Internet-Draft Yoshihiro Ohba
(Editor)
Expires: April, 2003 Subir
Das
Basavaraj
Patil
Hesham
Soliman
Alper
Yegin

October 25,
2002

Problem Statement and Usage Scenarios for PANA

<draft-ietf-pana-usage-scenarios-03.txt>

Status of This Memo

Abstract

This document addresses a set of problems which a network layer protocol called PANA (Protocol for carrying Authentication for Network Access) is trying to solve in the area of network access authentication and describes several usage scenarios where PANA is applicable. It also helps to facilitate the discussion for PANA requirements and security threat analysis that are used as basis of actual PANA protocol design.

Table of Contents

1 Introduction

Network access in most cases requires some form of authentication. Generally authentication is performed at the time of link establishment. Authentication for network access is usually tied to the access technology itself. As a result specific authentication schemes are implemented depending on the type of network being accessed. An example would be the use of 802.1x for authenticating to an 802.11 network and PPP authentication in the case of a dial-up connection to an ISP. Authentication for network access may be performed at a higher layer, either IP or at the application layer. This has the advantage of decoupling the association of authentication from the access technology. The assumption here is of course that link layer connectivity is provided by the access network operator.

This I-D discusses various scenarios where a network or higher layer authentication protocol may be deployed.

2. Terminology

Following terminologies are defined for this document. See also [PANAREQ].

Device

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

Device Identifier (DI)

The identifier used by the network as a handle to control and police the network access of a PANA 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.

Enforcement Point (EP)

A node where decisions on per-packet enforcement policy are enforced for devices by using Device Identifier information indicated by a PAA. Per-packet enforcement includes per-packet filtering and may include cryptographic per-packet protection as well.

PANA Client (PaC)

The entity wishing to obtain network access from a PANA authentication agent within a network. A PANA client is associated with a network device and a set of credentials to prove its identity within the scope of PANA.

PANA Authentication Agent (PAA)

The entity whose responsibility is to authenticate the credentials provided by a PANA client and grant network access service to the device associated with the client and identified by a DI.

Access Point

A first-hop L2 attachment point from a PaC device.

Access Router

A first-hop router from a PaC device.

3. Problem Statement

Access networks which are not physically secured from unintended usage usually require clients to go through an authentication and authorization process. Network access authentication of clients require a protocol between the client and the network to execute one or more authentication methods (e.g., CHAP, TLS, SIM, etc.). In the light of proliferation of various access technologies (e.g., GPRS, IEEE 802.11, DSL, etc.), it is important that the authentication methods are not tied to the underlying link-layer. Authentication protocol must be able to carry various authentication methods regardless of the underlying access technologies.

An important aspect of an authentication protocol is the ability to

provide dynamic service provider selection to the clients. Regardless of their network access provider (NAP), clients should be able to select an Internet access provider (ISP) of their choice. This is usually achieved by clients presenting an identifier which carries domain information during the authentication process. For example an

NAI[RFC2486]: john@anyisp.com. The authentication agent in the access network would consult the backend authentication servers in the given domain, and the respective ISP service will be used once access is authorized. This is also essential in providing roaming service to clients. Separation of NAP from ISP, and a single NAP providing service for clients from multiple ISPs are made possible by this feature.

Support for various authentication methods, including the ones that can provide dynamic service provider selection and roaming can be achieved by using an authentication protocol that can carry EAP [RFC2284]. EAP acts as an encapsulation of arbitrary authentication methods, but it still requires a transport between the client and the access network. Among all the link-layers, only IEEE 802 defines how to carry EAP on the link-layer [802.1X]. Any other link-layer has to resort to using PPP/PPPoE [RFC1661,RFC2516] as a link-layer agnostic way of carrying EAP. Inserting this additional layer(s) between the link-layer and network-layer to achieve this goal is an inadequate method. Using PPP just for client authentication incurs extra round-trips, generates overhead of PPP processing for data packets, and forces the network topology into a point-to-point model.

Defining a network-layer transport for EAP would provide a cleaner solution to this problem. Such a solution would not only provide support of various authentication methods, dynamic service provider selection and roaming by carrying EAP, but it will also define a link-layer agnostic carrier for this protocol. This goal will be achieved without having to incur additional costs and limitations of inserting another layer in the stack as in the case of PPP.

Meanwhile, in the absence of such a standard solution, some architectures are forced to design their own ad-hoc solutions to the problem. One such solution is the application-layer authentication method implemented by http redirects and web-based login. In addition to being a non-standard solution, this provides an incomplete network access authentication with well-known vulnerabilities, and therefore regarded as a stop-gap solution.

Another method designed to provide network access authentication is based on overloading an existing network-layer protocol. Mobile IPv4 [RFC3344] protocol has a built-in authentication mechanism. Regardless of whether mobile nodes need to use a foreign agent in an access network, registration via a foreign agent can be required by using an appropriate flag in the agent advertisements. This forces the nodes to register with a foreign agent, and therefore utilizes Mobile IPv4 protocol for network access authentication. Such a solution has very limited applicability as a link-layer agnostic

method since it relies on use of Mobile IPv4 protocol.

4. Usage Scenarios

The first three subsections describe PANA usage scenarios categorized in terms of lower layer security. Other subsections describe scenarios that are not categorized in terms of lower layer security.

4.1. PANA with Physical Layer Security

In the networks where a certain degree of security is provided at physical layer, authenticating the client is still essential since physical layer does not provide information on the client, but per-packet authentication and encryption may not necessarily be provided at higher layers. DSL networks that are implemented on top of point-to-point phone lines are such an example. In this type of networks, PANA is just used for client authentication and a hook to an appropriate access control.

In DSL networks, there are a number of deployment scenarios with regard to client configuration and client authentication. In DSL networks where PPP is used for both configuration and authentication (and IP encapsulation), the providers may not require to migrate to use PANA. On the other hand, there are some DSL networks that use some configuration method other than PPP, i.e., DHCP or static configuration. Those networks use either an ad-hoc network access authentication method such as http-redirect with web-based login or no authentication method at all. A standard, L2 agnostic network access authentication is needed for this type of DSL networks and PANA can be used to fill the demand.

4.2. PANA with Link Layer Security

In certain networks, link layers may be secured by means outside the scope of an authentication protocol. A higher layer authentication protocol in such cases will provide access authorization. For example, web-based login in current Wi-Fi networks. One can enable WEP security to protect the authentication messages. However, it is also possible that the link layer can be secured following a successful authentication by virtue of key exchange or other means.

Wireless data networks such as, CDMA2000 networks require the user/device authentication with the MSC/VLR before providing access to the data network. This authentication which is specific to the technology. Hence the link layer is secured following this authentication.

CDMA2000 networks offer two types of data services namely simple IP and Mobile IP. Simple IP requires the user to provide authentication data via PPP. Radius based AAA is used in the backend to verify the credentials provided by the user before allowing network access. Currently CDMA2000 networks include PPP as part of the protocol stack between the MN and the PDSN (Packet Data serving Node - equivalent to the Access Router), and hence are able to rely on PPP functionality to authenticate a user accessing the data network. However it is possible that future releases of the standard may not use PPP but

adopt simple framing schemes such as HDLC or variants. In such a scenario network access authentication can be done using a protocol such as PANA.

When the MN chooses Mobile IPv4 service, authentication is done by the Foreign agent in the PDSN which interacts with the AAA server. Authentication data as well as the MNs identity, which is the NAI is included in the Mobile IPv4 Registration Request message and the

foreign agent then uses the NAI and the data from the MN-AAA auth extension in the Radius request message. Only after a successful response message from the Radius server is the registration request message forwarded to the home agent. This model is combining an IP mobility scheme with network access authentication. A better approach would be to separate network access and Mobile IPv4. PANA would be used to authenticate the user for network access and Mobile IPv4 messages would be sent after authentication has completed. Such a model would enable different authentication schemes to be supported since EAP is used rather than relying on just HMAC-MD5 which is the default algorithm for the MN-AAA auth extension. Authentication for network access and authentication/authorization for enabling IP Mobility should be separated. This can be accomplished by using PANA for network access while allowing Mobile IP implementations to adhere to the specification [RFC3344].

The IP mobility solution for IPv6 networks is slightly different from the IPv4 networks. When Mobile IPv6 is deployed in such networks, the FA would no longer exist and hence the current scheme used would no longer work. In such a scenario the MN will have to authenticate using another mechanism and PANA is a possible solution.

Since link layer security is enabled as a result of authentication to the MSC/VLR, authentication at an upper layer is an acceptable technique.

4.3. PANA in the Absence of Any Lower Layer Security

Ethernet links composed of legacy hubs and switches and early deployment of Wi-Fi networks (802.11b) do not use link layer authentication or security mechanisms such as, 802.1X. In absence of such lower layer security not only providers are unable to control the unauthorized use of their networks but also users feel insecure while exchanging sensitive information. In order to support authentication functionality in such legacy systems, many providers today use a higher-layer authentication scheme, such as http-redirect commonly known as web-based login. In this method, once the link is established, users' traffic are re-directed to a web server which in turn generates a web-based login forcing users to provide the authentication information. While this method solves the problem partially by allowing only authorized users to access the network it does not enable the lower layer security such as, per-packet authentication and encryption, etc. Moreover, it is a non-standard ad

hoc solution.

In such scenarios, a standard network layer solution such as, PANA is suitable since it provides link-layer agnostic network access authentication. In fact, PANA can provide support of various authentication schemes and also capable of enabling lower layer security. For example, a link can be protected by negotiating encryption keys between PaC and PAA after successful authentication. Although PANA does not define key distribution protocol or mechanism, it is possible to use PANA to enable per-packet protection mechanism such as, IPsec and WEP, to secure communication in the edge subnet. This is achievable if authentication carrier protocol that is used by PANA supports key distribution mechanism. Hence, for legacy networks

where lower layer authentication and key distribution mechanisms are absent PANA could be very useful. So in a way, PANA can help bootstrapping L2 authentication without a pre-shared secret."

4.4. Mobile IP

Mobile IPv4 defines its own authentication extensions to authenticate and authorize mobile nodes at the foreign agents and home agents. One of the possible modes of Mobile IPv4 is when the mobile node uses a co-located care-of address and doesn't rely on any mobility management functionality of the foreign agent on the access network. In this case, mobile node can send its registration request directly to the home agent.

Even in the co-located care-of address case, the protocol has a way to require mobile nodes to register with a foreign agent by setting Registration-Required bit in the agent advertisements. This forces mobile nodes to send their registration requests via foreign agent, and therefore gives the foreign agent a chance to authenticate and authorize the node for network access.

This method can only be used in IPv4 networks where every client implements mobile node functionality. Even for IPv4 clients, a better approach would be to replace this protocol-specific authentication method by a common authentication protocol such as PANA. PANA can be used with any client regardless of Mobile IPv4 support.

PANA can also be used with IPv6 clients, or dual-stack clients. Mobile IPv6 protocol doesn't define a foreign agent in the access networks, therefore it cannot provide any protocol support for access authentication. Network access authentication can be handled by PANA regardless of IP version of the clients and independent of whether they support or use Mobile IP.

4.5. Personal Area Networks

A Personal Area Network would consist of one or more routers connecting one or more hosts to the Internet. Hosts may also communicate directly to each other (e.g. if a shared link is used). Communicating through the mobile router is inefficient and could waste scarce battery power in such device. This should be limited to cases where two hosts do not support the same link layer. It is also important that hosts are authorized to communicate to other hosts in a PAN or gain access to the Internet via the mobile router. Such authentication should be independent of the underlying link layer (e.g. more than one link layer may be used in a PAN), but maybe be

used to bootstrap link layer or IP layer authentication for further communication.

Current cellular systems lack a single authentication mechanism that can be used to allow hosts in a PAN (behind a mobile router) to gain access to other hosts in a PAN or (simultaneously)to the Internet via the mobile router.

The current 3GPP architecture assumes that a split User Equipment

(UE) TE and MT [RFC3314] are possible when PPP is run between them for authentication and access control. If more than one device (e.g. laptop, PDA ...etc) needs to be connected to the MT (typically mobile phone), each one would need to setup a PPP connection to the MT. This is a typical case of a Personal Area Network (PAN) trying to connect to the Internet via 3GPP network. However, this configuration is inefficient; if devices behind the MT need to communicate with each other, they can only do so via the MT. Unless some PPP switching is done in the MT, packets between these devices will need to go over the air interface (WCDMA) and get routed through the network and back to the MT. This adds significant cost as a result of bandwidth inefficiency and battery consumption in the MT. All these issues point towards the need to evolve this architecture towards having a multi-access link between the MT and various TEs. Different multi-access link layers can be utilized for this scenario. A link layer agnostic authentication protocol (PANA) is the main enabler for this scenario, as it would allow hosts connected to the MT to authenticate themselves to the MT (The MT implements an IP stack) and gain access to both, the PAN and the Internet via the MT.

The use of PANA in this scenario would imply that hosts have a PaC function that allows them to authenticate themselves to gain network access. A router on this subnet (i.e. the MT interfacing to the 3GPP network) would contain a PAA server. In this scenario, there would be no need for authorizing devices through consultation with a backend AAA server; pre-configured secrets would suffice for such a small network.

Although IKE (with shared secrets or public keys) can be used for network access authentication in this scenario with some implementation specifics and limitations, it is not designed by nature for network access authentication and would require the use of IPsec tunnel mode for access control, which is not desired in many cases where layer 2 encryption exists. Using a standardized (layer 2 independent) protocol specialized for network access (i.e., PANA) will better fit this scenario.

4.6. Limited Free Access

Certain networks might allow clients to access a limited topology without any explicit authentication and authorization. However, the policy may be such that an access beyond this topology requires authentication and authorization. For example, in an airport network,

information such as, flight arrival and departure gate numbers, airport shops and restaurants, etc., are offered as free services by the airlines or airport authorities for their passengers. In order to access such information, users can simply plug in their devices into the network without performing any authentication. On the other hand, access to further services or sites using such local networks requires authentication and authorization. The access network can detect such an attempt and initiate authentication. Once users perform the authentication it will be allowed to go beyond the free access zone. PANA can be an enabler to such limited free access scenarios since PANA authentication is not performed before IP address configuration and it also allows the network to initiate the authentication whenever appropriate.

4.7. Multiple-Interface Device

A device can have multiple interfaces of homogeneous or heterogeneous technologies. PANA can be used by such a device as a unified higher-layer network access authentication carrier that is independent of the types of the interfaces. There are two possible scenarios for PANA: simultaneous activation and interface switching.

In case of simultaneous activation, the multiple interfaces of a device may be activated at the same time for various requirements such as increased bandwidth, load balancing and reliability.

In case of interface switching, one of the multiple interfaces of a device is activated at a time and the device may switch from one interface to another.

In both cases, each interface may or may not be connected to the same IP subnet. When each interface is connected to a distinct IP subnet, each IP subnet may not be owned by the same service provider, which indicates that the simultaneous activation case is related to host multihoming.

5. Acronyms

AAA: Authentication, Authorization and Accounting

AP: Access Point

AR: Access Router

DSL: Digital Subscriber Line

EAP: Extensible Authentication Protocol

GPRS: General Packet Radio Service

HDLC: High-level Data Link Control

MSC: Mobile Switching Center

MN: Mobile Node

MT: Mobile Termination

NAI: Network Access Identifier

PAA: PANA Authentication Agent

PaC: PANA Client

PPP: Point-to-Point Protocol

TE: Terminal Equipment

UE: User Equipment

VLR: Visiting Location Register

6. Acknowledgments

The authors would like to thank James Carlson, Jacques Caron, Paal Engelstad, Henry Haverinen, Prakash Jayaraman, James Kempf, Thomas Narten, Erik Nordmark, Reinaldo Penno, Phil Roberts, David Spence, Barani Subbiah, George Tsirtsis, Cliff Wang and the rest of the PANA Working Group for the ideas and support they have given to this document.

7. References

[802.1X] IEEE Standard for Local and Metropolitan Area Networks, "Port-Based Network Access Control", IEEE Std 802.1X-2001.

[PANAREQ] R. Penno, et al., "Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology", Internet-Draft, Work in progress.

[RFC1661] W. Simpson, "The Point-to-Point Protocol (PPP)", RFC 1661 (STD 51), July 1994.

[RFC2284] L. Blunk, et al., "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[RFC2486] B. Aboba, et al., "The Network Access Identifier", RFC 2486, January 1999.

[RFC2516] L. Mamakos, et al., "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.

[RFC3314] M. Wasserman et al., "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", RFC 3314, September 2002.

[RFC3344] C. Perkins, "IP Mobility Support for IPv4", RFC 3344, August 2002.

8. Authors' Information

Yoshihiro Ohba
Toshiba America Research, Inc.
P.O. Box 136
Convent Station, NJ 07961-0136

USA
Phone: +1 973 829 5174
Fax: +1 973 829 5601
Email: yohba@tari.toshiba.com

Subir Das
MCC 1D210R, Telcordia Technologies
445 South Street, Morristown, NJ 07960
Phone: +1 973 829 4959

email: subir@research.telcordia.com

Basavaraj Patil
Nokia
6000 Connection Dr.
Irving, TX. 75039
USA
Phone: +1 972-894-6709
Email: Basavaraj.Patil@nokia.com

Hesham Soliman
Ericsson Radio Systems AB
Torshamnsgatan 29,
Kista, Stockholm 16480
Sweden
Phone: +46 8 4046619
Fax: +46 8 4047020
Email: Hesham.Soliman@era.ericsson.se

Alper E. Yegin
DoCoMo USA Labs
181 Metro Drive, Suite 300
San Jose, CA, 95110
USA
Phone: +1 408 451 4743
Email: alper@docomolabs-usa.com