Demonstration of the Acoustic Cryptanalysis

Tomas Fabsic, Ondrej Gallo, Viliam Hromada

Slovak University of Technology

Bratislava, Slovakia

Abstract

In 2014, an acoustic cryptanalysis attack on RSA was presented by Daniel Genkin, Adi Shamir and Eran Tromer. The authors demonstrated that acoustic emanations from a laptop can be used to reveal the private key in implementations of RSA in older versions of GnuPG. We repeated their attack and in this presentation we state our observations and demonstrate the fundamental principles of the attack.