Vorwort

Für die hier vorliegende 4. Auflage wurde das Buch grundlegend überarbeitet. Die Reihenfolge der Kapitel wurde an die in Vorlesungen zu Computernetzen übliche angepasst: Zunächst werden Sicherheitstechnologien der unteren Netzwerkschichten eingeführt, um dann das TCP/IP-Schichtenmodell nach oben hin zu durchlaufen. Dies ist auch deshalb sinnvoll, weil Sicherheitsmechanismen auf der Anwendungsebene of „darunter“ liegende Protokolle nutzen. So beruht z.B. die Sicherheit von Single-Sign-On-Protokolle und die Sicherheit von Webanwendungen ganz wesentlich auf den Eigenschaften des SSL/TLS-Protokolls, das daher vorher erläutert werden muss.

Alle Kapitel wurden erweitert und aktualisiert, der Umfang der behandelten Technologien wurde erheblich ausgeweitet. In Kapitel 2 werden EAP-Protokolle und PPTPv2 vorgestellt. Kapitel 3.2 wurde um Abschnitte zu WEP, RC4, WPA, IEEE 802.1X und IEEE 802.11i erweitert. In Kapitel 5 wurde der Abschnitt zu NAT Traversal hinzugefügt. Das zentrale Thema SSL/TLS wurde um Abschnitte zu neuen Angriffen und zu neuen formalen Analysen ergänzt. In einem neuen Kapitel zur Sicherheit von Webanwendungen werden deren Bausteine (HTTP und HTML 5) erläutert, klassische Webangriffe (XSS, CSRF, SQLi) beschrieben, und als wichtiger Sonderfall Single-Sign-On-Protokolle behandelt.

Auch die behandelten, praktisch relevanten Angriffsszenarien wurden erweitert: Die Neuauflage behschreibt erstmals Padding Oracle-Angriffe auf Blockchiffren im CBC-Modus (Abschnitt 1.7.2), Wörterbuchangriffe (Abschnitt 2.5.1), der Angriff auf WEP (Abschnitt 3.3.4), Angriffe auf IPSec (Abschnitt 5.7), neue Angriffe auf SSL/TLS (Abschnitt 7.10) und, wie schon oben erwähnt, klassische Angriffe auf Webanwendungen.

Ziel war es auch, die Abhängigkeiten verschiedener Bereiche voneinander klarer darzustellen. Als Beispiel seien hier die EAP-Protokolle genannt: Sie wurden erstmals im Zusammenhang mit PPP genannt (Abschnitt 2.7), werden heute hauptsächlich im WLAN-Bereich eingesetzt (Abschnitt 3.5), und verwenden Mobilfunk- und SSL-Technologien (Abschnitte 4.3, 7.7).

Diese Neuauflage wurde unterstützt durch den Wettbewerb „Aufstieg durch Bildung“ des Bundesministeriums für Bildung und Forschung (BMBF). Hier wurden im Rahmen des Projekts „Open Competence Center for Cyber Security“ die Module Netzsicherheit 1 und 2 entwickelt, deren Stoffumfang durch dieses Buch abgedeckt wird.

Bedanken möchte ich mich bei den Probelesern der einzelnen Kapitel, die mitgeholfen haben, die Anzahl der Druckfehler zu minimieren: Florian Feldmann, Dennis Felsch, Matthias Horst, Tibor Jager, Christian Mainka, Vladislav Mladenov und Marcus Niemietz. Ein ganz besonderer Dank geht an Christoph Bader und Florian Bergsma, die mich inhaltlich und bei allen Fragen rund um LaTeX unterstützt haben.

Bochum im Juni 2014

Jörg Schwenk

http://www.springer.com/978-3-658-06543-0

Sicherheit und Kryptographie im Internet
Theorie und Praxis
Schwenk, J.
2014, XV, 351 S. 211 Abb., Softcover
ISBN: 978-3-658-06543-0