ISO/IEC TR 5891:2024-04 (E)

Information security, cybersecurity and privacy protection - Hardware monitoring technology for hardware security assessment

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Abbreviated terms **2**

5 Relationship to existing standards **2**
5.1 Standards of security assessment 2
5.2 Relationship to ISO/IEC 15408-3 3
5.3 Relationship to ISO/IEC TS 30104 3

6 Background **3**
6.1 Complexity and security 3
6.2 Challenges in defining hardware security assessment techniques 3

7 Hardware monitoring technologies **4**
7.1 Overview 4
7.2 Research in academic areas 4
7.3 Industrial cases 5
7.4 Purpose 6
7.4.1 Security 6
7.4.2 Debugging 7
7.4.3 Tuning performance 8
7.4.4 Fault tolerance and QoS 8
7.4.5 Physical specification measurement 9
7.4.6 Application-specific monitoring 10
7.5 Carrier type 10
7.5.1 Middleware 10
7.5.2 Software 11
7.5.3 Hardware-assisted monitors 13
7.5.4 Software vs. hardware-assisted solutions 16
7.6 Target entity 16
7.6.1 IP cores 16
7.6.2 Processing units 17
7.6.3 Memory 17
7.6.4 Peripheral devices 18
7.7 Objective patterns 18
7.7.1 Information content 18
7.7.2 Physical specification 18
7.7.3 Behaviours 18
7.8 Deployment method 19
7.8.1 General 19
7.8.2 Intrusiveness 19
7.8.3 Offline or online 19
7.8.4 Synchronous or asynchronous 19
7.8.5 Single or multiple monitors 19
7.8.6 Scalability 19
7.8.7 Resilience and redundancy 20
7.8.8 Compatibility 20

7.8.9 Impact on performance 20
7.8.10 Lawful and ethical data handling regulations and requirements 20

8 Utilizing monitoring technologies for hardware security assessment 20
8.1 Existing state-of-the-art security assessment approaches 20
8.2 How hardware monitoring can help 21
8.3 Challenges 22

9 Certification for monitoring hardware 24

Bibliography 27