is used as the identity, the attacker can learn the domain to which the PaC belongs to. The identity of the PaC, which is most interesting to the attacker, should be protected from the following attacks.

T7.2.1.1: A malicious node can learn identities by eavesdropping.

T7.2.1.2: A malicious node can send falsified identity requests to learn the identity of the PaC. It might typically happen by initiating an authentication exchange with the PaC and proceed till the identity is revealed. This is known as polling attack [RAT].

If the link is not shared, other nodes in the network cannot eavesdrop on the link. If the PaC ensures that it responds to identity requests only from the PAA at the other end (by verifying the IP address) of the link, it can avoid the spoofing attacks. This assumes that the network does ingress filtering to prevent some other node from sending a spoofed identity request.

If the link is shared and layer 2 does not provide encryption, then any node eavesdropping on the link can learn the identity. If the layer 2 provides encryption, then the identity can be hidden from the attacker. Polling attack is still possible even if the layer 2 is secured. The attacker can pretend to be a PAA and initiate the authentication request to learn the identity of the PaC.

Requirement 2:

PANA SHOULD protect the identity of the PaC from eavesdropping and polling attack.

7.2.2 Spoofing success or failure

An attacker can send falsified authentication success or failure to the PaC. By sending false failure, the attacker can prevent the client from accessing the network. By sending false success, the attacker can let any node gain access to the network.

If the link is not shared, it may be hard to launch this attack as the attacker needs to inject this packet at the right time and the PaC can always reject packets coming from any other source address other than the PAA.

If the link is shared and even if per-packet authentication is present at layer 2, the attack is still possible. The node which is already authenticated at layer 2 can still pretend to be a PAA and spoof the success or failure.

This attack is possible whenever the authentication is one way where the client is providing its credentials for accessing the network but it never verifies the credentials of the server.

7.2.3 MiTM attack

A malicious node can claim to be PAA to the real PaC and claim to be PaC to the real PAA. This is a MiTM attack where the PaC is fooled to think that it is communicating with real PAA and the real PAA is fooled to think that it is communicating with real PaC.

Requirement 3:

When the PaC and PAA mutually authenticate each other i.e the AS verifies the identities of PaC and PaC verify the identity of the AS, this attack can be averted.

7.2.4 Replay Attack

A malicious node can replay the messages that caused authentication failure or success at a later time to create false failures or success.

This threat is absent if the link is not a shared medium. If the link is shared, then the attacker can replay old messages to revoke the access to the client. Even if per-packet authentication is present at

layer 2, the attacker can pretend to be a PAA and replay the old messages.

Requirement 4:

PANA MUST be resistant to replay attacks.

7.3 PaC leaving the network

When the PaC leaves the network, it needs to inform the PAA before disconnecting from the network so that the resources used by PaC can be accounted properly. PAA may also choose to revoke the access any time if it deems necessary. Disconnect and revocation messages needs to be protected to avoid the following attacks.

T7.3.1: A malicious node can pretend to be a PAA and revoke the access to PaC.

T7.3.2: A malicious node can pretend to be a real PaC and disconnect from the network.

T7.3.2: A malicious node can use the above 2 schemes to disconnect the PaC from the network and steal its IP address and MAC address to gain unauthorized access into the network.

This threat is absent if the link between PaC and PAA is not a shared medium.

If the link is shared, any node on the link can spoof the disconnect message. Even if the layer 2 has per-packet authentication, the attacker can pretend to be a PaC e.g. by spoofing the IP address, and disconnect from the network. Similarly, any node can pretend to be a PAA and revoke the access to the PaC.

Requirement 5:

Disconnect and revocation messages MUST be authenticated.

7.4 Attacks on normal communication

PaC is exchanging data with some other node. Following threats are possible.

T7.4.1: Attacker can modify data packets.

T7.4.2: Attacker can use the IP address and MAC address of a different PaC to gain unauthorized access to the network.

Once the PaC is successfully authenticated, EP will have filters in place to prevent unauthorized access into the network. The filters will be based on something that will be carried on every packet. For example, the filter could be based on IP and MAC address where the packets will be dropped unless the packets coming with certain IP address match the MAC address also. Attacker can spoof both the IP and MAC address and inject packets into the communication of some other node.

This threat is absent in links that are not shared as simple ingress filtering can prevent one node from impersonating as another node.

If the link between PaC and PAA is shared, it is easy to launch this attack. Layer 2 authentication cannot prevent the node from using the IP address of some other node.

If the PaC is using a secure VPN service e.g. using IPsec, IPsec already provides per-packet data origin authentication and integrity. In this case, this threat is not present.

Requirement 6

PANA MUST be able to derive keys in order to enable per-packet authentication and integrity. PaC SHOULD be able to negotiate this feature if needed.

T7.4.3: Attacker can eavesdrop on the communication to learn useful information.

If the link between PaC and PAA is not a shared medium, attackers cannot eavesdrop and hence this threat is absent in such links.

If the layer 2 is shared, anyone can eavesdrop on the communication. If the layer 2 already provides encryption, then other nodes cannot learn any information by eavesdropping.

If the PaC is using a secure VPN service e.g. using IPsec, IPsec already provides per-packet confidentiality by encrypting the packets. In this case, this threat is not present.

Requirement 7

PANA MUST be able to derive keys in order to enable confidentiality. PaC SHOULD be able to negotiate this feature if needed.

T7.4.4: Attacker can replay packets at a later point in time causing old packets to be re-injected.

If the link between PaC and PAA is not a shared medium, attacker cannot inject packets into the communication and hence this threat is absent in such links.

If the layer 2 is shared and even if it is secure, an attacker can easily replay old packets.

If the PaC is using a secure VPN service e.g. using IPsec, IPsec already provides replay protection. In this case, this threat is not present.

Requirement 8

PANA per-packet authentication MUST provide anti-replay service.

7.5 Miscellaneous attacks

T7.5.1: Attacker can bombard the PAA with lots of authentication requests. This can lead to DoS attack, if the resources needed for discarding the request are more than what is needed for authenticating a real PaC. At least, PAA should not try to allocate resources till it completes authentication. EP may need to add filters at the beginning (as soon as the address is assigned) to prevent unauthorized access. Adding filters might consume resources if it has to allocate one for each PaC it is authenticating. PAA should not allocate resources till the authentication is completed.

T7.5.2: PaC acquires IP address before PANA authentication begins using methods like e.g., DHCP in IPv4 and auto-configuration in IPv6 [PANAREQ]. If IP addresses are assigned before authentication, it opens up the possibility of DoS attack where malicious nodes can deplete the IP addresses by assigning multiple IP addresses. This threat does not apply to IPv6 if stateless auto-configuration [ADDRCONF] is used. If stateful mechanism is used in IPv6 e.g., DHCPv6, then this attack is still possible. Address depletion attack is not specific to PANA, but a known attack in DHCP [DHCP-AUTH]. If PANA assumes that the client has an IP address already, it opens up the network to the DoS attack where addresses could be depleted.

Requirement 9

PANA should not assume that the client has a valid IP address.

8.0 Summary of Requirements

- o PANA MUST not assume that the discovery process is protected.

- o The authentication exchange SHOULD protect the identity of the PaC from eavesdropping and polling attack.

- o PaC and PAA MUST mutually authenticate each other to prevent MiTM attacks.

- o Disconnect and revocation messages MUST be authenticated.

- o PANA MUST be able to derive keys in order to enable per-packet authentication, integrity, confidentiality and protection against replay attacks. PaC SHOULD be able to negotiate this feature if needed.

- o PANA SHOULD not assume that the PaC has a valid IP address.

9.0 Security Considerations

This draft discusses various threats when using PAA for authenticating network access and does not give rise to any threats.

References

i Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

2. Bernard Aboba, “Pros and Cons of Upper Layer Network Access”

3. Arunesh Mishra, William A. Arbaugh, An Initial Security Analysis of the IEEE 802.1x Standard

4. IEEE. Standard for port based network access control. IEEE Draft P802.1X

5. [PANAUS] Yoshihiro Ohba et. al, Problem Space and Usage Scenarios for PANA, draft-ietf-pana-usage-scenarios-02.txt

6.[RAT] Dan Harkins et. al, Design Rationale for IKEv2, draft-ietf-ipsec-ikev2-rationale-00.txt

7.[NAI] B. Aboba, M. Beadles, The Network Access Identifier

8. [PANAREQ] A. Yegin et al., Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology, Internet-Draft, Work in progress

9. [ADDRCONF] Susan Thomson et.al IPv6 Stateless Address Configuration, RFC2462.

10. [DHCP-AUTH] R. Droms, et. al Authentication for DHCP messages, RFC3118.

11. [KEYWORDS] S. Bradner, Key words for use in RFCS to indicate requirement levels, RFC 2119, March 1997

Acknowledgments

Thanks to Alper Yegin and Basavaraj Patil for the initial feedback on this document. Pekka Nikkander provided comments that helped clarify this document and also helped identify some threats. Michael Thomas pointed out the missing replay attack and helped clarify the document.

Author's Addresses

Mohan Parthasarathy
Tahoe Networks

San Jose
Email: mohanp@tahoenetworks.com