

Inhaltsverzeichnis

1	Einführung und Motivation	1
2	Fallstudien	7
2.1	Online-Kartenkauf am Beispiel bahn.de.....	9
2.1.1	Überblick.....	9
2.1.2	Geschäftsmodell.....	11
2.1.3	Kundensicht	12
2.1.4	Geschäftsvorgänge	13
2.1.5	Sicherheitsanforderungen.....	14
2.1.6	Testkonzept	24
2.2	ebay	24
2.2.1	Übersicht und Geschäftsmodell	25
2.2.2	Kundensicht	26
2.2.3	Spezielle Sicherheitsanforderungen	29
3	Sicherheitskonzepte und Analysen	33
3.1	Security Policies	33
3.2	Allgemeine Vorgehensweise	34
3.2.1	Risikoanalyse der Geschäftsvorgänge.....	35
3.2.2	Security Context.....	38
3.2.3	Basisarchitektur.....	40
3.2.4	Bedrohungsmodelle	42
3.3	Bedrohungsmodelle für bahn.de.....	44
3.3.1	Sicherheit auf Clientseite	45
3.3.2	Die Verantwortung des Servers	49
3.3.3	Kommunikation mit dem Kunden.....	50
3.4	Beispiel einer Sicherheitsanalyse im Embedded Control Bereich	52
3.4.1	Ausgangsszenario.....	53
3.4.2	Analyse des Ausgangsszenarios.....	55
3.4.3	Modifiziertes Szenario	59
3.5	„The People Problem“	61

4	Sicherheitsdienste	65
4.1	Authentifikation.....	65
4.1.1	Authentifikation durch Passwörter.....	66
4.1.2	Authentifikation durch Challenge-Response-Verfahren	68
4.1.3	Kontext-Weitergabe, Delegation und Impersonation.....	69
4.2	Vertraulichkeit.....	70
4.3	Integritätsschutz.....	70
4.4	Nicht-Abstreitbarkeit	71
4.5	Verfügbarkeit.....	71
4.6	Authorisierung.....	72
4.6.1	DAC – Discretionary Access Control	72
4.6.2	MAC – Mandatory Access Control.....	73
4.6.3	RBAC – Role Based Access Control	74
4.6.4	Multi-Level Security	75
5	Kryptografische Algorithmen.....	77
5.1	Allgemeines.....	77
5.2	Symmetrische Verschlüsselungsalgorithmen	79
5.2.1	DES und AES	79
5.2.2	Betriebsmodi für Blockchiffren	80
5.3	Hashfunktionen.....	81
5.3.1	Kollisionen.....	81
5.3.2	Schlüsselabhängige Hashfunktionen.....	83
5.3.3	Password-Based Encryption (PBE).....	84
5.4	Asymmetrische Algorithmen.....	85
5.4.1	RSA-Verfahren	85
5.4.2	Diffie-Hellman-Protokoll und diskrete Logarithmen.....	86
5.4.3	Digitale Signaturen	88
5.4.4	Performance-Fragen.....	89
5.5	Zertifikate	89
5.5.1	Zertifikate nach X.509	90
5.5.2	Attributzertifikate.....	92
5.5.3	Zurückziehen von Zertifikaten	93
5.5.4	Certificate Revocation List (CRL).....	94
5.5.5	Online Certificate Status Protocol (OCSP)	94
5.6	Authentifikationsprotokolle nach X.509.....	95
5.6.1	One-Pass Authentication	95
5.6.2	Three-Pass Authentication	96
5.6.3	Three Pass Mutual Authentication	97
5.7	Zufallswerte.....	98
5.7.1	Schlüsselerzeugung.....	98
5.7.2	Challenges.....	99
5.7.3	SessionIDs.....	99

- 5.8 Kryptografie mit Java 99
 - 5.8.1 Java Cryptography Architecture (JCA)..... 100
 - 5.8.2 Symmetrische Verschlüsselung 101
 - 5.8.3 Hashfunktionen und MACs..... 102
 - 5.8.4 Asymmetrische Kryptografie 102
 - 5.8.5 Zertifikate..... 103
 - 5.8.6 Erzeugung von Zufallszahlen..... 103
- 5.9 Übersicht 104

- 6 Sicherheit in Verteilten Systemen..... 105**
 - 6.1 Lokale versus verteilte Sicherheit..... 106
 - 6.2 Authentisierung in verteilten Systemen..... 107
 - 6.2.1 Authentisierung versus Identifizierung 107
 - 6.2.2 Authentisierung mit Passwörtern 109
 - 6.2.3 Software-Architektur der Authentisierung
mit Passwörtern..... 115
 - 6.3 Delegation und Impersonation..... 120
 - 6.3.1 Begriffsklärung 120
 - 6.3.2 Delegation von Aufträgen..... 123

- 7 Basisprotokolle..... 127**
 - 7.1 http Authentication 127
 - 7.1.1 Basic Authentication 128
 - 7.1.2 Digest Authentication 128
 - 7.2 Kerberos 129
 - 7.2.1 Funktionsweise 129
 - 7.2.2 Principals und Domänen 132
 - 7.2.3 Attacken auf Kerberos 133
 - 7.2.4 Delegation mit Kerberos 134
 - 7.2.5 Cross-Domain-Authentisierung 136
 - 7.2.6 Kerberos Erweiterungen 137
 - 7.2.7 Microsoft Passport 138
 - 7.3 SSL/TLS..... 139
 - 7.3.1 Aufbau von SSL..... 140
 - 7.3.2 Handshake..... 142
 - 7.3.3 Ciphersuites..... 145
 - 7.3.4 Performanzfragen..... 148
 - 7.3.5 SSL Security 150
 - 7.3.6 Zusammenfassung..... 152

- 8 Authentication Frameworks 155**
 - 8.1 GSS-API..... 155
 - 8.1.1 Überblick..... 156
 - 8.1.2 Ein Beispiel..... 157

8.1.3	GSS-API Mechanismen	158
8.1.4	Simple and Protected Negotiation Mechanism (SPNEGO)	159
8.1.5	Delegation in GSS-API	160
8.2	SASL	161
8.2.1	Funktionsweise	162
8.2.2	SASL Mechanismen	162
8.3	Zusammenfassung und Bewertung	163
9	Middleware Security	165
9.1	CORBA	165
9.1.1	SECIOP und SSLIOP	166
9.1.2	CSIV2 und SAS	167
9.2	Remote Method Invocation (RMI)	170
9.3	.NET	171
9.3.1	Allgemeines	171
9.3.2	Code Access Security (CAS)	172
9.3.3	Role Based Security (RAS)	174
9.4	Simple Object Access Protocol (SOAP)	175
9.4.1	Allgemeines	175
9.4.2	SOAP Security	176
10	Content-Level Security	179
10.1	Aktuelle Trends	180
10.2	Architektur und Infrastruktur	181
10.2.1	Infrastruktur	182
10.2.2	CMS Sicherheitsarchitektur	185
10.2.3	Abbildung der Berechtigungen auf das Sicherheitsmodell der Firma	188
10.2.4	Rollenmodellierung am Beispiel Portal Access Control	192
10.2.5	Benutzer-Berechtigungs-Systeme (BBS)	196
10.2.6	Geschäftsprozesse: Workflow und Realität	203
10.2.7	Zugriffskontrolle beim Endnutzer	207
10.3	Spezielle Probleme von Content Security	210
10.3.1	Records Management	210
10.3.2	Mobile Dokumente	211
10.3.3	Multi-Level Security (MLS)	213
10.3.4	Enterprise Search Engine Security	216
11	Sicherheit der Infrastruktur	225
11.1	Absicherung der Infrastruktur durch Firewalls und DMZs	226
11.1.1	Firewall-Architekturen	227
11.1.2	Reverse Proxy als Point-of-Contact	231
11.1.3	Beispiel Nevis Web	234

- 11.1.4 Gegenseitige Authentisierung von Komponenten und Knoten..... 238
- 11.1.5 Applikationsdesign für zentrale Firewall-Umgebungen 241
- 11.1.6 Sessionkonzept..... 242
- 11.2 Verkleinerung der Angriffsfläche..... 248
 - 11.2.1 Maßnahmen..... 248
 - 11.2.2 Ein Beispiel aus der Praxis..... 253
- 11.3 Single-Sign-On für Portale 261
 - 11.3.1 Vorstellung einer Portallösung mit Weitergabe der Identität..... 261
 - 11.3.2 Aufgaben der Autoritäten..... 263
 - 11.3.3 Heuristiken für Softwareentwickler 265
 - 11.3.4 Das Firmenportal 266
 - 11.3.5 Integration vorhandener Legacy Systeme 267
 - 11.3.6 Ausbau des Security Contexts..... 270
 - 11.3.7 Step-Up Authentication..... 270
 - 11.3.8 Sicherheitsanmerkungen zu Single-Sign-On..... 270
- 11.4 Mobile Infrastruktur 271

- 12 Föderative Sicherheit..... 275**
 - 12.1 Föderatives Identitätsmanagement 276
 - 12.2 Föderatives Trust Management 278
 - 12.3 Föderative Sicherheit am Beispiel eines Portals..... 281
 - 12.3.1 Physische Architektur 282
 - 12.3.2 Einfacher föderativer Web-SSO zwischen Domänen 283
 - 12.4 Standards für föderatives Identitätsmanagement..... 290
 - 12.4.1 SAML 291
 - 12.4.2 Liberty Alliance 293
 - 12.4.3 Web Services Federation 294
 - 12.5 Sicherheitsanalyse 296

- 13 Schlussbetrachtungen..... 301**

- Abkürzungsverzeichnis 303**

- Literaturverzeichnis 305**

- Index 309**