Blinzler, Andreas

PANA
Problem Statement & Usage Scenarios

Internet Security

Research Paper

Georg – Simon – Ohm

University of Applied Sciences

Department of computer sciences

Contents

1 Introduction

Network access authentication is required in most scenarios, because only authenticated and authorized clients are able to access a network. This is accomplished via protocols like PPP, PPPoE, IEEE 802.1x, etc. So authentication should prevent unauthorized access.

For this various mechanisms are currently used by networks: physical security isolates unintended clients physically from the access network. But there are scenarios where physical security might not be practical (e.g. public access networks, wireless networks); in the absence of physical security a higher layer access authentication mechanism is needed – link-layer authentication mechanisms are used then. But not all link-layers support multiple authentication methods or allow independent authentications. Therefore a higher authentication mechanism is needed; generally a network- or higher-layer mechanism can be used instead or in addition to link-layer security and physical security.

Currently there is no standard protocol to perform network access authentication above the link-layer. Instead some ad-hoc and inadequate solutions are used. For this PANA[1] will be developed to fill this gap. PANA will define a network layer access authentication protocol.

Positioning

The PANA working group is considering network access authentication function being performed at or above the network layer. So PANA will be defined to perform network access at the IP-layer.

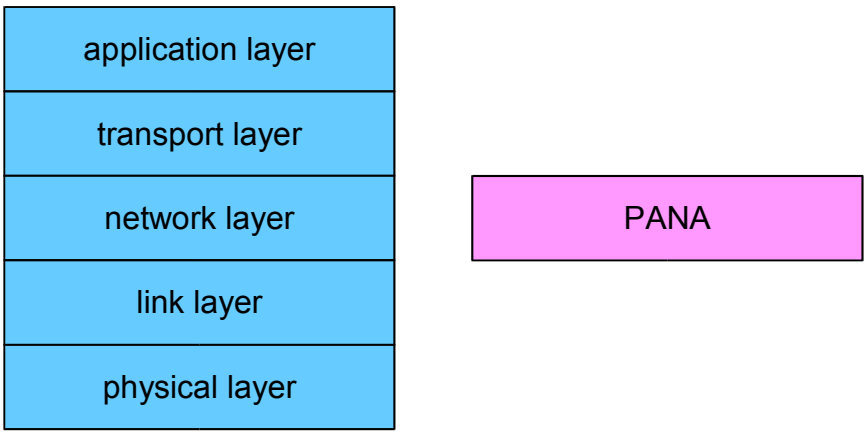

Illustration 1: Positioning of PANA (OSI layer model)

1 Protocol for carrying Authentication for Network Access

2 Problem statement

2.1 Introduction to PANA

Clients have to go through an authentication and authorization process for network access. For that PANA should be used. PANA is not a usual protocol for network access, it will provide this protocol. PANA is a protocol between a terminal and a network.
For instance if several authentication methods are used parallel, there would be an assembly of methods with the same aim. PANA will reduce this, by putting there a standard protocol for network authentication. This protocol must execute one or more authentication methods like PAP, CHAP, TLS, SIM, etc. It is important that the authentication methods are not technology specific, that means tied to the underlying link-layer (e.g. GPRS, IEEE 802.11, DSL, etc.). So this authentication protocol must be able to support various authentication methods regardless of the underlying access technology.

2.2 Separation between NAP and ISP

Some deployment scenarios require a separation between a NAP[2] and ISP[3]. The NAP provides physical and link-layer connectivity for an access network, which is managed by the NAP. The ISP provides Internet connectivity for the NAP.
The dynamical selection of the ISP is an important aspect of network access. This is usually achieved by using link-layer specific selectors during link-establishment or by presenting a client identifier, which carries the ISP domain information during the authentication process (e.g Network Access Identifier [RFC2486]). The authentication agent in the access network would consult the backend authentication server in the given domain, and the respective ISP service will be used once the client is authorized.
So there are two authentication possibilities:

1. 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.

2 Network Access Provider
3 Internet Service Provider

2. Nevertheless there are scenarios where NAP and ISP require independent authentication by the client. The NAP authentication is realized with a link-layer mechanism, the ISP authentication is left to network layer mechanisms. An example of such a multi-layered authentication can be seen in CDMA2000[4] networks as described in chapter 3.2.

2.3 EAP

As mentioned above, PANA will provide an authentication protocol for network access. The EAP[5] is this earlier mentioned protocol. EAP encapsulated many different authentication methods. Among the various types of link-layers, only IEEE 802 defines how to carry EAP on the link-layer (IEEE 802.1x). Other link-layers have to use PPP or PPPoE [RFC1661, RFC2516] to carry EAP on the link-layer. For it an extra layer is inserted – with consequences: additional round trips at connection time; overhead of PPP processing is generated, even for subsequent packages; a network model is forced into a point-to-point model. Because IP-packets could be carried over any link-layer technology without incurring additional cost or limitation on the architecture, it is much better to carry EAP directly over IP. In this manner EAP could achieve greater applicability.

2.4 Client authentication with PANA

The primary purpose of PANA is to authenticate a client to a server for network access. This can be managed by bounding the initial client authentication 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 a secure physical or link-layer channel is present and assured a priori. This cryptographic keying material can be generated and distributed by the EAP methods. The key can be used with link-layer ciphers or IPSec for providing this pre-packet authentication. But the generated keys can not generally be readily used with IPSec, therefore a key exchange protocol like IKE [RFC2409] may be used.

4 Code Division Multiple Access
5 Extensible Authentication Protocol

2.5 Ad-hoc mechanisms

Until PANA is developed, architectures that use neither IEEE 802 nor PPP as link-layers are forced to design their own ad-hoc authentication mechanisms to solve the problem of authentication for network access.

Application-layer authentication method
This method is implemented by *HTTP-redirects with web-based login*. It is a non-standard solution that provides incomplete network access authentication with well-known vulnerabilities. Such a solution is regarded as a stop-gap mechanism.

Overload of an existing network layer protocol
The Mobile IPv4 [RFC3344] protocol for instance has a built-in authentication mechanism. The mobile nodes are forced to register with a foreign agent. In this manner network access authentication with Mobile IPv4 can be achieved. Such a solution has very limited applicability as a link-layer agnostic method since it relies on the deployment of the Mobile IPv4 protocol.

3 Usage scenarios

3.1 PANA with physical layer security

Even in networks with physical layer security client authentication may still be essential, because the physical layer does not provide the identity of the client.
In DSL networks for instance there are a lot deployment models. These variations in DSL deployment models make it difficult to define a single authentication scheme that would operate at the link-layer and works with any physical topology. But a 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. So PANA can be used for client authentication. PANA would build the basis for an appropriate access control mechanism.

3.2 PANA with link-layer security

Certain cellular link-layers (GSM[6] and CDMA2000) provide their own authentication mechanism and ciphering of data. This technology specific authentication enables authorization for link access by the NAP. In addition to that it can provide per-packet authentication, integrity and replay protection at the link-layer. When such networks are used for accessing the Internet via some ISP, authentication has to be done by authenticating the client at the network layer. Such networks do not provide authorization at the network layer. That is why another layer of authentication is needed (multi-layered authentication).

CDMA2000 is a good example where multi-layered authentication takes place for network access. In CDMA2000 networks the user or device is required to authenticate with the MSC[7]/VLR[8] before providing access to the network. For it CDMA2000 has its own authentication mechanism. This mechanism uses the cellular authentication and voice encryption (CAVE) algorithm and provides cipher keys to the mobile and the base station. In this manner the link-layer should be secured for all subsequent voice and data traffic carried on the radio link.

CDMA2000 knows two modes of operation: in the Simple IP mode the ISP authentication is provided by using CHAP within PPP; the Mobile IP mode supports a challenge/response style authentication.

Because CDMA2000 is a packet data network, 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 benefit of the use of running IP directly over a simplified framing protocol instead of PPP (Simple IP mode). In the case of the Mobile IP mode, the need of the challenge/response style authentication scheme can be deprecated, too.

3.3 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. This can either due to the lack of adequate client authentication capabilities on the link-layer technology or to the difficulty of deployment, physical security is not practical for public access wireless networks. The absence of lower layer security and authentication mechanisms means that service

6 Global System for Mobile communication
7 Mobile Switching Center
8 Visiting Location Register

providers are unable to control the unauthorized use of their networks and that the end users feel insecure about using such networks. To support authentication functionality in such systems many providers use today a higher layer authentication scheme, such as *HTTP-redirect with web-based login*. In this method, once the link is established the users' traffic is re-directed to a web-server. This server generates a web-based login forcing the user to provide his or her authentication information. This method solves the problem partially, because on the one hand only authorized users are allowed to access the network, but on the other it does not enable the lower layer security over the radio link (per-packet authentication and encryption). Moreover this method is a non-standard ad-hoc solution; it provides only support for a limited set of authentication methods.
In such scenarios a standard mechanism is necessary that provide network access authentication irrespective of whether the underlying layers are secured or not. Such a solution would be PANA at the network layer. PANA can specify appropriate authentication methods, which derive and distribute keys for authentication, integrity and confidentiality of data traffic either at the link-layer or at the network layer. For example if the link-layer does not support the desired authentication method but support ciphering, PANA can be used to bootstrap the latter or, if the 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.
So a successful PANA authentication can result in a secured network environment although the underlying layers are not secured. In addition to that PANA will provide support to various authentication schemes and providers can use a single framework across multiple environments.

3.4 Mobile IP

Mobile IPv4 defines its own authentication mechanisms, which authenticate and authorize mobile nodes at the foreign and home agents.
The mobile node has a permanent home address. In the case that the mobile node is not on the home network, it notifies a router on the home network called the home agent (HA). The home agent has to forward the packages to it's new address, called its *co-located care of address* at the foreign network. The router at the foreign network, the foreign agent (FA), is allowed to receive and to send packages on behalf of the mobile node. The foreign agent has the correct address, while the mobile node retains its incorrect home address. In the case that the mobile node is on the home network, it sends and receives packets directly at its home agent. But the protocol can force mobile nodes to re-

gister with a foreign agent by setting the r*egistration required* bit in the agent advertisements. Mobile nodes send their registration requests via the foreign agent even though they do not have to interact with that agent otherwise. The intent for this is the requirement of access networks: only authenticated mobile nodes are allowed to access the network.

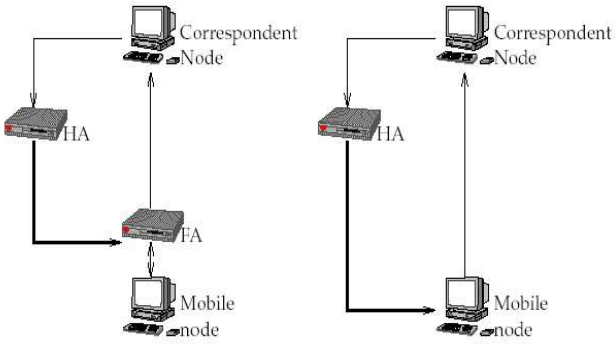

Illustration 2: Mode of operation: mobile node not on home network (left), mobile node on home network (right)

This method can only be used in IPv4 networks. So every client implements mobile node functionality. It would be better to replace this protocol specific authentication method by a common authentication protocol such as PANA. PANA could be used with any client, regardless of Mobile IPv4 support or not. Also PANA could support various authentication methods and could be used with IPv6 only or dual-stack clients.
So 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.

3.5 PAN

A PAN[9] is the interconnection of devices within the range of an individual person. For example the short wired or wireless connection between a cellular phone, PDA and Laptop would form a PAN.

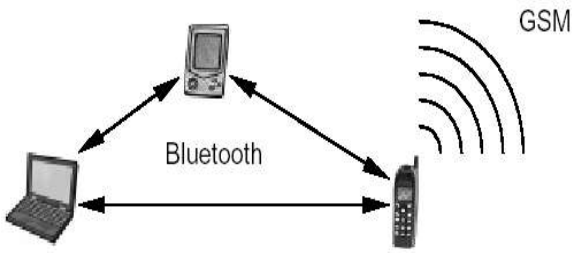

Illustration 3: PAN

9 Personal Area Network

The devices can directly communicate with each other and access the Internet, if anyone of them is designated as a mobile router for providing gateway functionality. Just like any access network a PAN also requires authentication and authorization. The mobile router can terminate the link from different PAN nodes, so it acts like a first-hop router and can perform access control as an authentication agent.

Different nodes for instance might be using different link-layer technologies to the mobile station. That is why 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 a PAN is its small scale. So there is no need of roaming support. Further their authentication process does not necessarily require a managed backend AAA[10] infrastructure for verification. Locally stored information can be used in this kind of PANA deployment without relying on an AAA backend.

An example for this is the 3GPP architecture. The 3GPP architecture allows a separation of the MT[11] and TE[12]. A TE can be connected to the Internet via a MT by establishing a PPP connection. One or more TEs can be connected to a MT to form a PAN. Currently no direct communication between the TEs is possible. They have to go through the cellular interface of the MT. A solution to this limitation could be the use of shared links, like Ethernet, between a TE and MT. Shared links would allow TEs to communicate directly with each other and PANA can be used for authenticating the PAN nodes.

3.6 Limited free access

Certain networks might allow clients to access a limited topology without any explicit authentication and authorization. An airport network could be an example for such networks. Informations such as departure gateways, flight schedules, etc. are offered as free services by the airlines. To access such information users can simply plug-in their devices into the network without performing any authentication.

The network will only offer link-layer connectivity and limited network access to users. The access to further services and sites using such local networks requires authentication and authorization. If users want such services the access network detects that attempt and initiate authentication. Have

10 Authentication, Authorization and Accounting
11 Mobile Termination
12 Terminal Equipment

users performed the authentication they are allowed to go beyond the free access zone. PANA can be used in this scenario as an enabler to such limited free access scenarios and can offer a flexible access control framework for public access networks.

4 Conclusion

To put it in a nutshell there are two reasons for using PANA. When the link-layer do not have an authentication mechanism a higher layer authentication mechanism is needed as described above. Additionally PANA defines the authentication protocol EAP. But not all link-layers support carrying EAP. Assuming every link-layer will sometimes define how to carry EAP is not realistic and using PPP authentication for shared media is inefficient as shown above. So PANA can be used to carry EAP directly over IP to achieve greater applicability

When the link-layer provides an authentication mechanism a higher layer authentication mechanism is also needed. Multi-layered authentication as mentioned in the chapters about the separation between the NAP and ISP and CDMA2000 networks is a good example for that. Therefore network or higher layer authentication mechanisms can be used instead or in addition to physical security and link-layer security. But a common higher layer authentication carrier protocol needs to be standardized. Web-based authentication for example is widely used in hot-spot networks, but it is known to be proprietary hack.

As a concluding remark it can be said that PANA as a standardized protocol can achieve network access authentication at or above the network layer and is consequently not tied to the underlying link. So PANA is applicable in various scenarios like Mobile IP networks , PANs and limited scope networks.

A Acronyms

AAA	Authentication, Authorization and Accounting
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
GPRS	General Packet Radio Service
IKE	Internet Key Exchange
ISP	Internet Service Provider
MSC	Mobile Switching Center
MT	Mobile Termination
NAP	Network Access Provider
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
TE	Terminal Equipment
VLR	Visiting Location Register
PANA	Protocol for carrying Authentication for Network Access
IP	Internet Protocol
PAN	Personal Area Network
OSI	Open System Interconnection
PAP	Password Authentication Protocol
CHAP	Challenge Handshake Authentication Protocol
TLS	Transport Layer Security
CDMA	Code Division Multiple Access
RFC	Request For Comments
HTTP	Hypertext Transfer Protocol
3GPP	3rd Generation Partnership Project

B References

[PANA006] **Problem Statement and Usage Scenarios for PANA**
Y. Ohba (Editor), April 2003
draft-ietf-pana-usage-scenarios-06.txt

[TANNE03] **Computer Networks**
Andrew S. Tannenbaum
Pearson Education, Inc., 4th Edition, 2003

[EIZEN04] **Mobile Radio GSM Introduction**
Prof. Dr. Eizenhöfer
Lecture script *FWPF Mobilfunk* summer semester 2004

[RFC2486] **The Network Access Identifier**
B. Aboda, et. al., January 1999

[RFC1661] **The Point-to-Point Protocol (PPP)**
W. Simpson, July 1994

[RFC2516] **A Method for Transmitting PPP over Ethernet (PPPoE)**
L. Mamakos, et. al., February 1999

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

[RFC3344] **IP Mobility Support for IPv4**
C. Perkins, August 2002