PANA Working Group
Internet Draft
Document: draft-ietf-pana-threats-eval-02.txt
Expires: September 2003

<M. Parthasarathy>
<Tahoe Networks>

March 2003

# PANA Threat Analysis and security requirements

## Status of this Memo



## Copyright Notice



## 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.

PANA threat analysis March 2003

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.

A client wishing to get access to the network must carry on multiple steps. First, it needs to discover the IP address of the PANA authentication agent (PAA) and then execute an authentication protocol to authenticate itself to the network. Once the client is authenticated, there might be other messages exchanged during the lifetime of the network access. This document discusses the threats in these steps without discussing any solutions. The requirements arising out of these threats will be used as input to the PANA working group.

## 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 computer, PDA, etc.) that requires access to a provider's network.

Network Access Server (NAS)

Network device that provides access to the network.

Enforcement Point (EP)

A node that is capable of filtering packets sent by the PaC 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 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. It 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.

Compound methods





Authentication protocol where a sequence of methods is used inside an independently established tunnel between the client and server [TUN-EAP].

## 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. Note that the usage of word trust above does not mean trust relationship. It just denotes the belief about how the nodes involved in PANA behave in the future. In these environments, one may observe the following.

- The link between PaC and PAA may be a shared medium e.g. Ethernet or may not be a shared medium e.g. DSL network.

- All the PaCs may be authenticated to the access network at layer 2 (3GPP2 CDMA network) and share a security association with layer 2 authentication agent (802.11 Access point), but still do not 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 Trust Relationships

PANA authentication involves a client, PANA agent (PAA), Authentication server (AS) and an Enforcement point (EP). The communication paths involved between the various entities are as follows.

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

This document discusses the threats involved in path (1) and (2).

If PAA and EP are co-located, the path between PAA and EP (3) can be considered secure. Even when they are not co-located, the network operators can setup a security association between PAA and EP to secure the traffic between them. Hence it is assumed that path (3) is secure.





The authentication server (AS) could be co-located in the same network as PAA or with the back-end system. If it is co-located, then the path (4) can be considered secure. If it is not co-located, there are various threats possible in this path. [RAD-EAP] discusses the possible threats in this path. This implies that if RADIUS is used as the protocol between PAA and AS, then all the vulnerabilities that are mentioned in [RAD-EAP] are applicable to PANA. As it is beyond the scope of PANA to address these threats, this document does not discuss this further.

There is no pre-existing trust between PaC and EP. When PaC is successfully authenticated, it will further enable key derivation between PaC and EP, which can be used to secure the link. For example, EAP keying framework [EAP-KEY], defines a three party EAP exchange where the clients derive the transient sessions keys to secure the link between PaC and NAS in their final step. Similarly, PANA will provide the ability to derive keys between PaC and EP that can be used to secure the link further. This is further discussed in section 6.4 below.

## 6.0 Threat Scenarios

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 denial of service (DoS), man-in-the-middle (MITM) and service theft attacks.

The threats are grouped by the various stages the client goes through to gain access to the network. Section 6.1 discusses the threats related to PAA discovery. Section 6.2 discusses about the authentication itself. Section 6.3 discusses about the threats involved while leaving the network. Section 6.4 discusses about service theft. Section 6.5 discusses the miscellaneous threats.

## 6.1 PAA Discovery

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

T6.1.1: A malicious node can pretend to be a PAA by sending a spoofed advertisement.

T6.1.2: 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.

T6.1.3: 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.

In existing dial-up networks, the clients authenticate to the network but generally do not verify the authenticity of the messages coming from Network Access Server (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 and the phone network to provide the service, without

which the network operator will not make any profit. Since in this environment, nodes in the network cannot directly communicate with each other and 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 (including the nodes that are authenticated at layer 2). Hence, the threat is still present in such networks. It is difficult to protect the discovery process, as there is no a priori trust relationship between PAA and PaC. In IEEE 802.11i, the discovery [Beacon, Probe Request/Response] process itself is not protected because the discovered capabilities are included in a subsequent secured exchange allowing spoofing to be discovered later. It is also possible that EP might be able to filter out the packets coming from PaC that resembles PAA packets.

Requirement 1

PANA MUST not assume that the discovery process is protected. Since, it is difficult to protect the discovery process, the information exchanged during the discovery process SHOULD be limited.

## 6.2 Authentication

This section discusses the threats specific to the authentication protocol. Section 6.2.1 discusses the possible threat associated with success/failure indications that are transmitted to PaC at the end of the authentication. Section 6.2.2 discusses the man-in-the-middle attack when compound methods are used. Section 6.2.3 discusses the replay attack and section 6.2.4 discusses about the device identifier attack.

### 6.2.1 Success or Failure Indications





An attacker can send false 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 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 with pair-wise keys, 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 because the success or failure indication is not protected using a security association between PaC and PAA. In order to avoid this attack, PaC and PAA should mutually authenticate each other. In the process of mutually authenticating each other, they should be able to derive keys to protect the success/failure indications.

Requirement 2

PaC and PAA MUST mutually authenticate to each other using methods that can derive keys, which in turn can protect the success and failure indications.

### 6.2.2 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.

An instance of MITM attack, when compound authentication methods are used is described in [TUN-EAP]. In these attacks, the server first authenticates to the client. As the client has not proven its identity yet, it acts as the man-in-the-middle, tunneling the identity of the legitimate client to gain access to the network. The attack is possible because there is no verification that the same entities participated among the compound methods. It is not possible to do such verification, if compound methods are used without being able to create cryptographic binding among them. This implies that PANA will be vulnerable to such attacks if compound methods are used without being able to cryptographically bind them.

Requirement 3

When compound authentication methods are used in PANA, the methods MUST be cryptographically bound.

### 6.2.3 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 using pair-wise keys, 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 replay protection, the attacker can still replay the PANA messages (layer 3) for denying service to the client.

Requirement 4

PANA MUST be resistant to replay attacks.

### 6.2.4 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 5

The device identifier transmitted from the PaC to PAA MUST be protected.

## 6.3 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. Following are the possible threats.

T6.3.1: A malicious node can pretend to be a PAA and revoke the access to PaC.

T6.3.2: A malicious node can pretend to be a real PaC and transmit a disconnect message.

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.

In some link layers, e.g., 802.11, disassociate and de-authenticate messages are not protected (even with 802.11i). In such link layers, protecting PANA messages may not be very useful as the attacker can attack using the link layer mechanisms rather than PANA.

Requirement 6

PANA MUST be able to protect disconnect and revocation messages.

## 6.4 Service theft

An attacker can gain unauthorized access into the network by stealing the service from another 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.

T6.4.1: Attacker can spoof both the IP and MAC address to gain unauthorized access.

T6.4.2: Attacker can spoof both the IP and MAC address of any node 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 using pair-wise keys, it can prevent the attacker from gaining unauthorized access using the layer 2 identifier of some other node. But it cannot prevent the nodes from using the IP address of some other node. Hence, the attacker can still inject false data by spoofing IP addresses.

If the PaC is using a secure VPN service back to the corporate network 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 this does not prevent the attacker from gaining unauthorized access by spoofing the device identifier of the authorized client.

T6.4.2 itself is beyond the scope of PANA. But PANA MUST be able to prevent service theft (T6.4.1). In some cases e.g. non-shared links, it is sufficient to provide access control information like IP address, MAC address, etc., to EP, which in turn can prevent unauthorized users from gaining access to the network. In the case of shared links, it is not sufficient. PANA MUST be able to provide sufficient guidelines for deriving transient keys between PaC and EP.

For example, EAP keying document [EAP-KEY] defines methods to derive such keys between the various entities involved in EAP. This key can be further used to setup a security association (e.g., IPsec) between PaC and EP to prevent service theft on shared links.

Requirement 7

PANA MUST be able to provide sufficient access control information like IP address, MAC address etc. to EP for preventing service theft. PANA MUST be able to provide sufficient guidelines for deriving keys between PaC and EP which can be further used to setup a security association for preventing service theft on shared links.





## 6.5 Miscellaneous attacks

T6.5.1: There are various forms of DoS attacks that can be launched on the PAA or AS.

- Attacker can bombard the PAA with lots of authentication requests. If PAA and AS are not collocated, PAA may have to allocate resources to store some state about PaC locally before it receives the response from the backend AS. This can deplete memory resources on PAA.
- The attacker can force the PAA or AS to make a public key computation with minimal effort, that can deplete the CPU resources of the PAA or AS.

T6.5.2: 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. If stateless auto-configuration [ADDRCONF] is used, the attacker can respond to duplicate address detection probes sent by any node on the network effectively not allowing the node to configure a link local address. 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.

Requirement 8

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

## 7.0 Summary of Requirements

1. PANA MUST not assume that the discovery process is protected. Since, it is difficult to protect the discovery process, the information exchanged during the discovery process SHOULD be limited.

2. PaC and PAA MUST mutually authenticate to each other using methods that can derive keys, which in turn can protect the success and failure indications.

3. When compound authentication methods are used in PANA, the methods MUST be cryptographically bound.





4. PANA MUST be resistant to replay attacks.

5. The device identifier transmitted from the PaC to PAA MUST be protected.

6. PANA MUST be able to protect disconnect and revocation messages.

7. PANA MUST be able to provide sufficient access control information like IP address, MAC address etc. to EP for preventing service theft. PANA MUST be able to provide sufficient guidelines for deriving keys between PaC and EP which can be further used to setup a security association for preventing service theft on shared links.

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

## 8.0 Security Considerations

This document discusses various threats with IP based network access protocol.

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


## 10.0 Informative References


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







6. Arunesh Mishra, William A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard"

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

8. [RADIUS] C. Rigney et.al, "Remote Authentication Dial In User Service".

9. [EAP-KEY] Bernard Aboba et. al, "EAP keying framework", Work in Progress.

10. [ADDRCONF] Susan Thomson et. al "IPv6 Stateless Address

Autoconfiguration", RFC2462.

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

12. [RAD-EAP] Bernard Aboba, et. al "Radius support for Extensible authentication protocol", draft-aboba-radius-rfc2869bis-08.txt

13. [TUN-EAP] J. Puthenkulam et. al "The compound authentication binding problem", draft-puthenkulam-eap-binding-01.txt

## 12.0 Acknowledgments

The author would like to thank the following people (in no specific order) for providing comments: Alper Yegin, Basavaraj Patil, Pekka Nikkander, Bernard Aboba, Francis Dupont, Michael Thomas, Yoshihiro Ohba, Gabriel Montenegro and Tschofenig Hannes.

## 13.0 Revision Log

Changes between revision 01 and 02

- Renamed the section "Assumptions" to "Trust relationships" and added more text to clarify the relationship between PaC and EP.
- Added more text for threats in PAA 96 AS path
- Merged the "Type of Attacks" section into "Threat Scenarios"
- Removed the requirement on DoS attack
- Reworded most of the requirements

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 as a requirement from that section.
- Added a new threat "Device Identifier attack".

## 14.0 Author's Addresses

Mohan Parthasarathy
Tahoe Networks
3052 Orchard Drive
San Jose, CA 95134

Phone: 408-944-8220
Email: mohanp@tahoenetworks.com

## 15.0 Full Copyright Statement







Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.