☰ **Item Navigation**

Supplemental Reading for Asymmetric Encryption Attack

An asymmetric encryption attack happened in 2010 to <u>Sony with their Playstation 3</u> game console. It turns out they weren't ensuring the randomized seed value was changed for every signature. This resulted in a hacker group called 'fail0verflow' being able to recover the private key that Sony used to sign software for the platform. This allowed modders to write and sign custom software that was allowed to run on the otherwise very locked down console platform. This <u>resulted in game piracy</u> becoming a problem for Sony, as this facilitated the illicit copying and distribution of games, causing a significant loss in sales.

Mark as completed

👍 Like   👎 Dislike   🚩 Report an issue