Secure Roaming and Infrastructure Sharing for Multi-Operator WMNs

André Egners
Research Group IT Security
UMIC Research Center
RWTH Aachen University

Ulrike Meyer
Research Group IT Security
UMIC Research Center
RWTH Aachen University

ABSTRACT

Wireless mesh networks consist of a wireless infrastructure of mesh routers which are connected to the Internet via mesh gateways. While previous security research in the area mainly focused single-operator networks, this paper proposes a comprehensive security architecture for multi-operator wireless mesh networks. Our proposal allows for a secure deployment of infrastructure components (routers and gateways) as well as mesh client. The multi-operator support of our architecture does not only cover mesh client roaming, but also the deployment of infrastructure components of one operator in the administrative domain of the other operator. Our architecture is thus - to the best of our knowledge - the first to support secure infrastructure sharing between operators. Note that our solution is based on open standards and protects traffic generated by mesh clients from insider attackers such as compromised mesh routers, mesh routers operated by malicious operators, and curious or malicious routing mesh clients.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*

; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless Communication*

General Terms

Security

Keywords

Wireless Mesh Networks, EAP, Key Management, Security, Multi-Operator, Insider Attackers, Roaming, Infrastructure Sharing.

1. INTRODUCTION

Wireless Mesh Networks (WMNs) consist of a wireless infrastructure of Mesh Routers (MRs) which are connected to the Internet via Mesh Gateways (MGs). Some (or all of these) MRs act as Network Access Server (NAS) to Mesh Clients (MCs). MCs connected to a WMN can communicate with other MCs on the same WMN or any other node on the Internet. In addition, MCs may also act as MRs.

WMNs are often considered to be operated by a single operator that owns the infrastructure nodes and offers connectivity to MCs that registered with them directly. There are, however, a variety of applications that profit from or even require multi-operator support. The most obvious is the support of roaming clients as known from mobile telephony networks. Here an MC is not only able to use the WMN operated by his home operator, i.e., the operator it registered with, but also the WMN of any other Foreign Operator (FO) that has a roaming agreement with its Home Operator (HO). In addition, there are application scenarios in which the infrastructure nodes, i.e., the MRs and MGs, forming the WMN are operated by different operators. An example for such an application is building automation using WMN technology, with different companies being responsible for other parts of the building. Also, community networks in which users contribute their own network equipment require this form of multi-operator support. Finally, disaster recovery scenarios can highly profit from multi-operator support using a common mixed infrastructure formed by the network equipment of different first responder units.

Roaming security in WMNs is quite similar to other wireless networks and mainly involves the support of authentication and key agreement across different operators. Adequately protecting mixed infrastructure networks is, however, quite challenging. In particular, it requires procedures for the secure deployment of infrastructure nodes across different operators. In addition, mixed infrastructure networks imply that nodes deployed in the same WMN can differ greatly with respect to their hardness against attacks. In particular, MRs and routing MCs should not be considered uncompromisable and trustworthy.

Many security solutions for single-operator WMNs have been proposed in the past (e.g. [4, 13, 14, 10, 11]). Other approach additionally offer roaming support (e.g. [20, 8, 2, 19, 15, 18]). However, only one of these is based on open standards [2] and compatible with off-the-shelf hardware. Moreover, none of the prior security proposals for multi-operator WMNs supports secure infrastructure sharing between operators, i.e., the secure deployment of an infrastructure component (MR or MG) of one operator in the network of another operator. A particularly interesting single-operator solution suggested in the past was recently proposed in [6]. As op-

SAC'13 March 18-22, 2013, Coimbra, Portugal.

posed to all other proposals before, it allows for the secure deployment of infrastructure nodes such as mesh routers, mesh gateways as well as mesh clients in a WMN operated by a single operator. In addition, it takes insider attackers into account and is secure against malicious infrastructure components as well as curious or malicious routing MCs. Finally, it is based on open standards and works with off-the-shelf hardware.

In this paper we propose a comprehensive security architecture for multi-operator WMNs supporting roaming clients as well as mixed infrastructures. Our proposal is based on the single-operator solution proposed in [6]. However, we considerably extend this proposal to securely support roaming MCs and secure the deployment of infrastructure nodes across different operators. Our solution is based on open standards and protects traffic generated by MCs from insider attackers such as compromised MRs, MRs operated by malicious operators, and curious or malicious routing MCs.

Our paper is structured as follows: In Section 2 we discuss our network architecture, security requirements, and the necessary foundations. Next, in Section 3 we shortly introduce the deployment framework which we use as a basis. After introducing our approach in Section 4 and evaluating its security in Section 5, we conclude the paper in Section 7.

2. SYSTEM MODEL AND FOUNDATIONS

This section discusses the network assumptions as well as the foundations necessary to understand our proposal.

2.1 Network Model

In the following we distinguish two multi-operator scenarios, namely (1) classic fully separate networks as in most roaming scenarios. Additionally, we consider (2) mixed networks which are a novel concept that has not been considered thus far in any prior research in this area.

2.1.1 Separated Networks

In multi-operator networks which are fully separate, a single network consists strictly of infrastructure devices of one specific operator. More specifically, infrastructure devices such as MRs, MGs, Authentication, Authorization and Accounting (AAA) server of each network are the property of the operator. Additionally, in both of the scenarios MGs, MRs, and MCs may serve as the point of network attachment, i.e., NAS, for newly joining MCs or MRs. Figure 1 shows an example on the left side. The network is operated by the operator *Red* which maintains the MRs, MGs and the AAA server which may be co-located with a MG. A MC of the operator *Blue* is currently roaming in this network.

2.1.2 Mixed Networks

In so-called mixed networks devices of one operator may not only connect to devices of the same operator, but also to devices of other operators. We assume a network consisting of infrastructure devices of multiple operators, either private and/or commercial. However, each operator is assumed to be running his own AAA server, e.g., at its Home Network (HN). While considering mixed networks, the notions of *HN* and *FN* become somewhat fuzzy. In contrast to a HN which is maintained by the MC's home operator, the Foreign Network (FN) is maintained by different operator. Therefore, we define a HN of a device as the network in which its AAA is operated, even though the network itself

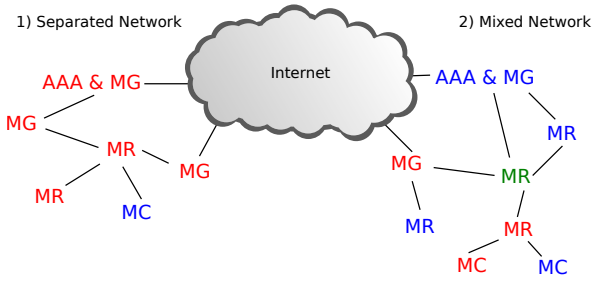


Figure 1: Multi-Operator Network Model

may consist of devices from multiple operators. Thus, for an infrastructure device being in a FN means being connected to a network where the *local* AAA server is not operated by its HO.

Furthermore, we assume MGs not to be co-located with the AAA server, except for MGs of the local domain. Deploying an AAA server in a FN is not considered as they store sensitive user data and credentials onto which operators typically enforce restrictive policies. Figure 1 depicts an example of a mixed multi-operator scenario on the right side. Devices of different operators are connected to each other while the blue operator is responsible for running the local AAA server.

2.2 Multi-Operator Security Requirements

The wireless multi-hop nature makes WMNs particularly vulnerable to active and passive external attackers on the wireless links. Attackers may try to gain unauthorized network access or may try to eavesdrop on or manipulate the traffic in the WMNs. Moreover we consider MRs and MCs, which may also route traffic, to be untrusted. These devices may be placed in easily accessible areas and can therefore be compromised. Compromised MRs and routing MCs may try to eavesdrop on and manipulate the traffic flowing through them. Therefore, MC traffic to and from MGs must be end-to-end protected.

In order to secure multi-hop traffic of MCs (e.g., towards the Internet), an Internet Protocol Security (IPsec) security association could be bootstrapped with a MG. Securing multi-hop client traffic in roaming scenarios in networks with multiple operators can be differentiated into two subscenarios. Securing the traffic between the roaming MC and the MG of its HN (cf. Section 4.2.2), and securing the traffic between the MC and the MG of the currently visited FN (cf. Section 4.2.3). Nonetheless insider threats are relevant for both scenarios, mixed networks still pose an increased threat as devices from different operators may not be equally trustworthy. It may for instance be desirable to secure MC traffic by a VPN-like setup to the MC's HN instead of using the MG of the FN if it is not fully trusted.

The same holds true for authentication traffic between a NAS and the AAA server. It is especially important for MCs that MRs which relay their authentication traffic to the AAA server have secure connection. Also, once the MC or MR has been authenticated, a secure multi-hop connection must be established as the MC may not trust the local operator, especially not the MRs which may be placed in physically insecure locations.

Besides secure authentication and access control for all devices (MRs, MGs and MCs), hop-by-hop link layer security

is required to prevent outside attacks such as eavesdropping and traffic manipulation. This leads to the following security requirements:

R1 Prevent unauthorized nodes from joining the network

R2 Allow the operator for convenient revocation of compromised nodes

R3-6 Confidentiality, integrity, and replay protection of each direct (single-hop) wireless link & local broadcast between NAS and AAA; MC and MG; any two nodes in the WMN wishing to communicate with each other

R7 Fast and secure re-authentication during handover

To meet R1 and R2 a protocol for mutual authentication between joining nodes and the AAA server is required (e.g., Extensible Authentication Protocol (EAP)), as well as a mechanism to exclude compromised nodes from the network. In order to meet the requirements R3-R7 mechanisms establishing security associations between the communicating parties must be bootstrapped.

2.3 Domain Specific Keys

Domain Specific Keys are an important concept when discussing EAP-based multi-operator networks. These keys are specific to a domain, i.e., they are generated in or for a specific WMN. When an explicit *usage* for a key is specified, e.g., to derive a handover key, it is referred to as Usage Specific Root Key (USRK) according to RFC5295 [17]. To support roaming and authentication delegation in other domains, a so-called Domain Specific Key Hierarchy can be used. In this case, Domain Specific Usage Specific Root Key (DSUSRK) are derived from a Domain Specific Root Key (DSRK). RFC5295 discusses how to derive these keys from the Extended Master Session Key (EMSK).

According to the document, DSRKs or DSUSRKs can *"be made available to and used within specific key management domains"* [17], i.e., from the AAA server of one domain to the AAA server of another domain. However, the (secure) key transport between AAA servers (e.g., Remote Dial-in User Service (RADIUS)) has not been specified yet. Recently Hoeper et al. [9] proposed a method to transport keys used by the EAP re-Authentication Protocol (ERP) [7] (which are DSUSRKs) between different key management domains. The authors discuss message transport and that it needs to be secure, however, how the respective security mechanism could be bootstrapped is omitted.

Depending on the trust relationship between the domains, the exporting domain may also chose only to export the DSUSRKs. This effectively limits the allowed applications in the FN. However, in the following we assume that a full domain specific key hierarchy is exported to the FN. This theoretically enables the FN to generate additional DSUSRKs for specific application scenarios in its network.

3. FSASD

The Framework for establishing Security Associations for Sequentially Deployed WMN (FSASD) introduced in [6] provides a solid basis to be extended to achieve our goal to secure community and commercial multi-operator WMNs. It meets all the necessary security requirements for mixed and separated multi-operator scenarios. In addition, FSASD is

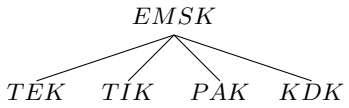


Figure 2: The FSASD Key Hierarchy [6].

the only security framework for WMNs which explicitly addresses insider attacks from malicious or compromised MRs and routing MCs. The authors have also shown that FSASD is compatible to the IEEE 802.11s standard and that it can be implemented using OTS hardware supporting the IEEE 802.1X and 802.11i standard.

The EMSK is used as root in a hierarchy of keys (cf. Figure 2). From the EMSK an IPsec security association (containing an encryption key TEK and an integrity key TIK) is derived. If later on the node N_1 that joined the network acts as NAS, these keys are used to protect the authentication traffic between N_1 and the AAA server with IPsec. The two remaining keys Peer Authentication Key (PAK) and Key Derive Key (KDK) in the key hierarchy are used for authentication and key derivation during bootstrapping of the security associations required.

FSASD also allows to bootstrap security associations between any two authenticated nodes by using Three-Party Handshake Protocol for Sequential Deployment (3PHSD) which interfaces with FSASD. The goal of 3PHSD is to allow any two already authenticated nodes A and B participating in the WMN to establish a security association with each other. In particular, 3PHSD can be used to set up an IPsec security association between MC and MG or to set up a link layer security association for CCMP between a moving MC (or MR) and its new NAS during handover. We use the following notations:

- A, B, S : Identity of Peer A, Peer B, and Server S;
- PAK_{AS} : Peer Authentication Key between A and S;
- K_{AB} : Resulting pairwise key between A and B;
- $\{x\}_{k1}$: x encrypted and authenticated by key $k1$;
- N_A, N_B, N_S : Nonce of A, B, and S;
- t_A : Timestamps of A;
- $\{N_A, t_A, B\}_{PAK_{AS}}$: Token 1;
- $\{N_A, N_B, N_S, A, B\}_{PAK_{AS}}$: Token 2.

A 3PHSD protocol run consists of four messages:

(M1) $A \rightarrow B : A, \{N_A, t_A, B\}_{PAK_{AS}}$

(M2) $B \rightarrow S : A, \{N_A, t_A, B\}_{PAK_{AS}}, N_B$

(M3) $S \rightarrow B : \{N_A, N_B, N_S, A, B\}_{PAK_{AS}}, K_{AB}$

(M4) $B \rightarrow A : \{N_A, N_B, N_S, A, B\}_{PAK_{AS}}$

After Peer A has generated K_{AB} using the parameters of M4 and after Peer B has received K_{AB}, they can use it as a basis to establish a security association. If 3PHSD is used during association, e.g., in a handover scenario, K_{AB} can be the basis for the 802.11i 4-way handshake.

4. APPROACH

Now we introduce our multi-operator key hierarchy extension allowing secure deployment of all infrastructure nodes as well as secure and efficient roaming of MCs. The key hierarchy of [6] can be extended such that multi-operator scenarios are supported without sacrificing the original security properties. In the following we use $\langle device \rangle^{allegiance}_{location}$ to express operator allegiance of devices and its current location. For instance, MR^{ψ}_{π} means that MR belongs to Operator ψ and is currently located in the network of Operator π. $\langle key \rangle^{x}$ refers to a *domain specific key* to be used in the Domain x, e.g., PAK^{π} refers to the PAK of a device that can be used in the Domain π.

4.1 Extending the Key Hierarchy

In FSASD the EMSK is a Root Key. Subsequently derived USRKs such as the PAK are used to bootstrap other security mechanisms. As such, the EMSK is also an USRK, as its sole purpose is to derive the keys on the next level in the key hierarchy which themselves have a specific purpose.

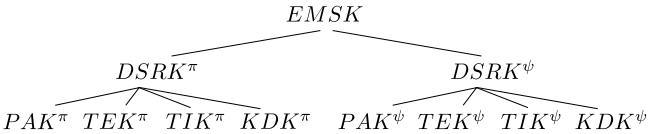


Figure 3: The Domain Specific FSASD Key Hierarchy for Operators π and ψ.

If we now extend this notion from one single domain to a set of domains > 1, we need to introduce so-called *Domain Specific Keys*. These keys are used and valid only in domains specific to their definition. For instance, when the key hierarchy is generated for the domain of Operator ψ, a so-called DSRK needs to be derived from the EMSK. The $DSRK^{\psi}$ (cf. Figure 3) now represents the root of the FSASD key hierarchy for the domain ψ. Subsequently derived keys using $DSRK^{\psi}$ are defined for a specific usage and the domain ψ, i.e, they are so-called DSUSRKs.

The FSASD key hierarchy has been generated by the AAA server of a domain the authenticating device belongs to. A AAA server can for instance export the $DSRK^{\psi}$ to Operator ψ, and the $DSRK^{\pi}$ to Operator π. In their respective domains, these operators are now able to generate the Domain Specific Usage Specific Root Keys (DSUSRKs) for their key management domain (cf. Figure 3). In the following we assume that the full domain specific key hierarchy is exported to the FN.

4.2 Operator-separated Networks

In the following we assume that the network of each operator is deployed according to the FSASD security architecture as discussed in Section 3. Operators must have a bilateral service agreement in order to allow roaming of clients from different operators in their own network. In the next section we discuss the use case of a client roaming from its *Home Operator* ψ (HO) to a *Foreign Operator* π (FO). Deploying MCs, MRs and MGs of the same operator work according to the original FSASD approach.

4.2.1 Client Roaming

A client in allegiance to Operator ψ, MC^{ψ}, is roaming in a foreign network (FN) of Operator π denoted as MC^{ψ}_{π}.

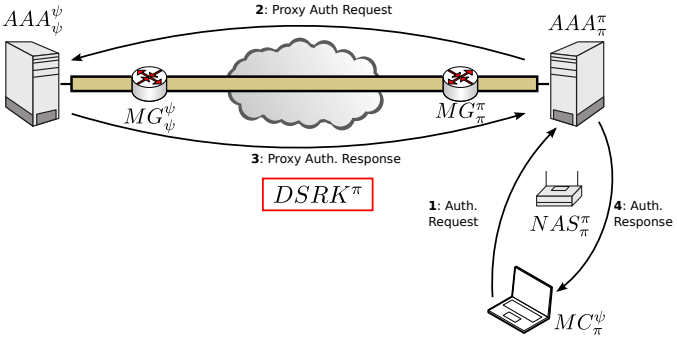


Figure 4: MC^{ψ}_{π} authentication in the domain π

When the client first connects to a NAS (the MR it associates to) of the foreign domain it will initiate a regular EAP authentication. Recall that we assume the network of both domains ψ and π to be deployed using FSASD, i.e., most importantly the authentication traffic is secured by IPsec from the NAS to the AAA server.

A client of Operator ψ connecting in the FN π, i.e., MC^{ψ}_{π} involves the following steps (cf. Figure 4):

1. MC^{ψ}_{π} associates to NAS^{π}_{π} which relays the authentication requests to the RADIUS server, AAA^{π}_{π}.
2. AAA^{π}_{π} recognizes the request being a roaming device of Operator ψ and proxies the message [16].
3. AAA^{ψ}_{ψ} authenticates MC^{ψ}_{π}, derives FSASD domain specific keys and relays the response to AAA^{π}_{π}.
4. AAA^{ψ}_{ψ} also exports the $DSRK^{\pi}$ of MC^{ψ}_{π} to AAA^{π}_{π}.
5. AAA^{π}_{π} relays the response to NAS^{π}_{π} enabling NAS^{π}_{π} and MC^{ψ}_{π} to authenticate each other based on the IEEE 802.11i 4-way handshake.

As the connecting device does not belong to the local domain, the AAA server of Operator π will proxy the EAP authentication request to the devices' *Home Network* (HN), i.e., the AAA server of Operator ψ. The decision to which domain the request needs to be forwarded can be based on the *Network Access Identifiers* (NAI) [1]. Forwarding the request from the AAA of one domain to the AAA of another domain must use a secure connection.

The key transport between RADIUS servers has not been specified yet. If the bilateral service agreement between operators includes securing the connection between their AAA servers (e.g., by using IPsec), we also consider the issues as resolved. However, if this is not the case, we propose that the MGs of cooperating operators could be authenticated by the respective AAA of the other operators in context of FSASD. As a consequence, the MG of Operator ψ would be able to bootstrap an IPsec connection with the AAA server of Operator π based on the TEK^{π}, and TIK^{π} (cf. Figure 3) and vice versa. This would resolve the issue of secure communication between the AAA servers of different operators. The MG is either assumed to be co-located with a local AAA server, or having been authenticated by the AAA server and thus having a secure channel to it.

Depending on the trust relationship between the domains, the home AAA server can choose whether to export the

completely domain specific key hierarchy to the AAA of the other domain, or only export DSUSRKs such as the PAK. As a result of this process MC_π^ψ has been authenticated in cooperation between Operator ψ and π. All keys were transported securely whether using wire or wireless technology, and the link layer security between MC_π^ψ and NAS_π^π has been enabled.

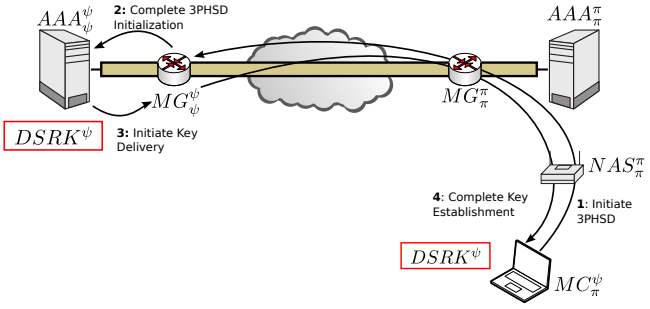


Figure 5: Bootstrapping IPsec to MG_ψ^ψ in the HN

4.2.2 Securing MC Multi-Hop Traffic: $MC_\pi^\psi \leftrightarrow MG_\psi^\psi$

Suppose the HN is controlled by Operator ψ and a client MC_π^ψ is currently roaming in the FN of Operator π. After the client has successfully been deployed using the mechanism described in Section 4.2.1, MC_π^ψ can start 3PHSD [6] with the MG of its HO, i.e., MG_ψ^ψ. Recall that each device the WMN of Operator ψ has been authenticated using FSASD, i.e., each device is in possession of the FSASD key hierarchy; also MG^ψ. The protocol flow is depicted in Figure 5. Also compare the notations from Section 3.

The first message M1 sent from MC_π^ψ to MG_ψ^ψ contains a nonce and a timestamp of the client and the identity of MG_ψ^ψ. This message is encrypted and integrity protected by the key PAK^π which is a DSUSRK for domain π which is shared between MC_π^ψ and AAA_ψ^ψ. When MG_ψ^ψ receives M1, it generates and appends a nonce and its identity and transfers it via the secure connection to AAA_ψ^ψ as message M2. Recall that the MG is either co-located with the AAA, or has been authenticated by the AAA, thus having bootstrapped an IPsec connection based on the FSASD key hierarchy. The AAA_ψ^ψ now generates the key K, appends it to the parameters for MC_π^ψ, i.e., the nonces of MC_π^ψ, AAA_ψ^ψ and MG_ψ^ψ, which are encrypted and integrity protected by PAK^π and sends it as message M3 to MG_ψ^ψ. MG now relays the secured message to MC_π^ψ which can now generate the key K using the contents of message M4.

This key can now be used to set up a secure multi-hop connection (e.g., an IPsec tunnel) between MC_π^ψ in the network of Operator π and MG_ψ^ψ of its HO. The MC's traffic is kept confidential from all intermediaries of the FO and between the two networks.

4.2.3 Securing MC Multi-Hop Traffic: $MC_\pi^\psi \leftrightarrow MG_\pi^\pi$

Roaming MCs could also use the MG of the FN which they are currently roaming in (cf. Figure 6).

The message flow is similar to the case discussed in Section 4.2.2. Recall that once MC_π^ψ has been authenticated by the network of Operator π, the $DSRK^\pi$ of MC_π^ψ is transferred from AAA_ψ^ψ to AAA_π^π. As a result, the roaming client

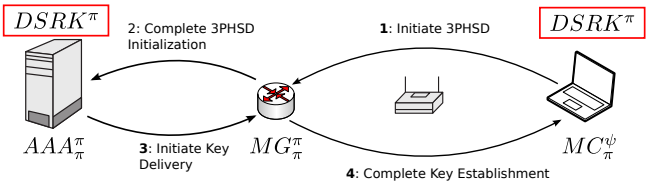


Figure 6: Bootstrapping IPsec to a MG in the FN

does now share a key with the local AAA server AAA_π^π of the FN, namely PAK^π. This key enables the execution of 3PHSD with the gateway MG^π of the FN. The first message M1 is secured by encrypting an integrity protecting it using the key PAK^π which is a DSUSRK for the Domain π. M2 between MG_π^π and AAA_π^π is secured by the IPsec security association which has been bootstrapped during the FSASD deployment (if they are not co-located). Otherwise the message transfer is considered to be secured as it is most likely the same physical entity. Message M3 is sent after AAA_π^π has generated K. It sends it to MG_π^π along with the encrypted and integrity protected parameters for MC_π^ψ. Once MC_π^ψ has received the parameters and has generated the key K, an IPsec connection securing the multi-hop traffic between MC_π^ψ and MG_π^π can be bootstrapped based on K.

4.3 Mixed-Infrastructure Networks

In the following we assume FSASD-deployed network of devices of multiple operators. We now discuss the cases of different devices of the domain of Operator ψ connecting to the network.

4.3.1 Connecting Mesh Routers

When an infrastructure device connects to a mixed network, it either associates to a NAS a different operator (1), or one of the same operator (2). In any case, the NAS has already been authenticated, .i.e., FSASD security associations can be assumed, especially those securing authentication traffic between NAS and AAA.

However, to which operator the NAS in question belongs to is not irrelevant. Each MR serving as a NAS has an IPsec connection to its HO AAA server securing authentication traffic. For instance, if MR_π^ψ has an IPsec connection to AAA_ψ^ψ, while being connected in the FN domain of Operator π, authentication traffic for devices belonging to a different operator (e.g., the local Operator π) must always be relayed through AAA_ψ^ψ. As a result, the authentication traffic of a device MR_π^π is delayed by the indirection $MR_\pi^\psi \rightarrow AAA_\psi^\psi \rightarrow AAA_\pi^\pi$. We therefore argue that any device, irrelevant of operator allegiance, should bootstrap the IPsec connection securing the authentication traffic with the *local* AAA server (in the following AAA_π^π) of the present network. Figure 7 shows the steps involved for authenticating MR_π^ψ in the local domain of Operator π.

On the one hand, authentication requests of devices not belonging to the domain of Operator ψ have to be proxied by AAA_π^π to their HO and AAA_ψ^ψ anyway. On the other hand, authentication request of devices of Operator π are thereby not delayed due to traversing through a AAA server of a different operator. In addition, this behavior is standard compliant to RADIUS which only proxies request of devices belonging to domains different from its own domain.

Bootstrapping the IPsec security association is based on

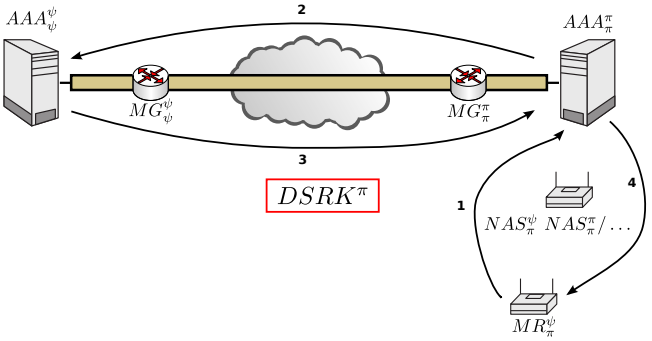


Figure 7: Authenticating MR^{ψ}_{π} in the domain π

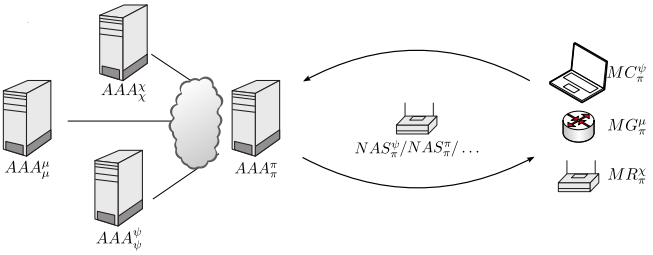


Figure 8: Authenticating arbitrary devices in the domain π

the $DSRK^{\pi}$ (and the derived keys TEK^{π} and TIK^{π} (cf. Figure 3)) which AAA^{ψ}_{ψ} exports to AAA^{π}_{π} for a connecting device MR^{ψ}_{π}.

4.3.2 Connecting Mesh Gateways

Adding more gateways to WMN increases the overall bandwidth. Particularly devices for which the hop distance to a possible new gateway is less than the distance to other gateways will profit from decreased latency and increased bandwidth. The deployment of a new gateway to a mixed network is very similar to the router deployed discussed in the previous section. For instance, once a gateway, e.g., MG^{ψ}_{π}, has been authenticated in the mixed network of the local domain of Operator π by the mechanism described in Section 4.3.1, it can be easily be integrated. As such, MGs can bootstrap an IPsec connection based on the DSUSRKs with the local AAA server; just as MRs.

Recall that DSRKs are transferred from the gateway's HN to the local FN. MCs, irrelevant of operator allegiance, can thus bootstrap an IPsec connection to MG^{ψ}_{π} in operator domain π. For instance, 3PHSD messages between MC^{ψ}_{π} and AAA^{π}_{π} can be secured using their shared key PAK^{π}. The messages between MG^{ψ}_{π} and AAA^{π}_{π} are secured by their IPsec connection.

4.3.3 Connecting Mesh Clients

A MC connecting to a mixed network is essentially the same as in the case of separately operated networks. During association it is irrelevant to which operator the NAS has its allegiance to as the NAS will have an IPsec connection to the AAA server of the *local domain*. The MC's authentication traffic is therefore either proxied by the local AAA to its home domain, or the MC belongs to the local domain and its authentication traffic is destined for the local AAA anyway. In either case, the MC will generate the FSASD key hierarchy specific to the domain it is currently connected to. If it is a foreign domain, DSRKs will be exported from the MC's home AAA to the local AAA.

Bootstrapping IPsec to a gateway is achieved by running 3PHSD. As discussed in Section 4.3.2, gateways are authenticated using FSASD and DSRK may be exported from home to local AAA servers. As the connection between MG and AAA servers is assumed to be secure in both co-located and non co-located scenarios, MCs can simply run 3PHSD with MGs regardless of the MG's operator allegiance. For instance, in the local domain of operator π messages between MC^{χ}_{π} and AAA^{π}_{π} can be encrypted and authenticated based on the shared PAK^{π} and messages between MG^{μ}_{π} and AAA^{π}_{π} based on their IPsec connection.

Figure 8 shows the authentication of arbitrary devices in a mixed network scenario in the local domain of Operator π. All but the requests of devices of Operator π have to be proxied to the AAA of the HO of the device.

5. SECURITY CONSIDERATIONS

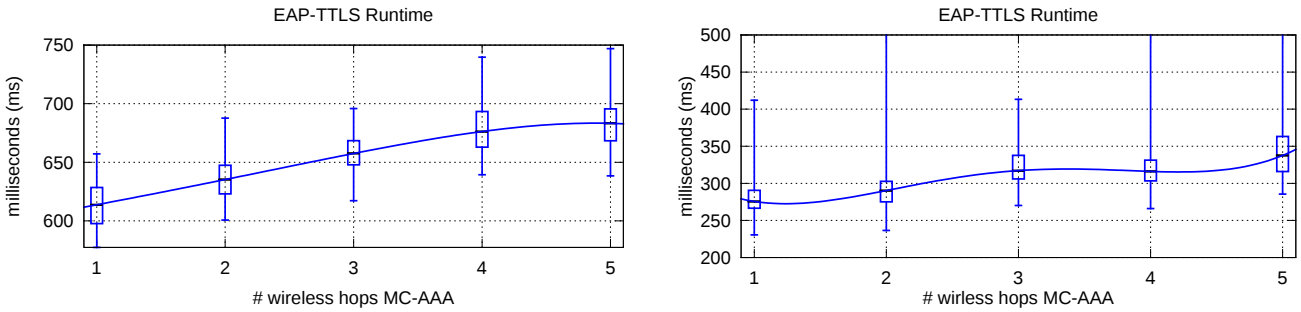
Three important security aspects have to be considered: Deriving and exporting domain specific keys (1), security of separated networks (2), and security of mixed networks (3).

The derivation of the DSRKs should be done as defined in [17] which also states that DSRKs should not be exported to domains with uncertain authorization, i.e., rather DSUSRKs should be exported selectively.

Regarding transport from one domain to another requires confidential and authentic key transport. In [9] the so-called *Key Distribution Exchange* (KDE) is proposed which aims to specify the transport of domain specific keys in context of ERP. We assume the AAA and a MG to be either co-located or both being individual entities. To make use of the key hierarchy that is created during device authentication, a device, i.e., a gateway or the AAA would have to be authenticated by the operator requiring key transport. The connection MG↔AAA is secured either by both being co-located, or by the gateway having been authenticated by the AAA. Thus, we achieve authentic, integrity protected and confidential key transport from one domain to another.

In the setting of separated networks we only need to consider roaming MCs, e.g., MC^{ψ}_{π} associating to MR^{π}_{π}. Authentication traffic from NAS to the local AAA server is secured by their bilateral IPsec connection. Proxying the MC's request to the AAA server of its HN is secured by the secure connection between the two operator networks.

Once the DSRK, or selected DSUSRKs have been securely exported to the AAA server of the FN, additional security mechanism can be bootstrapped. For instance, the MC^{ψ}_{π} can choose to either bootstrap an IPsec connection to a MG of its Home Network (HN), or to a local gateway MG^{π}_{π} of the FN. Compared to using the MG of the HN a performance increase will be the result as the traffic does not need to be home-routed as known from some Mobile-IP scenarios [3]. However, the MC multi-hop connection to a local MG in a FN primarily safeguards from the intermediate hops of the FN, i.e., insider attackers such as routers and possible other clients of arbitrary operators. Traffic of MC^{ψ}_{π} leaving the gateway of the FN is vulnerable to eavesdropping by the foreign operator if no additional security measures such as TLS are used on higher layers It is thus a trade-off between trust and performance. Link layer communication between MC^{ψ}_{π}



(a) (b)

Figure 9: (a) Old results / (b) improved results

and NAS_{π}^{π} is authentic, integrity protected and confidential based on keys derived during the EAP.

In the mixed-network scenario, export of domain specific key material is secured by the same mechanisms as in separated networks. Authentication traffic of MCs, MRs, or MGs with allegiance to arbitrary operators in the local domain of another operator is secured by IPsec between the local AAA and the NAS the device is connecting from. The operator allegiance of the NAS is irrelevant to the authentication process as well as to the connecting device, as each NAS has an IPsec connection to the local AAA server instead of to the AAA of the home operator. Traffic initiated by MCs is secured against untrustworthy intermediaries using IPsec to either the MG of the MCs HO, or the MG operated by the local operator.

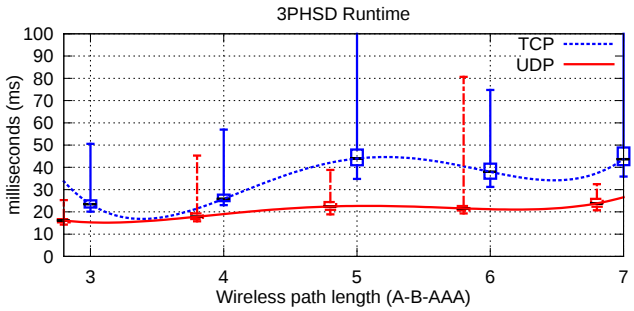


Figure 10: 3PHSD Results

6. PERFORMANCE CONSIDERATIONS

This section provides some details on the testbed used to evaluate our architecture and discusses the performance implication in the multi-operator scenario.

6.1 WMN Testbed Setup

Our WMN testbed is set up with respect to security and performance using PC Engines ALIX system boards. All devices run on *Voyage-Linux*, which is a Debian Squeeze based embedded Linux distribution. We use the Linux kernel version 3.2.9 and support 802.11/abgn modes. Each device has a 500 MHz AMD Geode CPU, 256 Megabytes of RAM and two Atheros AR5008 wireless controllers. The testbed uses the *batman-adv* (v2012.0.0) routing protocol which will automatically adapt to new network topologies. We currently use *wpa_supplicant-0.7.3* and *hostapd-1.0*. The first wireless card allows MRs to connect other MRs of the WMN, while the second card can be used to distribute connectivity, i.e., act as NAS to other MRs or MCs. When a device boots, it will automatically try to connect to the MR with the highest signal strength. As WMNs are self-healing, a new connection will automatically be established if connectivity is lost. The AAA server (meshctrl) of the testbed is located on a virtual machine running on a server box. It is based on Debian Linux 6.0.2 using an Intel(R) Xeon(R) E5450@3.00 GHz with 1024 Megabytes RAM. MGs can reach the meshctrl host via a 100 MBit Ethernet connection.

6.2 Performance Implications

The performance of FSASD as originally proposed is only minimally affected by expanding it to a multi-operator concept. In [6] we evaluated the EAP authentication performance in a real-world 802.11 testbed which included an impact evaluation of using IPsec between NAS and AAA. Authentication using EAP-TTLS over 1-5 hops between NAS and AAA ranged roughly from 580ms to 680ms.

As can be seen in Figure 9 we were able to improve the runtime of EAP-TTLS considerably since. We observed significant overall improvement in our testbed after switching to newer versions of batmand, wpa_supplicant and hostapd. Additionally, Figure 10 shows the runtime of 3PHSD (cf. Section 3), which for instance is used to bootstrap a security association between MC_{π}^{ψ} and MG_{ψ}^{ψ}

In the infrastructure-separated networks (cf. Section 4.2) a delay respective to the latency between the networks of both operators will be added onto the duration of the first full authentication of a roaming client. As Clancy et al. [5] we assume the added (possibly intercontinental) latency to be roughly 100-300ms [12]. Communication originating in FN and destined to HN of the device will be affected by the increased latency, in particular bootstrapping IPsec between a roaming MC and the HN. Mechanisms relying on DSRKs exported from HN to FN, e.g., IPsec from MCs to MGs, or handovers in FN, will not suffer from increased latency, but will rather profit since communication with the HN is not necessary.

7. CONCLUSION

In this paper we propose the first security architecture for WMNs that provides full multi-operator support in commercial as well as community scenarios. Our architecture supports the secure deployment of all components in a WMN, i.e., routers, gateways, and clients. These components may be operated by a single operator or shared by different operators in order to achieve better network coverage and service quality. In addition, our architecture enables secure roaming of mesh clients between WMNs (with potentially mixed infrastructure). The deployment and management of network devices is based on EAP, RADIUS, IPsec, and a three party protocol allowing authenticated devices to bootstrap security associations with other devices even when roaming to a FN. Compared to a single-operator architecture, our proposal inflicts only a minimal performance decrease, which is due to the latency between networks of different operators across the Internet.

Acknowledgments

This work has been supported by the UMIC Research Center, RWTH Aachen University.

8. REFERENCES

[1] Arkko J. Aboba B., Beadles M. and P. Eronen. The Network Access Identifier. Technical report, December 2005.

[2] L. Buttyan and L. Dora. An Authentication Scheme for QoS-aware Multi-operator maintained Wireless Mesh Networks. In *IEEE WoWMoM*, 2009.

[3] Perkins C. IP Mobility Support for IPv4, Revised. Technical report, November 2010.

[4] Omar Cheikhrouhou, Maryline Laurent-Maknavicius, and Hakima Chaouchi. Security Architecture in a multi-hop Mesh Networks. In *SAR*, 2006.

[5] T. Clancy. Secure Handover in Enterprise WLANs: CAPWAP, HOKEY, and IEEE 802.11r. *Wireless Communications, IEEE*, 2008.

[6] André Egners, Hendrik Fabelje, and Ulrike Meyer. FSASD: A Framework for Establishing Security Associations for Sequentially Deployed WMN. In *IEEE WoWMoM*, June 2012.

[7] Cao Z. et al. EAP Extensions for the EAP Re-authentication Protocol (ERP). Technical report, July 2012.

[8] Bing He and D.P. Agrawal. An Identity-based Authentication and Key Establishment Scheme for Multi-operator maintained Wireless Mesh Networks. In *IEEE MASS*, 2010.

[9] Ohba Y. Hoeper K., Nakhjiri M. Distribution of EAP-Based Keys for Handover and Re-Authentication. Technical Report 5749, March 2010.

[10] Md. Shariful Islam, Young Yig Yoon, Md. Abdul Hamid, and Choong Seon Hong. A Secure Hybrid Wireless Mesh Protocol for 802.11s Mesh Network. In *ICCSA'08*.

[11] Ramanarayana Kandikattu and Lillykutty Jacob. A Secure IPv6-based Urban Wireless Mesh Network (SUMNv6). 2008.

[12] Jonathan Ledlie, Paul Gardner, and Margo Seltzer. Network Coordinates in the Wild. In *USENIX NSDI*, 2007.

[13] Fabio Martignon, Stefano Paris, and Antonio Capone. MobiSEC: A Novel Security Architecture for Wireless Mesh Networks. In *Q2SWinet*, 2008.

[14] Kui Ren. A Sophisticated Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks. In *ICDCS'08*.

[15] Kui Ren, Shucheng Yu, Wenjing Lou, and Yanchao Zhang. PEACE: A Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks. *Parallel and Distributed Systems, IEEE Transactions on*, 2010.

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

[17] J. Salowey, L. Dondeti, V. Narayanan, and M. Nakhjiri. Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK). RFC 5295 (Proposed Standard), August 2008.

[18] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang. SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks. *Dependable and Secure Computing, IEEE Transactions on*, 2011.

[19] Ze Wang, Maode Ma, Wenju Liu, and Xixi Wei. A Unified Security Framework for Multi-domain Wireless Mesh Networks. In *ACM ICICS*, 2011.

[20] Yanchao Zhang. ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks. *Selected Areas in Communications'06*.