

# ISO/IEC TS 30104:2015-05 (E)

## Information Technology - Security Techniques - Physical Security Attacks, Mitigation Techniques and Security Requirements

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Symbols and abbreviated terms .....	5
5	Physical security .....	5
6	Physical security invasive mechanisms .....	6
6.1	Overview .....	6
6.2	Tamper proof .....	7
6.3	Tamper resistant .....	7
6.4	Tamper detection .....	7
6.5	Tamper evident .....	7
6.6	Additional physical security considerations .....	8
6.6.1	Summary .....	8
6.6.2	Size and weight .....	8
6.6.3	Mixed and Layered Systems .....	8
7	Physical security invasive attacks and defences .....	8
7.1	Overview .....	8
7.2	Attacks .....	9
7.2.1	Attack mechanisms .....	9
7.2.2	Machining methods .....	9
7.2.3	Shaped charge technology .....	11
7.2.4	Energy attacks .....	11
7.2.5	Environmental conditions .....	12
7.3	Defences .....	12
7.3.1	Overview .....	12
7.3.2	Tamper resistant .....	13
7.3.3	Tamper evident .....	14
7.3.4	Tamper detection sensor technology .....	15
7.3.5	Tamper responding .....	18
8	Physical security non-invasive mechanisms .....	20
8.1	Overview .....	20
8.2	Mixed and Layered Systems .....	20
9	Physical security non-invasive attacks and defences .....	20
9.1	Overview .....	20
9.2	Attacks .....	20
9.2.1	Overview .....	20
9.2.2	External Probe attacks .....	20
9.2.3	External EME attacks .....	21
9.2.4	Timing analysis .....	21

9.3	Defences .....	21
10	Operating Envelope Concept .....	22
11	Development, delivery and operation considerations .....	22
11.1	Introduction .....	22
11.2	Development .....	22
11.2.1	Functional test and debug .....	22
11.2.2	Security testing .....	22
11.2.3	Environmental testing .....	23
11.2.4	Factory installed keys or security parameters .....	23
11.3	Delivery .....	23
11.3.1	Documentation .....	23
11.3.2	Packaging .....	24
11.3.3	Delivery verification .....	24
11.4	Operation .....	24
11.4.1	Overview .....	24
11.4.2	Implementation feedback .....	24
11.4.3	Feedback during attack .....	24
12	Physical security evaluation and testing .....	24
12.1	Overview .....	24
12.2	Standards .....	25
12.2.1	FIPS PUB 140-2, Security Requirements for Cryptographic Modules .....	25
12.2.2	Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules .....	25
	Security requirements for cryptographic modules .....	25
	Test requirements for cryptographic modules .....	26
	-- Evaluation criteria for IT security -- Part 1: Introduction and general model .....	26
	techniques -- Evaluation criteria for IT security -- Part 2: Security functional components .....	26
	techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components .....	27
	Methodology for IT security evaluation .....	27
12.3	Programs and schemes .....	27
12.3.1	NIST and CSE Cryptographic Module Validation Program .....	27
12.3.2	Japan Cryptographic Module Validation Program .....	27
12.3.3	Korea Cryptographic Module Validation Program .....	27
12.3.4	Common Criteria .....	28
	Annex A (informative) Example of a physical security design .....	29
	Bibliography .....	30