# Chapter 3
# Information-Centric Networking, E-Government, and Security

**Balkis Hamdane**
*Carthage University, Tunisia & University of Tunis – El Manar, Tunisia*

**Sihem Guemara El Fatmi**
*Carthage University, Tunisia*

## ABSTRACT

*The internet was initially proposed to interconnect a few trusted hosts. However, its continued success has caused many security problems. New internet services, such as e-government, must address these security issues. A host-centric security model tied to information location and based on various partial corrections has been proposed. However, this model hasn't brought radical solutions and has largely contributed to architecture ossification. In this context, the idea of a clean slate approach, satisfying the new requirements and without any compatibility obligation, has emerged. The information-centric networking approach represents one of these architectures. Its main idea is to consider the named information as the central element rather than the IP addresses. To ensure security requirements, it adopts an information-centric security. This chapter is a survey on security in the ICN, satisfying the internet security requirements in general and particularly e-government services.*

DOI: 10.4018/978-1-5225-5984-9.ch003

## INTRODUCTION

The e-government concept refers to the use of Information and Communications Technologies (ICT) to implement public services. It aims to facilitate access to government information and services to citizens, businesses and government agencies. When it is set up correctly, it contributes greatly in improving the quality of service. However, it must ensure several challenges. Security represents one of the most important challenges (Sulaiman, Othman, Othman, Rahim, & Pee, 2015; Gorantla, Gangishetti, & Saxena, 2005). This is due to the use of the Internet as a medium of providing e-government services. Indeed, at its design, the Internet focused on the interconnection of a few trusted remote hosts. However, its continued success has caused many security issues and more sophisticated attacks (Lagutin, 2010). Several security protocols have emerged (Dierks, 2008; Frankel & Krishnan, 2011; Weiler & Blacka, 2013). However, in addition to the generated performance problems, each protocol aims to secure a particular protocol and their composition doesn't necessarily guarantee a secure system (Lagutin, 2010). On the other hand, the security model links the security of content to (1) the security of the host storing it and (2) the security of the communication channel used to retrieve it (Yaqub, 2016) (Peltier and Simon, 2012). But a communication channel is not permanent. A user who stores content, previously retrieved from the original source, can't be sure that this content hasn't been modified (by malicious software for example). In addition, a second user interested in the same content can't get it from the first one, although he is geographically closer. He must recover it from the original source, by establishing a secure channel.

In this context, the idea of a revolutionary and a clean slate approach, proposing an alternative architecture for the Internet, was born (Lagutin, 2010). The Information Centric Networking (ICN) approach (Lagutin, 2010; Bari, Rahman Chowdhury, Ahmed, Boutaba, & Mathieu 2012; Weiler & Blacka, 2013; Yaqub, 2016), represents one of the most emerging architecture. This approach considers the named content as the central element rather than the IP addresses, which identify the hosts in the current networks. It also replaces the traditional security model by a content-oriented one. This model is based on the integration of security mechanisms in the content itself as well as the use of an adequate naming system. Thus, citizens can ensure the security of retrieved content, regardless of its source and at any time (Smetters & Jacobson, 2009).

This chapter aims first to present the basic concepts of the ICN approach in general and more particularly those related the security aspect. It also aims to explain how the ICN meets the security requirements in e-government services (Piro et al., 2014). That's why, a use case for an e-government service over ICN is provided. It