Challenges and Solutions for Secure Information Centric Networks: A Case Study of the NetInf Architecture

Jonathan Loo and Mahdi Aiash

School of Science and Technology
Middlesex University, UK

Abstract

A large number of emerging Internet applications requires information dissemination across different organizational boundaries, heterogeneous platforms, and a large, dynamic population of publishers and subscribers. A new information-centric network architecture called Network of Information (NetInf) has been developed in the context of the FP7 EU-funded 4WARD project. This architecture can significantly improve large scale information distribution. Furthermore, it supports future mobile networks in situations with intermittent and heterogeneous connectivity and connects the digital with the physical world to enable better user experience. However, NetInf is still in an early stage of implementation and its security is yet to be evaluated. The security concern of NetInf is a major factor for its wide-scale adoption. Therefore, this paper uses the X.805 security standard to analyse the security of the NetInf architecture. The analysis highlights the main source of threats and suggests approaches to tackle them. The paper also defines a threat model against the NetInf and proposes corresponding security services.

Keywords: Network of Information, Information Centric Networks, X.805 standard

1. Introduction

Communication in the current Internet is based on the Client-Server model, where servers share their resources and offer services to clients. In this model,

communicating entities exchange the information among themselves. However, new trends in communication systems place more attention on WHAT data are being exchanged rather than WHO are exchanging them [1] [2]. This led to a new communication model, referred to as Information (or Data)-Centric Networking (ICN). The principal paradigm in this model is not an end-to-end communication between hosts. Instead, an increasing demand for highly scalable and efficient distribution of content has motivated the development of architectures such as [3] [4] [5] [6] that focus on information objects, their properties, and receiver interest in the network to achieve efficient and reliable distribution of such objects [7].

The main reason for advocating the departure to the information-centric model is that the current Internet is mostly used for content access and delivery, with a high volume of digital content delivered to users who are only interested in the actual content rather than the source location [1]. In this sense, content names are decoupled from hosts or servers addresses. So unlike current IP-based addresses which use a single numbering system to identify hosts and define their locations, the ICN separates the roles of identifier and locator, which implies that each data object will be identified, using a unique name called Named Data Object (NDO) without being mapped to a specific location. This will lead to one of the salient features of the ICN which is application-independent caching of contents, where network elements like routers will be able to cache recent contents and resend them when requested by other end-users, called requesters.

Security considerations for ICNs differ somewhat from more typical host-based networking scenarios. Broadly, it can be stated that content-security is more interesting while less interest is needed in channel security, when compared with host-based networking. Keeping this in mind, it is crucial to realize that more traditional threats (e.g., snooping, Denial of Service and Impersonation attacks) still exist in ICN and hence current countermeasures may stay relevant. However, many aspects of handling security in ICNs are only at an early stage of development [8]. **Research efforts in the area ICN security have been mainly focusing on developing new generic mechanisms and security**

measures for ICNs without considering the differences between ICN architectures. Less research efforts considered providing security for specific ICN architectures such as PSIRP and CCNx [?] [5] , respectively.

The NetInf architecture is one example of ICNs that has been initially conceived in the FP7 project 4WARD [?] and then has evolved further during the FP7 project SAIL. Despite the fact that prototype implementations of the NetInf protocol and corresponding applications have already been developed, security in NetInf is still considered as an "Open Issue" in the implementation documents [?]. This is the main motivation for investigating the security-side of NetInf aiming at highlighting the main source of threats and suggesting potential security services. However, there is a need for a systematic approach to evaluate security in NetInf. Therefore, different standards have been considered in this paper such as the The European Network and Information Security Agency (ENISA) [?], the European Telecommunications Standards Institute (ETSI) [?] and the X.805 standard of the ITU Telecommunication Standardization Sector (ITU-T) [9].

The X.805 has been highly regarded as a comprehensive and generic framework for assessing end-to-end security in different networking systems such as the 4G and IEEE 802.15.4 networks [?] [?] as well as in emerging technologies such as the Internet of Things (IoTs), virtualization and Cloud computing as in [?] [?]. Therefore, in this paper, we focus on evaluating the security of NetInf in the light of the ITU-T recommendation X.805 security architecture for end-to-end communication. We identify and assess the security dimensions, planes and layers in NetInf as defined in the X.805 framework. Based on the analyses, we identify potential threats and attacks against the NetInf and highlight possible security services to address them. It is worth pointing out that the main contribution of this paper is to identify

the security threats and corresponding security services rather than to propose solutions in terms of security mechanisms. The authors acknowledge the need for more investigation and research to develop security measures to address the highlighted security threats.

The rest of this paper is organized as follows: Section 2 surveys a number of information centric architectures. More details about the NetInf architecture and an overview of the X.805 standard are given in Section 3. The security discussion based on the X.805 is given in Section 4. The paper concludes in Section 5.

2. An Overview of Information Centric Network Architectures

This section illustrates few of the most-known ICN approaches at a high level with the purpose of providing a general understanding.

2.0.1. Data-Oriented Network Architecture (DONA)

The DONA relies on a new class of network entities called resolution handlers (RHs). Name resolution is accomplished through the use of two basic functions: Register and Find [3]. As shown in Fig 1, initially, nodes that are authorized to act as data sources send Register packets to register their NDOs with the local RH. Each RH will maintain a registration table that maps a name to both a next-hop RH and the distance to the copy (in terms of the number of RH hops, or some other metric). When a client request a specific data (identified by a unique NDO), it sends a Find packet to the local RH, when a FIND arrives, the forwarding rule is straightforward: if there is an entry in the registration table, the FIND is sent to the next-hop RH (and if there is more than one, the choice is based on the local policy and which entry is closest). Once a copy of the data is found, it will be returned through the reverse RH path.

2.0.2. Content-Centric Networking (CCN)

In CCN, NDOs are published at nodes, and routing protocols are used to distribute information about the NDOs location. Communication is initiated by

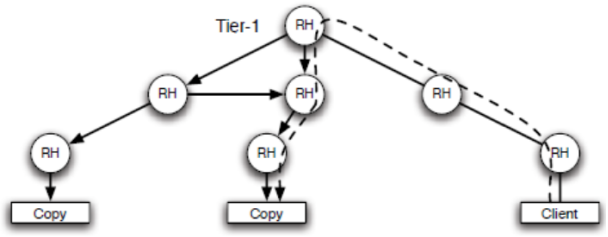

Figure 1: The Registration Stage (solid arrows). Routed Data (dashed arrows) [3]

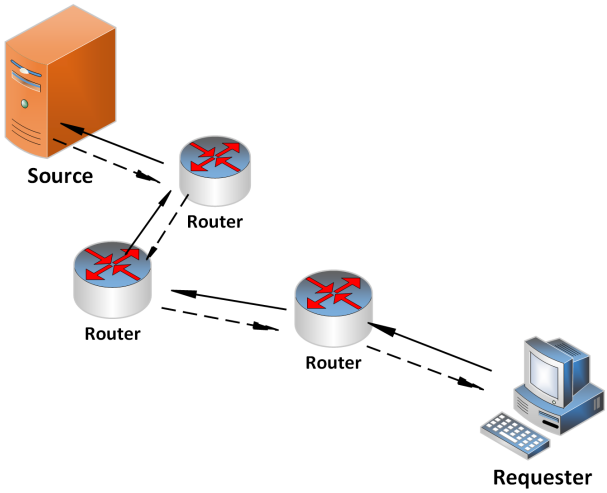

Figure 2: The Request (solid arrows). Forwarded Data (dashed arrows)

issuing a request messages (referred to as Interest). An Interest is routed by a data name instead of a host identifier. Because the data name has a hierarchical structure like a file system pathname such as /CCN.org/cnlab/ccnpaper', each CCN router can forward an Interest in a hop-by-hop manner [4]. A CCN router maintains a pending interest table (PIT) for outstanding requests, this enables request aggregation as a CCN router will not forward a second request for the same NDO. Once a copy of the request data is found, it will be routed back on the reverse request path, as shown in Fig 2.

The CCNx protocol is an open source transport protocol for CCN architecture. Through the implementation of CCNx, a number of

trust and security mechanisms have been proposed such as the mechanisms proposed in [?] to uniquely identify users and devices requesting and publishing contents in CCN architecture.

2.0.3. Publish-Subscribe Internet Routing Paradigm (RSIRP)

This approach is based on the concept of publish/Subscribe (Pub/Sub) model, where hosts can join a network, publish data, and subscribe to publications. However, when a node publishes data, no data transfer actually takes place. Only when a node subscribes to a named piece of data, the network finds the publication and creates a delivery path from the publisher to the subscriber [5]. The network architecture is composed of three modules: Rendezvous module which is a distributed database that maps the wanted data to the subscriber. The Forwarding module, which is used to deliver data from one location to another, the forwarding procedure is based on label switching as each packet will have a label that will help the router to decide on the next hop to forward the packet. The Topology module creates and maintains delivery trees used for forwarding traffic accomplished by the forwarding module. A node publishes its NDOs to Rendezvous and when another node subscribes to this NDO, the publication and Subscription are matched by the Rendezvous module. If there is a tree for the sub/pub, then data transfer starts straight away, otherwise the forwarding module will forward data based on the labels of the packets.

2.0.4. The Green ICN

The Green ICN project [**?**] does not propose a new ICN architecture, rather it optomize current ICN architecture in terms of energy consumption. The project highlights the fact that current ICN proposals do not sufficiently address energy efficiency, hence it investigates new methods for ICN architectures to operate in a highly scalable and energy-efficient way. The GreenICN project focuses mainly two exemplary application scenarios:

- **Disaster scenario:** The focus here is to provide an efficient way to distribute disaster notification and critical rescue information after disasters

where energy and communication resources are at lost level.

- **Video Scenario:** Considering the increasing popularity of on-demand Internet streaming media service such as Netflix and Youtube as well as the wide spread of smart mobile and tablet devices, the majority of Internet traffic is going to be video streaming [**?**]. Therefore, the GreenICN project aims at providing scalable and efficient video delivery system both in normal and disaster situations.

2.0.5. The Named Data Networking (NDN)

Named Data Networking (NDN) is an ongoing research effort that aims to move the Internet into the future with a content-centric design that is capable of efficient content distribution and seamless mobility support, the project is funded by the U.S. National Science Foundation under its Future Internet Architecture Program [**?**]. Communication and data retrieval in NDN is based on two types of packets namely, Interest and Data packets. Data objects are identified using hierarchical addressing structure which also defines the location of data objects. Similar to the DONA architecture, requesters request specific data objects by sending Interest packets which holds the name of requested data objects. Using the included name, Interest packets are forwarded towards data sources. Then, data objects will be routed back to requesters -in Data packets- following the reverse path from the requester to the source [**?**].

2.0.6. The Network of Information (NetInf) Architecture

NetInf is a networking approach that provides access to named data objects (NDOs). Generally speaking NetInf architecture strives to achieve the following [8]

1. To enable access of named objects, and defines a naming scheme for these objects. The NetInf naming scheme is designed to make objects accessible not only via NetInf protocols, but also via other ICN protocols.
2. To perform routing and forwarding based on the NDOs.

3. The NDOs are independent of the location of the object in the network topology.
4. To forward messages between end-points of the network. The message includes a source and a destination identifier from the NetInf name space. This is in analogy with the source and destination address in an IP packet.
5. To support communications between multi-domain NetInf networks.

More details about the NetInf come in the following section.

A number of research papers have discussed the security of different ICN networks in particular the PSIRP architecture as in [17]. The security of CCN architecture has also been investigated and analysed as part of the CCNx project [?]. To the best of our knowledge, no such analysis of the security of NetInf has been introduced.

3. Related Work

3.1. The NetInf Architecture and Elements

On the most basic level, the NetInf network architecture can be viewed as having three distinct parts: publishers hosting and launching the data objects, subscribers or requesters asking for data objects identified by NDOs, and the NetInf's routing/forwarding elements spanning over the inter-domain topology along which payload data is delivered. The publishers advertise potential publications in the NetInf system and serve the data contents to the forwarding layer when it receives a new subscription via the routing layer. The NetInf system acts as a middleman between publishers and subscribers, and is involved in configuring the forwarding path for data delivery [8]. Three pairs of messages have been defined as part of the NetInf architecture:

- The GET/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.

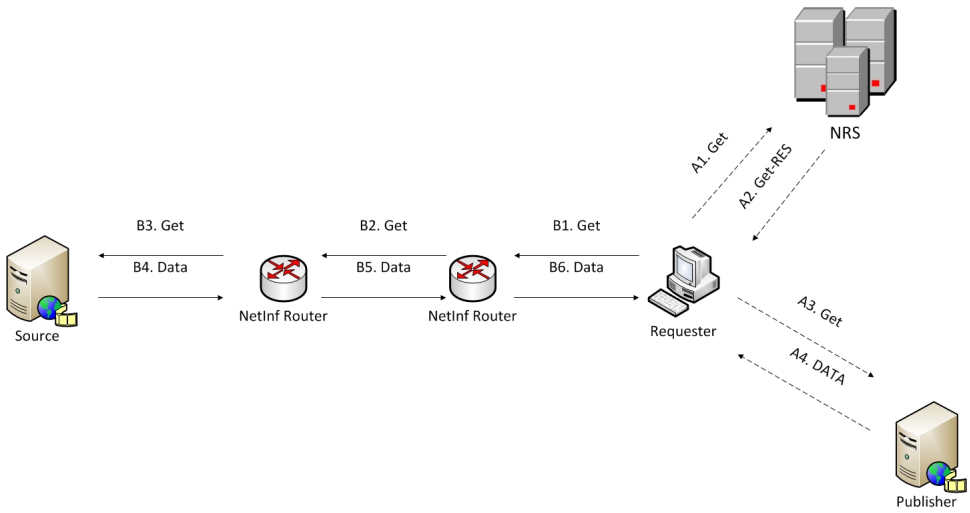

Figure 3: The NetInf Message Flow. The Name Resolution mode (dashed Arrows). The Name-Based Routing (solid Arrows)

- The PUBLISH/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.

As shown in Fig 3,The NetInf combines two modes for retrieving NDOs:

1. 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.

2. 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.

3.2. Standards for Security Analysis

3.2.1. The European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA) is a European Union (EU) agency dedicated to preventing and addressing network security and information security problems. ENISA publishes regular recommendations for implementing and managing a wide spectrum of network and information security technologies such as Cloud Computing, security for on-line services and application [**?**] [**?**].

3.2.2. The European Telecommunications Standards Institute (ETSI)

The ETSI issues standards that provide guidance and support for a comprehensive analysis of threats, vulnerabilities, risks and for the compilation of a specific set of security requirements. Taking into consideration that the security architecture of a particular system is always unique and the threats and security requirements are very specific to that system. The ETSI keeps on issuing standards for implementing individual technologies such as the Global System for Mobile Communications (GSM) [**?**]. Despite the fact that the ETSI has not yet proposed standards for ICN, some already existing standards for managing and implementing security services in emerging technologies such as Next-Generation-Networks (NGN) [**?**] as well as guidelines for security policies in communication systems [**?**] could be beneficial at the stage of implementing security mechanisms in ICN.

3.2.3. The ITU-T X.805 Standard

Network security and reliability become a main concern for service providers, network operators and users. In spite of the importance, threats to networking systems may happen in any layers such as services and infrastructure as well

as any planes such as user and management. Because it is complex to analyze security of networking systems, the The International Telecommunication Union (ITU) developed the X.805 standard as a systematic analysis tool based on the Bell Labs Security Model [3] [10]. By employing a modular approach, the X.805 builds a structured framework that effectively drives consideration of all possible threats and vulnerabilities for end-to-end network security. Moreover it provides a comprehensive, multilayered, end-to-end network security framework across eight security dimensions in order to combat network security threats.

Due to these reasons, the X.805 will be used in this paper to investigate the security threats in the NetInf architecture.

3.3. An overview of the X.805 architecture

As described in [9], the X.805 standard defines three security layers (applications, services and infrastructure), three security planes (end user, control and management) which are identified based on the activities performed over the network, and also eight security dimensions to address general system vulnerabilities (Access Control, Authentication, Non-Reputation, Data Confidentiality, Communication Security, Data Integrity, Availability, and Privacy). The concept of security layers represents hierarchical approach to secure a network; it maps network equipment to different layers and shows how the network elements in upper layers can rely on the security of the lower layers. Security planes represent the types of activities that occur on a network, the concept of security planes could be instrumental for ensuring that essential network activities are protected independently (e.g. compromise of security at the End-user Security Plane does not affect functions associated with the Management Security Plane) [9]. Each security plane is applied to every security layer to yield nine security perspectives and each security perspective has unique vulnerabilities and threats. Figure 4 shows the complete architecture of the X.805 standard including security layers, planes and dimensions.

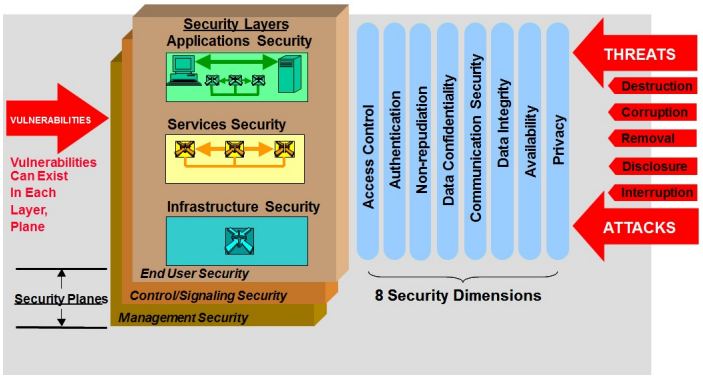

Figure 4: The X805 Architecture

4. Security Evaluation of the NetInf

In this section we apply the X.805 standard to analyse the security of NetInf. The security of NetInf could be discussed at two different levels namely, application and infrastructure.

- **The Application Level:** It involves the data publishers and the subscribers domains, these might neither trust each other nor trust the NetInf infrastructure.

- **The Infrastructure Level:** It consists of the NetInf network elements that provides services such as routing, caching and forwarding to the applications. The infrastructure may not trust publishers and subscribers. Components of the infrastructure such as in-network caching entities may not necessarily trust each other as well.

Considering the X.805 architecture in section 3.3, it is obvious that the functionality of the NetInf is related to the Infrastructure Security Layer which is concerned with the security of network links and elements, and the Application Security Layer which deals with the security of network-based applications accessed by end-nodes. Below, we discuss the eight security dimensions in the context of NetInf operation and try to relate them to the two security layers when feasible:

1. **Access Control:** A potentially major concern for the NetInf architecture is that it does not provide any inbuilt support for an authorization framework or for access control. Once content has been published and cached in the system by routers or end-points, not controlled by the publisher, the publisher has no way to enforce access control, determine which users have accessed the content or revoke its publication. In fact, in some cases, it is even difficult for the publishers themselves to perform access control, where requests do not necessarily contain host/user identifier information [10]. At the Infrastructure Layer, an inappropriate access control policy allows an unauthorized node to access NDOs that were intended for limited audience, not including the unauthorized node. While at the Application Layer, an unauthorized node might publish an object that is intended to be returned to requesters instead of the correct object.

   To address these challenges, access control mechanisms based on encrypting the content could be implemented, but the necessity of distributing keys out-of-band appears to degrade the advantages of in-network caching. This also creates significant challenges when attempting to manage and restrict key access. Another possible solution is by implementing authorization and access control scheme such as the ones presented in [11] [12].

2. **Authentication:** For fully secure content distribution, content access requires that the receiver needs to be able to reliably assess [10]

   - **Data Validity:** To make sure that the received NDOs are complete, uncorrupted copies of what have originally been published;
   - **Data Provenance:** To verify if the receiver can identify the publisher, and if so, whether it and the source of any cached version of the NDO can be adequately trusted.
   - **Data Relevance:** To ensure that the received object fulfils the request that the receiver asked.

   NetInf uses the Named Information (ni) URI scheme [13] to identify content. This allows NetInf to assure validity without any additional infor-

mation but gives no assurance on provenance or relevance. A SEARCH request allows an application to identify relevant content, returned in the SEARCH RESP message.

When operating in the Name Resolution mode, there is a need to achieve an end-to-end authentication which, in this context, means that if subscriber A receives a message claiming to have originated from publisher B, A can verify that B is indeed the publisher of the message. This level of authentication is more relevant to the Application Security Layer of the X.805. While point-to-point is another level of authentication that is relevant to the Infrastructure Security Layer of X.805 and is applicable in the Named-Based Routing operation mode. Point-to-point authentication is concerned only with the immediate end points of communications: if A receives a message from B, A can verify that B is indeed the sender of the message where A and B can be publishers, subscribers or network servers. On one hand, point-to-point authentication could be achieved using current mechanisms such as Public Key Infrastructure (PKI) and digital signature [14], where the publisher will digitally sign the data and the signature will be verified later on by the requester. The problem with such approach is the need for a trusted third party for issuing the digital certificate and distributing the corresponding keys. End-to-end authentication, on the other hand, requires the NetInf system to be trusted and resilient against a wide variety of threats such as impersonation and routers cache poising. One potential solution is to use Naming Security (NS) services which integrate security aspects and the naming concept by providing a cryptographic strength binding between objects' names and the the object returned by the NetInf in response to a request. There are various mechanisms that may be used for this service such as using the Named Information Uniform Resource Identifier (ni URI) [13] to identify content.

3. **Non-repudiation:** There is a need for monitoring and accounting the system's activities; publishers, requesters and NetInf nodes should be held accountable for their actions. When considering the two security layers of

X.805, this dimension can be discussed as follows:

- The Application Security Layer: The importance of this dimension is even more significant in commercial application of the NetInf architecture, where publishers charge requesters for the information they provide. From the requester point of view, they need to make sure that publishers charge them fairly based on their access. While publishers need to audit requesters usage of the system. The nature of the NetInf system, however, means there may be no direct relationship between a publisher and requesters. Furthermore, a publisher has no way of knowing which requesters receive (and should be charged for) particular datagrams.

  One possible solution is to use an out-of-band solution based on the concept of digital signature [15] where a publisher signs the data using its private key and bills subscribers by selling keys that decrypt selected data. Another possible solution is based on the cellular business model [16], in this model both publishers and requesters need to trust the NetInf system to account fairly, the NetInf infrastructure can bill requesters according to the amount of information they receive and pay publishers according to the information they provide without there being any direct relationship between publishers and requesters. The infrastructure would keep track of who received what NDOs at what frequency and who publishes them. Periodically the system would bill the subscribers and send a portion of the payment to the appropriate publishers [17]. Obviously, this solution requires extending the capabilities of the NetInf system to keep track and monitors the system utilization. Furthermore, such system should be scalable to a global scale.

- The Infrastructure Security Layer: At this layer, non-repudiation mechanisms are concerned with assuring that system nodes such as NetInf routers adhere to security rules and are held accountable on

their activities. This means that there is a need for identifying individual nodes at the network-level. One possible solution is the Packet Level Authentication (PLA) protocol [18]. The PLA is based on the assumption that per packet public key cryptographic operations are possible at wire speed in high speed networks due to new cryptographic algorithms and advances in semiconductor technology. It has been used in [19] to provide availability, accountability and to protect the network infrastructure of the PSIRP architecture.

4. **Data Confidentiality:** This security dimension is relevant to both security layers.

   - The Application Security Layer: At this layer, data confidentiality mechanisms are needed to maintain publication confidentiality; can publishers control which subscribers may receive particular publications? [17]. Publication confidentiality might not be relevant in open applications where publishers offers their information and data to everyone. In such applications publishers do not know and perhaps do not care to know the identity of the requesters who receive their information. In other applications, however, it is important that publications be kept secret from ones who are not legitimate subscribers. One possible solution to maintain publication confidentiality is to use one of the group key distribution mechanisms such as [20] [21] [22], where the publisher will pre-distribute keys with all potential requesters. Obviously, this is an out-of-band approach that requires pre-arrangements between the publishers and subscribers.

   - The Infrastructure Security Layer: Data confidentiality at this layer is mainly concerned of preventing data from being exposed while on transit. Keeping in mind the name-based routing operational mode of NetInf, one major issue here is whether publishers and requester should trust the NetInf infrastructure to perform routing without exposing data contents. The severity of this issue increases dramati-

cally when considering the fact that information may travel through network segments that are not necessarily trusted. Enhanced versions of event-notification services such as Siena or Yeast [23] [24] could be deployed. In the Siena system the publications travel along the shortest path from the publisher to the subscribers. Because of the way the routing mechanism works, a network node in Siena only knows its immediate predecessor and successor in the path. End-point anonymity is preserved in any path that has more than two hops.

5. **Communication Security:** Point-to-Point model is the predominant communication model of current host-centric networks such as the Internet. In this model, users need to approach a defined end-point (using the IP address and port number) to access resources; therefore, security is mainly achieved by securing the communication channels between the two end-points, largely via Secure Socket Layer (SSL)/TLS or IPsec VPNs [25] [26]. Unfortunately, such mechanisms will not be as efficient in ICNs: firstly, the concept of point-to-point is different in ICN; requesters request data objects or NDOs without really being aware of their actual location. Secondly, requesters might get chunks of data from different sources none of which might be the publisher, setting up a secure connection with each potential source will be a very time consuming and exhaustive process. Therefore, there is a need to move from connection-oriented into information-oriented design of security mechanisms.

6. **Data Integrity:** This dimension is relevant to both security layers:

   - The Application Security Layer: At this layer the term data integrity involves information integrity, authenticity and validity. Integrity protection methods will ensure that any violation or fabrication of information elements' content will be detectable. Authenticity means that the information that is received by the subscriber is identical with the subscriber's initial request, and it is not forged. Validity

means that the information items announced by the publisher and then forwarded to the subscriber are identical and match the subscriber's request [27].

- The Infrastructure Security Layer: In this layer, concept of integrity refers mainly to system integrity [17]; the Integrity of the NetInf system can be put at risk if malicious faults arise at the infrastructure level (e.g., infrastructure hosts are compromised). A malicious server can insert bogus subscriptions and act as a bogus subscriber to neighbouring servers. Moreover, it can ignore the routing algorithm entirely and route messages to arbitrary destinations or drop them completely.

7. **Availability:** Denial-of-service (DoS) attacks may require more effort on ICN than on TCP/IP but they are still feasible. One reason for this is that it is difficult for the attacker to force repeated requests for the same content onto a single node; ICNs naturally spread content so that after the initial few requests, subsequent requests will generally be satisfied by alternative sources, blunting the impact of a DoS attack [10]. In addition to the standard infrastructure attacks to which all distributed applications are vulnerable, NetInf systems open up some new classes of attacks which are relevant to both security layers.

   - The Application Security Layer: malicious publications and subscriptions can be used to overload the system; subscribers flood publishers with bogus subscription messages

   - The Infrastructure Security Layer: DoS attacks might target the caching and routing plane of the NetInf; attackers might generate loads of unwanted traffic like SPAM which will be cached by intermediate nodes, hence overloading the caching plane and leading to cache overflow. Alternatively, an attacker pollutes the content of a cache, resulting in incorrect returned objects, possibly as a denial of service [8]. The end result is that the efficiency of caches can be

decreased by attackers with the goal of DoS.

To tackle these issues, the NetInf infrastructure needs to make sure that no data should be delivered unless there is a valid subscription from the subscriber. Prevention of unwanted traffic will improve availability, since all parties will be able to serve valid users.

8. **Privacy:** Privacy is a main area where the ICN architectures have not been significantly analyzed [10]. Caching implies a trade-off between network efficiency and privacy. The activity of users is significantly more exposed to the scrutiny of cache owners with whom they may not have any relationship. Although in many ICN architectures, the source of a request is not explicitly identified, an attacker may be able to obtain considerable information if s/he can monitor transactions on the cache and obtain details of the objects accessed, the topological direction of requests and information about the timing of transactions. The persistence of data in the cache can make life easier for an attacker by giving a longer timescale for analysis.

   The privacy issue is relevant to both security layers:

   - The Application Security Layer: The main issue at this layer is the privacy of subscription information; can requesters obtain their requested NDOs without revealing their subscription information and credentials to the publishers or infrastructure?. One possible solution is the Private Information Retrieval mechanisms [28] [29] and secure circuit evaluation mechanisms [30] [17] which enable users to retrieve database entries without disclosing the entries.
   - The Infrastructure Security Layer: At this layer the main concern is exposing the cached information, content can be extracted by any attacker connected to the cache, putting users' privacy at risk.

4.1. Threat Model and Security Requirements

The analysis in Section 4 highlights new threats in ICNs generally and in the NetInf architecture in particular. In this section we will use the analysis

results to define a threat model against the NetInf architecture. Similarly to the analysis approach, the threat models will highlights possible attack scenarios at both the Application and Infrastructure security layers.

1. The Application Security Layer:

   - *False Content Injection (FC)* is where a unauthenticated publishes an object that is intended to be returned to requesters instead of the correct object. This is analogous to actions taken by companies working on behalf of copyright owners in publishing "bad" versions of music, that may contain a warning or advertisement for a legal equivalent of the intended object [8].
   - *Privacy Invasion (PI):* A malicious or a compromised publisher will leak subscription information.
   - *Unauthorized Access (UA):* is where an unauthorized node accesses an object that was intended for a limited audience, not including that node.
   - *False Accusation (FA):* is where a malicious publisher attempts to make it appears as if a requester has requested an object , when that is not in fact the case. For example, the malicious publisher might charge a subscriber for information s/he never requested or acquired.

2. The Infrastructure Security Layer:

   - *Unauthorized Cache Access (UCA):* is where an unauthorized node accesses a cached object from a local router.
   - *Privacy Invasion (PI):* The SEARCH message of NetInf architecture enables routers and nodes to check the cache contents of other nodes. In the case of edge routers, knowing this information will enable an active attacker to get an idea about the sort of activities, local nodes or requesters are doing. More seriously, an attacker might be able to predict the next NDO to be fetched.
   - *Cache Misuse (CM):* Caches could be misused in the following ways:

Threat Model	
The Application Security Layer	False Content Injection Privacy Invasion Unauthorized Access False Accusation
The Infrastructure Security Layer:	Unauthorized Cache Access Privacy Invasion Cache Misuse Routing Misuse

Table 1: Threat Model defines potential attacks at two layers

(a) Attackers can use caches as storage to make their own content available.

(b) Attackers pollutes the content of a cache, resulting in incorrect returned objects, possibly as a denial of service.

- *Routing Misuse (RM):* Attackers might compromise a router and modify the routing plane so that transactions are routed in a way beneficial to the bad-actor, but detrimental to some other legitimate subscribers. Furthermore, attackers might direct all traffic to a compromised publisher where provided NDOs have malicious codes such as malware or trojan horses.

Security Layer	Attacks	Security Services
Application Layer	False Content Injection	Data Origin Authentication Content Authentication Services Authorization Services Unauthorized Access False Accusation
		Out-of-band PKI Distributed auditing systems
Infrastructure Security Layer	Unauthorized Access to cached data Cache Misuse Routing Misuse	Zoning techniques Data Provenance services Trusted Computing
Application and Infrastructure Layers	Privacy Invasion	Privacy preserving Services

4.2. Security Services

In order to tackle the threats highlighted in the above threat model, this section will describe potential security services and mechanisms that could be integrated with the NetInf architecture.

1. *False Content Injection (FC):* For successful FC, an attacker needs to bypass the authentication, authorization and access control mechanisms and being able to impersonate a legitimate publisher. Therefore, to mitigate this threat, there is a need for a combination of security services:

   - Data Origin Authentication (OA): This service enable requesters to verify that data has been generated and published by expected publisher. Example of such service is the digital signature algorithm to provide "proof of origin", and also allowing sensitive message contents to be protected from tampering as will be discussed later on.
   - Content Authentication (CA): This service aims to verify that the data or NDO is genuine and real; not counterfeit or copied. Such service could be achieved by including extra information in the meta-data of the NDO that verify the publisher, time of publication, copy or original, etc. It is crucial however, to maintain meta-data integrity.

- Authorization (AZ): It refers to the general ability of an entity to control which other entities are supposed to be able to gain access to an object. Different approaches could be used to enforce this service such as centralized authorization and access control mechanisms such as RADIUS and DIAMETER [31] [32] or distributed authorization mechanisms such as the one in [33]

2. *Privacy Invasion (PI):* As described in the Threat Model, the PI is possible at the Application and Infrastructure levels. Privacy preserving mechanisms such as onion-routing (the TOR for example [34])or other obfuscatory routing schemes may provide a certain level of privacy. Furthermore, the fact that in-network stores return objects may also act so as to make tracking user actions more difficult. However, the fact that in-network stores cost money will likely result in their operators being willing to share information, including tracking information, with third parties.
3. *Unauthorized Access (UA):* As explained in section 4, an out-of-band approach, based on the PKI could be used to share keys between the publisher and the potential requesters. Only requesters with the valid corresponding keys will be able to get the data.
4. *False Accusation (FA):* In order to address this threat, there is a need for an efficient auditing system that logs all activities, distributed audit service such as XDAS [35] could be used for this reason.
5. *Unauthorized Access to cached data (UAC):* Due to the feature of in-network store/cache of the ICNs, attackers might get access to data cached in local routers. One possible solution for this threat is by using the Scope concept [19]. Scopes are abstract entities that control how publications are disseminated. The scope authorizes one or more data sources such as routers to host/cache the publication data or NDOs.
6. *Cache Misuse (CM):* To mitigate this threat, evidence gathering mechanisms would be required, along with cryprographic and time based mechanisms in order to provide a data Provenance service and making sure that

data has been cached by an expected router.

7. *Routing Misuse (RM):* This threats highlights the issue of the trustworthiness and integrity of the NetInf infrastructure. One possible solution is based on the concept of Trusted Computing [36]. Trusted computing is an approach to build systems such that their integrity can be verified. It is based on the concept of transitive trust where initial trust in a hardware module is delegated to other system components. The industry standard trusted hardware module is the Trusted Platform Module (TPM) [37].

5. Conclusion

NetInf is an information-centric communication paradigm that supports dynamic, many-to-many communications in a distributed environment. In such an environment, publishers publish information in the form of events and subscribers have the ability to express their interests in an event or a pattern of events by sending subscription filter to the NetInf network. Despite the fact that some desired security features have been provided in NetInf using the a newly developed naming scheme, there is still a need for a thorough security analysis to highlight any potential threat. Therefore, the paper investigates the security issue of the NetInf architecture using the X.805 standard. Eight security threats have been analysed and discussed in that context. The paper also discusses a number of proposals to secure NetInf. The discussion highlights the fact that different proposals have addressed different security threats; however, no integrated approach has been proposed to address all of them. Therefore, our future work is to develop a comprehensive security framework that addresses the highlighted security threats in this paper.

References

[1] G. X. G. P. G. K. Katsaros, C. Stais, On the incremental deployment of overlay information centric networks, Future Network and Mobile Summit (2010) 1–8.

[2] L. Y. L. T. W. Z. N. W. T. H. C. S. Xu, Y., A novel cache size optimization scheme based on manifold learning in content centric networking, Journal of Networks and Computer Applications (2014) 273–281.

[3] M. C. K. K. I. S. B. C. T. Koponen, A. Ermolinskiy, S. Shenker, A data-oriented (and beyond) network architecture, SIGCOMM (2007) 181–192doi:10.1145/1282380.1282402.

[4] D. Kim, J. Kim, Y. Kim, H. Yoon, I. Yeom, Mobility support in content centric networks, SIGCOMM, (2012) 13–18doi:10.1145/2342488.2342492.

[5] T. T. M. Sarela, T. Rinta Aho, Rtfm: Publish/subscribe internetworking architecture, ICT Mobile Summit.

[6] E. D. D. Kutscher, S. Farrell, The netinf protocol, Internet Draft.

[7] C. I. D. K. B. O. B. Ahlgren, C. Dannewitz, A survey of information-centric networking, IEEE Communication Magazine 50 (2012) 26–36. doi:10.1109/mcom.2012.6231276.

[8] T. Edwall, The network of information: Architecture and applications.

[9] Z. Zeltsan, Itu-t recommendationx.805 and its application to ngn.

[10] E. D. S. S. G. B. P. M. K. Pentikousis, B. Ohlman, Information-centric networking: Evaluation methodology, Internet-Draft.

[11] K. M. A. C. Abdelberi, D. Emiliano, U. Ersin, Privacy in content-oriented networking: Threats and countermeasures, SIGCOMM Comput. Commun. Rev 43 (2013) 25–33. doi:10.1145/2500098.2500102.

[12] M. G. F. F. Nikos, P. G. C., Access control enforcement delegation for information-centric networking architectures, ICN (2012) 85–90doi:10.1145/2342488.2342507.

[13] C. D. B. O. A. K. P. H.-B. S. Farrell, D. Kutscher, Naming things with hashes, Request for Comments: 6920.

[14] A. Carlisle, L. Steve, "Understanding PKI: concepts, standards, and deployment considerations, Addison-Wesley Longman Publishing Co., Inc., 2002.

[15] M. Wenbo, Modern Cryptography: Theory Practice, Prentice Hall Professional Technical Reference, 2003.

[16] A. L. J. L. M. Aiash, G. Mapp, A secure framework for communications in heterogeneous networks, AINA.

[17] D. E. A. W. C. Wang, A. Carzaniga, Security issues and requirements for internet-scale publish-subscribe systems, HICSS (2002) 118–173.

[18] D. G. Andersen, T. K. D. M. S. S. H.Balakrishnan, N. Feamster, Holding the internet accountable, 6th ACM Workshop on Hot Topics in Networking (96Hotnets).

[19] A. D. Lagutin, K.Visala, Roles and security in a publish/subscribe network architecture, ISCC (2010) 68–74.

[20] O. K. W. William, Y. Alec, P. Ramesh, A technique for remote authenticationdoi:10.1016/0003-4916(63)90068-X.

[21] M. D. S. R. M. Needham, Using encryption for authentication in large networks of computers, Communications of the ACM 21 (1978) 993–999.

[22] H. Chen, A multi-issued tag key agreement with time constraint for homeland defense sub-department in nfc environment, Journal of Network and Computer Applications (2014) 88–98.

[23] D. R. A. Carzaniga, A. Wolf, Design and evaluation of a wide-area event notification service, ACM Transactions on Computer Systems 19 (2001) 332–383.

[24] J.-T. L. Ki-Yeol Ryu, An enhancement of siena event routing algorithms, Information Networking: Wireless Communications Technologies and Network Applications 2344 (2002) 623–633. doi:10.1007/3-540-45801-8_59.

[25] T. P. S. Turner, Prohibiting secure sockets layer (ssl) version 2.0, Request for Comments: 6176.

[26] R. A. S. Kent, Security architecture for the internet protocol, Request for Comments: 2401.

[27] G. C. P. N. Fotiou, G. F. Marias, Publish-subscribe internetworking security aspects, Trustworthy Internet (2011) 3–15doi:10.1007/978-88-470-1818-1_1.

[28] E. K. B. Chor, O. Goldreich, M. Sudan., Private information retrieval, FOCS (1995) 41–50.

[29] T. M. G. Di Crescenzo, R. Ostrovsky., Single database private information retrieval implies oblivious transfer, EUROCRYPT.

[30] M. Abadi, J. Feigenbaum, On hiding information from an oracle, In the proceedings of the Ninth Annual ACM Conference on Theory of Computing (1987) 195–203.

[31] A. L. A. DeKok, Remote authentication dial-in user service (radius) protocol extensions, Request for Comments: 6929.

[32] E. G. G. Z. J. A. P. Calhoun, J. Loughney, Diameter base protocol, Request for Comments: 3588.

[33] S. L. T.Y.C. Woo, Designing a distributed authorization service, Infocom 2 (1998) 419–429. doi:10.1109/INFCOM.1998.665058.

[34] Anonymity online.
URL https://www.torproject.org/docs/tor-manual.html.en

[35] T. O. Group, Distributed audit service (xdas) (1998).

[36] R. Anderson, Cryptography and competition policy - issues with trusted computing, in Economics of Information Security, from series Advances in Information Security 12.

[37] D. P. Solutions, Enhancing it security with trusted computing group standards.