

Spis treści

Podziękowania	11
O autorze.....	13
Wprowadzenie	15
CZEŚĆ I. Bezpieczeństwo baz danych	19
Rozdział 1. Problematyka bezpieczeństwa baz danych.....	21
1.1. Ataki na bazy danych.....	22
1.1.1. Typy ataków	22
1.1.2. Ataki na poufność	23
1.1.3. Ataki na integralność	24
1.1.4. Ataki na dostępność	26
1.1.5. Modele zagrożeń.....	27
1.2. Zewnętrzne wymagania dotyczące zabezpieczenia bazy danych.....	29
1.2.1. Ustawodawstwo.....	30
1.2.2. Zgodność z zasadami biznesu.....	33
1.2.3. Regulacje handlowe.....	33
1.2.4. Utrata reputacji	33
1.3. Podsumowanie	34
Rozdział 2. Ochrona baz danych za pomocą kryptografii.....	35
2.1. Krótkie przypomnienie baz danych.....	35
2.2. Czym jest kryptografia.....	37
2.2.1. Kryptografia symetryczna.....	38
2.2.2. Kryptografia z kluczem publicznym.....	39

2.2.3.	Mieszanie kryptograficzne.....	40
2.3.	Stosowanie kryptografii	41
2.3.1.	Ochrona poufności.....	41
2.3.2.	Zapewnienie integralności	44
2.4.	Ryzyko kryptograficzne	45
2.5.	Ataki kryptograficzne	46
2.5.1.	Pośredni dostęp do kluczy	47
2.6.	Zaciemnianie.....	49
2.7.	Przezroczyste szyfrowanie	50
2.8.	Podsumowanie	52
CZĘŚĆ II. Infrastruktura kryptograficzna		55
Rozdział 3. Podstawy infrastruktury kryptograficznej.....		57
3.1.	Architektura aplikacji.....	58
3.2.	Architektura kryptograficzna	60
3.3.	Klucze kryptograficzne	62
3.3.1.	Rozdzielanie kluczy.....	62
3.3.2.	Rodziny kluczy	63
3.3.3.	Cykl życia klucza.....	66
3.3.4.	Zakres klucza.....	68
3.3.5.	Zmęczenie klucza	71
3.3.6.	Migracja kluczy	73
3.3.7.	Zastępowanie kluczy	74
3.3.8.	Aliasy kluczy i dokumentacja kluczy	75
3.4.	Podsumowanie	76
Rozdział 4. Maszyny kryptograficzne i algorytmy		77
4.1.	Maszyny lokalne	78
4.2.	Maszyny dedykowane.....	80
4.2.1.	FIPS 140	81
4.3.	Algorytmy kryptograficzne.....	82
4.3.1.	Algorytmy symetryczne.....	82
4.3.2.	Tryby działania	83
4.4.	Podsumowanie	89
Rozdział 5. Klucze: sejfy, dokumentacja i menadżerowie		91
5.1.	Sejfy na klucze.....	91
5.1.1.	Ochrona sejfów	93
5.1.2.	Tworzenie kopii zapasowych i odzyskiwanie kluczy	96
5.2.	Dokumentacja kluczy.....	97
5.3.	Menadżer kluczy	100
5.3.1.	Strefy kluczy.....	100

5.3.2. Zarządzanie kluczami	103
5.4. Podsumowanie	103
Rozdział 6. Dostawcy i konsumenci kryptograficzni	105
6.1. Dostawca.....	106
6.2. Konsument	108
6.3. Podsumowanie	110
CZĘŚĆ III. Projekt kryptograficzny	113
Rozdział 7. Zarządzanie projektem kryptograficznym.....	115
7.1. Kultura bezpieczeństwa	116
7.2. Zaangażowanie klienta.....	117
7.3. Zakres projektu	119
7.4. Role w projekcie	120
7.5. Podsumowanie	121
Rozdział 8. Uściślanie wymagań.....	123
8.1. Wymagania dotyczące bezpieczeństwa, reguły i standardy	125
8.2. Powszechnie wymagania	126
8.2.1. Kontrola dostępu.....	126
8.2.2. Czyszczenie danych.....	127
8.2.3. Dzienniki i monitorowanie	128
8.2.4. Typowe zagrożenia.....	129
8.2.5. Poufność informacji.....	130
8.3. Ocena wymagań.....	131
8.4. Określenie standardu kryptograficznego.....	132
8.5. Klasyfikacja danych.....	133
8.6. Podsumowanie	135
Rozdział 9. Uściślanie projektu	137
9.1. Schematy blokowe	138
9.2. Wytyczne projektowe	140
9.2.1. Minimalizacja atakowanego obszaru	140
9.2.2. Przypisywanie możliwie niewielu przywilejów.....	141
9.2.3. Rozdzielanie zadań	142
9.2.4. Zagłębianie ochrony	143
9.2.5. Bezpieczne awarie	144
9.2.6. Domyślne bezpieczeństwo.....	144
9.2.7. Planowanie strategii obronnej.....	145
9.3. Modelowanie zagrożeń	145
9.4. Wzorce bezpieczeństwa	147
9.5. Projektowanie systemu kryptograficznego	148

9.5.1. Wyszukiwanie i profile	150
9.6. Podsumowanie	152
Rozdział 10. Bezpieczne tworzenie oprogramowania.....	153
10.1. Wskazówki bezpiecznego tworzenia oprogramowania.....	154
10.1.1. Czyszczenie wszystkich wejść i wyjść	154
10.1.2. Wykonywanie z możliwie małymi przywilejami	155
10.1.3. Usuwanie wrażliwych danych z pamięci	156
10.1.4. Zapisywanie wszystkich zdarzeń związanych z bezpieczeństwem.....	157
10.1.5. Sprawdzanie kodu i binariów	158
10.1.6. Test bezpieczeństwa jednostki.....	159
10.1.7. Korzystanie z przewodnika po bezpieczeństwie języka lub platformy	160
10.2. Podsumowanie	160
Rozdział 11. Testowanie.....	161
11.1. Funkcjonalne testowanie bezpieczeństwa	162
11.1.1. Kontrola dostępu.....	162
11.1.2. Czyszczenie danych.....	163
11.1.3. Dzienniki i monitorowanie	164
11.1.4. Popularne zagrożenia.....	165
11.1.5. Poufność informacji.....	165
11.1.6. Sprawdzanie zamiast testowania.....	166
11.2. Testy penetracyjne	166
11.3. Posumowanie	170
Rozdział 12. Wdrożenie, obrona i plan zamknięcia.....	171
12.1. Wdrożenie	171
12.2. Obrona	173
12.3. Plan zamknięcia	175
12.4. Podsumowanie	176
CZĘŚĆ IV. Przykładowy kod	177
Rozdział 13. O przykładach.....	179
13.1. Programy użytkowe i popularne usługi.....	180
13.2. Przykładowa maszyna i sejf na klucze.....	183
13.3. Podsumowanie	184
Rozdział 14. Sejf na klucze	185
14.1. Klucz lokalny	186
14.2. Lokalny skład kluczy	189
14.2.1. Generowanie klucza szyfrującego klucze	190

14.2.2. Generowanie klucza w lokalnym składzie kluczy	192
14.2.3. Szyfrowanie klucza.....	193
14.2.4. Zapisywanie klucza do składu kluczy.....	195
14.2.5. Zastępowanie klucza szyfrującego klucze	197
14.3. Dostęp do lokalnego klucza	200
14.4. Podsumowanie	201
Rozdział 15. Dokumentacja	203
15.1. Alias klucza.....	204
15.1.1. Tworzenie nowego aliasu klucza	206
15.1.2. Czytanie aliasu klucza z dokumentacji	208
15.1.3. Czytanie bieżącego żywego klucza.....	210
15.1.4. Zapisywanie aliasu klucza	211
15.1.5. Określanie stanu klucza	212
15.1.6. Zoptymalizowane sprawdzanie stanu	214
15.2. Podsumowanie	215
Rozdział 16. Menadżer kluczy	217
16.1. KeyTool	218
16.1.1. Interakcja z KeyTool	218
16.1.2. Generowanie klucza szyfrującego klucze	221
16.1.3. Ładowanie nowego klucza do składu kluczy.....	222
16.1.4. Oglądanie kluczy	223
16.1.5. Wycofywanie kluczy	225
16.1.6. Usuwanie kluczy.....	225
16.1.7. Aktualizacja oczekujących kluczy	227
16.2. Podsumowanie	231
Rozdział 17. Maszyna.....	233
17.1. Maszyna lokalna	233
17.2. Podsumowanie	236
Rozdział 18. Pokwitowania i dostawca	237
18.1. Wyniki żądań szyfrowania i odszyfrowania	237
18.2. Pokwitowania.....	238
18.2.1. Pokwitowanie kryptograficzne	239
18.2.2. Pokwitowanie złożone	239
18.3. Dostawca.....	241
18.3.1. Szyfrowanie danych biznesowych.....	241
18.3.2. Odszyfrowywanie danych biznesowych.....	242
18.3.3. Zastępowanie kluczy	244
18.4. Podsumowanie	244

Rozdział 19. Konsument	247
19.1. Informacja o kliencie	249
19.2. Informacje o karcie kredytowej	251
19.3. Menadżer klienta.....	252
19.3.1. Wykorzystanie menadżera klienta	253
19.3.2. Dodawanie klienta	255
19.3.3. Oglądanie rekordu klienta.....	258
19.3.4. Szukanie klientów.....	261
19.3.5. Zastępowanie klucza.....	263
19.4. Podsumowanie	267
Rozdział 20. Wyjątki	269
20.1. Wyjątek aliasu.....	269
20.2. Wyjątek niepoprawnego stanu klucza.....	269
20.3. Wyjątek związany z nieznalezieniem klucza	270
20.4. Wyjątek nieznalezienia żywego klucza.....	270
20.5. Wyjątek związany z wieloma ID aliasów	271
20.6. Wyjątek związany z nieznalezieniem klienta.....	272
20.7. Podsumowanie	272
Rozdział 21. Działający system.....	273
21.1. Określanie kluczy.....	273
21.1.1. Generowanie klucza szyfrującego klucze	273
21.1.2. Tworzenie nowego klucza	274
21.2. Praca z informacjami klienta.....	276
21.3. Zastępowanie klucza	278
21.4. Zastępowanie klucza szyfrującego klucze	282
21.5. Podsumowanie	283
Bibliografia	285
Słownik terminów.....	287
Słownik angielsko-polski.....	289
Skorowidz.....	291