Chapter 79

Enhancing Security and Trust in Named Data Networking using Hierarchical Identity Based Cryptography

Balkis Hamdane
Sup'Com, ENIT, Tunis, Tunisia

Rihab Boussada
ENSI, Manouba, Tunisia

Mohamed Elhoucine Elhdhili
ENSI, Manouba, Tunisia

Sihem Guemara El Fatmi
Sup'Com, Aryanah, Tunisia

ABSTRACT

Named data networking (NDN) represents a promising clean slate for future internet architecture. It adopts the information-centric networking (ICN) approach that treats named data as the central element, leverages in-network caching, and uses a data-centric security model. This model is built mainly in the addition of a signature to each of the recovered data. However, the signature verification requires the appropriate public key. To trust this key, multiple models were proposed. In this article, the authors analyze security and trust in NDN, to deduct the limits of the already proposed solutions. They propose a security extension that strengthens security and builds trust in used keys. The main idea of this extension is the derivation of these keys from data name, by using hierarchical identity-based cryptography (HIBC). To confirm the safety of the new proposal, a formal security analysis is provided. To evaluate its efficiency, a performance evaluation is performed. It proves that by adopting the proposed extension, performance is comparable, even better in some cases than plain NDN.

DOI: 10.4018/978-1-7998-5351-0.ch079

INTRODUCTION

Since its conception, the Internet has undergone radical changes. Its primary use has changed from a simple communication between trusted hosts to a data distribution (Carofiglio, Morabito, Muscariello, Solis & Varvell., 2013). This new context has motivated the development of the Information Centric Networking (ICN) approach (Xylomenos et al., 2014), (Yaqu., Ahmed, Bouk & Kim, 2016). This approach aims to provide an efficient data distribution by treating data as the central element and by leveraging in-network caching.

Named Data Networking (NDN) (Zhang et al., 2010) is a promising ICN architecture. Its communication model is based on two packet types: (1) Interest representing the request and (2) Data representing the desired data. An Interest packet is broadcasted by a requester on all available interfaces. A Data packet represents the response to an Interest packet. It is mainly composed by a name, data and a signature linking the name to the data. This Data packet is sent from the first node intercepting the request and having data with the same name. Indeed, NDN natively supports on-path caching; each network node keeps a copy of all Data packets that it sends to their final destinations and this to meet future demands. Although caching improves data distribution, it prevents the use of traditional security mechanisms, tied to specific locations. A security model based on data, regardless of the source, is therefore adopted. This model is essentially based on the integration of a signature in each Data packet. Indeed, this signature is calculated on the various fields of the packet (including the name and data), using the producer private key. Its verification by a requester ensures the corresponding producer authentication. In addition, it guarantees that the received data have not been altered (data integrity) and that they match the name indicated in the Interest packet (name authenticity). Indeed, this name is the same as that of the Data packet. However, the signature verification requires the producer public key. Information integrated in this packet allows the recovery of this key in another Data packet. A trust mechanism, allowing the requesters to decide whether a public key is acceptable to verify the signature is therefore necessary. NDN doesn't impose any particular trust model, but leaves the choice to applications. Various trust models were proposed. However, each one has some limits and is vulnerable to an identified attack.

To enhance security and to mitigate the identified attack, the authors propose in (Hamdane, Serhrouchni, Fadlallah & Guemara El Fatmi, 2012) an extension. This extension relies mainly on the derivation of this producer public key directly from data name, by using Hierarchical Identity-Based Cryptography (HIBC) (Gentry and Silverberg, 2002). Indeed, in HIBC, any unique single string can form a valid public key. The private key is generated from the public key and the public parameters and the secret key of a trusted Private Key Generator (PKG). By adopting this extension, a requester can verify data packet signatures using directly the corresponding name. This ensures intrinsically producer authentication, data integrity and name authenticity.

In this paper, the authors analyze the security and the trust in NDN. They then extend and improve their earlier work. The first main enhancement relates to the modification of the name structure. With this modification, not only producer authentication, data integrity and name authenticity are insured, but also producer identification and relevance. The second main enhancement relates to the proposal of a model to trust PKG public parameters (necessary in all signing and verification operations). To validate the proposal, it is integrated into the current prototype of NDN. Its formal validation as well as its performance analysis are also provided.