Related Work	References
Basic Privacy attack	[3]*, [4], [6]*, [8]
Black-box attack	[1], [2], [5], [7]
Gray-box attack	[9], [10]

* marked references in basic privacy attack can be specified explicitly to be white box or black box attacks

[1] Papernot, Nicolas, Patrick McDaniel, and Ian Goodfellow. "Transferability in machine learning: from phenomena to black-box attacks using adversarial samples." *arXiv preprint arXiv:1605.07277* (2016).
[2] Rosenberg, Ishai, et al. "Generic Black-Box End-to-End Attack against RNNs and Other API Calls Based Malware Classifiers." *arXiv preprint arXiv:1707.05970* (2017).
[3] Tramèr, Florian, et al. "Stealing Machine Learning Models via Prediction APIs." *USENIX Security Symposium*. 2016.
[4] Huang, Ling, et al. "Adversarial machine learning." *Proceedings of the 4th ACM workshop on Security and artificial intelligence*. ACM, 2011.
[5] Papernot, Nicolas, et al. "Practical black-box attacks against machine learning." *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. ACM, 2017.
[6] Fredrikson, Matt, Somesh Jha, and Thomas Ristenpart. "Model inversion attacks that exploit confidence information and basic countermeasures." *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015.
[7] Shokri, Reza, et al. "Membership inference attacks against machine learning models." *Security and Privacy (SP), 2017 IEEE Symposium on*. IEEE, 2017.
[8] Grosse, Kathrin, et al. "Adversarial perturbations against deep neural networks for malware classification." *arXiv preprint arXiv:1606.04435* (2016).
[9] DeMott, Jared, Richard Enbody, and William F. Punch. "Revolutionizing the field of grey-box attack surface testing with evolutionary fuzzing." *BlackHat and Defcon* (2007).
[10] S.-M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard. Deepfool: a simple and accurate method to fool deep neural networks. CVPR, 2016.