Trusted DRM on P2P Network

Chou-Chen Yang[1,*], Jyun-Yi Jiang[2], and Ju-Chun Hsiao[2]

[1] Department of Management Information Systems
National Chung Hsing University
Taichung 402, Taiwan, R.O.C
cc.yang@nchu.edu.tw

[2] Department of Management Information Systems
National Chung Hsing University
Taichung 402, Taiwan, R.O.C
{g9629004, g9729001}@nchu.edu.tw

Received 13 July 2009; Revised 19 August 2009; Accepted 8 September 2009

Abstract. Peer-to-peer file sharing has become a common tool to exchange digital content in Internet. However, duo to a large number of unauthorized files are distributed over peer-to-peer network, users may download the digital files without copyrights thus violate intellectual property rights unconsciously. In this paper, we propose a trusty system named TDRM, which aims to protect every file being exchanged legally. TDRM is constructed on hybrid P2P structure, and adopts technologies including identity-based cryptosystem, digital rights management, secure authentication and payment mechanism. We also show our scheme is more secure, efficient, scalability, and low computational cost.

Keywords: Peer-to-peer network, digital rights management, trusted computing, identity-based cryptosystem

References

[1] Internet World Stats, http://www.internetworldstats.com.

[2] F. Vanier, "World Broadband Statistics: Q4 2008," http://point-topic.com/contentDownload/operatorsource/dslreports/world%20broadband%20statistics%20q4%202008.pdf, 2009.

[3] K. Taima, "Can We Ever Charge Napster Users?," *IEEE Multimedia*, Vol. 9, pp. 76-81, 2002.

[4] U. Lechner and B. F. Schmid, "Communities-Business Models and System Architectures: The Blueprint of MP3.com, Napster and Gnutella Revisited," *Proceedings of the 34th Hawaii International Conference on System Sciences*, 2001.

[5] "Napster Faces Copyright Charges," *Computer Fraud & Security*, Vol. 2001, No.11, pp. 2-2, 2001.

[6] J. S. Beuscart, "Napster Users between Community and Clientele: The Formation and Regulation of a Sociotechnical Group," *Sociologie du travail*, Vol. 47, pp. 1-16, 2005.

[7] R. Stern, "Napster: A Walking Copyright Infringement?," *IEEE Micro*, Vol. 20, pp. 4-5, 2000.

[8] M. F. Radcliffe, "Grokster: The New Law of Third Party Liability for Copyright Infringement under United States Law," *Computer Law & Security Report*, Vol. 22, pp. 137-149, 2006.

[9] S. Ortiz, "Proponents Try to Rehabilitate Peer-to-Peer Technology," *Computer*, Vol. 41, pp. 16-19, 2008.

[10] Y. Cheng, L. Jianbo, Z. Yichun, S. Aina, "The Implementation Architecture of Content Protection in P2P Network," *International Conference on Computational Intelligence and Security Workshops*, pp. 455-458, 2007.

[11] J. Nutzel and R. Grimm, "Potato System and Signed Media Format - An Alternative Approach to Online Music Business," *Third International Conference on Web Delivering of Music*, pp. 23-26, 2003.

* Correspondence author

[12] T. Kalker, D. H. J. Epema, P. H. Hartel, R. L. Lagendijk, M. V. Steen, "Music2Share - Copyright-Compliant Music Sharing in P2P Systems," *Proceedings of the IEEE*, Vol. 92, pp. 961-970, 2004.

[13] G. Gu, B. Zhu, S. Li, S. Zhang, "PLI: A New Framework to Protect Digital Content for P2P Networks," *Applied Cryptography and Network Security*, pp. 206-216, 2003.

[14] Z. Xinwen, L. Dongyu, C. Songqing, S. Ravi, "Towards Digital Rights Protection in BitTorrent-Like P2P Systems," *Proceedings of the 15th ACM/SPIE Multimedia Computing and Networking*, 2008.

[15] I. Gupta, K. Birman, P. Linga, A. Demers, R. Renesse, "Kelips: Building an Efficient and Stable P2P DHT through Increased Memory and Background Overhead," *Peer-to-Peer Systems II*, pp. 160-169, 2003.

[16] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, H. Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications," *Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communication*, pp. 149-160, 2001.

[17] S. Ratnasamy, P. Francis, M. Handley, R. Karp, S. Schenker, "A Scalable Content-Addressable Network," *Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 161-172, 2001.

[18] A. Rowstron and P. Druschel, "Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems," *Proceedings of the IFIP/ACM International Conference on Distributed Systems Platforms (Middleware 2001),* Heidelberg, Germany, Nov. 12-16, pp. 329-350, 2001.

[19] B. Zhao, J. Kubiatowicz, A. Joseph, "Tapestry: An Infrastructure for Fault-tolerant Wide-area Location and Routing," University of California at Berkeley, 2001.

[20] M. Portmann, P. Sookavatana, S. Ardon, A. Seneviratne, "The Cost of Peer Discovery and Searching in the Gnutella Peer-to-Peer File Sharing Protocol," *Ninth IEEE International Conference on Networks*, pp. 263-268, 2001.

[21] M. Ripeanu, "Peer-to-Peer Architecture Case Study: Gnutella Network," *First International Conference on Peer-to-Peer Computing*, pp. 99-100, 2001.

[22] I. Clarke, O. Sandberg, B. Wiley, T. Hong, "Freenet: A Distributed Anonymous Information Storage and Retrieval System," *Designing Privacy Enhancing Technologies*, Vol. 2009, pp. 46-66, 2001.

[23] P. L. Piccard, B. Baskin, C. Edwards, G. Spillman, M. H. Sachs, L. P. Paul, B. Brian, E. Craig, S. George, H. S. Marcus, "eDonkey and eMule," *Securing Im and P2P Applications for the Enterprise Burlington: Syngress*, pp. 267-283, 2005.

[24] W. Ku and C. H. Chi, "Survey on the Technological Aspects of Digital Rights Management," *Information Security*, Vol. 3225, pp. 391-403, 2004.

[25] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Advances in Cryptology*, pp. 47-53, 1985.

[26] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Advances in Cryptology — CRYPTO 2001*, pp. 213-229, 2001.

[27] K. G. Paterson, "ID-Based Signatures from Pairings on Elliptic Curves," *Electronics Letters*, Vol. 38, pp. 1025-1026, 2002.

[28] Q. Wang and Z. Cao, "Identity Based Proxy Multi-Signature," *Journal of Systems and Software*, Vol. 80, pp. 1023-1029, 2007.

[29] Y. Ming, X. Q. Shen, Y. M. Wang, "Identity-Based Encryption with Wildcards in the Standard Model," *The Journal of China Universities of Posts and Telecommunications*, Vol. 16, pp. 64-68, 2009.

[30] Y. Yu, B. Yang, Y. Sun, S. L. Zhu, "Identity Based Signcryption Scheme without Random Oracles," *Computer Standards & Interfaces*, Vol. 31, pp. 56-62, 2009.

[31] C. C. Yang, T. Y. Chang, M. S. Hwang, "A New Anonymous Conference Key Distribution System Based on the Elliptic Curve Discrete Logarithm Problem," *Computer Standards & Interfaces*, Vol. 25, pp. 141-145, 2003.

[32] C. Gorantla, R. Gangishetti, A. Saxena, "A Survey on ID-Based Cryptographic Primitives," 2005.

[33] L. Chen, "An Interpretation of Identity-Based Cryptography," *Foundations of Security Analysis and Design IV*, pp. 183-208, 2007.

[34] M. Schlosser, M. Sintek, S. Decker, W. Nejdl, "HyperCuP - Shaping Up Peer-to-Peer Networks," 2002.

[35] X. Shi, J. Han, Y. Liu, L. M. Ni, "Popularity Adaptive Search in Hybrid P2P Systems," *Journal of Parallel and Distributed Computing*, Vol. 69, pp. 125-134, 2009.

[36] S. S. Cao, W. Yin, X. Y. Chen, "A Robust Cluster-Based Dynamic-Super-Node Scheme for Hybrid Peer-to-Peer Network," *The Journal of China Universities of Posts and Telecommunications*, Vol. 14, pp. 21-26, 2007.

[37] S. G. M. Koo, K. Kannanb, C. S. G. Lee, "On Neighbor-Selection Strategy in Hybrid Peer-to-Peer Networks," *Future Generation Computer Systems*, Vol. 22, pp. 732-741, 2006.