A Formally Verified Initial Authentication and Key Agreement Protocol in Heterogeneous Environments Using Casper/FDR

Mahdi Aiash

School of Science and Technology, Middlesex University,
London, UK
M.Aiash@mdx.ac.uk

Abstract. Future mobile networking will involve the convergence of different wireless networks such as 2G, 3G, WiMax and Long Term Evolution. The wide scale deployment of such heterogeneous networks will precipitate a radical change in the network infrastructure, where currently closed systems such as 3G will have to operate in an open environment. This brings to the fore certain security issues which must be addressed, the most important of which is the initial Authentication and Key Agreement to identify and authorize mobile nodes on these various networks. This paper proposes a new security protocol to authenticate the mobile terminal in heterogeneous networks.

Keywords: Authentication and Key Agreement Protocols, Casper/FDR, Heterogeneous Networks.

1 Introduction

Unlike current communication systems such as 2G and 3G [1] which introduce closed environments where the core network is controlled and owned by sole network operators and thus its security is mainly based on the assumption that, the core network is physically secure,the above discussion highlights the fact that we are moving towards an open, heterogeneous environment where the core network is not controlled by a single operator, so multiple operators will have to cooperate. This new open architecture, will bring about new security threats such as initially authenticating the mobile nodes in this open environment. This paper proposes a novel Authentication and Key Agreement (AKA) protocol that considers the open nature of heterogeneous networks.

The rest of this paper is organized as follows: Section 2 describes the open architecture of the future, heterogeneous networks as introduced in [2]. Section 3 presents the new proposed protocol. The paper concludes in Section 4.

2 Overview of Future Networks

In Next Generation Networks, multiple operators have to cooperate in order to provide continuous connectivity. However, since each network operator uses a

J. Lopez, X. Huang, and R. Sandhu (Eds.): NSS 2013, LNCS 7873, pp. 742–748, 2013.

different network architecture, interoperability might be a key challenge. One proposed solution for this problem is having a central management entity, called Core-End Point (CEP) to control the resource of the different networks and coordinate the multiple operators [3] [2] [4]. As shown in Fig 1, this future Internet

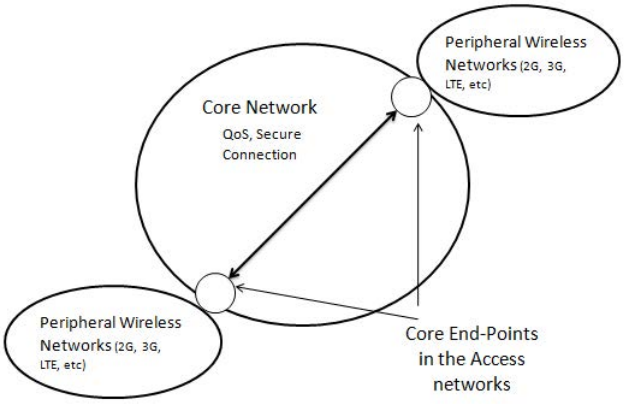

Fig. 1. The Future Internet Architecture

could be viewed as composed of several Core End-Points, interconnected over the super fast backbone of the Internet. Each CEP is responsible for managing multiple, wireless peripheral networks such as Wimax, WiFi or mobile technologies in a local context. A detailed view of the the Core End-Point's structure along with the attached networks is shown in Fig 2. The figure shows a hierarchical architecture, where the bottom level is represented by several Access Points (APs) and Access Routers (ARs), that communicate with the wireless interfaces in the mobile terminals. The middle level comprises a number of technology-specific domains, where each domain represents a certain network operator and technology such as 2G, 3G and Wi-Fi. For these domains to interoperate, the Core End-Point, which is residing at the top level acts as a central administrative domain to control the inter-domain functions and provide overall management. In order to deal with the QoS and security tasks in this architecture, a number of operational entities have been proposed as follows: The Central A3C server (CA3C), the Central QoS Broker (CQoSB), the Domain A3C Server (DA3C), the Domain QoS Broker (DQoSB), the Access Router (AR). These entities cooperate to provide security and QoS-related tasks as described in [2].

2.1 Verifying Security Protocols Using Formal Methods and Casper/FDR Tool

Previously, analysing security protocols used to go through two stages. Firstly, modelling the protocol using a theoretical notation or language such as Communication Sequential Processes (CSP) [6]. Secondly, verifying the protocol using

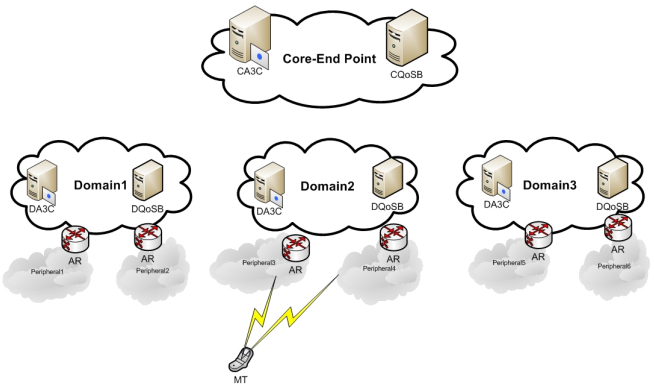

Fig. 2. The Network Structure

a model checker such as Failures-Divergence Refinement (FDR) [7]. However, describing a system or a protocol using CSP is a quite difficult and error-prone task; therefore, Gavin Lowe [5] has developed the CASPER/FDR tool to model security protocols, it accepts a simple and human-friendly input file that describes the system and compiles it into CSP code which is then checked using the FDR model checker. The proposed protocol in this paper has been verified using the Casper/FDR tool.

3 The Proposed Solution

In order to address the security threats in NGNs and to provide a better security in the core network, our proposed solution presumes the existence of secure connection between all the network entities (Auth, DA3C, CA3C) in the core network.

3.1 The Key Hierarchy

As shown in Fig 3, the security materials comprise a top level Unique Key uk(MT), which is pre-shared between the MT and the CA3C server. Similar to the (Ki) key in GSM [1] , the uk(MT) is stored into the MT's SIM card and is never used for encryption purposes rather, it is only used for deriving further security keys. The second level key is the Domain Specific Master Key (DSMS), as the name implies, this key is unique at the domain level and is derived using an irreversible function F1 as follows: DSMS=F1(uk(MT), seq1, Auth_Domain_Name), where seq1 is a fresh sequence number, the Auth_Domain _Name is the corresponding domain name. Since each domain might have more than one Authenticator, the MT could join the domain via any of its Auths, thus, a different Secret Key (SK) has to be used for each Authenticator. One Authentication Key (AK) is used for mutual authentication between the MT

and the network. Similar to F1, two irreversible function F2 and F3 are used to derive AK and SK as follows: AK = F2 (seq1, DSMS), SK = F3(seq1, AuthID, DSMS). Where AuthID is the ID of the Auth and is broadcasted by the Auth in the form of AuthID@DomainName. Defining the Key Derivation Function (KDF) used by F1-F3 functions is beyond the scope of this paper.

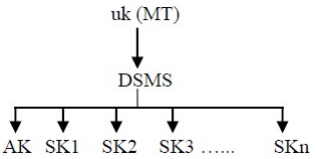

Fig. 3. The Key Hierarchy

Table 1. Notation

The Notation	Description
MT	The Mobile Terminal
Auth	Is the Access Router in the peripheral network
AuthID	The Authenticator unique ID has the format AuthID@domainname
CA3C	Core-endpoint entity, which has QoS and Security related responsibilities
se1(DA3C)	Pre-shared secret key between the CA3C and the DA3C
se2(Auth)	Pre-shared secret key between the DA3C and the Authenticator (Auth)
uk(MT)	Unique secret key shared between the CA3C and the MT
DSMS	Domain specific- Master Key DSMS= F1 (uk(MT), seq1, Auth-domain name)
AK	Authentication key AK= F2 (seq1, DSMS)
SK	Secret Key SK = F3 (Seq1, AuthID, DSMS), used to encrypt all the messages between the MT and the network
F1, F2, F3	Irreversible Key Derivation Functions
InitAuth flag	A flag set only in the initial authentication. In case of handover, this flag will not be set
HoAckm	Joining/Handover Acknowledgement message used by the DA3C server to inform the CA3C in the CEP about a successful authentication
seq1, seq2	Sequence numbers
{m}{K}	Encrypting the message (m) using the key (K)

3.2 The Security Protocol

To secure the core network, we propose the presence of a certain trust relationship between the network's entities and thus secure channels have already been established between the CA3C, the DA3Cs and between the DA3Cs, the Auths. Such secure channels could be guaranteed by using different mechanisms such as IP security (IPSec)or any other Virtual Private Network (VPN) protocols. Alternatively, this could be achieved using out-of-band approach such as agreeing on security materials among the multiple operators.

By considering the notation in Table 1, the AKA protocol is explained as follows:

After starting the mobile device, the MT picks the access routers' advertisements (Adv) which contain information about the access network such the AuthID and the domain name. The MT uses this information to generate a Domain-Specific Master Key (DSMS).

Phase 1
Msg 1: Auth → MT: Adv
Generate the DSMS= F1(uk(MT), seq1, AuthID)

The protocol starts when the MT sends a joining message Msg 2 to the Auth. The Auth responds by sending authentication request AuthReq as Msg 3.

Phase 2
Msg 2. MT → Auth: AccReq
Msg 3. Auth → MT: AuthReq

By using the DSMS, the MT derives the Authentication Key (AK) and composes Msg 4, this message consists of a fresh sequence number seq1 used as a challenge, Authentication ID (AuthID); the Mobile terminal identity (MT) , and a set Initauth flag (InitAuth=1). The Auth passes this message to the DA3C and from there to the CA3C as Msg 5 and Msg 6. Using the included mobile ID, the CA3C looks up the corresponding uk(MT) and uses it to generate a fresh Domain Specific Master key DSMS.

Phase 3
Generate the AK = F2(seq1, DSMS)
Msg 4. MT → Auth: MT, seq1, AuthID, Initauth
Msg 5. Auth → DA3C: {MT, seq1, AuthID, Initauth}{se2(Auth)}
Msg 6. DA3C → CA3C: {MT, seq1, AuthID, Initauth}{se1(DA3C)}
Generate the DSMS= F1(uk(MT), seq1, AuthID)

The DSMS key is included in Msg 7. Using the information in this message, the DA3C generates the Authentication Key (AK) and returns the previously sent sequence Seq1 and a new sequence number Seq2 all the way to the MT as Msg 8 and Msg 9. These messages are encrypted using the derived AK. Since

the MT has the required information to derive all the keys (DSMS, SK, AK), the MT verifies the contents of Msg 9 and derives the Secret Key SK.

Phase 4
Msg 7. CA3C → DA3C: {DSMS, seq1, AuthID, MT, Initauth}{se1(DA3C)}
Generate the AK = F2(seq1, DSMS)
Msg 8. DA3C → Auth: {{seq1, seq2}{AK}}{se2(Auth)}
Msg 9. Auth → MT:{seq1,seq2}{AK}
Verify the message contents, then derive the SK:= F3(seq1, DSMS, AuthID)
The MT returns Seq2 all the way to the DA3C as Msg 10 and Msg 11. The DA3C verifies the contents of Msg 11 and derives the Secret Key SK.

Phase 5
Msg 10 . MT → Auth:{seq2}{AK}
Msg 11. Auth → DA3C :{{seq2}{AK}}{se2(Auth)}
Verify the message contents, then derive the SK:= F3(seq1, DSMS, AuthID)
Upon verifying the Msg 11, the DA3C authenticates the MT and acknowledges this to the CA3C, and then generates the Secret Key (SK) and passes it to the Auth in Msgs12, 13. Using the SK, the Auth sends an encrypted access response message to the MT as Msg 14.
Phase 6
Msg 12. DA3C → CA3C:{HoAckm}{se1(DA3C)}
Msg 13. DA3C → Auth:{SK}{se2(Auth)}
Msg 14. Auth → MT:{AccRes}{SK}

Formal Verification: A Casper input file describing the protocol was prepared. For conciseness, only the #Specification and the #Intruder Information headings are mentioned here. The security requirements of the system are defined under the # Specification heading. The lines starting with the keyword Secret define the secrecy properties of the protocol. The lines starting with Agreement and WeakAgreement define the protocol's authenticity properties.

 # Specification

```
Secret(MT,AK,[DA3C])
Secret(DA3C,AK,[MT])
Secret(MT,SK,[DA3C, Auth])
Agreement( MT, DA3C, [seq2])
Agreement(DA3C, MT, [AK])
WeakAgreement(MT, Auth)
WeakAgreement(Auth,MT)
WeakAgreement(Auth, DA3C)
WeakAgreement(DA3C, Auth)
```

The # Intruder Information heading specifies the Intruder identity, knowledge and capability. The first line identifies the Intruder as Mallory, the Intruder

knowledge defines the Intruder's initial knowledge, i.e., we assume the Intruder knows the identity of the participants and can intercept and replay all the exchanged messages.

 # Intruder Information
`Intruder = Mallory`
`IntruderKnowledge = {mt, da3c, Mallory, ca3c, Authid, auth, uk(Mallory)}`
After simulating the protocol, Casper/FDR found no attacks

4 Conclusion

This paper investigates the security issue in heterogeneous networks. In particular, it tries to address the issue of authenticating mobile nodes when initially joining the network. Therefore, a new AKA protocol has been proposed, the protocol is formally verified using formal methods approach based on the Casper/FDR tool.

References

1. Jochen, S.: Mobile Communications. Addison Wesley (2003)
2. Aiash, M., Mapp, G., Lasebae, A.: A QoS framework for Heterogeneous Networking. In: ICWN 2011 (2011)
3. International Telecommunication Union (ITU-T), Global Information Infrastructure, Internet Protocol Aspects and Next Generation Networks, Y.140.1 (2004)
4. Almeida, M., Corujo, D., Sargento, S., Jesus, V., Aguiar, R.: An End-to-End QoS Framework for 4G Mobile Heterogeneous Environments. In: OpenNet Workshop (2007)
5. Lowe, G., Broadfoot, P., Dilloway, C., Hui, M.: Casper, A compiler for the Analysis of security protocol, `http://www.comlab.ox.ac.uk/gavin.lowe/Security/Casper/` (accessed January 1, 2013)
6. Ryan, P., Schneider, S., Goldsmith, M., Lowe, G., Roscoe, A.W.: The modelling and analysis of security protocols. Pearson Ltd. (2010)
7. Formal Systems (Europe) Ltd.: Failures-Divergence Refinement. FDR2 User Manual, `http://www.fsel.com/documentation/fdr2/fdr2manual.pdf` (accessed January 1, 2013)