Chapter 8
The Map-and-Encap Locator/Identifier Separation Paradigm: A Security Analysis

Damien Saucez
Inria Sophia Antipolis, France

Luigi Iannone
Telecom ParisTech, France

Olivier Bonaventure
Université catholique de Louvain, Belgium

ABSTRACT

Internet lacks of strong security mechanisms, opening the way to a plethora of different manners in which integrity and availability can be compromised by malicious activities. Furthermore, the trend shows an increase of security threats, at least in the foreseeable future. Despite such situation, new proposals for Future Internet architectures mostly aiming at solving scalability issues do rather neglect security aspects.

Among candidate Future Internet architectures, the ones based on the Locator/Identifier separation paradigm has been largely explored, but security had no major role in these research activities. We present a security threats analysis of such approach using the Locator/Identifier Separation Protocol (LISP) as a running example.

The chapter does not overview the merits of the Locator/Identifier separation paradigm. Rather, the aim is to provide a thorough analysis of the security aspects, assessing the security level of the architecture and providing recommendations on possible practices to improve it.

DOI: 10.4018/978-1-4666-4305-5.ch008

INTRODUCTION

Since its creation, the Internet has grown at a rapid pace and the protocols, whose principles have been designed more than thirty years ago at the dawn of the Internet, are starting to show their scalability and maintainability limits (Meyer, Zhang, & Fall, 2007; BGP Routing Table Analysis Report).

To give the Internet a second birth, removing (or at least evading) current limitations, allowing continuing its growth, improving its scalability and performance, Future Internet architectures are under consideration, mostly (if not always) based on the Locator/Identifier separation paradigm. It exists a general consensus in the research community, but also among Internet operators and manufacturers, that such a paradigm is the most promising technology that, if correctly engineered, can be incrementally deployed, enhancing Internet's scalability and even providing additional benefits (e.g., scalable support for multi-homing and flexible traffic engineering) (Li, 2011; Quoitin, Iannone, de Launois, & Bonaventure, 2007; Saucez, Donnet, Iannone, & Bonaventure, 2008).

Due to its open nature, in the Internet attacks and security threats are commonplace, and where their number is relentlessly growing (Wood et al., 2012). Therefore, for every proposed Future Internet architecture, its security model and threats analysis becomes of primary importance, and should be carried out with care, preferably even before any commercial deployment (Bos et al., 2009). Unfortunately, reality is different. Current research activities on Future Internet seldom tackle security aspects, very often providing only a very short and high-level analysis.

In the aim of bridging this gap, this chapter presents a security analysis for map-and-encap based Locator/Identifier separation approaches, taking the Locator/Identifier Separation Protocol (LISP) as running example of such kind of architectures in order to provide real and concrete cases.

The Locator/Identifier Separation Protocol (LISP) (Farinacci, Fuller, Meyer, & Lewis, 2012), first proposed by Cisco at the IRTF (Internet Research Task Force) and now under specification at the IETF (Internet Engineering Task Force), is an instantiation of the paradigm separating locators and identifier. Its success is also due to its inherent properties of incremental deployability, which is a very important adoption incentive factor for any new architecture. Indeed, in order to design a viable solution, existing constrains (e.g., current OS protocol stack implementations, inter-domain routing, and prefix allocation policies) have to be taken into account, avoiding disrupting the existing communication infrastructure, whilst providing benefits, hence incentives, for early adopters (Iannone & Levä, 2010).

The present chapter starts by providing some background information, describing the map-and-encap Locator/Identifier separation in its LISP instantiation. Except for the LISP specific header, the main functioning of the protocol is valid for any other solution in the same class (e.g., Menth, Hartman, & Klein, 2010; Frejborg, 2011; Jen, Meisel, Massey, Wang, Zhang, & Zhang, 2007). The reader familiar with LISP or the general Locator/Identifier separation paradigm can safely skip this overview. Then, a brief introduction on the main class of attacks (at network layer) and the way they are carried out is proposed.

It is out of scope to present an exhaustive taxonomy of all possible attacks that can be carried out in the Internet; rather, the focus is limited to threats that are relevant in the Core/Edge separation context. Note, that this does not mean that other attacks are not possible, but only that there is no difference (i.e., they can be carried out in the exact same way) between the new architecture and the current Internet architecture. Furthermore, here we assume a generic IP connectivity/transfer service, without making the difference between using IPv4 or IPv6, since, in the present context and from a security viewpoint, the two versions are equivalent. Afterward, the presented class of attacks is instantiated in the context of LISP, in order to analyze the threats and the available