

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Motivation . . . . .	1
1.2	Outlining Fundamental Terms for this Discussion . . . . .	2
1.3	Objectives . . . . .	5
1.4	Achieving these Goals . . . . .	6
1.4.1	Approach . . . . .	6
1.4.2	Evaluation Criteria . . . . .	9
1.4.3	Limitations . . . . .	10
1.5	Principal Contributions . . . . .	11
<b>2</b>	<b>Literature Survey</b>	<b>13</b>
2.1	Overview . . . . .	13
2.2	Search Space . . . . .	14
2.3	(Closely) Related Work . . . . .	15
2.4	Terminology and Structure for Extracting Activities . . . . .	17
2.5	Implications from Educational Science for E-Learning Systems . . . . .	18
2.5.1	Social Support by Cooperation and Communication . . . . .	19
2.5.2	Activities of Students as Important Step of the Learning Process	21
2.5.3	Priority to Meet Learning Objectives . . . . .	23
2.5.4	Flexible Learning . . . . .	24
2.5.5	Integration into Learning Environment . . . . .	26
2.6	Security Engineering for E-Learning . . . . .	27
2.6.1	Software Architecture . . . . .	27
2.6.2	Security Concepts . . . . .	30
2.7	Resulting Limitations for Practical Systems . . . . .	32
2.7.1	Complexity and Character of E-Learning Systems . . . . .	32
2.7.2	Security Restraints . . . . .	33
2.8	Conclusion . . . . .	34

<b>3</b>	<b>Preparation of the Threat Analysis</b>	<b>37</b>
3.1	Overview . . . . .	37
3.2	Role Based Access Control . . . . .	38
3.3	Identification of Assets . . . . .	40
3.3.1	Procedure . . . . .	40
3.3.2	E-Learning . . . . .	44
3.3.3	Information Security Services . . . . .	51
3.3.4	Web Services . . . . .	53
3.4	Conclusion . . . . .	56
<b>4</b>	<b>Analysis of Threats in E-Learning Systems</b>	<b>59</b>
4.1	Overview . . . . .	59
4.2	Threat Analysis Approach . . . . .	60
4.2.1	Comparison of Approaches . . . . .	60
4.2.2	Critical Discussion of FTA Approach . . . . .	62
4.3	Analysis of E-Learning Assets . . . . .	63
4.3.1	Introduction to Fault Tree Terminology . . . . .	64
4.3.2	Scenario: Purchased Advanced Training with Mentoring . . . . .	65
4.3.3	Threats of E-Learning Assets . . . . .	66
4.4	Analysis of Information Security Service Assets . . . . .	71
4.4.1	Scenario: Distant University with Various Study Courses . . . . .	71
4.4.2	Threats of Information Security Service Assets . . . . .	72
4.5	Analysis of Web Service Assets . . . . .	76
4.5.1	Scenario: Various Training Providers with Single Authentication . . . . .	76
4.5.2	Threats of Web Service Assets . . . . .	77
4.6	Perpetual Concept Related Issues . . . . .	81
4.6.1	Enrolment and Role Hierarchy . . . . .	81
4.6.2	Supervision and Observation . . . . .	82
4.6.3	Import and Export Functionality . . . . .	83
4.7	Low Level Event Based Threats . . . . .	84
4.7.1	Investigative Process . . . . .	85
4.7.2	Exploitation . . . . .	87
4.8	Conclusion . . . . .	90
<b>5</b>	<b>Case Studies</b>	<b>93</b>
5.1	Overview . . . . .	93
5.2	Learning Management System . . . . .	93
5.2.1	Term Definition and Functionality . . . . .	93
5.2.2	Selection of Learning Management Systems . . . . .	94

5.3	Information Security Services . . . . .	99
5.3.1	Authentication . . . . .	99
5.3.2	Access Control . . . . .	100
5.3.3	Data Confidentiality . . . . .	102
5.3.4	Data Integrity . . . . .	104
5.3.5	Non-Repudiation . . . . .	104
5.3.6	Availability . . . . .	105
5.4	Conceptual Shortcomings . . . . .	105
5.4.1	Deactivation of Foreign Mail Addresses . . . . .	105
5.4.2	Personal (Contact) Data in Search for Users . . . . .	106
5.4.3	Generalisation and Module Inclusion . . . . .	107
5.5	Conclusion . . . . .	109
<b>6</b>	<b>Recommendations</b>	<b>111</b>
6.1	Overview . . . . .	111
6.2	Management Strategies . . . . .	112
6.3	Implementation Concepts and Technical Remarks . . . . .	113
6.3.1	Base System Protection and Implementation . . . . .	113
6.3.2	Authentication . . . . .	117
6.3.3	Availability . . . . .	118
6.4	Organisational Concept and Policies . . . . .	120
6.4.1	Data Confidentiality . . . . .	121
6.4.2	Data Integrity . . . . .	124
6.4.3	Non-repudiation . . . . .	125
6.4.4	Access Control . . . . .	127
6.5	User Support and Human Factor . . . . .	128
6.5.1	Guidance and (Security) Usability . . . . .	128
6.5.2	Security Education and User Involvement . . . . .	130
6.6	Security Agent for Practical Support . . . . .	132
6.6.1	General Specifications . . . . .	132
6.6.2	Integrity Protection by Digital Signatures . . . . .	134
6.6.3	Realisation . . . . .	136
6.6.4	Application in MOODLE . . . . .	137
6.6.5	Conclusion of the Security Agent Project . . . . .	138
6.7	Conclusion . . . . .	138
<b>7</b>	<b>Conclusion and Future Work</b>	<b>141</b>
<b>A</b>	<b>Complete Fault Tree Analysis Results</b>	<b>159</b>

- A.1 Overview . . . . . 159
- A.2 Main Tree . . . . . 162
  - A.2.1 Block 1: E-Learning Assets . . . . . 162
  - A.2.2 Block 2: Information Security Service Assets . . . . . 169
  - A.2.3 Block 3: Web Services Assets . . . . . 181
- A.3 Redundant Subtrees . . . . . 189