Security Evaluation of RNGs — The Updated Evaluation Guidelines AIS 20 and AIS 31

Werner Schindler

Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

Many cryptographic applications need random numbers. Weak RNGs may drastically reduce the strength of principally strong cryptographic mechanisms. Thus a solid and reliable security evaluation of RNGs is indispensable.

The Common Criteria do not provide a concrete evaluation methodology for RNGs. In the German scheme evaluation guidelines for deterministic RNGs (AIS 20) and for physical RNGs (AIS 31) have been effective since 1999, resp. since 2001. Last year the corresponding mathematical-technical documents were updated. Some 'old' functionality classes have essentially been kept unchanged (with partially increased requirements and assigned with new names), and new functionality classes have been introduced.

In this presentation requirements and security goals of the most relevant functionality classes are worked out, and typical applications are addressed.