Journal of The Korea Society of Computer and Information
Vol. 22 No. 4, pp. 75-82, April 2017

www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.04.075

Strengthening Authentication Through Content Centric Networking

Sung-Jin Kim*, Jae-Kyung Park**

Abstract

While the internet has evolved in terms of information sharing and efficiency, it is still prone to security attacks and remains vulnerable even when equipped with a security mechanism. Repeated patching against hacks involves excessive wear of system equipment and high costs.

Methods of improving network security include the introduction of security equipment and network partitions, but they have not been fully effective. A fundamental solution is the Operation Content Network (OCN), which enables the strengthening of authentication.

In this paper, Instead of following the existing TCP/IP system, OCN establishes an immunity-based security system through content-centric communications. Data transmission occurs over a Content Centric Network (CCN), which is provided with a protocol verified by the CCNx group. Areas protected by OCN rely only on CCN for communication without using any IP. As such, it defends the system against unknown attacks, including zero-day attacks.

▸ Keyword : CCN, authentication, network security, contents, next-generation network

I. Introduction

The internet has evolved in terms of information sharing and efficiency, and enhances security through separate mechanisms. That is, the internet itself is prone to security attacks, and remains vulnerable even when equipped with a security mechanism. IP addresses are easily retrievable due to the lack of concern over content security, and all services are assumed to be safe. However, this IP paradigm is highly insecure, unsuitable for mobile services, and fails to satisfy security requirements. In recent years, there has been an explosive increase in internet traffic and the number of internet-related devices including Internet of Things (IoT) and smartphones. Services involving UCC and other massive data have caused difficulties in data utilization. Moreover, the lack of security over the internet has worsened with the continuous increase in cyber crimes and cyber terrorism. As shown in Fig. 1, cyber terrorism has persisted over the years, and cyber crime is on the rise.

Fig. 1. Increase in the number of cyber crimes

• First Author: Sung-Jin Kim, Corresponding Author: Jae-Kyung Park
*Sung-Jin Kim (sujnkim@gmail.com), Dept. of IT Policy and Management, Soongsil University Graduate School
**Jae-Kyung Park (jakypark@kopo.ac.kr), Dept. of Information Security, SeoulGangseoCampus, Korea Polytechnics
• Received: 2017. 03. 13, Revised: 2017. 03. 20, Accepted: 2017. 04. 04.

While the internet has evolved in terms of information sharing and efficiency, it is still prone to security attacks and remains vulnerable even when equipped with a security mechanism. Repeated patching against hacks involves excessive wear of system equipment and high costs.

Content-Centric Networking (CCN) technology has been proposed as a new networking architecture that resolves the fundamental weaknesses of the internet by emphasizing content instead of assuming the typical host-centered structure. This method provides content to users in a safe and quick manner by using names instead of IP addresses. It is unnecessary for users to know the location of desired content, and protecting end-to-end data channels in a world where network connections are of a global scale involves too much overhead. As shown in Fig. 2, CCN uses content as the entity of networking, thereby eliminating the need for IP addresses.

Some attempts to overcome the aforementioned issue include the introduction of security equipment and network partitions, but they have not been fully effective. This paper proposes strengthening authentication using CCN, which serves as a solution to existing security issues of the internet.

Fig. 2. Information sharing through various media

II. Related Work

1. TCP/IP Security Issues

1.1 Expandability

According to Mun-sik Kang (2009), ARPANET consisted of only four computers when it was first established in 1969. Today, it links more than 260 million host computers from more than 180 countries, which translates to 1.45 billion users or a daily average of 1 million users. The size of routing tables is increasing exponentially with multi-hosting and traffic engineering. Myung-ki Shin (2007) expects networks to grow more complex due to the 50 to 100-fold increase in internet bandwidth and the adoption of ubiquitous access or multi-homing. As such, the lack of expandability has been identified as a key issue of the internet today.

1.2 Mobility

The internet, which began with a few computers connected via cables, has expanded to millions and is becoming more complex by the day. The IP address system was effective since terminals remained in the same location. However, with the emergence of mobile devices such as laptops and smartphones, terminals connecting to the internet frequently changed physical locations even while sending and receiving messages. Under the current address system, the communication process is disrupted when the internet is unable to detect the movement of terminals to new locations. Research on internet mobility has begun to resolve the discontinuity of message transmission arising from the moving of terminals. The mobility of the internet includes mechanisms that ensure the continuity of services even during location management and relocation of mobile terminals.

1.3 Diversity

For the past few decades, the internet was developed to efficiently transmit data over wired networks. Path optimization, transmission mechanisms for reliable communication, and algorithms for efficient use of links have all been developed based on the characteristics of wired networks. However, recent efforts to integrate wireless devices and wireless network technologies with the internet have highlighted the need to reassess existing internet technologies. With the expansion of terminals from PCs, servers, and routers to mobile devices having limited battery and computing capacities, data transmission has changed from high-speed and low data loss over wired networks to low-speed and high data loss over various wireless networks. Thus, internet technologies should be redesigned to accommodate wireless devices and networks.

1.4 Security

Security is an important issue in all types of

communication. The internet has experienced many security attacks, and various solutions have been proposed. Attacks against the internet include electronic eavesdropping, illegal access and manipulation of information, and crashing of specific websites. Whenever such attacks occurred, security patches or mechanisms were added to the existing internet instead of developing new technology. These solutions manage to improve security but sacrifice transmission efficiency, which interferes with the implementation of security technologies. The problem of poor transmission efficiency has grown more prominent with the integration of wireless devices and networks with the internet. The limited characteristics of wireless devices and networks make them not only more vulnerable to security attacks, but also incompatible with solutions previously used for wired networks. As such, the expansion of the internet to wireless devices requires a more fundamental solution to resolve security issues.

2. Content Centric Network

CCN is a next-generation network that improves content transmission capacity and strengthens security by emphasizing content over IP addresses, shifting its focus from where to what. CCN assigns specific names to content such that data processing can be performed without IP addresses, as shown in Fig. 3. When CCN is used, service requestors or attackers cannot access the content server, preventing them from gaining any information about the OS, web, applications, and services. Attackers may request and receive content, but they are supplied with cached content, and this too can only be received after proper authentication.

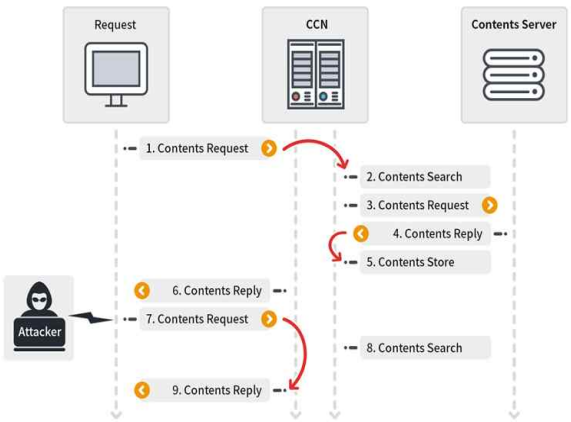

Fig. 3. CCN connection process

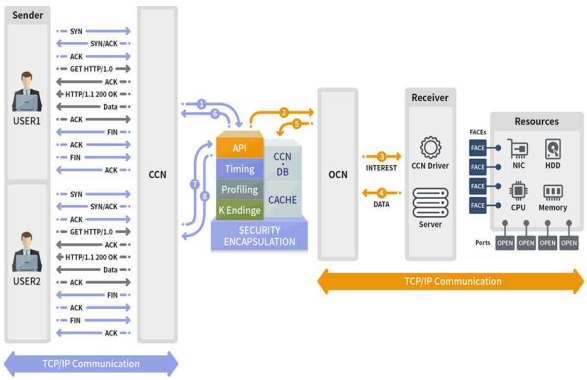

Fig. 4. Detailed CCN protocol

III. The Proposed Scheme

This section recognizes the need for an innovative approach to eliminate the aforementioned risks, and proposes the use of Operation Content Network (OCN) as a new internet paradigm. Content and services will remain key elements of the internet even in the future. Security is another important aspect. Moreover, hacking can be easily performed by general users using free hacking software. Against this backdrop, OCN creates a paradigm shift for the internet. With the introduction of OCN, attacks based on IP protocols and related hacking tools no longer have any effect. As such, the internet environment must ensure information sharing and exchange, as shown in Fig. 2, and secure services should be promoted through social communities or mobile media.

1. Operation Content Network (OCN)

OCN uses the CCN mechanism for data transmission but provides a more secure mechanism by additional elements, as shown in Fig. 3.

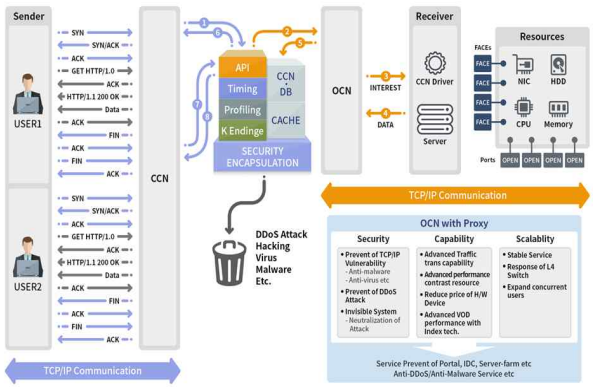

Fig. 5. Concept of OCN

The characteristics of OCN are as follows.

- Real time system

The real-time system of OCN is based on artificial intelligence. Each real-time checking processor (equipped with a global timer) predicts internal problems.

- Multiple device support

OCN, using Java, exists in the current internet. Because its objects are generated differently from that of Java, OCN is able to support multiple devices.

- Plan ahead

OCN assumes that hacking involves repeated attempts and thus predicts attacks based on past attempts. It plans ahead to strengthen the system against possible variations in attack patterns while cleaning up the surrounding network environment in real time.

- Profiling Guideline

OCN profiling oversees connections, blocking, and priorities. Related policies and guidelines are applied to the OCN mechanism to be supplied to various users.

- Heart Beat (ATM)

An absolute time system is needed for real-time services. OCN uses a global timer with an accuracy of up to one-trillionth by relying on artificial satellites. This generates the OCN ATM.

- Ensure proper security and encryption

The structure and internal elements of OCN are not publicly known. Data encryption and security measures have been employed for IP addresses, IP protocols, and IP ports.

The security features of OCN are described below and presented in Fig. 6.

1) The structure and internal elements of OCN are not publicly known.

2) The OCN structure has no IP address, and this renders most hacking tools useless.

3) The OCN structure has no IP protocol.

4) The OCN structure has no IP port.

5) OCN technology emphasizes security and reliability (hardware and software).

6) The OCN paradigm was developed to meet the demands of the cyber age. It is a mechanism that supports u-cities, u-governments, and u-worlds (where “u” stands for ubiquitous).

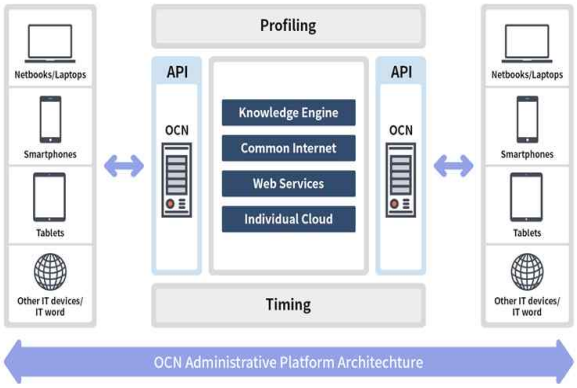

Fig. 6. OCN platform architecture

2. Advantages and Limitations Compared to TCP/IP

2.1 Efficiency of System Performance

The existing TCP/IP method relies on the host-to-host method, as shown in Fig. 7. This gives it a more inefficient structure and requires larger bandwidths.

On the other hand, OCN is content-centric and minimizes server load through caching, as shown in Fig. 8.

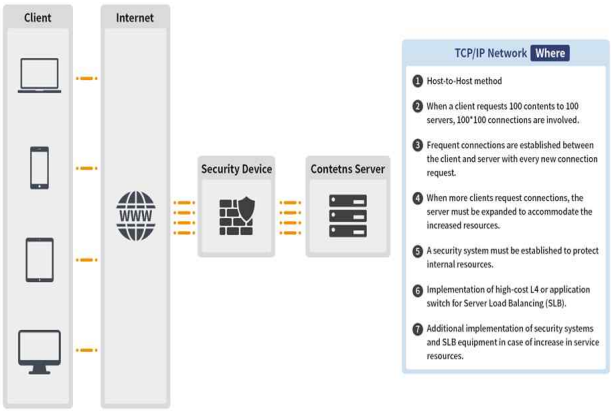

Fig. 7. Content transmission under TCP/IP

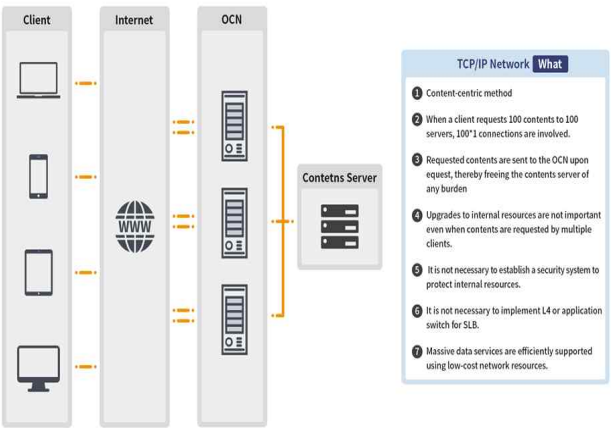

Fig. 8. OCN content transmission technology

The example in Fig. 9 demonstrates the performance and efficiency of OCN. Data is provided in a cached form through the middle node, such that the network is used efficiently and response time is minimized. The storage space in the application server and DB server is significantly reduced, contributing to greater savings in investment cost.

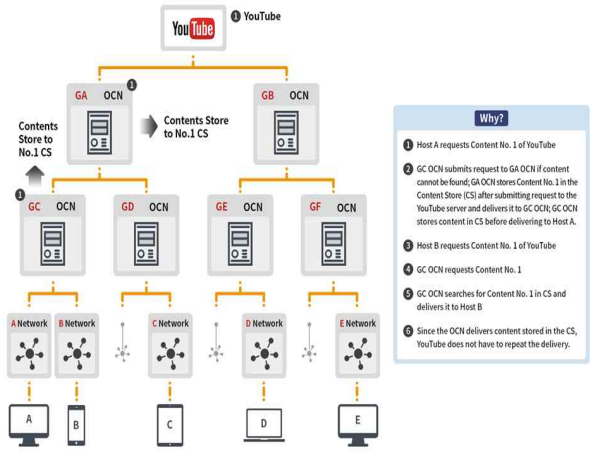

Fig. 9. Example of using OCN

2.2 Stability of System Security

When applied to the entire domain, OCN becomes completely immune to existing cyber threats, as shown in Fig. 10. ANUBIS, developed in the form of security equipment for servers, has been optimized for cloud services. ANUBIS is also cost efficient as it replaces switches and several security devices. ANUBIS-S, launched in November 2015, is OCN equipment featuring security functions. ANUBIS-RS, launched in February 2016, offers routing and switching functions.

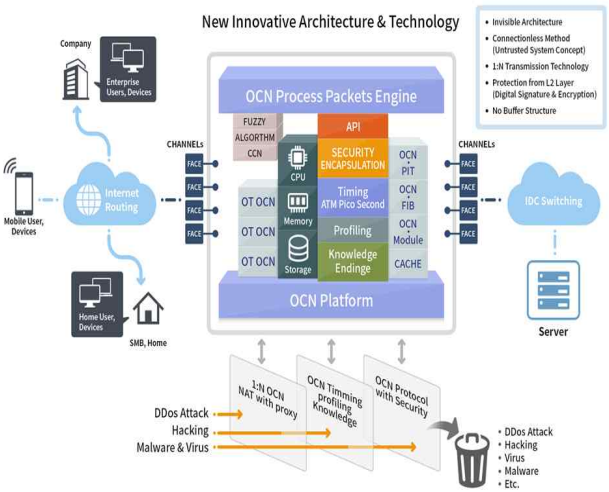

Fig. 10. Application of OCN to the entire domain

2.3 Limitations of OCN

OCN clearly has limitations. Unless all networks convert to ONC, abnormal hacking can be performed via internal networks. That is, managers must adopt the TCP/IP approach for server management and maintenance if only ANUBIS-S is applied, and malicious codes may infiltrate through PCs in the internal network and cause damage, similar to hacking. However, this is more an issue of network configuration, and not an inherent problem of OCN.

Another problem is that, although OCN is less susceptible to hacking because it is not widespread, this does not imply that OCN itself can block hacking completely. In the future, OCN may be hacked if its weaknesses become known.

Because OCN was developed with an emphasis on security, it will be less vulnerable than TCP/IP to general attacks. To resolve these issues, OCN products must be supplied not by CAT companies alone, but in cooperation with CISCO or other security companies.

IV. Test and Discussion

The tests were conducted using ANUBIS and a Windows 8 server. The two attacks consisted of a DDoS attack and a malicious code.

The test schematic is given in Fig. 11. The performance and functions of ANUBIS were tested by separately testing the In-Line-Mode and Out-of-Path mode.

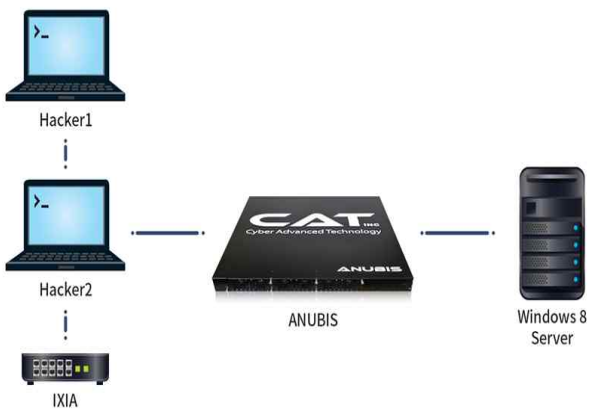

Fig. 11. Schematic diagram of hacking demonstration

A) ANUBIS IXIA test

The test was carried out up to 40Gbps, with attack sampling data mixed into attacks. The system managed to defend against all attacks. Because the IXIA data were too massive to be fully received, bandwidth tests and attack packet strike tests were conducted, as shown in Fig. 13. ANUBIS maintained steady performance throughout the tests and defended the system against all IXIA attack patterns.

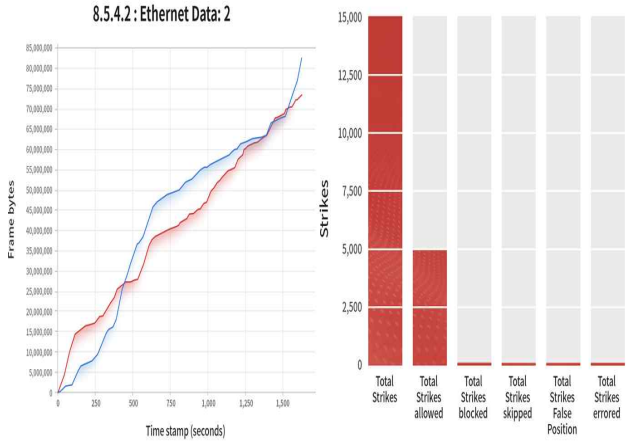

Fig. 12. IXIA test result

B) Out-of-Path test

The Windows 8 server was scanned with ANUBIS excluded. The server did not exhibit major weaknesses, and server ports could be identified. The scanning was performed using MetaSploit to maintain objectivity.

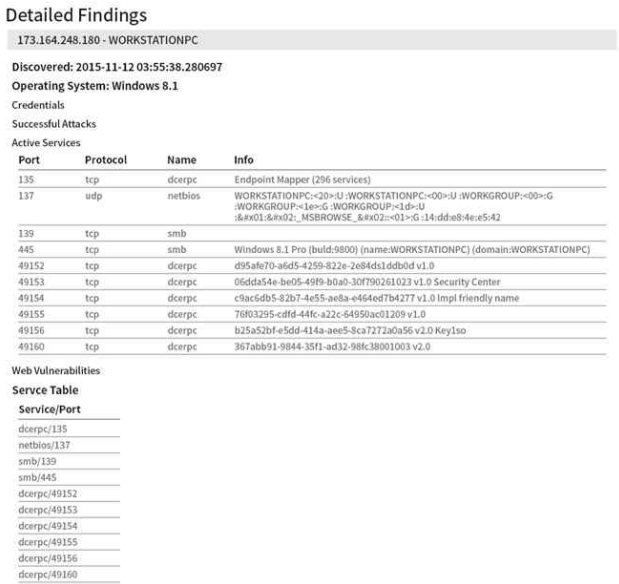

Fig. 13. MetaSploit scanning results

C) In-Line mode test

Unlike the results provided above, scanning was not possible after connecting the ANUBIS equipment. This indicates that the scanning attempts were blocked by ANUBIS.

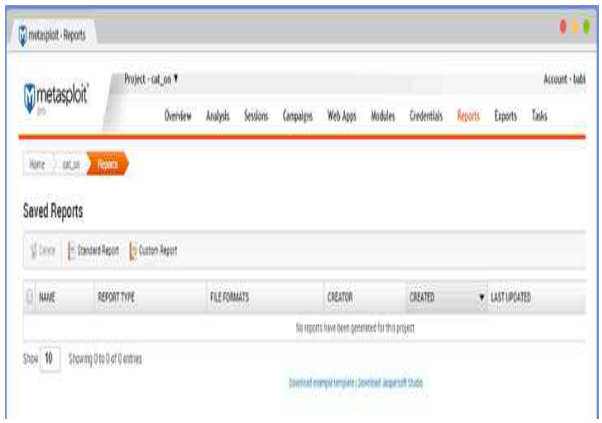

Fig. 14. MetaSploit scanning failure

D) Zero-Day attack test

The hackers failed to access the system, as shown below Fig. 15.

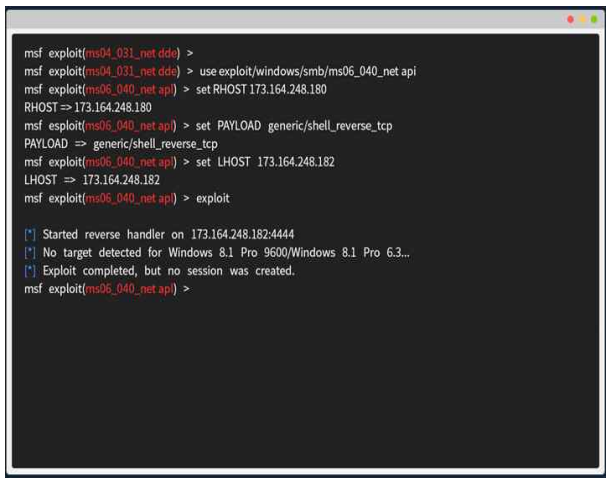

Fig. 15. BackTrack 5

E) Additional tests

The same results were obtained for SAMBA, DCERPC, MSRPC, and NETBIOS performed separately by hackers.

V. Conclusion

The amount of IP traffic has continuously expanded with recent changes in the global environment, and

Internet-related companies must address security issues, especially considering that data increases at a daily average of 23%, as shown in Fig. 17. Various solutions, going beyond the improvement of hardware performance, must be developed for efficient traffic management. Security is another factor that should be taken into account when processing massive amounts of data.

CCNx (www.ccnx.org) was an attempt to improve the efficiency and security of traffic transmissions in light of the changing environment, and Xerox's PARC (www.parc.com) has led commercialization efforts. CCN, which serves as a solution to the existing issues of TCP/IP, has been identified as an area requiring research in the Emerging Networks Consortium (ENC). A 12 Tbps high-performance CCN router was developed in a joint study between CISCO and PARC, and a prototype is already available. Further research is being conducted by industry leaders seeking to dominate the concent-centric network market.

Products designed for TCP/IP, with a history of more than 40 years, are structurally susceptible to cyber attacks. Security patches supplied after hacking involve high costs and are not as effective against similar attacks. The most realistic way of overcoming this issue is to create a paradigm shift. The proposed system is not only completely immune to hacking attacks that worked on TCP/IP, but also offers advantages such as improved performance and lower costs.

While Korea boasts the world's most advanced internet infrastructure, it is vulnerable to hacking threats from North Korea and China. The proposed mechanism, which is impenetrable to existing cyber attacks, should be further studied and invested in. This paper lays a foundation for the implementation of related technologies.

REFERENCES

[1] Veres, J. Hybrid Printed Sensors for Customizing the IOT . MEMS & Sensors Executive Congress 2016.

[2] Wunderer, T. Electron beam pumping for high power deep-UV emitters. European Materials Research Society Meeting. Sep 19, 2016

[3] Mei, P. ; Whiting, G.; Schwartz, D. E.; Ng, T.; Krusor, B. S.; Ready, S. E.; Veres, J.; Street, R. A.; Integrated Digital Printing of Flexible Circuits for Wireless Sensing. SPIE Optics + Photonics 2016 .; San Diego , CA USA. Date of Talk, Aug 28, 2016

[4] David Cheriton and Mark Gritter, "TRIAD: a Scalable Deployable NAT-based Internet Architecture," Technical Report, http://www-dsg.stanford.edu/triad/#papers, January 2000

[5] Mark Gritter and David Cheriton,"An architecture for content routing support in the Internet," 3rd USENIX symposium on Internet technologies and systems, 2001 [3] T. Koponen et al, "A Data-Oriented (and Beyond) Network Architecture,"ACM Sigcomm 2007

[6] Van Jacobson, et al,"Networking Named Content," ACM CoNEXT 2009

[7] Jaehoon Kim, et al, "Content Centric Network-based Virtual Private Community," IEEE ICCE, Las Vegas, January 2011

[8] Van Jacobson, et al, "Custodian-based Information Sharing," IEEE Communication Magazine, July 2012

[9] "Host Identity Protocol (HIP) Architecture," R. Moskowitz, et al, IETF (Internet Engineering Task Force) RFC 4423, May 2006.

[10] "Shim6: Level 3 Multihoming Shim Protocol for IPv6," E. Normark, et al, IETF RFC 5533, June 2009.

[11] "Architectural implications of Locator/Identifier," D. Meyer and D. Lewis, IETF draft-meyer-loc-idimplications-01.txt, January 2009 [10] "Content Centric Networking," a private presentation at Samsung Advanced Institute of Technology (SAIT), May 13, 2010

[12] Statistics for OC-3 prices: Telegeography research.

[13] Statistics for memory prices: http://www.jcmit.com/memoryprice.htm

[14] "Greening the Internet with Content-Centric Networking," Uichin Lee et al, 1st International ICST Conference on E-Energy, 2010

[15] Project CCNx: http://www.ccnx.org/

[16] Named Data Networking project web site: http://www.named-data.org/

[17] ENC (Emerging Network Consortium), http://www.parc.com/services/focus-area/emerging-networksconsortium/

[18] IRTF ICNRG (Information-Centric Networking Research Group), http://trac.tools.ietf.org/group/irtf/trac/wiki/icnrg

[19] FP7 4WARD Project - Networking of Information (NetInf): http://www.4ward-project.eu/

[20] Publish-Subscribe Internet Routing Paradigm (PSIRP):

http://www.psirp.org/

[21] Swarun Kumar, et al, “CarSpeak: A ContentCentric Network for Autonomous Driving,” ACM SigComm’12, Helsinki, August 2012

Authors

Sung Jin Kim, Currently, in a doctoral course in Soongsil University IT Policy Department, and graduated from Security department of Information Science graduate school in Soongsil University,

and lives in Seoul, Korea, and representative director of ITNOMADS Co., Ltd. who have worked as an expert in IT field for 28 years. Interested field: Network security, database security, next generation network security as IoT information security field. E-mail: sujnkim@gmail.com

Jae-Kyung Park graduated from Hong-ik University in 2002 with a Ph.D. He currently lives in Seoul and is a professor at Seoul Polytechnic University in Seoul, Korea.
Areas of interest are network security and cyber security.