Study of PANA Architecture and its Applicability on Emerging Network Environments for Secure Network Access

Prof. Er. Dangat G.D[*], Prof. Sayyed S. G[**]

[*] Asst. Prof, Computer Engg Department, K. B. P. College of Engg. & Poly, Satara
[**] Asso. Prof, Computer Engg Department, K. B. P. College of Engg. & Poly, Satara

I. Introduction

Network access authentication is a key procedure for network operator to control user access to the network service. The IETF recently finished its major work in this area by standardizing an IP based protocol named Protocol for Carrying Authentication for Network Access (PANA).

We provide a fruitful analysis of PANA Architecture based on develop IETF Standard deployed on IPv4 and next generation network environments.

II. Literature Survey

Up to the early 2000s there was no standard protocol to transport network access authentication information,. For example

1.Using Point-to-Point Protocol over Ethernet (PPPoE) to implement an authentication protocol, but it complicates the implementation of multicast-based services over PPPoE.

2.In Mobile Internet Protocol version 4 (MIPv4) has an extension to support network access authentication that requires a *foreign agent* in the visited network.

3.In Wi-Fi networks *captive portal*, has been implemented on top of Hypertext Transfer Protocol (HTTP).This variety of choices greatly complicates the management of authentication and network access control

To solve this problem, the Internet Engineering Task Force (IETF), through the PANA Working Group (WG), has developed the Protocol for Carrying Authentication for Network Access (PANA)[2] and an associated architecture [3] to carry network access authentication regardless of the access technology.

III. Objectives and Scope/Limitations of the Present Investigations/Study

1. PANA [2] is an application protocol using the User Datagram Protocol (UDP) as transport, which has been specially conceived by the IETF to carry the Extensible Authentication Protocol (EAP) in order to support different authentication mechanisms for network access, regardless of the underlying network access technology.

2. EAP [4] was standardized by the IETF to provide a flexible authentication framework for network access.

3. Various solutions can be considered as an alternative to PANA. AAA protocols, DHCP, TCP and IKEv2 are considered here as potential alternatives to PANA for EAP transport. AAA protocols such as RADIUS or Diameter (or a subset of them) do not have message formats that satisfactorily meet the requirements (see RFC 4058) for an EAP lower-layer protocol. Some header fields are too large, some too short, some are not present at all, and so on. PANA, designed from scratch with its own message format, matches the EAP transport requirements. EAP over DHCP2 has complexity problems that eliminated it as a candidate for the IETF EAP standard. These include:

4. Difference in messaging direction between EAP and DHCP (e.g., EAP requests and DHCP requests are sent in opposite ways)

5. Difficulty with integrating (stateful) EAP authenticator and stateless DHCP relay agent

IV. Scope

Applicability of PANA

1) On emerging network (IPV4)
2) Next Generation Network
3) Wireless multihop and smart grid
4) Mobile network

V. Limitation

The TCP option for EAP transport adds burdensome redundancy. Its strong reliability functionality is not required. In contrast, by using timers and sequence numbers, PANA fully satisfies the EAP lower-layer protocol requirement on ordered message delivery and the reliability requirement for messages exchanged after the authentication and authorization phase (e.g.,*PANA-Notification-Request* and *PANA-Termination-Request* messages require a response from the communicating peer to complete the notification and session termination operations, respectively). Hence, the lighter weight UDP based PANA transport is also less complex and more efficient. The final alternative here is IKEv2 [9], which is also defined on top of UDP and supports EAP authentication to interwork with AAA. However, IKEv2 mandates a Diffie-Hellman key exchange, which is considered more expensive than other cryptographic operations like the simple hash-based message

authentication code(HMAC) operation specified in RFC 5191 for the PANA SA. Also, an IPSec SA is always created in [9] while it is not required for many access networks. For these reasons, IKEv2 does not replace PANA, which is a more open, flexible and less constrained solution for network access authentication.

VI. Investigation

PANA-related IETF RFCs have been produced. As a consequence of typical pre-analysis within IETF, two informational documents were delivered: one to define the requirements for PANA (RFC 4058) and another (RFC 4016) that analyzes the security requirements and threats for PANA. Based on these initial RFCs, the PANA base specification (RFC 5191) and PANA architecture (RFC 5193) were delivered. The PANA state machine (RFC 5609), which provides a guide for developers to implement PANA, was also submitted. During the development of this initial set of specifications, several features were identified as extensions to the basic protocol functionality and therefore removed from the initial set of specifications for simplicity.

The first extension is the specification of a PAA discovery mechanism used by a PaC to Ascertain the PAA's IP address to be used during a PaC-initiated PANA authentication. RFC 5192 defines such a discovery mechanism using DHCP (v4/v6).

The second extension details the PEMK derivation algorithm (RFC 5807) that is used for Generating cryptographically independent PEMKs for different EPs.

The third extension is the so-called PANA pre-authentication (RFC 5873). The objective of PANA pre-authentication is to reduce EAP authentication latency during handoff in mobile environments.

VII. Research Methodology/ Requirements of the Research Work

We provide a detailed analysis of PANA Architecture based on IETF standards by implementing & deploying on an existing and emerging network environments for Network Access Security for the internet by Carrying Authentication and also describing its applicability to both existing, next generation network, Wireless and Mobile network environments.

VIII. Research Design

1) Designing of EAP authentication framework

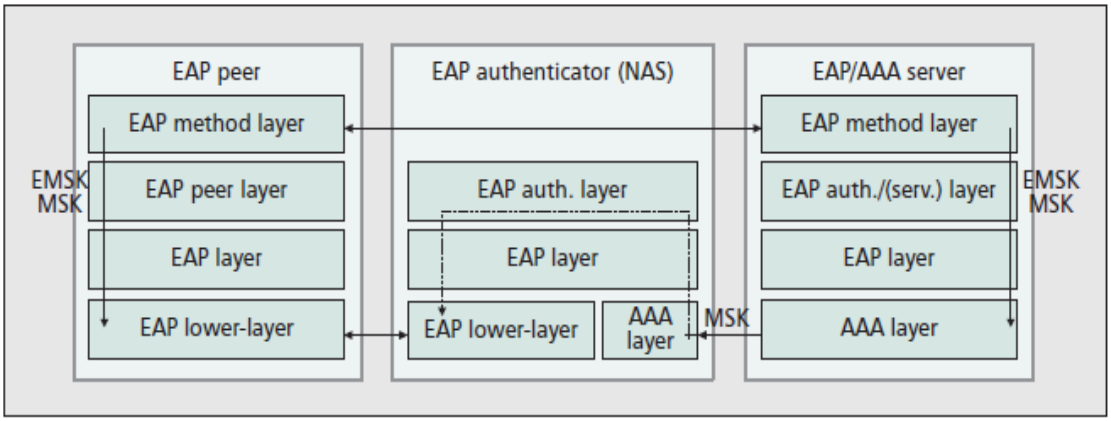

Figure 1. *EAP authentication framework.*

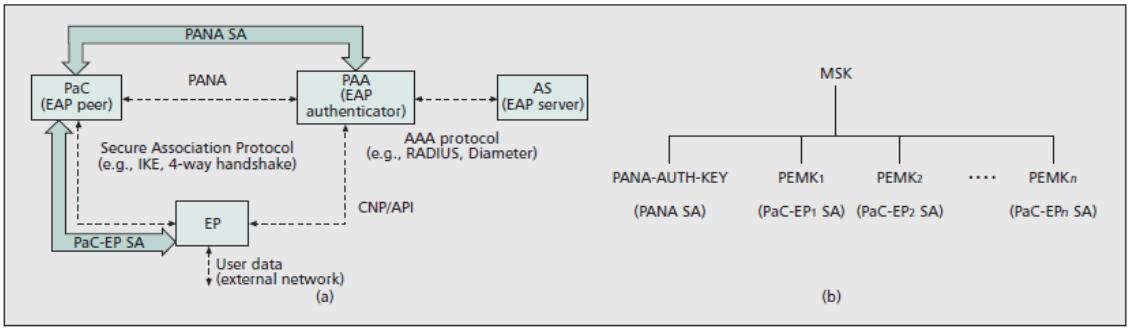

Figure 2. *PANA framework.*

2) Designing of PANA Architecture

a) Designing of PANA Client(PaC)

b) Designing of PANA Agent(PAA)
c) Designing of Enforcement point(EP)
d) Designing of Authentication server(AS)
3) Designing of PANA framework
4) Designing of four Phases
1) Authentication and authorization phase
2) Access phase
3)Re-Authentication phase
4)Termination phase
5)Designing of PANA execution based on EAP-TLS method

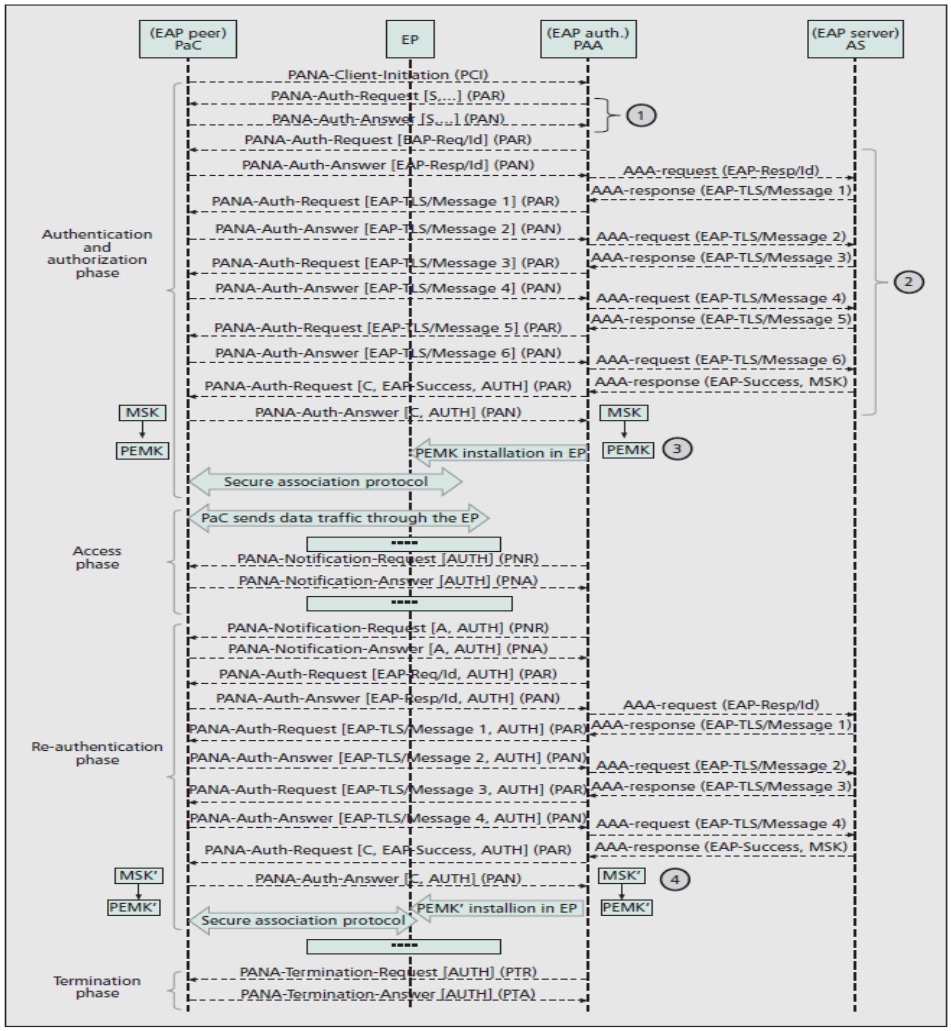

Figure 3. *Example of a typical PANA execution based on the EAP-TLS method.*

IX. Conclusion

We have provided a detail survey of the PANA protocol which is the contribution made by IETF in the field of network access authentication . we have shown the PANA architecture and its associated entities involved in the protocol operation. We have also explained a set of PANA related IETF RFC's produced by the PANA WG.

The basic function of PANA to carry EAP over UDP takes maximum advantage of EAP characteristics of lower – layer independence and authentication method independence. As a result, PANA is gaining interest as a potential candidate for network access authentication in both existing and emerging network scenario.

X. References/Bibliography

Documents	Content
RFC 4016	Associated threat analysis and security requirements for the PANA protocol
RFC 4058	The general requirement of PANA are described
RFC 5191	The PANA base specification is described

RFC 5192	New DHCPv4 and DHCPv6 option are specified. PaC can discover the available PAAs within a network
RFC 5193	The PANA framework and the general architecture are described
RFC 5609	A description of the PaC and PAA
RFC 5807	Specification of the PaC-EP Master Key(PEMK) derivation process for the EP and the PaC using
RFC 5872	Rules for allocating protocol fields in PANA are relaxed
RFC 5873	Extension to the PANA base Protocol to support PANA pre-authentication
RFC 5873	Extension which specifies the PANA Relay Element(PRE) functionality

Table 1: PANA Related IETF RFCs

REFERENCES

[1] M. O'Droma and I. Ganchev, "The Creation of a Ubiquitous Consumer Wireless World Through Strategic ITU-T Standardization," IEEE Commun. Mag., vol. 48 no. 10, Oct. 2010, pp. 158–65.

[2] D. Forsberg et al., "Protocol for Carrying Authentication for Network Access (PANA)," IETF RFC 5191, May 2008.

[3] P. Jayaraman et al., "Protocol for Carrying Authentication for Network Access Framework," IETF RFC 5193, May 2008.

[4] B. Aboba et al., "Extensible Authentication Protocol (EAP)," IETF RFC 3748, June 2004.

[5] C. Rigney et al., "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2865, June 2000.

[6] S. Gordon, "Towards Verification of the PANA Authentication and Authorization Protocol Using Coloured Petri Nets," Proc. 10th Wksp. and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools, Aarthus,Denmark, Oct. 2009, pp. 61–80

[7] P. Calhoun and J. Loughney, "Diameter Base Protoco,"IETF RFC 3588, Sept. 2003Authentication

[8] V. Fajardo, Y. Ohba, and R. Marin-Lopez, "State Machines for Protocol for Carrying for Network Access (PANA)," IETF RFC 5609, Aug. 2009.

[9] C. Rigney et al., "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2865, June 2000.

[10] P. Calhoun and J. Loughney, "Diameter Base Protoco,"IETF RFC 3588, Sept. 2003.

[11] V. Fajardo, Y. Ohba, and R. Marin-Lopez, "State Machines for Protocol for Carrying Authentication for Network Access (PANA)," IETF RFC 5609, Aug. 2009.

[12] C. Kaufman et al., "Internet Key Exchange Protocol Version 2 (IKEv2)," IETF RFC 5996, Sept. 2010.

[13] A. Dutta et al., "Media-Independent Pre-Authentication Supporting Secure Interdomain Handover Optimization,"IEEE Wireless Commun., vol. 15, no. 2, Apr. 2008, pp. 55–64.

[14] "Machine-to-Machine Communications (M2M); Functional Architecture," ETSI Technical Specification 102 690 v. 1.1.1

[15] Rafa Marine Lopez," Network Access Security for the internet : Protocol for Carrying Authentication for Network Access" IEEE Communication Magazine March 2012

AUTHORS

First Author – Prof. Er. Dangat G.D (Asst. Prof), Computer Engg Department, K. B. P. College of Engg. & Poly, Satara, Email: dangat_ganesh@yahoo.com
Second Author – Prof. Sayyed S. G. (Asso. Prof), Computer Engg Department, K. B. P. College of Engg. & Poly, Satara