

Ali Sunyaev

Health-Care Telematics in Germany

Design and Application
of a Security Analysis Method



A 261610

RESEARCH

Contents

List of Figures	xvii
List of Tables	xix
1 Introduction	1
1.1 Motivation	3
1.2 Objectives of the Thesis	6
1.3 Research Methodology	9
1.3.1 Design Science	10
1.3.2 Research Design	11
1.3.3 Design Theory	13
1.3.4 Theoretical Contribution and Research Outcome	14
1.4 Practical Implications, Users, and Beneficiaries	15
2 Healthcare Telematics in Germany with Respect to Security Issues	17
2.1 German Healthcare	17
2.1.1 Structure of German Healthcare	18
2.1.2 Characteristics of the German Healthcare Sector	19
2.1.2.1 Information Exchange and Distributed Information Flows in German Healthcare System	19
2.1.2.2 Current Problems	20
2.1.2.3 Specifics of the German Healthcare Domain	21
2.2 Information Systems in Healthcare	22
2.2.1 Seamless Healthcare	24
2.2.2 Interoperability, Standards and Standardization Approaches in Healthcare	24
2.2.2.1 Communication Standards	27
2.2.2.2 Documentations Standards and Standardization Approaches	31
2.2.3 Healthcare IS Architecture Types	33
2.2.3.1 Monolithic System	34
2.2.3.2 Heterogeneous System	35
2.2.3.3 Service-Oriented IS Architecture	35

2.2.4	Implications for Security Issues of Healthcare Information Systems	36
2.3	Healthcare Telematics	39
2.3.1	Definitions and Objectives of Healthcare Telematics	39
2.3.2	German Healthcare Telematics	42
2.3.2.1	Healthcare Telematics Infrastructure	42
2.3.2.2	Electronic Health Card	44
2.3.3	Risk and Security Issues of Healthcare Telematics	46
2.4	Summary	52
3	Catalogue of IS Healthcare Security Characteristics	53
3.1	Legal Framework	54
3.1.1	Privacy	54
3.1.2	Legal Requirements	55
3.2	Protection Goals	56
3.2.1	Dependable Healthcare Information Systems	57
3.2.2	Controllability of Healthcare Information Systems	59
3.3	Characteristics of IS Security Approaches with Respect to Healthcare	62
3.3.1	Literature Review	64
3.3.2	Overview of Healthcare IS Security Approach Characteristics	66
3.3.2.1	General IS Security Approach Characteristics	66
3.3.2.2	General IS Security Approach Characteristics with Reference to Healthcare	67
3.3.2.2.1	Type of the IS Security Approach	68
3.3.2.2.2	Common Characteristics	69
3.3.2.2.3	Methodology	73
3.3.2.2.4	Surrounding Conditions	76
3.3.2.3	Healthcare-Specific IS Security Approach Characteristics	77
3.4	Summary	81
4	Analysis of IS Security Analysis Approaches	83
4.1	Overview	83
4.2	Review of Literature	84
4.3	Existing Literature Reviews	87

4.4	Theoretical Background	91
4.5	Systematization of IS Security Analysis Approaches	93
4.5.1	Checklists	95
4.5.2	Assessment Approaches	96
4.5.2.1	Risk Assessment Approaches	96
4.5.2.2	Security Control Assessment Approaches	98
4.5.3	Risk Analysis Approaches	101
4.5.4	IT Security Management Approaches	102
4.5.4.1	The Plan-Do-Check-Act Approach of ISO 27001	104
4.5.4.2	Best Practice Models	105
4.5.5	Legislation Accommodations	106
4.6	Analysis of IS Security Analysis Approaches with Respect to Healthcare	108
4.6.1	Examination of IS Security Approaches with Respect to General IS Security Approach Characteristics	110
4.6.2	Examination of IS Security Approaches with Respect to General IS Security Approach Characteristics with Reference to Healthcare	111
4.6.3	Examination of IS Security Approaches with Respect to Healthcare Specific IS Security Approach Characteristics	113
4.7	Summary	114
5	Designing a Security Analysis Method for Healthcare Telematics in Germany	117
5.1	Introduction	117
5.2	Research Approach	118
5.3	Method Engineering	120
5.4	Description of Method Elements	121
5.4.1	Method Chains and Alliances	121
5.4.2	Method Fragments	122
5.4.3	Method Chunks	126
5.4.4	Method Components	126
5.4.5	Theoretical Background	127
5.5	Formal Description of the Concept of Method Engineering	128
5.6	HatSec Security Analysis Method	132

5.6.1	From Plan-Do-Check-Act Approach to a IS Security Analysis Method for Healthcare Telematics	133
5.6.2	Design of the HatSec Security Analysis Method	134
5.6.2.1	Method Blocks and Method Fragments	136
5.6.2.2	Overview of the Building Blocks of the HatSec Method	137
5.6.2.3	Perspectives of the HatSec Method	138
5.6.2.4	Context and Preparation of the Security Analysis	139
5.6.2.5	Security Analysis Process	143
5.6.2.6	Security Analysis Product	148
5.6.2.7	Two Sides of the HatSec Method	152
5.6.2.8	HatSec Structure	154
5.7	Review of the HatSec Security Analysis Method	161
5.8	Summary	165
6	Practical Application of the HatSec Method	167
6.1	Selected Case Studies	168
6.2	Assessment and Classification of Threats around the Electronic Health Card	169
6.2.1	Overview	170
6.2.2	Identification and Classification of the Attackers	171
6.2.3	Identification and Classification of the Attack Types	173
6.2.4	Summary	175
6.3	Analysis of the Applications of the Electronic Health Card	176
6.3.1	Overview	177
6.3.2	Data Acquisition	177
6.3.3	Process Analysis	178
6.3.3.1	Actual Process	178
6.3.3.2	Process Groups	180
6.3.3.3	Future Process with eHC	181
6.3.4	Patient Survey	183
6.3.4.1	Age Groups Analysis	184
6.3.4.2	Usage Groups Analysis	186
6.3.5	Summary	187

6.4	Analysis of a Proposed Solution for Managing Health Professional Cards in Hospitals Using a Single Sign-On Central Architecture	187
6.4.1	Overview	188
6.4.2	Induced Process Changes	189
6.4.2.1	General Changes	189
6.4.2.2	Discharge Letter Process.....	190
6.4.3	Existing Approaches for Managing Smart Cards in Hospitals.....	191
6.4.3.1	The Decentralized Approach	191
6.4.3.2	The VerSA Approach	191
6.4.3.3	Disadvantages	192
6.4.4	The Clinic Card Approach.....	192
6.4.4.1	Technical Architecture.....	193
6.4.4.2	Smart Card Management Unit	194
6.4.4.3	The Clinic Card and Card Middleware	194
6.4.4.4	Connector	195
6.4.4.5	Remote Access.....	195
6.4.4.6	Unique Characteristics of the Central Approach	196
6.4.4.7	Discharge Letter Process.....	197
6.4.5	Comparison of the Presented Approaches.....	198
6.4.5.1	Evaluation Framework.....	198
6.4.5.2	Hardware Requirements and Integration	198
6.4.5.3	Session Management	199
6.4.5.4	Usability	199
6.4.5.5	Further Value-Adding Aspects	200
6.4.6	Summary.....	200
6.5	Security Analysis of the German Electronic Health Card's Components on a Theoretical Level.....	201
6.5.1	Overview	201
6.5.2	Components and Documents Considered in this Security Analysis.....	202
6.5.2.1	Security Analysis of the Electronic Health Card's Components	203
6.5.2.1.1	Cross-Component Analysis	203
6.5.2.1.2	Key for the Combination of Medical and Administrative Data	203
6.5.2.1.3	Unauthorized Transfer of Medical Data.....	203
6.5.2.1.4	Missing Backup Method for Honoring Prescriptions.....	203
6.5.2.1.5	Possibility to Honor the Same Prescription Twice.....	204
6.5.2.1.6	Unassigned Assumption About the Security Implied by the Used "Zone-Concept"	204

6.5.2.1.7	Adjustment of Minimum Standards Happens Infrequently	204
6.5.2.1.8	<i>Inadequate Assumption About the Security of the Systems</i> Inside the Healthcare Telematics Infrastructure.....	205
6.5.2.1.9	Security by Obscurity.....	205
6.5.2.2	Analysis of the Connector.....	205
6.5.2.2.1	Imprecise Specification of the Blacklist Management.....	205
6.5.2.2.2	Imprecise Specification of the Trusted Viewer Interface.....	206
6.5.2.2.3	Security Issues Concerning the Communication with the Trusted Viewer	206
6.5.2.2.4	Security Issues Concerning the Communication with the Primary System	207
6.5.2.3	Analysis of the Primary System.....	208
6.5.2.3.1	Insufficient Classification of the Processed Data.....	208
6.5.2.3.2	Unassigned Assumption About the Presence of Security Measures Provided by Present Primary Systems	208
6.5.2.3.3	Analysis of the Card Reader.....	209
6.5.2.4	Additional Deficiencies Found During this Security Analysis.....	209
6.5.2.4.1	Missing Specification for Services to Manage eHC Data by the Insured	209
6.5.2.4.2	Missing Backup Processes for Essential Healthcare Telematics Processes.....	210
6.5.2.4.3	Possibility of Health Insurance Number Readout by Unauthorized Persons.....	210
6.5.2.4.4	Logs for SMC Access on the Primary System May Not Be Reliable.....	210
6.5.2.4.5	Problematic Assumptions about the Environment of the Medical Service Provider	211
6.5.2.4.6	Insider Attacks from Medical Service Provider's Personnel Not Considered in Threat Analysis	211
6.5.2.4.7	Potential for an Attack on the Medical Service Provider's LAN Considered As Too Low	211
6.5.2.4.8	Missing Best-Practices Recommendations for Software Keys	211
6.5.2.4.9	Missing Emergency Plans Regarding New Attacks on Components and Cryptographic Methods	212
6.5.3	Attack-Tree Analysis.....	212
6.5.4	Summary.....	212

6.6	Security Analysis of the German Electronic Health Card's Peripheral Parts in Practice.....	213
6.6.1	Overview	215
6.6.2	Laboratory's / Physician's Practice Configuration.....	215
6.6.3	Network Traffic Analyzes and its Consequences.....	217
6.6.4	Attacking the German Electronic Health Card.....	218
6.6.4.1	Permanent-Card-Ejection.....	220
6.6.4.2	Fill or Delete Prescriptions	220
6.6.4.3	Block a Card's PIN	221
6.6.4.4	Destroy a Card	222
6.6.4.5	Spy Personal Information	222
6.6.5	Summary.....	224
6.7	Case Studies: Lessons Learned	225
7	Appraisal of Results	227
7.1	Overview	227
7.2	Progress of Cognition.....	229
7.3	Design Proposals for Healthcare Telematics	230
	Bibliography	233
	Appendix	269