3GPP TSG SA WG3 Security S3-030~~xxx~~736
18th – 21th November, 2003
Munich, Germany

~~3GPP TSG SA WG3 Security – S3#XX S3-XXXXXX~~
~~24 April 2003~~10 November 2003

~~Jorvas, FI~~

~~S~~Agenda Item: WLAN

Source: ~~OY LMF Ericsson AB, Ericsson Research~~Ericsson

Title: ~~Diameter vs. Radius~~Security of EAP or SSID based network advertisements

Document for: Discussion

~~Agenda Item: T.B.D~~WLAN

~~Abstract~~

~~*This paper presents major differences between Diameter and Radius protocols, and discusses finally how suitable the protocols are for WLAN inter-working in 3GPP.*~~

~~Appendix A~~1. Introduction

~~Diameter [DIAMETER] and 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 major differences between those protocols and is an initial point to evaluate protocols against the 3GPP requirements.~~The 3GPP and IETF are currently discussing various mechanisms for network discovery and selection. This functionality provides a way for the user to get information on what networks are available behind an access point, and to indicate a desired network when he logs in. As a part of the network selection process, the access points can advertise the available networks using some protocol mechanism. Two potential mechanisms for this have been discussed:

- link-layer based mechanisms, such as conveying this information through announcing multiple SSIDs in 802.11 networks [1], and

- EAP based mechanisms, such as conveying this information in a reserved field of the EAP Identity Request message [3].

The purpose of this contribution is to clarify the security properties of these mechanisms. We conclude that the EAP Identity Request message is not, and can not be, cryptographically protected. We also conclude that a limited form of protection for SSIDs is possible, though not very useful in this particular situation.

~~The 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 without extensions to the protocol. On the other hand, some protocols have special needs, like IMS, which relies on the Diameter. Further, Radius is the AAA protocol that is currently widely used in WLAN environments. 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.~~

~~Appendix B~~2. ~~Comparison~~Advertisements in EAP Identity Requests

The EAP identity request message is sent as the first message in the EAP protocol. Typically, it is sent from an access point, though a recently published RFC 3579 also allows it to be sent from an AAA proxy [7]. However, the primary purpose of the EAP identity response message is to retrieve a NAI that shows how subsequent EAP messages are to be routed [6]. This implies that the request can only be sent by an entity close to the access point; all routing decisions have to be made in nodes beyond this.

As a result, the user's home network does not get to send the EAP identity request on which at least the initial routing will be based. Current AAA protocols do not convey the contents of the EAP identity request to the home network either; only the response is sent according to RFC 3579, for instance.

In addition (and partly because of the above), the contents of the EAP identity request are not authenticated within EAP or EAP methods. The home network will not be able to tell whether the access network provided an incorrect EAP identity request or if a man-in-the-middle changed the message while it was in transit.

As a result, any advertisement information provided within EAP identity request packets is not (and can not be) cryptographically protected. The information provided is a string. Non-legitimate parties could present the same kind of strings as legitimate access parties. Furthermore, malicious access operators could present some other strings than they agreed to in their contracts.

In addition, current EAP methods (such as [3, 4, 8]) do not protect the contents of the EAP identity response messages beyond the authentication of the user identified in them; any decorations attached to the NAI would not be taken into account.

Note also that the use of additional EAP protection layer such as PEAPv2 does not address this vulnerability. It is not possible, because PEAPv2 to cannot support the protection of the identity request that has been sent before the initiation of PEAPv2 and because the AAA server does not have a copy of the request that was sent.

As a result, EAP-based mechanisms do not protect network-selection-related advertisements nor do they protect the chosen network information.

3. Advertisements in Link-Layer Beacons

It has also been suggested that link-layers would use existing network identifiers such as the SSID in 802.11 networks as advertisements of intermediate networks. An access point could advertise multiple SSIDs, each representing a “virtual access point” through which you can connect to the network associated with the SSID.

The access point sends out beacons indicating its presence and parameters such as SSID; each beacon can contain one SSID. If the access point has multiple SSIDs, multiple beacons are sent out. The client indicates the desired SSID when attaching to the access point.

Like in EAP, the advertised set of SSIDs is not communicated to the home network. Unlike EAP, however, the chosen SSID is communicated to the home server. The access point sends the SSID within an attribute of an AAA protocol. In addition, 802.11i allows cryptographic verification of some Information Elements in its 4-way handshake that is run after EAP. For instance, the chosen SSID could be verified in this manner (the current standards do not mandate that you have to send the SSID IE for this verification, only that you can). This prevents outside parties from changing the SSID so that the client and the access point would believe a different SSID was selected.

However, since the access point alone tells the selected information to the home AAA server, there is no guarantee that the information the access point gives to the client and to the AAA server is the same. The SSID is not communicated within EAP, so neither the client or the home AAA server can verify that all three parties have the same information. Only the access point can do this.

> *Note: There has been some proposals related to the scoping of keys delivered from EAP. It would be possible to provide a cryptographic binding of the keys to parameters such as SSID [2]. However, the current consensus in IETF and IEEE appears to be that this is not needed, would complicate the standards needlessly, and would introduce backwards compatibility problems. It is possible to remedy this by providing an extension to EAP methods that allows the cryptographic verification of some of the parameters advertised by access points. However, such extensions are unlikely to be available within the Release 6 timeframe.*

As a result, the cryptographic validation of SSID-based advertisements is not possible today, and the validation of the chosen SSID is possibly only in a limited manner which relies on the correct behaviour of the access point.~~This chapter compares Radius [RADIUS] and Diameter [DIAMETER] against following properties: failover, 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 draft [DIAMETER] and is now more suitable for discussion. As a summary, the differences are as follows:~~

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

~~3.Conclusions~~

~~*Property:*~~	~~*Radius:*~~	~~*Diameter:*~~
~~Failover~~	~~Not defined (depends on~~	~~Supported~~

	~~implementation)~~	
~~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.~~

4. Conclusions

Neither EAP or link-layer mechanisms support the cryptographic protection of network-selection related advertisements today. Only a limited support for the protection of the chosen network is available. It is suggested that this vulnerability is recognised as a current limitation and that means outside the protocols are used to mitigate its effects.

5. References

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

~~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 roaming support features found in diameter.~~

~~Radius has several extensions, which offer improvements to the basic protocol. However, most of the extensions are under progress, and therefore it is quite unpredictable to determine when the standardisation work in IETF finishes. 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.~~

~~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.References

[1] IEEE Std 802.11i/D2.0, March 2002, "Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".

[2] draft-ietf-eap-keying-01.txt, November 2003, “EAP Key Management Framework”.

[3] draft-ietf-eap-rfc2284bis-06.txt, October 2003, " Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-11, October 2003, "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-12, October 2003, "EAP SIM Authentication".

[6] RFC 2486, January 1999, "The Network Access Identifier".

[7] RFC 3579, September 2003, “RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)”.

[8] RFC 2716, October 1999, "PPP EAP TLS Authentication Method".

~~[DIAMETER] P. R. Calhoun, et. al., “Diameter Base Protocol”, IETF Work in Progress.~~

~~[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.~~

~~[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.~~

Appendix A.

~~A.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 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.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 defines an application-layer authentication and integrity scheme that is required only for use with Response packets. While 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 does not provide support for per-packet confidentiality. In accounting, 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, 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.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 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.~~

~~A.4.Agent support~~

~~Agent support includes Proxies, Redirects and Relays.~~

~~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.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 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.Audit-ability~~

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

~~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.Capability negotiation~~

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

~~Radius~~

~~Radius does not support error messages, capability negotiation, or a mandatory/non-mandatory flag for attributes. Since 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.Peer discovery and configuration~~

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

~~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 an administrative burden, and creates the temptation to reuse the Radius shared secret, which can result in major security vulnerabilities if the Request Authenticator is not globally and temporally unique as required in Radius.~~

~~Diameter~~

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

~~A.9.Roaming support~~

~~*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-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 does not provide explicit support for proxies, and lacks audit-ability and transmission-level security features, 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].~~