

Inhaltsverzeichnis

| | | |
|----------|---|----|
| 1 | Einleitung | 1 |
| 1.1 | Motivation | 1 |
| 1.2 | Ziele des Buches | 2 |
| 1.3 | Gliederung des Buches | 3 |
| 2 | Grundlagen | 5 |
| 2.1 | CPU-Ringe | 5 |
| 2.2 | Verwendung der CPU-Ringe | 7 |
| 2.3 | Virtualisierung und die CPU-Ringe | 8 |
| 2.4 | Zero-Knowledge-Beweis | 10 |
| 2.5 | Clark-Wilson-Integritätsmodell | 11 |
| 3 | Trusted Computing | 13 |
| 3.1 | Definition des Begriffs „Trusted Computing“ | 14 |
| 3.2 | Ziele des Trusted Computing | 16 |
| 3.3 | Das Trusted Computing System (TCS) | 19 |
| 3.3.1 | Die Trusted Computing Platform (TCP) | 21 |
| 3.3.2 | Das Trusted Operating System (TOS) | 21 |
| 3.3.3 | Die Trusted Computing Base (TCB) | 21 |
| 3.4 | Trusted Computing und Secure Computing | 22 |
| 4 | Die TCP der Trusted Computing Group | 25 |
| 4.1 | PC-Referenzarchitektur | 26 |
| 4.2 | Trusted Building Block (TBB) | 27 |
| 4.2.1 | Root of Trust for Measurement (RTM) | 28 |
| 4.2.2 | Root of Trust for Reporting (RTR) | 28 |
| 4.2.3 | Root of Trust for Storage (RTS) | 29 |
| 4.3 | Das Trusted Platform Module (TPM) | 29 |
| 4.3.1 | TPM-Einheiten | 31 |
| 4.3.2 | TPM-Zugriffskontrolle und Kommunikationsprotokoll | 37 |
| 4.3.3 | TPM-Initialisierung | 40 |

| | | |
|----------|---|-----------|
| 4.3.4 | Betriebszustände des TPM (Opt-In) | 41 |
| 4.3.5 | Erweiterte TPM-Konfiguration (Opt-In) | 43 |
| 4.3.6 | TPM-Eigentümer einrichten und entfernen | 44 |
| 4.3.7 | TPM-Schlüsseltypen und Schlüsselverwaltung | 46 |
| 4.3.8 | TPM-Selbstschutzmaßnahmen (Tamper-Resistant) | 50 |
| 4.4 | Sicherheitsfunktionen der TCP | 51 |
| 4.4.1 | Integrity Measurement, Storage and Reporting | 51 |
| 4.4.2 | Initialisierung der Chain of Trust | 52 |
| 4.4.3 | Remote Attestation | 55 |
| 4.4.4 | Kryptographische Operationen | 56 |
| 4.5 | Identität der TCP und entstehende Datenschutzprobleme | 57 |
| 4.5.1 | Erzeugung eines Attestation-Identity-Zertifikats | 58 |
| 4.5.2 | Direct Anonymous Attestation (DAA) | 60 |
| 4.5.3 | Löschen des Endorsement Key | 60 |
| 4.5.4 | Deaktivieren des TPM | 61 |
| 4.6 | Plattform-Zertifikate (Platform Credentials) | 61 |
| 4.7 | Probleme und Einschränkungen der TCP | 63 |
| 5 | Erweiterungen und Alternativen zur TCG | 65 |
| 5.1 | Intel Trusted Execution Technology (TXT) | 65 |
| 5.2 | AMD Presidio Technology | 68 |
| 5.3 | IBM SecureBlue | 69 |
| 6 | Anforderungen an vertrauenswürdige Betriebssysteme | 71 |
| 6.1 | Dynamic Chain of Trust (Integrity Measurement) | 71 |
| 6.2 | Dynamic Chain of Trust (Integrity Protection) | 72 |
| 6.3 | Bewertung der Systemintegrität (Integrity Validation) | 73 |
| 6.4 | Remote Attestation (Remote Integrity Validation) | 74 |
| 6.5 | Trusted Software Stack | 75 |
| 6.5.1 | TPM Device Driver | 76 |
| 6.5.2 | TCG Device Driver Library (TDDL/TDDLI) | 76 |
| 6.5.3 | TSS Core Services (TCS/TCSI) | 77 |
| 6.5.4 | TCG Service Provider (TSP/TSPI) | 77 |
| 6.5.5 | Einsatzszenarien des TSS | 78 |
| 6.6 | Protected Execution | 79 |
| 6.7 | Trusted-GUI und Trusted Input/Output | 80 |
| 7 | Trusted-Computing-Infrastruktur | 83 |
| 7.1 | Public Key Infrastructure (PKI) | 84 |
| 7.1.1 | Ausstellung der Plattform-Zertifikate | 84 |
| 7.1.2 | Ausstellung der AIK-Zertifikate | 85 |
| 7.1.3 | Verwendung der AIK-Zertifikate | 86 |
| 7.1.4 | Zusammenfassung | 88 |
| 7.2 | Certificate-Management-Protokoll | 89 |
| 7.3 | Remote-Attestation-Protokoll | 89 |

| | | |
|-----------|---|-----|
| 8 | Theoretische und praktische Lösungsansätze | 91 |
| 8.1 | Integrity Measurement und Integrity Protection | 91 |
| 8.1.1 | AEGIS | 91 |
| 8.1.2 | SEBOS | 92 |
| 8.1.3 | Copilot | 93 |
| 8.1.4 | <i>Trusted Grub</i> | 94 |
| 8.1.5 | IBM Integrity Measurement Architecture (IMA) | 95 |
| 8.1.6 | BIND – Binding Instructions and Data | 98 |
| 8.2 | Remote Attestation | 100 |
| 8.2.1 | Trusted Network Connect (TNC) | 100 |
| 8.2.2 | Microsoft Network Access Protection (NAP) | 102 |
| 8.2.3 | Cisco Network Admission Control (NAC) | 103 |
| 8.2.4 | Property-Based Attestation | 104 |
| 8.2.5 | WS-Attestation | 105 |
| 8.2.6 | Sicherheit des Attestation-Protokolls | 108 |
| 8.3 | Trusted Software Stack (TSS) | 110 |
| 8.3.1 | TrouSerS | 110 |
| 8.3.2 | Trusted Java | 111 |
| 8.3.3 | TPM/J | 111 |
| 8.4 | Protected Execution | 111 |
| 8.4.1 | Terra Architecture | 113 |
| 8.4.2 | Nizza Architecture | 115 |
| 8.4.3 | Perseus Architecture | 118 |
| 8.4.4 | Xen-Hypervisor-Erweiterungen | 120 |
| 8.5 | Trusted Graphical User Interface (Trusted-GUI) | 122 |
| 8.5.1 | Dynamic Security Skins | 122 |
| 8.5.2 | Nitpicker – Overlay Window Management | 123 |
| 9 | Trusted-Computing-Systeme | 127 |
| 9.1 | European Multilaterally Secure Computing Base | 127 |
| 9.2 | Open Trusted Computing | 128 |
| 9.3 | Intel Virtual Appliances/RedHat Embedded IT Software (EIT) | 128 |
| 10 | Fazit | 131 |
| 11 | Trusted Computing mit Windows Vista | 133 |
| 11.1 | Die Geschichte von Windows Vista | 134 |
| 11.2 | Sicherheitsfunktionen in Windows Vista | 135 |
| 11.3 | Windows Vista TPM Support | 136 |
| 11.4 | Secure Startup und Full Volume Encryption (FVE) – BitLocker | 137 |
| 11.5 | Kernel Integrity Checks/Driver Signing (nur 64-Bit-Versionen) | 140 |
| 11.6 | Windows Resource Protection (WRP) | 143 |
| 11.7 | PatchGuard (nur 64-Bit-Versionen) | 144 |
| 11.8 | User Account Control | 144 |
| 11.8.1 | User Account Protection (UAP) | 145 |

- 11.8.2 Mandatory Integrity Control (MIC) 147
- 11.8.3 Secure Desktop (Trusted Path) 148
- 11.8.4 UI Privilege Isolation (UIPI) 150
- 11.9 Windows Service Hardening 150
- 11.10 Zusammenfassung und Schlussfolgerung 151
- Literaturverzeichnis 153

- Sachverzeichnis** 159