

























- aggregation of multi-domain network events and statistics. In *Proc. USENIX Security'10*, 2010.
- [9] D. R. Choffnes, F. E. Bustamante, and Z. Ge. Crowdsourcing service-level network event monitoring. In *Proceedings of the ACM SIGCOMM 2010 conference*, SIGCOMM '10, pages 387–398, New York, NY, USA, 2010. ACM.
- [10] G. Cormode and S. Muthukrishnan. An improved data stream summary: the count-min sketch and its applications. *Journal of Algorithms*, 55(1):58 – 75, 2005.
- [11] R. Cramer and I. Damgård. Multiparty computation, an introduction. In *Contemporary Cryptology*, Advanced Courses in Mathematics - CRM Barcelona, pages 41–87. Birkhuser Basel, 2005.
- [12] A. Dainotti, R. Amman, E. Aben, and K. C. Claffy. Extracting benefit from harm: using malware pollution to analyze the impact of political and geophysical events on the internet. *SIGCOMM CCR*, 42(1):31–39, 2012.
- [13] I. Damgård, M. Geisler, M. Krøigaard, and J. Nielsen. Asynchronous multiparty computation: Theory and implementation. In S. Jarecki and G. Tsudik, editors, *Public Key Cryptography – PKC 2009*, volume 5443 of *Lecture Notes in Computer Science*, pages 160–179. Springer Berlin Heidelberg, 2009.
- [14] M. Djatmiko, D. Schatzmann, A. Friedman, X. Dimitropoulos, and R. Boreli. Collaborative network outage troubleshooting with secure multiparty computation. *IEEE Communications Magazine*, November 2013.
- [15] Downtetector outage detection service. <http://www.downtetector.com>.
- [16] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In S. Halevi and T. Rabin, editors, *Theory of Cryptography*, volume 3876 of *Lecture Notes in Computer Science*, pages 265–284. Springer Berlin Heidelberg, 2006.
- [17] E. Glatz and X. Dimitropoulos. Classifying internet one-way traffic. In *Proceedings of the 2012 ACM conference on Internet measurement conference*, IMC '12, pages 37–50, New York, NY, USA, 2012. ACM.
- [18] D. Gupta, A. Segal, A. Panda, G. Segev, M. Schapira, J. Feigenbaum, J. Rexford, and S. Shenker. A new approach to interdomain routing based on secure multi-party computation. In *Proceedings of the 11th ACM Workshop on Hot Topics in Networks*, HotNets-XI, pages 37–42, New York, NY, USA, 2012. ACM.
- [19] A. Hanemann, J. W. Boote, E. L. Boyd, J. Durand, L. Kudarimoti, R. Lapacz, D. M. Swany, S. Trocha, and J. Zurawski. Perfsonar: a service oriented architecture for multi-domain network monitoring. In *Proceedings of the Third international conference on Service-Oriented Computing*, ICSOC'05, 2005.
- [20] W. Henecka and M. Roughan. Strip: Privacy-preserving vector-based routing. In *IEEE International Conference on Network Protocols*, 2013.
- [21] M. Hirt, C. Lucas, U. Maurer, and D. Raub. Passive corruption in statistical multi-party computation. In *Proc. ICITS'12*. Springer-Verlag, 2012.
- [22] E. Katz-Bassett, H. V. Madhyastha, J. P. John, A. Krishnamurthy, D. Wetherall, and T. Anderson. Studying black holes in the internet with hubble. In *Proceedings of the 5th USENIX NSDI Symposium*, pages 247–262, Berkeley, CA, USA, 2008. USENIX Association.
- [23] E. Katz-Bassett, C. Scott, D. R. Choffnes, I. Cunha, V. Valancius, N. Feamster, H. V. Madhyastha, T. Anderson, and A. Krishnamurthy. Lifeguard: practical repair of persistent route failures. In *Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication*, SIGCOMM '12, pages 395–406, New York, NY, USA, 2012. ACM.
- [24] D. Many, M. Burkhart, and X. Dimitropoulos. Fast private set operations with sepia. Technical Report 345, ETHZ, March 2012.
- [25] NANOG. <http://www.nanog.org/>.
- [26] outages@outages.org. The outages mailinglist. <http://puck.nether.net/mailman/listinfo/outages>.
- [27] RIPE Routing Information Service. <http://www.ripe.net/data-tools/stats/ris/routing-information-service>.
- [28] M. Roughan and Y. Zhang. Privacy-preserving performance measurements. In *Proceedings of the 2006 SIGCOMM workshop on Mining network data*, MineNet '06, pages 329–334, New York, NY, USA, 2006. ACM.
- [29] M. Roughan and Y. Zhang. Secure distributed data-mining and its application to large-scale network measurements. *SIGCOMM Comput. Commun. Rev.*, 36(1):7–14, Jan. 2006.
- [30] Route Views Page. <http://www.routeviews.org>.
- [31] D. Schatzmann, S. Leinen, J. Kögel, and W. Mühlbauer. FACT: flow-based approach for connectivity tracking. In *Proc. PAM'11*, pages 214–223, Berlin, Heidelberg, 2011. Springer-Verlag.
- [32] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, Nov. 1979.
- [33] X. Shi, Y. Xiang, Z. Wang, X. Yin, and J. Wu. Detecting prefix hijackings in the internet with argus. In *Proceedings of the 2012 ACM conference on Internet measurement conference*, IMC '12, pages 15–28, New York, NY, USA, 2012. ACM.
- [34] The Swiss Education and Research Network (SWITCH). <http://www.switch.ch>.
- [35] B. Tierney, J. Metzger, J. Boote, E. Boyd, A. Brown, R. Carlson, M. Zekauskas, J. Zurawski, M. Swany, and M. Grigoriev. perfonar: Instantiating a global network measurement framework. In *4th Workshop on Real Overlays and Distributed Systems*, 2009.
- [36] M. Zhang, C. Zhang, V. Pai, L. Peterson, and R. Wang. Planetseer: internet path failure monitoring and characterization in wide-area services. In *Proceedings of the 6th OSDI Conference*, pages 12–12, Berkeley, CA, USA, 2004. USENIX Association.
- [37] C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis. A light-weight distributed scheme for detecting ip prefix hijacks in real-time. In *Proceedings of the ACM SIGCOMM 2007 Conference*, pages 277–288, New York, NY, USA, 2007. ACM.