Internet-Draft
Expires: October, 2003

Yoshihiro Ohba (Editor)
TAIS
Subir Das
Telcordia Technologies
Basavaraj Patil
Nokia
Hesham Soliman
Ericsson
Alper Yegin
DoCoMo USA Labs

April 28, 2003

Problem Statement and Usage Scenarios for PANA

<draft-ietf-pana-usage-scenarios-06.txt>

Status of This Memo

Abstract

Network access authentication is a function that is typically required in most scenarios. This is accomplished in most networks via protocols such as PPP, PPPoE, IEEE 802.1X and others. The PANA (Protocol for carrying Authentication for Network Access) WG is considering the network access authentication function being performed at or above the IP layer. This document captures the

various usage scenarios/applicability of a protocol that is used for network access authentication that is at layer-3 or above and additionally identifies the problem being addressed by the WG.

Table of contents

1 Introduction

Networks in most cases require some form of authentication in order to prevent unauthorized access. Only authenticated and authorized clients are able to attach to an access network for sending and receiving IP packets.

There are various mechanisms currently used by networks to prevent unauthorized access. In its simplest form, unintended clients can be physically isolated from the access networks. But there exist some scenarios where a solution based on physical security might not be practical. Public access networks and wireless networks are such

examples. In the absence of physical security (and sometimes in addition to it) a higher layer access authentication mechanism is needed. Link-layer based authentication mechanisms are used whenever they can serve the needs of a particular deployment model. However, not all link-layers support multiple authentication methods or allow independent authentications for the link access and Internet service providers. A higher layer authentication mechanism is needed whenever such additional requirements are not met by the underlying link-layers. Generally a network or higher layer mechanism can be used instead of or in addition to available link-layer and physical security. Currently there is not a standard protocol to perform network access authentication above the link-layer. Instead, a number of ad-hoc and inadequate solutions are being used to overcome the problem. PANA will be developed to fill this gap by defining a network-layer access authentication protocol.

This document discusses the need for a standard network access authentication protocol and covers various usage scenarios where such a protocol is applicable.

2. Acronyms

AAA: Authentication, Authorization and Accounting

DSL: Digital Subscriber Line

EAP: Extensible Authentication Protocol

GPRS: General Packet Radio Service

HDLC: High-level Data Link Control

IKE: Internet Key Exchange

ISP: Internet Service Provider

MSC: Mobile Switching Center

MN: Mobile Node

MT: Mobile Termination

NAI: Network Access Identifier

NAP: Network Access Provider

PPP: Point-to-Point Protocol

PPPoE: PPP over Ethernet

TE: Terminal Equipment

UE: User Equipment

VLR: Visiting Location Register

3. Problem statement

Access networks usually require clients to go through an authentication and authorization process for network access. Network access authentication of clients necessitates a protocol between the client and the network to execute one or more authentication methods (e.g., PAP, CHAP, TLS, SIM, etc.). With the increasing number of the various types of networks being deployed (e.g., GPRS, IEEE 802.11, DSL, etc.), it is important that the authentication methods are not tied to the underlying link-layer (technology specific). An authentication protocol must be able to support various authentication methods regardless of the underlying access technology.

Some deployment scenarios require a separation between a network access provider (NAP) and an Internet service provider (ISP), where the NAP provides physical and link-layer connectivity to an access network it manages, and the ISP provides Internet connectivity for the NAP. An important aspect of network access is the ability to enable dynamic ISP selection during the initial connection process. This is usually achieved by either using link-layer specific selectors during link establishment or by presenting a client

identifier which carries the ISP domain information during the authentication process. An example of such a client identifier would

be the NAI[RFC2486] (e.g., 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 the client access is authorized. This is also essential in providing roaming service to clients. A single authentication between the client and the ISP is generally sufficient for both NAP and ISP access by relying on the pre-established trust relation between the NAP and the ISP. Nevertheless, there are some scenarios where NAPs and ISPs require independent authentication by the client. If the NAP authentication is performed using a link-layer mechanism, ISP authentication can be left to a network-layer mechanism. An example of a multi-layer authentication can be seen in cdma2000 networks as described in section 4.2.

The Extensible Authentication Protocol (EAP) [RFC2284bis] offers a natural way to encapsulate many different authentication methods. Among the various types of link-layers, only IEEE 802 defines how to carry EAP on the link-layer [802.1X]. Other link-layers resort to using PPP/PPPoE [RFC1661,RFC2516] as a link-layer agnostic way of carrying EAP. The ungainly insertion of this extra layer incurs additional round-trips at connection time, generates overhead of PPP processing even for subsequent data packets, and forces the network topology into a point-to-point model. EAP could achieve greater applicability if it could be carried directly over IP. That way, the resulting IP packets could be carried over any link technology without incurring additional cost or limitation on the architectures.

In general terms, PANA will be defined as a network-layer transport for EAP. PANA can be used over any link-layer. The primary purpose of PANA is to authenticate a client to a server for the purpose of network access. Initial client authentication needs to be bound to subsequent traffic to prevent spoofing of data packets and resulting service theft. Therefore, this authentication may be required to generate cryptographic keying material unless presence of a secure physical or link-layer channel is assured a priori. The task of generating and distributing such keying material can be accomplished by various EAP methods. Once the keying material is present, it can be used with link-layer ciphers or IPsec for providing subsequent per-packet authentication. It should be noted that the keying material produced by the authentication methods is generally not readily usable by IPsec. A key exchange protocol like IKE [RFC2409] may be used to create the required IPsec security associations. The mechanisms that are used to turn keying material produced by the initial authentication method into link-layer or network-layer ciphers are outside the scope of PANA protocol.

Until a standard solution like PANA is developed, architectures that use neither IEEE 802 nor PPP as link-layers are forced to design their own ad-hoc mechanisms to address the problem of authentication for network access. One such mechanism 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 is regarded as a stop-gap mechanism.

Another method designed to provide network access authentication is based on overloading an existing network-layer protocol. The 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 for network access authentication. Such a solution has very limited applicability as a link-layer agnostic method since it relies on the deployment of the Mobile IPv4 protocol.

4. Usage scenarios

In this section, the first three subsections describe generic PANA usage scenarios categorized in terms of lower-layer security. The remaining subsections describe specific scenarios for Mobile IP, personal area networks, and limited free access.

4.1. PANA with physical layer security

Even in networks where a certain degree of security is provided at the physical layer, authenticating the client may still be essential if the physical layer does not provide the identity of the client. However, per-packet authentication and encryption may not be necessary. DSL networks that are implemented on top of point-to-point phone lines are such an example. In such networks, PANA can be used for client authentication and be the basis for an appropriate access control mechanism.

In DSL networks, there are a number of deployment models with respect to client configuration and client authentication. In DSL networks where PPP or PPPoE is used for both configuration and authentication, PANA may not be required. On the other hand, there are some DSL networks that use some configuration method other than PPP or PPPoE, i.e., DHCP or static configuration. Such 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, link-layer agnostic network access authentication would be an improvement for this type of network deployments. In addition, the variations in DSL deployment scenarios, particularly the variation in physical topology between the DSL modem and the ISPs edge router, makes it difficult to define a single authentication scheme which operates at the link-layer and works with any physical topology. It is possible that a link-layer agnostic, single network access authentication solution may be required in the future for DSL deployments as long as the variations in deployment topologies are expected to continue.

4.2. PANA with link-layer security

Certain cellular link-layers such as GSM and cdma2000 provide their own authentication mechanisms as well as ciphering of data sent over the radio link. This technology specific authentication enables authorization for link access by the NAP, and can provide per-packet

authentication, integrity and replay protection at the link-layer. In the case where such access networks are used for accessing the Internet via some ISP, it does not provide authorization at the network-layer which can only be done by authenticating the client to an ISP. So, this necessitates another layer of authentication. It should be noted that this second authentication takes place over a secure channel.

cdma2000 is a good example of such an architecture where multi-layered authentication for network access takes place. cdma2000 networks require the user/device to authenticate with the MSC/VLR before providing access to the packet data network. The technology specific access authentication which uses the CAVE (cellular authentication and voice encryption) algorithm also provides cipher keys to the mobile and the base station for securing the link layer for all subsequent voice and data carried on the radio link. In the Simple IP mode of operation in cdma2000 service, the ISP authentication is provided by using CHAP within PPP. In the Mobile IP mode of cdma2000, the Mobile IPv4 protocol supports a challenge/response style authentication. For a high level overview of the cdma2000 architecture refer to [RFC3141].

As the packet data network architecture in cdma2000 evolves, PANA could be supported as a single unifying network-layer authentication mechanism. This would result in the replacement of CHAP authentication via PPP with the added benefit of considering the use of running IP directly over a simplified framing protocol instead of PPP. In the case of Mobile IP mode of operation the need for the challenge response scheme could be deprecated as well as enabling the smooth migration to Mobile IPv6 deployment, the reason being the decoupling of IP mobility from access authentication.

4.3. PANA in the absence of any lower-layer security

There are scenarios where neither physical nor link-layer access control is available on the network. One possible cause of this scenario is due to the lack of adequate client authentication capabilities (i.e., authentication methods) on the link-layer technology being used even when the link-layer has sufficient cipher suite support. It is desirable to support various authentication methods without being limited to the ones that are specific to the underlying technology. Another cause for the lack of lower-layer authentication is due to the difficulty of deployment. For example, physical security is not practical for public access wireless networks.

In the absence of such lower-layer security and authentication mechanism not only are service providers unable to control the unauthorized use of their networks but also end-users feel insecure about using such networks at all. In order to support authentication functionality in such 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 is 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 however does not enable the lower-layer security such as, per-packet authentication and encryption over the radio link. Moreover, it is a non-standard ad hoc solution that provides support for only a limited set of authentication methods.

In such scenarios, a standard mechanism is necessary which can provide network access authentication irrespective of whether the underlying layers are secured or not. A solution like PANA at the network layer may be adequate if it can specify appropriate authentication methods that can derive and distribute keys for authentication, integrity and confidentiality of data traffic either at the link or at the network layer. For example, if link-layer does not support the desired authentication method but supports ciphering, PANA can be used to bootstrap the latter. On the other hand, if link-layer neither supports the desired authentication method nor ciphering, PANA can be used to bootstrap higher layer security protocols, such as, IKE and IPsec. Thus a successful PANA authentication can result in a secured network environment although the underlying layers were not secured to begin with. Also assuming PANA will provide support to various authentication schemes, providers will have the advantage using a single framework across multiple environments.

4.4. Mobile IP

Mobile IPv4 defines its own authentication extensions to authenticate and authorize mobile nodes at the foreign agents and home agents. In the co-located care-of-address mode, the mobile node itself is the tunnel end-point for packets tunneled from the home agent to the mobile. In this mode of operation the mobile does not rely on the existence of a foreign agent in the visited network. In this case, a mobile node can send its registration request directly to the home agent. However 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 the Registration-Required bit in the agent advertisements. This forces mobile nodes to send their registration requests via the foreign agent, even though they do not have to interact with that agent otherwise. The intent of forcing the mobile to register via the foreign agent is primarily driven by the access networks requirement to authenticate mobile nodes before allowing 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 and it can support various authentication methods. PANA can also be used with IPv6-only clients or dual-stack clients. The Mobile IPv6 [MIPv6] protocol doesn't define a foreign agent in the access networks and provide any protocol support for access authentication. PANA can provide the access network authentication in the case of Mobile IPv6.

Network access authentication can be handled by PANA regardless of

the IP version of the clients and independently of whether they support or use Mobile IP.

4.5. Personal area networks

A personal area network (PAN) is the interconnection of devices within the range of an individual person. For example connecting a cellular phone, PDA, and laptop together via short range wired or wireless links would form a PAN.

Devices in a PAN can directly communicate with each other, and access the Internet if any one of them is specifically designated as a mobile router for providing gateway functionality. Just like any access network, a PAN also requires authentication and authorization prior to granting access to its clients. A mobile router can terminate the link-layer from different PAN nodes, and therefore it acts as the first-hop router for them. Additionally, it can also perform access control as an authentication agent. Different nodes might be using different link-layer technologies to connect to a mobile router. Therefore, it is desirable to use authentication methods independent of the underlying link and rely on a link-layer agnostic authentication protocol like PANA to carry authentication information.

Another characteristic of PANs is its small scale. Only a handful of nodes are expected to be part of a given PAN without a need to support roaming in the PAN; therefore the authentication process does not necessarily require a managed backend AAA infrastructure for credential verification. Locally stored information can be used in this kind of PANA deployment without relying on a AAA backend.

The 3GPP architecture allows separation of MT (mobile termination, such as cellular phone) and TE (terminal equipment, such as laptop) [RFC3314]. TE can be connected to the Internet via MT by establishing a PPP connection. One or more TEs can be connected to a MT to form a PAN. The current architecture does not allow direct communication between the TEs (if more than one are connected to the MT) without having to go through the cellular interface of the MT. This architecture will benefit from using shared links (e.g.,

Ethernet) between the TE and MT. Shared links would allow TEs to communicate directly to each other without having to send data through the power-limited MT or over the expensive air interface. PANA can be used for authenticating PAN nodes when shared links are used between the TEs and MT.

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 any 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., is 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. In fact, the network will only offer link-layer connectivity and limited network layer access to users. On the other hand, access to further services or sites using such local networks requires authentication and authorization. If users want such services, the access network can detect that attempt and initiate authentication. This also allows the network to initiate the authentication whenever appropriate. 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 and can offer a flexible access control framework for public access networks.

5. Security considerations

This document identifies the need for a standard network-layer authentication protocol and illustrates a number of possible usage scenarios. The actual protocol design is not specified in this document, neither are the security considerations around it. The scenarios described in this document are used as input to a separate security threats analysis document [SECTHREAT]. Eventually, the requirements are derived from both the scenarios described in this document and also the threats analyzed in the latter document. These requirements are being collected in the [PANAREQ] document.

6. Acknowledgments

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

7. References

7.1. Normative references

[MIPv6] D. Johnson, et al., "Mobility Support in IPv6", (draft-ietf-mobileip-ipv6-21.txt).

[PANAREQ] R. Penno, et al., "Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology" (draft-ietf-pana-requirements-05.txt).

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

[RFC2284bis] L. Blunk, et al., "Extensible Authentication Protocol (EAP)" (draft-ietf-eap-rfc2284bis-02.txt).

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

[SECTHREAT] M. Parthasarathy, "PANA Threat Analysis and security requirements" (draft-ietf-pana-threats-eval-03.txt).

7.2. Informative references

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

[RFC3141] T. Hiller et al., "CDMA2000 Wireless Data Requirements for AAA", RFC 3141, June 2001.

8. Authors' information

Yoshihiro Ohba
Toshiba America Information Systems, Inc.
9740 Irvine Blvd.
Irvine, CA 92618-1697
USA
Phone: +1 949 583 3273
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

9. Intellectual property notices

10. Copyright notice