

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Einführung | 1 |
| 2 | TCP/IP-Grundlagen für das Tunneling | 5 |
| 2.1 | Einleitung | 5 |
| 2.2 | Einige Worte zum OSI-Modell | 9 |
| 2.3 | Die wichtigen Protokolle | 10 |
| 2.4 | Link Layer: ARP | 10 |
| 2.5 | Internet Layer: IPv4 | 12 |
| 2.6 | Internet Layer: ICMPv4 | 15 |
| 2.7 | Internet Layer: IGMP | 19 |
| 2.8 | Internet Layer: IPv6 | 20 |
| 2.9 | Internet Layer: ICMPv6 | 23 |
| 2.10 | Transport Layer: UDP | 25 |
| 2.11 | Transport Layer: TCP | 26 |
| 2.12 | Application Layer: HTTP | 34 |
| 2.13 | Application Layer: Domain Name System | 37 |
| 3 | Tunneling-Protokolle | 43 |
| 3.1 | Serial Line Internet Protocol (SLIP) | 43 |
| 3.2 | Das Point-to-Point-Protokoll (PPP) | 44 |
| 3.3 | Layer 2 Tunneling Protocol (L2TP) | 47 |
| 3.4 | Dual Stacks und IPv6 over IPv4 gemäß RFC 4213 | 53 |
| 3.5 | IPIP und IP-in-IP | 55 |
| 3.6 | Generic Packet Tunneling bei IPv6 | 56 |
| 3.7 | Teredo | 57 |
| 3.8 | General Routing Encapsulation (GRE) | 59 |
| 3.9 | IPSec | 61 |
| 3.10 | Point-to-Point Tunneling Protocol (PPTP) | 65 |
| 3.11 | SOCKS | 68 |
| 3.12 | Tunneling im Bereich der Gebäudeautomatisierung | 70 |
| 3.13 | Sicherheitsaspekte von regulären Tunneln | 72 |
| 4 | Geheimes Tunneling | 75 |
| 4.1 | Geheimes Tunneling im LAN | 75 |
| 4.2 | Geheimes Tunneling auf dem Internet Layer | 76 |
| 4.3 | Geheimes Tunneling über ICMP | 77 |
| 4.4 | Geheimes Tunneling über TCP und UDP | 78 |

| | | |
|----------|---|------------|
| 4.5 | Geheimes Tunneling über Plaintext-Protokolle | 79 |
| 4.6 | Protocol Hopping Covert Channels | 81 |
| 4.7 | Protocol Channels | 84 |
| 5 | Grundlagen verdeckter Kanäle | 95 |
| 5.1 | Was ist ein verdeckter Kanal? | 95 |
| 5.2 | Anwendungsgebiete verdeckter Netzwerkkanäle | 96 |
| 5.3 | Abgrenzung zu Seitenkanal-Angriffen | 97 |
| 5.4 | Arten verdeckter Kommunikationskanäle | 98 |
| 5.5 | Non-interference: Verdeckte Kanäle im MLS-Kontext | 101 |
| 5.6 | Umgang mit verdeckten Kanälen | 102 |
| 6 | Prävention und Detektion verdeckter Kanäle | 103 |
| 6.1 | Shared Resource Matrix Methodology | 103 |
| 6.2 | Covert Flow Trees | 107 |
| 6.3 | Code-Modifikationen nach Agat | 112 |
| 6.4 | ACK-Filter | 114 |
| 6.5 | Store And Forward Protocol (SAFP) | 115 |
| 6.6 | Die Pump | 116 |
| 6.7 | Einweg-Links (Blind Write-Up) | 117 |
| 6.8 | Upwards Channel | 118 |
| 6.9 | Quantized Pump | 118 |
| 6.10 | Spurious Processes Approach | 120 |
| 6.11 | Fuzzy Time zur Einschränkung von Timing Channels in VMs | 124 |
| 6.12 | Paketnormalisierung | 126 |
| 6.13 | Drei Verfahren zur Zeitkanal-Detektion nach Cabuk et al. | 131 |
| 6.14 | Zeitkanal-Detektion nach Zander | 135 |
| 6.15 | Zeitkanal-Detektion nach Berk et al. | 138 |
| 6.16 | Detektion in Geschäftsprozessen | 140 |
| 6.17 | Früherkennung in VoIP-Kommunikation | 142 |
| 6.18 | Detektion von ISN-basierten Covert Channels | 142 |
| 7 | Fortgeschrittene Themen für verdeckte Kanäle | 145 |
| 7.1 | Übersicht | 145 |
| 7.2 | Optimierte Speichernutzung für PHCC | 145 |
| 7.3 | Protokollwechsel und Forwarding optimieren | 148 |
| 7.4 | Das Normalisierungsproblem der NEL-Phase | 149 |
| 7.5 | Limitierung von Protokoll-wechselnden Kanälen | 154 |
| 7.6 | Verdeckte Kanäle in der Gebäudeautomation | 159 |
| | Anhang | 163 |
| | Literaturverzeichnis | 165 |
| | Sachverzeichnis | 175 |

<http://www.springer.com/978-3-8348-1640-5>

Tunnel und verdeckte Kanäle im Netz
Grundlagen, Protokolle, Sicherheit und Methoden
Wendzel, S.
2012, VIII, 179 S. 57 Abb., Softcover
ISBN: 978-3-8348-1640-5