Privacy Protection Based on Oblivious Transfer in Content-Centric Networking

Rui Chen[1], Zhen Chen [2,3], Junwei Cao[3], Ziwei Hu[4], Jing Zhou[4], and Jinghong Guo[4]

1. Department of Computer Science and Technology
Tsinghua National Lab for Information Science and Technology (TNLIST)
Tsinghua University, Beijing 100084, China
halfjuice@gmail.com
2. Fundamental Industry Training Center (iCenter)
Tsinghua University, Beijing 100084, China
*zhenchen@tsinghua.edu.cn
3.Research Institute of Information Technology
Tsinghua National Lab for Information Science and Technology (TNLIST)
Tsinghua University, Beijing 100084, China
jcao@tsinghua.edu.cn
4.State Grid Smart Grid Research Institute, Beijing 102209, P. R. China

Abstract. We present the method of user privacy protection in Content-Centric Networking (CCN) based on Oblivious Transfer (OT). Content-Centric Networking (CCN) is new network architecture to match the modern Internet usage by switching host-to-host model to content based model. Although the caching mechanism in CCN has made full use of bandwidth resource, there are certain risks that critical user data might be exposed to third-party, and very little effort has been made on ensuring such security. In this paper, Oblivious Transfer has been proposed for CCN security usage. We setup the requirements for user privacy protection in CCN, and propose CCN-CPIR, a fully user privacy protection scheme based on OT. Then, we design and implement CCN-CPIR based on 1-n OT protocol using C++. CCN-CPIR not only provides fully user privacy protection, but also outperforms former Java implementation in speed, which is a strong concern in CCN router implementation. Finally, we set up an experimental platform in LAN and conduct performance evaluation. Our experimental results show the potentials for practical usage as improved efficiency.

Keywords: Content Centric Network, Privacy, Oblivous Tranfer, Private Informantion Retrieval, Performance Evaulation

1 Introduction

The Internet is a de-facto big content pools with big content dissemination overlay network such as big Web sites, CDN and P2P networks, while its original design is to share computing resources with remote users in host-to-host model. To address the un-match in-between Internet usage and its design model, a new network architecture called Content-Centric Networking (CCN), aka Named Data Networking, is recently proposed by Von Jacobson et al. [1-3]. The fundamental principles of CCN have been shared with other designs such as Content-Oriented Network(CON) Architecture or Information-Centric Networking(ICN) [16, 19-20].

In CCN, a unique identifier of content has been assigned by user or ISP. The content is requested by its name instead of where (host) it is. The CCN content router will transparently cache content for future access. Because of these content-oriented features, CCN possesses many useful advantages in content delivery. Currently most of the research work focuses on CCN naming, caching, routing and security as suggested in [1].

Privacy protection in Information-Centric Networking (ICN) is the highlight research topics as pointed out in [18]. S. Arianfar et al. [4] present an privacy protection approach to leverages computational asymmetry by forcing the adversary to perform sizable computations to reconstruct each content request, hence to deter an adversary to effectively monitor the content requests of a large number of users. In CCN scenario, the content router aggregates all the same content requests, and a content provider may not know which content is accessed by which user, which seems a kind of built-in privacy protection scheme. But all the content in network will be requested, routed and disseminated by name, the users' access behavior exposed to the network, hence a big challenge to user privacy which thwarts the practical deployment of CCN. Some related researches[5-8] have already concerned privacy protection in CCN.

In our research work, CCN user privacy protection scheme is investigated among the three participants: user, CCN-ISP and CCN-content provider. We propose CCN-CPIR, a user privacy protection scheme based on Oblivious Transfer (OT) to address the requirements for user privacy protection in CCN. Then, we design and implement CCN-CPIR based on 1-n OT protocol using C++, which not only provides user privacy protection, but also improves the Java-version PIR implementation. Finally, an experimental platform in LAN is set up and CCN-CPIR is evaluated and experiments results show the potentials for practical usage as improved efficiency.

The rest of this paper is organized as follows. Section II introduces the challenges of user privacy protection and design requirements, and the fundamentals of OT protocol. Section Ⅲ describes the design and implementation of CCN-CPIR user privacy protection scheme. Section Ⅳ describes the evaluation in our experimental platform and give some insights on the results. And finally Section Ⅴ concludes the paper.

2 Background

2.1 User privacy protection challenges in CCN

Tobias Lauinger [5] investigates the security and scalability problem in CCN. CCN consist of three participants and four components. The participants includes end users, content sources, and ISPs connect end users and sources by forwarding Interests and data. The four components include end user equipment, routers, content sources, and links. The potential attackers include malicious end users, ISP and content source or provider and attack can target to any of the four components.

Every data may be cached at any CCN content router, while combined with intrinsic support for multicast or broadcast delivery this leads to a very efficient use of the network when many people are interested in the same content. But this also cause privacy issues.

In a so-called cache snooping attack [5], a malicious neighbor attack that aims at extracting communication traces from a cache is called the cache snooping attack, i.e. obtaining a copy of the cache's contents, Analyzing access to a given name, and Cloning conversations.

Filip Pitaru [6] discusses the ethical and legal implications, privacy and security concerns about CCN as new experimental technologies, and points out that if the security and privacy concerns of CCN have not been addressed, the CCN cannot be deployed and implemented in a large scale practical usage.

To solve the privacy concern in content oriented network includes CCN, Somaya Arianfer et al. [4] propose a privacy preserving scheme for content oriented network. This scheme make the attacker cost highly computation to acquire user privacy, though this scheme cannot provide ideal privacy protection.

2.2 Design requirements for user privacy protection

We consider our propose scheme satisfied the following requirements.

1) *Privacy protection*

We assume neither malicious ISP nor end users can break the user privacy protection scheme without the confirmation of users.

2) *Non-infrastructure support*

Caching introduces a fundamental tradeoff between efficiency and privacy. The CCN protocol efficiently delivers named content rather than connecting hosts to other hosts. We assume that the infrastructure will perform the basic CCN functions, such as routing and transmission without no special privacy-oriented services or mechanisms in content router.

3) *Cache Snooping Resistant*

We assume even the malicious end users who shared with victim users with the same cache in content router, and launch cache snooping attack cannot break the user's privacy.

2.3 Obvlious Transfer

Oblivious Transfer Protocol, simply called OT, is a more stringent version of Private Information Retrieval, acronyms PIR. Michael O. Rabin [9-14] firstly propose this wholly new idea in 1984. And it is now still an ongoing hot research in this area.

The OT protocol usage scenario is described as follows: Alice possesses a set of contents $x_1, x_2, \ldots, x_n$, Bob is interested in the content specified by subscript b ($1 \le b \le n$), but will not allow Alice to know what is he really interested. After finishing 1-n OT interaction in-between both sides, this delicate scheme make Bob fulfills what is his expectation, and acquire the content x_b, while Alice know nothing about which content bob has really retrieved.

The detailed interactive process in shown in Table 1, wherein as one can see the communication complexity of OT protocol is $O(n)$.

Alice			Direc-tion	Bob		
Private	Public	Comments	<==>	Private	Public	Comments
$m_1, \ldots, m_n$		Messages				
d	N, e	Generate RSA key pairs	=>		N, e	Reception of RSA key pairs
	$x_1, \ldots, x_n$	Generate n random messages	=>		$x_1, \ldots, x_n$	Reception of n random messages
				k, b, x_b		Generate k randomly and specify the b-th message
	v		<=		$v = (x_b + k^d) \bmod N$	Encrypt x_b
$k_i = (v - x_i)^d \bmod N$		Generate n, k_i respectively				
	$m_i' = m_i + k_i$	Encrypt n message respectively	=>		$m_0', m_1', \ldots, m_n'$	Reception of n cipertext
				$m_b = m_b' - k$		Decrypt the cipher to plain text

TABLE I. 1-N OBLIVOUS TRANSFER PROTOCOL BASED ON RSA PKCS

Although many theoretic works have been done in this area, rather few implementations have been published. In the following section, we will propose a new C++ implementation of 1-n oblivious transfer protocol, improving the former Java implementation with faster encryption. This implementation can be better used in potential application scenery of oblivious transfer.

3 The design and implementation of CCN-CPIR

Our design also follows today's standard router memory hierarchy. The packet store is kept in the DRAM and the index table is kept in the SRAM. The design of packet store follows the description in [9]. But the design of index table is quite different. We will detail our design in the following.

3.1 CCN-CPIR protocol

Assume Bob does not trust the interactive process. He indeed need to query Alice for something but will not allow Alice to know what he really interested in. Note that in CCN all the interaction will be cached in access content router, the malicious end user might try to launch cache snooping attack to break the bob's privacy.

To deal with the privacy issue in CCN, we design the CCN-CPIR protocol based on 1-n OT protocol. The detailed interactive process is shown as follows:

1) *Acquire Alice's public key and public parameters*

Bob ---- >>>> Alice
Interest: /Alice/OT/PK_certficate
In return,
Alice ---- >>>> Bob
Data: PK_certificate (N,e)

2) *Transfer n random messages*

Bob ---->>>> Alice
Interest: /Alice/OT/*nonce*_random_messages
In return,
Alice ---- >>>> Bob
Data: nonce, $x_1, x_2, \ldots, x_n$

3) *Transfer query parameter v*

Alice---->>>> Bob
Interest: /Bob/OT/*nonce*_query_parameter
In return,
Bob ---- >>>> Alice
Data: v

4) *Transfer query results*

Bob---->>>>Alice
Interest: /Alice/OT/v_results/
In return,
Alice ---- >>>> Bob
Data: $m_0', m_1', \ldots, m_n'$

Note: nonce is one time random number specified by Bob in each session.

3.2 CCN-CPIR architecture

CCN-CPIR architecture is shown in Figure 1. For the performance issues, we implement our project with C++.

All the basic libs are defined in common.h, which defines 8-bit, 16-bit, 32-bit, and 64-bit integer.

The fundamental function in Number theory is defined in nalgo.h and nalgo.cpp, such as extended Euclidean algorithm, inverse and power operations.

Content source message access interface is defined in message.h and message.cpp. In our implementation, the entire content messages store consists of an array of integers; string conversion can be supported in the future. The random message generation is also implemented in the message module.

The basic public key interface is defined in key.h and key.cpp, RSA PKCS is also implemented in key.cpp based on the number theory algorithm defined in nalgo module, as the fundamental component of OT protocol.

Figure 1. Architecture design of CCN-CPIR.

The client side (Bob) and server sider (Alice) is defined in server.h and client.h

We make the final CCN-CPIR open source, and the full version can be checked in Google code [17].

4 Experimental Evaluation Of CCN-CPIR

4.1 Experiment settings

Our experiment is performed on the experimental platform. Our machines use the 2.5 GHz Intel Core2 Duo CPU and 4GB of RAM. The operation system is Windows 7 Ultimate. The communication between client and server is in Ethernet LAN environment. Hence the latency is mostly reflecting the encryption and decryption cost.

4.2 Experiment results

The performance of CCN-CPIR is evaluated by the time consumption of the retrieval of entire content store using 1-n oblivious transfer. We increase the volume number of the content items in content stores gradually and measure the time consumption.

Table 2. Experiments results when $n < 10^7$

size	10^1	10^2	10^3	10^4	10^5	10^6	10^7
time(ms)	29	30	35	75	453	4648	51340

As shown in Table 2, when the volume (n < 10000) in content stores is small, the difference in time consumption is quite small, because most of the time is cost by the process of encryption/decryption and communication delay.

Table 3. Experiments results when $n > 10^5$

size	10^5	$2x\ 10^5$	$4x10^5$	$8x10^5$	$16x10^5$	$32x10^5$	$64x10^5$
time(ms)	453	959	1948	4005	7976	16072	32897

After the volume number reaches 10^5, we make volume number increased more steadily and the results are shown in Table 3. When the number is large enough, the time spending is in a linear with the number. The results are shown in Fig. 2.

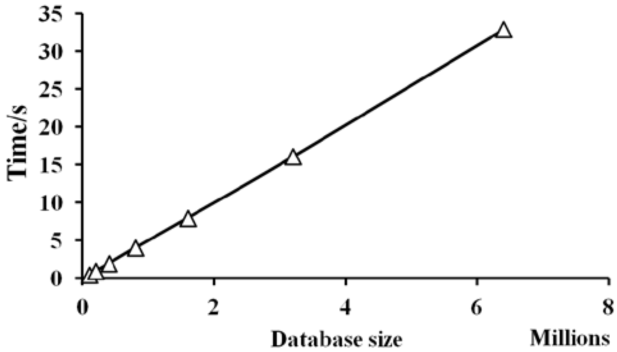

Figure 2. Performance evaluation of CCN-CPIR.

When the volume of the content store is about 106 (1 million), the time consumption is nearly about 5 second, which is still in an acceptable level.

In consideration of high communication complexity issue, there's also a solution to reduce communication complexity by deploying data across multiple uncooperative servers, which vastly increase usability of OT method. However, this approach still requires the O(n) 1-n OT implementation as building blocks. So it is still critical to address high performance 1-n OT implementation.

5 Conclusion And Future Work

CCN is a promising architecture to solve the mismatch between Internet usage and its communication model in new ways. However, the users' privacy (content request and access behavior) will fully be exposed to the network. Hence a big challenging issue deters the users' adoption and thwarts the practical deployment of CCN.

Oblivious Transfer is a protocol whose theory has been well studied, and it is a powerful tool when applied to ensure CCN's security. In this way, content are ciphered during their path to the destination, and the data client retrieved from the server will be fully protected. This is especially useful when security-related application comes to CCN network, such as electrical payments, authentication and so on.

Moreover, such "marriage" will ask for a fundamental requirement of performance, and as the conducted experiment suggests, CCN-CPIR has shown an acceptable running speed in CCN application. And there will be a good trade off to reach the balance of security and performance.

The future work includes using elliptic curve cryptosystem PKCS instead of RSA cryptosystem, and performance improvement in encryption and decryption speed. Also, the conversion between the string and integer need to be further studied in CPIR implementation.

6 Acknowledgment

This work was supported in part by National Natural Science Foundation of China (grants No.61472200 and No. 61233016), Ministry of Science and Technology of China under National 973 Basic Research Program (grant No. 2013CB228206), State Grid R&D project "Research on the Architecture of Information Communication System for Internet of Energy" (grant No. SGRIXTKJ[2015]253), and National Training program of Innovation and Entrepreneurship for Undergraduates (No. 201610003B009, 201610003B010, 201610003031, 201610003032, 201610003033, 201610003B034).

7 References

1. Van Jacobson, Diana K. Smetters, James D. Thornton, Michael F. Plass, Nicholas H. Briggs, Rebecca L. Braynard, Networking Named Content, ACM CoNext, Rome, Italy, 2009.
2. Named Data networking project, http://www.named-data.net/
3. CCNx project https://www.ccnx.org/
4. Somaya Arianfar, Teemu Koponen, Barath Raghavan, and Scott Shenker, On Preserving Privacy in Information-Centric Networks, ACM Sigcomm workshop ICN, 2011.
5. Tobias Lauinger, Security and Scalability of Content-Centric Networking, Master's Thesis, TU Darmstadt, Darmstadt, Germany and Eurécom, Sophia-Antipolis, France, September 2010.

6. Filip Pitaru, Content Centric Networks: ethical and legal implications, privacy and security concerns of new experimental technologies, Technical Report, 2010.
7. Walter Wong and Pekka Nikander, Secure Naming in Information-centric Networks, ACM Sigcomm Workshop ReArch, 2010.
8. InKwan Yu, Bin Song, Jiseong Son and Doo-Kwon Baik, Discovering credentials in the content centric network, International Conference on Information Networking (ICOIN), Jan. 2011.
9. M. Rabin, "How to exchange secrets by oblivious transfer," Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.
10. F. Saint-Jean, "Java implementation of a single-database computationally symmetric private information retrieval (CSPIR) protocol," Citeseer2005.
11. H. Lipmaa, "An oblivious transfer protocol with log-squared communication," Information Security, pp. 314-328, 2005.
12. S. Even, et al., "A randomized protocol for signing contracts," Communications of the ACM, vol. 28, pp. 637-647, 1985.
13. "Oblivious Transfer," in Wikipedia, ed, 2011.
14. C. Gentry and Z. Ramzan, "Single-database private information retrieval with constant communication rate," Automata, Languages and Programming, pp. 803-815, 2005.
15. J. Rexford and C. Dovrolis, “Future Internet architecture: clean-slate versus evolutionary research,” Communications of the ACM, vol. 53, no. 9, pp. 36–40, 2010.
16. J. Moreira, S. Midkiff, and M. Gupta, “A comparison of java, c/c++, and fortran for numerical computing,” Antennas and Propagation Magazine, IEEE, vol. 40, no. 5, pp. 102--105, 1998.
17. Rui Chen et al., CPIR project, http://code.google.com/p/cpir.
18. Ali Ghodsi, Teemu Koponen, Barath Raghavan, Scott Shenker, Ankit Singla, James Wilcox, Information-Centric Networking: Seeing the Forest for the Trees, In Proc of SIGCOMM Workshop on ICN, 2011.
19. Hong-Feng Xu, Zhen Chen, Rui Chen, Junwei Cao, Live streaming with content centric networking, Third International Conference on Networking and Distributed Computing, pp. 1-5, IEEE, Oct. 2012.
20. Junwei Cao, Shuo Chen, Zhen Chen, Yangyang Ming, Zhongda Yuan, Ziwei Hu, Jing Zhou, and Jinghong Guo. Underlay Implementation of Named Data Networking. The Sixth International Conference on Networking and Distributed Computing, 2016.