PANA Threat Analysis and Security Requirements Research Paper

Georg-Simon-Ohm Fachhochschule Nürnberg
Internet Security

by
Stefan Hertel

Topics

- **Introduction**
  - PANA Working Group
  - Relation of the Draft to PANA Working Group
  - Contents of the Draft
  - Position in Internet Layer Model
  - Acronyms and Definitions
  - Network Structure

- **PANA Usage Scenarios**
  - Linked by a Shared Medium
  - Linked by a Non-Shared Medium
  - Linked at Layer 2 with Security Association

- **PANA Threat Scenarios**
  - PAA Discovery
  - Authentication - Success or Failure Indication
  - Authentication - Man in the Middle Attack
  - Authentication - Replay Attack
  - Authentication - Device Identifier Attack
  - PaC leaving the Network
  - Service Theft
  - PAA-EP Communication
  - Miscellaneous Attacks

- **Literature**

Introduction

This Research Paper is based on [1]. The draft was created in May 2003 and has expired in November 2003 as all drafts do after 6 months.

PANA Working Group

PANA (Protocol for carrying authentication for Network Access) working group develops methods for authenticating clients to the access network using IP based protocols.

Relation of the Draft to PANA Working Group

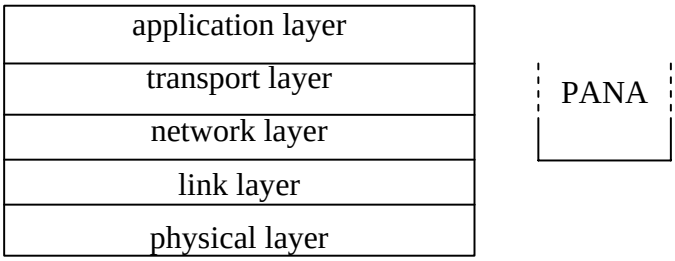
The draft [1] discusses the threats to such authentication protocols. To avoid those threats some requirements to security arise. These security requirements are used as additional input to the PANA working group to help designing the IP based network access authentication protocol.

Contents of the Draft

When a client wishes to get access to the network it must carry on multiple steps. These are at first the discovery of an authentication agent and then the accomplishment of an authentication process. Also there may be further communication on access authentication protocol level during the lifetime of the connection.
The document [1] discusses the threats in these steps but does not discuss or provide any solutions. The security requirements are used as mentioned above.

Position in Internet Layer Model

PANA working group is considering the network access authentication function being performed at or above the IP layer:



Acronyms and Definitions

PaC: PANA Client
An entity who is wishing to obtain network access from a PANA authentication agent.

PAA: PANA Authentication Agent (PAA)
Is responsible to authenticate the PANA client and grant the network access service.

AS: Authentication Server (AS)
Authenticates the PANA client. Can be part of the same entity as PANA authentication agent or part of the back-end infrastructure.

DI: Device Identifier (DI)
It might contain, depending on the access technology, IP address, link-layer address or other. Therefore it may be a network card.
A PANA client should be associated with a DI on a PANA authentication agent.

EP: Enforcement Point (EP)
A node between PaC and PAA that can filter packets sent by the PaC

Compound methods:

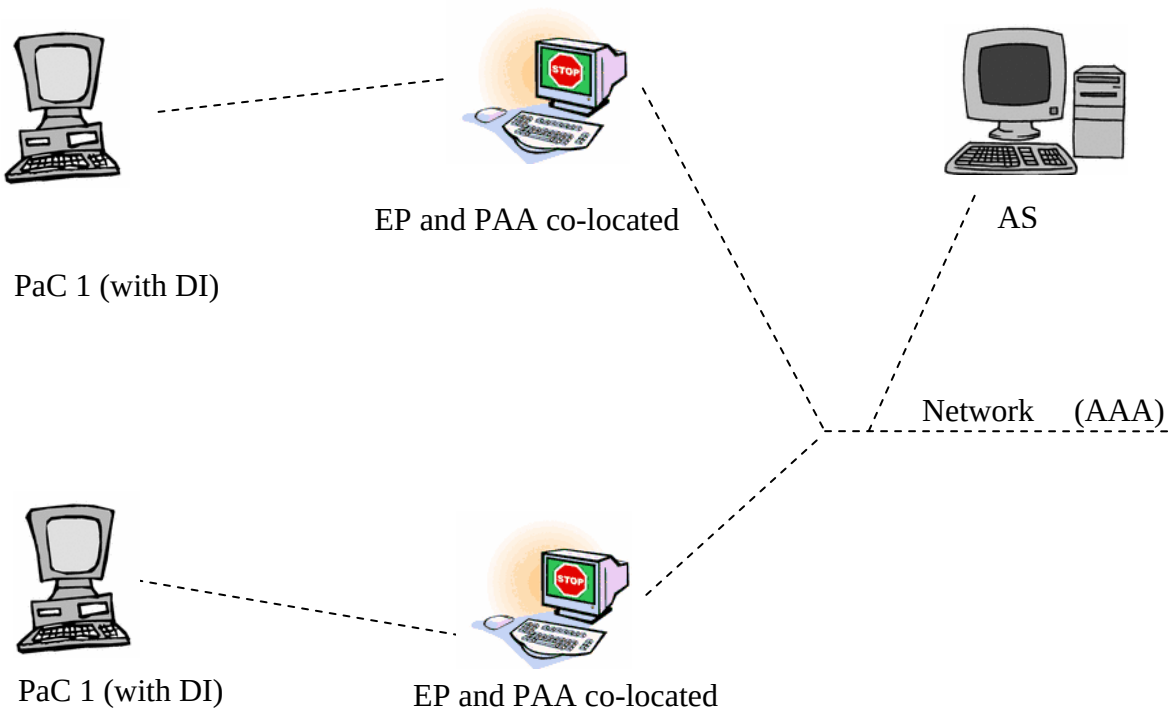
Securing weaker authentication protocols using tunnels like TLS or IPSEC.

AAA:

Authentication, Authorization and Accounting

Network Structure

One possible network structure scenario for the use of PANA is shown in the following graphik:

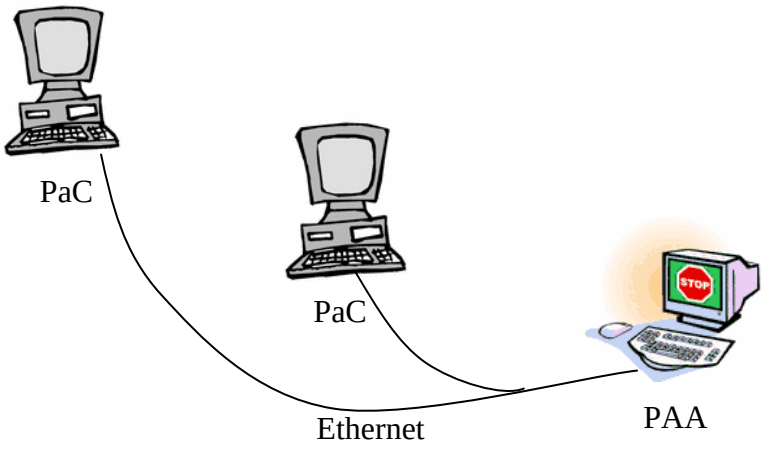


PANA Usage Scenarios

There are 3 usage scenarios how a PaC can be linked to the PAA. Not all of them can be found under all circumstances. When talking about possible threats the usage scenario, which is the easiest to be attacked, has to be taken into consideration. In this way the scenarios affect the threat model of PANA.

If no assumption can be made about the type of a link it is considered the same as if being shared by more than one node.

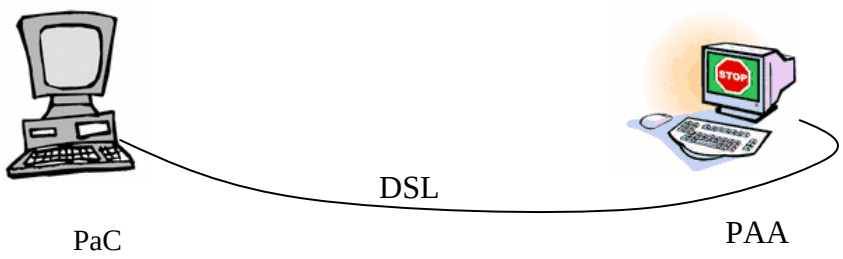
Linked by a Shared Medium



When using a shared medium like ethernet, the link between PaC and PAA is assumed to be not physical secure.

Usage Scenario 1

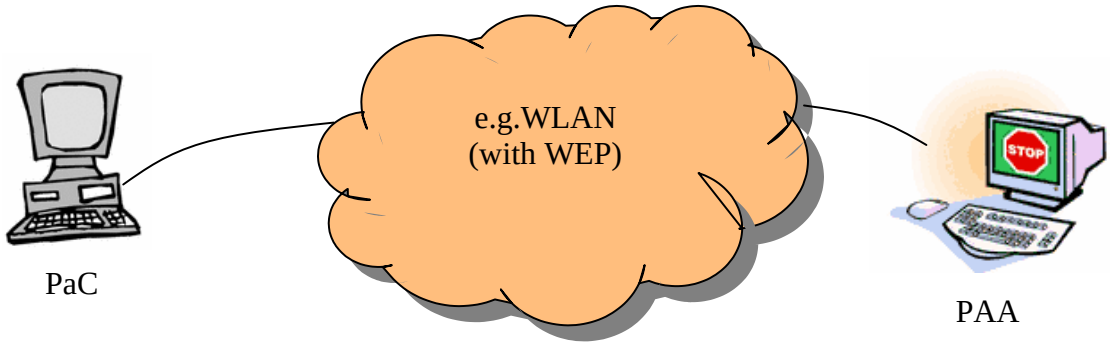
Linked by a Non-Shared Medium



Usage Scenario 2

A link between PaC and PAA using a non-shared medium like DSL is assumed to be physical secure.

Linked at Layer 2 with Security Association



Usage Scenrio 3

There may be an authentication to the network at layer 2, maybe even with sharing a security association, but there is still no trust between PaC and PAA. This fact is not really amazing as it is popular known that a security mechanism like WEP can be broken and link layer addresses can be spoofed.

PANA Threat Scenarios

When a client goes through the necessary steps to authenticate to the network the attacks discussed in the following are possible. Due to these threats, and taking the usage scenarios in consideration, are arising the security requirements for the design of the network access protocol.

PAA Discovery

In the initial stage the PaC does not know the PAA. The discovery process can be accomplished in two ways. Either the PaC discovers the PAA by sending solicitations and the PAA answers to them or the PAA is receiving advertisements from the PAA.
In general a client authenticates to the network but does not verify the authenticity of the messages from network access server.
In common dial-up networks or when using a point-to-point connection like dsl this is no problem to securtiy because the PAA can take it for granted that it is talking to the PAA.
If a shared medium scenario applies, it is very difficult to protect the discovery process because there is no a priori trust relationship between the PaC and the PAA.
A malicious node could pretend being the PAA. If there is some additional information, like the supported authentication mechanisms, included in the discovery packets this could lead to some kind of downgrade attack.
It is possible in some environments to produce relief with an EP which filters packets from a PaC

which resemble PAA packets.
The reduction of potential harm can be achieved by limiting the amount of security-critical information sent during the PAA discovery process.

Security Requirement 1
PANA must not assume that the discovery process is protected.
Due to the fact that it is difficult to protect the discovery process, the exchange of information, which can be used by an attacker to acquire access data, during the discovery process should be limited.

Authentication - Success or Failure Indication
PANA, like some existing authentication protocols, e.g. EAP, is expected to have some messages that indicate special states. This does not only include success or failure indications transmitted during the authentication process. All PANA messages exchanged prior to the establishment of a shared secret are affected.
A threat here is possible if a shared medium is used. Considering usage scenario 3 this is a possible threat even if there is an authentication mechanism at layer 2.
An attacker could prevent a PaC from accessing the network by sending a false failure message. Or he could prematurely end authentication exchange by sending a false success message and so deny service to the PaC.
The attack can be avoided if the indications are protected by keys. There are two possibilities to use such an protection mechanism. One is that PaC and PAA mutually authenticate each other and establish the keys needed to protect the indications in this process. If this is not possible and it is not the first time the PaC tries to connect to the network, the keys in the previously established session can be used.

Security Requirement 2
PaC and PAA must be able to mutually authenticate each other in PANA.
PANA must be able to establish keys between PaC and PAA to protect the PANA messages.

Authentication - Man in the Middle Attack
A malicious node claims being PaC to the PAA and being PAA to the PaC. Both are fooled because they think they are talking to their real communication partner but in truth they communicate with an attacker. This is called a man in the middle attack.
Man in the middle attacks are possible in usage scenario 1 and 3. Even in the case if layer 2 provides per packet protection. One could say this is no problem when using a secure tunnel mechanism, e.g. IPSEC. But these compound methods [2] do not provide security in general. An attacker could act as man in the middle by first authentication to the PaC and then tunnelling the client's data to the PAA. The security of the tunnel is broken then. In this case the attacker gains access to the less secure authentication protocol and can gain unauthorized network access and even the client's authentication data.
This is a possible attack because there is no verification that the same entities participated among the compound methods. To avoid this there has to be a cryptographic binding established between the compound used protocols.

Security Requirement 3
When compound authentication methods are used in PANA, the methods must be cryptographically bound.

Authentication - Replay Attack
An attacker can store PANA messages exchanged between PaC and PAA. This is possible in usage scenario 1 and 3. There might be an encryption at layer 2. In this case the attacker would have to guess the correct packets he needs to replay, but it is still possible. Also if layer 2 provides mechanisms to prevent replay attacks the PANA messages could still be replayed.

A malicious node can replay messages that caused authentication failure or success later. So he could gain access to the network or deny service to the authorized client. The attacker can replay other pana messages too and so at least deny service to the PaC.

Security Requirement 4
PANA must be able to protect itself against replay attacks.

Authentication - Device Identifier Attack
As seen in the network structure picture, the first communication partner of the PaC is the EP. PAA may be co-located with the EP. Typical PaC authenticates at PAA and PAA then passes the authenticated PaC's device identifier's data to the EP which then allows PaC's communication packets to pass through.
Now if usage scenario 2 applies, meaning the link is not shared, a device identifier attack is not possible because no attacker can pretend being the PaC by spoofing his device identifier's data. If layer 2 already provides per packet protection, the threat can be avoided. Then changing the MAC address is not possible. Further the EP needs to filter both, MAC and IP address of the client and can detect and drop spoofed packets now.
Else a possible attack could look like this. A malicious node starts communicating with the PaC. Remember the possible attacks from PAA discovery. The fooled PaC now communicates with the attacker who modifies IP source and adjusts checksums of the packets recieved from the client. He does the same with return packets from the network too. After the PaC has successful authenticated the attacker gains network access, because the EP now has stored the attacker's DI data in his table for authorized users.

Security Requirement 5
PANA must be able to protect the device identifier against spoofing when it is exchanged between the PaC and PAA.

PaC leaving the Network
To achieve a better commerce of system resources, a PaC informs the PAA before disconnecting so that the resources used for this PaC can be cleared. Another possibility is, that the PAA needs to revoke the access to a client for some reason, e.g. an idle timeout of a client.
This leads to 3 possible threat scenarios. An attacker can revoke network access to the PaC by pretending he is the PAA. Another one is that the attacker can pretend being the PaC and send a disconnect message to the PAA. In both cases the service is denied for the authorized user. These threats apply only in usage scenario 1 and 3.
The third threat is a PaC that leaves the network without notifing the PAA so EP still takes the PaC's DI data for valid. This can happen for example when a system crash occurs or the network cable is unplugged. Now an attacker can pretend being the PaC and start using the network by spoofing the PaC's IP and MAC address resembling the device identifier attack. If layer 2 provides per packet protection this threat does not apply too, because it is impossible to spoof the MAC address. But without this additional security mechanism this threat is possible in all three usage scenarios.

Security Requirement 6
PANA must be able to protect disconnect and revocation messages.
PANA must not depend on the PaC sending a disconnect message.

Service Theft
An attacker can use the DI data of an authorized and authenticated PaC to gain access to the network services. This could happen for example when the attacker sniffs network and spoofs both of authorized client's MAC and IP address. He gains access when the EP stores these too and provides network service because of them.
Service theft is a possible threat at shared links only according to usage scenario 1 and 3. Like

mentioned in the last threat scenarios this threat does not apply if layer 2 provides per-packet protection.

Security Requirement 7
In order to prevent this threat PANA must be able to establish a shared secret between PaC an PAA which can be used to setup a security association between PaC and EP. With an established cryptographic protection between PaC and EP service theft on shared links is prevented.

PAA-EP Communication
PAA must send access control information to EP after a PaC's successful authentication. In common this information will contain at least the DI.
Communication between PaC and EP is not threatened if eavesdropping the communication between them is not possible. For example if the communication is done on a separate link or if PAA and EP are co-located.
If eavesdropping is possible here, an attacker could take advantage from that and gain DI information of an authorized and authenticated PaC. With that knowledge he could spoof the real PaC and one of the threats mentioned before, e.g. service theft, can apply.
If communication between PAA and EP is done on a shared link this leads to another possible attack. A malicious node could pretend to the EP to be the real PAA and store some DI information of his own, gaining unauthorized network access.

Security Requirement 8
The communication between PAA and EP must be protected against eavesdropping and spoofing attacks.

Miscellaneous Attacks
At last there are the DOS attacks. It is hard evade DOS attacks so every mechanism used in PANA has be considered carefully, e.g. strong encryption needs lot of computing time from which these attacks benefit.
There are three possible attacks. First an attacker can bombard the PAA with authentication requests. For each the PAA has to perform a request to the AS, wait for the answer and create a rejection message. Depending on the system architecture this takes some time and reduces bandwith for service data. Or the PAA could run out of memory.
The second one is that the attacker forces the PAA to do computational intensice operations, e.g. cryptographic computations. This can deplete cpu resources of the PAA.
At last there is the address depletion attack. This is not really specific to PANA because the protocol needs some underlying architecture. And according to [3] PANA must not make any assumptions on the protocols or mechanisms used for IP address configuration of the PaC. But it could deny the service and in this case it has to be mentioned here.
A malicious nodes can deplete the IP addresses by assigning multiple IP addresses when using DHCP in IPv4 like in IPv6. Or if stateless auto-configuration is used, the attacker can respond to duplicate address detection probes so the sending node can not obtain an IP address.

Security Requirement 9
PANA should not assume that the PaC has acquired an IP address before PANA begins.
Due to the fact that this requirement points to the address depletion attack, which is no more PANA specific, this requirement is not a "must" like the others but a "should". Nevertheless someone trying to launch a DOS attack would benefit from the fact, if the security requirement 9 is ignored.

Literature

[1] draft-ietf-pana-threats-eval-04
[2] draft-puthenkulam-eap-binding-02
[3] draft-ietf-pana-requirements-07