3GPP TSG-SA3 Meeting #28 ***Tdoc S3-030299***
Berlin, Germany 6th-9th May, 2003

Title:	LS on the specification of 802.11i and WPA link layer security and Radius to Diameter interworking
Response to:	S2-031510 Security in WLAN and 3G interworking
Release:	Rel-6
Work Item:	WLAN Interworking Security
Source:	SA3
To:	SA2
Cc:	

Contact Person:

Name:	Colin Blanchard
Tel. Number:	+44 1473 605353
E-mail Address:	colin.blanchard@bt.com

Attachments: S3-030265 Co-Existence of RADIUS and Diameter

1. Overall Description

SA3 would like to thank SA2 for their response regarding the specification of 802.11i and WPA link layer security. It was SA3 original working assumption that we should be able treat these aspects as a "black box" and just provide support for mutual authentication and generation of keying material in line with the requirements set out in the SA2 response. However, SA3 note the comment by SA2 "As well as protecting the WLAN air interface, the above techniques can be used to build support for non-repudiation of WLAN accounting records". In addition, SA3 have also been considering the implications of the trust relation between the Cellular Operator and the WLAN Access Provider and the impact of this on the WLAN Interworking Security TS 33.234. Until this work is complete, SA3 are unable to confirm that the WPA defined encryption meets the security requirements for WLAN-3GPP inter-working.

On the issue of Radius to Diameter interworking, SA3 has been studying the security implications. A contribution (S3-030265 Co-Existence of RADIUS and Diameter) which makes a number of **recommendations which were endorsed by SA3**, is attached, for consideration by SA2.

2. Actions

SA2 to comment on the recommendations in (S3-030265 Co-Existence of RADIUS and Diameter)

3. Dates of Next TSG SA WG3 Meetings:

Meeting	Date	Location
SA3#29	15-18 July 2003	San Francisco, USA
SA3#30	7-10 October	Europe (TBA)

	2003	

3GPP TSG SA WG3 Security — S3#28
6 - 9 May 2003,
Berlin, Germany

Tdoc ⌘S3-030265

~~**Jorvas, FI**~~

Source: Ericsson

Title: Co-Existence of RADIUS and Diameter

Document for: Discussion

Agenda Item: T.B.D

Abstract

This paper presents ~~major~~ the differences between Diameter and ~~Radius~~RADIUS protocols, and discusses ~~finally how suitable the protocols are for~~for the use of these protocols in WLAN inter-working in 3GPP in an interoperable manner. We also discuss the security-related impacts of this, as well as the status of, e.g., EAP support in both of these protocols in IETF.

~~Appendix A~~1. Introduction

Diameter [DIAMETER] and ~~Radius~~RADIUS [RADIUS] protocols define a framework for carrying authentication, authorization and accounting information between the Network Access Server (NAS) and Authentication Server (AAA Server). This discussion paper presents the ~~major~~ differences between the~~o~~se protocols ~~and is an initial point to evaluate protocols against the 3GPP requirements~~ and discusses the transition of the network from one protocol to the other. The transition mechanism is based on ~~the~~ IETF~~'s~~ standard-track proposals.

~~The Radius~~RADIUS is a client-server protocol, while Diameter is based on a peer-to-peer model. Therefore, it is difficult, e.g., to implement server initiated messages in ~~Radius~~RADIUS without extensions to the protocol. ~~On the other hand~~Also, ~~some protocols have special needs, like IMS, which relies~~some existing applications such as the IMS rely on specific protocol extensions, which can only run on top of ~~the~~ Diameter. ~~Further,~~

Currently, ~~Radius~~RADIUS is the AAA protocol that is ~~currently~~ most widely used in WLAN environments and all 802.1X and 802.11i compliant access points are expected to support RADIUS. Diameter, on the other hand, has only recently been approved as a standards-track RFC in IETF, and hence there are not many access points yet ~~that~~ supporting it. This paper discusses how both protocols can live in the same network and existing access points can be used~~Basically, there raises a question: is it too strong requirement to require all inter-working WLANs to support Diameter? One solution is a translation box between Radius and Diameter protocols. However, we should not make too many compromises in the security either~~. This has some implications for the features and security of the AAA system when using those access points. These implications are listed here as well.

Finally, the IETF status of RADIUS and Diameter drafts related to WLAN inter-working is outlined.

~~Appendix B~~2. Comparison

~~This chapter~~Chapter 8 ~~–~~compares ~~Radius~~RADIUS [RADIUS] and Diameter [DIAMETER] against following properties: failover mechanisms, transmission-level security, reliable transport, agent support, server-initiated messages, audit-ability, transition support, capability negotiation, peer discovery and configuration, roaming support. The ~~text is edited mainly on account of draf~~material has been derived largely from~~t~~ [DIAMETER] ~~and is now more suitable for discussion~~. As a summary, the differences are as follows:

~~More information can be found from Appendix A.~~

Property:	*~~Radius~~RADIUS:*	*Diameter:*
Failover mechanisms	Not defined (depends on implementation)	Supported
Transmission-level security (authentication and integrity)	Defined only for response packets. In [RADEAP] extension IPs~~S~~ec and IKE support is optional.	IPs~~S~~ec support is mandatory and TLS support is optional for access points, both for servers and proxies.
Reliable transport	UDP. Reliability varies between implementations.	TCP/SCTP. Reliable.
Accounting support	Defined in a non-standards track extension RFC. Reliability in various network and device error situations is implementation dependent.	Supported. The base protocol defines mechanisms for reliable transport and failover as above, and the accounting behaviour in network partition situations is controlled.
Agent s~~S~~upport	Not a part of the core protocol, though [DYNAUTH] extension defines server-initiated messages. Status of the definition (Internet Draft) and support in products is unclear.	Supported.
Audit-ability	Not supported.	Supported / optional, but the required Diameter component is still being standardized.
Capability negotiation	Not supported	Supported
Peer discovery and configuration	Manual configuration	Dynamic
Roaming support	Not suitable for global roaming in open environments due to lack of security.	Secure and scalable roaming support.

~~More information can be found from Section 86.~~

3. Transition support

While Diameter does not share a common protocol data unit (PDU) with RadiusRADIUS, considerable effort has been expended in enabling backward compatibility with RadiusRADIUS, so that the two protocols may be deployed in the same network. Initially, it is expected that Diameter will be deployed within new network devices, as well as within gateways enabling communication between legacy RadiusRADIUS devices and servers. This capability, described in [NASREQ], enables Diameter support to be added to legacy networks, by addition of a gateway or serverproxy speaking both RadiusRADIUS and Diameter.

3.Conclusions

Property:	*Radius:*	*Diameter:*
Failover	Not defined (depends on implementation)	Supported
Transmission-level security (authentication and integrity)	Defined only for response packets. In [RADEAP] extension IPSec and IKE support is optional.	IPSec support is mandatory and TLS support is optional
Reliable transport	UDP. Reliability varies between implementations.	TCP/SCTP. Reliable.
Agent Support	Not defined. In [DYNAUTH] extension server-initiated messages are optional.	Supported.
Audit-ability	Not supported.	Supported / optional. Data object security is defined in [AAACMS] extension.
Transition support	Not defined	Supported in extension [NASREQ].
Capability negotiation	Not supported	Supported
Peer discovery and configuration	Manual configuration	Dynamic
Roaming support	Not suitable for global roaming in open environments due to lack of security.	Secure and scalable roaming support.

RadiusRADIUS is currently widely used protocol in WLAN environments. At the same time RadiusRADIUS is missing several important features (see above), like such as server initiated messages and basic securitymay not operate with the highest possible security turned on. It is obvious that Diameter is better protocol than Radius in every field, but it is not very widely deployed yet. Therefore, gradual migration from RadiusRADIUS to Diameter seems to be one potential way to go further.

It seems reasonable to start from an initial model of the AAA network where most or all of the access points implement only RADIUS, and a core which uses Diameter but is capable of talking to the RADIUS-only capable access points. This would mean that a leaf AAA proxies should support both RADIUS and Diameter. As Diameter-capable access points are inserted to the network, they can be taken into use immediately. An advantage of placing the RADIUS/Diameter-capable nodes on the leafs of the network is that it becomes

~~It is an open question, what is the correct place to put translation service in the 3GPP-WLAN networks. There seems to be two main alternatives. Firstly, every AAA server should support both Radius and Diameter. Secondly, it is possible to put up a translation server between ASN and AAA servers in the operator network. The closer the translation server is to the ASN the more~~ easier ~~it is, e.g.,~~ to take advantage of ~~of roaming support~~the features found in D~~d~~iameter. For instance, even accounting may be more reliable if only the first hop is run in RADIUS but the traversal of the access provider, roaming consortium, and home operator proxies is done via DIAMETER.

~~<INSERT HERE A BRIEF DISCUSSION OF HOW RADIUS-DIAMETER TRANSLATION WORKS>~~

The actual translation gateway must be able to run both RADIUS and Diameter protocols. The [NASREQ] extension defines a framework for the protocol conversion, where the RADIUS attribute space is included into Diameter, which eliminates the need to perform many attribute translations. However, some explicit translations between RADIUS and Diameter attributes must be made, like translating vendor specific and accounting information.

Some Diameter related messages ~~are drop out, in the gateway~~can not be translated~~,~~ during the communication with RADIUS client, ~~like~~such as messages initiated by Diameter server. ~~In general, RADIUS lacks of several features, which are implemented in Diameter. Further, <INSERT HERE A DISCUSSION OF WHAT FEATURES ARE LOST IN TRANSLATION (per diameter-nasreq)>~~

Interoperability between RADIUS and DIAMETER in the presence of some of the non-standard RADIUS extensions ~~(such as server initiated messages)~~ has not been ~~studied~~specified.

4. Security in Transition

~~The attribute conversion between the RADIUS and Diameter protocols may take place in both directions. However, in the 3GPP-WLAN environments, the focus is on RADIUS client and Diameter server communication. The protocol conversion needs some additional security properties to the gateway.~~

The gateway ~~may need~~needs to add ~~authentication information while sending packets from RADIUS client to Diameter server~~use RADIUS application layer security mechanisms towards RADIUS, and IPsec or TLS towards Diameter. Given the use of the hop-by-hop security mechanisms, this translation can be performed without the knowledge of the original sender of the message. RADIUS requires pre-shared keys, while Diameter can take advantage of either IKE or TLS.

In addition, the translation gateway must secure attribute data towards the home server using Diameter ~~specific techniques~~CMS techniques (when the RFC is published). ~~In the other direction, the gateway must encrypt data using RADIUS shared key. The~~That is, end-to-end security mechanisms can be employed between the translation proxy and the home server, but not between the RADIUS-only access point and the translation proxy. ~~RADIUS requires pre-shared keys, while Diameter can take advantage of IKE.~~

~~Base RADIUS RFC does not include IPSec support, but RFC 2869bis recommends the usage of IPSec. The transition towards IPSec usage will not eventually be a very big step, because most of the current NAS already have IPSec implementation in their IP stack. RFC 2869bis replaces the old Radius support for EAP RFC. RFC 2869bis is on standard track~~

and will be ready soon. Therefore, we base our recommendations in the section 6 on forthcoming RFCs, which are near the last call.

Appendix D5. Standardization Status

RadiusRADIUS authentication is a standards-track RFC, while RADIUS accounting is an informational RFC. RadiusRADIUS has several extensions, which offer improvements to the basic protocolextensions. However, most Many of the extensions are under progress, and therefore it is quite unpredictable to determine when the standardisation work in IETF finishesInternet Drafts, and it is not even clear whether they will be completed as RFCs. Currently, [RADEAP] defines EAP support for Radius. When the standardization work is ready for Radius support for EAP, the co-operation between EAP and Diameter will be defined on the same way.

On the other hand, while the core parts of Diameter have been approved as standards-track RFCs (base protocol and transport have been approved, the NASREQ extension will be soon), the CMS security extension is still being worked on. Diameter deploymentss during 2003 can not take advantage of a standards-based CMS security, but need to rely on either transport or IP layer security.

The support for EAP in RADIUS is being reissued as RFC 2869bis, to clarify a number of interoperability issues that have been recognised. Base RADIUS RFC requires only the use of the application level MAC for some (not all) messages, but RFC 2869bis recommends the usage of IPsec. The Internet Draft [RADEAP] has passed IETF Last Call. When this draft is approved as an RFC, the same technical solution will be used to produce the DIAMETER EAP support RFC.

However, there is currently no standardised way to transport AAA-derived session keys from the home AAA server to the access point. The Microsoft vendor-specific attributes [MSATTR] are widely used, though believed to be quite insecure by today's standards. IETF is working on a keying framework for EAP along with standardisation of session key transport attributes.

6. Recommendation

We make the following recommendations on the basis of mature IETF Internet-drafts, which are on standard-tracks:

- Consider the adoption of Diameter – RADIUS compatibility mode i.e. support of both protocols along with the necessary translation mechanisms in order to enable the use of RADIUS-only access points. Such translation should occur as near the the leavesfs of the network as possible. As not all functions can be translated in full, some loss of functionality occurs for those devices, which use RADIUS, and this should be documented.

- Additionally, take a stand on whether IPsec is required in those cases where RADIUS is used, as currently required in RFC 2869bis. This may help to eliminate some of the vulnerabilities of RADIUS.

- Adopt the use of RFC 2869bis and corresponding Diameter counterpart as the standard for running EAP over AAA protocols.

- The participation of SA3 member companies in the standardisation of EAP keying framework and key transport is highly desired.

~~One of the biggest problems in Radius is related to transportation of session keys between AAA server to the access point (AP). The access point may reside physically in insecure place, and therefore, end-to-end security should be guaranteed between AAA server and AP with IPSec define in [RADEAP].~~

~~4.~~7. References

[DIAMETER] P. R. Calhoun, et. al., “Diameter Base Protocol”, IETF Work in Progress (approved as an RFC).

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

[RADEAP] B. Aboba, and P. Calhoun, "RADIUS Support for Extensible Authentication Protocol (EAP)", IETF work in progress.

[RADACCT] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC3162] B. Adoba, et. al., ”RADIUS and IPv6”, RFC 3162, August 2001.

[ACCMGMT] B. Aboba, J. Arkko, D. Harrington. "Introduction to Accounting Management", RFC 2975, October 2000.

[AAATRANS] B. Aboba, J. Wood, "Authentication, Authorization and Accounting (AAA) Transport Profile", IETF Work in Progress (approved as an RFC).

[DYNAUTH] Chiba, M., et al., "Dynamic Authorization Extensions to RADIUS", IETF work in progress.

[AAACMS] P. Calhoun, W. Bulley, S. Farrell, "Diameter CMS Security application," IETF Work in Progress.

[NASREQ] P. Calhoun, W. Bulley, A. Rubens, J. Haag, "Diameter NASREQ Application", IETF work in progress.

[ROAMREV] B. Aboba, et. al. "Review of Roaming Implementations", RFC 2194, September 1997.

[ROAMCRIT] B. Aboba, G. Zorn, "Criteria for Evaluating Roaming Protocols", RFC 2477, January 1999.

[PROXYCHAIN] B. Aboba, J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[MSATTRS] G. Zorn, “Microsoft Vendor-specific RADIUS Attributes”, RFC 2548, March 1999.

8. Appendix: RADIUS – Diameter Differences ~~A.~~

~~A.1.~~8.1. Failover

In the event that a transport failure is detected with a peer, it is necessary for all pending request messages to be forwarded to an alternate agent, if possible. This is commonly referred to as failover.

~~Radius~~RADIUS

~~Radius~~RADIUS does not define failover mechanisms, and as a result, failover behaviour differs between implementations.

Diameter

In order to provide well-defined failover behaviour, DIAMETER supports application-layer acknowledgements, and defines failover algorithms and the associated state machine.

~~A.2.~~8.2. Transmission-level security

End-to-end security services include confidentiality and message origin authentication. These services can be provided by supporting message integrity and confidentiality between two peers, communicating through agent.

~~Radius~~RADIUS

~~Radius~~RADIUS defines an application-layer authentication and integrity scheme that is required only for use with Response packets. While ~~Radius~~RADIUS Extensions [RADEAP] defines an additional authentication and integrity mechanism, use is only required during Extensible Authentication Protocol (EAP) sessions. While attribute hiding is supported, ~~Radius~~RADIUS does not provide support for per-packet confidentiality. In accounting, ~~Radius~~RADIUS Accounting [RADACCT] assumes that replay protection is provided by the back-end billing server, rather than within the protocol itself.

While [RFC3162] defines the use of IPsec with ~~Radius~~RADIUS, support for IPsec is not required. Since within IKE authentication occurs only within Phase 1 prior to the establishment of IPsec SAs in Phase 2, it is typically not possible to define separate trust or authorization schemes for each application. This limits the usefulness of IPsec in inter-domain AAA applications (such as roaming) where it may be desirable to define a distinct certificate hierarchy for use in a AAA deployment than for some other use of IPsec from the same node.

Diameter

In order to provide universal support for transmission-level security, and enable both intra- and inter-domain AAA deployments, IPsec support is mandatory in Diameter clients, and TLS support is optional.

~~A.3.~~8.3. Reliable transport

As described in [ACCMGMT], reliable transport is a major issue in accounting, where packet loss may translate directly into revenue loss.

~~Radius~~RADIUS

~~Radius~~RADIUS runs over UDP, and does not define retransmission behaviour; as a result, reliability varies between implementations.

Diameter

In order to provide well-defined transport behaviour, Diameter runs over reliable transport mechanisms (TCP, SCTP) as defined in [AAATRANS]. Diameter also defines an accounting mode, which can be used during network partitions and other transmission problems.

8.4. Accounting Support

Support for accounting relates to reliable transport of accounting data and ability to perform failovers as discussed above. In addition, different applications require different accounting record contents and generation mechanisms, and the treatment of fatal transport problems may be different in different sitautions.

RADIUS

RADIUS accounting exists as an Informational RFC and is not a Standards Track protocol. As discussed above, there are some limitations in the reliability and failover mechanisms in RADIUS.

RADIUS employs just one form of accounting, an event-based mechanism. The accounting data transported over it has a limited space for new defined attributes and a limited length of data in those attributes.

Diameter

Diameter accounting is a part of the Standards Track base protocol. In addition to the reliable transport and failover support, the specification provides the following:

- Application and home server directed control of error situations, such as network partitions.
- Application and home server directed control of the accounting record generation either as an event, start-stop, or interim.
- Large attribute space and length.

~~A.4.~~8.5. Agent support

Agent support includes Proxies, Redirects and Relays.

~~Radius~~RADIUS

~~Radius~~RADIUS does not provide for explicit support for agents. Since the expected behaviour is not defined, it varies between implementations.

Diameter

Diameter defines agent behaviour explicitly.

~~A.5.~~8.6. Server-initiated messages

Server-initiated messages contain features such as unsolicited disconnect or re-authentication / re-authorization on demand across a heterogeneous deployment

~~Radius~~RADIUS

~~Radius~~RADIUS does not support server-initiated messages. However, there exists an Internet Draft [DYNAUTH] which adds this capability. (We can not indicate how widely this feature is supported, but at this point at least it is not an approved standards-track RFC.)

Diameter

Support for server-initiated messages is mandatory in Diameter.

~~A.6.~~8.7. Audit-ability

The audit-ability property allows the system to detect if untrusted proxies modify attributes or even packet headers.

~~Radius~~RADIUS

~~Radius~~RADIUS does not define data-object security mechanisms. Combined with lack of support for capabilities negotiation, this makes it very difficult to determine what occurred in the event of a dispute.

Diameter

While implementation of data object security is not mandatory within Diameter, these capabilities are supported, and are described in [AAACMS]. However, this feature is not only an Internet Draft and is believed to require significant additional work before being approved as a standards-track RFC.

~~A.7.~~8.8. Capability negotiation

Capability negotiation allows the discovery of peer's capabilities like, protocol version number, supported applications, security mechanisms, etc.

~~Radius~~RADIUS

~~Radius~~RADIUS does not support error messages, capability negotiation, or a mandatory/non-mandatory flag for attributes. Since ~~Radius~~RADIUS clients and servers are not aware of each other's capabilities, they may not be able to successfully negotiate a mutually acceptable service, or in some cases, even be aware of what service has been implemented.

Diameter

Diameter includes support for error handling, capability negotiation, and mandatory/non-mandatory attribute-value pairs (AVPs).

~~A.8.~~8.9. Peer discovery and configuration

Allowing for dynamic agent discovery make it possible for simpler and more robust deployment of services.

~~Radius~~RADIUS

~~Radius~~RADIUS implementations typically require that the name or address of servers or clients be manually configured, along with the corresponding shared secrets. This results in a n administrative burden, and creates the temptation to reuse the ~~Radius~~RADIUS shared secret, which can result in major security vulnerabilities if the Request Authenticator is not globally and temporally unique as required in ~~Radius~~RADIUS.

Diameter

Through DNS, Diameter enables dynamic discovery of peers. Derivation of dynamic session keys is enabled via transmission-level security.

~~A.9.~~8.10. Roaming support

~~Radius~~RADIUS

The ROAMOPS WG provided a survey of roaming implementations [ROAMREV], detailed roaming requirements [ROAMCRIT], defined the Network Access Identifier (NAI)[NAI], and documented existing implementations (and imitations) of ~~Radius~~RADIUS-based roaming [PROXYCHAIN]. In order to improve scalability, [PROXYCHAIN] introduced the concept of proxy chaining via an intermediate server, facilitating roaming between providers. However, since ~~Radius~~RADIUS does not provide explicit support for proxies, and lacks audit-ability and transmission-level security features, ~~Radius~~RADIUS-based roaming is vulnerable to attack from external parties as well as susceptible to fraud perpetrated by the roaming partners themselves. As a result, it is not suitable for wide-scale deployment e.g. on the Internet [PROXYCHAIN].

Diameter

By providing explicit support for inter-domain roaming and message routing, audit-ability [AAACMS], and transmission-layer security features, Diameter addresses these limitations and provides for secure and scalable roaming. However, a part of the functions required for this are still being standardized in [AAACMS].