ISSN: 2321-7782 (Online)
Volume 3, Issue 12, December 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Service Centric Networking Based Queue and Latency Aware Service Selection Process

Dr. K. Swathi[1]
Professor and Principal,
Department of Computer science &Engineering,
Cauvery College of Engineering & Technology,
Trichy (TN)

B. J. Vidhaya[2]
Scholar,
Department of Computer science &Engineering,
Cauvery College of Engineering & Technology,
Trichy (TN)

Abstract: ***Information-centric networking (ICN) is a new communication paradigm that focuses on content retrieval from the network regardless of storage location or physical representation of this content. In ICN, securing the content itself is much more important than securing the infrastructure or the end-points. To achieve the security goals in this new paradigm, it is crucial to have a comprehensive understanding of the 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. It also provides taxonomy of these attacks in ICN, which are classified into four main categories: naming, routing, caching, and other miscellaneous related attacks. Further, the paper shows the relation between ICN attacks and unique ICN attributes; ICN attacks and security requirements: confidentiality, integrity, availability, and privacy. Finally, the paper presents the severity levels of ICN attacks and discusses the existing ICN security solutions.***

I. INTRODUCTION

ACCORDING to Cisco Visual Networking Index 2013, global IP traffic per month will reach approximately 126 Exabytes and the sum of all forms of video will be between the range of 80 to 90 percent of global consumer traffic by the year 2017. These new requirements of increasing demand for highly scalable and efficient distribution of content require new alternative solutions for the upcoming internet era, as the existing internet architecture is becoming inadequate. Information-centric networking (ICN) is one of these alternatives. ICN architectures focus on contents or information objects and their properties in the network. ICN is also concerned about receiver interests. In order to achieve these goals, ICN relies on location independent naming, innetwork 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 has some similarities and differences with other related technologies like distributed database (DDB), data grids, peerto- peer networks (P2P), content distribution networks (CDN), and cloud computing. ICN is considered as a new architecture in terms of naming, routing, caching, and security.

One of the major components in the new paradigm is the "security" component. ICN changes the security model from securing the path to securing the content, which is available to all ICN nodes. As a consequence, new attacks have appearedwith this new security model in addition to the legacy attacks that may have an impact on ICN. The security in ICN will be an integral part of the architecture rather than added as an overlay.

II. RELATED WORK

Title: Enhancing cache robustness for content-centric networking

Authors: M. Xie, I. Widjaja, and H. Wang

Published In : Proc. of the IEEE Infocom, 2012.

With the advent of content-centric networking (CCN) where contents can be cached on each CCN router, cache robustness will soon emerge as a serious concern for CCN deployment. Previous studies on cache pollution attacks only focus on a single cache server. The question of how caching will behave over a general caching network such as CCN under cache pollution attacks has never been answered. In this paper, we propose a novel scheme called CacheShield for enhancing cache robustness. CacheShield is simple, easy-to-deploy, and applicable to any popular cache replacement policy. CacheShield can effectively improve cache performance under normal circumstances, and more importantly, shield CCN routers from cache pollution attacks. Extensive simulations including trace-driven simulations demonstrate that CacheShield is effective for both CCN and today's cache servers. We also study the impact of cache pollution attacks on CCN and reveal several new observations on how different attack scenarios can affect cache hit ratios unexpectedly.

Title: A survey of information-centric networking

Authors: B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman,

Published in: IEEE Communications Magazine, vol. 49, no. 7, July 2012, p. 26-36

The information-centric networking (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. The goal is to provide a network infrastructure service that is better suited to today¿s use (in particular. content distribution and mobility) and more resilient to disruptions and failures. The ICN approach is being explored by a number of research projects. We compare and discuss design choices and features of proposed ICN architectures, focusing on the following main components: named data objects, naming and security, API, routing and transport, and caching. We also discuss the advantages of the ICN approach in general.

Authors: A. Mohaisen, X. Zhang, M. Schuchard, H. Xie, and Y. Kim

Title: Protecting access privacy of cached contents in information centric networks

Published in: SIGCOMM13, Hong, Kong, China, May 2013, pp. 1001-1003

In information centric network (ICN), contents are fetched by their names from caches deployed in the network or from origin servers. Once the contents are fetched from the origin server, it is replicated and cached in all routers along the routing and forwarding paths from the user that issues the interest to the origin server, thus allowing further "interests" by other users to be fulfilled quickly. However, the way ICN caching and interest fulfillment work pose a great privacy risk; the time difference between response for interest of cached and uncached contents can be used as an indicator to infer whether or not a near-by user previously requested the same contents requested by the adversary. This work introduces the extent to which the problem is applicable in ICN and provides several solutions to address it.

III. MODULES

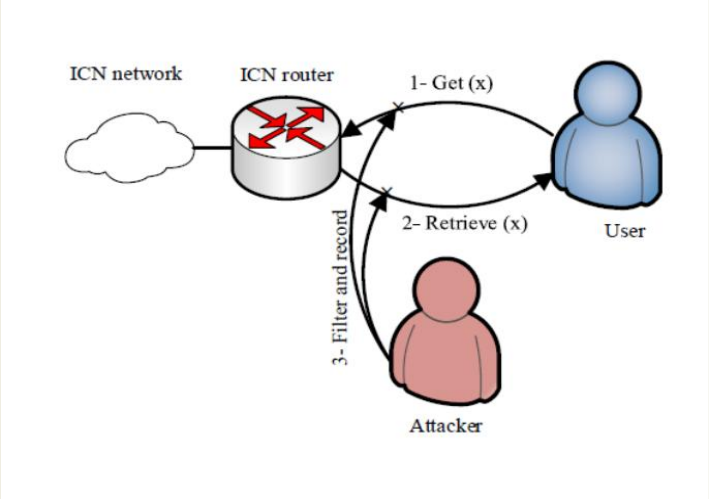
Naming related attacks

The attacks in this category can be classified into watchlist and sniffing attacks. In ICN, the network nodes can access user requests The attacker uses this attribute in addition to location independent naming to perform these types of attacks. There is a generic assumption that the attacker who compromises an ICN node or router can access it and monitor requesters. In an ICN,

there is no host identifier; hence an attacker needs to compromise an ICN node in order to track requesters and record who requested what. For content filtration and/or deletion attack, this assumption is not required at all.

a) Watchlist:

An attacker has a predefined list of content names that he/she wants to filter or delete. Then the attacker monitors network links to perform a real-time filtering. The attacker may delete the request and/or record requester's information, in case of any matching against the predefined list. In addition, the attacker may try to delete the matched content itself. As depicted in Figure 3, the attacker captures user requests to filter and record who requested what. The attacker also filters and records return contents, which contain information about the publisher and the data. The filtration is based on the attacker's predefined list.



b) Sniffing:

Unlike the predefined list in the watchlist attack, the attacker monitors the network to check the data if it should be marked in order to filter or eliminate it. The data should be marked if it contains the specified keywords. The attack scenario is the same as the watchlist attack. The main difference is that the attacker does not have a predefined list, but he/she makes some analysis on requests or on the content.

Naming related attacks have an impact on the following:

Censorship: Using the naming related attacks, an attacker can censor the contents that he/she wishes.

Privacy: Using these types of attacks, an attacker can monitor the content requests of a large number of users and knows about the requesters. The ICN network accesses the user's requests, which results in a worse privacy situation.

Denial of service: An attacker prevents user's requests for the marked content, leading to unanswered requests.

Routing related attacks

The attacks in this category can be classified into distributed denial of service (DDoS) and spoofing attacks. The DDoS attacks can be classified into resource exhaustion and timing attacks. Resource exhaustion can be categorized into infrastructure, source, mobile blockade, and flooding attacks. Spoofing attacks can be divided into jamming, hijacking, and interception attacks. Infrastructure. An attacker sends a large number of requests for available/unavailable content. As ICN architectures try to find the closest copy from the best available location, these requests take different routes towards the source causing overload conditions. If the number of these requests is significantly high, it leads to a denial of service. This attack may be further amplified, as regular users send retransmission requests after a specified time. Similar to the hijacking attack, this threat can be mitigated because routing mechanisms in ICN attempt to route towards multiple locations. As illustrated in Figure 4, the attacker, who controls many end systems, sends a large number of requests to one or more ICN routers to fill the routing table

and exhaust processing and memory resources. As a consequence, the attacked routers forward these requests to the neighboring nodes, which in turn forward it to the next neighboring nodes and so on. If the number of invalid requests is so high, any legitimate request takes a longer response time. Consequently, if the response time exceeds the request timeout period, then the request may not be answered. This scenario can lead to denial of service or at least long delays.

Source:

In ICN, attacking a single source may also lead to overload conditions for the routing infrastructure. An attacker sends a large number of requests to a specific content source to degrade its performance. As a consequence, this attack increases the response time of content delivery for this content source or its access router. In addition to this effect, the attack can lower the data return rate and affect requests of all nodes in the paths to receivers. The attack scenario is similar to the infrastructure attack scenario. This attack not only affects the attacked source, but also affects the overall network.

Mobile blockade:

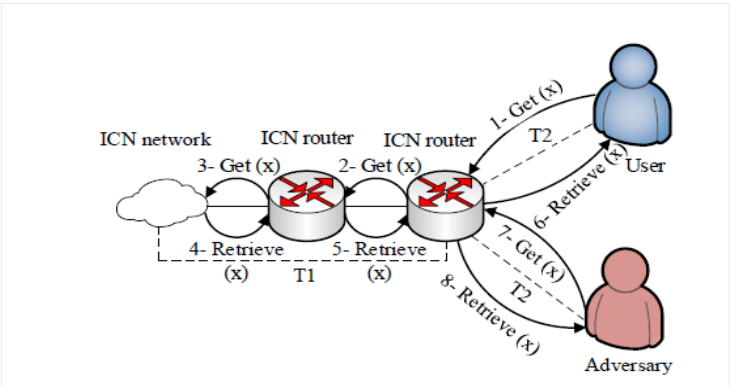
A mobile attacker can overload a region by traversing neighboring networks on circular paths while sending a significant number of content requests. The attacker aims to overload the mobile access routers to make it exceed the state timeout that leads to a blockade of the regionally available networks. The retransmission of requests is part of the mobility aspect in an ICN environment that adds difficulty in detecting this attack. The attack scenario presented in Figure 5 is similar to the infrastructure attack scenario. The difference is that the mobile attacker sends a high number of requests to neighboring networks, whereas the attacker is traversing between the networks in a circular and continuous manner.

Flooding:

The existing solutions for flooding attacks in ICN are designed to limit the number of requests, which are not appropriate for ICN [27], [36], [37]. An attacker can send a large number of requests that exceeds this limit. The attacked node accepts a certain number of requests and then ignores the remaining requests. As a consequence, the attacker succeeds to overload the overall infrastructure and harms all proximate users. Additionally, as ICN is a content centric architecture, i is difficult to apply limits for request rate per end user because there is no host identifier. The attack scenario is also similar to the infrastructure attack scenario. The difference is that the attacker sends a number of requests that exceeds the limits of the ICN nodes, and therefore ICN neglects the legitimate requests directed to the attacked nodes.

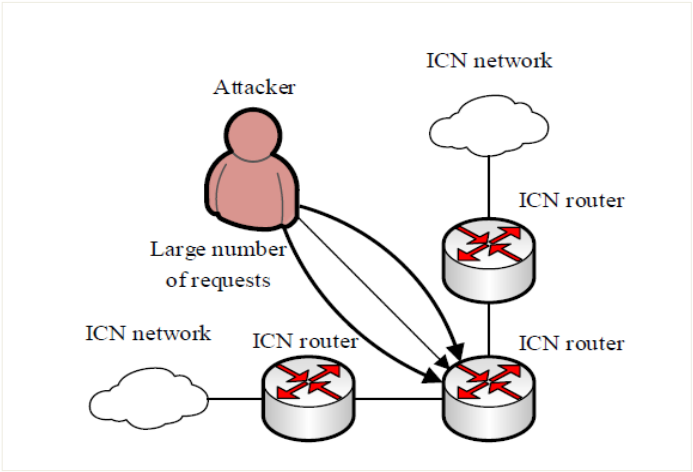
Timing:

This refers to increasing the request timeout for some ICN nodes to violate the consistency between the ICN asynchronous publication and the subscription process. An attacker sends a large number of requests to degrade the performance of some routers, so that request routing and data forwarding exhibit longer delays. The attack scenario is also similar to the infrastructure attack scenario. The difference is that the attacker sends a large number of requests through one or more routes to increase the request timeout for legitimate user's requests.



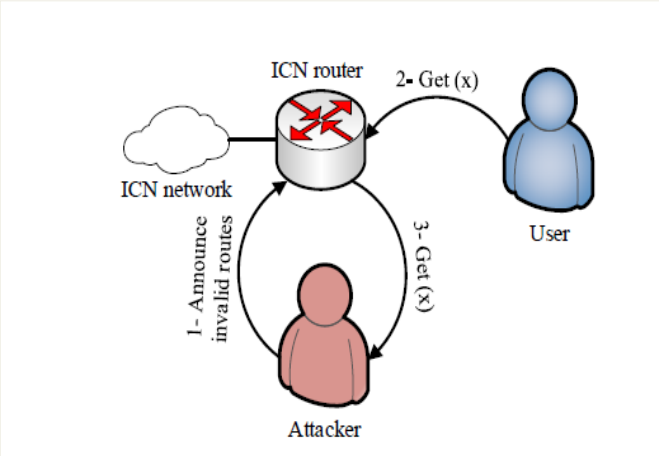
Jamming:

A node on a shared link sends a large number of malicious unnecessary content requests. The attacker who masquerades as a trusted subscriber sends the malicious requests to disrupt the information flow in the system. The ICN network replies and the content is sent to the destination without a receiver. This attack scenario is similar to the infrastructure attack scenario. The difference, as presented in Figure 6, is that the attacker sends requests to a shared node, which forwards it to neighboring nodes.



Hijacking:

Unlike host-centric architectures, any node in ICN can cache and publish/subscribe contents. An attacker who masquerades as a trusted publisher may announce invalid routes for any content. Content requests from users in the proximity of the attacker are directed towards these invalid routes. Consequently, these requests will be unanswered, which lead to a DoS. The effect of this attack may be exacerbated, if the attacker has the ability to hijack invalid routes on a large scale. The effect of this attack is lessened because the Routing mechanisms in ICN attempts to route towards multiple locations. As depicted in Figure 7, the attacker announces invalid routes for some contents to attract the user requests. When legitimate users send requests for one of these malicious routes, ICN nodes forward these requests to the malicious



Interception:

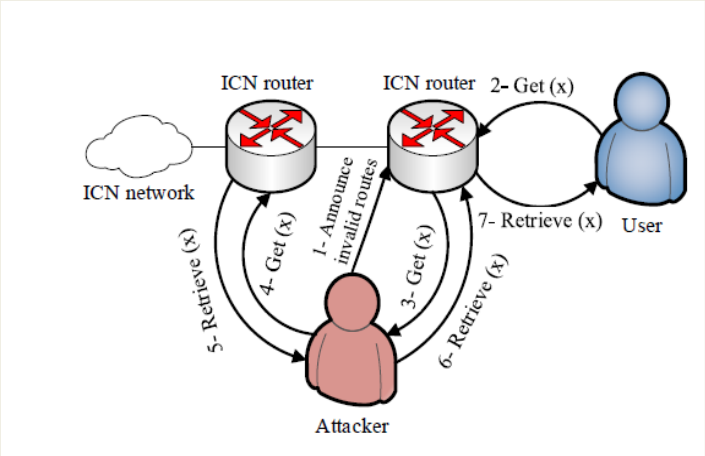
This attack is similar to the usual "man in the middle" attack. Unlike a hijacking attack, an attacker who masquerades as a trusted publisher announces invalid routes, while maintaining a record of valid routes to the content. Content requests can then be captured and sent to the proper location. Although the receiver gets the content normally, the attacker gains knowledge of the requested content. As shown in Figure 8, the attacker announces invalid routes for some contents to attract the user's requests. When legitimate users send requests for one of the malicious routes, ICN nodes forward these requests to the attacker's malicious node. The attacker records who requested this content and then forwards it to get the actual data. When the actual data

arrives to the attacker's node, the attacker forwards it back to the requested ICN node, which in turn forwards it to the legitimate user. For the user, the scenario seems to be normal, but actually the attacker violates the user's privacy.

Routing related attacks have an impact on the following:

Denial of service:

DoS may occur due to many attacks in this category, such as sending many requests for unavailable contents or to a single source, mobile blockade, flooding, hijacking, and timing. Consequently, intermediate timers delete requests with the expired timeouts, which may lead to DoS or at least long delays.



Routing related attacks have an impact on the following:

Denial of service:

DoS may occur due to many attacks in this category, such as sending many requests for unavailable contents or to a single source, mobile blockade, flooding, hijacking, and timing. Consequently, intermediate timers delete requests with the expired timeouts, which may lead to DoS or at least long delays.

Resource exhaustion:

There are many sources for resource exhaustion in the ICN infrastructure that come from misuse or uncontrolled traffic such as sending a large number of requests and flooding attacks.

Path infiltration:

In ICN, copies of content are typically distributed to many untrusted locations, and therefore it is difficult to authenticate valid origins for contents. Hijacking and interception are the major sources of path infiltration in ICN as attackers may announce invalid.

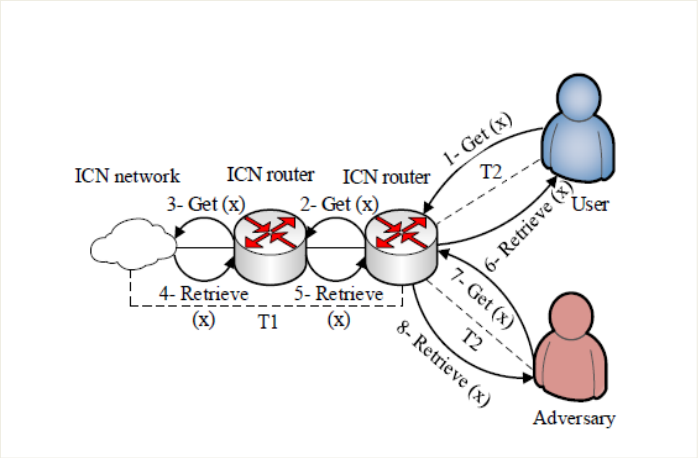
Caching related attacks

The attacks in this category can be classified into time analysis, bogus announcements, and cache pollution attacks. The cache pollution can be classified further into random and unpopular request attacks.

Time analysis:

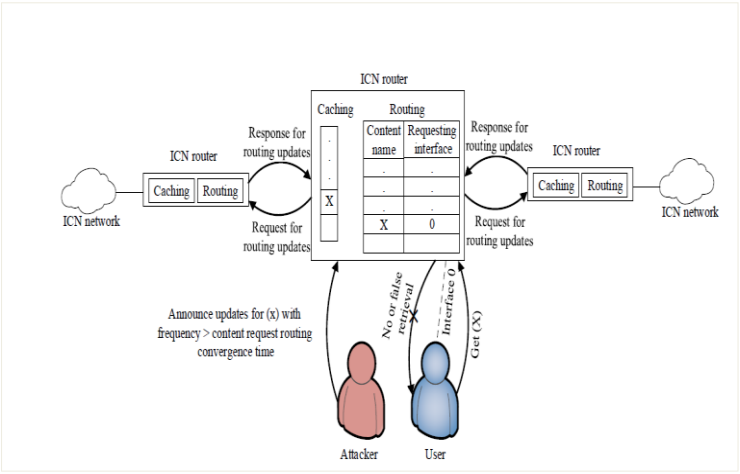
In ICN, any node can potentially cache any content. An adversary measures the time difference between request response times for cached and uncached ontent. This difference can be used to conclude if a proximate user has previously requested the same content as the requested one by the adversary. This attack violates the user's privacy as the adversary can gain information about this proximate user. As depicted in Figure 9, T1 is the time required to send the request and receive data between the content source and the closest router to the user or the adversary, and T2 is the time required to send the request and receive data

between the user or the adversary and the closest router. When a legitimate user requests certain content, the ICN infrastructure forwards the request to the content source and returns the data to the user in a total time of T1+T2. Then if the adversary requests the same content, he/she gets it in time T1 as there is already a cached copy of the content. The adversary uses this time difference to know if a proximate user requested this content before or not.



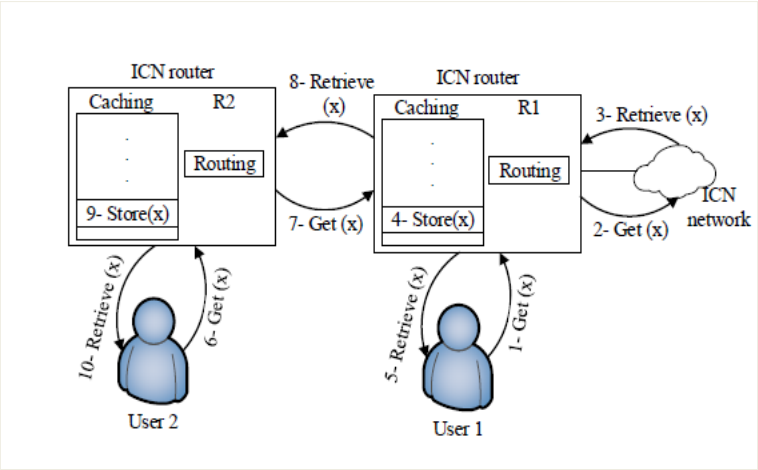
Bogus announcements:

As the caching system is a major part of the ICN architecture, an attacker can send many announcement updates for content or cached copy at a frequency that exceeds the local content request routing convergence time, to violate the caching and routing systems. As a consequence, an ICN will not be able to match the legitimate requests in the existence of these network quick updates. These overloaded announcements lead to incomplete and erroneous content retrieval as illustrated in Figure 10.



Random requests:

An attacker aims to spoil the ICN innetwork caching system and to change the content popularity. The attacker forces ICN caches to store unpopular contents by sending random requests for these unpopular contents. An unpopular content refers to a content that is not frequently requested. Alternatively, the attacker may request false contents to fill the caches with invalid contents. A content is fake if it is modified or does not come from the intended source, or it is not the content requested by the user. As shown in Figure 11, in the normal case, if a second user requests a cached copy, he/she gets the data from the closest available location as the caching system caches each content passing through it. As shown in Figure 12, in the attacked case, the attacker sends a massive number of random requests to spoil the caching system. In the latter case, if the second user requests the same content, his request takes the full path as the first user.



Unpopular requests:

An attacker only requests unpopular contents to spoil the ICN in-network caching and changes the content popularity. This attack requires a prior knowledge of the content popularity. The attack scenario has similar effectas the random requests case.

Caching related attacks have an impact on the following:

Privacy:

The caching mechanism in ICN is uniform, democratic and pervasive, which causes a greater privacy risk than in current architectures. As in the time analysis attack, the adversary can know whether a proximate user has previously requested this content or not and that violates user's privacy.

Denial of service:

Bogus announcements cause many updates to contents that lead to incomplete or erroneous data states. The mapping system will not be able to process these updates and, as a consequence, users do not retrieve the required contents.

Miscellaneous attacks

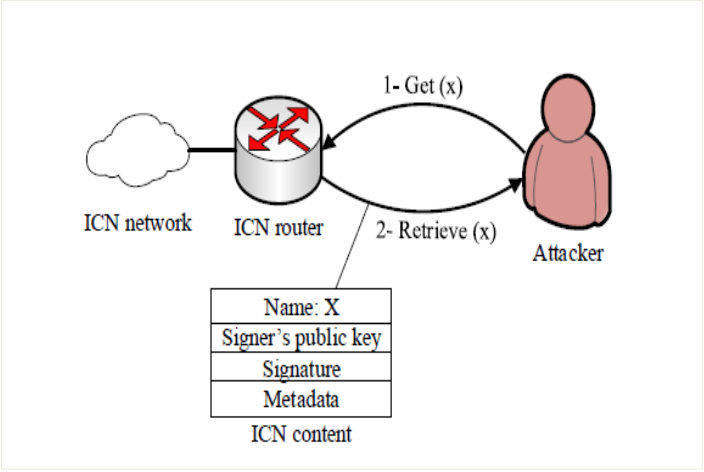
The other miscellaneous attacks can be classified into packet mistreatment, breaching signer's key and unauthorized access attacks.

Packet mistreatment:

This refers to normal active network attacks during data transmission that also includes the replay attacks. An attacker, who has access to a link fraudulently or Maliciously, tries to block, change, or reply to requested data many times. In this attack scenario, the attacker accesses ICN nodes or network links to do the following: modify packets during transmission or, reply it many times to requester or, generate content on behalf of a legitimate user.

Breaching signer's key:

An attacker can use any common attack to breach the signer's keys. This problem with ICN has a greater impact as publishers sign contents that are available for a long time and in large volumes. As shown in Figure 13, the attacker retrieves specific contents to break the signer's key. The data contains publisher public information and signature. This data may be large enough to simplify the attacker's task to get the signer's key.



Unauthorized access:

An attacker can access a certain content sent to a specific user or group of users that he/she is not allowed to access. In ICN, unauthorized access attacks become easier because an attacker can use any available copy for a content, which is distributed in different network locations.

Miscellaneous attacks have an impact on the following:

Congestion:

The attacker redirects the packets to heavily loaded links, which can lead to congestion in the network. In addition, packet mistreatment attacks can result in lowering of the connection throughput.

Denial of service:

The attacker sends a large number of packets toward a source or network entity causing DoS using packet mistreatment attacks.

Masquerading:

The attacker claims that he/she is a trusted entity. If the attacker succeeds to get the signer's key, then he/she can intercept, analyze, and/or corrupt the communications.

Unauthorized access to data:

In ICN, routers have direct access to content requests. Therefore, if the attacker Succeeds to hack a router, then he/she is able to monitor the requests submitted by the users. This allows the attacker to discover user requests and monitor the user's daily life. For example, the attacker might track a certain user by capturing his/her requests.

IV. CONCLUSION

The future internet comes with high requirements of information dissemination, which motivate the research community to find alternative solutions. ICN, as one of these solutions focuses on contents to provide a scalable and efficient content delivery. There are many proposals for ICN architectures like DONA, NetInf, NDN, and PURSUIT. ICN has attributes that make it unique from host-centric architectures. ICN mainly depends on location independent naming, in-network caching, and name-based routing.

This paper presents five major aspects relating to security in ICN. First, we develop a taxonomy of ICN attacks and classify the attacks into four categories: naming, routing, caching, and other miscellaneous related attacks. We describe each attack and the impacts of each category of ICN attacks. Second, we derive the relationships between ICN attacks and unique ICN attributes. We show for each attack how the attacker depends on the corresponding attributes to perform his/her attack. Third,

we derive the relationships between ICN attacks and security requirements and discuss the impact of each attack on the requirements. Fourth, we calculate the severity levels for the attacks based on ten evaluation metrics. Fifth, we survey the existing ICN security solutions.

V. Future Enhancement

Our goal is to provide more efficient service access; users address services only by name and in-network load balancing techniques route requests towards service instances such that the average response time as seen by the clients is optimized. We argue that network metrics such as hop-count are not sufficient for service selection and that load-balancing should be done by service routers.

References

1. B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, (2012) ”A survey of information-centric networking”, IEEE Communications Magazine, vol. 49, no. 7, pp. 26-36.
2. Md. F. Bari, S. R. Chowdhury, R. Ahmed, R. Boutaba, and B. Mathieu,(2012) ”A survey of naming and routing in information-centric networks”, IEEE Communications Magazine, vol. 49, no. 12, pp. 44-53.
3. D. Cheriton and M. Gritter, ”TRIAD: A scalable deployable NATbased Internet architecture”, Technical Report, January 2000. [Online].
4. C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, (2010) ”Secure naming for a network of information”, in Proc. of the IEEE Infocom, March 2010, pp. 1-6.
5. V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. Braynard,(2009) ”Networking named content”, CoNEXT’09, ACM,pp. 1-12.
6. T. Koponen, M. Chawla, B. G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, (2007) ”A data-oriented (and beyond) network architecture”, SIGCOMM Comput. Commun. Rev.,vol.37,no. 4, pp. 181- 192.
7. D. Lagutin, K. Visala, and S. Tarkoma, (2010) ”Publish/subscribe for internet: PSIRP perspective”, Towards the Future Internet, IOS Press, vol. 4, pp. 75-84.
8. A. Mohaisen, X. Zhang, M. Schuchard, H. Xie, and Y. Kim,(2013) “Protecting access privacy of cached contents in information centric networks” Published in: SIGCOMM13, Hong, Kong, China, May, pp. 1001-1003
9. J. Pan, S. Paul, and R. Jain,(2011) ”A survey of the research on future internet architectures”, IEEE Communications Magazine, vol. 49, no. 7, pp. 26-36.
10. C. Tsilopoulos, X. Vasilakos, K. Katsaros, G. Polyzos, G. Xylomenos, C.Ververidis, V.Siris, and N. Fotiou,(2013) ”A survey of information-centric networking research”, IEEE Communications Surveys & Tutorials

Author(s) Profile

Dr. K. Swathi, obtained her under-graduation in B.E., (Computer Science & Engineering) from Bharathidasan University, Trichy in 1999. She obtained her M.E. degree in Computer and Communication Engineering from Anna University, Chennai in 2004.She obtained Ph.D degree in Faculty of Information & Communication Engineering from Anna University, Chennai in 2014. Presently, she is working as Associate Professor in Computer Science & Engineering, Cauvery College of Engineering and Technology, Trichy in 2008. She has 14 years teaching experience and also she had attended many workshops, seminars and conferences on Research issues in Image processing. She has published papers in international journals and presented papers in various Conferences. She is the life member of Indian Society for Technical Education (ISTE). Her areas of interest include Image processing, Data mining, network security and Software engineering.

B. J. Vidhaya, was born in Kumbakonam, Tamilnadu, India, in 1986. She received the B.E. degree in Computer Science and Engineering from Oxford engineering college, Trichy affiliated to Anna University Trichirapalli, India, in 2009, and Currently she is pursuing her M.E. degree in computer science and engineering at Cauvery Engineering college, Trichy affiliated to Anna university, Chennai., India, Her area of interest is Network Security.

