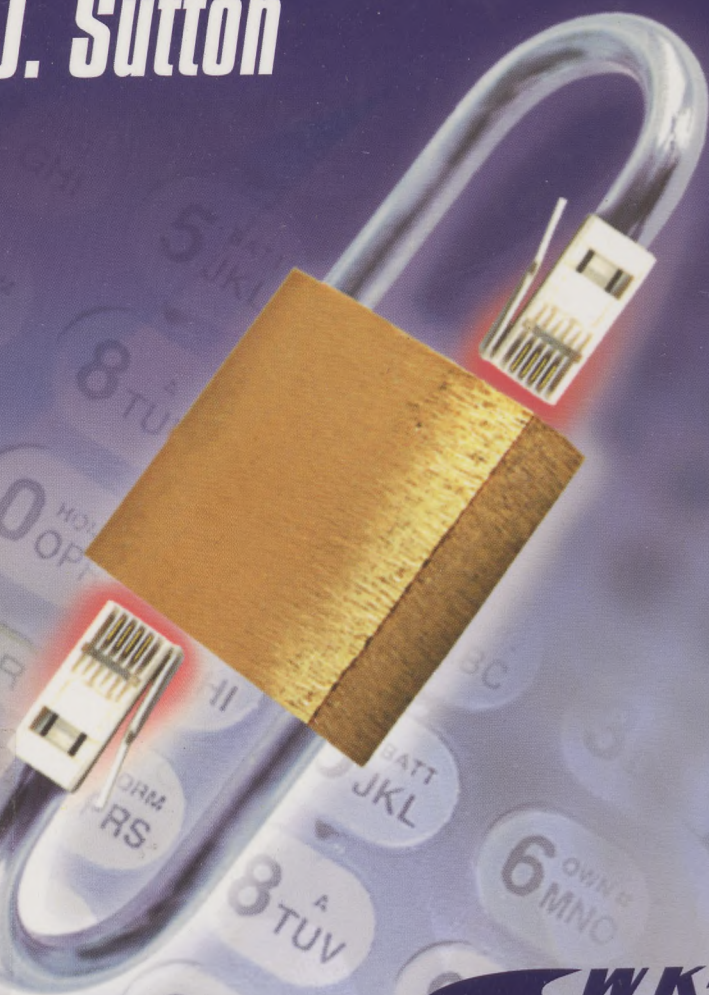


Bezpieczeństwo telekomunikacji

Roger J. Sutton



WKT





Bezpieczeństwo telekomunikacji

Praktyka i zarządzanie

Mojej rodzinie, bez której wsparcia, pomocy i cierpliwości nie starczyłoby mi wytrwałości i dyscypliny do napisania tej książki. Mojej matce, Margaret Jean Sutton, która jako członek ATS podczas drugiej wojny światowej miała także swój udział w zapewnieniu bezpieczeństwa brytyjskiej telekomunikacji.

Tym wszystkim, których kocham i tym, którzy z pewnych niejasnych powodów, znanych tylko im samym, obdarzyli mnie swoim uczuciem.

Ludziom wielu narodowości, języków, ras i wyznań, z którymi łączyła mnie przyjaźń przełamująca wszelkie bariery międzyludzkie i dzięki której moje podróże były tak bardzo satysfakcjonujące.

16-27-1
Roger J. Sutton

Bezpieczeństwo telekomunikacji Praktyka i zarządzanie

Tłumaczył z języka angielskiego
Grzegorz Stawikowski



Wydawnictwa Komunikacji i Łączności
Warszawa

Dane o oryginale:

Roger J. Sutton: Secure Communications. Applications and Management

© Copyright 2002 by John Wiley & Sons, Ltd

All Rights Reserved. Authorized translation from the English language edition published by John Wiley & Sons, Ltd.

Projekt okładki: Dariusz Litwiniec

Opiniodawca: prof. dr hab. inż. Jacek Wojciechowski

Redaktor: Krzysztof Wiśniewski

Redaktor techniczny: Alicja Pietrzak

Korekta: zespół

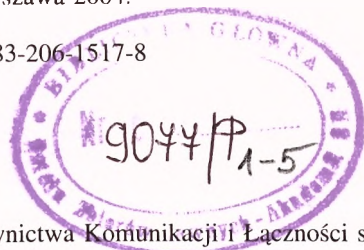
654:621.391.7

W książce opisano bezpieczeństwo telekomunikacji oraz zarządzanie nim z uwzględnieniem różnych metod ochrony, a zwłaszcza szyfrowania. W aspekcie bezpieczeństwa przedstawiono różne rodzaje sieci komunikacyjnych cywilnych i wojskowych (m.in. przesyłanie głosu, telefonię stacjonarną, telefonię komórkową, radiokomunikację, sieci faksowe, transmisję i przechowywanie danych w komputerach osobistych, protokoły internetowe oraz pocztę elektroniczną). Podano zagrożenia bezpieczeństwa telekomunikacji, różne metody ochrony informacji, praktyczne porady dotyczące rzeczywistych rozwiązań w zakresie sprzętu i oprogramowania, przykłady bezpiecznych sieci łączności cywilnej i wojskowej oraz wytyczne dotyczące zarządzania, obsługi i szkolenia.

Odbiorcy: wszyscy zainteresowani problematyką bezpieczeństwa telekomunikacji, studenci oraz słuchacze kursów doszkalających w tym zakresie.

© Copyright for the Polish edition by Wydawnictwa Komunikacji i Łączności sp. z o.o., Warszawa 2004.

ISBN 83-206-1517-8



Wydawnictwa Komunikacji i Łączności sp. z o.o.

ul. Kazimierzowska 52, 02-546 Warszawa

tel. (0-22) 849-27-51; fax (0-22) 849-23-22

Dział handlowy tel./fax (0-22) 849-23-45

tel. 849-27-51 w. 555

Prowadzimy sprzedaż wysyłkową książek

Księgarnia firmowa w siedzibie wydawnictwa

tel. (0-22) 849-20-32, czynna pon.–pt. 10.00–18.00

e-mail wkl@wkl.com.pl

Pełna oferta WKŁ w INTERNECIE <http://www.wkl.com.pl>

Wydanie 1. Warszawa 2004.

Druk i oprawa: Drukarnia Naukowo-Techniczna S.A.

Warszawa, ul. Mińska 65

Spis treści

PRZEDMOWA	11
1 ZAGROŻENIA I OCHRONA DANYCH	13
1.1 Zagrożenia bezpieczeństwa telekomunikacji	17
1.2 Uwierzytelnianie	17
1.3 Poufność	20
1.4 Integralność	21
1.5 Dostępność	23
1.5.1 Osobiste numery identyfikacyjne PIN i hasła	23
1.5.2 Biometryczne narzędzia dostępu	27
1.5.3 Procedura kontroli wezwania-odzew	29
1.5.4 Moduły odporne na penetrację	29
1.6 Przypadkowy przeciek informacji lub zagrożenia standardu Tempest	30
1.6.1 Definicje związane z przypadkowym przeciekiem informacji	30
1.6.2 Przypadkowy przeciek informacji	31
1.6.3 Składowe harmoniczne modulowane	32
1.6.4 Sprzężenie elektroniczne	34
1.6.5 Rozwiązania stosowane w konstrukcji sprzętu elektronicznego	35
2 WPROWADZENIE DO SZYFROWANIA I ZARZĄDZANIA BEZPIECZEŃSTWEM	39
2.1 Skramblowanie analogowe	39
2.1.1 Fonemy i struktura sygnału mowy	40
2.1.2 Skramblowanie częstotliwości	41
2.1.3 Skramblowanie elementów wydzielonych w czasie	43
2.2 Szyfrowanie cyfrowe	45
2.2.1 Szyfrowanie strumienia cyfrowego	45
2.2.2 Szyfrowanie blokowe	48
2.2.3 Podsumowanie	52
2.3 Algorytmy szyfrujące	53
2.3.1 Szyfrowanie symetryczne	53
2.3.2 Szyfrowanie asymetryczne	54
2.3.3 Algorytmy funkcji skrótu	56
2.3.4 Kody uwierzytelniania wiadomości MAC	56
2.3.5 Algorytmy podpisów cyfrowych	57
2.3.6 Algorytmy uzgadniania lub wymiany kluczy szyfrujących	58
2.3.7 Porównanie algorytmów asymetrycznych i symetrycznych	58
2.4 Żegnaj DES, witaj AES	58
2.5 Podstawowe zasady zarządzania kluczami szyfrującymi	59
2.5.1 Generowanie kluczy szyfrujących	61
2.5.2 Przechowywanie kluczy szyfrujących	64

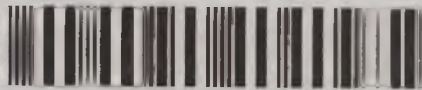
2.5.3	Dystrybucja kluczy szyfrujących	64
2.5.4	Zmiany kluczy szyfrujących	66
2.5.5	Zniszczenie kluczy szyfrujących	71
2.5.6	Separacja	72
2.6	Ocena sprzętu szyfrującego	74
3	BEZPIECZEŃSTWO ROZMÓW W WOJSKOWYCH SYSTEMACH ŁĄCZNOŚCI	77
3.1	Szyfrowanie analogowe w krótkofalowej łączności radiowej dalekiego zasięgu marynarki wojennej	79
3.1.1	Działanie łączności okrętowej	80
3.1.2	Właściwości urządzenia szyfrującego (skramblera)	81
3.1.3	Synchronizacja	85
3.1.4	Parametry bezpieczeństwa	86
3.1.5	Dystrybucja i zarządzanie kluczami szyfrującymi	87
3.2	Samodzielny cyfrowy szyfrator mowy	88
3.2.1	Schemat łączności wojsk lądowych	88
3.2.2	Właściwości cyfrowego szyfratora mowy	89
3.2.3	Synchronizacja	92
3.2.4	Parametry bezpieczeństwa	95
3.2.5	Zarządzanie kluczami szyfrującymi	96
3.3	Zintegrowany moduł cyfrowego szyfratora mowy	102
3.3.1	Typowe właściwości	102
3.3.2	Parametry kryptograficzne	102
3.3.3	Inne parametry i właściwości bezpieczeństwa	103
4	BEZPIECZEŃSTWO TELEFONII	106
4.1	Zagrożenia łączności telefonicznej	107
4.2	Techniki sieciowe	109
4.2.1	Chroniona łączność telefoniczna	109
4.2.2	Łączność satelitarna INMARSAT	110
4.3	Rozwiązania bezpiecznej telefonii	115
4.3.1	Chronione urządzenie telefoniczne STU III/IIB	116
4.3.2	Alternatywne metody zapewnienia bezpieczeństwa telefonicznego	118
4.3.3	Elementy bezpieczeństwa sprzętowego	122
4.3.4	Funkcje i architektura systemu ochrony telefonu	123
4.4	Zarządzanie kluczami szyfrującymi i dostępem	125
4.4.1	Kompletny system kluczy szyfrujących	126
4.4.2	Sieć ZAPPA	130
4.5	Przykład realizacji sieci	131
4.6	Dystrybucja kluczy szyfrujących	134
4.7	Podsumowanie	135
5	SYSTEMY OCHRONY TELEFONII KOMÓRKOWEJ GSM	136
5.1	Podstawowa architektura systemu GSM	136
5.1.1	Składniki systemu GSM	137
5.1.2	Podsystemy GSM	140
5.1.3	Styk radiowy Um w systemie GSM	141
5.2	Standardowe elementy bezpieczeństwa systemu GSM	142
5.2.1	Centrum uwierzytelnienia AuC	143
5.2.2	Rejestr stacji własnych HLR	144
5.2.3	Rejestr stacji obcych VLR	144
5.2.4	Karta SIM	144

5.2.5	Międzynarodowy numer identyfikacyjny abonenta IMSI oraz tymczasowy numer identyfikacyjny abonenta TMSI	146
5.2.6	Standardowe szyfrowanie w systemie GSM	146
5.2.7	Ataki kryptograficzne na algorytmy GSM	149
5.2.8	Wielodostęp z podziałem czasowym TDMA	152
5.2.9	Przeskoki częstotliwości	152
5.3	Niestandardowe środki bezpieczeństwa dla użytkowników GSM	153
5.3.1	Niestandardowy proces szyfrowania	155
5.3.2	Systemy szyfrowania z kluczami szyfrującymi	159
5.3.3	Algorytmy i parametry szyfrowania	161
5.3.4	Architektura systemu bezpieczeństwa	161
5.3.5	Elementy sprzętowe jednostki szyfrującej	162
5.3.6	Schemat bezpiecznego systemu łączności telefonów komórkowych GSM ze stałymi stacjami abonenckimi	162
5.4	Zarządzanie kluczami szyfrującymi i jego narzędzia	163
5.4.1	Dystrybucja i ładowanie kluczy szyfrujących	164
5.4.2	Karty mikroprocesorowe i czytniki	164
5.4.3	Podpisy kluczy szyfrujących	165
5.5	Systemy transmisji pakietowej GPRS	165
6	BEZPIECZEŃSTWO PRYWATNYCH SIECI	
	RADIOKOMUNIKACYJNYCH VHF/UHF	169
6.1	Zastosowanie i elementy sieci VIPNET	169
6.1.1	Grupa pokładowa	169
6.1.2	Grupa eskorty	171
6.1.3	Grupa bliskiego wsparcia	172
6.1.4	Grupy abonentów telefonicznych	172
6.2	Zagrożenia	172
6.2.1	Poufność	173
6.2.2	Integralność	173
6.2.3	Autentyczność	173
6.2.4	Dostęp	173
6.3	Środki bezpieczeństwa	173
6.3.1	Ochrona poufności	174
6.3.2	Uwierzytelnianie	176
6.3.3	Kontrola dostępu	177
6.4	Architektura i budowa sieci komunikacji	179
6.4.1	Grupa bliskiego wsparcia	179
6.4.2	Grupa eskorty	179
6.4.3	Grupa pokładowa	181
6.5	Elementy sieci i funkcje sprzętu	182
6.5.1	Radiotelefony przenośne pracujące w pasmie UHF	182
6.5.2	Stacje bazowe i przemienniki	188
6.5.3	Przystawka telefoniczna	189
6.5.4	Narzędzia zarządzania bezpieczeństwem	191
6.6	Zarządzanie bezpieczeństwem i kluczami szyfrującymi	192
6.6.1	Funkcje centrum zarządzania	192
6.6.2	Zarządzanie częstotliwościami	193
6.6.3	Zarządzanie kluczami szyfrującymi	196
6.7	Inne funkcje bezpieczeństwa	199
6.7.1	Zdalne kasowanie kluczy szyfrujących	199
6.7.2	Zdalne blokowanie	199
6.7.3	Ciche śledzenie	200

7	OBRONA RADIOELEKTRONICZNA – PRZESKOKI CZĘSTOTLIWOŚCI	201
7.1	Rozpoznanie radioelektroniczne	201
7.2	Atak radioelektroniczny	201
7.3	Obrona radioelektroniczna	202
7.3.1	Formy ataku radioelektronicznego	202
7.3.2	Techniki rozszerzania pasma	207
7.3.3	COMSEC oraz TRANSEC	213
7.4	Zastosowania wojskowe	214
7.4.1	Wymagania dotyczące aplikacji	214
7.4.2	Wymagania dotyczące działania	214
7.4.3	Wymagania bezpieczeństwa	215
7.4.4	Wymagania przeciwwzakłóceńowe	215
7.4.5	Wspólna lokalizacja	216
7.4.6	Schemat łączności obrony powietrznej	217
7.4.7	Schemat łączności współdziałania z lotnictwem	219
7.5	Zarządzanie i architektura sieci	219
7.6	Właściwości sieci stosujących technikę przeskoków częstotliwości	224
7.6.1	COMSEC	224
7.6.2	TRANSEC	225
7.7	Narzędzia i zarządzanie danymi oraz kluczami szyfrującymi	234
7.7.1	Dane algorytmu szyfrującego	234
7.7.2	Dane częstotliwości	235
7.7.3	Dane ustawienia wstępnego	236
7.7.4	Parametry konfiguracji	236
7.7.5	Dystrybucja kluczy szyfrujących	236
7.7.6	Problem czasu	238
7.8	Elementy sprzętowe	240
8	SZYFROWANIE DANYCH MASOWYCH I NA POZIOMIE ŁĄCZA	243
8.1	Podstawowa technika szyfrowania na poziomie łącza	243
8.2	Proces szyfrowania	246
8.3	Parametry kryptograficzne	248
8.4	Zarządzanie siecią i kluczami szyfrującymi	249
8.5	Ochrona łączy wojskowych	256
9	BEZPIECZENSTWO SIECI FAKSOWYCH	260
9.1	Podstawowa technika faksymilowania	261
9.2	Podstawy działania faksu szyfrującego	262
9.2.1	Faksowanie przez łącze telefoniczne	262
9.2.2	Faksowanie przez łącze radiowe	263
9.2.3	Protokół faksowy standardu G3	263
9.3	Ręczny lub automatyczny wybór kluczy szyfrujących	265
9.3.1	Sieci faksowe z wieloma kluczami szyfrującymi	267
9.3.2	Sieci faksowe z pojedynczym kluczem szyfrującym	268
9.3.3	Transmisja faksowa przez łącze radiowe	268
9.4	Architektura sieci faksowej	268
9.4.1	Właściwości sieci DEFNET	269
9.4.2	Podsieć ministerstwa obrony	269
9.5	Zarządzanie kluczami szyfrującymi i niezbędne narzędzia	270
9.5.1	Zarządzanie kluczami szyfrującymi dla sieci DEFNET	270
9.5.2	Generowanie kluczy szyfrujących	271

9.5.3	Wytyczne użytkowania	272
9.5.4	Dystrybucja parametrów i kluczy szyfrujących	273
9.6	Faksowanie przez łącza satelitarne	273
10	BEZPIECZEŃSTWO KOMPUTERÓW OSOBISTYCH	275
10.1	Zagrożenia bezpieczeństwa komputera	278
10.2	Sposoby zabezpieczenia	278
10.2.1	Nieuprawniony odczyt danych przechowywanych na lokalnym nośniku danych	278
10.2.2	Nieuprawniony odczyt „usuniętych” danych	279
10.2.3	Nieuprawniony odczyt danych przechowywanych w odległej stacji sieci lokalnej	279
10.2.4	Nieuprawniona ingerencja w dane przechowywane na serwerze podłączonym do sieci lokalnej	281
10.2.5	Podśluchiwanie w niepewnej sieci lokalnej lub w sieci publicznej	282
10.2.6	Zwodzenie i podszywanie się pod użytkownika	282
10.2.7	Nieuprawniona ingerencja w dane podczas komunikacji w sieci publicznej	283
10.2.8	Nieuprawniony dostęp do chronionego systemu	283
10.2.9	Atak na zasadzie pełnego przeglądu	284
10.2.10	Nieskuteczna ochrona i zarządzanie kluczami szyfrującymi	285
10.2.11	Analiza resztkowych informacji jawnych	285
10.2.12	Ujawnienie informacji w związku z zagubieniem lub kradzieżą sprzętu albo zmianą personelu ochrony	286
10.2.13	Przechowywanie lub przesyłanie wiadomości w trybie jawnym z powodu zagubienia lub niezgodności kluczy szyfrujących	286
10.2.14	Nielegalny dostęp do sprzętu podczas konserwacji lub napraw	286
10.2.15	Nieuprawnione wtargnięcie do środowiska komputera osobistego podczas połączenia z siecią publiczną lub z siecią niepewną	287
10.3	Ochrona dostępu	288
10.3.1	Systemy kontroli dostępu	288
10.3.2	Dostęp za pomocą karty mikroprocesorowej	288
10.3.3	Dostęp za pomocą kart PC	290
10.3.4	Dostęp za pomocą modułu PCMCIA	291
10.4	Ochrona procesu uruchomienia komputera za pomocą sprzętu zintegrowanego na płycie z kartą inteligentną	291
10.5	Bezpieczeństwo sieci lokalnej	291
10.5.1	Stacja robocza działająca w sieci lokalnej	292
10.5.2	Bezpieczeństwo komputera przenośnego w czasie podróży służbowej	294
10.6	Modelowe rozwiązanie zapewniające bezpieczeństwo komputerów osobistych	295
10.7	Administrowanie systemem	298
11	BEZPIECZEŃSTWO POCZTY ELEKTRONICZNEJ	301
11.1	Schemat poczty elektronicznej	301
11.2	Zagrożenia	303
11.2.1	Ujawnienie informacji	304
11.2.2	Modyfikacja wiadomości	304
11.2.3	Atak powtarzania wiadomości	304
11.2.4	Podszywanie się	305
11.2.5	Zwodzenie	305
11.2.6	Pozbawienie usługi	306
11.3	Atakujący i ich motywacja	306
11.4	Metody ataku	307
11.5	Środki ochrony	307
11.6	Wskazówki dotyczące bezpieczeństwa poczty elektronicznej	310

12	BEZPIECZEŃSTWO WIRTUALNYCH SIECI PRYWATNYCH	312
12.1	Wiadomości wstępne	312
12.2	Definicja wirtualnej sieci prywatnej	313
12.3	Protokoły	314
12.4	Formaty nagłówka pakietu	316
12.5	Lista powiązań zabezpieczeń	320
12.6	Tabela tuneli	320
12.7	Tabele tras	321
12.8	Filtrowanie pakietów	322
12.9	Zagrożenia i sposoby ochrony	323
12.9.1	Ataki wewnątrz sieci publicznej	323
12.9.2	Ataki wewnątrz węzłów sieci wiarygodnej	324
12.9.3	Ataki w celu uzyskania dostępu do sieci prywatnej	324
12.10	Przykład sieci dyplomatycznej	324
13	TRANSMISJA DANYCH W WOJSKOWYCH SIECIACH ŁĄCZNOŚCI	328
13.1	Aplikacje	329
13.1.1	Dane przesyłane w łączach radiowych	329
13.1.2	Automatyczne żądanie powtórzenia ARQ i korekcja błędów w przód FEC	330
13.1.3	Użycie terminali GAN w aplikacjach związanych z polem walki	331
13.2	Terminale danych i ich funkcje	331
13.3	Parametry techniczne	332
13.4	Zarządzanie bezpieczeństwem	334
13.4.1	Kontrola dostępu	334
13.4.2	Szyfrowanie danych	334
13.4.3	Utrata danych	334
13.4.4	Standard Tempest	335
13.5	Zarządzanie kluczami szyfrującymi	335
13.6	Polowe sieci pakietowe	336
13.6.1	Urządzenia do radiowej transmisji pakietowej	336
13.6.2	Pakietowa transmisja danych	337
14	ZARZĄDZANIE, OBSŁUGA I SZKOLENIE	340
14.1	Środowiska zarządzania bezpieczeństwem	342
14.1.1	Środowisko globalne	342
14.1.2	Środowisko lokalne	346
14.2	Infrastruktura i planowanie	347
14.2.1	Cele strategiczne	347
14.2.2	Cele taktyczne	348
14.2.3	Cele bieżące	348
14.3	Schemat organizacyjny	348
14.4	Szkolenie	349
14.5	Obsługa klienta	352
14.6	Rozwiązywanie problemów	352
14.6.1	Etap poszukiwania	353
14.6.2	Etap klasyfikacji	353
14.6.3	Etap diagnostyki	353
14.6.4	Wybieranie rozwiązań	353
	Literatura	355
	Wykaz skrótów	356
	Słownik podstawowych pojęć	359



W książce opisano praktyczne aspekty bezpieczeństwa telekomunikacji oraz zarządzania sieciami. Przedstawiono różne rodzaje sieci komunikacyjnych i wojskowych oraz szeroki zakres zagadnień, w tym: przesyłanie głosu, telefonię stacjonarną, telefonię komórkową, radiokomunikację, sieci faksowe, transmisję i przechowywanie danych w komputerach osobistych, protokoły internetowe oraz pocztę elektroniczną.

Czyt.

004.056

W niniejszej publikacji podano:

- zagrożenia bezpieczeństwa telekomunikacji,
- różne metody ochrony informacji,
- praktyczne porady dotyczące rzeczywistych rozwiązań w zakresie sprzętu i oprogramowania,
- przykłady bezpiecznych sieci telekomunikacyjnych cywilnych i wojskowych,
- wytyczne dotyczące zarządzania, obsługi i szkolenia

Wydawnictwa Komunikacji i Łączności

www.wkl.com.pl

ISBN 83-208-1517-8

9 788320 615173