WIRELESS WORLD

RESEARCH FORUM

Securing Network Attachment and Compensation

Seppo Heikkinen, Tampere University of Technology, Finland, seppo.heikkinen@tut.fi
Mark Priestley, Vodafone Group R&D, UK, mark.priestley@vodafone.com
Jari Arkko, Ericsson Research NomadicLab, Finland, jari.arkko@ericsson.com
Pasi Eronen, Nokia Research Center, Finland, pasi.eronen@nokia.com
Hannes Tschofenig, Siemens Corporate Technology, Germany,
hannes.tschofenig@siemens.com

***Abstract*— A multitude of security mechanisms are employed when a node attaches to a network. Additionally, some further procedures, like configuration and ensuring compensation, need to be followed before connectivity is enabled. This paper takes a holistic view on the matter by providing a secure and efficient procedure for network attachment and compensation that ensures that the charging of service is based on actual usage and prevents repudiation of legitimate charging records.**

***Index Terms*— Network attachment, Compensation, Security, Ambient Networks.**

Introduction

Typical network attachment procedures in a wireless environment include several steps that the client has to perform before being able to receive meaningful services, which often is plain connectivity. As these steps can take place in several different layers, with minimal co-operation between them, the overall solution is often inefficient. For example, with WLAN access the attachment procedure requires many roundtrips that can add up to several seconds. Typically, this signaling does not include measures to ensure that the service provider is able to provide evidence of the services it has provided to a particular user when claiming the corresponding compensation. In addition, the configuration of security mechanisms is often so complex or burdensome that it is left halfway or completely undone.

This paper adopts the principles and design presented in [10] and [11] and depicts an integrated way to attach to a network and provide a non-repudiable charging solution for future networks. We believe that this kind of combined procedure is needed in order to provide an efficient and secure solution for the changing and convoluted ecosystem that the new wireless technologies will bring forth.

This paper is organized as follows: The next section of the paper describes the network attachment procedure in detail, whereas the following two sections discuss the compensation issues in general and the hash-chain based protocol solution for non-repudiable billing. The final section concludes our paper.

This document is a byproduct of the Ambient Networks Project, partially funded by the European Commission under its Sixth Framework Programme. It is provided “as is” and without any express or implied warranties, including, without limitation, the implied warranties of fitness for a particular purpose. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Ambient Networks Project or the European Commission.

Network Attachment

Principles

The concept of network attachment is not always clearly defined as it can contain a wide array of functions that different entities have to perform before they are able to communicate. In some cases, just establishing network layer connectivity is deemed to be the most relevant aspect of network attachment, whereas in this paper we try to take a more holistic view by considering the co-operation across different layers and compensation aspects, thus extending the study beyond just the client and the access point.

The most challenging aspects arise when the network attachment takes place between two different administrative domains. There a number of security sensitive actions need to take place in order to secure the exchange of information necessary to establish the basic mechanisms for subsequent interaction. The bootstrapping of these procedures is key to many of these actions as there might not be any trust relationship between the different parties and hence, no pre-existing security association. Sometimes this might require manual intervention, like in the case of DHCP security [1]. As this case has shown, the consequence often is that the security methods are not employed.

The fundamental issue adopted from the architecture design depicted in [10] is the use of cryptographic identifiers. In essence, these are hashes of the public keys. They are used as a replacement of conventional identifiers, e.g., MAC addresses, and provide cryptographic means to verify the identity of an entity. Moreover, authorization statements can be bound to them, thus making it possible to have more granular authorization schemes as to what actions are permitted. In other words, the mere authenticity of an entity may not be enough to grant access, for example, as it is often done today. It is worth noting that the design also makes it possible to have a case where the access point is required to present statement to the client that it is authorized to provide access. Additionally, the keys can be ephemeral in nature, i.e., they are used only for a short period and then discarded. This helps to alleviate privacy concerns. Cryptographic identifiers can also be used to bind different layers of operation more tightly with each others, so that certain man-in-the-middle attacks (cf. [4]) can be avoided.

The proposed design also suggests to piggyback information elements with the handshake messages, so that relevant signaling information can be exchanged early in the protocol. This reduces roundtrips and helps in establishing basic connectivity early on and enables the secure provision of zero configuration. The information elements can also be used to convey some legacy authentication schemes as well as compensation related information.

In order to promote efficiency, the system should support the delegation of different tasks. This way the node is able to transfer some of its responsibilities to the network, thus reducing the need to traverse radio interface. This is done with help of authorization statements, for which potential options are for example SAML [2] and SPKI certificates [3] with suitable encoding.

Protocol View

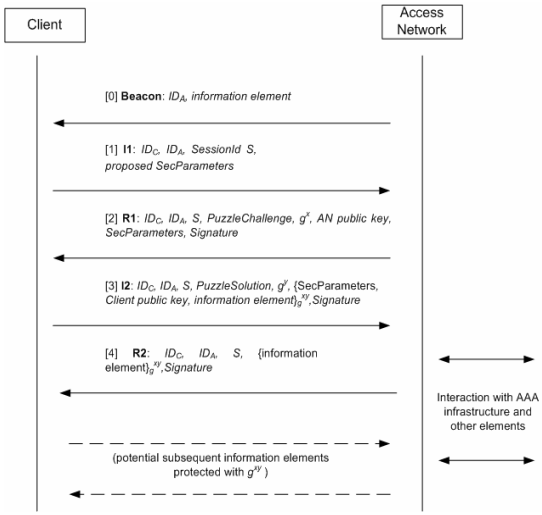

Figure 1: Network Attachment Flow

Figure 1 shows the protocol flows taking place between the client and the access network [11]. It takes advantage of the lessons learnt and concepts employed in protocols like HIP [5] and IKEv2 [6] and some preliminary sketches of the different flows appeared already in [12].

In the first phase the access network transmits a beacon that tells its identity and possibly some other relevant information that the access network wants to reveal. This could be, for example, capability information that could help the client to decide whether it should proceed with the attachment procedure. In some cases, it might be possible that the beacon message is omitted and the client needs to have some other form of trigger for the initiation of the attachment

procedure.

The client initiates the actual procedure by sending an I1 message that uses the access network and client identifiers as target and source, respectively. In cases which the access network does not wish to advertise itself, the client has the option of leaving out the target identifier and solicit an answer from the available access points unless the identifier is known by some other means. The message also includes a session identifier to distinguish between potentially simultaneous session taking place in parallel and a set of security parameters that the client proposes to be used.

The access network replies with R1 message that along with identifier and session information includes a cryptographic puzzle, the Diffie-Hellman key of the access network, its public key and the security parameters that are going to be used in the communication with the client. The access network signs the message with its private key.

The puzzle scheme is used to mitigate the effect of potential denial of service attack, even though it can be argued that it punishes valid clients too severely, especially the ones that have limited processing capabilities. This is because the idea of puzzle scheme is to make the client invest the computation resources required to solve the puzzle before further communication is allowed or any state is created. It should also be noted that the access network may need to have some predefined set of security parameters from which it tries to find a suitable match to the ones proposed by the client. This way the access network is able to calculate signature beforehand, otherwise the calculation could provide a venue for denial of service.

In the third step the client transmits the solution to the puzzle along with its Diffie-Hellman response. At this point the Diffie-Hellman procedure has produced a session key [20] that can be used to encrypt information, such as the public key of the client and some information elements that the client does not wish to disclose to potential eavesdroppers. Encryption with the public key is provided for the sake of privacy protection. The client also signs the message.

The fourth message concludes the initial message exchange and with it the access network can send some additional properties it wishes to advertise to the client, such as IP address assignment. They are protected with the established session key, which the access network can now calculate based on the response it got from the client. This message is signed as well.

Thus, with this set of messages the parties have verified the identities of each others and they can be certain that they are communicating with the same entity. Of course, this does not mean that there is any knowledge who the other party actually is. There might be some predefined information about the identifiers that could result to additional rights, like connectivity, but the approach could also be opportunistic in similar way as with SSH [7]. In this setting the achieved property is a sameness guarantee. This is suited for cases where the initial enrollment procedure can be secured, i.e., where no MITM adversaries can launch an attack. It might be possible to completely omit a AAA infrastructure in some of these scenarios, such as in home networks.

A third approach utilizes some from of trusted third party that is able to authenticate the user or vouch for a particular user. This could be some statements that are presented during the protocol run or the third party can be included in the protocol run with some additional messages much like in EAP [8]. For the vouching to have some meaning it is needed that the both parties are able to trust this third party.

Communication Channel

As shown, the protocol flow uses information elements to convey information between the parties, thus establishing a logical communication channel of its own [10]. The elements are envisaged to be extensible structures, such as e.g., XML, that can contain information or assertions about the properties of an entity, be a request to perform some action, the corresponding response or some event type of information. As the parties have established a session key it is possible to exchange protected information elements even after the initial handshake messages.

The channel can therefore be used to transmit signaling information bootstrap further protocols. This could be, for example, DHCP [16] or mobility management [13]. The idea is similar to the one presented in [9] that suggested piggybacking DHCP with HIP. Additionally, the use of cryptographic identities makes it natural to employ CGA type of schemes [14] to bind the identity with

the address. Other proposals that combine the securing of configuration provisioning with the attachment process exist as well (see, for example [15]). [10] and [11] show additional examples of the signaling tasks that can be performed.

With the help of this protected channel the client can perform the delegation of tasks as mentioned earlier. Delegation takes place in the form of authorization statements, so whenever the access network is performing a task on behalf of the client, it has to present this statement as a proof that is allowed to proxy the said task.

Compensation

When protocol interaction within the same administrative domain takes place then security measures relating to compensation, such as non-repudiation of service usage, are typically not a big concern. This could be, for example, in a home environment or in an enterprise network that is tightly controlled and regulated by administrative staff. In regular setting, however, in which different administrative domains wish to engage in communication, compensation mechanisms become important. Compensation addresses the allocation and transfer of information representing monetary values between users, providers and owners, in exchange for use of services and resources.

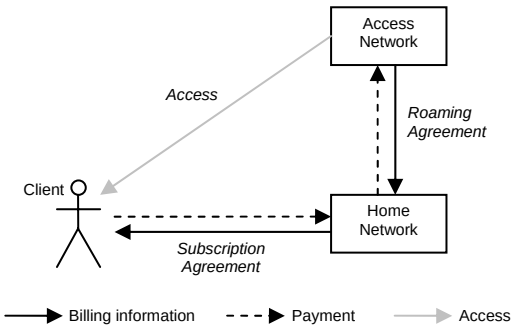

Figure 2: Roaming interactions related to compensation

Within current roaming agreements (see Figure 2), such as those between GSM operators, there is a disincentive for either party to act dishonestly as the potential penalty for such an action, e.g., jeopardizing the agreement, loss of reputation, possible exclusion from industry bodies, is normally far greater than any potential gains. As a result each operator trusts the accounting and charging mechanisms and processes within the other operator's network to provide accurate information. No cryptographic techniques for non-repudiation are used.

In future network access scenarios, where the role of the access or visited operator might be taken by smaller and/or ad-hoc networks, and roaming agreements might be more dynamic, for example the dynamic roaming agreements proposed in [11], the above kind of trust assessment will not always hold. Therefore, it is desirable that the charging scheme exhibits the following properties [11]:

1. Provides cryptographic non-repudiation of service usage that can be used to for billing records
2. Minimizes any requirements for additional messaging
3. Minimizes the cost of processing requirements on the client but not at the cost of additional messaging.
4. Is modular to support cases in which non-repudiation is not possible or desirable e.g. legacy systems
5. Supports current pre- and post-payment subscription models
6. Minimizes any potential for fraud, e.g., double spending

The goal of the non-repudiable charging protocol is to provide an access network with cryptographic evidence that a particular client consumed a certain resource at a particular time at a given price. The access network can then present this evidence to the client's home network when billing them for the client's service usage.

Hash-chain based Non-Repudiation

Overview

The following describes a protocol for payment scheme which uses cryptographically generated tokens (hash chains) and digital signatures to provide non-repudiable charging for subscription based compensation model. [24] first proposed the use of one-way hash chains for one-time password authentication. Subsequently, one-way hash chains have been used as a basic building block for source authentication in multicast groups, payment protocols and in many other security protocols (see e.g. [17], [21]). The solution adapts the ideas in [18].

A one way hash chain is created by recursively applying a one-way hash function to an initial random seed value, e.g., $H^i(x) = H(H^{i-1}(x))$, where x is the initial random seed

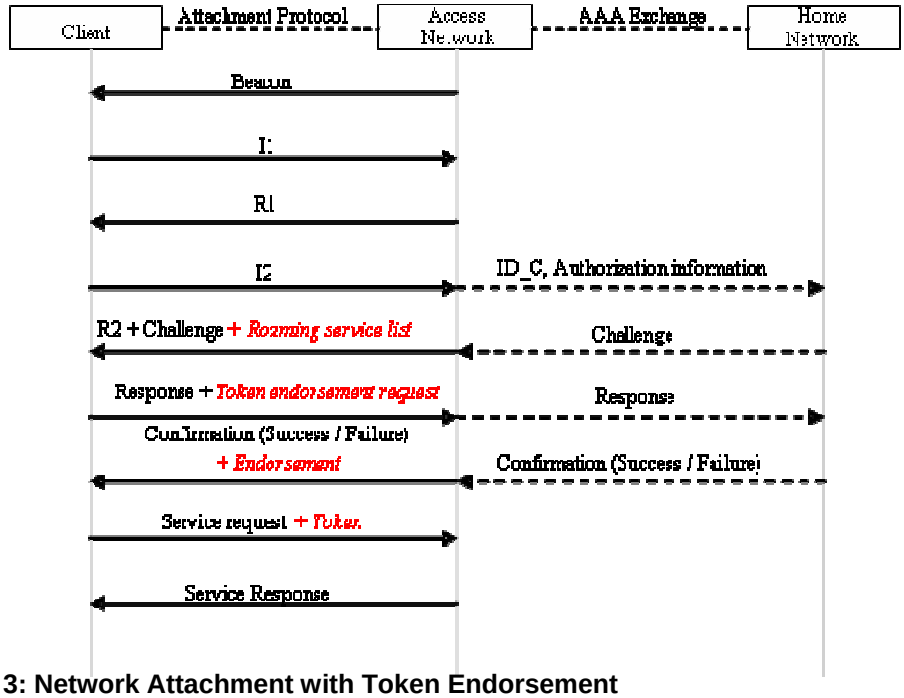

Figure 3: Network Attachment with Token Endorsement

value, H(x) is a one way hash function of x, i = 1,2,3,…n and n is the length of the hash chain. Typically, the user then provides the service provider with whom they wish to use the hash chain with the hash chain anchor, $H^n(x)$, signed with their private key. If the signature can by verified by the service provider (or a trusted third party) and the service request is acknowledged, and the user can "pay" for a service by releasing pre-images of the hash chain anchor, at pre-defined intervals.

In the following protocol no attempt is made to link the tokens (hash chain pre-images), presented by the client to the access network, to a monetary value relevant to the client; instead the tokens are linked (implicitly) to the Inter-Operator Tariff (IOT) values that form part of the roaming agreement between the Operators. The protocol assumes that control of user credit and mechanisms for advice of charge are handled by separate mechanisms. The decision to de-couple the evidence of a client's usage from the charge for that usage is based on the observation that the pricing structure in the subscription agreement between the client and the home network may be different to the IOTs in the roaming agreement between the access network and the home network. Without a linear relationship between these pricing strategies, designing a multi-purpose protocol introduces additional requirements that invariably result in inefficiencies.

Service Usage Protocol

Figure 3 shows a sketch of the general protocol flow, showing how the messages can be piggybacked on the messages used for network attachment protocol. An explanation of the messages is provided below.

The following notation is used for the remainder of this document:

e{K, X} = X encrypted with key K

m{K, X} = MAC function over content X using key K

v{A, X} = Signature of A over X

First, the client and the access network complete the Network Attachment Protocol (NAP) described earlier in this paper (see Figure 1 for details). A shared secret g^{xy} is generated between the client and the access Network. To authorize the client's access the access network completes a AAA exchange with the client's home network using some typical AAA exchange like those provided by EAP. The authentication could happen for example with the help of EAP-AKA that takes advantage of the security mechanisms provided by UMTS [19]. Typically these kinds of procedures would use the existing AAA

protocols like RADIUS [22] and DIAMETER [23] between the access network and the AAA operator. During this exchange the home network must store the binding between the client's temporary and permanent identifiers. Furthermore, the Confirmation message sent by the home network to the access network as part of a successful AAA procedure should include the temporary identity of the client (ID_C) and be signed by the home network (ID_H), e.g.

Access Network ← Home Network

Confirmation message + v{ID_H, (ID_C)}

This is to provide non-repudiable evidence that the home network authorized the client's temporary identity to the access network, which it could otherwise deny and may require extensions to the AAA protocols previously listed. It should be noted that the protocol does not provide a substitute for the protocols required to keep track of a client's credit, e.g., for pre-pay subscriptions.

Once the NAP has been completed, the access network sends the client a list of roaming services (R_A). The Roaming Service List also contains a time or volume based token release frequency (FR) for each service (SV). A service may have multiple token release frequencies, e.g., for different time periods or QoS, in order to allow support flexible pricing models, without requiring an explicit value to be attributed to a token endorsement. This has the advantages of allowing the client to create general use tokens. The roaming service list should also contain an indication of the allowable lifetime for an endorsement, the expiry value (E). This value can also be used by the client to estimate the length of the hash chain to use in the token endorsement request. The signature of the access network covers the entire message.

Client ← Access Network

v{ID_A , (ID_C, ID_A, S, e{ g^{xy}, R_A})}

Where:

R_A = ((SV_0(FR_0 , FR_1 , ...)), (SV_1(FR_0 , FR_1 , ...), ...), E)

Next a Key Derivation function (KDF) is used to derive a Cipher Key (CK) and Integrity Key (IK) from the secret key g^{xy}.

KDF (g^{xy}) = (CK, IK)

These two keys will be used between the client and access network for the non-repudiation of the charging protocol. The creation of the IK also enables the use of a MAC (Message Authentication Code) function to protect the integrity of the messages between the client and the access network, without requiring the use of computationally more expensive digital signatures. The key derivation step is required to provide key separation, e.g. to use separate keys for integrity and encryption functions.

The reader should also note that there also needs to be a cryptographic binding between the keys used to encrypt the non-repudiation protocol and the key(s) used to protect the services being accessed. Without such a binding, replay attacks are possible. This could be as simple as using CK for all services (including the non-repudiation protocol) or might require separate key derivations for each service.

Once the client has received the roaming service list (R_A) from the access network during the NAP, it generates a Token Endorsement Request (see Figure 4). This message contains; the cryptographic identifiers of the client and access network (ID_C and ID_A respectively), the session identifier (S), the list of services and token presentation frequencies presented by the access network (R_A), the hash chain anchor (AR) of a pre-generated hash chain (encrypted with the symmetric key CK) and expiry time (E). The MAC function (m{}) covers the entire message to provide integrity protection.

Client → Access Network

m{IK, (ID_C, ID_A, S, e{CK, (v{ID_C, (ID_A, R_A, AR, E)})}}

R_A is included in this message to ensure that the access network has not changed the presentation frequencies agreed between itself and the home network in the message it presented to the client[1]. ID_A is included in the

[1] This information will be presented to the home network when the access network "cashes" the endorsement. If there is any discrepancy the home network can refuse payment. The access network must check

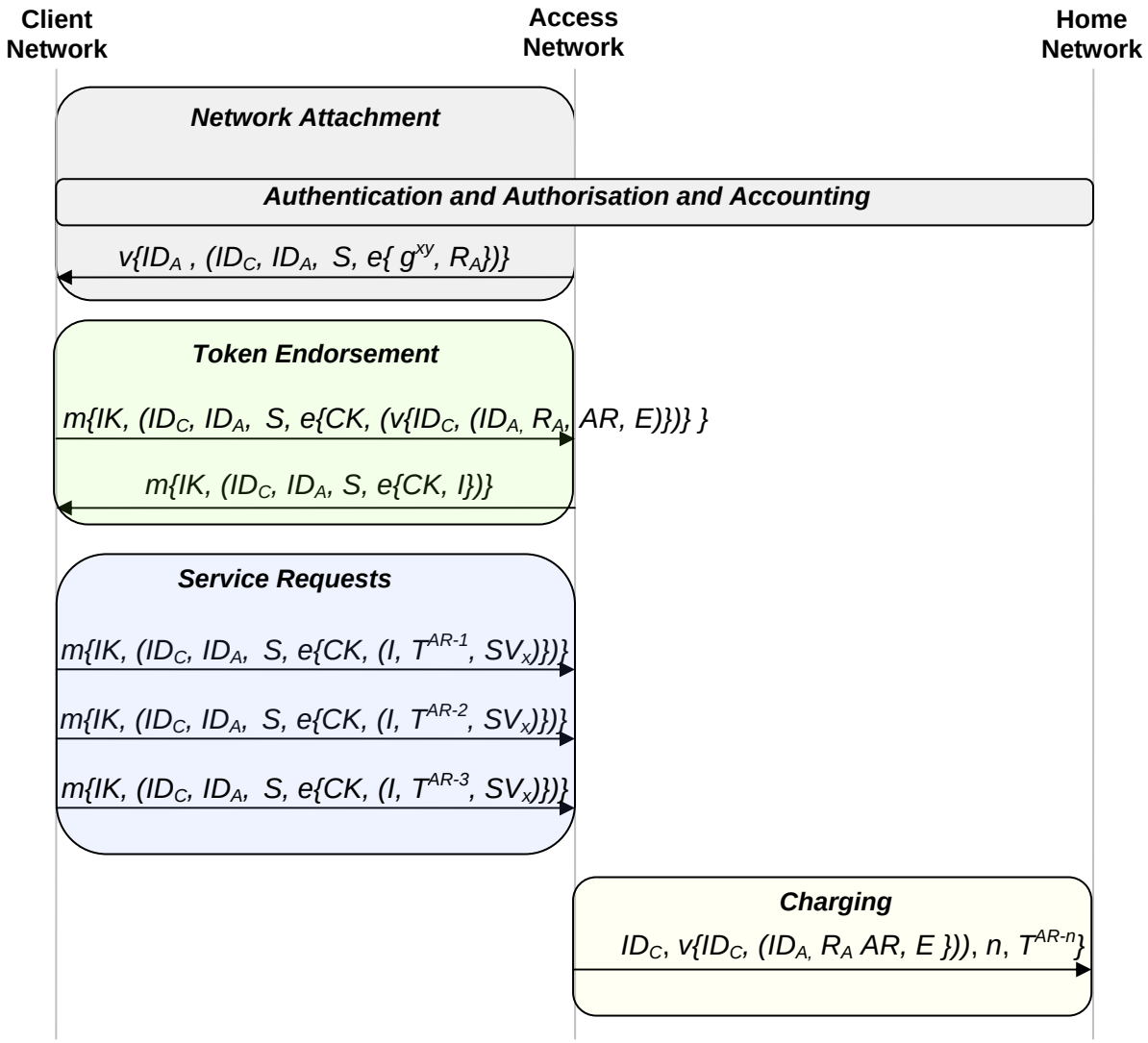

Figure 5: Protocol for Non-Repudiable Charging

payload of the message to stop the endorsement being "cashed" by any other access network than that which issued it. The lifetime of a token endorsement request indicated by the expiry value (E) should be set to match the value provided by the access network in Roaming Service List.

On receiving the token endorsement request, the access network verifies its source and if satisfied replies to the client with an acceptance message. This message includes; the cryptographic identifiers of the client and access network (ID_C and ID_A respectively), the session identifier (S) and an identifier for the endorsement (I) (encrypted with the symmetric key CK). The MAC function (m{}) covers the entire message to provide integrity protection.

Client ← Access Network

m{IK, (ID_C, ID_A, S, e{CK, I})}

The identifier for the endorsement should be constructed such that it is unique to both the client and the access network, e.g. it could be the result of a hash function over the concatenation of AR and ID_C.

When the client wishes to use a service it sends a Service Request message to the access network. This message contains; the cryptographic identifiers of the client and access network (ID_C and ID_A respectively), the session identifier (S), the service ID (SV_X) of the requested service, the endorsement identifier (I) and the next Token available in the endorsed hash chain (T^{AR-1} to T^{AR-L}, where L is the length of the hash chain). Symmetric key CK is used to encrypt the message payload. The MAC function (m{}) covers the entire message to provide integrity protection.

that this value is the correct when contained in the client message.

Client → Access Network

$m\{IK, (ID_C, ID_{A,} S, e\{CK, (I, T^{AR-1}, SV_x)\})\}$

When the access network wants to periodically receive payment for the roaming services that it has provided to the client from the home network, it must submit the necessary evidence within the Charging message. The charging message will therefore include; the client identity (ID_C), the token endorsement request provided by the client ($v\{ID_C, (ID_{A,} R_A AR, E \})$), the number of tokens used by the client (n), and the last token issued by the client (T^{AR-n})[2]. This message should be protected using a pre-establish security association between the access network and the home network (not shown in notation).

Access Network → Home Network

$ID_C, v\{ID_C, (ID_{A,} R_A AR, E \})), n, T^{AR-n}$

To verify the charging information the home network must:

(1) Verify the signature of the client over the token endorsement request.

(2) Be able to link the client's temporary and permanent identifiers.

(3) Check whether the charging information has been provided within the allowable period. This period should be set to be a certain period, e.g. 7 days, after the expiry value of the token endorsement request. This is required to mitigate against the possibility that the access network could generate the pre-images of the hash chain anchor provided by the client and thereby create false billing records[3].

(4) Verify the validity of the hash chain from the hash chain anchor included in the token endorsement request to the final token presented by the client. The number of hash operations required to get from the hash chain anchor to the final token should equal the number of tokens claimed by the access network.

If all of these checks are satisfied the home Network can be confident that a particular client used a specific amount of service with a particular access network.

For efficiency reasons it may be beneficial for a client to continue to use a previously endorsed set of tokens when re-attaching to an access network. During re-attachment the client and the access network once again complete the Network Attachment Protocol. To provide traceability protection against eavesdroppers the client uses a new alias (ID_{C2}). In addition the new encryption and integrity keys (CK_2 and IK_2 respectively) are generated. The client can then prove ownership of the endorsed tokens to the access network by including the previously endorsed endorsement identifier (I) signed using the private key of the identity that the endorsement was granted to (ID_{C1}). The access network could then be confident that the client is the owner of the endorsement (assuming that the client is not able to distribute private keys). The reader should be aware that the benefits provided by the re-use of an endorsement come at the cost of loosing the client's untraceability towards the access network, as the client now provides a link between their old and new identities.

Client → Access Network

$m\{IK_{2,} ID_{C2}, ID_{A,} S, e\{CK_{2,}, (v\{ID_{C1}, I\})\})\}$

Conclusion

In this paper we have presented a solution for attaching a node to a network that does not only take into account securing the initial attachment between two nodes, but also considers the other procedures that are needed in order to provide connectivity service. This includes aspects related to configuring the IP level, and also discusses the importance of compensation, which requires non-repudiation mechanisms to be in place to address the new risks associated with the changing dynamics between operators.

The presented key points of the network attachment procedure were cryptographic identifiers, decoupling of authentication and authorization, delegation and zero configuration. Additionally, it promotes the

[2] If the home network disputes that it has authorised the client to the access network it may also be necessary for the access network to present the Confirmation message containing the Client's temporary identity signed by the home network.

[3] It is felt to be highly unlikely that this type of activity could be profitable for an access network if the value per token is relatively low.

idea that having some of opportunistic security which is better than having no security at all.

With the number of operators expected to continue to increase in the future the different stakeholders can no longer rely on the today's roaming trust model for fraud prevention. Therefore, there is a need for mechanisms that enable non-repudiation in terms of service usage. We described one way of using hash chains as non-repudiable indication of service usage between a client and access network that also gives guarantees to the service provider that the service usage can not be disputed by the client or the home network.

By combining the above procedures we are able to provide a consistent and simple solution that is both secure and minimizes roundtrips and takes into account also the business model aspects of the network attachment.

REFERENCES

[1] Droms R., Arbaugh W. Authentication of DHCP Messages. IETF RFC 3118. 2001

[2] Cantor S., Kemp J., Philpot R., Maler E., Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. 2005

[3] Ellison C. et al. SPKI Certificate Theory. IETF RFC 2693. 1993

[4] Asokan, N., Niemi, V. and Nyberg, K. Man-in-the-middle in tunnelled authentication in http://eprint.iacr.org/2002/163/, 2002.

[5] Moskowitz, R., Nikander, P., Jokela, P. and Henderson, T. Host Identity Protocol. Internet Draft draft-ietf-hip-base-04 (Work in Progress), IETF. 2005

[6] Kaufman C. (ed). Internet Key Exchange (IKEv2) Protocol. Internet Draft draft-ietf-ipsec-ikev2-17 (Work in Progress), IETF. 2004

[7] Ylonen, T., Lonvick C. SSH Protocol Architecture. Internet Draft draft-ietf-secsh-architecture-22. 2005

[8] Blunk L., Vollbrecht J. PPP Extensible Authentication Protocol (EAP). IETF RFC 2284. 1998

[9] Heikkinen, S. Tschofenig, H., and Gelbord, B. Network Attachment and Address configuration using HIP. Workshop on HIP and Related Architectures, Washington DC. 2004

[10] Arkko J., Eronen P., Tschofenig H., Heikkinen S., Prasad A. Quick NAP - Secure and Efficient Network Access Protocol. (to appear)

[11] Ambient Networks WP7. Deliverable D7-2 Ambient Network Security Architecture. 2005 (to be published)

[12] Arkko, J., Eronen, P., Nikander, P. and Torvinen, V. Secure and Efficient Network Access. Extended abstract presented in the DIMACS workshop , NJ, USA. 2004

[13] Johnson D., Perkins C., Arkko J. Mobility Support in IPv6. IETF RFC 3775. 2004

[14] Aura T. Cryptographically Generated Addresses (CGA). IETF RFC 3972. 2005

[15] Faria D, Cheriton D. DoS and Authentication in Wireless Public Access Networks. ACM Workshop on Wireless Security. 2002.

[16] Droms R., Dynamic Host Configuration Protocol. IETF RFC 2131. 1997

[17] Tewari H., O'Mahon D. Multiparty micropayments for Ad Hoc Networks. Proceedings of the IEEE Wireless Communications and Networking Conference. 2003

[18] Zhou J., Lam. K. Undeniable Billing in Mobile Communication. Proceedings of 4th ACM/IEEE International Conference on Mobile Computing and Networking. 1998

[19] Arkko, J. and Haverinen, H. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA).Internet Draft draftarkko-pppext-eap-aka-15 (Work In Progress), IETF. 2004

[20] Diffie W., Hellman M.E. New directions in cryptography. IEEE Transactions on Information Theory 22. 1976

[21] Blaze M. et al. TAPI: Transactions for Accessing Public Infrastructure. Proceedings of Personal Wireless Communications (PWC 2003). 2003

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

[23] Calhoun P., Loughney J., Guttman E., Zorn G., Arkko J. Diameter Base Protocol. IETF RFC 3588

[24] Lamport L. Password authentication with insecure communication.Communications of the ACM, vol. 24, no. 11. 1981.