AES-T1700

- Trojan description
  - Modulating an (unused) pin on a chip generates an RF signal. This signal can be used to transmit the key bits. This attack is performed at 1560KHz and can be received with an ordinary AM radio. The data carried by the AM signal needs to be easily interpreted by a human. A beep scheme is utilized where a single beep followed by a pause represents a ‘0’ and a double beep followed by a pause represents a ‘1’. A description on detail implementation of AM transmission can be found at [1]. In this implementation, the Trojan gets activated after each 128'hFFFF_FFFF_FFFF_FFFF_FFFF_FFFF_FFFF_FFFF encryptions.

- Trojan taxonomy
  - Insertion phase: Design
  - Abstraction level: Register Transfer level
  - Activation mechanism: Internally conditionally triggered
  - Effects: Leak Information
  - Location: Processor
  - Physical characteristics: Functional

Please send your concerns/questions to

Dr. Hassan Salmani at SalmaniHSN@gmail.com

Administrator at admin@trust-hub.org

Reference:

[1] Alex Baumgarten, Michael Steffen, Matthew Clausman, Joseph Zambreno, "A case study in hardware Trojan design and implementation," International Journal of Information Security, Volume 10, Issue 1, pp. 1-14, 2011.