

Defining Privacy Levels for IP Address Anonymization

Wongyos Keardsri¹ Yunyong Teng-amnuay¹ and Passakon Prathombutr²

¹ *Information System Engineering Laboratory (ISEL), Center of Excellence in Software Engineering
Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University
Phayathai Road, Pathumwan, Bangkok 10330, Thailand*

² *National Electronics and Computer Technology Center (NECTEC)
National Science and Technology Development Agency (NSTDA)
Thailand Science Park, Phaholyothin Road, Klong Luang, Pathumthani 12120, Thailand
E-mail: g49wkr@cp.eng.chula.ac.th, Yunyong.T@Chula.ac.th, prathom@nectec.or.th*

Nowadays, an IP address anonymization is an important technique for network analysis and Internet research. The method of anonymization is the changing of original IP address to anonymized IP address to keep the private information of users in network and to prevent suitable a disclosure and violation of user privacy. The well-known anonymization techniques are TCPdpriv [1], Crypto-PAn [2], Multiple Access Level [3], and TSA [4]; however, they are unsuitable for network analysis functions. The current techniques anonymize all 32 bits of IP address unnecessarily. In fact, we can anonymize the necessary bits or parts of IP address for different privacy levels. In this paper, we propose 5 privacy levels for anonymization scheme. The first level is non-anonymization; all 32 bits of IP address are not anonymized. The second level is n-left anonymization; only n bits of IP address from network part are anonymized. The third level is n-right anonymization; only n bits of IP address from host part are anonymized. The fourth level is full anonymization; all 32 bits of IP address, which consist of host and network parts, are anonymized. The last level is randomly full anonymization; all 32 bits of IP address are randomized before being anonymized. We apply these privacy levels to prefix-preserving IP address anonymization, the technique which can preserve network relationship among the same network group from original IP addresses. Our anonymization scheme is applicable to an administrator who analyzes packet data. The scheme benefits any organizations in exchanging network data, and also appropriates for packet tracers and sniffers.

REFERENCES

1. G. Minshall, *TCPdpriv Command Manual*, July 1996.
2. J. Xu, J. Fan, M. H. Ammar, and S. B. Moon, *Prefix-preserving IP Address Anonymization: Measurement based Security Evaluation and a New Cryptography based Scheme*, IEEE International Conference on Network Protocols (ICNP), 2002, 280-289.
3. Q. Zhang and X. Li, *An IP Address Anonymization Scheme with Multiple Access Levels*, Lecture Notes in Computer Science (LNCS), Springer-Verlag Berlin/Heidelberg, International Conference on Information Networking (ICOIN), 2006, 793-802.
4. R. Ramaswamy, T. Wolf, High-Speed Prefix-Preserving IP Address Anonymization for Passive Measurement Systems, *IEEE/ACM Transactions on Networking (TON)*, 2007, **15**(1), 26-39.

ACKNOWLEDGMENTS

The financial support from Thailand Graduate Institute of Science and Technology (TGIST) is gratefully acknowledged. The scholar ID is TG-44-09-50-076M and the grant number is TGIST 01-50-076.
