IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 21-23
www.iosrjournals.org

A Novel Approach to Improving Security and Content Access Control in Named Data Networking

Shyama Francis[1], Deepa K Daniel[2]
[1]*(Department of Computer Science and Engineering, College of Engineering Perumon, India)*
[2]*(Department of Computer Science and Engineering, College of Engineering Perumon, India)*

Abstract: *Named Data Networking(NDN) is an emerging technique in future internet .In NDN use of IP address is replaced by content name. Content accessed by NDN is secure because contents are signed by the content provider before delivering it. Integrity and authenticity of the content verified by the NDN nodes by verifying signature associated with it .Traditionally using heavy weight signature generation and verification algorithms are not appropriate for this task .Due to this content pollution and denial of service attack occur in NDN. Caching and location independent content access in NDN reduces the capacity of the content provider to control content access. Here propose light weight integrity verification architecture (LIVE) to solve these two problems effectively. LIVE use light weight signature generation and verification algorithms for signature generation and verification. Also it enables the capability of content provider to control content access by sending integrity verification tokens to only authorized nodes.*

Keywords: *Access control, content provider, Data security, NDN*

I. Introduction

Named data networking is a new architecture in which communication is done without the use of ip address. In NDN interest and data packets contain content name in place of ip address. NDN design is secure because data packets are signed by the content provider before delivering it. Each NDN node that receive these data packet can check integrity and authenticity by verifying the signature associated with it. Currently using signature generation and verification algorithms are heavyweight so it is difficult to achieve universal integrity verification in NDN. NDN support caching and location independent content access so NDN nodes can cache or consume contents without permission from the content provider. Here propose a new technique LIVE, which take the extension of existing security mechanism to find a single solution for integrity verification and content access control. LIVE use one way hash functions to generate content signatures. Integrity of the content can be check by verifying these signatures. Only after success full integrity verification NDN nodes can cache or consume data packets .So it can prevent nodes from accessing corrupted contents. Using appropriate key update mechanism content provider can manage the verification capacity of NDN nodes. Content provider can control the content access in NDN by giving integrity verification tokens to authorized nodes only.

II. Existing System

Content centric network is a new architecture in which data packets are delivered by using content name instead of ip address. CCN can manage host based threats that affect ip network. It achieves security, scalability and performance [1] Information centric networking support multicast, mobility and support. Information items can stored in any location. It create difficulties in access control. Every information item associated with a pointer to a function attached by information owner which implements access control policy for protecting that item from unauthorized user [2].

Digital signature system relay on conventional encryption mechanism. It requires a small amount of memory and reduces the computational cost. The capacity of this system to sign messages is not limited [3]. Using two non-interactive protocol achieves the functionality of public key digital signature. It increases the speed and reduce the computational cost. All messages transmitted between the routers are signed by COSP and IOSP protocols [4].

ANDaNA consider the privacy relevant feature of NDN.It try to achieve communication privacy and anonymity. It is an onion routing overlay network. It find the privacy issues in NDN and perform security analysis and design a tool for this [5].

NDN is affected by two types of attack. They are interest flooding and content poisioning.Here using a push back mechanism to identify malicious nodes. Content pollution can be avoided by self-certifying interest and contents [6].

Privacy and confidentiality in content based publish subscribe system is achieved by an efficient cryptography based approach. Third party brokers make the decision for routing data without identifying the data [7].

A capability based operating system called EROS used for commodity processes. Using this approach access of an object can be revoked. A version number is associated with each object and its capabilities. If version number is not match with the capability it become invalid [8].

An identity based capability system can combine subject identifiers in the capabilities. This is done by changing the semantics of the item. Security policies are introduced by allowing monitoring and recording of capability propagations. It achieve frequent revocation. This design need low cost and less storage [9].

SCION can control the routing of data and it can isolate failures. It use trust information's for end to end communications. Trust domain can find routing failures and achieve scalable routing approach. This system can control many attacks and it achieves high resilience, scalability and isolation of failures [10].

III. Proposed System

LIVE use light weight content integrity and authenticity verification to protect NDN nodes from accessing fake data packets. Unauthorized content access done by NDN nodes avoided by implementation of light weight content security policies. A content producer can control content access in NDN by creating different integrity status for a single content object. Content signatures are made by the signature generation module in content producer. These signatures shows the content integrity and authenticity status. The contents status is verified by the integrity verification module present in each NDN nodes.

LIVE create signatures by using one way hash functions. During integrity verification each node can verify this hash based signatures. Content create tokens according to its security policies for sign and verify contents. Security policies for each content object can be implemented by attaching different security levels with respect to the nodes in the network. There are three security levels for content objects in NDN.They are non-cacheable, 1-cacheable, and all-cacheable.

Content producer differentiate NDN nodes into two groups, authorized nodes and unauthorized nodes. The authorized nodes can get private tokens and unauthorized nodes retrieve public tokens. Authorized NDN routers and end users get separate private tokens.NDN nodes with private tokens can succeed the integrity verification of a valid signature.

If a node can verify the signature successfully it shows that the content is not fake and that node cache or consume that content otherwise drop the data to avoid unauthorized content access. LIVE use a light weight encryption technique to enable content confidentiality for highly sensitive content. Using content integrity verification LIVE can control content access in NDN.It use hash functions to achieve light weight, practical and simple integrity verification and computation overhead can be reduced.

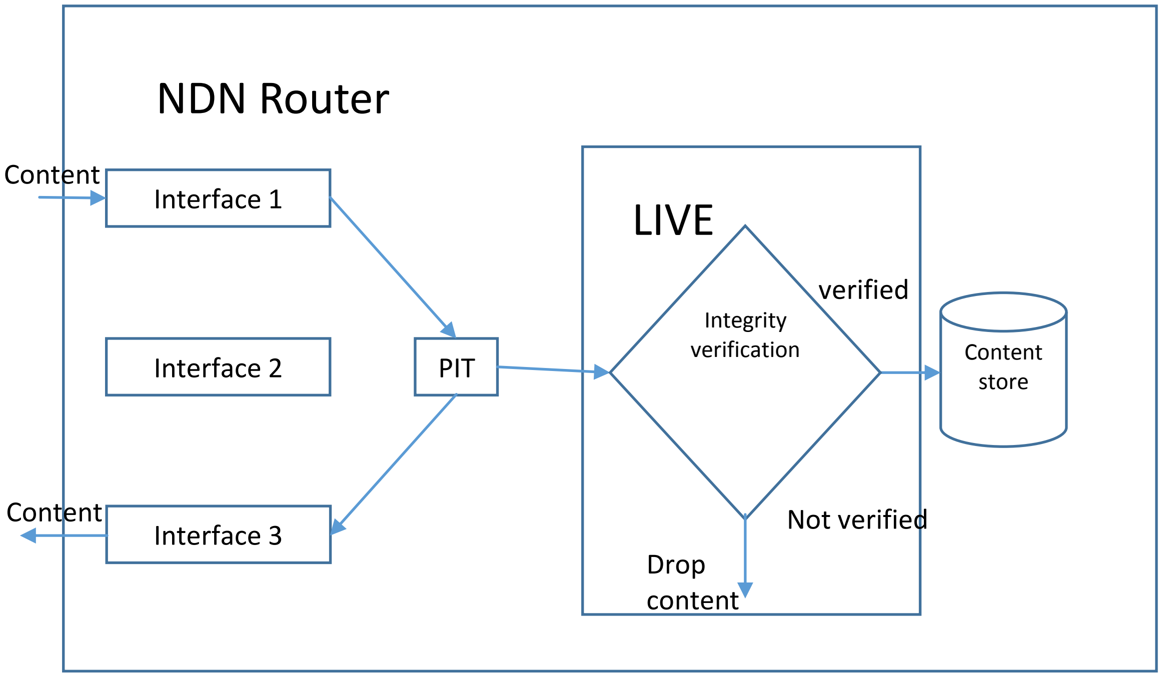

Figure: LIVE Implementation

IV. Conclusion

Here propose a new technique, LIVE to find solution for problems in existing named data networking. Using light weight signature generation and verification algorithm LIVE can achieve efficient integrity and authenticity verification in NDN. LIVE apply light weight content security policy in NDN to avoid un-authorized content access done by NDN nodes. It enables content provider to control content access in NDN.

Acknowledgements

We thank members of Computer Science and Information technology department of College of Engineering Perumon for their valuable support and feedback.

References

[1] V. Jacobson, D. K. Smetters, J. D. Thornton, M. Plass, N. Briggs, and R. Braynard, “Networking named content,” *Commun.. ACM, vol. 55, no. 1, pp. 117–124*, 2012.

[2] N. Fotiou, G. F. Marias, and G. C. Polyzos, “Access control enforcement delegation for information-centric networking architectures,” in *Proc.ACM SIGCOMM Workshop Inf.-Centric Netw., 2012, pp. 85–90.*

[3] R. C. Merkle, “A digital signature based on a conventional encryption function,” in *Proc. CRYPTO, 1987, pp. 369–378.*

[4] K. Zhang, “Efficient protocols for signing routing messages,” *in Proc. NDSS, 1998, pp. 1–7.*

[5] S.DiBenedetto, P. Gasti, G. Tsudik, and E. Uzun, “ANDaNA: Anonymous named data networking application,” in *Proc. NDSS,*2012

[6] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, “DoS and DDoS in named data networking,” in *Proc. ICCCN, 2013, pp. 1–7.*

[7] M. Nabeel, N. Shang, and E. Bertino, “Efficient privacy preserving content based publish subscribe systems,” in *Proc. 7th ACMSACMAT 2012, pp. 133–144.*

[8] J. S. Shapiro, J. M. Smith, and D. J. Farber, “EROS: A fast capability system,” in *Proc. 17th ACM SOSP, 1999, pp. 170–185.*

[9] L. Gong, “A secure identity-based capability system,” in *Proc. IEEE Symp. Secur. Privacy*, May 1989, *pp. 56–63.*

[10] X. Zhang, H.-C. Hsiao, G. Hasker, H. Chan, A. Perrig, and D. G. Andersen, “SCION: Scalability, control, and isolation on next generation networks,” in *Proc. IEEE Symp. Secur. Privacy*, May 2011, pp. 212–227.