How do you run some security-sensitive code on a computer where you believe that the operating system may have been modified by sophisticated malicious software? We survey different approaches to bootstrap trust in commodity computers. One such approach is Flicker, an infrastructure for executing the security-sensitive code in isolation, with minimal assumptions. Since the isolation guarantee is based on only 250 lines of code within the flicker infrastructure, it may be feasible to use automatic theorem provers to formally prove security properties of this approach.