RADEXT
Internet-Draft
Expires: April 27, 2006

J. Arkko
Ericsson
P. Eronen
Nokia
J. Korhonen
Teliasonera

October 24, 2005

Policy Decisions for Users with Access to Multiple Services
draft-arkko-radext-multi-service-decisions-02

Status of this Memo

Copyright Notice

Abstract

This draft relates to the use of Authentication, Authorization, and Accounting (AAA) where the same user credentials can be used on many different types of devices, ranging from wireless access points to Virtual Private Network (VPN) gateways. This draft discusses how to use existing AAA and authentication protocols and extensions to

determine what service was provided, agree about this among all the participating parties, and use this information as a basis for policy decisions.

Table of Contents

1. Introduction

This draft relates to the use of Authentication, Authorization, and Accounting (AAA) where the same user credentials can be used on many different types of devices, ranging from wireless access points to virtual network gateways. For instance, a user may have credentials that can be used in the Extensible Authentication Protocol (EAP) [6]. Such credentials could be used to access a 802.11 Wireless LAN, 802.16 networks, PANA-based DSL [8], or to gain VPN access via a gateway that supports IKEv2 [7].

Among other things, this draft discusses how AAA servers can determine what service was provided. This is important in some situations where, for policy reasons, the type of the service needs to be known. Such policy may be based on, for instance, commercial or security considerations.

For example, the AAA server may wish to deny 802.1X wireless LAN access from a service for a specific subscriber, but allow the same subscriber to use IKEv2-based VPNs. The attributes discussed in this document will provide this information to the AAA server. The AAA server uses this information at the moment of the authorization decision, and once this decision is taken, the rest of the exchange is not affected.

Similarly, it can be useful to ensure that the client, NAS, and AAA server all know what service was provided, or even ensure that the client knows the NAS has provided a service that the AAA server has authorized.

Earlier work in this space includes [11], [12], and [10] to which this work is in debt.

2. Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "OPTIONAL", "RECOMMENDED", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [1].

3. Policy Decisions

Security-related policies can be required when potential service types have different perceived security levels. For instance, network access using a particular link layer type might be considered insecure, while other link layer types or VPN access would be secure.

A more subtle need knowledge about the provided service relates to possibility of compromised nodes. In a large distributed network it is often desirable that the compromise of a single node does not affect other nodes. For instance, it would be desirable that a compromised 802.11 access point can not be turned into a company VPN gateway.

An example of a business-related policy is a subscription that applies only to a particular type of an access.

4. Deployment Considerations in a Roaming Setting

AAA servers may have full knowledge of what services specific NASes offer. For instance, a AAA server may know that a NAS with one address and a shared secret is a Wireless LAN access point, and another NAS with a different address and secret is a VPN gateway. This information can be configured in the AAA server and used for making policy decisions.

Generally, such configuration is, however, infeasible in a roaming setting, due to the large number of potential NASes and the different organizations involved. (There can be some situations where this is still possible even with roaming. For instance, if the roaming network provides only Wireless LAN access, and the operator's own device provides VPN access then it is always possible to distinguish the two.)

Due to these problems, we typically rely on information transferred in the AAA protocols to make policy decisions. For instance, many service parameters (interface speed, type) are carried in the protocols and an informed decision is possible. Nevertheless, as discussed in [10], such information is vulnerable to lying NASes.

5. Ensuring Parties Have the Same Information

Where EAP is used, [10] can provide a channel that ensures the NAS has provided the same information to the client and the AAA server.

This solution requires support from EAP methods. As a result, it may not always apply, if an EAP method that does not support it is used. While the specification supports most popular EAP methods, no deployment of this solution is known to date.

6. Determining the Type of Service

6.1. Service-Type Attribute

This attribute represents the highest level of service provided by a NAS. The current allocation is shown below:

1	Login
2	Framed
3	Callback Login
4	Callback Framed
5	Outbound
6	Administrative
7	NAS Prompt
8	Authenticate Only
9	Callback NAS Prompt
10	Call Check
11	Callback Administrative
12	Voice
13	Fax
14	Modem Relay
15	IAPP-Register [IEEE 802.11f]
16	IAPP-AP-Check [IEEE 802.11f]
17	Authorize Only [RFC3576]

Most current network access falls under the "2 - Framed" value. New values could be allocated, but generally it is more appropriate to allocate new NAS-Port-Type values than a complete new Service-Type value. It is also expected that implementations may deal with Service-Type attribute in a special way, so changes to this attribute would lead to code impacts.

6.2. NAS-Port-Type Attribute

The current assignment of NAS-Port-Type values is shown below:

```
 0  Async
 1  Sync
 2  ISDN Sync
 3  ISDN Async V.120
 4  ISDN Async V.110
 5  Virtual
 6  PIAFS
 7  HDLC Clear Channel
 8  X.25
 9  X.75
10  G.3 Fax
11  SDSL - Symmetric DSL
12  ADSL-CAP - Asymmetric DSL, Carrierless Amplitude Phase
    Modulation
13  ADSL-DMT - Asymmetric DSL, Discrete Multi-Tone
14  IDSL - ISDN Digital Subscriber Line
15  Ethernet
16  xDSL - Digital Subscriber Line of unknown type
17  Cable
18  Wireless - Other
19  Wireless - IEEE 802.11
20  Token-Ring
21  FDDI
22  Wireless - CDMA2000
23  Wireless - UMTS
24  Wireless - 1X-EV
25  IAPP
26  FTTP - Fiber to the Premises
```

This attribute can in general distinguish a number of different physical port types, for instance between 802.11 Wireless LANs (value 19) and Token Ring (20) [4]. New port types can be allocated easily as new access technologies come into use.

Distinguishing different virtual ports is not possible, however. This is because just one value (5 - Virtual) has been allocated for them.

Some additional values have also been suggested in [13]:

```
30        PPPoA (PPP over ATM [RFC3336])
31        PPPoEoA (PPP over Ethernet [RFC2516] over ATM)
32        PPPoEoE (PPP over Ethernet [RFC2516] over Ethernet
33        PPPoEoVLAN (PPP over Ethernet [RFC2516] over VLAN)
34        PPPoEoQinQ (PPP over Ethernet [RFC2516] over IEEE
          802.1QinQ)
38        IPSEC [RFC2411]
```

6.3. Tunnel-Type and Tunnel-Medium-Type Attributes

Tunnel attributes defined in RFC 2868 [3] make it possible to distinguish between different types of tunnel types and media over which the tunnel is run. The current tunnel types are:

1	Point-to-Point Tunneling Protocol (PPTP)
2	Layer Two Forwarding (L2F)
3	Layer Two Tunneling Protocol (L2TP)
4	Ascend Tunnel Management Protocol (ATMP)
5	Virtual Tunneling Protocol (VTP)
6	IP Authentication Header in the Tunnel-mode (AH)
7	IP-in-IP Encapsulation (IP-IP)
8	Minimal IP-in-IP Encapsulation (MIN-IP-IP)
9	IP Encapsulating Security Payload in the Tunnel-mode (ESP)
10	Generic Route Encapsulation (GRE)
11	Bay Dial Virtual Services (DVS)
12	IP-in-IP Tunneling
13	Virtual LANs (VLAN) [RFC3580]

And the medium types are:

1	IPv4 (IP version 4)
2	IPv6 (IP version 6)
3	NSAP
4	HDLC (8-bit multidrop)
5	BBN 1822
6	802 (includes all 802 media plus Ethernet "canonical format")
7	E.163 (POTS)
8	E.164 (SMDS, Frame Relay, ATM)
9	F.69 (Telex)
10	X.121 (X.25, Frame Relay)
11	IPX
12	Appletalk
13	Decnet IV
14	Banyan Vines
15	E.164 with NSAP format subaddress

Together with the NAS-Port-Type attribute, these attributes make it possible to distinguish, for instance, between IPsec- and L2TP-based tunnels. Furthermore, it is possible to separate the medium over which the tunnel runs from the tunnel itself. These attributes are today primarily used to control mandatory tunneling from a NAS (i.e., from NAS to somewhere else, not between NAS and the client).

Note that the role of the tunnel (incoming or outgoing) is not

explicitly communicated. If this information is needed, it can be recovered by comparing the NAS-IP-Address attribute to the Tunnel-Client-Endpoint and Tunnel-Server-Endpoint addresses. This comparison assumes, however, that the addressing domains are the same, which may not always be the case. For instance, a typical VPN gateway would provide a Tunnel-Server-Endpoint of its public IP address and a NAS-IP-Address of its internal network interface.

Similarly, if the NAS needs both types of tunnels simultaneously, the attributes can not distinguish between them. For instance, if a NAS has terminated an IPsec tunnel, the AAA server can not request it to create another mandatory tunnel to another location. This is because the NAS would interpret such request (in Access-Accept) as a rejection of its incoming IPsec tunnel. This prevents, for instance, the use of a AAA server to control which VLAN an incoming VPN users should be directed to.

Another limitation is that RFC 2868 attributes do not explicitly distinguish between different key management mechanisms for tunnels. We do not know, however, to how large extent other than the default key management mechanisms are being employed. For instance, it seems fairly safe to assume that either IKEv1 [9] or IKEv2 [7] is used to key IPsec-based VPNs. Other alternatives do exist, however.

6.4. Discussion

As long as a suitable NAS-Port-Type value exists, it can be reliably be used to determine the type of the service. What remains is distinguishing different virtual services from each other. Both NAS-Port-Type value additions (see [13] and tunnel attribute approaches have been suggested.

One open issue is whether the proposed NAS-Port-Type value "IPsec" should be used instead of "Virtual" when using an IPsec-based virtual service. Another question is under what assumptions the tunnel attribute support is sufficient when both incoming and outgoing tunnels are considered.

7. Recommendations

It is suggested that new physical interface types lead to the allocation of new NAS-Port-Type values.

New higher-layer network access mechanisms, such as PANA, can acquire either a new NAS-Port-Type value or new Tunnel-Type value. In the former case, however, existing DSL or Ethernet port type allocations are not used. This would also create an additional need to have combinations represented in the port types, e.g., PANA over Ethernet and PANA over DSL. As a result, it is recommended that a new Tunnel-Type value, or another similar attribute be used for that purpose. (Intuitively, PANA is not a "tunnel". The question of whether PANA and other "layer 2.5" solutions should be categorized as tunnels deserves some discussion.)

Existing RFC 2868 attributes are sufficient for some situations, but not all. We have not determined whether the remaining cases are important enough to need specific support. If such support would be needed, one option would be to provide additional distinguishing tunnel attributes, such as tunnel role. Another approach would be to provide an independent attribute model.

A common scenario is where both physical (e.g., 802.11) access and a VPN service is being deployed using the same credential. One approach for distinguishing these two in an AAA transaction is to use the values NAS-Port-Type = 5 (Virtual) or NAS-Port-Type = 38 (IPSEC) to represent a VPN service, and all other values to represent a physical access. Value 38 is currently not defined in any RFC or even active draft, and hence only value 5 would be a practical choice. However, this approach is not guaranteed to operate correctly when types of services are being developed.

It has been suggested that this approach could in addition use of tunnel attributes, but this is not recommended due the overloading of their semantics for both incoming and outgoing tunnels.

8. Security Considerations

Security is one of the reasons for attempting to carry information about the type of provided virtual service to the AAA servers, as discussed in Section 1.

This draft does not add any new protocol mechanisms, and as such it does not add new security issues beyond those that already exist for general AAA usage. See [2] and [5] for further discussion.

Note that while providing information from a NAS to a AAA server helps enforce policies, it is unable to deal with rogue NASes, as there is no way forgeries by legitimate (but turned rogue) NASes can be detected. Where EAP is used for authentication, the end-to-end secure channel between the EAP peer and the EAP server can help ensure that all parties at least agree on what the provided service was [10]. That is, the NAS would be forced to tell the same information both to the peer and the AAA server.

9. References

9.1. Normative References

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

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

[3] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[4] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

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

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

[7] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-17 (work in progress), October 2004.

[8] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-05 (work in progress), July 2004.

9.2. Informative References

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

[10] Arkko, J. and P. Eronen, "Authenticated Service Identities for the Extensible Authentication Protocol (EAP)", draft-arkko-eap-service-identity-auth-00 (work in progress), April 2004.

[11] Mariblanca, D., "EAP lower layer attributes for AAA protocols", draft-mariblanca-aaa-eap-lla-01 (work in progress), June 2004.

[12] Lebovitz, G., "EAP lower layer attributes for AAA protocols", draft-lebovitz-ipsec-scalable-ikev2cp-00.txt (unpublished)

(work in progress), March 2003.

[13] Zorn, G., "Additional Values for the NAS-Port-Type Attribute", draft-zorn-radius-port-type-00 (work in progress), February 2005.

Appendix A. Contributors

Glen Zorn and David Mariblanca were members of our team, and contributed greatly to the discussions.

Appendix B. Acknowledgements

We would like to thank Jouni Korhonen, Dave Nelson, and Bernard Aboba for interesting discussions in this problem space.

Authors' Addresses

Jari Arkko
Ericsson
Jorvas FI-02420
Finland

Email: jari.arkko@ericsson.com

Pasi Eronen
Nokia Research Center
P.O. Box 407
FI-00045 Nokia Group
Finland

Email: pasi.eronen@nokia.com

Jouni Korhonen
Teliasonera Corporation
P.O. Box 970
FI-00051 Sonera
Finland

Email: jouni.korhonen@teliasonera.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.