Exploiting machine learning to subvert your spam filter. In *Proceedings of the 1st USENIX Workshop on Large-Scale Exploits and Emergent Threats*. LEET'2008. USENIX, 1-9.

[45] P. Oechslin. Making a Faster Cryptanalytic Time-Memory Trade-Off. In *Proceedings of 23rd Annual International Cryptology Conference*. CRYPTO'2003. Springer, 2729: 617-630.

[46] P. Prakash, M. Kumar, R. R. Kompella, and M. Gupta. Phishnet: predictive blacklisting to detect phishing attacks. In *Proceedings of the 29th Conference on Information Communications*. INFOCOM'2010. IEEE, 1-5.

[47] M. A. Rajab, L. Ballard, N. Lutz, P. Mavrommatis, and N. Provos. CAMP: Content-agnostic malware protection. In *Proceedings of the Network and Distributed System Security Symposium*. NDSS'2013.

[48] R. N. Rodrigues, L. L. Ling, and V. Govindaraju. Robustness of multimodal biometric fusion methods against spoof attacks. *Journal of Visual Languages & Computing*. 2009. Elsevier, 20(3): 169-179.

[49] B. I. P. Rubinstein, B. Nelson, L. Huang, A. D. Joseph, S. Lau, S. Rao, N. Taft, and J. D. Tygar. Stealthy poisoning attacks on PCA-based anomaly detectors. *ACM SIGMETRICS Performance Evaluation Review*. 2009. ACM, 37(2): 73-74.

[50] G. Salton and M. J. McGill. Introduction to modern information retrieval. 1983. McGraw-Hill.

[51] A. Slowinska, T. Stancescu, and H. Bos. Howard: A Dynamic Excavator for Reverse Engineering Data Structures. In *Proceedings of the Network and Distributed System Security Symposium*. NDSS'2011.

[52] N. Šrndić and P. Laskov. Practical evasion of a learning-based classifier: A case study. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*. SP'2014. IEEE, 197-211.

[53] F. Toolan and J. Carthy. Phishing detection using classifier ensembles. *eCrime Researchers Summit*. eCRIME'2009. IEEE, 1-9.

[54] K. Tretyakov. Machine learning techniques in spam filtering. *Data Mining Problem-oriented Seminar*. 2004. MTAT, 60-79.

[55] S. Udupa, S. Debray, and M. Madou. Deobfuscation: Reverse engineering obfuscated code. In *Proceedings of the 12th Working Conference on Reverse Engineering*. WCRE'2005. IEEE.

[56] T. Wang, T. Wei, G. Gu, and W. Zou. TaintScope: A checksum-aware directed fuzzing tool for automatic software vulnerability detection. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*. SP'2010. IEEE, 497-512.

[57] W. Weir, S. Aggarwal, B. D. Medeiros, and B. Glodek. Password Cracking Using Probabilistic Context-Free Grammars. In *Proceedings of the 2009 IEEE Symposium on Security and Privacy*. SP'2009. IEEE, 391-405.

[58] C. Whittaker, B. Ryner, and M. Nazif. Large-scale automatic classification of phishing pages. In *Proceedings of the Network and Distributed System Security Symposium.* NDSS'2010.

[59] B. Yadegari, B. Johannesmeyer, B. Whitely, and S. Debray. A generic approach to automatic deobfuscation of executable code. In *Proceedings of the 2015 IEEE Symposium on Security and Privacy*. SP'2015. IEEE.

[60] Y. Zhang, J. I. Hong, and L. F. Cranor. Cantina: a content-based approach to detecting phishing web sites. In *Proceedings of the 16th International Conference on World Wide Web*. WWW'2007. ACM, 639-648.

[61] H. Zhang, G. Liu, T. Chow, and W. Liu. Textual and visual content based anti-phishing: A bayesian approach. *IEEE Transactions on Neural Networks*. 2011. IEEE, 22(10): 1532-1546.