

Inhaltsverzeichnis

1. Einleitung	1
1.1. Kontext	2
1.2. Bestehende Ansätze und Verwandte Arbeiten	4
1.3. Forschungsfrage und Herausforderungen	6
1.4. Ergebnisse dieser Arbeit	7
1.5. Aufbau der Arbeit	8
2. Entwicklungsparadigmen für Security und Privacy	9
2.1. Grundlegende Begriffe	9
2.1.1. Software Security	11
2.1.2. Privacy	12
2.1.3. Reaktives Vulnerability Management	13
2.1.4. Entwicklung sicherer Software	14
2.2. Secure Development Lifecycle	17
2.2.1. ISO Security-Managementprozesse	17
2.2.2. Microsoft Security Development Lifecycle	18
2.2.3. Security Touchpoints	20
2.3. Agile Modellgetriebe Entwicklung	21
2.3.1. Modellverarbeitung mit MontiCore	25
2.3.2. Architekturbeschreibungssprachen	29
3. Anforderungen an Modelle und Werkzeuge	33
4. Security-Architekturmodellierung mit MontiSecArc	37
4.1. Modellelemente	38
4.1.1. Trust Level	40
4.1.2. Critical Port	43
4.1.3. Encrypted Connector	44
4.1.4. Authorization	45
4.1.5. Authentication	47
4.1.6. Drittanbieterkomponenten	49
4.1.7. Physische Security	50
4.2. Weitere Verwandte Arbeiten	54
5. Security-Architekturanalyse mit MontiSecArc	59
5.1. Modellierung von Flaw Correction Pattern	61

5.2.	Formalisierung bekannter Flaws als Flaw Correction Pattern	65
5.2.1.	<i>Untrusted Connector</i>	65
5.2.2.	<i>Vulnerabilities von Drittanbieterkomponenten</i>	66
5.2.3.	Physische Security	67
5.2.4.	<i>Multiple Access Points</i>	68
5.2.5.	Security-Designprinzipien	69
5.2.6.	identity Link und Encrypted Connector	73
5.2.7.	Analyseergebnisse priorisieren	74
5.3.	Flaw Smells	75
5.3.1.	identity Link und Access	75
5.3.2.	identity Link und Trust Level	76
5.3.3.	Verschlüsselte Pfade	77
5.3.4.	Konventionen	78
5.3.5.	Effektive Zugriffsrechte	79
5.3.6.	Ports ohne Zugriffskontrolle	79
5.3.7.	Unterstützung einer manuellen Security-Architekturanalyse	80
6.	Modellgetriebene Entwicklung von Systemen mit MontiSecArc	81
6.1.	Security-Implikationen der Modellgetriebenen Entwicklung	81
6.2.	Übersetzung von MontiSecArc in ein verteilt ausgeführtes System	83
6.3.	Generierung eines Network Intrusion Detection Systems	87
6.4.	Implementierung der Generatoren	88
7.	Zustandsbasierte Security-Tests für Webapplikationen	95
7.1.	Angriffe auf das HTTP Session Management	95
7.2.	Identifikation von Session Management Vulnerabilities	100
7.2.1.	Funktionales Session-Modell	100
7.2.2.	Security-Tests	102
8.	Sichere Eingabe- und Ausgabeverarbeitung mit MontICoder	107
8.1.	Bestehende Ansätze	109
8.2.	Korrektes Unparsen und Encoden	112
8.3.	Unparser und Encoder definieren	115
8.3.1.	Sprachkomposition	117
8.4.	Anwendung von Unparsern und Encodern	119
8.4.1.	Sprach Features reduzieren	120
8.4.2.	Encoding für ausführbare Sprachen	121
8.5.	MontICoder	122
9.	Modellgetriebene Entwicklung von Privacy	125
9.1.	Privacy-Bedenken von Nutzern	125
9.2.	Herausforderungen bei der Realisierung von Privacy	126
9.3.	Anwendungsszenario und existierende Lösungen	127
9.4.	Privacy Development Language	129

9.5. Generierung der Privacy Policy	133
9.6. Nutzerinteraktion	137
10. Evaluation und Fallstudien	141
10.1. Anwendung von MontiSecArc im Kontext des Projekts SensorCloud	141
10.1.1. Entwurf und Durchführung der Evaluation	141
10.1.2. Szenario und exemplarische Lösung	142
10.1.3. Einfluss von MontiSecArc auf die erstellten Architekturbeschreibungen	144
10.2. Anwendung von MontiCoder für HTML und JavaScript	149
10.3. Anwendung der Privacy Development Language im Projekt IPACS	152
11. Schluss	157
11.1. Ergebnisse	157
11.2. Grenzen der Ansätze	160
11.3. Weiterführende Arbeiten im Kontext der Forschungsfrage	161
11.4. Zusammenfassung	161
Literaturverzeichnis	163
Abbildungsverzeichnis	183
Listings	185
Tabellenverzeichnis	187
Definitionen	189
A. Grammatiken	191
B. Lebenslauf	199