PANA Working Group
Internet-Draft
Expires: December 14, 2007

P. Jayaraman
Net.Com
R. Lopez
Univ. of Murcia
Y. Ohba (Ed.)
Toshiba
M. Parthasarathy
Nokia
A. Yegin
Samsung

June 12, 2007

Protocol for Carrying Authentication for Network Access (PANA) Framework

draft-ietf-pana-framework-09

Status of this Memo

Copyright Notice

Abstract

This document defines the general PANA framework functional elements, high-level call flow, and deployment environments.

Table of Contents

1. Introduction

PANA (Protocol for carrying Authentication for Network Access) is a link-layer agnostic network access authentication protocol that runs between a client that wants to gain access to the network and a server on the network side. PANA defines a new EAP [RFC3748] lower layer that uses IP between the protocol end points.

The motivation to define such a protocol and the requirements are described in [RFC4058]. Protocol details are documented in [I-D.ietf-pana-pana]. Upon following a successful PANA authentication, per-data-packet security can be achieved by using physical security, link-layer ciphering, or IPsec [I-D.ietf-pana-ipsec]. The server implementation of PANA may or may not be co-located with the entity enforcing the per-packet access control function. When the server for PANA and per-packet access control entities are separate, SNMP [I-D.ietf-pana-snmp] may be used to carry information between the two nodes.

PANA is intended to be used in any access network regardless of the underlying security. For example, the network might be physically secured, or secured by means of cryptographic mechanisms after the successful client-network authentication.

This document defines the general framework for describing how these various PANA and other network access authentication elements interact with each other, especially considering the two basic types of deployment environments.

1.1. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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 [RFC2119].

2. General PANA Framework

PANA is designed to facilitate authentication and authorization of clients in access networks. PANA is an EAP [RFC3748] lower-layer that carries EAP authentication methods encapsulated inside EAP between a client node and a server in the access network. While PANA enables the authentication process between the two entities, it is only a part of an overall AAA (Authentication, Authorization and Accounting) and access control framework. A AAA and access control framework using PANA is comprised of four functional entities.

Figure 1 illustrates these functional entities and the interfaces (protocols, APIs) among them.

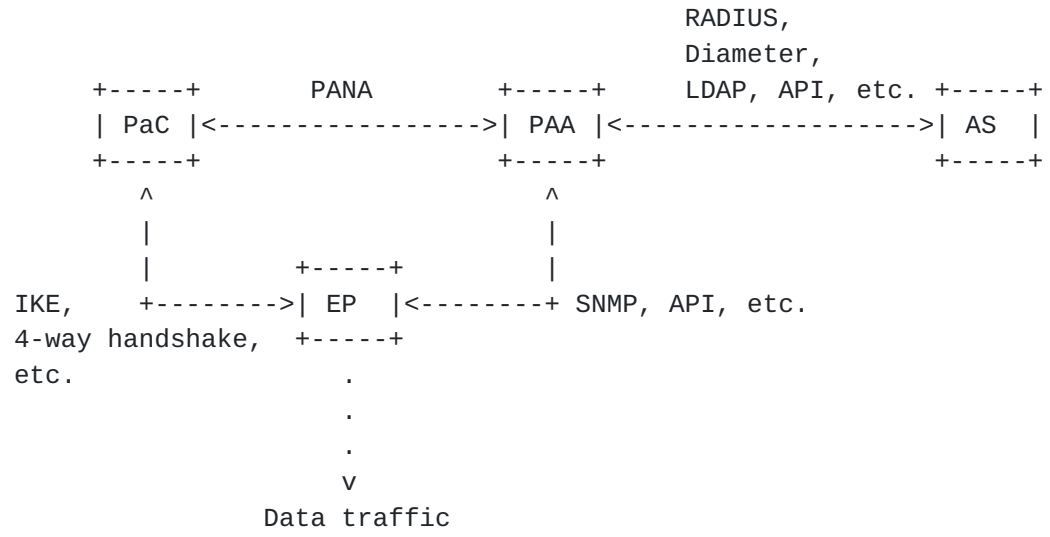

Figure 1: PANA Functional Model

PANA Client (PaC):

The PaC is the client implementation of PANA. This entity resides on the node that is requesting network access. PaCs can be end hosts, such as laptops, PDAs, cell phones, desktop PCs, or routers that are connected to a network via a wired or wireless interface. A PaC is responsible for requesting network access and engaging in the authentication process using PANA.

PANA Authentication Agent (PAA):

The PAA is the server implementation of PANA. A PAA is in charge of interfacing with the PaCs for authenticating and authorizing them for the network access service.

The PAA consults an authentication server in order to verify the

credentials and rights of a PaC. If the authentication server resides on the same node as the PAA, an API is sufficient for this interaction. When they are separated (a much more common case in public access networks), a protocol needs to run between the two. AAA protocols like RADIUS [RFC2865] and Diameter [RFC3588] are commonly used for this purpose.

The PAA is also responsible for updating the access control state (i.e., filters) depending on the creation and deletion of the authorization state. The PAA communicates the updated state to the Enforcement Points in the network. If the PAA and EP are residing on the same node, an API is sufficient for this communication. Otherwise, a protocol is required to carry the authorized client attributes from the PAA to the EP. Separated PAA and EPs MUST implement SNMP [I-D.ietf-pana-snmp], although the use of this protocol is optional (i.e., a substitute PAA-to-EP protocol may be used).

The PAA resides on a node that is typically called a NAS (network access server) in the access network. For example on a BRAS (Broadband Remote Access Server) [DSL] in DSL networks, or PDSN (Packet Data Serving Node) [3GPP2] in 3GPP2 networks. The PAA may be one or more IP hops away from the PaCs.

Authentication Server (AS):

The server implementation that is in charge of verifying the credentials of a PaC that is requesting the network access service. The AS receives requests from the PAA on behalf of the PaCs, and responds with the result of verification together with the authorization parameters (e.g., allowed bandwidth, IP configuration, etc). This is the server that terminates the EAP and the EAP methods. The AS might be hosted on the same node as the PAA, on a dedicated node on the access network, or on a central server somewhere in the Internet.

Enforcement Point (EP):

The access control implementation that is in charge of allowing access (data traffic) of authorized clients while preventing access by others. An EP learns the attributes of the authorized clients from the PAA.

The EP uses non-cryptographic or cryptographic filters to selectively allow and discard data packets. These filters may be applied at the link-layer or the IP-layer [I-D.ietf-pana-ipsec]. When cryptographic access control is used, a secure association protocol (e.g., [RFC2409], [RFC4306], [802.11i]) needs to run

between the PaC and EP. After completion of the secure association protocol, link or network layer per-packet security (for example TKIP, IPsec ESP) is enabled for integrity protection, data origin authentication, replay protection and optionally confidentiality protection.

An EP is located between the access network (the topology within reach of any client) and the accessed network (the topology within reach of only authorized clients). It must be located strategically in a local area network to minimize the access of unauthorized clients. It is recommended but not mandated that the EP be on-path between the PaC and the PAA for the aforementioned reason. For example, the EP can be hosted on the switch that is directly connected to the clients in a wired network. That way the EP can drop unauthorized packets before they reach any other client node or beyond the local area network.

Some of the entities may be co-located depending on the deployment scenario. For example, the PAA and EP would be on the same node (BRAS) in DSL networks. In that case a simple API is sufficient between the PAA and EP. In small enterprise deployments the PAA and AS may be hosted on the same node (access router) that eliminates the need for a protocol run between the two. The decision to co-locate these entities or otherwise, and their precise location in the network topology are deployment decisions that are out of the scope of this document.

3. Call Flow

Figure 2 illustrates the signaling flow for authorizing a client for network access.

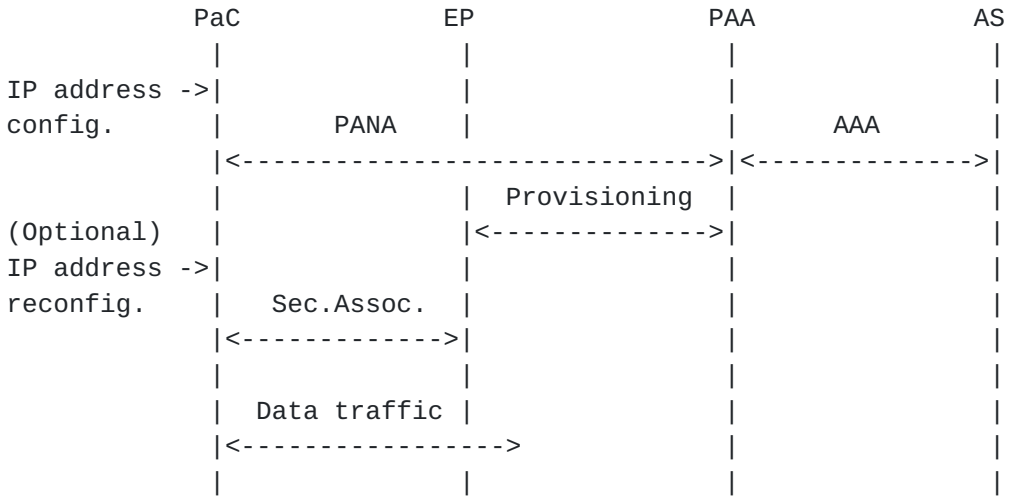

Figure 2: PANA Signaling Flow

The EP on the access network allows general data traffic from any authorized PaC, whereas it allows only limited type of traffic (e.g., PANA, DHCP, router discovery, etc.) for the unauthorized PaCs. This ensures that the newly attached clients have the minimum access service to engage in PANA and get authorized for the unlimited service.

The PaC dynamically or statically configures an IP address prior to running PANA. After the successful PANA authentication, depending on the deployment scenario the PaC may need to re-configure its IP address or configure additional IP address(es). For example, a link-local IPv6 address may be used for PANA and the PaC may be allowed to configure additional global IPv6 address(es) upon successful authentication. Another example: A PaC may be limited to use a IPv4 link-local address during PANA, and allowed to reconfigure its interface with a non-link-local IPv4 address after the authentication. General-purpose applications cannot use the interface until PANA authentication succeeds and appropriate IP address configuration takes place.

An initially unauthorized PaC starts the PANA authentication by discovering the PAA, followed by the EAP exchange over PANA. The PAA interacts with the AS during this process. Upon receiving the authentication and authorization result from the AS, the PAA informs the PaC about the result of its network access request.

If the PaC is authorized to gain the access to the network, the PAA also sends the PaC-specific attributes (e.g., IP address, cryptographic keys, etc.) to the EP by using another protocol (e.g., SNMP). The EP uses this information to alter its filters for allowing data traffic from and to the PaC to pass through.

In case cryptographic access control needs to be enabled after the PANA authentication, a secure association protocol runs between the PaC and the EP. Dynamic parameters required for that protocol (e.g., endpoint identity, shared secret) are derived from successful PANA authentication; these parameters are used to authenticate the PaC to the EP and vice-versa as part of creating the security association. For example, see [I-D.ietf-pana-ipsec] for how it is done for IKE based on using a key-generating EAP method for PANA between the PaC and PAA. The secure association protocol exchange produces the required security associations between the PaC and the EP to enable cryptographic data traffic protection. Per-packet cryptographic data traffic protection introduces additional per-packet overhead but the overhead exists only between the PaC and EP and will not affect communications beyond the EP.

Finally, filters that are installed at the EP allow general purpose data traffic to flow between the PaC and the intranet/Internet.

4. Environments

PANA can be used on any network environment whether there is a lower-layer secure channel between the PaC and the EP prior to PANA, or one has to be enabled upon successful PANA authentication.

With regard to network access authentication two types of networks need to be considered:

a. Networks where a secure channel is already available prior to running PANA

This type of network is characterized by the existence of protection against spoofing and eavesdropping. Nevertheless, user authentication and authorization is required for network connectivity.

One example is a DSL network where the lower-layer security is provided by physical means (a.1). Physical protection of the network wiring ensures that practically there is only one client that can send and receive IP packets on the link. Another example is a cdma2000 network where the lower-layer security is provided by means of cryptographic protection (a.2). By the time the client requests access to the network-layer services, it is already authenticated and authorized for accessing the radio channel, and link-layer ciphering is enabled.

The presence of a secure channel before PANA exchange eliminates the need for executing a secure association protocol after PANA. The PANA session can be associated with the communication channel it was carried over. Also, the choice of EAP authentication method depends on the presence of this security during PANA run. For example, weak authentication methods, such as EAP-MD5, may be used for such networks but not for the others.

b. Networks where a secure channel is created after running PANA

These are the networks where there is no lower-layer protection prior to running PANA. A successful PANA authentication enables generation of cryptographic keys that are used with a secure association protocol to enable per-packet cryptographic protection.

PANA authentication is run on an insecure channel that is vulnerable to eavesdropping and spoofing. The choice of EAP method must be resilient to the possible attacks associated with such an environment. Furthermore, the EAP method must be able to create cryptographic keys that will later be used by the secure

association protocol.

Whether to use a link-layer per-packet security (b.1) or a network layer security (b.2) is a deployment decision and outside the scope of this document. This decision also dictates the choice of the secure association protocol. If link-layer protection is used, the protocol would be link-layer specific. If IP-layer protection is used, the secure association protocol would be IKE and the per-packet security would be provided by IPsec AH/ESP regardless of the underlying link-layer technology.

5. Security Considerations

Security is discussed throughout this document. For protocol-specific security considerations, refer to [RFC4016] and [I-D.ietf-pana-pana].

6. IANA Considerations

This document has no actions for IANA.

7. Acknowledgments

We would like to thank Bernard Aboba, Yacine El Mghazli, Randy Turner, Hannes Tschofenig, Lionel Morand, Mark Townsley, Jari Arkko, Pekka Savola, Tom Yu, Joel Halpern, Lakshminath Dondeti, David Black, and IEEE 802.11 Working Group for their valuable comments.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4016] Parthasarathy, M., "Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements", RFC 4016, March 2005.

[I-D.ietf-pana-snmp] Mghazli, Y., "SNMP usage for PAA-EP interface", draft-ietf-pana-snmp-06 (work in progress), June 2006.

[I-D.ietf-pana-pana] Forsberg, D., "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-15 (work in progress), May 2007.

[I-D.ietf-pana-ipsec] Parthasarathy, M., "PANA Enabling IPsec based Access Control", draft-ietf-pana-ipsec-07 (work in progress), July 2005.

[RFC4058] Yegin, A., Ohba, Y., Penno, R., Tsirtsis, G., and C. Wang, "Protocol for Carrying Authentication for Network Access (PANA) Requirements", RFC 4058, May 2005.

[DSL] DSL Forum Architecture and Transport Working Group, "DSL Forum TR-059 DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services", September 2003.

8.2. Informative References

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[802.11i] Institute of Electrical and Electronics Engineers, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements", IEEE Standard 802.11i, 2004.

[3GPP2] 3rd Generation Partnership Project 2, "cdma2000 Wireless IP Network Standard", 3GPP2 P.S0001-B/v2.0, September 2004.

Authors' Addresses

Prakash Jayaraman
Network Equipment Technologies, Inc.
6900 Paseo Padre Parkway
Fremont, CA 94555
USA

Phone: +1 510 574 2305
Email: prakash_jayaraman@net.com

Rafa Marin Lopez
University of Murcia
30071 Murcia
Spain

Email: rafa@dif.um.es

Yoshihiro Ohba
Toshiba America Research, Inc.
1 Telcordia Drive
Piscateway, NJ 08854
USA

Phone: +1 732 699 5365
Email: yohba@tari.toshiba.com

Mohan Parthasarathy
Nokia
313 Fairchild Drive
Mountain View, CA 94043
USA

Phone: +1 408 734 8820
Email: mohanp@sbcglobal.net

Alper E. Yegin
Samsung Advanced Institute of Technology
Istanbul,
Turkey

Phone: +90 533 348 2402
Email: alper.yegin@yegin.org

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).