Secure and Efficient Network Access

Jari Arkko[1], Pasi Eronen[2], Pekka Nikander[1], and Vesa Torvinen[1]

[1] Ericsson Research NomadicLab, firstname.lastname@nomadiclab.com
[2] Nokia Research Center, firstname.lastname@nokia.com

Extended abstract – August 31, 2004

1 Introduction

The protocol stacks currently used for network access have a number of limitations, such as long attachment and movement latencies [1] (an attachment typically requires over twenty link and IP layer messages), denial-of-service vulnerabilities, difficulties in trusting a set of access nodes distributed to physically insecure locations, and so on.

A number attempts are currently being made to improve the efficiency, security and functionality of network access, particularly with mobile nodes. These attempts include link-layer enhancements, parameter tuning [8], network access authentication mechanisms (such as IEEE 802.1X), fast handover mechanisms [5, 2], and IP layer attachment improvements (such as Optimistic DAD [6]).

This extended abstract sketches a new architecture that deviates from current designs. We claim that instead of focusing on a single layer (link-layer) or a single function (authentication), it is necessary to look at the problem as a whole: what tasks are necessary in order to have a node attach to a network? How can that node move into another attachment point? What nodes need to communicate with what other nodes, and when? What is the best order of the tasks so that the number of roundtrips is minimized? Are there tasks that need to be securely bound together, such as IP address address assignments and QoS, ingress filtering, or local mobility services?

Our design ideas deal with the different aspects of the network access problem, are efficient in terms of roundtrips and radio resource usage, capable of fast movements, have high resistance to denial-of-service attacks, and protect the privacy of the participants. Lessons from protocols such as IKEv2 [4] and HIP [7] have been used.

From a high-level point of view, an attachment to a network consists of a transaction between the mobile node, access node, router, access network, home network, possibly some mediating networks, and possibly also some mobility related nodes such as home agents. Some of these entities, such as access networks, are not explicitly addressed or identified in current designs. Similarly, home-network based authentication mechanisms authenticate access nodes only indirectly.

2 The Proposed Architecture

All involved parties are explicitly identified with a hash of their public key. These hashes replace conventional MAC addresses, and serve as a convenient mechanism to bind the entities to their identities securely. The public keys of the nodes can be generated by themselves and do not need a PKI. Identity privacy is supported through ephemeral public keys, since long-term identifiers should be avoided especially in devices such as cellular phones where the radio part is always active.

For efficiency, tasks can be delegated to the network devices, reducing expensive radio roundtrips. These tasks need not be related to the link layer processing only. For instance, the mobile node can request the access node to allocate an IP address or inform the mobile node's home agent about the current location. The mobile node provides the basic information necessary to perform these tasks (such as interface identifier) and, depending on the task, signs a certificate to delegate the right for this specific task to the access node, making various delegated tasks possible (cf. [3]).

Rich information needs to be delivered to clients both during the network attachment or later (for handoff guidance or advice of charge purposes, for instance), signed by the party that owns the information. Caching at local access nodes speeds up the process of retrieving information from further away in the network. All information should be represented in the same extensible syntax (such as XML) and compressed for over-the-air transmission.

3 Example

In the following we sketch a possible protocol run:

This document has been produced partially in the context of the Ambient Networks Project. The Ambient Networks Project is part of the European Community's Sixth Framework Program for research and is as such funded by the European Commission. All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability in respect of this document, which is merely representing the authors view.

1. The access node sends a beacon message, identifying itself with the hash of its public key. It also sends along information affecting the attachment decision that it wants to advertise, such as what payment models it supports, what roaming partnerships it has, what subnets it can provide fast roaming with, and what middlebox services it offers.

2. The client and the access node initiate an attachment procedure. A Diffie-Hellman exchange is run as early as possible to protect all subsequent communications, including all management operations and negotiations. This also enhances the privacy of the participants.

   This procedure can be modeled after protocols such as IKEv2 or HIP. For instance, the uses a two roundtrip exchange, where the responder (access node) can stay stateless until the client has proven its commitment to by solving a puzzle, the client's identity can be kept hidden until the server has been authenticated, and link-layer encryption keys can be derived as a side-effect of this exchange.

   In this phase the client and the access node also authenticate the claimed hash-based identities to ensure that the peer actually knows the private key corresponding to the public key used in the hash.

3. The next task is to establish that the access node is trusted by the client to offer the services it claims to. Usually, this is achieved through the home network vouching for this. However, due the use of the hash-based identities, also pre-provisioned database or certificates sent in the beacon message are possible.

4. In parallel with the above task, the access node verifies that the client is authorized to get the services. Authentication and authorization of the user (not the device) can involve other parties beyond the access node. Depending on the capabilities of the involved nodes, this can be based on micropayments, authorization certificates, or other existing user credentials.

5. The client may also request services beyond connectivity. The requests for these services are independent of each other, and can be addressed to specific entities, all in parallel with the above. For instance, the client may request the access node to perform IP address allocation on its behalf or return a ticket that allows the client to open pinholes in a local firewall or a NAT. The client may also create a certificate that delegates the access node to send a binding update to a home agent on the behalf of the client.

6. This channel for communication between the client and other nodes can also be used after access has been granted. For instance, it can be used for periodic micro-payments, or for notifying the user that his pre-paid balance is running low.

4 Fast Handoffs

We define the access network to be the area within which fast handoffs are possible. Beacons transmit the identity of the access network as one of the advertised properties. In the initial authorization phase an access node sends two certificates to the client: the first certificate is signed by the access network, and tells that the access node is a part of the access network. The second certificate is signed by the access node and tells that this particular client is allowed to perform a fast handoff with a given set of explicitly listed authorization parameters (cf. [3]).

Upon contacting a new access node, the client performs the initial Diffie-Hellman exchange, but does not proceed with the home-network based authorization process. Instead, it presents the certificates it obtained from the first access node. The new access node inspects these certificates for validity, and ensures that the requested service falls within the defined authorization parameters. This makes handoffs possible without a prior setup phase needed in [2]. (Note that certain authorization parameters, such as concurrent session limits may require monitoring that can not be achieved on a single access point alone. In this case a message is sent further on to the network to ensure that such parameters have been obeyed.)

References

[1] Alimian, A. and Aboba, B. Analysis of Roaming Techniques. IEEE 802.11 WG, document 802.11-04/0377r1, 2004.

[2] Arbaugh, W. and Aboba, A. Handoff Extension to RADIUS. Internet Draft draft-irtf-aaaarch-handoff-04.txt (Work In Progress), IRTF, October 2003.

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

[4] Kaufman, C. (Ed.) Internet Key Exchange (IKEv2) Protocol. Internet Draft draft-ietf-ipsec-ikev2-14.txt (Work In Progress), IETF, May 2004.

[5] Mishra, A., Shin, M., Arbaugh, W., Lee, I. and Jang, K. Proactive Key Distribution to support fast and secure roaming. IEEE 802.11 submission IEEE-03-084r1-I, January 2003.

[6] Moore, N. Optimistic Duplicate Address Detection for IPv6. Internet Draft draft-ietf-ipv6-optimistic-dad-01.txt (Work In Progress), IETF, June 2004.

[7] Moskowitz, R., Nikander, P., Jokela, P., Henderson, T. Host Identity Protocol. Internet Draft draft-ietf-hip-base-00.txt (Work In Progress), IETF, June 2004.

[8] Velayos, H. and Karlsson, G. Techniques to Reduce IEEE 802.11b MAC Layer Handover Time. Laboratory for Communication Networks, KTH, Royal Institute of Technology, Stockholm, Sweden, TRITA-IMIT-LCN R 03:02, April 2003.