Network Working Group
Internet-Draft
Expires: September 10, 2009

S. Winter (Editor)
RESTENA
K. Hoeper
Motorola
March 9, 2009

Threat Model for Networks Employing AAA Proxies
draft-hoeper-proxythreat-02.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 10, 2009.

Copyright Notice

Abstract

This memo defines a threat model for access networks with AAA proxies. Use cases of current and future applications in which AAA proxies are employed are described and it is discussed how proxies could launch attacks in the defined use cases. The risk associated with these attacks in each use case is analyzed. In addition, mitigation techniques used in current AAA deployments are discussed and best practices for mitigating the identified attacks are identified. As a result, this draft can serve as a guideline for risk assessments and problem mitigation by providers, implementers and protocol designers of systems with proxies.

Table of Contents

1. Introduction

Currently, AAA proxies are implemented in many access networks serving a variety of purposes. For example, proxies provide a scalable solution for access management in large networks. Furthermore, proxies can enable roaming because mobile nodes (MN) can access other networks by authenticating to their home server through local proxies.

The introduction of proxies can change the security model of a network as well as of the implemented protocols. As a consequence, AAA proxies may introduce new security vulnerabilities. However, currently the role of AAA proxies in networks and all their security implications are not considered in many existing RFCs and Internet drafts. The relationship with [RFC4962] is the most glaring aspect of the problem, but the progress of numerous drafts in a number of working groups is affected by the so-called "proxy problem". Recently, there have been attempts to reconcile the widespread deployment of AAA proxies with the security requirements of individual Internet protocols or protocol extensions.

While the re-occurrence of the proxy problem in several WGs may be bothersome and slow down progress, the problems are more severe for providers and users of already existing implementations with proxies. Doubts exist whether current security claims stated in RFCs and Internet Drafts are still valid for implementations with proxies. Hence, providers of networks with proxies that rely on such security claims may have unknowingly introduced new vulnerabilities to their systems that have not been covered in the respective protocol specifications. For the same reasons, users of such systems may be unknowingly exposed to attacks.

Concluding, the proxy problem may affect existing and future implementations of Internet protocols whose specifications neglected proxies in their security considerations. If security issues introduced by proxies are not identified and addressed, future protocol specifications will suffer from the same problems.

1.1. Goals of this Document

Since the "proxy problem" challenges the credibility of existing RFCs and slows down the progress of many IETF WGs, it seems necessary to revisit this problem in detail and make the results available to all current and future IETF WGs and other standard bodies.

This document shows how AAA proxies may change the security models of networks and their employed protocols in several use cases. Even more importantly, the document analyses the feasibility as well as

severity of the identified threats. In addition, existing techniques that mitigate some of the attacks and their effectiveness are discussed. From the previous discussions best practices to prevent and mitigate attacks by proxies are derived.

As a result, this draft can be used as a tool for risk assessment of a network with AAA proxies or protocols implemented in such networks. This draft shows which attacks by proxies are feasible in particular use cases under certain conditions. It is up to the provider/ implementer/protocol designer to decide whether the identified threats justify the costs that would be introduced by countermeasures such as infrastructure and/or protocol modifications.

Current and future drafts that are subject to the "proxy problem" could reference this document to point out possible vulnerabilities and risks.

1.2. Scope

This document focuses on security issues related to AAA proxies and the discussions and results in this memo should not be applied to other types of proxies. However, it is encouraged to work on similar documents for other kind of proxies.

1.3. Terminology

This section defines terms that are frequently used in this document.

AAA
: Authentication, Authorization, and Accounting (AAA). AAA protocols include RADIUS [RFC2865] and Diameter [RFC3588].

AAA Server
: A server which provides AAA services via an implemented AAA protocol to mobile nodes.

AAA Client
: A network entity sending AAA requests to the AAA server and receiving AAA replies from the AAA server. NAS and AAA proxy can both act as AAA client.

AAA Proxy
: An AAA proxy provides routing for AAA requests and replies. An AAA proxy appears to act as an AAA client to the AAA server and as AAA server to the AAA client. In this draft, pure re-direct proxies as supported by Diameter are not considered. Only AAA proxies that are capable of modifying attributes and may possess cryptographic keying material are considered.

2. Problem Statement

Unlike some other network entities that simply forward packets in the network, AAA proxies are designed to have additional capabilities and properties such that the AAA protocols executed through AAA proxies may have the following features:

- AAA proxies are able to insert, modify and/or delete AAA attributes
- AAA proxies share pairwise AAA keys with the AAA server and/or other AAA proxies;
- AAA proxies and NAS cannot be distinguished by AAA server;
- AAA proxies and AAA server cannot be distinguished by NAS;
- AAA proxy chains cannot be distinguished from single proxies by neither NAS nor AAA server.

The above special features may lead to new security vulnerabilities. For example, a proxy could maliciously modify or delete some attributes of an AAA request/reply in order to launch an attack. Or a proxy in possession of AAA keying material can break the end-to-end integrity and/or confidentiality between NAS and AAA server that is assumed in some protocols. The last three bullets show that the other communicating entities might not even be aware of the proxies on the communication path. In the case of a single proxy or a chain of proxies [RFC2607] between NAS and AAA server, not every party authenticates to all parties it communicates with as required in [RFC4962]. The sum of these and other security issues imposed by AAA proxies is referred to as "proxy problem" in this document.

3. Related Work

[Editor's note: Any additional references that should be mentioned here?]

Proxy-related security issues have been raised within the IETF for a long time and several issues as well as mitigation techniques are discussed in a number of RFCs, e.g. in [RFC2607], [RFC3748], [RFC5247], [RFC3588].

[RFC2607] considers chaining of RADIUS proxies in roaming scenarios. Section 7 in RFC 2607 gives a good overview of security threats in such scenarios.

[RFC3748] points out some potential security risks introduced by AAA proxies during an EAP execution. For example, AAA proxies may have an impact on authorization decisions and identity protection.

Among other things, [RFC5247] considers how EAP executions can meet the requirements in [RFC4962] even in the presence of AAA proxies. RFC 5747 identifies several security issues introduced by AAA proxies in the system (e.g. decryption of data traffic between peer and authenticators as well as impersonation of authenticators) and discusses some mitigation techniques.

Diameter [RFC3588] introduces the concept of relay agents that, unlike proxies, do not need to modify messages. This reduces the number of intermediaries in the network that need to possess keying material and, thus, reduces the risk of rouge proxies abusing keying material for launching attacks.

While these and other issues and mitigation techniques have been discussed in various places, this document attempts to use these previous results to summarize important security issues in one place, comment on the security of current practices, and identify good solutions for the mitigation of the identified flaws.

4. Use Cases

[Editor's note: Any more use cases?]

For easier identification of vulnerabilities as well as analysis of feasibility and severity of attacks, a representative set of use cases for AAA proxies in networks are supplied here.

4.1. Enterprise Network Management

In enterprise networks or other local networks with a single administrative domain, AAA proxies are used to enable easy and scalable network access in large networks. Here, instead of having a direct connection between each NAS and the authentication server, groups of NAS' can be connected to proxies in proximity. The proxies are then attached to the authentication server, resulting in a scalable network infrastructure. This is illustrated in Figure 1 for a network with two AAA proxies, where proxy 1 serves NAS 1 to NAS i and proxy 2 serves NAS j to NAS n. Hierarchical proxy routing can further simplify key management, as has been pointed out in RFC 2607. Note that this would lead to proxy chaining.

Other reasons why proxies may be used in enterprise networks are that the administrator wants to assign different sets of offered services

and policies for different groups of NAS'. In that case a proxy adjusts the AAA request from a certain NAS to the specified policy for this NAS, and/or adjusts the AAA reply to the capabilities of the NAS. This requires the proxy to modify or delete AAA attributes. For example, a NAS talking to proxy 1 only supports weak authentications (e.g. to constrained devices) but in return only limited services are made available to MNs connecting through this NAS. On the other hand, requests routed through proxy 2 may demand stronger authentication but provide a larger variety of services and information.

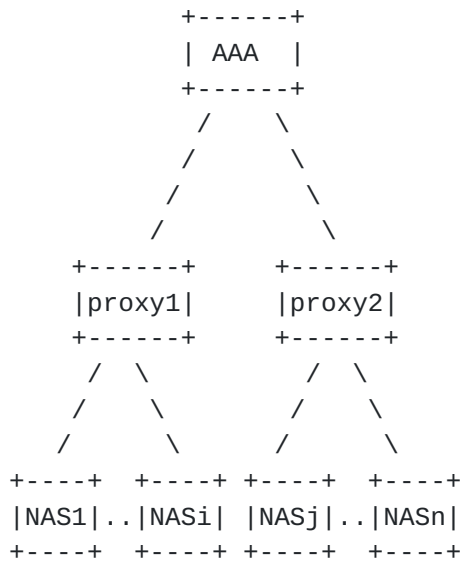

Figure 1: Enterprise Network With Two Proxies.

4.2. Free International Roaming

AAA proxies are used to enable roaming across administrative domains with roaming agreements. Note that roaming agreements may imply that proxies from one domain share AAA keys with proxies from the other domain or may be capable of establishing such shared keys. A proxy in domain 1 (lets say the home domain of MN) can serve as entry point for roaming requests from a domain 2 (lets say a visited domain). Even though the roaming is free in this use case (and thus billing unnecessary), it can be very important in such applications that policies of both domains are observed (e.g. the minimum age of users or minimum security level of provided services). To ensure this, the home proxy may need to adjust incoming AAA requests and outgoing AAA replies according to the capabilities and policies of visited and home networks, respectively, as well as the roaming agreements between them.

Note that the path for AAA communications between the visited domain

and the home domain may consist of several proxies, i.e. a proxy chain. Here, the roaming agreements between domain 1 and domain 2 specify the relationship between proxies in domain 1 (say the first proxy in the chain) and proxies in domain 2(say the last proxy in the chain). However, successful AAA functionality may require roaming agreements between each neighboring pair of proxies in the proxy chain (e.g. to share pairwise keys). For this reason, either the existing roaming agreement between domain 1 and domain 2 needs to extend to the intermediated proxies or additional agreements are needed. The described roaming scenario is illustrated in Figure 2.

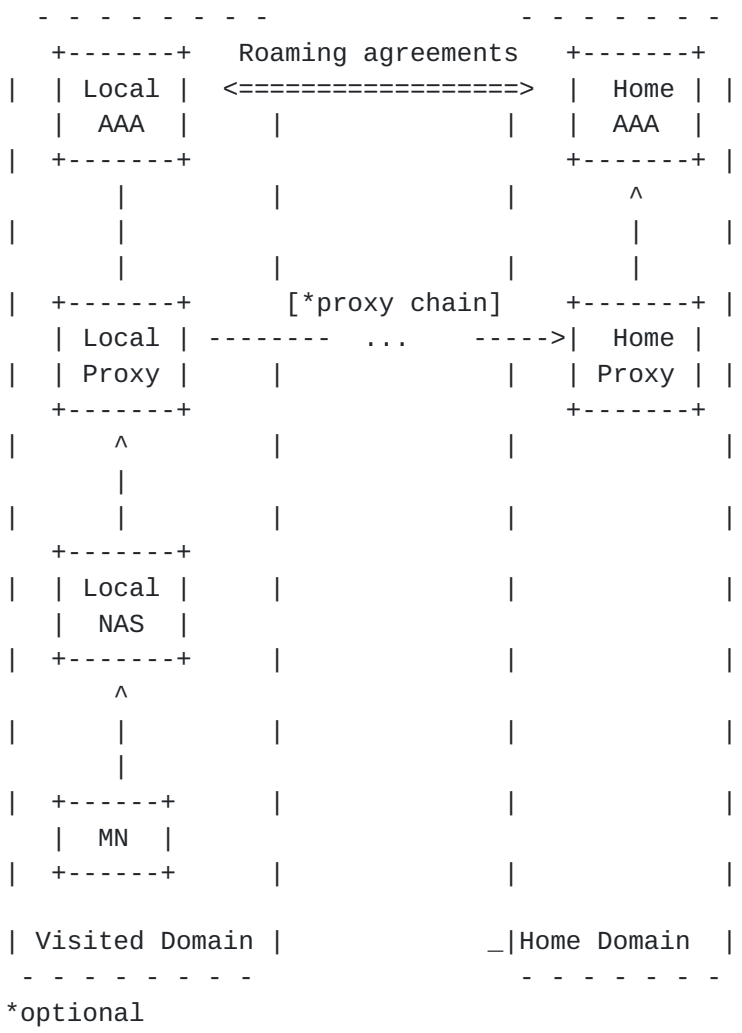

Figure 2: International Roaming Utilizing Proxies.

An example of an existing network enabling international roaming free of charge is eduroam [EDUROAM]. Eduroam is a world-wide WLAN roaming network for users in education and research. The network consists of a hierarchy of RADIUS servers interconnecting participating sites. The hierarchy consists of a root level proxy, used for international

roaming between different top-level domains, country-level proxy servers for roaming between institutions in the same top level domain, and institutional servers to perform the actual authentication (these servers may optionally further relay proxy requests to departments within their own institution at their discretion). Most RADIUS servers are duplicated for resiliency purposes. This architecture leads to a proxy path with at least five RADIUS servers in a chain when roaming internationally.

4.3. Billable International Roaming

In many roaming scenarios, the MN will be billed for the used roaming services according to the roaming agreements between the MN's home network and the visited network. The network architecture with proxies is the same as in the previous use case (see Figure 2), however additional billing information needs to be exchanged. Please note that authentication and accounting data may not take the same routing path [RFC2607]. As a consequence this document distinguishes between authentication proxy and accounting proxy for this use case.

5. Threat Model

To be able to analyze security vulnerabilities introduced by AAA proxies and their risks, a threat model needs to be established first. Section 5.1 describes the different players in the threat model. Section 5.2 defines the attacks an AAA proxy may launch in any of the use cases that have been described in Section 4.

5.1. Network Entities and their Trust Relationships

Since this document focuses on potential security risks introduced by AAA proxies, all other network entities (such as AAA servers and NAS) and MNs are assumed to execute all protocol steps faithfully and do not behave maliciously in any way. The practicability of these assumptions is out of scope of this document.

The above assumptions are generally based on the following trust relationships:

- Within a home domain (can be also considered as an intra-domain) it is assumed that all entities are correctly configured and not controlled by a malicious party. This can be achieved by intrusion detection systems or other means to detect so-called malicious insiders.

- The trust relationships between a home network and other local networks are specified in roaming agreements. These roaming

agreements imply that the home network trusts the local network to faithfully carry out the roaming services that have been agreed on under specified conditions (e.g. roaming fees).

This document deals with potential security threats introduced by AAA proxies. The attacks (as specified in the next Section) are executed by an AAA proxy that is either controlled by an adversary or mis-configured. Naturally for insider attacks, this requires some of the above trust relations to be violated, which will be discussed in Section 6. In this threat model the following types of malicious proxies are distinguished:

1. Proxies in the home network

2. Proxies in the visited network

3. Proxies in a proxy chain between the home and the visited networks

Furthermore, these three proxy types are split into authentication and accounting proxies.

5.2. Potential Attacks

This section lists potential attacks by proxies depending on the AAA deployment environment. In particular, the following sections distinguish proxy attacks on AAA backends in which the exchanged AAA messages are: (1) unauthenticated and send in cleartext; (2) authenticated and send in cleartext; and (3) authenticated and encrypted. The two latter sections discuss how some attacks can be mitigated by using already available AAA techniques for protecting messages.

5.2.1. Unauthenticated AAA messages send in clear

For obvious reasons, exchanging unprotected AAA messages (i.e. unauthenticated and not encrypted) from NAS to AAA server through intermediaries and vice versa offers the most attack points to a rogue or misconfigured AAA proxy. For the same reason, not only proxies but any entity with access to the backend (e.g. routers, relay agents) could launch the following attacks in this setting:

1. Passively eavesdrop on network traffic
   Traffic analysis can be used to track the activity and/or mobility of particular users. To do so the attacker needs to be able to correlate identifiers used in the AAA messages to users or network entities.
   Monitoring network traffic can be carried out by any entity with

access to the backend network and is thus not limited to AAA proxies.

2. Replay data packets
   This attack consists of two phases: (1) the recording of data packets of previous network authentications and (2) the replaying of this data at a later time. This leads to impersonation of the message originator and can be exploited for creating false billing statements, unauthorized network access, and many more. Replay attacks can be carried out by any entity with access to the backend network and is thus not limited to AAA proxies.

3. Re-direct data packets
   Any proxy could maliciously re-direct AAA data packets. It appears that this attack can only be exploited for Denial of Service (DoS) attacks [Editor's note: Is this true?] which are often not preventable by cryptographic means.
   Re-directing attacks require access to the routing path and thus can be carried out by routers, proxies and other intermediaries on the routes.

4. Drop data packets
   As for re-direction attacks, any proxy can drop packets causing re-transmissions potentially leading to a denial of service. [Editor's note: Is there any other attack?].
   This attack can be executed by all entities on the routing paths and thus can be carried out by routers, proxies and other intermediaries on the routes. Note that this attack cannot easily be distinguished from "natural" packet losses.

5. Not executing checks
   Sometimes a proxy needs to perform certain checks upon receiving an AAA message and its further actions depend on the result of the check. Such checks may be necessary to enable a proper flow of the AAA messages in the backend or to prevent or detect attacks by other entities in the backend.
   For example, a first-hop proxy may be required to check whether some particular address attributes in the received message match the address of the sender of the message. This could, e.g., prevent impersonation attacks by a NAS. By (volunteeringly or unvolunteeringly) not performing checks, the proxy opens the door to the described and other attacks.

6. Extract confidential information from network traffic
   In this attack confidential information is extracted from exchanged AAA messages. This could affect the privacy and confidentiality of exchanged information, e.g. user identities and user passwords, respectively. Session keys obtained from

exchanged AAA messages compromise protected communications between a NAS and a MN if such keys will be used to derive further keys to protect this link. Also accounting information could be a target.
Where AAA protocols do not encrypt their payload or parts of it on the wire, any attacker with access to the backend network may extract confidential information from the exchanged AAA packets.

7. Fabricate fake data packets
In this attack, the attacker fabricates valid AAA messages. This can be exploited for unauthorized network access, fabrication of accounting data to charge for unused services or don't charge for used services and other very damaging attacks.
If AAA messages are completely unprotected in the backend, any entity with access to the backend can fabricate packets that do not need to contain some secret or otherwise unknown information. However, fabricated packets for network access or billing information may require secret passwords or certain identifiers. In that case the attacker first needs to observe this secret information in a first phase of this attack before using this information in a fabricated packet.

8. Modify messages
In this attack, the attacker modifies exchanged data. This can be exploited for impersonation attacks, manipulating accounting data and many other very damaging attacks.
Completely unprotected messages are susceptible to this attack which can be launched by any entity on the routing path.

9. Insert, modify or drop AAA attributes
Some proxies are able to insert, modify or drop AAA attributes to enforce local policies. These capabilities can be exploited by malicious proxies for many attacks. For example, a proxy could grant or deny authorization for network access even if this is against the local policy. Unprotected AAA attributes can be modified by any proxy or other intermediary. This can be exploited for severe attacks, e.g. a proxy could forge NAS-IP-Address, NAS-IPv6-Address, or NAS-Identifier to cause that keying material is send to another NAS. Such modifications can also lead to granting network access to an entity different from the one requesting network access. In addition, any AAA attribute (protected or unprotected) that is not bound to any other protected AAA message or attribute can be dropped unnoticed by any proxy or other intermediary on the routing path.

5.2.2. Authenticated AAA messages send in clear

This section considers attacks that can be launched by proxies in AAA backends in which AAA messages provide message authentication but are not encrypted. Here, the authentication includes the exchanged data as well as the AAA attributes. If a part of the message is not authenticated, the discussion of the previous section applies. Basically the attacks are the same, but some of them only work under certain conditions described in the following (see Section 5.2.1 for the definition of the attacks):

1. Passively eavesdrop on network traffic
   Authenticated messages can be still monitored by any entity with access to the backend networks.

2. Replay data packets
   Proper message authentication mitigates replay attacks by including time variant information (such as timestamps, nonces, and/or sequence numbers) into each message. This type of countermeasure is typically included in AAA protocols such as RADIUS and Diameter. However, there are legacy operation modes in RADIUS that can be replayed easily (e.g. Access-Request packets without the Message-Authenticator attribute, which is against the Recommendation of [RFC5080]).

3. Re-direct data packets
   Re-direction attacks cannot be mitigated by message authentication.

4. Drop data packets
   Authenticated messages can be still dropped by proxies and intermediaries on the routing path.

5. Not executing checks
   Same as in Section 5.2.1.

6. Extract confidential information from network traffic
   Confidential information can be still extracted from authenticated AAA messages that send data in the clear.

7. Modify messages
   Modifying authenticated messages requires the knowledge of the key used to protect the data. If a proxy is in possession of this key, it can still modify messages. Note that other intermediaries such as routers and relay agents do not possess any keys required for the attack.

8. Modify or drop AAA attributes
   Authenticated AAA attributes can still be modified or dropped by a proxy that is in possession of the authentication key. This is a fairly common scenario because proxies need to be able to enforce local system policies and thus are required to modify or drop AAA attributes in certain situations.

5.2.3. Authenticated and encrypted AAA messages

In networks in which AAA messages are authenticated and encrypted proxies can still launch the same attacks as described in the two previous section, however, the conditions for a success may require proxies to be in possession of the used keying material. These attacks are then specific to proxies and cannot be launched by other intermediaries (such as routers and relay agents) any longer. The condition for successful attacks on authenticated and encrypted AAA messages by proxies can be summarized as follows:

1. Passively eavesdrop on network traffic
   If identifiers, addresses and information identifying an entity are encrypted, rogue proxies cannot simply eavesdrop on AAA communications to perform traffic analysis any longer. Analyzing the network traffic would require an active attack by a proxy in possession of the encryption keys.

2. Replay data packets
   Authentication can mitigate this problem (see previous section), encryption does not provide further protection.

3. Re-direct data packets
   Re-direction attacks cannot be mitigated by neither message authentication nor encryption.

4. Drop data packets
   Messages can be still dropped by proxies and intermediaries on the routing path.

5. Not executing checks
   Same as in Section 5.2.1.

6. Extract confidential information from network traffic
   The extraction of confidential information from encrypted messages requires now the knowledge of keying material. This attack is especially attractive if cryptographic keys are exchanged in the AAA messages. Only proxies in possession of the encryption keys are able to decrypt, all other intermediaries cannot.

7. Modify messages
   Same as in Section 5.2.2.

8. Modify or drop AAA attributes
   Same as in Section 5.2.2.

6. Risk Analysis

This section uses the threat model in Section 5 to analyze the feasibility and severity of the identified attacks in each of the uses cases discussed in Section 4. An attack is only considered a risk, if the attack is feasible and the impact is sufficiently severe to justify the attack's costs from an attacker's perspective.

6.1. Feasibility

It can be observed that the feasibility of attacks by proxies depend on the use case, the type of employed proxies, and whether the proxy possesses keying material required for an attack.

In general, the existence of malicious home proxies in an enterprise network (and thus the feasibility of attacks in such networks) is fairly unlikely because enterprise networks can be efficiently protected. For such an attack, the trust assumption in the home network must be violated (see Section 5.1).

On the other hand, in roaming scenarios, the attacks by proxies (as listed in Section 5.2) can be classified as more probable because they can be carried out by local proxies and/or proxies in a proxy chain between home and visited network. The trustworthiness of visited proxies is specified in the respective roaming agreements, while the trustworthiness of proxies in proxy chains may depend on a chain of roaming agreements. In a proxy chain, both ends of the chain (i.e. home and visited network) have roaming agreements with each other as well as neighboring pairs of proxies in the chain. Only if the chain consists of three or less proxies, the home network directly trusts all proxies (up to two) in the chain. For chains longer than three (including the end points) trust is transitive, i.e. the home proxy does not directly trust all proxies on the chain but rather trusts its direct neighbor to only have agreements with other trusted proxies and so forth. This results into a chain of trust. It can be observed, that a violation of this chain of trust is more likely than a direct trust violation in the home or visited network. Furthermore, the longer the proxy chain, the more diluted may the trust relations become and the more likely is a compromised or mis-configured proxy as part of the proxy chain.

In any case, attacks in roaming use cases require that a trust relation as part of the roaming agreements is violated (see Section 5.1).

In addition, the feasibility of attacks depend whether they require knowledge of keying material. For instance, attacks 1-5 in Section 5.2) do not require the knowledge of keying material and thus can be executed by any proxy or other intermediary. On the other hand, attacks 6-9 may require the knowledge of the AAA keying material that has been used to protect the data under attack. However, the possession of keying material is likely because AAA protocols are often based on hop-by-hop security using shared keys. In addition, proxies often need to be able to adjust (protected) AAA attributes to meet local requirements.

6.2. Severity

In enterprise networks, the severity of attacks are rather limited, because the exchanged data would not be of great value for an attacker and the exploitation of fabricated of modified packets is limited (e.g. because of the lack of accounting data and mobility pattern of users).

The severity of all attacks in roaming scenarios is higher due to the higher value of the exchanged information and offered services. For instance, traffic analysis attacks (attack 1) could be of interest to track the movements of particular mobile users. DoS attacks (attacks 3 and 4) could bring down the entire services, so the risk can be considered moderate to severe depending on the offered services.

Especially accounting information is an attractive target for an adversary. However, the information of free roaming services (use case 2) can be of value as well. For example, in [EDUROAM] data can contain the age, nationality, and other personal information of the mobile user wishing to access the network. Modification attacks can also be a severe risk, e.g. under aged users can control proxies to modify the age in order to pass the age limit for a requested service or local proxies may modify the roaming information to make their network services more attractive but later charge more. In addition modification attacks can be used for the downgrading of negotiated security credentials. Fabrication attacks can be classified as extremely severe in use case 3, because a malicious accounting proxy could fabricate false accounting information, such that the home network is charged for roaming fees even though no mobile node actually roamed.

7. Mitigations Techniques and Best Practices

Some of the aforementioned challenges when deploying an AAA fabric with proxies can be mitigated technically, but most of them can only be mitigated by an appropriate policy or code of conduct between the entities in the proxy fabric. This section consists of two parts: the first section describes deployed AAA fabrics as well as existing mitigation techniques and analyses which of the aforementioned challenges are mitigated technically, policy-wise, or not at all. The second part identifies best practices for AAA systems employing proxies, basically combining known techniques to address the attacks.

7.1. Current Practices

7.1.1. Authentication and Encryption of AAA messages

RADIUS and Diameter both support authentication and encryption for AAA packets. AAA authentication and encryption mitigate attacks # 2, 6, 7, 8 and 9 in Section 5.2 by intermediaries that are not in possession of the used keying material. However, as discussed in Section 5.2, these techniques do not provide end-to-end security. Hence rogue proxies could use their keys to break authentication and confidentiality of the exchanged data.

7.1.2. RadSec

[TBD]

7.1.3. Relay Agents

Diameter enables the implementation of redirect functionality (see [RFC3588]) in which so-called relay agents relay AAA messages directly from the source to the destination. These relays do not need to store keying material which distinguishes them from AAA proxies. Thus, deploying relay agents mitigates all attacks that require the knowledge of keying material.

7.1.4. AAA in EAP executions

During an EAP execution the authenticator often acts as a pass-trough device between peer and the authentication server [RFC3748]. The authenticator and the authentication server use an AAA protocol to encapsulate the EAP messages exchanged between each other. RFC 5247 considers how AAA guidelines in RFC 4962 can be met during EAP executions even in the presence of proxies. Recall that RFC 4962 does not address the proxy problem. RFC 5247 identifies several direct or indirect attacks by proxies that have been covered in Section 5.2 and suggests using the redirect functionality to mitigate

these attacks. In addition, instead of relying on a proxy executing a check, RFC 5247 recommends to rather use EAP channel bindings ([I-D.ietf-emu-chbind]) to address the attack. Basically this removes a crucial security check that needs to be executed by a proxy by another mitigation technique that does not depend on proxies at all (here EAP peer and the authentication server ensure the prevention of the attack by implementing and executing channel bindings).

7.1.5. Federated Authentication: eduroam

Eduroam is a world-wide roaming consortium exclusively for the education and research sector (i.e. schools, universities, research centres) [EDUROAM]. It is exclusive in the sense that only education users may hold a user account from a participating organisation to log in.

Technology-wise, it's an IEEE 802.1X-based roaming fabric which interconnects the individual educational organisations via a hierarchy of RADIUS servers. These organisations manage their user accounts independently. The RADIUS hierarchy provides realm-based routing to facilitate international roaming. Only EAP mutual authentication is used to authenticate users, EAP payloads typically being TTLS-PAP, PEAP-MSCHAPv2 and TLS to protect the user's credentials in transit: the inner credentials are only ever exposed at the user's 'home' authentication server, thus preserving privacy. Both wireless and wired 802.1X are implemented.

There is no per-session or per-volume accounting, i.e. it is 'free'(eligibility fees from the Identity Provider side notwithstanding). A service provider ('hotspot'), typically a university, runs on the principle of mutuality: their users are granted global roaming rights, while their hotspot in turn allows any international users to roam at their site. Participant organisations cover their own operational costs.

Mitigates:

1. Traffic analysis: ?

2. Replay: ?

3. Re-direct: ?

4. Drop packets: ?

5. Attack on confidentiality:?

6. Data fabrication: yes, stops fraus accounting

7. Message modification: partial, EAP payloads in Auth only

8. Attribute modification: ?

7.1.6. Authentication at Untrusted Third Party ISP: Using OTP

[Editor's note: Need volunteer who knows how Cisco's OTP is deployed to write this section]

Mitigates:

1. Traffic analysis: ?

2. Replay: ?

3. Re-direct: ?

4. Drop packets: ?

5. Attack on confidentiality:?

6. Data fabrication:?

7. Message modification:?

8. Attribute modification: ?

7.1.7. Non-Recommended Practices

An example of a bad, but unfortunately widely implemented practice is to send plain text credentials through proxies. This is done by most WiFi hotspot roam ops ('captive portals').

[Editor's note: Is this worth elaborating on? Any more examples of bad practices?]

7.2. Best practices

[Editor's note: Please help to extend the list of good mitigation techniques]

From the previous discussions the following mitigation techniques are considered good practices to thwart the attacks by proxies described in Section 5.2:

- Use authentication and encryption for all sensitive data exchanged in the AAA messages

- Keep the number of proxies in the network that require the knowledge of keys to an absolute minimum, e.g. by analysing the function and corresponding capabilities of each proxy and/or using redirect functionality in Diameter.

- Replace security checks relying on proxies by security checks that can be performed by other, more trustworthy, entities. For example use channel bindings.

- Implement additional, external means guarding the integrity of the home or enterprise network that help to detect and remove compromised and misconfigured proxies.

- Formulate roaming agreements between all participating networks and establish security policies for all participating entities. This establishes responsibilities in the case a misbehaving proxy causes damage.

Only a combination of the above technical and policy-based mitigation techniques can thwart most of the identified attacks by rogue proxies.

8. Security Considerations

[TBD]

9. IANA Considerations

This document has no IANA considerations.

10. Conclusions

This draft facilitates implementers and providers of networks with AAA proxies as well as protocols designers to carry out a risk analysis of threats introduced by AAA proxies. The result of such analysis enables to decide whether the potential security vulnerabilities introduced by AAA proxies in the network justify the costs of necessary system or protocol modifications to thwart the identified attacks. A set of existing countermeasures partially used in already deployed AAA networks have been discussed and good practices for mitigating attacks by proxies have been identified.

As a result of the presented discussions, it can be observed that security solutions thwarting proxy attacks can be expected not to be of pure technical nature. The feasibility of attacks highly depends on the reliability of security policies in enterprise networks and roaming agreements in roaming applications.

11. Acknowledgments

Thanks to everybody contributing to the proxy list and/or the meeting in Philadelphia, especially Bernard Aboba, Alan DeKok, Pasi Eronen, Dan Harkins, Sam Hartman, Russ Housley, Tim Polk, Klaas Wierenga, and Glen Zorn. Special thanks to Stefan Winter for providing the eduroam application as one of the use cases.

12. References

12.1. Normative References

12.2. Informative References

[EDUROAM] Wierenga, K. and S. Winter, "Deliverable DJ5.1.4: Inter-NREN Roaming Architecture: Description and Development Items", 2006, <http://www.geant2.net/roaming-techspec.pdf>.

[I-D.ietf-emu-chbind] Clancy, T. and K. Hoeper, "Channel Binding Support for EAP Methods", November 2008.

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4962] Housley, R. and B. Aboba, "Guidance for Authentication, Authorization, and Accounting (AAA) Key Management", BCP 132, RFC 4962, July 2007.

[RFC5080] Nelson, D. and A. DeKok, "Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes", RFC 5080, December 2007.

[RFC5247] Aboba, B., Simon, D., and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework", RFC 5247, August 2008.

Authors' Addresses

Stefan Winter
RESTENA Foundation
6, rue Richard Coudenhove-Kalergi
Luxembourg 1359
Luxembourg

Phone: +35 242 44091
Email: stefan.winter@restena.lu

Katrin Hoeper
Motorola
1301 E Algonquin Road
Schaumburg, IL 60196
USA

Phone: +1 847 576 4714
Email: khoeper@motorola.com