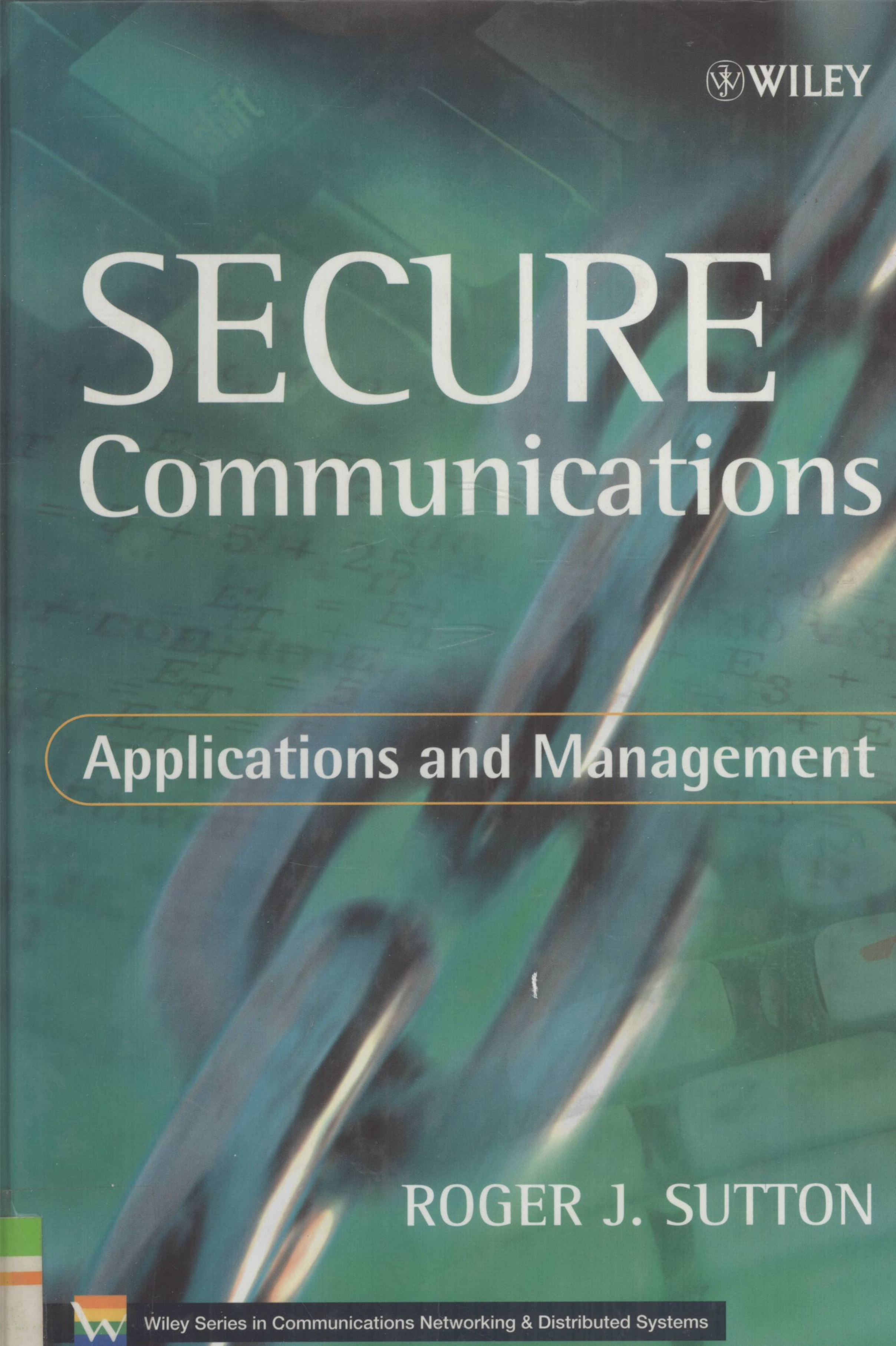

WILEY

SECURE Communications

Applications and Management

ROGER J. SUTTON

Wiley Series in Communications Networking & Distributed Systems

Secure Communications
Applications and Management

Roger J. Sutton
Crypto AG, Switzerland

JOHN WILEY & SONS, LTD

Baffins Lane, Chichester,
West Sussex, PO19 1UD, England
National 01243 779777
International (+44) 1243 779777

e-mail (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on http://www.wiley.co.uk or http://www.wiley.com

Neither the author(s) nor John Wiley & Sons, Ltd accept any responsibility or liability for loss or damage occasioned to any person or property through using the material, instructions, methods or ideas contained herein, or acting or refraining from acting as a result of such use. The author(s) and Publisher expressly disclaim all implied warranties, including merchantability of fitness for any particular purpose.

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where John Wiley & Sons, Ltd is aware of a claim, the product names appear in initial capital or capital letters. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

Other Wiley Editorial Offices

John Wiley & Sons, Inc., 605 Third Avenue,
New York, NY 10158-0012, USA

WILEY-VCH Verlag GmbH
Pappelallee 3, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 33 Park Road, Milton,
Queensland 4064, Australia

John Wiley & Sons (Canada) Ltd, 22 Worcester Road
Rexdale, Ontario, M9W 1L1, Canada

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01,
Jin Xing Distripark, Singapore 129809

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0471 49904 8

Typeset in Times by Deerpark Publishing Services Ltd, Shannon, Ireland.
Printed and bound in Great Britain by Biddles Ltd, Guildford and King's Lynn

This book is printed on acid-free paper responsibly manufactured from sustainable forestry, in which at least two trees are planted for each one used for paper production.

Secure Communications

WILEY SERIES IN COMMUNICATIONS NETWORKING & DISTRIBUTED SYSTEMS.

Series Editor: David Hutchison, Lancaster University
Series Advisers: Harmen van As, TU Vienna
Serge Fdida, University of Paris
Joe Sventek, Agilent Laboratories, Edinburgh

The 'Wiley Series in Communications Networking & Distributed Systems' is a series of expert-level, technically detailed books covering cutting-edge research and brand new developments in networking, middleware and software technologies for communications and distributed systems. The books will provide timely, accurate and reliable information about the state-of-the-art to researchers and development engineers in the Telecommunications and Computing sectors.

Other titles in the series:

Wright: Voice over Packet Networks
Jepsen: Java in Telecommunications

Dedication

To my family without whose support, advice and patience, I would not have had the stamina and discipline to see this production through. To my mother, Margaret Jean Sutton who as a member of the ATS during the Second World War, played a small role in the securing of Britain's communications.

To those whom I have loved and those whom, for some obscure reason and known only to themselves, have seen fit to hold me in their affections.

To those people of many nations, language, race or creed with whom I have shared friendships that have broken through all manmade barriers and who have made my journeys so delightfully rewarding.

Preface

This is not a book about cryptography, it is about how to apply cryptography to secure telecommunications. There are many fine manuscripts written on the subjects of cryptography and of telecommunications, but few that address the practical links between the two. In the eyes of the Cryptographer and in the ideals of those who employ him, security is often a matter of algorithms and mathematical statistics. Yet this is just the tip of the iceberg and what lies beneath this 'pristine peak' is a domain that is full of circumstance and danger. It is this grey area that I have addressed in this book and is written on the back of fifteen years experience in applying cryptography, technological know-how and psychological persuasion to the securing of my client's communications. In my experience the weak links in security have not necessarily been the strength of algorithms and hardware but rather in the way and diligence, or lack of it, that these have been implemented. As a result, what is the actual state of security at the communications level of an organisation is often very far removed from the grand ideals of the strategic decision makers. This book is aimed at providing a warning to those with their heads in the clouds and providing guidance to those who are given the task of implementing their strategies.

Secure Communications is essentially written in two parts and although some distinction is drawn between the technologies of voice and data communications, the two components are really a) The technical and philosophical aspects of security, support of chapters one, two and fourteen and b) The application chapters. The supporting chapters are included to provide background preparation material to the less cryptographically experienced reader. The application chapters also provide a varying degree of technical support specific to the medium in question, for without some knowledge of the medium technologies, it is impossible to assess the strengths and weaknesses of that technology, with any confidence.

Whilst there are many common factors between the applications, I have tried to view the problems of each platform from a different point of view. There are two reasons for my adopting this approach. The first is that it would be difficult to address each communications technology in any depth without having the security aspects readily at hand. This convenience is at the cost of some repetition that would be apparent to any cover-to-cover reader. The second reason being that each technology and each application can present many different approaches to securing them and to mass these into a single chapter would be too demanding and perhaps tedious for many a reader. Therefore, whilst I have striven to offer more complete platform packages in the application chapters, reading through the whole book should present a comprehensive package of alternative solutions. Essentially, I have sought to stimulate thought on the weaknesses of various communication technologies and present the strengths of a selection of solutions. The security manager reading this manuscript is expected to carry out something of a cut and paste exercise in applying the solutions suggested here, to secure his specific application.

One of the difficulties encountered in writing a book about security is the gaining of access to useful material and the freedom to publish it. Manufacturers and clients understandably strive to maintain their security and as a result, there have been times when I have experienced difficulty in acquiring material and permission to publish it. This is the nature of the industry and the reader, like the author, has to accept it. There are also occasions when the purists might argue that detail has been lost in some of the modelling that I have adopted. Bearing in mind the target audience of the book, these times were when I felt that the general concept was more important to portray rather than the delving into specific and complex issues.

Disclaimer

The author would like to point out that the opinions expressed in this text are solely those of his own and not of his employer, their agents or clients.

Acknowledgement

In writing this book, I am deeply indebted to my friend, Peter Mash for his writing of Chapter 12 and his many other contributions throughout. To Ralph Bühler, Dr. David Callaghan, Torgrim Jorgensen, Harry Kernohan, Dr. Richard Weber and others, for their technical criticisms and most valuable advice, I give my sincere thanks. Without their support, I could not have entertained writing this book. To Elisabeth for her advice and patience and meticulousness in proof reading the text, I offer my admiration and gratitude for tackling an arduous task.

Roger J. Sutton
106112.1717@compuserve.com

Figures 2.2, 3.6, 4.2, 5.10, 5.11, 5.18, 5.19, 6.5, 10.6 and 14.3 were reproduced with the kind permission of Crypto AG, Switzerland.

44 33 20 21 40 42 20 40 52 21 51 20 40 40 43 45 40 43
52 33 33 54 21 12 51 50 43 32 22 21 52 41 40 31 40 34
52 44 20 33 32 42 53 55 54 43 20 40 50 51 50 43 44 20
33 32 44 33 33 54 21 13 30 33 53 50 43 20 10 43 40 50
13

Glossary

Advanced encryption standard (AES): The replacement algorithm for DES, produced by Vincent Rijman and Joan Daemen.
Algorithm: A cryptographic procedure that defines how ciphering/deciphering is carried out.
Asymmetric algorithm: A cryptographic algorithm that uses different keys for encryption and decryption.
Authentication: The process of verifying that a particular name belongs to a particular entity.
Biometric access: The science of applying biological characteristics of a user as access tokens to a device or system, e.g. fingerprints.
Black designation: A designation given to cables, components, equipment and systems, which carry un-classified signals.
Block cipher: A cipher that encrypts data in blocks of a fixed size.
Brute force attack, exhaustive key search: The process of trying to recover a key or password by trying all the possibilities.

Certificate, public key: A specially formatted block of data that contains a public key and the owner's identification. The certificate carries the digital signature of a certifying authority to authenticate it.
Cipher: A procedure that transforms data from plaintext to ciphertext.
Cipher block chaining (CBC): A block mode cipher that combines the previous block of ciphertext with the current block of plaintext before encrypting it.
Cipher feedback (CFB): A block cipher mode that feeds previously encrypted ciphertext through the block cipher to generate the key that encrypts the next block of ciphertext.
Ciphertext: Data that have been encrypted by a cipher.
Compromising emanations: The radiation of electromagnet signals that can carry unintentionally, information about data within the system.
Confidentiality: The ability to ensure that information is not disclosed to persons who are not explicitly intended to read it.
Cryptanalysis: The process of trying to recover secret keys, or text from a ciphertext.
Cryptography: Mechanisms used to protect information by applying transformations to plaintext that are difficult to reverse without possessing knowledge of that mechanism.

Data encryption standard (DES): A block cipher that uses a key length of 56 bits, which is widely used in commercial systems.
Decipher; decrypt: Change from ciphertext into plaintext.

Diffie–Hellman (DH): A public key cipher algorithm that generates a shared secret between two parties after they have exchanged some random generated data.
Digital signature: A data value generated by a public key algorithm, which is based upon the contents of a block of data and a private key, yielding a individualised cipher checksum.
Down line loading: A method of key/parameter distribution to cipher machines by means of a secure channel.
Dongle: An electronic access device.

Electronic code book (ECB): A block cipher that consists of applying a cipher, or code to block of data in sequence, one block at a time.
Electromagnetic compatibility (EMC): The stray electromagnetic radiation (noise) given out by an electronic device that may adversely affect the operation of another device.
E-mail: Electronic mail protocol for sending messages between users of a network.
Encapsulating security payload (ESP): A data packet that is entirely encrypted, including the address header, to which another header is attached for the purpose of hiding the original header.
Enigma: A German cipher machine that used a series of wired rotors to encrypt messages for data transmission, during the Second World War.
Exclusive OR: A computational device, often in the form of an electronic gate, that adds two bits together, i.e. modulo 2 addition and discards any carry on.
Exhaustive key search: See 'Brute force attack'.

Firewall: A device that is installed at a point in a computer network where data flow in and out of that network and control that flow according to the rules programmed in the device.

Integrity: The ability to ensure that information has not been modified except by people who are explicitly intended to modify it.
International Data Encryption Algorithm (IDEA): A block cipher algorithm developed in Switzerland.
Internet protocol: A protocol that carries individual packets between hosts.
IP address: The host address used in IP transmission.

Key distribution centre, key management centre: A device that provides secret keys for a secure network and organises the distribution of those keys throughout the network components.
Key encryption key (KEK), key transport key (KTK): A cipher key that is used to encrypt session and/or data keys but is never used to cipher data payloads.
Key escrow: A mechanism for the storage of cipher keys, so that a third party can recover them if necessary and use them to decipher the other party's ciphertext.
Key length: The length, in binary digits of a cipher key. Typically 56, 128, or 256.
Key stream: The output of a key generator that is used to convert plaintext into cipher text and vice versa.
Key stream period: The time taken for a key stream to repeat itself.

Local area network (LAN): A network that consists a single type of data link that resides within a physically specified area.

Masquerade: A method of attack whereby an entity takes on the identity of another user without authorisation.
Message authentication code: A method of authenticating text or data messages by the use of encrypting keys.
Modulo 2 addition: The binary addition of two bits, by an exclusive OR function.
National Security Agency (NSA): An agency of the US government that is responsible for the interception of communications for intelligence reasons and for the development and control of cipher systems to protect the government of the USA.
Non-repudiation: The inability of a message signatory to deny that the message came from him/her, by the use of public key encryption.

One-time pad: A Vernam cipher in which one bit, or character, newly and randomly generated, is used for every bit, or character of data.
One-time password: A password that can only be used once.
One-way hash function: A hash function for which it is infeasible to construct two blocks of data that yield the same hash value.
Over the air (OTAR): A method of key/parameter distribution to cipher machines by means of a secure channel otherwise called 'over the air re-keying'.

PC card (PCMCIA): A standard plug-in peripheral that is often used in laptop computers and can be adapted to function as modems or as cipher modules containing algorithms and other sensitive parameters.
Pretty good privacy (PGP®): An algorithm written by Phil Zimmerman to provide a high standard of encryption for the general public, amongst others. Free versions are widely available on the Internet.
Private key: A key that is one part of a key pair, used in public key cryptography that belongs to an individual user and must be kept secret. Data ciphered by a user's private key can only be deciphered by that user's public key.
Public key: A key that is one part of a key pair, used in public cryptography that is distributed publicly. Data ciphered by a user's public key can only be deciphered by that user's private key.
Public key algorithm: An asymmetric algorithm that uses a pair of keys, a public and a private key for ciphering and deciphering.

Random number: A number whose value cannot be predicted.
Red designation: A designation given to cables, components, equipment and systems, which carry classified signals.
Red/black separation: A design concept that separates parts of a system carrying plaintext from parts that carry ciphertext.
Replay: An attack whereby an intercepted message is retransmitted with the intent of confusing the receiver of the legitimate message.
Rivest, Shamir, Adelman (RSA®): A public key system that can encrypt or decrypt data and also apply or verify a digital signature.
Router: A device that carries IP packets between networks and is used to direct those packets to the next station in the transmission route.

Secret key: A cipher key to transform a plaintext into a ciphertext and vice versa.
Server: The device in a network that provides services to clients and other entities on the network, e.g. printing services.
Session key: A cipher key that is intended to encrypt data during a limited period of time, typically for a single transmission after which the key is usually discarded.
Spoofing: Similar to masquerading, i.e. pretending to be somebody else.
Stream cipher: A cipher that operates on a continuous data stream instead of processing it block by block at a time.
Symmetrical algorithm: A cipher algorithm that uses the same key for encryption and decryption.

Tamperproofing/resistance: The technique of providing logical and physical protection to a cipher machine or module, rendering it infeasible to attack.
Tempest: The term given by the US government to identify the problem of compromising radiations.
Time authentication: A technique used by cipher machines to remove the threat of message replay.
Transmission control protocol: Internet protocol that supports remote terminal connections.
Triple DES: A cipher that applies the DES cipher three times.
Trojan horse: A program with secret functions that accesses information without the operator's knowledge and is usually used to circumvent security barriers.
Tunnel mode: ESP mode that encrypts an entire IP packet including the original header.

ULTRA: The code name used to describe a British code-breaking system during the Second World War.

Vernam cipher: Cipher developed for encrypting teletype traffic by computing the exclusive OR (modulo 2 addition) of the data bit stream and key bit stream as commonly used in stream ciphers.
Virtual private network: A secure communication system that uses encryption to exclude all other users and hosts from the 'network'.
Virus: A small program that attaches itself to a legitimate program so that when the latter is being run, the virus copies itself to another legitimate program.

Wide area network: A network that connects host computers and sites across a wide geographical area.

Acronyms and Abbreviations

AES	Advance encryption standard
ASIC	Application specific integrated circuit
ATM	Asynchronous transfer mode
AuC	Authentication centre
BS	Base station
BSC	Base station controller
BSS	Base station system
BTS	Base transceiver station
CCD	Charged couple device
CEPT	Conférence des Administrations Europèenes des Postes et Telecommunications
CMOS	Complementary metal oxide semiconducter
DES	Data encryption standard
DCE	Data connection equipment
DCN	Data communications network
DLL	Down line loading
DTE	Data terminal equipment
EMC	Electro-magnetic compatibility
FM	Frequency modulation
GSM	Global system for mobile communications
HF	High frequency (3–30 MHz)
IDEA	International data encryption algorithm
IV	Initialisation vector
INMARSAT	International Marine Satellite Organisation
LES	Land earth station
MES	Mobile earth station
MS	Mobile station
OTA	Over the air
PABX	Private automatic branch exchange
PC	Personal computer or printed circuit
PCB	Printed circuit board
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal identification number
PGP	Pretty good privacy
PSTN	Public switched telephone network

TCP	Transmission control protocol
TDMA	Time division multiple access
UHF	Ultra high frequency (300–3000 MHz)
VHF	Very high frequency (30–300 MHz)
VPN	Virtual private network
WAN	Wide area network
WS	Work station

Key abbreviations

CEK	Card encryption key for ciphering chip cards
CMK	Customer master key: a source key used to generate a session key
DK	Disk encrypting key: a key used to cipher hard or floppy disks
FLK	Future link key: a source key to be used to generate a session key for a specific communications link, at a later time
KEK	Key encryption key: a general term describing a key used to protect a message encrypting key, usually during transport
KSK	Key storage key: a key used to encrypt ciphering keys stored in memory
KTK	Key transport key/key transfer key: a key used to cipher a message encrypting key during its transport
CHK	Channel or link key: source key used to generate session keys for a specific link
MCK	A key, often link specific, that is used as a source key for the generation of session keys. See CMK
MK	Management database key: a key used to cipher management data on a key management centre
NCHK	Next channel key: a link key for future use
PaCHK	Past channel key: a link key that was used in the past
PrCHK	Present channel key: a link key that is being used at present
SK	Secret key: the data encryption key
SK-B	Secret broadcast key: a data encryption key used to cipher data simultaneously to a number of stations
TRK	Tamper resistance key: a unique, logical protective key ciphering sensitive data within a tamperproof/resistant module
Xx	Default keys

Contents