PANA Working Group
Internet Draft

Document: draft-ietf-pana-threats-01.txt
Expires: June 2003

<Mohan
Parthasarathy>
<Tahoe Networks>

January 2003

PANA Threat Analysis and security requirements

Status of this Memo

Abstract

The PANA (Protocol for carrying authentication for Network Access) working group is developing methods for authenticating clients to the access network using IP based protocols. This document discusses the threats in general without referring to a specific authentication protocol. The security requirements arising out of these threats will be used as additional input to the PANA WG for designing the IP based network access protocol.

Table of Contents

1.0 Introduction

The PANA (Protocol for carrying authentication for Network Access) working group is developing methods for authenticating clients to the access network using IP based protocols. This document discusses the threats in general without referring to a specific authentication protocol.

There are multiple steps involved for any client wishing to get access to the network. First, it needs to discover the IP address of the PANA authentication agent (PAA) and then authenticate itself to the network using the PANA protocol. Once the client is authenticated, there might be other messages exchanged during the lifetime of the network access. This document discusses the threats present in these steps without referring to a specific authentication protocol. It does not discuss any solutions for the threats. The requirements arising out of these threats will be used as input to the PANA WG.

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

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.

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.

4.0 Usage Scenarios

PANA is 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.

- The link between PaC and PAA may not a shared medium e.g. DSL network.
- The link between PaC and PAA may be a shared medium e.g., Ethernet.
- All the PaCs may be authenticated to the access network at layer 2 already e.g., 3GPP2 CDMA network. Note that the clients still don't trust each other.
- 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. Note that the clients still don't trust each other.

The scenarios mentioned above affect the threat model of PANA. This document discusses the various threats in the context of the above network access scenarios for a better understanding of the threats.

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 of these 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) attacks, which include

interception, insertion, deletion, modification, replaying, reflection back at the sender and redirecting messages.

3) Service theft, Stealing the service of an authorized client without authenticating to the network.

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 biddingdown 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 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 prematurely end the authentication exchange effectively denying service for the PaC.

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, it is easy to spoof these packets. If layer 2 provides per-packet encryption, it might make it hard for the attacker to guess the success/failure packet that the client would accept. Even if the node is already authenticated at layer 2, it 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.

7.2.2 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 2

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.

7.2.3 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. The attacker can also potentially replay other messages of the PANA protocol to deny service to the PaC.

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 deny service to the client.

If the packets are encrypted at layer 2, it will make it hard for the attacker to learn the unencrypted (i.e., original) packet that needs to be replayed. Even if layer 2 provides per-packet integrity, the attacker can still replay the PANA messages (layer 3) for denying service to the client.

Requirement 3

PANA MUST be resistant to replay attacks.

7.2.4 Device Identifier attack

When the client is successfully authenticated, PAA sends access control information to EP for granting access to the network. The access control information typically contains the device identifier

of the PaC, which is obtained from the IP headers and MAC headers of the packets exchanged during the authentication process. The attacker can gain unauthorized access into the network using the following steps.

- An attacker pretends to be a PAA and sends advertisements. PaC gets fooled and starts exchanging packets with the attacker.
- The attacker modifies the IP source address on the packet, adjusts the UDP/TCP checksum and forwards the packet to the real PAA. It does the same on return packets also.
- When the real PaC is successfully authenticated, the attacker gains access to the network as the packets contained the IP address (and potentially the MAC address also) of the attacker.

This threat is absent if the link is not a shared medium. If the layer 2 provides per-packet protection, then it is not possible to change the MAC address and hence this threat may be absent in such cases if EP filters both on IP and MAC address. If the link is shared, it is easy to launch this attack.

Requirement 4

PANA MUST be able to protect against Device Identifier attack.

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.

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

PANA MUST be able to protect disconnect and revocation messages.

7.4 Service theft

An attacker can gain unauthorized access into the network by stealing the service of authenticated/authorized client. 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. Following are the possible threats.

T7.4.1: Attacker can spoof both the IP and MAC address to gain unauthorized access. The attacker just gets a free ride using the network access of some other client.

T7.4.2: Attacker can spoof both the IP and MAC address of any client and inject data packets into its data stream.

These threats are 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. If layer 2 provides per-packet protection, it can prevent the users from gaining unauthorized access. But it cannot prevent the nodes from using the IP address of some other node. Hence, the attacker can still inject false data.

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, it prevents the attacker from injecting false data. But the attacker can still gain unauthorized access.

Requirement 6

PANA MUST be able to provide sufficient access control information like IP address, MAC address, keys etc., to EP, which in turn can prevent unauthorized users from gaining access to the network.

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. In general, there is always the need to forward the request to the backend AS for authentication. This implies that the PAA may have to allocate resources to store some state about the PaC locally, before it receives the response from the backend AS. This can deplete resources locally if the PAA is bombarded with requests.

Requirement 6

PANA MUST be resistant to DoS attacks.

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 7

PANA should not assume that the PaC has acquired an IP address before PANA begins.

8.0 Summary of Requirements

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

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

- PANA MUST protect against Device Identifier attack.

- o PANA MUST be able to protect disconnect and revocation messages.

- o PANA MUST be able to provide sufficient access control information like IP address, MAC address, keys etc., to EP, which in turn can prevent unauthorized users from gaining access to the network.

- o PANA SHOULD not assume that the PaC has acquired an IP address (through other means) before PANA begins.

- o PANA MUST be resistant to DoS attacks.

9.0 Security Considerations

This draft discusses various threats when using PAA for authenticating network access. This will be taken as input by PANA WG for designing the IP based authentication protocol.

10.0 Normative References

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

2. [PANAUS] Yoshihiro Ohba et. al, Problem Space and Usage Scenarios for PANA, draft-ietf-pana-usage-scenarios-03.txt

3. [PANAREQ] A. Yegin et al., Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology, draft-ietf-pana-requirements-04.txt

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

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

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

11.0 Informative References

7. Bernard Aboba, Pros and Cons of Upper Layer Network Access, BURP BOF.

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

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

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

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. Device identifier attack came out of the discussion with Yoshihiro Ohba.

Revision Log

These are the changes between revision 00 and 01.

-Removed unused terms from section 3.0

-Removed identity protection as a threat after feedback from Atlanta IETF55 meeting.

-Renamed the section Attacks on Normal data communication to Service theft. Removed confidentiality mentioned in that section.

-Clarified text in lots of places.

- Added device identifier attack.

Author's Addresses

Mohan Parthasarathy
Tahoe Networks
3052 Orchard Drive
San Jose, CA 95134
Email: mohanp@tahoenetworks.com