Journal of Network and Computer Applications 50 (2015) 73–79

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

An integrated authentication and authorization approach for the network of information architecture

Mahdi Aiash *, Jonathan Loo

School of Science and Technology, Middlesex University, London, UK

ARTICLE INFO

Article history:
Received 28 January 2014
Received in revised form
1 June 2014
Accepted 27 June 2014
Available online 22 July 2014

Keywords:
Network of information
Information centric networks
Formal methods
Authentication
Authorization

ABSTRACT

Several projects propose an information centric approach to the network of the future. Such an approach makes efficient content distribution possible by making information retrieval host-independent and integration into the network storage for caching information. Requests for particular content can, thus, be satisfied by any host or server holding a copy. One well-established approach of information centric networks is the Network of Information (NetInf) architecture, developed as part of the EU FP7 project SAIL. The approach is based on the Publish/Subscribe model, where hosts can join a network, publish data, and subscribe to publications. The NetInf introduces two main stages namely, the Publication and Data Retrieval through which hosts publish and retrieve data. Also, a distributed Name Resolution System (NRS) has been introduced to map the data to its publishers. The NRS is vulnerable to masquerading and content poisoning attacks through invalid data registration. Therefore, the paper proposes a Registration stage to take place before the publication and data retrieval stage. This new stage will identify and authenticate hosts before being able to access the NetInf system. Furthermore, the Registration stage uses (cap)abilities-based access policy to mitigate the issue of unauthorized access to data objects. The proposed solutions have been formally verified using formal methods approach.

1. Introduction

Information-Centric Networking (ICN) is an emerging paradigm envisaged by a growing body of researchers. ICN architectures leverage the role of information as the building block of the Internet architecture as opposed to the current end-host oriented paradigm. ICN architectures have better support for multicast, mobility, and security (Fotiou et al., 2012). In ICN architectures, efficient information dissemination is expected to be supported by dispersing an information item in many network locations using in-network caches and Content Distribution Networks (CDNs) (Sipat et al., 2009).

The Network of Information architecture is an ICN approach developed as part of the Scalable and Adaptive Internet Solutions (SAIL) project (Edwall, 2013). The SAIL NetInf project is centred around a well-defined set of architecture invariants (such as unique naming, location-independence and a strict information-centric service model) and puts particular emphasis on supporting multi-technology/multi-domain interoperability (Kutscher et al., 2013). The project also takes into account developments elsewhere in ICN research (e.g., Content Centric Networking (CCN), Data-Oriented Network Architecture (DONA) and Publish-Subscribe Internetworking Routing Paradigm (PSIRP)) (Teemu et al., 2007; Zhang et al., 2013; Kutscher et al., 2013).

In NetInf, data objects such as web pages, articles or videos are named and identified using the Uniform Resource Identifier for Named Information (URI-ni) format (Baker et al., 2012), hence these objects are referred to as Named Data Objects (NDOs). The NetInf architecture is composed of three main components:

- *The Publishers*: These are NetInf nodes acting as source of NDOs and willing to make these objects accessible to subscribers.
- *The Subscribers* (*or Requesters*): These are NetInf nodes that request specific NDOs.
- *The NetInf System*: This is represented as a network of NetInf routing/forwarding nodes, spanning over the inter-domain topology along which payload data is delivered. Three types of nodes are needed for the operation of the NetInf system: (1) cache-capable nodes to support the functionality of in-network caching of NDOs (2) Name-Based routers which route and forward NDOs towards subscribers and (3) the Name Resolution System (NRS) is a distributed system which is aware of the network locations where an NDO might potentially be available for retrieval.

Generally speaking, the operation of the NetInf architecture goes through two stages: the Publication Stage, where publishers publish

* Corresponding authors.

http://dx.doi.org/10.1016/j.jnca.2014.06.004
1084-8045/

their NDOs to the NetInf system. The Data Retrieval Stage, where subscribers request specific NDOs from the NetInf system. The requested NDOs will be then forwarded to towards the requesting subscribers. These two stages will be explained in Section 2.

Currently, the research concentrates mainly on defining the NetInf overall architecture as well as the structure of the NetInf messages such as the Get-Req/ Get-Resp and Publish-Req/Publish-Resp (more details about these messages in Section 2). The security-related research is still at the stage of defining threat models, highlighting various possible attacks as in Edwall (2013) and defining basic security measures as part of the URI-ni naming scheme (Baker et al., 2012). Therefore, this paper introduces a new approach to address the authentication and authorization issues of implementing the NetInf architecture.

Our main concern here is the security of the Publication Stage, where publishers publish NDOs to the NetInf system. Another major concern is to address the issue of unauthorized access to published NDOs. For a secure publication, two requirements need to be verified namely, the authenticity of publishers and the validity of the published NDOs. Indeed, a malicious node might spoof another publisher ID and publish invalid NDOs. This is very similar to poisoning attacks against Domain Name Server (DNS) or routing tables (Gregg, 2006). To stop such attacks, we need to thwart masquerading threats; therefore, a pre-publication stage, called Registration Stage, is proposed in this paper. During the Registration Stage, both publishers and subscribers need to authenticate themselves with the NetInf system. Therefore, as part of the Registration Stage, we propose a new authentication protocol based on the ID-Based Cryptography (IBC) (Shamir, 1985). The IBC helps to certify the messages sender as the real owner of the NDO that will update the NetInf system. The main advantage of using the IBC over traditional Public Key Infrastructure is that since the public key will be derived from the nodes' identifiers, IBC eliminates the need for a public key distribution infrastructure, details about IBC are in Section 5.2.

To address the issue of an unauthorized access of NDOs, the paper will introduce an authorization and access control approach based on the (cap)abilities-based access control policy (Gollmann, 2011; Chen, 2014). The (cap)abilities-based access control policy has been used to secure the microkernel of the Valencia's Simple Tasker (VSTa) operating system. The proposed authorization (access control) approach is integrated with the proposed authentication protocol as core components of the Registration Stage.tool (Lowe et al., 2009). In summary, the paper's contribution is to introduce an integrated authentication and authorization approach that achieves the following:

- To verify the identity of data publishers and subscribers through a novel ID-Based authentication protocol.
- To tackle the issue of unauthorized access to published data by using a cap(ability)-based access policy.

The proposed security measures have been verified using a formal methods approach based on the Casper/FDR. The rest of this paper is organized as follows: the NetInf system is described in Section 2. Section 3 defines the security problem of the Registration Stage of the NetInf. Section 4 describes some related work. The proposed Registration Stage along with the authentication and authorization mechanisms are presented in Section 5. The paper concludes in the conclusion section.

2. An overview of the NetInf

In NetInf architecture, publishers advertise potential publications in the NetInf system and serve the data contents upon receiving requests. The NetInf system acts as a middleman between publishers and subscribers and is involved in configuring the forwarding path for data delivery (Edwall, 2013). Three pairs of messages have been defined as part of the NetInf architecture:

- The GET-REQ/GET-RESP messages: The GET message is used by a requester to request an NDO from the NetInf network. A node responding to the GET message would send a GET-RESP that is linked to the GET request using the message-Id (msg-id) from the GET message.
- The PUBLISH-REQ/PUBLISH-RESP messages: The PUBLISH message allows a publisher to push the name and a copy of the NDO to the network. A node receiving a PUBLISH message may choose to cache the NDO according to local policy and availability of resources and returns PUBLISH-RESP message, otherwise, it may choose to forward the message to other nodes without sending the response message.
- The SEARCH/SEARCH-RESP messages: The SEARCH message allows the requester to send a set of query tokens containing search keywords. The node that receives the SEARCH message, will either respond if the NDO is in its own cache or forward the SEARCH message.

These messages are supposed to be transported over a Convergence Layer (CL) protocol. As stated in Kutscher et al. (2013), no CL protocol has been defined yet, but any protocol that allows NetInf messages to be passed without loss of information can be used as a NetInf Convergence Layer (NetInf-CL) protocol. These three pairs of message define the transactions of the Publication and Data Retrieval Stages as follows:

1. *The Publish Stage*: Publishers publish their NDOs to the NetInf system by sending the PUBLISH-REQ message to the first hop node which might choose to cache the included information and responds with a PUBLISH-RESP message. Otherwise, it passes the PUBLISH-REQ to the next hop route. A node that caches NDO might update the NRS with the location of the NDO.
2. *The Data Retrieval Stage*: As shown in Fig. 1, the NetInf combines two modes for data retrieval:
   (a) The name resolution: In this mode, the publisher publishes an NDO using PUBLISH message with a Name Resolution Service (NRS). In this case, a requester will approach the NRS first (using the GET message) which will direct him to the information publisher.
   (b) The name-based routing: In this mode, the GET message will be forwarded hop-by-hop between NetInf nodes until a cached copy of the requested NDO is found or the original publisher is reached.

3. Problem definition

In NetInf, like other ICN architectures, the primary goal is to retrieve content from the network, regardless of their locations. As described in the previous section, the NetInf architecture has defined the required messages to publish and retrieve NDOs. However, there is no specified approach to secure these messages, rather, security in NetInf is mainly based on object naming scheme. With the NetInf naming scheme, each NDO is given a unique identifier (ID) with cryptographic properties. Together with additional metadata, the ID can be used to verify data integrity, owner authenticity and several other security properties (Dannewitz et al., 2010). The scheme relies on proven mechanisms like cryptographic hashing and public-key certificate chains to