Presented at
Nordsec 2005

A Security Architecture for an Open Broadband Access Network

Martin Gilje Jaatun,
Inger Anne Tøndel,
and Maria Bartnes Dahl
SINTEF ICT
Trondheim, Norway
Email: Martin.G.Jaatun@sintef.no

Thomas J. Wilke
PRZ
Technische Universität Berlin
Berlin, Germany
Email: tjw@prz.tu-berlin.de

October 12, 2005

Abstract

Europe is experiencing a rapid growth in residential broadband coverage, but due to usage patterns and cost structures, only a fraction of the available bandwidth is actually being consumed. This implies that most residential broadband subscribers have excess capacity, and the idea of the Open Broadband Access Network (OBAN) project is that this capacity can be shared with passers-by.

In order for the residential broadband subscribers to open up their networks, and for the potential wireless customers to sign up for OBAN service, the security of both parties must be ensured. OBAN needs to solve the problems posed by the fact that a visiting OBAN user and a residential access point operator have no pre-existing trust relationship. This paper describes an architecture that achieves this. In addition, the architecture ensures that all participating parties are able to prove the amount of traffic transferred in any given OBAN session. This enables a broader range of business models with respect to charging of visiting OBAN users, remuneration of residential subscribers, and cooperation between service providers. This may in turn result in new business opportunities.

Keywords—Authentication, Excess Capacity, Security Architecture, Wireless Access Networks

1 Introduction

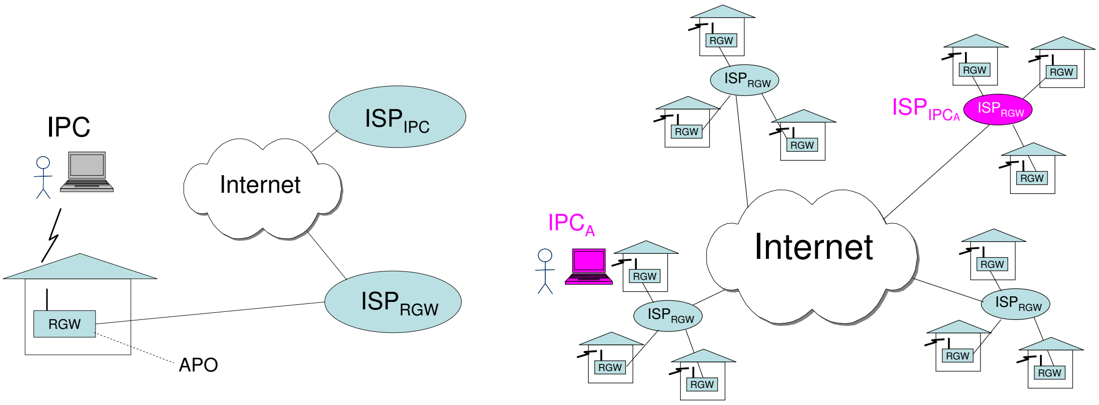
The world is experiencing increased broadband coverage in residential areas, but due to usage patterns and pricing models, only a fraction of the available bandwidth is actually being consumed [1]. The excess capacity could be put to good use, however, if residential installations were to share their bandwidth through public wireless access points [2]. In a nutshell, this is what OBAN [3] is all about. The general background for the project is discussed in detail in e.g. [4] and [5]; in this introductory section we will give a brief overview of OBAN, but otherwise concentrate on security aspects.

1.1 The OBAN Concept

The idea of OBAN is to place publicly available wireless access points in homes (and possibly business premises). These access points are operated by an Access Point Operator (APO), which may or may not be the owner of the premises. The available bandwidth is shared between residential users and visiting OBAN users, in the following referred to as IPCs (IP Customers). The bandwidth may be shared in different ways, either with a fixed amount reserved for the residential user, or by the use of various priority schemes (see [6]).

There are various possible scenarios for OBAN deployment, but a solution that will be applicable to many markets is illustrated in Figure 1(a). In this scenario, we assume that a residential broadband user is offered the use of a Residential Gateway (RGW[1]) from his Internet Service Provider ($\mathrm{ISP_{RGW}}$). This

[1] Also referred to as simply "RG" in other documentation



(a) OBAN Parties

(b) An OBAN Community

Figure 1: Overview of OBAN Parties, and the Big Picture

RGW could be designed as a replacement for any existing broadband router, and will contain wireless access point functionality. The RGW will be administered by the APO, which in this scenario may be the residential user or ISP$_{\mathrm{RGW}}$. Even in the latter case the residential user will always have opportunity for limited local configuration.

IPCs are required to have a subscription with a participating ISP, known as ISP$_{\mathrm{IPC}}$ in this context. When an IPC is in range of an RGW, a connection will be established with ISP$_{\mathrm{RGW}}$, which in turn will forward the IPC's credentials to ISP$_{\mathrm{IPC}}$. The ISP$_{\mathrm{IPC}}$ then acknowledges that the IPC is indeed a valid customer, and promises to honour any obligations made by this user while visiting this particular RGW.

Once authenticated, the IPC can use wireless IP services much like a residential user. Should the IPC wander out of the range of the current RGW, OBAN supports roaming if another RGW is within range (but see also section 2). As indicated by Figure 1(b), a single ISP$_{\mathrm{RGW}}$ will typically have several RGWs under its administrative control.

All ISPs participating as OBAN Service Providers will typically play two roles in the OBAN community, as illustrated in Figure 1(b). On one hand, they will serve as ISP$_{\mathrm{RGW}}$ to their residential users, but also as ISP$_{\mathrm{IPC}}$ for their users on the move.

1.2 Business Models

Many different business models can be envisaged for OBAN, both when it comes to organisation and accounting.

Regarding accounting, IPCs could be billed based on the amount of services consumed, or simply based on a flat monthly fee, to name a couple of alternatives. The solution proposed in this paper will be able to support billing based on service consumption, but this does not exclude simpler options. Flexibility in accounting is also relevant for the residential users, since the remuneration strategy chosen will depend on how these pay for their IP services. Note that there will be a significant incentive for residential users to join the OBAN concept; either increased bandwidth, reduced subscription cost, or both. It is even conceivable that in certain high-volume locations, the residential user may make a net profit on the OBAN participation, in effect getting broadband access for free *and* making extra money.

For residential users in down-town locations, usage patterns are likely to be the inverse of visiting OBAN users, i.e. visiting users are likely to be active during business hours, while residential users primarily are active after-hours. This can result in a win-win situation, where a residential user can earn money on a 100% of spare broadband capacity without suffering reduced performance.

The most interesting organisational aspects relate to the administration of the RGW; several parties are candidates for the role of APO. The simplest approach would be to let ISP$_{\mathrm{RGW}}$ assume this role, since the APO and the ISP$_{\mathrm{RGW}}$ then would be the same party. However, there are also advantages in delegating this role to other parties. This way one may have pure ISP organisations that are specialized in providing connectivity at larger distances, while other parties may specialize in administering end-user equipment. ISPs may also see the advantage in letting the residential user perform more of the management duties, thus reducing the ISP's maintenance costs. The case where the APO is a separate entity from the ISP_{RGW} will therefore be supported.

1.3 Novel Contributions

Offering public wireless access is certainly not new, as anyone who has spent some time in major airports or hotels can verify. Using private residences as a platform for offering such services has also been done before, e.g. as implemented by LinSpot [7].

Roaming between hotspots has however only been possible on a limited scale, and certainly not between different service providers. Furthermore, public hotspots have to a large extent been vulnerable to so-called "evil twin" attacks [8], where a rogue access point may pose as a legitimate hotspot in order to steal username/password combinations or credit card information. Hype aside, it remains a fact that when arriving in a hotel in a strange city, the average user will have no way of determining whether a given access point accepting credit card information is a legitimate hotspot or a "phishing pond"[9].

Supporting roaming and secure use of public access points is an important part of the suggested security architecture, but just as important is the support of the new actor APO, which enables OBAN to handle more complex business structures. With the suggested security architecture, this can be done without sacrificing security requirements. We believe this may open up new business opportunities.

How OBAN addresses these issues will be described in the following.

1.4 Paper Outline

The rest of the paper is structured as follows:

- Section 2 sketches some mobility and QoS aspects of OBAN.
- Section 3 presents the primary security requirements for OBAN.
- Section 4 describes the relations between OBAN parties.
- Section 5 analyses threats that emerge specifically as a result of OBAN.
- Section 6 presents the security architecture for OBAN, focusing on session establishment and handover.
- Section 7 presents a discussion of our contribution.
- Section 8 concludes the paper.

2 Mobility and QoS

Mobility and quality of service (QoS) aspects of OBAN are described in [10] and [6], and while important, these will not be discussed in any detail here. However, for completeness we would like to direct the reader's attention to two specific features: Roaming to other networks, and a two-level Mobile IP [11] scheme.

2.1 Roaming

In a sparsely populated country such as Norway, any access network solution relying solely on wireless LAN access points will be unable to offer the required QoS and session mobility anywhere but select neighbourhoods – for the majority of locations, the service would degenerate to a "Hot Spot Service" as described in [7]. For this reason, the OBAN approach aims towards interoberability and roaming with other access networks, notably GSM/GPRS [12], UMTS [13] and WiMax [14] (the last, although not mentioned in [10], will be a natural extension as it becomes generally available). [10] describes how seamless mobility over heterogenous networks can be achieved; a handover to a different access network technology should not be noticeable for the OBAN user (except for reduced bandwidth when roaming from e.g. WiFi [2] to GPRS). The preferred choice of access technology will be influenced both by available bandwidth and cost. As new wireless access technologies become available to the end-user, they will naturally find their place in the hierarchy of preferred OBAN access methods: WiFi, WiMax, UMTS, GPRS, etc.

2.2 Home Away From Home

OBAN specifies a two-level Mobile IP scheme, where an IPC is assigned a "home-away-from-home"[2] address by the ISP_{RGW} it is currently visiting (i.e. the ISP of the RGW it is currently connected to). The "home-away-from-home" address is naturally in the domain of the ISP_{RGW}, and will represent the end-point of a secure tunnel from the terminal to the ISP_{RGW}. This adds a measure of privacy for the IPC with respect to its ISP_{IPC}, since the latter will not be able to identify the specific locations the IPC has visited without the cooperation of ISP_{RGW}.

Also note that the use of Mobile IP paves the way for accountability and metering of transmitted traffic, since all traffic to the IPC is tunnelled from the IPC's home address to the home-away-from-home address in ISP_{RGW}'s network, and from there forwarded to the current care-of-address of the IPC. In contrast to traditional Mobile IP, the traffic from IPC to "the world" is tunnelled back to the Home Agent via the home-away-from-home address. This also satisfies traditional regulatory concerns regarding the origin of communications, since the traffic generated by the IPC is first tunnelled to ISP_{IPC} before being let loose on the global Internet.

3 Requirements

An OBAN implementation should fulfil some basic security requirements. The security requirements that have been considered most important in our work are listed below.

R1: It should be possible to uniquely identify each party.

R2: Each party should be able to verify the correctness of the information relevant for their activities, and should have enough information to prove their case.

R3: Each party should only get the information necessary to fulfil their particular tasks.

R4: Signalling data should be protected when it comes to confidentiality, integrity and non-repudiation.

R5: Roaming should be both secure and efficient.

R6: Personal equipment placed at the premises of the residential user should not be available for use by IPCs.

Note the conspicuous absence of availability requirements – availability is considered an integral part of QoS, and is documented further in [6].

4 Relations Between Parties

For OBAN to be useful, all parties need to contribute towards the common goal of providing IP services to visitors. Consequently, the necessary trust relations and the different intentions of the parties are of high importance. Part of what makes OBAN special compared to other alternatives is the introduction of the party APO. When discussing relations between parties, the primary focus will be given to relations resulting from introducing this party. Note that in the protocol, the APO is not a communicating party per se, but will be represented by the RGW.

[2] In [10], the term "Gateway Foreign Agent" is used.

4.1 The Relation IPC – APO

The RGWs make it possible for IPCs to connect to their ISPs. In case an IPC acts illegally and/or creates technical problems the APO should be able to disconnect the terminal of this IPC. In case the IPC's behaviour results in financial losses for the APO, the APO should also be able to prove the course of events and the identities of the involved parties. On the other hand, the IPC wants privacy and anonymity. APOs should not have access to all communication of an IPC and should not know the true identity of the IPC.

4.2 The Relation APO – ISP

The APO will have a contract with an ISP that pays the APO for bridging services between terminals and this ISP. The conditions for payment may vary, but if the APO is to receive payment based on the amount of traffic that has been bridged by its RGW, they will both wish to be able to prove the amount of traffic that has been bridged.

It will also be in the APOs interest to get cost absorption confirmations from ISPs when delivering services to IPCs, since APOs normally do not have any contractual relationship with IPCs.

4.3 The Relation IPC – Residential User

Residential users have physical access to the RGW, and may also be the operator of the RGW. It should therefore be assured that residential users do not have the ability to influence the sessions of IPCs, for instance to earn more money.

4.4 The Relation APO – APO

The APOs may be paid based on the amount of traffic that is bridged between terminals and ISPs. To maximise revenue, the APOs want their RGWs to handle the traffic load as efficiently as possible. It should however be ensured that APOs cannot manipulate their RGWs in such a way the algorithm for distribution of terminals between RGWs becomes unfair, and other RGWs are excluded.

4.5 The Relation IPC – ISP

This is a traditional customer - supplier relationship. But in the case of OBAN, the IPC may also desire that the ISP is not able to determine the IPC's location while the latter is using the OBAN services.

4.6 The Relation ISP – ISP

This is a common relationship when intercommunication is required. In such cases ISPs may consume services from other ISPs and they may therefore both want to prove the amount of consumed services.

5 Threat Analysis

A fundamental premise of OBAN is that it should offer the same degree of security as seen in wired broadband connections to the Internet, and thus the threat analysis has only focused on threats specific to OBAN. This means that threats that relate to e.g. common Internet security have not been considered. The following aspects of OBAN seem to have a significant influence on the threat situation:

- Equipment is placed in the homes of individuals
- The structure of the network may be complicated, which will result in management challenges
- Wireless communication plays an important part

Threats that result from these factors will be discussed in the following subsections.

5.1 Equipment is Placed in the Homes of Individuals

The RGW will be placed in the homes of individuals, or on the premises of some enterprise. This means that no ISP is able to control the physical protection of the RGW, i.e. who has physical access to the RGW, how it is protected, etc. This results in increased probability for:

- Unauthorised theft or manipulation of the RGW
- Unauthorised access to data and operations on the RGW
- Unauthorised manipulation of the data or software of the RGW

Regarding residential users, one possible motivation for tampering with the device could be to increase the amount of traffic generated by IPCs, as seen from the $\mathrm{ISP}_{\mathrm{RGW}}$. Access to information on the communication of IPCs may also be one possible motivation for the residential users, as well as for intruders. Lack of physical control over the equipment may also result in reduced availability of service. Residential users may simply switch off the RGW, its power or its connection to the $\mathrm{ISP}_{\mathrm{RGW}}$ at any time. To increase the level of protection one should consider using special protection of the most critical parts of the RGW, i.e. logs, keys, algorithms etc. Possible mechanisms to achieve this includes using tamper-proof equipment, using hardware instead of software for critical functions[3], removing interfaces that are not strictly needed, enforcing proper access control, encrypting content, and utilizing integrity checks.

Since equipment of the residential user will be connected to the RGW it is also important to protect the equipment already present, and make sure it can function as before. For instance, it should not be possible for IPCs to use a network printer of the residential user.

It may be in the interest of a rogue APO to let the RGW falsely assume the identity of an ISP. If successful, other RGWs will communicate with the RGW as if it was an ISP. This could result in the owner of the RGW getting hold of a lot of information that may be used to his advantage, for instance to earn more money at the expense of other RGW owners. Authentication and encryption are appropriate security measures also in this case.

APOs may also want to manipulate their RGW for other reasons. If APOs are paid based on the amount of traffic that is bridged between terminals and ISPs, they may wish to manipulate their RGWs in such a way that the algorithm for distribution of terminals between RGWs becomes unfair, and other RGWs are excluded. If the APO is the same person as the residential user, the APO may also have easy physical access to the RGW.

5.2 Complex Structure of the Network

Managing a network consisting of equipment placed in extremely diverse physical locations may be a major challenge for the ISPs involved. All RGWs will need updates of functionality, security features, etc. from time to time. These updates should be performed in a manner that is as automated as possible, since it is inconvenient that the users hosting the RGW should be responsible for this task. The ISPs will accordingly need to make sure the active RGWs are in working order and functioning as specified at all times. To ease this task it is important to have a good overview of the network. It should be clear who is responsible for managing the network, the network should be well documented, and network management plans should be in place.

5.3 Wireless Communication

Wireless communication is important in many other systems than OBAN, for instance within GSM and UMTS, and in regular wireless networks. As for all wireless networks, there may be problems with interference, uncontrolled resource consumption and jamming. But in addition there may be a problem with false access points. As an example a terminal of an IPC or a residential user may be used to fake an access point. Other terminals will then communicate with this terminal as if it were an access point, possibly resulting in the fake access point getting access to personal information, for instance on the OBAN subscription of the terminal owner. Among other things, this could make it possible to use OBAN services at the expense of the IPCs.

[3] This will, however, have adverse impact on the maintainability of the equipment.

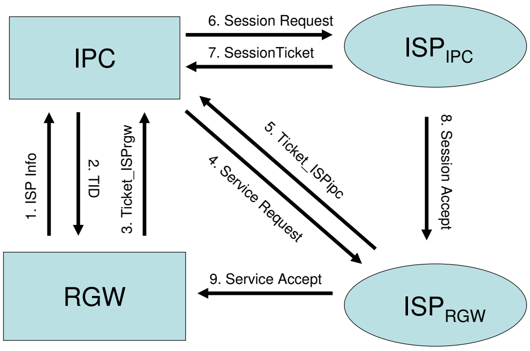


Figure 2: Session Establishment

To increase the protection from such forms of attacks, one should require authentication of access points. In addition one should encrypt any transmitted information that may be used to fake the identity of users.

5.4 Security of the Residential User Revisited

In order to convince residential users to participate in OBAN, security of the residential user's peripherals and other equipment is of paramount concern. However, the OBAN business model also depends on the residential user preserving strict access control to the "residential portion" of the wireless network. After all, who would want to run up charges on their OBAN account if there is an absolutely free residential network readily available from the same access point?

From this we may conclude that even in cases where the residential user also is the APO, steps must be taken to ensure that the RGW maintains a certain minimum of security, also with respect to the residential user. Among other things, this involves preventing the residential user from turning off encryption of the wireless traffic.

Residential users should be distinguished from IPCs, and only residential users should get access to their own local network. This can be achieved by using one Virtual Local Area Network (VLAN) for residential users and one VLAN for IPCs. As mentioned above, the VLAN of residential users need to be secured by the residential user. The use of such a VLAN solution implies that the residential user is not really an OBAN party, and is thus not considered further.

6 Security Architecture

The architecture is based on [15], but has been refined in order to concentrate on the authentication aspects.

6.1 Basic Mechanisms

The OBAN security architecture requires a Public Key Infrastrucure (PKI) where all parties are issued certificates from a universally trusted Certificate Authority[4].

Trust confirmations relayed via parties with which the recipient doesn't have a direct trust relation are transmitted in the form of *confirmation tickets*, inspired by the Kerberos authentication system [16]. However, since the use of shared symmetric keys would not be viable in an OBAN context, the tickets are instead created using a digital signature scheme. In similarity to Kerberos, we also assume the existence of "loosely syncronized" clocks.

[4] Or at least a CA universally trusted within OBAN. In theory, each ISP$_{\text{IPC}}$ could have operated a "unilateral" CA, relying on the direct security relationship between ISPs to generate cross signatures. We would maintain, however, that this is less maintainable and more complicated than having a single top-level CA.

1. $ISPinfo = IP_{ISP_{RGW}}, CERT_{ISP_{RGW}}, ID_{RGW}$
2. $TID_{RGW} = sign_{IPC}(E_{PK_{ISP_{IPC}}}(ID_{IPC}, subID_{RGW}), ID_{ISP_{IPC}})$
3. $Ticket_{ISP_{RGW}} = sign_{RGW}(TID_{RGW}, IP_{terminal}, ID_{RGW}, Timestamp_1)$
4. $ROT = E_{PK_{ISP_{RGW}}}(TID_{RGW}, IP_{terminal}, PK_{IPC}, Timestamp_2)$
   $ServiceRequest = sign_{IPC}(ROT, Ticket_{ISP_{RGW}}, Timestamp_3)$
5. $AST = sign_{ISP_{RGW}}(SessionKeyValidity, E_{PK_{IPC}}(SessionKey), Timestamp_4)$
   $SLD = ROT, Ticket_{ISP_{RGW}}$
   $AcceptReject = E_{PK_{ISP_{IPC}}}(AST, PK_{IPC}, SLD)$
   $Ticket_{ISP_{IPC}} = sign_{ISP_{RGW}}(MIP_{ah}, TicketValidity, AcceptReject, TID_{RGW}, Timestamp_5)$
6. $SessionRequest = sign_{IPC}(Ticket_{ISP_{IPC}}, CERT_{ISP_{RGW}})$
7. $SSC = sign_{ISP_{IPC}}(ID_{session}, Timestamp_6)$
   $SessionTicket = sign_{ISP_{IPC}}(ID_{session}, E_{PK_{IPC}}(SSC), AST, Timestamp_7)$
8. $SessionAccept = sign_{ISP_{IPC}}(AST, SessionValidity, E_{PK_{ISP_{RGW}}}(SSC), Timestamp_8)$
9. $ServiceAccept = sign_{ISP_{RGW}}(AST, SessionValidity, Ticket_{ISP_{RGW}}, E_{PK_{RGW}}(SSC), Timestamp_9)$

Figure 3: Detailed Session Initiation Messages

Certain characteristics of the RGW should be unalterable by the residential user, or any other unauthorized party. To achieve this, some sort of tamper-proof equipment should be considered for relevant parts of the RGW.

Since the RGW also bridges all traffic from the residential network, the RGW should authenticate itself to $\mathrm{ISP}_{\mathrm{RGW}}$ before any traffic is accepted by $\mathrm{ISP}_{\mathrm{RGW}}$. However, this is completely analogous to the situation with current broadband routers, and is thus considered out of scope for our protocol.

Since all application traffic is tunnelled first to the home-away-from-home agent in $\mathrm{ISP}_{\mathrm{RGW}}$'s network, the protocol will negotiate a session key to encrypt the traffic in this tunnel. No special provisions are made for encrypting the application traffic between $\mathrm{ISP}_{\mathrm{RGW}}$ and $\mathrm{ISP}_{\mathrm{IPC}}$; this is left to the application.

In the following, encryption with the public key of party "X" will be denoted $E_{PK_X}(\ldots)$, while creating a digital signature with the private key of "X" is denoted $sign_X(\ldots)$ (for brevity, this notation shall be interpreted to mean that both the signature and the signed data is transmitted).

6.2 Session Initiation

The session initiation process is illustrated in Figure 2, and the session initiation messages are written out in detail in Figure 3 (see Table 1 for a description of the protocol elements). As mentioned, it is assumed that the RGW has authenticated itself to $\mathrm{ISP}_{\mathrm{RGW}}$ in a conventional manner before the session initiation commences, but this is not considered part of the protocol.

Note that timestamps are used to ensure freshness of messages, in addition to control expiration of tickets. Each timestamp in the protocol is thus unique and created at the time of message compilation; this is indicated by an enumeration suffix. The numbering of timestamps has no other significance.

1. When wireless connectivity to the RGW has been established, the RGW will send IPC an *ISP Information Token*, containing the IP address and public key certificate of $\mathrm{ISP}_{\mathrm{RGW}}$. For convenience, the RGW also includes its own ID in the token. The token itself is not signed, since it will be followed later by a ticket.

2. IPC replies to the RGW with a signed token containing the ID of the IPC and the ID of $\mathrm{ISP}_{\mathrm{IPC}}$. The information identifying the IPC is combined with a descriptor chosen by the IPC (so that the IPC has a unique descriptor for each RGW it has been in contact with), and encrypted with the public key of $\mathrm{ISP}_{\mathrm{IPC}}$. This prevents the RGW from learning the true identity of the IPC, and also from tracking the IPC when it roams to other RGWs, but enables the RGW to recognise the IPC as a previous visitor if the IPC should return at a later time. We refer to this identifier token sent by IPC as TID_{RGW}, since it in effect is a temporary ID for this IPC while connected to this RGW.

   Note that since the identity of the IPC is encrypted with the public key of $\mathrm{ISP}_{\mathrm{IPC}}$, no other actors have access to this information.

3. The RGW responds with a ticket, $Ticket_{ISP_{RGW}}$, which enables the IPC to contact ISP_{RGW}. This ticket is signed by RGW, but otherwise sent in clear text, since it basically only is a confirmation that the RGW has capacity to spare and is accepting connections.

4. The IPC sends a service request containg a Request Origin Token (ROT) and $Ticket_{ISP_{RGW}}$ to ISP_{RGW}. The ROT contains information about the IPC (e.g. TID, public key and current temporary IP address), and is encrypted with the public key of ISP_{RGW} in order to prevent the RGW from tracking the IPC. ISP_{RGW} can extract the ID of ISP_{IPC} from the TID in the ticket, and IPC's public key from ROT. ISP_{RGW} will use IPC's public key to encrypt the session key which later will protect the tunnel between IPC and ISP_{RGW}.

5. ISP_{RGW} transmits to the IPC a signed $Ticket_{ISP_{IPC}}$ containing among other things the home-away-from-home address of IPC (MIP_{ah}). Buried in this ticket is also an Access Service Ticket (AST), which is encrypted with the public key of ISP_{IPC}. The AST will be returned to IPC once the session establishment is approved by ISP_{IPC} (see below). Since the sensitive information in this ticket already is encrypted, the ticket itself is unencrypted.

6. The IPC sends ISP_{IPC} a signed Session Request containing $Ticket_{ISP_{RGW}}$ and the certificate of ISP_{RGW}.

7. ISP_{IPC} replies with a Session Ticket, containing a session ID and a timestamp. It also contains an encrypted and signed Service Session Close (SSC) ticket (which the IPC is to use later when closing the connection), and the Access Service Ticket (AST) which contains the session key between IPC and ISP_{RGW}. The Session Ticket itself is not encrypted, since further communication is dependent on knowledge of the session key, not the session ticket.

8. ISP_{IPC} also creates a Session Accept message by signing a combination of the AST, SSC and a timestamp. The Session Accept message is then sent to ISP_{RGW}.

9. Upon receiving the Session Accept message, ISP_{RGW} transmits a Service Accept message to the RGW, at which point the RGW allows the IPC to communicate freely toward ISP_{IPC}[5] according to its Access Service Ticket and Session Ticket.

6.3 Failure Scenarios

Note that in all steps in the above described protocol that involve some kind of verification, a failure will result in a "deny" (*NAK*) message that will abort the session establishment.

In the following we describe some examples of possible failure in session establishment. Most of these failures represent a breach of the security policy.

6.3.1 Capacity of RGW Exceeded

The session establishment proceeds normally until RGW receives the TID (step 2). Upon receiving the TID, the RGW determines that its capacity has been exceeded, and that it can no longer offer meaningful service to new customers. Instead of replying with a ticket, it thus transmits a NAK message, and terminates the connection to IPC.

In case the APO for some reason has decided that it will not do business with a certain ISP_{IPC}, it will exhibit similar behaviour when it receives a TID which names the ISP_{IPC} in question.

6.3.2 Unrecognized Customer

The session establishment proceeds normally until ISP_{IPC} receives the Session Request (step 6), and extracts the public key of IPC. This is compared with the public key ISP_{IPC} has on file for IPC, and in case of a mismatch, ISP_{IPC} transmits a NAK and closes the connection. If, on the other hand, the public key matches, the signature of the TID_{RGW} is checked. If the signature is invalid, ISP_{IPC} likewise sends a NAK and closes the connection. In both cases, it also transmits a Service Level Deny (SLD) message extracted from the ticket to ISP_{RGW}.

[5] But remember that the traffic is first tunneled to the home-away-from-home address before being forwarded to ISP_{IPC}.

Table 1: Explanation of Protocol Elements

Term	Description
$ISPinfo$	ISP information token;
TID_{RGW}	Temporary ID for an IPC at a given RGW, created by IPC
$subID_{RGW}$	"Personal" ID for an RGW, chosen by IPC
$Ticket_{ISP_{RGW}}$	Ticket allowing the ISP to communicate with ISP_{RGW}
ROT	Request Origin Ticket
AST	Access Service Ticket
SessionKeyValidity	Specification of how long a session key is valid. This is configurable by ISP_{RGW}, and may be less than SessionValidity. If a session key expires before the session itself, it will have to be re-negotiated. This will result in the generation of a new AST.
SLD	Service Level Deny
AcceptReject	Structure used by ISP_{IPC} when accepting or rejecting an attempted session initiation. In the latter case it will extract the SLD and transmit to ISP_{RGW}, otherwise the AST and public key of IPC is used to create a session ticket.
MIP_{ah}	"Home away from home" Mobile IP address. Upon completion of the protocol, traffic from the terminal will be tunneled securely to this address, and then forwarded to the Home Agent.
TicketValidity	Specification of how long a ticket is valid.
SSC	Service Session Close ticket; used by IPC to terminate session
SessionValidity	Specification of how long a session is valid. This is configurable by ISP_{IPC}.

6.3.3 Fake Access Point

This is the situation if someone should introduce a fake access point (RGW) with connection to a genuine ISP_{RGW}.

The session establishment proceeds normally until ISP_{RGW} receives the Service Request (step 4). ISP_{RGW} will examine $Ticket_{ISP_{RGW}}$, and determine that it has not been signed by an RGW with which it has a contract. ISP_{RGW} will then send a NAK and close the connection.

6.3.4 Fake Access Point and ISP

A fake access point (i.e. fake RGW), having no relationship with a real ISP_{RGW}, may try to also act as a fake ISP_{RGW}. The session establishment proceeds normally until ISP_{IPC} receives the Session Request (step 6). It will first verify the correctness of ISP_{RGW}'s certificate (also checking that it belongs to an ISP_{RGW} with which it has a contractual agreement), and then the signature of $Ticket_{ISP_{IPC}}$. If either fails, it will send a NAK and close the connection (there is no point in sending an SLD here, since the Session Request did not come via a legitimate ISP_{RGW}).

6.3.5 Expired Ticket

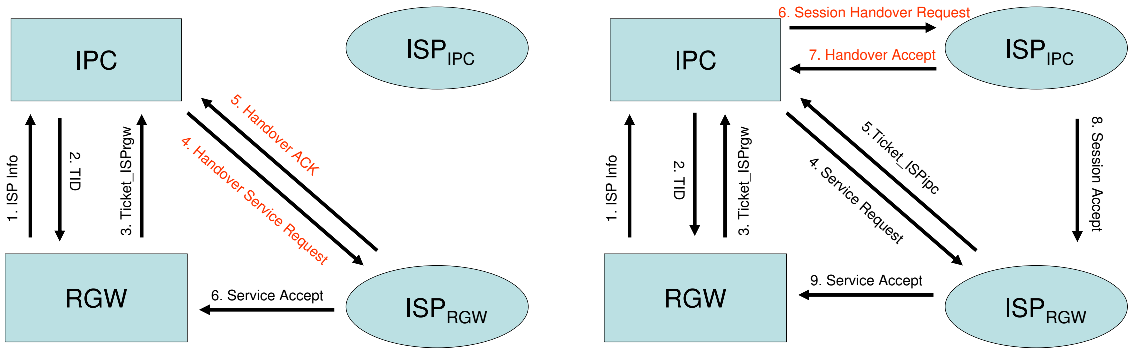
All tickets have a predefined expiration time, after which the recipient will reply to the ticket with a NAK, and close the connection. All other messages that are determined to be too old are treated similarly.

6.4 Handover

The handover process between RGWs will exhibit different characteristics depending on whether or not the old and the new RGW use the same ISP_{RGW}.

We first describe what happens when an IPC arrives at a new RGW connected to same ISP_{RGW} as the previous RGW (see Figure 4(a) and 5):

1. As with regular session establishment, the new RGW transmits the ISP Info upon completing the basic connectivity steps.



(a) Handover Within Same ISP$_{\mathrm{RGW}}$

(b) Handover Involving Different ISP$_{\mathrm{RGW}}$s

Figure 4: Handover

1. $ISPinfo$
2. TID_{RGW}
3. $Ticket_{ISP_{RGW}} = sign_{RGW}(TID_{RGW}, IP_{terminal}, Timestamp_{10})$
4. $HandoverServiceRequest = sign_{IPC}(ISPinfo, AST_{orig}, Ticket_{ISP_{RGW}}, Timestamp_{11})$
5. $HandoverACK = sign_{IPC_{RGW}}(AST_{orig}, Timestamp_{12})$
6. $ServiceAccept = sign_{ISP_{RGW}}(AST_{orig}, SessionValidity, Ticket_{ISP_{RGW}}, E_{PK_{RGW}}(SSC), Timestamp_{13})$

Figure 5: Detailed Handover Messages

2. Since the new RGW doesn't really need to know that this is a handover, the IPC replies as usual with TID_{RGW}.
3. The new RGW replies with a customary ticket for access to ISP$_{\mathrm{RGW}}$.
4. Since the IPC is aware that it already has a connection with a previous RGW, and can see from the ISP Information Token that the new RGW belongs to the same ISP$_{\mathrm{RGW}}$ as before, it then sends a Handover Service Request to ISP$_{\mathrm{RGW}}$, containing the ISP token, the original AST and the new $Ticket_{ISP_{RGW}}$.
5. ISP$_{\mathrm{RGW}}$ replies to IPC with a Handover Acknowledge.
6. ISP$_{\mathrm{RGW}}$ sends a Service Accept to the new RGW.

If the IPC arrives at a new RGW that is not connected to the same ISP$_{\mathrm{RGW}}$ as the previous RGW, the handover process becomes more complicated, and will basically require the same amount of messages as a session initiation. The only difference is that the IPC does not need to set up a new session with its ISP$_{\mathrm{IPC}}$. This can be seen in Figure 4(b). The new messages required for this type of handover are listed in Figure 6. Note that the element named $SessionTicket_{orig}$ in step 6 of Figure 6 is the original session ticket the IPC received when it first initiated the session.

6. $SessionHandoverRequest = sign_{IPC}(Ticket_{ISP_{IPC}}, SessionTicket_{orig}, Timestamp_{14})$
7. $HandoverAccept = sign_{ISP_{IPC}}(AST, Timestamp_{15})$

Figure 6: New Messages (with respect to Figure 3) for Handover, Different ISP$_{\mathrm{RGW}}$

6.5 Faster Handovers

Efficiency is important when it comes to handover, and the solution proposed here may be too time-consuming in many cases. Fortunately, there is room for improvement. One alternative is to do authentication in advance, prior to the actual handover. This might require the terminal to authenticate to all access points as soon as they are within range. Another alternative is utilizing delayed authentication; i.e. accepting unauthenticated connections, but tearing them down if they are not authenticated/confirmed by a set deadline. The effective time for unauthenticated communication will be limited, resulting in only a minimal risk of loss of income for the APO.

Due to restrictions in wireless network standards, terminals are not allowed to be connected to two different access points at the same time. Authentication in advance can therefore not be dependent on terminals requesting authentication at RGWs using the wireless network. However, other (as yet unspecified) mechanisms may be used for this purpose. Alternatively, RGWs may be responsible for pre-authentication. Each RGW could keep a list of neighbour RGWs which are to be contacted for pre-authentication, for instance by using the wired network. These options, and their security implications, are to be investigated in future work.

6.6 Session termination

Any party can terminate a session by sending a service session close ticket.

7 Discussion

In the following, we summarize our achievements and discuss our results in reference to other possible solutions.

7.1 Achievements

Based on the messages involved in session initiation, handover and session termination, trust between the involved parties is achieved. In general, actors who have a contractual relationship before any communication takes place will by definition trust each other. Trust establishment between these actors will therefore not be necessary, but they will need to authenticate each other.

7.1.1 IPC – RGW

The IPC does not need to trust the RGW. The only identity information provided to the RGW is a temporary ID and the ID of the ISP of the IPC. Without a proper agreement with an ISP, the RGW will not be able to handle the request and get paid. It may (in theory) function as a "man in the middle", but this will not result in any advantage. It cannot get to the confidential information that is transferred because it is encrypted, and it cannot communicate at the expense of the IPC since it does not have the necessary session key.

The RGW has the temporary ID of the IPC, and the APO will thus be able to prove the traffic sent by this IPC. In theory, if the IPC behaves badly, the RGW would later be able to recognise the IPC and deny access to communication. However, since the IPC chooses the temporary ID used for the RGW ($subID_{RGW}$), a rogue IPC would likely choose a new $subID_{RGW}$ for the next visit, and continue misbehaving with impunity. In order to effectively block misbehaving IPCs without sacrificing anonymity, some mechanism must be introduced that controls how $subID_{RGW}$ is selected. This remains an area for further study.

If the behaviour of the IPC justifies this, the APO will initiate action towards its $\mathrm{ISP}_{\mathrm{RGW}}$, which in turn will use its contractual relationship with the relevant $\mathrm{ISP}_{\mathrm{IPC}}$ in order to determine the real identity of the IPC. The specific procedures related to such "abuse-cases" will be subject to rules from relevant regulatory bodies.

The APO will have access to the home-away-from-home address of the IPC, MIP_{ah}, and will thus be able to track the IPC if it roams to a nearby RGW belonging to the same $\mathrm{ISP}_{\mathrm{RGW}}$. MIP_{ah} is a dynamic address, however, and will not be reused in future sessions.

7.1.2 IPC – ISP$_{\mathrm{RGW}}$

The IPC knows which ISP$_{\mathrm{RGW}}$ is bridging its traffic, and knows that ISP$_{\mathrm{IPC}}$ accepts this ISP. The IPC is also able to prove the amount of traffic that has been sent via this ISP$_{\mathrm{RGW}}$, and has confirmation that the ISP has approved the communication. The ISP$_{\mathrm{RGW}}$ will not know the true identity of the IPC, but will know the public key of the IPC. This means that it will be able to recognise the customer.

ISP$_{\mathrm{RGW}}$ has proof that the IPC is a customer of ISP$_{\mathrm{IPC}}$ and that ISP$_{\mathrm{IPC}}$ will honour any obligations made by this customer. ISP$_{\mathrm{RGW}}$ will also be able to prove the amount of traffic that has been sent by the customer.

7.1.3 IPC – ISP$_{\mathrm{IPC}}$

These actors will have a contractual relationship. Authentication is performed using digital signatures in accordance with the chosen PKI.

Both actors will be able to prove the amount of traffic that has been sent, but ISP$_{\mathrm{IPC}}$ will not know the real location of its customers.

7.1.4 RGW – ISP$_{\mathrm{RGW}}$

These actors will have a contractual relationship. Both actors will be able to prove the amount of traffic that has been bridged, and the RGW has confirmations that the IPCs that are served are accepted by ISP$_{\mathrm{RGW}}$.

7.1.5 RGW – ISP$_{\mathrm{IPC}}$

These actors have no special relationship.

7.1.6 ISP$_{\mathrm{RGW}}$ – ISP$_{\mathrm{IPC}}$

These actors will have a contractual relationship. They will be able to authenticate each other based on the knowledge of private and public keys. Both actors will be able to prove what services have been offered.

7.2 Fulfilment of Requirements and Mitigation of Threats

The architecture suggested seems well suited to the task of securing all OBAN partners. The requirements stated above are fulfilled:

- Each party has an identity descriptor that can be used to uniquely identify the party. (R1)
- Each party gets the information they need to be able to perform their task and prove their case in the event of a dispute. This is described in section 7.1. Tickets and acceptance messages are signed by the issuing party to achieve non-repudiation. (R2)
- The different parties only get access to the information that is necessary to fulfill their tasks. As an example, ISP$_{\mathrm{IPC}}$s do not get the exact location of their customers, they are only able to know which ISP$_{\mathrm{RGW}}$ the customers are connected to. Similarly, RGWs and ISP$_{\mathrm{RGW}}$s do not know the true identities of IPCs. (R3)
- Signalling data is protected with signatures and encryption where needed, to achieve confidentiality, integrity and non-repudiation. (R4)
- Handover is supported, and is made efficient when roaming between RGWs connected to the same ISP$_{\mathrm{RGW}}$. Handover may be cumbersome if roaming between RGWs connected to different ISP$_{\mathrm{RGW}}$s, so further effort should be spent exploring the options for fast handover described in section 6.5. (R5)
- Personal equipment of residential user is protected. IPCs are only allowed to communicate via ISP$_{\mathrm{RGW}}$, and are not allowed access to the local network. This local network must also be protected by other means by the residential user. (R6)

Regarding threats, protecting the core functionality of RGWs reduces the risk inherent in placing the RGW in premises that are not controlled by an ISP. At the same time, the degree of required trust in RGWs is reduced since no valuable data is sent through the RGW unencrypted. But the problem with complex configurations, and thereby complex maintenance has not been addressed. ISPs may choose to put this responsibility on residential users, if they have the role of an APO. However, residential users may not have the necessary skills to perform this task, resulting in lower quality of the service offered. Some sort of ISP involvement would therefore be beneficial.

7.3 Comparison to Common Security Mechanisms

We realize that an OBAN network has sufficiently many points of similarity with existing computer and telecommunications networks that one could have considered employing commonly available technologies for Authentication, Authorization and Accounting (AAA), as exemplified by [17] and [18]. Unfortunately, space does not permit a rigorous comparative analysis between the OBAN security architecture and commonly available alternatives, but in order to highlight some of the advantages of our architecture, we present a brief description of one concrete alternative below.

An alternative to our architecture could be to utilize 802.1X [19] and EAP-TTLS [20] for authentication. Using this solution, authentication of IPCs can still be performed. IPCs wishing access to OBAN services would send a request to the RGW. This request for service will be tunnelled to a TTLS server at the ISP_{RGW} which forwards the request to the ISP_{IPC}, which ultimately makes the decision. In many ways this is a viable solution. The problem with fake access points ("evil twins") can still be handled, the IPC will only get access to OBAN services if a relationship with a proper ISP_{IPC} is in place, and RGWs and ISP_{RGW}s will know that ISP_{IPC} will honour any obligations made by this customer. This solution has, however, some weaknesses compared to the security architecture suggested in this paper, particularly when it comes to proof of events. This is related to the introduction of the new party APO.

The advantages of the security architecture suggested for OBAN are as follows (these advantages relate to the description above, but are also relevant with respect to e.g. Diameter [18]) :

- ISP_{RGW} will not know the true identity of the IPCs that are served.
- The identities of IPCs are available in a form that can be used for identification in case of dispute.
- IPCs are able to know which RGW that has been used.
- RGWs are able to prove which IPCs have been served and how much resources have been consumed by each IPC. This can be done without relying on logs of other parties.
- All the parties will have access to all tickets and acceptances that will be relevant in case of dispute. As an example, the RGW receives an acceptance message that confirms that ISP_{RGW} has accepted the customer's request for service. In the same way the ISP_{RGW} receives an acceptance message that confirms that ISP_{IPC} has accepted the request and serves the IPC involved. These messages have been signed by the relevant party and can be saved for later use.
- The signed tickets and confirmations provide non-repudiation.
- Data is encrypted all the way to the ISP_{RGW}, not only to the access point.
- There is no need for a shared secret between ISPs and RGWs.

7.4 Business Opportunities

As a result of the work with OBAN, one now has a security architecture that is able to support a completely new party within communication services, namely the APO. This opens up new business opportunities. There is no longer a need to connect directly to some ISP to be able to roam. One can still use well known charging mechanisms, and this is possible without lowering security requirements. For ISPs this means possibilities for faster provision of higher capacity networks with a reduced need for heavy investments. Resources controlled by other parties can be utilized; this may also reduce maintenance costs. Some companies may specialize on administering end equipment like RGWs, while others may specialize in providing connectivity at larger distances. This may yield more effective communication provision, resulting in lower cost for all.

8 Conclusion

This paper has presented a security architecture for an Open Broadband Access Network. The idea of Open Broadband Access Networks is in itself appealing, since already available capacity can be used more efficiently. The architecture suggested is able to fulfil the security requirements in an OBAN environment. In addition, the architecture makes it possible to introduce a new party between the customer and the ISPs, without sacrificing security. This may again open up new business opportunities.

Acknowledgment

This paper is based on joint research in the EU 6$^{\text{th}}$ framework programme. The authors would like to thank all the participating OBAN partners for their contribution to the discussions leading up to the security architecture.

References

[1] 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.

[2] *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std. 802.11-1999, 2003.

[3] OBAN Consortium. [Online]. Available: http://www.ist-oban.org

[4] E. Edvardsen. (2004) Fixed and Mobile Convergence. BroadBand Europe 2004. [Online]. Available: https://medicongress.be/UploadBroad/Session%2009/Paper%2009-01.pdf

[5] T.-G. Eskedal, R. Venturin, I. Grgic, R. Andreassen, J. C. Francis, and C. Fischer, "Open Access Network Concept, a B3G Case Study," in *Proceedings of 13th IST Mobile & Wireless Communication Summit*, 2003.

[6] G. Hoekstra, O. sterb, R. Schwendener, J. Schneider, F. Panken, and J. van Bemmel, "Quality of Service Solution for Open Wireless Access Networks," in *Proceedings of 14th IST Mobile & Wireless Communications Summit*, 2005.

[7] LinSpot. [Online]. Available: http://www.linspot.com

[8] G. Fleischmann. (2005) "My Evil Twin". [Online]. Available: http://wifinetnews.com/archives/004718.html

[9] G. Ollmann. (2004, September) "The Phishing Guide – Understanding & Preventing Phishing Attacks". NGS Software. [Online]. Available: http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf

[10] 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.

[11] C. E. Perkins, "Mobile IP," *IEEE Communications Magazine*, vol. 40, no. 5, pp. 66–82, 2002.

[12] J. Cai and D. J. Goodman, "General packet radio service in GSM," *IEEE Communications Magazine*, vol. 35, no. 10, pp. 122–131, 1997.

[13] 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.

[14] *IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, IEEE Std. 802.16-2004, 2004.

[15] T. J. Wilke and T. H. Johannessen, "Multilateral Security for IP-Service Provisioning in Open Broadband Access Networks," in *BWAN 2005, International Workshop on Broadband Wireless Access Network on fixed network*. IEEE COMSOC, June 2005.

[16] B. C. Neuman and T. Ts'o, "Kerberos: an authentication service for computer networks," *IEEE Communications Magazine*, vol. 32, no. 9, pp. 33–38, 1994.

[17] C. T. de Laat, G. M. Gross, L. Gommans, J. R. Volbrecht, and D. W. Spence, "Generic AAA Architecture," RFC 2903, August 2000.

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

[19] *Port-Based Network Access Control*, IEEE Std. 802.1X-2001, 2001.

[20] P. Funk and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1)," Internet-Draft (Work in progress – expired), February 2005.