David Eckhoff, Tobias Limmer and Falko Dressler, "Hash Tables for Efficient Flow Monitoring: Vulnerabilities and Countermeasures," Proceedings of 34th IEEE Conference on Local Computer Networks (LCN 2009): 4th IEEE LCN Workshop on Network Measurements (WNM 2009), Zurich, Switzerland, October 2009, pp. 1087-1094.
doi: 10.1109/LCN.2009.5355211

There are no flows exported in the first export because there are no flows older than 30 s. The second export at 60 s will shorten the bucket list by the amount of flows received and progressed longer than 30 s ago. Although this should be a considerable percentage of all saved flows it only has temporary effects because the bucket list will instantly be filled again by the attacker. With an attack speed of 10 000 packets/s even the temporary effect is only marginal. N.B., an attack speed of 10 000 packets/s results in a transmission rate of about 4 MBit/s due to the small packet size of 54 byte.

V. Conclusion

The obvious countermeasure against the hash collision DoS is a hash function for which collisions cannot easily be created. Cryptographic hash functions such as MD5 [15] or SHA-1 [16] would provide such a feature but take too long to compute to be efficiently deployed in a flow monitor. It seems that a randomized permutation table could offer sufficient speed and security but this has yet to be tested. There might be an even easier solution using random values with simple addition and multiplication. Finding an optimal function for hash table organization in flow monitoring will be future research.

References

[1] R. Sommer and A. Feldmann, "NetFlow: information loss or win?" in *2nd ACM SIGCOMM Internet Measurement Workshop (IMW 2002)*. Marseille, France: ACM, November 2002, pp. 173–174.

[2] T. Limmer and F. Dressler, "Seamless Dynamic Reconfiguration of Flow Meters: Requirements and Solutions," in *16. GI/ITG Fachtagung Kommunikation in Verteilten Systemen (KiVS 2009)*. Kassel, Germany: Springer, March 2009, pp. 179–190.

[3] R. T. Lampert, C. Sommer, G. Münz, and F. Dressler, "Vermont - A Versatile Monitoring Toolkit Using IPFIX/PSAMP," in *IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation (MonAM 2006)*. Tübingen, Germany: IEEE, September 2006, pp. 62–65.

[4] L. Deri, "nProbe: an Open Source NetFlow Probe for Gigabit Networks," in *TERENA Networking Conference (TNC 2003)*, Zagreb, Croatia, May 2003.

[5] B. Claise, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information," IETF, RFC 5101, January 2008.

[6] J. Quittek, S. Bryant, B. Claise, P. Aitken, and J. Meyer, "Information Model for IP Flow Information Export," IETF, RFC 5102, January 2008.

[7] B. Claise, "Cisco Systems NetFlow Services Export Version 9," IETF, Tech. Rep. RFC 3954, October 2004.

[8] G. Carle, F. Dressler, R. A. Kemmerer, H. König, C. Kruegel, and P. Laskov, "Manifesto - Perspectives Workshop: Network Attack Detection and Defense," in *Dagstuhl Perspectives Workshop 08102 - Network Attack Detection and Defense 2008*, Schloss Dagstuhl, Wadern, Germany, March 2008.

[9] D. V. Sarwate, "Computation of Cyclic Redundancy Checks via Table Look-Up," *Communications of the ACM*, vol. 31, no. 8, pp. 1008–1013, 1988.

[10] Anarchriz/DREAD, "CRC and how to Reverse it," April 1999. [Online]. Available: http://www.woodmann.com/RCE-CD-SITES/Anachriz/programming/crc.htm

[11] K. Brayer and J. L. Hammond Jr, "Evaluation of error detection polynomial performance on the AUTOVON channel," in *National Telecommunications Conference*, vol. 1. New Orleans, LA: IEEE, December 1975, pp. 8–21 to 8–25.

[12] B. Maxwell, D. R. Thompson, G. Amerson, and L. Johnson, "Analysis of CRC methods and potential data integrity exploits," in *International Conference on Emerging Technologies*, Minneapolis, MI, August 2003, pp. 25–26.

[13] H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN Flooding Attacks," in *21st IEEE Conference on Computer Communications (IEEE INFOCOM 2002)*, New York, NY, June 2002.

[14] A. Turner, "tcpreplay." [Online]. Available: http://tcpreplay.synfin.net/trac/wiki/tcpreplay

[15] R. Rivest, "The MD5 Message-Digest Algorithm," IETF, RFC 1321, April 1992.

[16] D. Eastlake and P. Jones, "US secure hash algorithm 1 (SHA1)," IETF, RFC 3174, September 2001.