Günter Schäfer · Michael Roßberg

Netzsicherheit

- Grundlagen & Protokolle
- Mobile & drahtlose Kommunikation
- Schutz von Kommunikationsinfrastrukturen

2., aktualisierte und erweiterte Auflage

dpunkt.verlag

Prof. Dr.-Ing. Günter Schäfer
guenter.schaefer@tu-ilmenau.de

Dr.-Ing. Michael Roßberg
michael.rossberg@tu-ilmenau.de

Lektorat: Dr. Michael Barabas
Copy Editing: Ursula Zimpfer, Herrenberg
Satz: Dr.-Ing. Michael Roßberg, Illmenau
Herstellung: Frank Heidt
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN
Buch 978-3-86490-115-7
PDF 978-3-86491-547-5
ePub 978-3-86491-548-2

2., aktualisierte und erweiterte Auflage

Wieblinger Weg 17
69123 Heidelberg

5 4 3 2 1 0

Vorwort zur zweiten Auflage

Seit dem Erscheinen der ersten Auflage dieses Buches sind elf Jahre vergangen, in denen sich ebenso zahlreiche wie vielfältige Entwicklungen auf dem Gebiet der Netzsicherheit vollzogen haben. Tatsächlich ist die Zahl der Neuerungen so umfangreich, dass wir uns entschieden haben, die zweite Auflage dieses Buches als Autorenteam vorzubereiten, sodass das Buch nun von Herrn Michael Roßberg und mir gemeinsam gepflegt wird.

Dabei ist zum einen eine gründliche Überarbeitung und Ergänzung der in den einzelnen Kapiteln vermittelten Inhalte erforderlich geworden, die in der vorliegenden zweiten Auflage umfassend aktualisiert wurden. So wurden zahlreiche Entwicklungen im Bereich der Kryptografie aufgenommen, wobei diese sowohl neue Angriffe auf bereits in der ersten Auflage enthaltene kryptografische Algorithmen und Protokolle als auch neue Verfahren betreffen. Hierbei wurden einige in der Vergangenheit sehr wichtige Verfahren, wie DES und MD5, die heute als nicht mehr ausreichend sicher und damit als obsolet gelten, nicht gestrichen, da man an ihrem Beispiel nach wie vor wichtige Sachverhalte gut erklären und nachvollziehen kann. Das Kapitel über asymmetrische Kryptografie wurde um eine elementare Einführung in die Kryptografie auf Grundlage elliptischer Kurven ergänzt, da diese aufgrund der mathematischen Fortschritte bei der Berechnung diskreter Logarithmen von Ganzzahlen in der Praxis eine immer wichtigere Rolle spielt. Das in der ersten Auflage enthaltene Kapitel über mobile Internetkommunikation, in dem die Mobilitätsunterstützung auf Netzwerkschicht mittels Mobile IP und unterstützenden Protokollen für Authentisierung, Autorisierung und Accounting beschrieben wurde, haben wir gestrichen, da Mobile IP in den vergangenen zehn Jahren außer in geschlossenen Umgebungen keine nennenswerte praktische Akzeptanz erfahren hat.

Zum anderen wurde das Buch um einen neuen Teil ergänzt, der den Schutz von Kommunikationsinfrastrukturen vor gezielten Angriffen auf ihre Integrität und Verfügbarkeit in den Mittelpunkt des Interesses rückt. In diesen Teil wurde aus naheliegenden Gründen auch das bereits in der ersten Auflage enthaltene Kapitel über Internet-Firewalls integriert.

In der resultierenden Form eignet sich das Buch gut als Grundlage für zwei oder drei aufeinander aufbauende beziehungsweise teilweise auch unabhängig voneinander zu belegende Vorlesungen. Eine dreistufige Aufteilung könnte beispielsweise die Grundlagen der Datensicherheitstechnik (Teil 1) in einer ersten Vorlesung, ihre Anwendung in Netzen (Teile 2 und 3) in einer zweiten Vorlesung und den Schutz von Kommunikationsinfrastrukturen in einer dritten Vorlesung behandeln, wobei letztere unter Rückgriff auf einige zentrale Grundlagen aus dem ersten Teil auch unabhängig von den anderen belegt werden kann. Eine zweistufige Aufteilung würde die essenziellen Abschnitte des ersten Teils gemeinsam mit ihrer Anwendung in Netzen des zweiten und dritten Teils zusammenfassen, wobei hierfür mindestens eine 4 Semesterwochenstunden umfassende Vorlesung geplant werden sollte. Der Schutz von Kommunikationsinfrastrukturen kann in einer zweiten eigenständigen Vorlesung gelehrt werden. Mit der letztgenannten Variante haben die Autoren an der TU Ilmenau in den vergangenen Jahren sehr gute Erfahrungen gesammelt. Auf weiterführende Kapitel und Abschnitte (im Buch mit einem Sternchen markiert) kann jeweils verzichtet werden ohne das weitere Verständnis zu beeinflussen.

An dieser Stelle möchten wir unseren Hörerinnen und Hörern sowie zahlreichen weiteren Personen herzlich danken, die uns durch ihre Fragen und Anregungen vielfältige Hinweise für die Darstellung des Lehrstoffes in unseren Vorlesungsfolien und diesem Buch gegeben haben. Ebenso gilt besonderer Dank einigen Mitarbeitern des Fachgebiets Telematik/Rechnernetze an der TU Ilmenau für ihre Beiträge zu Vorlesungsfolien, deren Inhalte Eingang in die neue Auflage gefunden haben. Namentlich hervorheben wollen wir an dieser Stelle Herrn Prof. Dr.-Ing. Thorsten Strufe und Herrn Dr.-Ing. Mathias Fischer. Herr Prof. Dr. Martin Dietzfelbinger vom Fachgebiet Komplexitätstheorie und Effiziente Algorithmen der TU Ilmenau hat wertvolle Kommentare zu der Darstellung der asymmetrischen Kryptografie gegeben, die wir zu großen Teilen aufgreifen konnten. Für sämtliche gegebenenfalls noch verbleibende Versäumnisse und Mängel tragen selbstverständlich wir die Verantwortung, und wir werden daher weiterhin für Hinweise und Anregungen dankbar sein.

Ilmenau, im Mai 2014
Günter Schäfer und Michael Roßberg

Vorwort zur ersten Auflage

Dieses Buch entstand während meiner Tätigkeit als wissenschaftlicher Assistent im Fachgebiet Telekommunikationsnetze der Technischen Universität Berlin und beruht auf der Vorlesung *Network Security*, die dort seit dem Wintersemester 2000/2001 von mir gehalten wird.

Ein besonderer Dank gilt daher dem Leiter dieses Fachgebiets, Herrn Prof. Dr.-Ing. Adam Wolisz, der mir an seinem Lehrstuhl hervorragende Arbeitsbedingungen geschaffen und mich darüber hinaus von Anfang an in meinem Bestreben unterstützt hat, ein Lehrbuch über Netzsicherheit zu schreiben.

Herr Dipl.-Ing. Andreas Hess hat die Mühe auf sich genommen, den gesamten Text einer ersten Korrekturlesung zu unterziehen. An dieser Stelle möchte ich mich für seine zügigen Reaktionszeiten und seine zahlreichen Anregungen herzlich bedanken.

Dank gilt ebenfalls dem Lektorat des dpunkt.verlages, das mir stets hilfreich zur Seite stand und die Zusammenarbeit sehr angenehm gestaltete, sowie den mir unbekannten Fachgutachtern für ihre vielfältigen Hinweise.

Schließlich möchte ich mich bei den Hörern meiner Vorlesung für ihre zahlreichen Fragen und Anregungen bedanken, die mir eine Vielzahl von Ideen für die inhaltliche Gestaltung dieses Buches gegeben haben.

Wenn trotz all dieser Hilfe noch Fehler in diesem Lehrbuch verblieben sind, so liegt die alleinige Verantwortung dafür natürlich bei mir. Für Hinweise und Anregungen zum Stoff dieses Buches werde ich daher auch weiterhin sehr dankbar sein.

Berlin, im Januar 2003
Günter Schäfer