Presented at IFIP-SEC
2006, Karlstad Sweden
(Springer IFIP series)
ISSN 1571-5736

Secure Fast Handover in an Open Broadband Access Network using Kerberos-style Tickets

Martin Gilje Jaatun[1], Inger Anne Tøndel[1], Frédéric Paint[2], Tor Hjalmar Johannessen[2], John Charles Francis[3], and Claire Duranton[4]

[1] SINTEF ICT, Trondheim, Norway
[2] Telenor R&D, Fornebu, Norway
[3] Swisscom Innovations, Bern, Switzerland
[4] France Telecom R&D, Issy-les-Moulineaux, France
Martin.G.Jaatun@sintef.no

Abstract. In an Open Broadband Access Network consisting of multiple Internet Service Providers, delay due to multi-hop processing of authentication credentials is a major obstacle to fast handover between access points, effectively preventing delay-sensitive interactive applications such as Voice over IP. By exploiting existing trust relationships between service providers and access points, it is possible to pre-authenticate a mobile terminal to an access point, creating a Kerberos-style ticket that can be evaluated locally. The terminal can thus perform a handover and be authenticated to the new access point, without incurring communication and processing delays by involving other servers.

1 Introduction

The Open Broadband Access Network (OBAN) [1] seeks to utilise excess capacity available in residential broadband connections, by opening up private wireless access points to passers-by. It is intended as a multi-ISP network, where a roaming OBAN user may consume mobile IP services from residential wireless access points regardless of whether or not he has a contract with the same ISP as the residential user. In addition to serving as a lower-cost, higher-bandwidth alternative to services such as UMTS [2] or WiMAX [3], OBAN also intends to incorporate multi-lateral roaming agreements [4] towards such services, in effect creating a ubiquitous, world-wide network. A more detailed description of the OBAN concept can be found in [5] and [6].

1.1 Problem Definition

The ISP that the OBAN user has a subscription with is known as the OBAN Service Provider (OSP), while the ISP of the residential user (and access point) is known as ISP_{RU}. When the OBAN user wishes to use a residential network connected to an ISP_{RU} that is different from his/her own, the AAA[5] server of

[5] "Triple-A": Authentication, Authorisation and Accounting - e.g. RADIUS [7].

ISP_{RU} must act as a proxy toward a AAA server in the OSP's domain, since only the OSP can verify the OBAN user's credentials. However, this creates a problem with respect to executing the handover fast enough for the user to experience a seamless service [4]: Since the authentication protocol requires multiple round trips between several servers that potentially are situated physically far from each other, communication delays alone make it impossible to meet the requirement of a maximum handover latency of 120 ms[6].

1.2 Tickets to the Rescue

While a full authentication at every handover thus is unacceptably slow, the residential users and ISPs are unlikely to be enthusiastic about letting strangers with whom they have no prior trust relationship avail themselves of their networking resources without any form of access control. In order to solve this conundrum, we have to make use of trust relations that are already in place.

In a typical AAA configuration, the AAA server needs to be in possession of a shared secret with the 802.1X [9] authenticator; among other reasons in order to be able to securely communicate the session key that has been established as part of the authentication process between terminal and AAA server. This shared secret can be exploited to create a Kerberos-style ticket [10] that can be used to authenticate a terminal during handover, without on-line involvement of the OSP AAA server. The ticket will in effect represent a dynamic trust relationship between the terminal and the access point. Note that in contrast with the solution suggested in [11], the use of a Kerberos ticket does not require a mobile user to have visited the access point previously, nor does it require a trust relationship between access points.

2 Fundamental Components

Our solution to the fast handover problem requires some components that are briefly described in the following.

2.1 Residential Gateway

The most important hardware component of the OBAN network is the Residential Gateway (RGW), which among other things contains a RADIUS server. This RADIUS server will be responsible for verifying the Kerberos tickets, but will in all other respects act as a proxy toward the Mobility Broker (MB – see below). The RGW is placed as a gateway between the wireless access point and the fixed broadband connection.

[6] 120 ms is chosen as a conservative threshold for interactive applications such as Voice over IP, although computer networking textbooks such as [8] state that delays can be up to 150 ms without being perceived by a human listener.

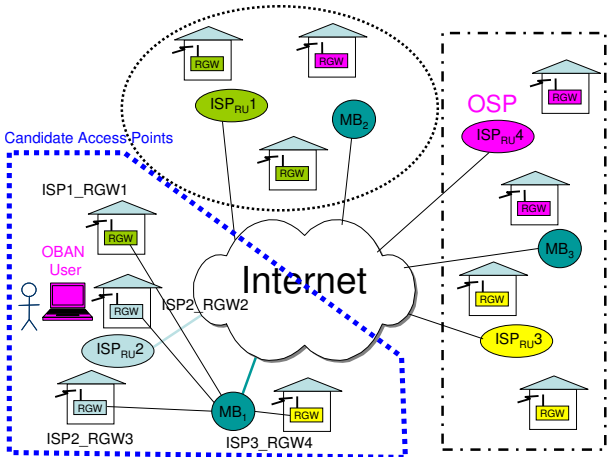

Fig. 1. An OBAN network with 3 Mobility Brokers

The 802.1X authenticator in the wireless access point must be configured in pass-through mode, with the embedded RADIUS server in the RGW as Authenticaton Server.

For simplicity, the term RGW may be in the following be interpreted as "RGW and access point".

2.2 Full Authentication

When a terminal first joins the OBAN network (i.e. when it is switched on), an OBAN user will not find it unreasonable that the connection process takes a fairly substantial amount of time; this is already the case when you turn on a GSM phone upon arriving in a new country.

Due to the desire to enable interoperability between OBAN and existing wireless communication networks, EAP-SIM [12] has been chosen as the full authenticaton method in OBAN. However, any EAP method that conforms to [13] could in theory be used.

2.3 Pre-authentication

A Kerberos ticket can be seen as a sort of letter of recommendation, where the recipient of the ticket doesn't know the sender; but since the recipient trusts the entity that created the ticket, it can also trust the sender. Prior to generating the ticket, the issuer will authenticate the terminal. This can be seen as a form of pre-authentication, where all the tedious work (with associated delays) is performed.

2.4 Mobility Broker

A ticket-based solution for fast handover *could* have been implemented using only existing infrastructure of ISP_{RU}s and OSPs, but to ease information gathering with respect to candidate access points, the Mobility Broker (MB) has been introduced as a new network component with respect to [6]. The MB is a neutral party that has a direct trust relationship with all ISPs in a given geographical area, and also a direct trust relationship with all the corresponding RGWs. For our purposes, the MB has three main functions:

- Serve as AAA proxy toward ISP_{RU} for full authentication
- Provide information about nearby access points via the CARD protocol [14]
- Issue Ticket-Granting Tickets (TGT) and access tickets to OBAN terminals.

Each MB will in effect represent the hub of a geographical "cell", as depicted in Fig. 1. This is analogous to base stations in e.g. GSM networks. A terminal should then be able to get TGTs for all ISPs in a given cell with a single full authentication.

Every RGW in the cell must have the MB configured as (proxy) authentication server. This also means that the MB will need to have a shared secret with each RGW in its cell. The MB must also have a shared secret with every ISP_{RU} in the cell, and will pass all authentication requests on to the relevant ISP_{RU}'s (proxy) AAA server. This implies that the MB cannot reside in the administrative domain of a single ISP, if there are other participating ISPs in the relevant cell. All tickets will be issued by the MB, regardless of which ISP_{RU} a given RGW belongs to. Handover between cells (i.e. from one MB to another) will then be a special case that for now requires a new full authentication[7].

Since the MB has complete overview of the terminal's geographical location, and also the location of all RGWs in its cell, the terminal does not need to identify candidate RGWs in order to get tickets for them; the MB already knows.

2.5 Brief Review of the Kerberos Ticket Concept

A Kerberos ticket consists primarily of an access key[8] and timestamp information which are encrypted with a (long-term) key known only to the issuer and to the final recipient. When the ticket is issued to the terminal, it must thus be accompanied by a structure that contains the same access key, but which is encrypted with a key that is in the possession of the client. Thus, what the terminal receives looks approximately like this:

$$E_{K_{terminal}}[AccessKey] + E_{K_{RGW}}[AccessKey, Timestamp]$$

[7] However, current efforts are looking into options that involve "make-before-break" session establishment using e.g. UMTS networks when transitioning between cells.

[8] In traditional Kerberos notation, the key embedded in the ticket is referred to as the *session key*; however, in an OBAN context, this is too easily confused with the session key for encryption of the wireless traffic; hence the name change.

Kerberos actor	OBAN party
AS (Authentication Server)	Mobility Broker (proxy toward OSP via ISP_{RU})
TGS (Ticket Granting Server)	Mobility Broker
C (Client)	OBAN user (terminal)
V (serVice granting server)	RGW

Table 1. Mapping from Kerberos to OBAN

When the client uses the ticket for authentication, it must prove to the recipient (e.g. the RGW) that it possesses the access key within the ticket. It does this by generating an authenticator[9] message; primarily by encrypting a challenge from the RGW (and some other information) with the access key. The recipient verifies this message, and if the timestamp in the ticket indicates that it has not expired, the recipient considers the client authenticated.

The possession of an access key in a TGT thus implicitly grants the OBAN user the right to request tickets for nearby RGWs; the possession of an access key in an RGW ticket grants the OBAN user access to the wireless access network.

The Kerberos tickets will have a limited validity, and we are assuming that it will be in the OBAN users' self interest to keep the access keys secret (i.e. that OBAN use is metered). If a flat-rate business model were to be applied to OBAN, however, additional misuse detection mechanisms (akin to the ones used to detect cloned cell phones) must be deployed.

Note that we don't attempt to create a full-blown multi-realm Kerberos authentication system, but in effect multiple disjoint Kerberos realms, based on each Mobility Broker. In the following, we assume that the reader is familiar with the Kerberos protocol (see e.g. [10] or [15]).

In Table 1 we provide a mapping from Kerberos terms to their respective OBAN counterparts. The fact that both the role of AS and TGS is assumed by the MB is no anomaly in Kerberos terms; this occurs so often that the combined AS-TGS pair frequently is referred to as the Key Distribution Centre (KDC).

3 Assumptions

The Kerberos-style ticket solution relies on some fundamental assumptions that will be elaborated below.

Pre-shared Secret: A fundamental assumption is that the access point (i.e., RGW) shares a secret with the AAA server. This is typically the case in a situation where 802.1X [9] is employed in conjunction with RADIUS [7].

Minimum Stay: The terminal needs to exhibit a "minimum stay-time" at each RGW, i.e. it has to stay connected for a certain minimum of time before moving on. The minimum stay is defined as the time required by the terminal to acquire all necessary tickets prior to the handover. Thus this minimum

[9] Not to be confused with the 802.1X authenticator.

time period will be longer or shorter depending on how many tickets are requested, which in turn depends on how well we can predict which RGW we will hand over to next. Depending on the expiry times of the tickets, a terminal may also already possess tickets for many candidate RGWs for $handover_{n+1}$ when it performs $handover_n$; this will reduce the minimum time between these two handovers.

Loosely Synchronised Clocks: Kerberos assumes that all participants have roughly the same idea of what the current time is, while allowing for a certain (configurable) clock skew. This is used to prevent replay of Kerberos authenticators, which must always be "fresh".
There is currently no automatic mechanism to ensure this loose synchronisation, but future investigations will show whether it will be possible to achieve it as a side-effect of the initial full authentication towards OSP.

4 Informal Description

In this section we provide an informal verbal description of the different phases of authentication in OBAN. The actors involved are depicted in Fig. 2.

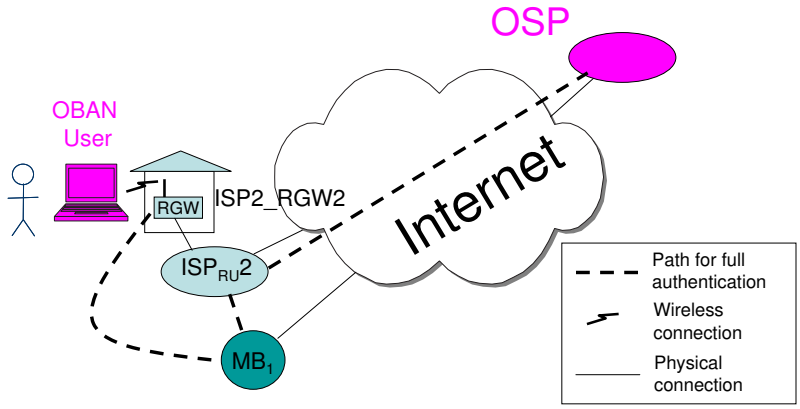

Fig. 2. OBAN actors involved with initial authentication

4.1 Initial Authentication

1. The RGW will always request authentication with a ticket when a new OBAN user arrives.
2. If the user has no ticket (i.e. this is a new session, not a handover), it will reply with an EAP-NAK.

3. Upon receipt of an EAP-NAK (or an expired ticket), the RGW will initiate a "normal" authentication using the preferred OBAN authentication protocol (e.g. EAP-SIM). This will be proxied by the RGW toward the Mobility Broker, which in turn will act as a proxy towards $\mathrm{ISP_{RU}}$, which finally proxies the messages towards OSP.
4. Upon successful completion of the EAP-SIM authentication, the OSP will issue an EAP-SUCCESS, which is forwarded back to the terminal via $\mathrm{ISP_{RU}}$, MB and RGW.

At this point, the terminal is authenticated, and may communicae towards the MB and the rest of the Internet.

4.2 TGT Acquisition

Once the terminal has authenticated successfully, it needs to get information on nearby RGWs, and get a TGT if it doesn't have one.

1. Upon completion of the normal authentication, the terminal will issue a CARD request, which will be forwarded to the mobility broker.
2. The MB will reply with information on nearby access points, including an URI indicating where the terminal may obtain the required tickets.
3. If the terminal does not possess a TGT for this MB, it will then initiate a new EAP-SIM authentication directly toward the MB, which will roughly assume the role of 802.1X authenticator, using $\mathrm{ISP_{RU}}$ as (proxy) authentication server. This EAP-SIM authentication will be encapsulated in HTTP messages[10]. Upon completion of this exchange, the MB and the terminal will have established a shared secret. This shared secret will be used in the following instead of the traditional long-term Kerberos key (i.e. password).
4. Upon successful completion of the second EAP-SIM authentication, the MB will issue a Ticket-Granting-Ticket (TGT) to the OBAN user. The shared secret is used to protect the Kerberos TGT access key that is transmitted back to the user along with the ticket.

The terminal is now in a position to request tickets for candidate RGWs.

4.3 Ticket Acquisition

1. The OBAN user will use the TGT to request a service ticket for the RGW (TicketRGW), using HTTP. From the CARD response above, it already possesses one or more URIs for requesting tickets. This ticket will contain a new access key to be used to encrypt the air interface[11]; the new access key is also transmitted to the OBAN user encrypted with the *TGT access key*. The ticket itself is encrypted with the (permanent) shared secret between RGW and MB.

[10] In theory, any suitable encapsulation protocol may be used.

[11] Strictly speaking, the access key will be used to *derive* the key that is used for traffic encryption.

2. MB returns TicketRGW to the OBAN user.

The terminal is now ready to perform a handover.

4.4 Ticket Usage

After the handover takes place, the OBAN user can now reply to the EAP-Request/Kerberos-OBAN with a ticket. The new RGW will verify the ticket, and admit the OBAN user without needing to communicate with any other parties.

5 Detailed Protocol Description

The following Message Sequence Charts (MSC) describe the EAP-Kerberos-OBAN protocol in detail, using EAP-SIM as full authentication protocol, with RADIUS as AAA-protocol. Note that the new EAP method EAP-Kerberos-OBAN strictly speaking only covers the description in section 5.4, but it is of course not particularily useful without the supporting encapsulated mechanisms for acquiring tickets.

In the following illustrations, protocol elements that are new with respect to commonly available solutions are highlighted using `red courier text`. In each MSC, actors that do not participate in the message exchanges are identified by rounded corners and grey fill colour.

5.1 Start and Identity

To limit the size of the MSCs, the EAPOL-Start message has been omitted. Since the Kerberos ticket contains a (pseudonym) ID, the EAP-Request/identity and EAP-Response/Identity have generally been removed from the protocol; the identity message is only needed for the "full" authentication, in order to identify the OSP of the terminal.

5.2 First-time Authentication

When a terminal is first switched on, the chosen RGW will request a Kerberos ticket, but the terminal doesn't have one, and replies with an EAP-NAK (Fig. 3). The RGW then initiates a full authentication pretty much as it would have done in the case of common enterprise authentication systems in use today (for brevity, the standard EAP-SIM messages are omitted from Fig. 3, see [16], [12] and [17] for further details).

When the first EAP-SIM authentication is complete, the terminal will request CARD information from the RGW (again, not shown for brevity). The terminal will then realise that it has no TGT for this MB, and initiate a second EAP-SIM authentication encapsulated in HTTP by sending a "TGT start" message. This authentication process results in the establishment of a shared secret between MB and terminal that is used to encrypt the TGT access key (randomly created by MB) that is transmitted along with the TGT in the final message.

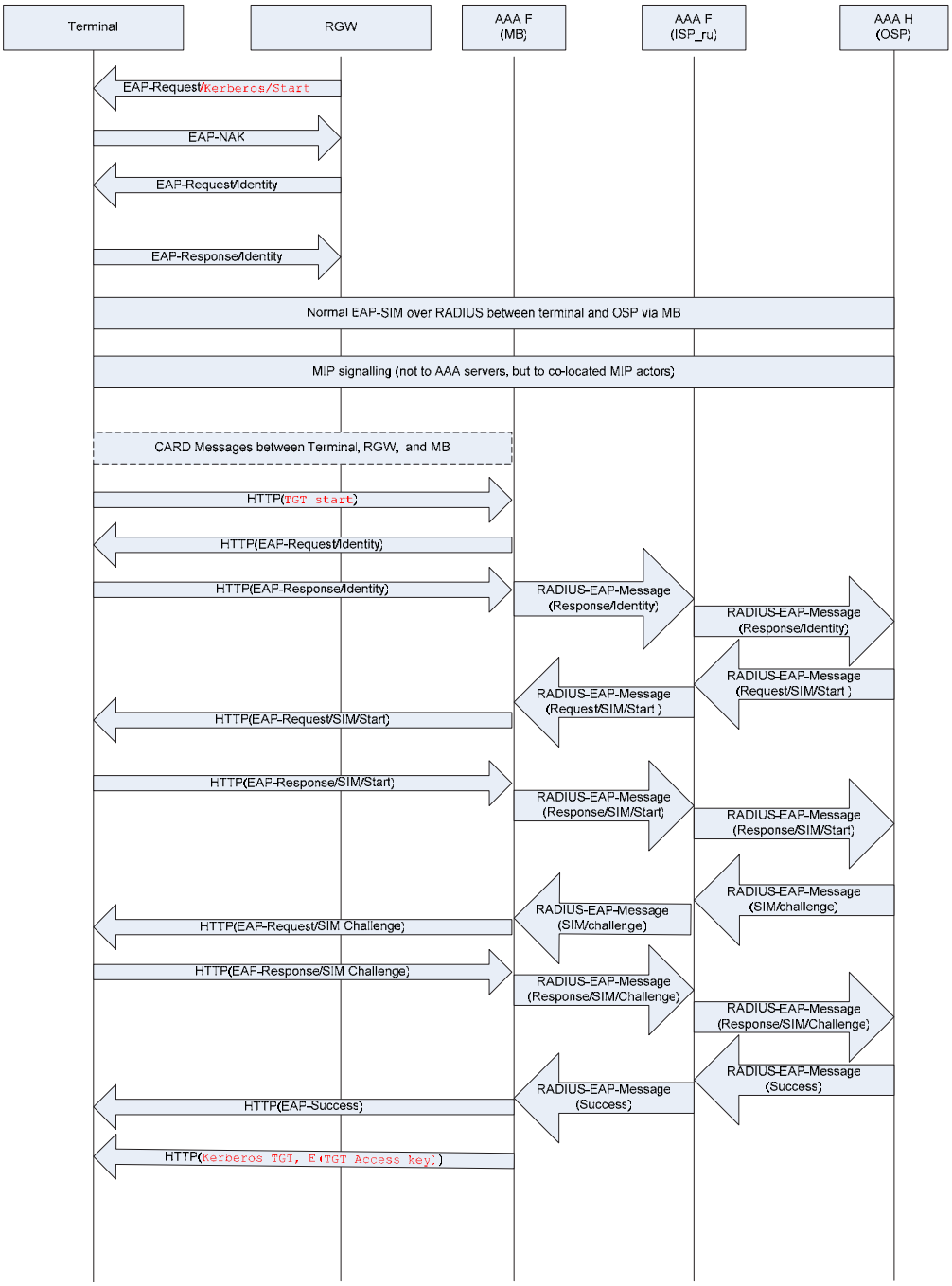

Fig. 3. Messages for initial authentication of OBAN Terminal

5.3 Ticket Request

Once the terminal has a valid TGT, the MB will issue service tickets to RGWs without bothering ISP_{RU} or OSP. In the messages previously received from the CARD server, URIs for requesting tickets for relevant RGWs are listed. Each URI will require the sequence depicted in Fig. 4, but multiple requests may of course be carried out in parallel.

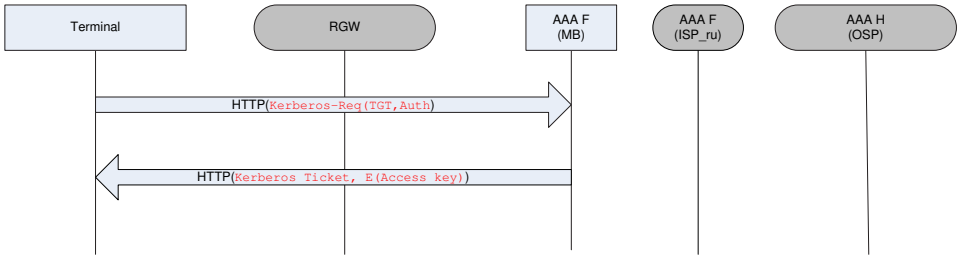

Fig. 4. Messages for requesting access tickets

5.4 Ticket Authentication

The message exchange in Fig. 5 illustrates the EAP-Kerberos-OBAN method, as it would be observed immediately after the terminal has associated with a new RGW. The terminal transmits the appropriate ticket along with a Kerberos authenticator (see section 2.5). Note that only the terminal and the RGW are involved in the authentication process.

5.5 Delay Estimation

During handover, only one[12] Round-Trip Time (RTT) is needed between the terminal and the RGW to achieve necessary layer 2 authentication of the terminal to the RGW. According to our preliminary studies, this RTT can be estimated to 5 ms in the best case scenario, and to 20 ms in the worst case scenario. In addition there will be some processing delay (decryption and evaluation of the ticket). Kerberos uses symmetric encryption, and thus Triple-DES can be viewed as a reasonable worst-case scenario with respect to algorithm efficiency. In this case decryption delay will be 108 clock cycles per encrypted byte[15]. Even with a low-end modern processor, this delay should be negligible. If AES is used (something that is preferable), the delay will be even smaller.

[12] This excludes the EAPOL/Start message, since it is present for all solutions.

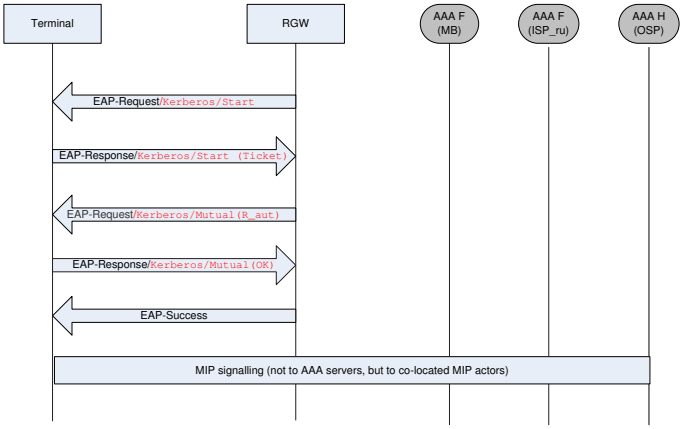

Fig. 5. MSC for Authentication with Ticket

The current description of the EAP-Kerberos-OBAN method requires an additional RTT to achieve mutual authentication of terminal and RGW. The delay due to authentication will therefore lie between 10 ms and 40 ms plus a negligible processing delay.

6 Mobility

The alert reader will have noticed that our proposed scheme only covers L2 authentication and encryption issues in connection with a handover. This implies that additional mechanisms must be applied to ensure that e.g. Mobile IP [18] sessions are retained during handover. This is the subject of ongoing research.

7 Conclusion

Kerberos-style tickets offer an opportunity for achieving fast, secure handover in wireless open broadband access networks. This paper has proposed a new EAP method, EAP-Kerberos-OBAN, which can be used to authenticate a roaming user to an access point without requiring communication with external servers, and without requiring a pre-existing trust relationship between the terminal and the access point.

Acknowledgments

This paper is based on joint research in the EU 6^{th} framework programme. The authors would like to thank all the participating OBAN partners for their

contribution to the fast handover effort. Special thanks to Frans Panken (Lucent Technologies Netherlands) for first suggesting the use of tickets for fast handover, as well as proposing to separate ticket acquisition from the initial authentication.

References

1. OBAN Consortium. [Online]. Available: http://www.ist-oban.org
2. J. F. Huber, D. Weiler, and H. Brand, "UMTS, the mobile multimedia vision for IMT 2000: a focus on standardization," *IEEE Communications Magazine*, vol. 38, no. 9, pp. 129–136, 2000.
3. *IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, IEEE Std. 802.16-2004, 2004.
4. F. Steuer, M. Elkotob, S. Albayrak, H. Bryhni, and T. Lunde, "Seamless Mobility over Broadband Wireless Networks," in *Proceedings of 14th IST Mobile & Wireless Communications Summit*, 2005.
5. E. Edvardsen, T. G. Eskedal, and A. Årnes, "Open Access Networks," in *INTERWORKING*, ser. IFIP Conference Proceedings, C. McDonald, Ed., vol. 247. Kluwer, 2002, pp. 91–107.
6. M. G. Jaatun, I. A. Tøndel, M. B. Dahl, and T. J. Wilke, "A Security Architecture for an Open Broadband Access Network," in *Proceedings of the 10th Nordic Workshop on Secure IT Systems (Nordsec)*, 2005.
7. C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865, June 2000.
8. J. F. Kurose and K. W. Ross, *Computer Networking - A Top-Down Approach Featuring the Internet*. Addison-Wesley, 2001.
9. *Port-Based Network Access Control*, IEEE Std. 802.1X-2001, 2001.
10. C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service (V5)," RFC 4120, July 2005.
11. T. Aura and M. Roe, "Reducing Reauthentication Delay in Wireless Networks," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, 2005.
12. H. Haverinen and J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Subscriber Identity Modules (EAP-SIM)," RFC 4186, January 2006.
13. D. Stanley, J. R. Walker, and B. Aboba, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs," RFC 4017, March 2005.
14. H. Chaskar, D. Funato, M. Liebsch, E. Shim, and A. Singh, "Candidate Access Router Discovery (CARD)," RFC 4066, July 2005.
15. W. Stallings, *Cryptography and Network Security - Principles and Practices*. Prentice Hall, 2003.
16. B. Aboba, L. J. Blunk, J. R. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (EAP)," RFC 3748, June 2004.
17. B. Aboba and P. R. Calhoun, "RADIUS (Remote Authentication Dial In User Service) support for Extensible Authentication Protocol (EAP)," RFC 2865, June 2000.
18. C. E. Perkins, "Mobile IP," *IEEE Communications Magazine*, vol. 40, no. 5, pp. 66–82, 2002.