Topic: **Arbitrary Code Execution: What it is and what you can do with it**

Members: Roger Ogden, Brik Royster

References:

Lineberry, Anthony. "Malicious Code Injection via/dev/mem." *Black Hat Europe* (2009): 11.

Giannetsos, Thanassis, et al. "Arbitrary code injection through self-propagating worms in von neumann architecture devices." *The Computer Journal* (2010): bxq009.

Fiskiran, A. Murat, and Ruby B. Lee. "Runtime execution monitoring (REM) to detect and prevent malicious code execution." *Computer Design: VLSI in Computers and Processors, 2004. ICCD 2004. Proceedings. IEEE International Conference on*. IEEE, 2004.

Holm, Hannes, et al. "Success Rate of Remote Code Execution Attacks-Expert Assessments and Observations." *J. UCS* 18.6 (2012): 732-749.

Jancewicz, Russell J., et al. "Malicious takeover of voting systems: arbitrary code execution on optical scan voting terminals." *Proceedings of the 28th Annual ACM Symposium on Applied Computing*. ACM, 2013.