Security Attacks in Information-Centric Networking

Chanda Tejaswini[1] Dr.M.I.Thariq Hussan[2] Vamshi Priya[3] E.Harika[4]

[2]Professor & Head,[1,3,4]B.Tech Scholars,

Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad-501506, Telangana, India

ABSTRACT

Information-centric networking (ICN) is an approach to evolve the Internet infrastructure away from a host-centric paradigm based on perpetual connectivity and the end-to-end principle, to a network architecture in which the focal point is named information. In this paradigm, connectivity may well be intermittent, end-host and in-network storage can be capitalized upon transparently, as bits in the network and on data storage devices have exactly the same value, mobility and multi access are the norm and anycast, multicast, and broadcast are natively supported. Data becomes independent from location, application, storage, and means of transportation, enabling in-network caching and replication. ICN is a new communication standard that focuses on content retrieval from the network regardless of storage location or physical representation of this content. The ICN concept is a significant common approach of several future Internet research activities. The approach leverages in-network caching, multiparty communication through replication, and interaction models decoupling senders and receivers. In ICN, securing the content itself is much more important than securing the infrastructure or the endpoints. To achieve the security goals in this new paradigm, it is crucial to have a comprehensive understanding of ICN attacks, their classification, and proposed solutions. In this paper, we provide a survey of attacks unique to ICN architectures and other generic attacks that have an impact on ICN. The ICN approach is being explored by a number of research projects.

Keywords: ICN, Attacks, Security.

1. INTRODUCTION

ICN architecture focus on contents or information objects and their properties in the network. ICN is also concerned about receiver interests and relies on location independent naming, in network caching, and name-based routing. In ICN, senders do not send content directly to receivers. A sender publishes advertisement messages to tell the network that it has some content to share, without necessarily knowing who may be interested in it. On the other side, a receiver declares its interest for some content, not necessarily knowing the senders who have published this content. The ICN network makes a delivery path from the sender to the receiver when there is a match between sender's publication and receiver's subscription. Finally, the content is transferred to the receiver.

ICN architectures focus on contents or information objects and their properties in the network. ICN is also concerned about receiver interests. ICN relies on location independent naming, in network caching, and name-based routing. We explore ICN security, privacy, and access control concerns in-depth, and present a comprehensive study of the proposed mechanisms in the state of the art. We categorize this survey into three major domains, namely security, privacy, and access control. In the security section, we address denial of service (DoS and distributed DoS) attacks and vulnerabilities unique to ICN, including cache pollution, content poisoning, and naming attacks. Despite many similarities between a classical DoS attack and the DoS attack in ICN, the latter is novel in that it abuses ICN's forwarding plane. The attack aims to overload a router's state tables, namely the pending interest table (PIT). The cache pollution attack targets a router's content locality with

the intention of altering its set of cached content resulting in an increase in the frequency of content retransmission, and reduced network goodput.

2. RELATEDWORK

2.1. Content Centric Networking (CCN)

CCN emphasizes content by making it directly addressable and routable. Endpoints communicate based on named data instead of IP addresses. CCN is characterized by the basic exchange of content request messages and content return messages. It is considered an information-centric networking (ICN) architecture. The goals of CCN are to provide a more secure, flexible and scalable network thereby addressing the Internet's modern-day requirements for secure content distribution on a massive scale to a diverse set of end devices. CCN embodies a security model that explicitly secures individual pieces of content rather than securing the connection or "pipe". It provides flexibility by using data names instead of host names (IP addresses). Additionally, named and secured content resides in distributed caches automatically populated on demand or selectively pre-populated. When requested by name, CCN delivers named content to the user from the nearest cache, traversing fewer network hops, eliminating redundant requests, and consuming less resources overall [1].

2.2. Named Data Networking (NDN)

NDN is a future internet architecture inspired by years of empirical research into network usage and a growing awareness of unsolved problems in contemporary internet architectures like IP. NDN has its roots in an earlier project, Content-Centric Networking (CCN), which Van Jacobson first publicly presented in 2006. The NDN project is investigating the proposed evolution from today's host-centric network architecture IP to data-centric network architecture (NDN). The belief is that this conceptually simple shift will have far-reaching implications for how people design, develop, deploy, and use networks and applications. Its premise is that the Internet is primarily used as an information distribution network, which is not a good match for IP, and that the future Internet's "thin waist" should be based on named data rather than numerically addressed hosts. The underlying principle is that a communication network should allow a user to focus on the data he or she needs, named content, rather than having to reference a specific, physical location where that data is to be retrieved from, named hosts. The motivation for this is derived from the fact that the vast majority of current Internet usage consists of data being disseminated from a source to a number of users. Named-data networking comes with potential for a wide range of benefits such as content caching to reduce congestion and improve delivery speed, simpler configuration of network devices, and building security into the network at the data level [2].

3. FRAMEWORK

Caching can be defined as having information, data and object temporarily saved in a location for predictive usage on frequent or closely related interval. Content caching as it relates to ICN is our concern in this work. Caching therefore will help in reducing the high cost in up streaming and down streaming of data, information and interest in ICN. Several studies have been conducted in recent times to curb the issues of caching in the web as it can be related to ICN. These include approaches borrowed and enhanced from the previous caching techniques on the web. However, with all the contributions and proposed ideas in ICN popular architectures (Xylomenos et al., 2013; Ahlgren et al., 2012; Tyson et al., 2013), the standardization of in-network and off-network caching is yet to be reached. We therefore aim at exposing the salient features worked upon on this issue (caching). Previously discussed ICN architectures and projects (CCN, DONA, PSIRP and NetInf) itemized the various forms of caching; thereby identifying the on-path off-path node caching. Various studies such as (Hassan et al., 2013; Nagaraj, 2014; Podlipnig and Böszörmenyi, 2003) suggested ways to fulfill the ICN dream of being promising with its advantages but caching being the common issue in all aforementioned ICNs. Major advantages of caching as mentioned earlier will reduce traffic, redundancy of information, bottle neck queuing and competitiveness on frequently accessed or visited domains. Some benefits enjoyed when the

cache is in place will include: better utilization of bandwidth, thereby reducing information wastes and high garbage collection (misuse of memory).

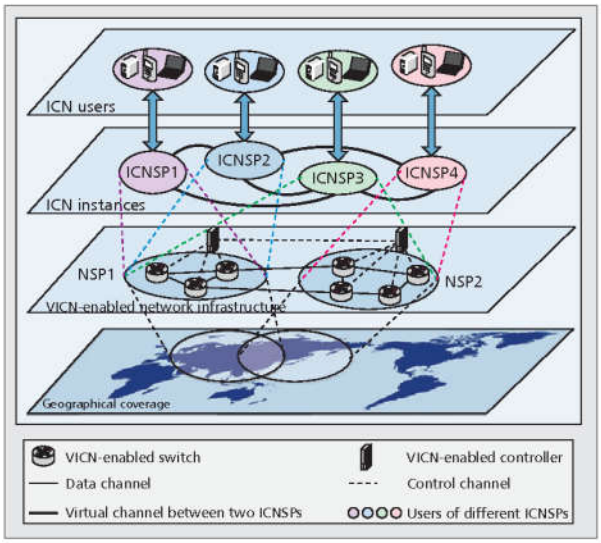

Figure 1. An overview of the VICN deployment scenarios.

However, to benefit from the advantages of caching, one may wonder when and how can caching be done? A study in (Sen Wang and Jun, 2013) however, suggested some ways of collaborative approach to propose key additions to caching in ICN architecture. The question still remains very challenging, particularly as it relates to ICN. We are going to expose caching in this section by relating caching in the context of ICN through types and forms of caching in the traditional internet.

4. FUNCTIONALITY

CCN (Jacobson et al., 2009) a popular and easily understandable ICN architecture. Its operations is in the form of client making a request into the network without necessarily specifying the address of who gives what information and how? This is solved by routing the request/interest sent by client 1 from (CCN) through a router/node that communicates with its neighbors (client 2 and 3) in search of an answer to that request. Subsequently, if the requested interest is identified at the first router, it is then routed back to the requester [4]. This forecast is part of the Cisco® Visual Networking Index (VNI), an ongoing initiative to track and forecast the impact of visual networking applications. This document presents the details of the Cisco VNI global IP traffic forecast and the methodology behind it. For a more analytical look at the implications of the data presented below, please refer to the companion document, The Zettabyte Era, or the VNI Forecast Highlights tool [3]. A CDN is a collection of network elements arranged for more effective delivery of content to end-users. Collaboration among distributed CDN components can occur over nodes in both homogeneous and heterogeneous environments. CDNs can take various forms and structures. They can be centralized, hierarchical infrastructure under certain administrative control, or completely decentralized systems. There can also be various forms of internetworking and control sharing among different CDN entities [5]. Mobile IP has been designed within the Internet Engineering Task Force (IETF) to serve the needs of the burgeoning population of mobile computer users who wish to connect to the Internet and maintain communications as they move from place to place. The basic protocol is described, with details given on the three major component protocols: agent advertisement, registration, and tunneling. Then route optimization procedures are outlined, and further topics of current interest are described [6]. There has been much interest in emerging Peer-to-Peer (P2P) network overlays because they provide a good substrate for creating large-scale data sharing, content distribution and application-level multicast applications. These P2P networks try to provide a long list of features such as: selection of nearby peers, redundant storage, efficient search/location of data items, data permanence or guarantees, hierarchical naming, trust and authentication, and anonymity [7]. PSIRP initiates

its operation by the subscriber sending interest/ request to a rendezvous handler at the client side. The operation is then followed by a subscription through the closest router station. This is however possible if the resulted interest has been met as a result of either a cache hit or published. Topology manager provides a route for the delivery of the required interest. The information produced by things, or associated with things, will be both huge and sensitive. For this reason new architectures for disseminating and processing this information in a reliable and efficient way should be explored. In this paper, we present architecture for the IoT, based on the Information-Centric Networking (ICN) paradigm. ICN architectures are built around information and information identifiers and they provide mechanisms for advertising, finding, and retrieving information [8]. Naming in this architecture is done uniquely by some statistical identities in pair. Figure 3 shows the functional decomposition of the proposed architecture: front-end servers offer an Application Programming Interface (API) and an internal engine that satisfies client requests by using the ICN based procedures, hereafter described. The back-end servers are composed by an ICN interface that deals with ICN packets received-from or going to the front-end servers, and by a local database engine that handles the local storage space.

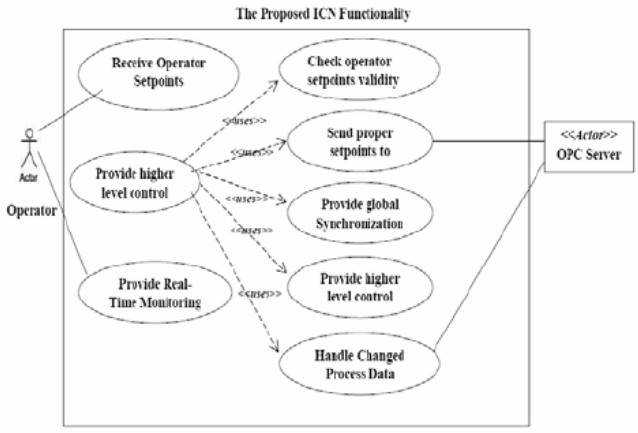

Figure 2: Proposed functionality of ICN

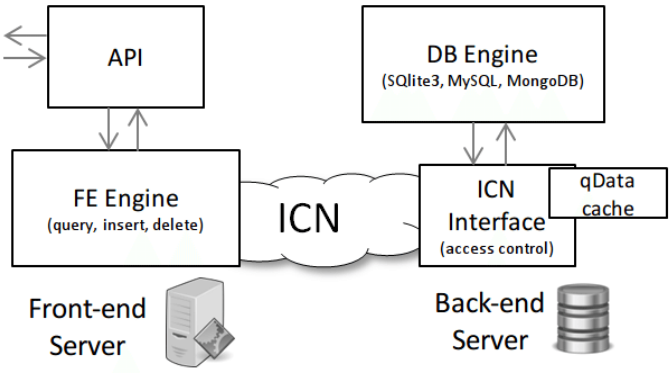

Figure 3: Front-end and back-end server functionality

5. CONCLUSION

In this survey, we have comprehensively explored the existing work in the domain of ICN security. We divided the content into three major sub-domains: security, privacy, and access control enforcement. We reviewed the existing work in each sub-domain, and highlighted the drawbacks and benefits of each proposed solution. Additionally, we provided potential future research directions to explore to overcome the mentioned shortcomings. In security section, we explored attacks such as denial of service, content poisoning, and cache pollution, and also presented the proposed models for secure naming, routing, and applications. The existing works in this sub-domain aim to prevent adversaries from degrading the user QoS and QoE through malicious behavior, such as interest flooding, cache pollution. Among

these attacks, DoS is the most widespread and the easiest to mount. A simple rate limiting approach can mitigate the impact of the attack to some extent; however, it also can starve legitimate clients. Thwarting content poisoning attack, despite its detection simplicity, requires computational resources at the intermediate routers, which makes it more severe. The fundamental principles of ICN should be closely followed during the design of new security mechanisms. Here, we specifically refer to the necessity of efficient access control enforcement mechanisms that are in agreement with ICN principles. ICN, in principle, promotes content availability by allowing pervasive caching, and hence requires more advanced, service-independent access control mechanisms. In this survey, we have identified some initial attempts towards an independent access control mechanism that can be enforced by any network caching entities efficiently. In this context it is not clear if there is a specific architecture that stands out as best for access control; but we note that all architectures are nascent and still under a lot of flux.

REFERENCES

1. https://en.wikipedia.org/wiki/Content_centric_networking
2. https://en.wikipedia.org/wiki/Named_data_networking
3. Cisco visual networking index: forecast and methodology:2013-2018," Cisco, Tech. Rep., June 2014[Online]. Avail-able:http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white paper c11-481360.pdf
4. V. Jacobson, D. Smetters, J. Thornton, M. Plass, N.Briggs, and R. Braynard, "Networking named content," in Proc. 5th Int'l Conf. Networking Experiments and Technologies (CoNEXT'09). Rome, Italy, Dec. 2009.
5. A. M. K. Pathan and R. Buyya, "A taxonomy and survey of content delivery networks," Grid Computing and Distributed Systems Laboratory, University of Melbourne, Technical Report, 2007. [Online]. Available: http://www.buyya.com/gridbus/cdn/reports/CDN-Taxonomy.pdf
6. C. E. Perkins, "Mobile IP," IEEE Commun. Mag., vol. 35, no. 5, pp. 84–99, May. 1997.
7. E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," Commun. Surveys Tuts., vol. 7, no. 2, pp. 72–93, 2005.
8. G. Xylomenos, X. Vasilakos, C. Tsilopoulos, V. A. Siris, and G. C. Polyzos, "Caching and mobility support in a publish-subscribe internet architecture," IEEE Commun. Mag., vol. 50, no. 7, pp. 52–58, Jul. 2012.