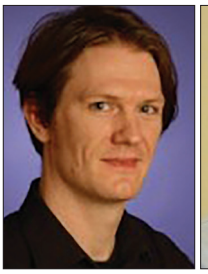
# INFORMATION-CENTRIC NETWORKING SECURITY


Xiaoming Fu


Dirk Kutscher


Satyajayant Misra


Ruidong Li

Over the last few decades, the sum of all forms of video data has grown explosively and is expected to reach 90 percent of all Internet traffic in the near future. Meanwhile, new applications, such as the Internet of Things (IoT), augmented reality, and automatic driving, are emerging as the major trends for the next evolution of the digital society, resulting in the generation and sharing of vast amounts of data. The existing Internet-based technologies, such as peer-to-peer networks, content distribution networks, and cloud computing, will be unable to handle such large amounts of data and provide the necessary quality of service (QoS) to the applications.

In this context, information-centric networking (ICN), characterized by name-based data retrieval and in-network data caching, has emerged as a promising candidate for future networks. It provides access to named data as first-order network service, providing a built-in mechanism for data provenance and greater potential for optimizing forwarding behavior compared to the traditional host-centric communication systems — the Internet today.

From the security perspective, ICN dramatically changes the model from securing the communication path to securing the content itself. Because of such a significant change, security is a particularly important topic, and ICN will enable new approaches with respect to confidentiality, access control, and trust management. This Series issue features recent and emerging advances in ICN security research. Of the 33 submitted papers, five were selected for this issue. The selected articles cover topics including security mechanisms overview for named data networking (NDN), security for an edge named function environment, secure NDN with attribute-based cryptography and software-defined networking (SDN), content protection for NDN, and the design of a security monitoring plane in NDN.

The first article, "An Overview of Security Support in Named Data Networking" coauthored by Zhiyi Zhang, Yingdi Yu, Haitao Zhang, Eric Newberry, Spyridon Mastorakis, Yanbiao Li, Alexander Afanasyev, and Lixia Zhang, presents an overview of the security mechanisms that have been developed for NDN. Their solution set mainly consists of an automated trust establishment scheme for authenticity and integrity, name-based access control for data confidentiality, and in-network storage for improving certificate availability.

One of the prospective ICN usage potentials is to provide in-network function execution, where applications are executed in specialized execution nodes at the edge of the network. The second article, "Open Security Issues for Edge Named Function Environments" contributed by Michał Krol, Claudio Marxer, Dennis Grewe, Ioannis Psaras, and Christian Tschudin, focuses on highlighting the open issues for securing distributed computing given an ICN substrate. The authors concluded the security challenges for an edge named function environment to be consumer authentication, secure input submission, privacy and confidentiality, correctness of functions and results, and automated interoperability.

The third article, "Securing Named Data Networking: Attribute-Based Encryption and Beyond" co-authored by Licheng Wang, Zonghua Zhang, Mianxiong Dong, Lihua Wang, Zhenfu Cao, and Yixian Yang, leverages advanced cryptographic algorithms (IBE/ABE) to provide authentication services and enhance the privacy-preserving capability for NDN. As a further improvement, software-defined networking (SDN) is used for deploying trust-roots for NDN.

The article "Content Protection in Named Data Networking: Challenges and Potential Solutions" co-authored by Yong Yu, Yannan Li, Xiaojiang Du, Ruonan Chen, and Bo Yang proposes a variety of digital signature schemes including cost-effective signatures, privacy-preserving signatures, network coding signatures, and post-quantum signatures to achieve the data integrity and origin authentication in NDN. Furthermore, pre-computation, batch verification, and server-aided verification are proposed to speed up the generation and verification processes for the signatures.

The last article, "A Security Monitoring Plane for Named Data Networking Deployment" by Tan Nguyen, Hoang-Long Mai, Guillaume Doyen, Rémi Cogranne, Wissam Mallouli, Edgardo Montes de Oca, and Olivier Festor, identifies typical attacks in ICN/NDN from a different aspect of security monitoring. In particular, they propose a monitoring plane design to capture a comprehensive set of 18 metrics for illustrating the NDN node state, which are instrumented with the faces, the content store, and the pending interest table. The authors recommend a Bayesian network to correlating these metrics to detect the abnormal behaviors.

This Series issue successfully addresses important security problems of ICN from the aspects of the emerging appli-

cation scenarios and the utilization of advanced technologies. Besides these studies, there are still open challenging problems for ICN that remain unsolved, such as how to balance the time length for caching encrypted data and the expiration time of cryptographic keys, how to securely manage data during its existence in network, how to enforce the backward and forward secrecy for secure access to data, how to preserve privacy, and how to secure data provisioning for intermittent connections.

We would like to take this opportunity to thank all the reviewers for their great support in reviewing the manuscripts. We also thank the Editor-in-Chief, Dr. Tarek S. El-Bawab, and the former Editor-in-Chief, Osman Gebizlioglu, for their supportive guidance during the entire process.

## BIOGRAPHIES

XIAOMING FU (fu@cs.uni-goettingen.de) received his Ph.D. from Tsinghua University and is currently a professor of computer science at University of Göttingen. He is interested in networked systems and services, cloud computing, mobile computing, big data, and social networks. He has served on several Editorial Boards (e.g., *IEEE TNSM*, *IEEE Communications Magazine*, Elsevier *ComNet*, *ComCom*) and conference committees (e.g., SIGCOMM, MobiCom, INFOCOM, ICNP, ICN), and as an elected officer of IEEE ComSoc's Technical Committees on Computer Communications and Internet.

DIRK KUTSCHER is leading IoT Networking Research at the Huawei German Research Center. He is co-chairing research groups in the Internet Research Task Force on Information-Centric Networking (ICNRG) and Decentralized Internet Infrastructure (DINRG). He has published several IETF RFCs, books, and research publications on Internet technologies. He has a Ph.D. from Universität Bremen. Previously he was the chief researcher for networking at NEC Laboratories Europe and worked as a visiting researcher at KDDI R&D Laboratories in Japan.

SATYAJAYANT MISRA is an associate professor in computer science at New Mexico State University. He received his Ph. D. from Arizona State University in 2009. His research interests include wireless sensors, anonymity, security, and survivability issues in future Internet, supercomputing and smart grid architectures. He was an editor of *IEEE Communications Surveys & Tutorials* and is an Editor of *IEEE Wireless Communications*. He has served on several conference committees, including as ACM ICN 2018 TPC Co-Chair.

RUIDONG LI is a senior researcher at the Network System Research Institute, National Institute of Information and Communications Technology (NICT). He received his Ph.D. degree in computer science from the University of Tsukuba in 2008. He is Chair of the IEEE SIG on big data intelligent networking, and Co-Chair of the Young Researcher Group in the AisaFI Forum. His current research interests include future networks, information-centric networking, big data networking, network security, the Internet of Things, and wireless networks.