

Contents

Foreword	xi
Preface	xiii
Acknowledgements	xix
Chapter 1 Introduction to Embedded Systems Security	1
1.1 What is Security?.....	1
1.2 What is an Embedded System?.....	2
1.3 Embedded Security Trends.....	4
1.3.1 Embedded Systems Complexity	4
1.3.2 Network Connectivity	12
1.3.3 Reliance on Embedded Systems for Critical Infrastructure.....	14
1.3.4 Sophisticated Attackers.....	15
1.3.5 Processor Consolidation.....	16
1.4 Security Policies	18
1.4.1 Perfect Security	18
1.4.2 Confidentiality, Integrity, and Availability	18
1.4.3 Isolation.....	19
1.4.4 Information Flow Control.....	20
1.4.5 Physical Security Policies.....	21
1.4.6 Application-Specific Policies.....	21
1.5 Security Threats.....	22
1.5.1 Case Study: VxWorks Debug Port Vulnerability	22
1.6 Wrap-up	23
1.7 Key Points.....	23
1.8 Bibliography and Notes.....	24
Chapter 2 Systems Software Considerations.....	25
2.1 The Role of the Operating System.....	26
2.2 Multiple Independent Levels of Security.....	27
2.2.1 Information Flow.....	27
2.2.2 Data Isolation	27
2.2.3 Damage Limitation	28
2.2.4 Periods Processing	28

2.2.5	Always Invoked.....	29
2.2.6	Tamper Proof.....	29
2.2.7	Evaluable.....	29
2.3	Microkernel versus Monolith.....	31
2.3.1	Case Study: The Duqu Virus.....	34
2.4	Core Embedded Operating System Security Requirements.....	34
2.4.1	Memory Protection.....	34
2.4.2	Virtual Memory.....	35
2.4.3	Fault Recovery.....	37
2.4.4	Guaranteed Resources.....	38
2.4.5	Virtual Device Drivers.....	41
2.4.6	Impact of Determinism.....	42
2.4.7	Secure Scheduling.....	45
2.5	Access Control and Capabilities.....	46
2.5.1	Case Study: Secure Web Browser.....	47
2.5.2	Granularity versus Simplicity of Access Controls.....	49
2.5.3	Whitelists versus Blacklists.....	51
2.5.4	Confused Deputy Problem.....	53
2.5.5	Capabilities versus Access Control Lists.....	53
2.5.6	Capability Confinement and Revocation.....	58
2.5.7	Secure Design Using Capabilities.....	60
2.6	Hypervisors and System Virtualization.....	61
2.6.1	Introduction to System Virtualization.....	64
2.6.2	Applications of System Virtualization.....	65
2.6.3	Environment Sandboxing.....	65
2.6.4	Virtual Security Appliances.....	65
2.6.5	Hypervisor Architectures.....	66
2.6.6	Paravirtualization.....	69
2.6.7	Leveraging Hardware Assists for Virtualization.....	70
2.6.8	Hypervisor Security.....	73
2.7	I/O Virtualization.....	74
2.7.1	The Need for Shared I/O.....	75
2.7.2	Emulation.....	75
2.7.3	Pass-through.....	76
2.7.4	Shared IOMMU.....	78
2.7.5	IOMMUs and Virtual Device Drivers.....	78
2.7.6	Secure I/O Virtualization within Microkernels.....	79
2.8	Remote Management.....	80
2.8.1	Security Implications.....	81
2.9	Assuring Integrity of the TCB.....	83
2.9.1	Trusted Hardware and Supply Chain.....	83
2.9.2	Secure Boot.....	84
2.9.3	Static versus Dynamic Root of Trust.....	84
2.9.4	Remote Attestation.....	87

2.10 Key Points.....	88
2.11 Bibliography and Notes.....	90
Chapter 3 Secure Embedded Software Development	93
3.1 Introduction to PHASE—Principles of High-Assurance Software Engineering.....	94
3.2 Minimal Implementation.....	95
3.3 Component Architecture.....	96
3.3.1 Runtime Componentization	98
3.3.2 A Note on Processes versus Threads.....	99
3.4 Least Privilege	100
3.5 Secure Development Process	100
3.5.1 Change Management.....	101
3.5.2 Peer Reviews	101
3.5.3 Development Tool Security	104
3.5.4 Secure Coding	107
3.5.5 Software Testing and Verification.....	146
3.5.6 Development Process Efficiency	154
3.6 Independent Expert Validation	156
3.6.1 Common Criteria.....	157
3.6.2 Case Study: Operating System Protection Profiles	160
3.7 Case Study: HAWS—High-Assurance Web Server	165
3.7.1 Minimal Implementation.....	166
3.7.2 Component Architecture	168
3.7.3 Least Privilege.....	168
3.7.4 Secure Development Process	169
3.7.5 Independent Expert Validation.....	169
3.8 Model-Driven Design	169
3.8.1 Introduction to MDD	170
3.8.2 Executable Models	174
3.8.3 Modeling Languages.....	177
3.8.4 Types of MDD Platforms.....	182
3.8.5 Case Study: A Digital Pathology Scanner.....	183
3.8.6 Selecting an MDD Platform	191
3.8.7 Using MDD in Safety- and Security-Critical Systems	201
3.9 Key Points.....	202
3.10 Bibliography and Notes.....	206
Chapter 4 Embedded Cryptography.....	209
4.1 Introduction.....	210
4.2 U.S. Government Cryptographic Guidance	211
4.2.1 NSA Suite B.....	212
4.3 The One-Time Pad.....	213
4.3.1 Cryptographic Synchronization	222

4.4	Cryptographic Modes	224
4.4.1	Output Feedback	224
4.4.2	Cipher Feedback	225
4.4.3	OFB with CFB Protection	226
4.4.4	Traffic Flow Security	227
4.4.5	Counter Mode	227
4.5	Block Ciphers	228
4.5.1	Additional Cryptographic Block Cipher Modes	231
4.6	Authenticated Encryption	232
4.6.1	CCM	233
4.6.2	Galois Counter Mode	233
4.7	Public Key Cryptography	233
4.7.1	RSA	236
4.7.2	Equivalent Key Strength	236
4.7.3	Trapdoor Construction	238
4.8	Key Agreement	239
4.8.1	Man-in-the-Middle Attack on Diffie-Hellman	241
4.9	Public Key Authentication	241
4.9.1	Certificate Types	242
4.10	Elliptic Curve Cryptography	244
4.10.1	Elliptic Curve Digital Signatures	245
4.10.2	Elliptic Curve Anonymous Key Agreement	245
4.11	Cryptographic Hashes	245
4.11.1	Secure Hash Algorithm	246
4.11.2	MMO	247
4.12	Message Authentication Codes	248
4.13	Random Number Generation	248
4.13.1	True Random Number Generation	249
4.13.2	Pseudo-Random Number Generation	254
4.14	Key Management for Embedded Systems	256
4.14.1	Case Study: The Walker Spy Case	257
4.14.2	Key Management—Generalized Model	258
4.14.3	Key Management Case Studies	264
4.15	Cryptographic Certifications	277
4.15.1	FIPS 140-2 Certification	277
4.15.2	NSA Certification	280
4.16	Key Points	285
4.17	Bibliography and Notes	287
Chapter 5 Data Protection Protocols for Embedded Systems		289
5.1	Introduction	290
5.2	Data-in-Motion Protocols	291
5.2.1	Generalized Model	291
5.2.2	Choosing the Network Layer for Security	296

5.2.3	Ethernet Security Protocols	297
5.2.4	IPsec versus SSL	301
5.2.5	IPsec	303
5.2.6	SSL/TLS	310
5.2.7	Embedded VPN Clients	313
5.2.8	DTLS	315
5.2.9	SSH	315
5.2.10	Custom Network Security Protocols	316
5.2.11	Application of Cryptography within Network Security Protocols	319
5.2.12	Secure Multimedia Protocols	320
5.2.13	Broadcast Security	324
5.3	Data-at-Rest Protocols	330
5.3.1	Choosing the Storage Layer for Security	332
5.3.2	Symmetric Encryption Algorithm Selection	334
5.3.3	Managing the Storage Encryption Key	338
5.3.4	Advanced Threats to Data Encryption Solutions	340
5.4	Key Points	342
5.5	Bibliography and Notes	345
Chapter 6	Emerging Applications	349
6.1	Embedded Network Transactions	350
6.1.1	Anatomy of a Network Transaction	351
6.1.2	State of Insecurity	351
6.1.3	Network-based Transaction Threats	352
6.1.4	Modern Attempts to Improve Network Transaction Security	355
6.1.5	Trustworthy Embedded Transaction Architecture	362
6.2	Automotive Security	366
6.2.1	Vehicular Security Threats and Mitigations	366
6.3	Secure Android	369
6.3.1	Android Security Retrospective	369
6.3.2	Android Device Rooting	371
6.3.3	Mobile Phone Data Protection: A Case Study of Defense-in-Depth	372
6.3.4	Android Sandboxing Approaches	373
6.4	Next-Generation Software-Defined Radio	380
6.4.1	Red-Black Separation	380
6.4.2	Software-Defined Radio Architecture	381
6.4.3	Enter Linux	382
6.4.4	Multi-Domain Radio	383
6.5	Key Points	385
6.6	Bibliography and Notes	386
Index	389	