The 'Million Message Attack' in 15 000 Messages

Graham Steel, INRIA, France

June 7, 2012

In our efforts to formally verify the correctness of cryptographic security APIs, we have recently been trying to reconcile our results using Dolev-Yao style models with standard cryptographic models in order to obtain stronger proofs of security (see e.g. CSF 11). One problem with trying to apply these results to real-world APIs is that most cryptographic hardware such as smartcards and HSMs still use RSA PKCS#1v1.5 padding for asymmetric encryption, a scheme which is known not to be "IND-CCA2" secure (the basic assumption we need for any hope of a soundness result). We hypothesise that the reason manufacturers have not upgraded is that the best known attack on RSA PKCS#1v1.5, due to Bleichenbacher, is known as the "million message attack", and is therefore not thought to represent a practical threat.

In order to accelerate the update of IND-CCA2 schemes, we have developed a new version of the Bleichenbacher attack that requires a median of only 15000 messages for a 1024 bit modulus. This makes it a highly practical threat. In this talk we will just give the main tricks. The full details and results on hardware will be presented at CRYPTO '12.

Joint work with Romain Bardou (INRIA, France), Riccardo Focardi (Università di Venezia Ca' Foscari, Italy), Yusuke Kawamoto (University of Birmingham, UK), Lorenzo Simionato (Università di Venezia Ca' Foscari, Italy) and Joe Kai-Tsay (Norges Teknisk-Naturvitenskapelige Universitet, Norway).