

IntrusionResistant

A system is called "intrusion resistant", if it, as a whole, continues to adhere to it's predefined rules even in case of a part of the system components violate these rules (accidentally or by malicious intent).

The aim of intrusion resistance is to counter-balance for the consequences of continued operation of an embraced device under violation of normaly system-guaranted assumptions (e.g., forged data, access rights).

Known ways to achieve that goal are tamper proofed hardware and systems based on ByzantineAgreement.

Remark: Eventually there is no such thing like tamper proofed hardware, just more complication to do so.

Last modifikation: Tue, 02 May 2006 19:29:31 +0200

Author(s): jfw,

Document number A849640f672ed0df0958abc0712110f3c page IntrusionResistant delivered to public at
Wed, 08 Sep 2010 15:52:48 +0200