Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Design and formal security evaluation of NeMHIP: A new secure and efficient network mobility management protocol based on the Host Identity Protocol

Nerea Toledo [a,*], Marivi Higuero [a], Jasone Astorga [a], Marina Aguado [a], Jean Marie Bonnin [b]

[a] Department of Communication Engineering, Faculty of Engineering, University of the Basque Country, Spain
[b] RSM Department, Telecom Bretagne, Institut Telecom, France

ARTICLE INFO

Article history:
Received 8 March 2012
Received in revised form
24 September 2012
Accepted 29 September 2012

Keywords:
Mutual authentication
Key exchange
Rekeying
Formal security evaluation
Network mobility
Host Identity Protocol

ABSTRACT

NEtwork MObility Basic Support (NEMO BS) is a standardized protocol for managing the mobility of a set of nodes that move together as a whole while having continuous connectivity to the Internet through one or more Mobile Routers (MRs). Because it is based on Mobile IPv6 (MIPv6), it inherits the properties of MIPv6, such as the use of IPsec. However, NEMO BS does not address all the features required by the demanding Intelligent Transportation Systems (ITS) scenario to provide an integrated and global secure mobility management framework. In addition, unlike MIPv6, the routing in NEMO BS is suboptimal, which makes difficult the provision of an adequate service performance. These characteristics make the application of the NEMO BS protocol not optimum in this scenario. An interesting strategy to provide security and good service performance is to consider a protocol that establishes and maintains Security Associations (SAs), such as the Host Identity Protocol (HIP). Different HIP-based approaches have been defined. However, these HIP-based network mobility solutions still present unsolved issues. In this article, we present a secure and efficient network mobility protocol named NeMHIP. NeMHIP provides secure and optimum mobility management and efficient end-to-end confidentiality and integrity protection apart from the basic security properties inherited from HIP. To evaluate the security provisions of NeMHIP, we have conducted a belief-based formal evaluation. The results demonstrate that the defined security goals are achieved by the protocol. Furthermore, we have performed an automated formal evaluation to validate additional security aspects of NeMHIP. Thus, we have modeled NeMHIP using the AVISPA tool and assessed its security when an intruder is present. The results confirm that NeMHIP is a secure protocol that ensures end-to-end confidentiality and integrity without introducing security leaks to the basic HIP. Thus, we have addressed the need found in the literature for providing security and efficiency in the network mobility scenario.

1. Introduction

The rapid progress in wireless access communication technologies and the fast penetration of smart user devices makes it possible to provide communication services in sophisticated scenarios such as mobile networks. A mobile network is a cluster of nodes that move together as a whole and require continuous Internet access. An example of this scenario is the

[*] *Corresponding author*. Tel.: +34 946017396; fax: +34 946014259.
E-mail address: nerea.toledo@ehu.es (N. Toledo).

0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2012.09.014

Intelligent Transportation Systems (ITS) scenario (ETSI EN 302 665, 2010). In this scenario, several nodes on a vehicle obtain anytime–anywhere connectivity to the Internet through one or more Mobile Routers (MRs) while moving. Fig. 1 shows a common ITS scenario.

A mobile network changes its location constantly, which implies that its location has to be tracked and that established connections between nodes onboard and nodes in the outside network have to be restructured as it moves. The mobility management handles the operations required for those purposes. When a mobile network undergoes a location change, its IP address usually changes as well. Peer nodes must be notified of this modification to maintain ongoing communications and the ability to be reached. Commonly, these procedures are performed by the MR, the entity in charge of providing communication services to the Mobile Network Nodes (MNNs).

It is important to note that if the mobility management protocol is not secure, communications will be vulnerable to security attacks. We next examine possible attacks and outline the required security services. Because the MR is the entity in charge of managing the location changes of a mobile network, that is, the IP address changes, the malicious behavior of a node acting as the MR could result in a communication service disruption for all the nodes located in the mobile network. For example, if a fake MR identifies a spoofed IP address, this attack could result in breakage of all the ongoing communications and prevention of new communications from being established. Furthermore, if the identified address corresponds to a victim Point of Attachment (PoA), a shortage of resources in the PoA could happen, leading to service disruption. Moreover, if a fake MR claims itself as the secondary MR in a multihomed mobile network advertising a fake network prefix, the MNNs could communicate with the fake MR, mounting for instance redirection attacks. Therefore, authentication support, integrity support, Denial of Service (DoS) attack protection, replay attack protection are considered mandatory security services between the parties involved in the network mobility management protocol.

In the ITS context, two types of services can be distinguished: ITS operational services and infotainment services. ITS operational services include services related to the operation and control of a vehicle. Due to the critical data transported by ITS operational services, authentication, integrity protection and replay attack protection are essential security services. In addition, in the case of infotainment services,

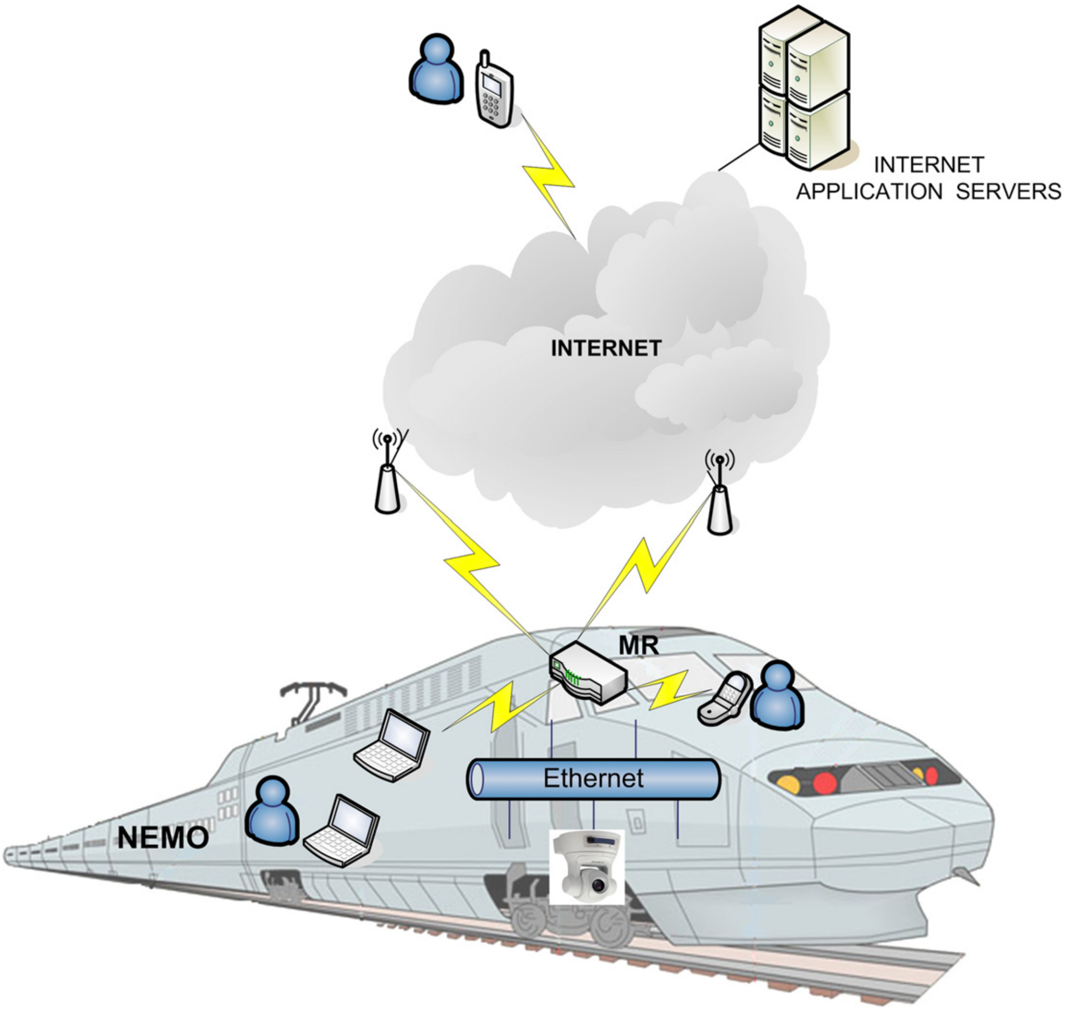

Fig. 1 – ITS scenario.