

Spis treści

SŁOWO WSTĘPNE	12
PRZEDMOWA	14
PODZIĘKOWANIA	18
WPROWADZENIE	19
Kto powinien przeczytać tę książkę?	20
Jakie tematy są omawiane w książce?	21
Część I: Koncepcje	21
Część II: Projektowanie	22
Część III: Implementacja	22
Poślowie	23
Dodatki	23
Dobra, bezpieczna zabawa	23
CZĘŚĆ I. KONCEPCJE	25
1	
PODSTAWY	27
Zrozumieć bezpieczeństwo	28
Zaufanie	29
Obdarzanie zaufaniem	30
Nie możesz zobaczyć bitów	31
Kompetencja i niedoskonałość	31
Poziomy zaufania	32
Decyzje dotyczące zaufania	33
Komponenty, którym ufamy w sposób pośredni	34
Bycie wiarygodnym	35
Klasyczne zasady	36
Bezpieczeństwo informacji — C-I-A	36
Złoty standard	40
Prywatność	46

2		
ZAGROŻENIA		49
Perspektywa napastnika		50
Cztery pytania		52
Modelowanie zagrożeń		52
Praca na bazie modelu		54
Identyfikacja aktywów		55
Identyfikacja obszarów ataku		57
Określanie granic zaufania		58
Identyfikacja zagrożeń		60
Łagodzenie zagrożeń		67
Rozważania o ochronie prywatności		68
Modelowanie zagrożeń w każdym miejscu		69
3		
ŁAGODZENIE		71
Przeciwdziałanie zagrożeniom		72
Strukturalne strategie łagodzenia skutków		73
Minimalizuj obszary ataku		73
Zawężanie okienka podatności		74
Zminimalizuj ekspozycję danych		75
Polityka dostępu i kontrola dostępu		76
Interfejsy		78
Komunikacja		79
Przechowywanie danych		80
4		
WZORCE		82
Cechy projektu		83
Ekonomia projektowania		84
Przejrzysty projekt		85
Minimalizacja narażenia		86
Najmniejsze przywileje		86
Jak najmniej informacji		87
Bezpieczny z założenia		89
Listy dozwolonych zamiast List zabronionych		90
Unikaj przewidywalności		92
Bezpieczna awaria		93
Zdecydowane egzekwowanie reguł		94
Pełna mediacja		94
Jak najmniej współdzielonych mechanizmów		95
Nadmiarowość		96
Wielowarstwowa obrona		97
Rozdzielanie przywilejów		98

Zaufanie i odpowiedzialność	100
Zasada ograniczonego zaufania	100
Przyjmij odpowiedzialność za bezpieczeństwo	101
Antywzorce	103
Reprezentant wprowadzony w błąd	103
Przepływ zwrotny zaufania	106
Haczyki innych firm	107
Komponenty, których nie da się załatać	107

5

KRYPTOGRAFIA	109
Narzędzia kryptograficzne	110
Liczby losowe	111
Liczby pseudolosowe	111
Kryptograficznie bezpieczne liczby pseudolosowe	112
Kody uwierzytelniania komunikatów	113
Używanie MAC do zapobiegania manipulacjom	114
Ataki metodą powtórzenia	114
Bezpieczna łączność z użyciem MAC	115
Szyfrowanie symetryczne	116
Jednorazowy bloczek	116
Zaawansowany standard szyfrowania	118
Używanie kryptografii symetrycznej	118
Szyfrowanie asymetryczne	119
Kryptosystem RSA	120
Podpisy cyfrowe	121
Certyfikaty cyfrowe	123
Wymiana kluczy	124
Korzystanie z kryptografii	125

CZĘŚĆ II. PROJEKT **129**

6

PROJEKTOWANIE Z UWZGLĘDNIENIEM BEZPIECZEŃSTWA	131
Uwzględnianie bezpieczeństwa w projektowaniu	133
Zadbaj o wyraźne doprecyzowanie założeń projektowych	134
Określanie zakresu	135
Określanie wymagań dotyczących bezpieczeństwa	136
Modelowanie zagrożeń	138
Wprowadzanie środków łagodzących	140
Projektowanie interfejsów	141
Projektowanie obsługi danych	141
Uwzględnianie prywatności w projekcie	142
Planowanie pełnego cyklu życia oprogramowania	144
Osiąganie kompromisów	145
Prostota projektu	146

PRZEGLĄDY BEZPIECZEŃSTWA	148
Logistyka SDR	149
Po co przeprowadzać SDR?	149
Kiedy należy przeprowadzić SDR?	149
Dokumentacja jest niezbędna	150
Proces SDR	150
1. Przystudiuj projekt	151
2. Pytaj	152
3. Identyfikuj	152
4. Współpracuj	153
5. Pisz	154
6. Śledź dokonywane zmiany	156
Ocena bezpieczeństwa projektu	156
Wykorzystanie czterech pytań jako wskazówek	156
Na co zwracać uwagę	160
Przegląd związany z prywatnością	160
Przeglądy aktualizacji	161
Zarządzanie różnicą zdań	161
Komunikuj się w taktowny sposób	162
Studium przypadku: trudny przegląd	163
Eskalowanie braku porozumienia	165
Ćwicz, ćwicz, ćwicz	165

CZĘŚĆ III. IMPLEMENTACJA 167

PROGRAMOWANIE Z UWZGLĘDNIENIEM ASPEKTÓW BEZPIECZEŃSTWA	169
Wyzwania	171
Złośliwe działanie	172
Podatności na ataki są błędami	173
Łańcuchy podatności na zagrożenia	174
Błędy i entropia	176
Czułość	177
Studium przypadku: GotoFail	178
Jednoliniowa podatność	178
Uwaga na „strzał w stopę”	180
Wnioski z GotoFail	181
Podatność na błędy w kodowaniu	182
Niepodzielność	183
Ataki związane z pomiarem czasu	183
Serializacja	185
Typowi podejrzani	186

9	BŁĘDY W NISKOPOZIOMOWYM PROGRAMOWANIU	187
	Podatności związane z arytmetyką	188
	Błędy w zabezpieczeniach dla liczb całkowitych o stałej szerokości	189
	Luki w zabezpieczeniach precyzji zmiennoprzecinkowej	192
	Przykład: niedomiar wartości zmiennoprzecinkowych	193
	Przykład: przepełnienie liczby całkowitej	196
	Bezpieczna arytmetyka	198
	Luki w zabezpieczeniach dostępu do pamięci	200
	Zarządzanie pamięcią	200
	Przepełnienie bufora	201
	Przykład: podatność alokacji pamięci	202
	Studium przypadku: Heartbleed	206
10	NIEZAUFANE DANE WEJŚCIOWE	211
	Walidacja	212
	Poprawność danych	214
	Kryteria walidacji	215
	Odrzucanie nieprawidłowych danych wejściowych	216
	Poprawianie nieprawidłowych danych wejściowych	217
	Podatności w łańcuchach znaków	218
	Problemy z długością	219
	Problemy z kodowaniem Unicode	219
	Podatność na wstrzyknięcia	221
	Wstrzyknięcie SQL	222
	Trawersowanie ścieżek	225
	Wyrażenia regularne	227
	Niebezpieczeństwa związane z językiem XML	228
	Łagodzenie ataków typu wstrzyknięcie	229
11	BEZPIECZEŃSTWO SIECI WEB	231
	Buduj, korzystając z gotowych frameworków	233
	Model bezpieczeństwa sieciowego	234
	Protokół HTTP	235
	Certyfikaty cyfrowe i HTTPS	237
	Zasada tego samego pochodzenia	241
	Cookies	242
	Często spotykane podatności w sieci Web	244
	Skrypty międzywitrnowe (XSS)	245
	Fałszowanie żądania pomiędzy stronami (CSRF)	248
	Więcej podatności i środków łagodzących	250

12

TESTOWANIE BEZPIECZEŃSTWA253

Czym jest testowanie bezpieczeństwa?	254
Testowanie bezpieczeństwa na przykładzie podatności GotoFail	255
Testy funkcjonalne	257
Testy funkcjonalne z wykorzystaniem podatności	258
Przypadki testowe do testowania bezpieczeństwa	258
Ograniczenia testów bezpieczeństwa	259
Pisanie przypadków testowych do testów bezpieczeństwa	260
Testowanie walidacji danych wejściowych	261
Testowanie podatności na ataki XSS	261
Testowanie odporności na błędne dane	264
Testy regresji bezpieczeństwa	265
Testowanie dostępności	267
Zużycie zasobów	267
Badanie progu	268
Rozproszone ataki typu Denial-of-Service	270
Najlepsze praktyki w testowaniu zabezpieczeń	270
Rozwój oprogramowania oparty na testach	270
Wykorzystanie testów integracyjnych	271
Testy bezpieczeństwa — nadrabianie zaległości	271

13

NAJLEPSZE PRAKTYKI W TWORZENIU BEZPIECZNYCH PROJEKTÓW273

Jakość kodu	274
Higiena kodu	274
Obsługa wyjątków i błędów	275
Dokumentowanie bezpieczeństwa	276
Przeglądy kodu pod kątem bezpieczeństwa	277
Zależności	278
Wybieranie bezpiecznych komponentów	278
Zabezpieczanie interfejsów	279
Nie wymyślaj na nowo koła w bezpieczeństwie	280
Postępowanie z przestarzałymi zabezpieczeniami	281
Klasyfikowanie zagrożeń	282
Oceny DREAD	282
Tworzenie działających exploitów	284
Podejmowanie decyzji w triażu	284
Zabezpieczanie środowiska programistycznego	285
Oddzielenie prac rozwojowych od produkcji	286
Zabezpieczanie narzędzi programistycznych	286
Wypuszczanie produktu na rynek	287

POŚŁOWIE	288
Wezwanie do działania	289
Bezpieczeństwo to zadanie każdego z nas	290
Zaprawiony w bezpieczeństwie	291
Bezpieczeństwo w przyszłości	292
Poprawa jakości oprogramowania	293
Zarządzanie złożonością	293
Od minimalizowania do maksymalizowania przejrzystości	294
Zwiększanie autentyczności, zaufania i odpowiedzialności oprogramowania	295
Dostarczanie na ostatnim kilometrze	297
Wnioski	301
 A	
PRZYKŁADOWA DOKUMENTACJA PROJEKTOWA	302
Tytuł: dokument projektowy komponentu rejestrującego prywatne dane	303
Spis treści	303
Sekcja 1. Opis produktu	303
Sekcja 2. Przegląd	304
2.1. Cel	304
2.2. Zakres	304
2.3. Pojęcia	304
2.4. Wymagania	306
2.5. Cele poza zakresem projektu	306
2.6. nierozstrzygnięte kwestie	307
2.7. Alternatywne rozwiązania	307
Sekcja 3. Przypadki użycia	308
Sekcja 4. Architektura systemu	308
Sekcja 5. Projekt danych	309
Sekcja 6. Interfejsy API	311
6.1. Żądanie Witaj	311
6.2. Żądanie definicji schematu	312
6.3. Żądanie dziennika zdarzeń	312
6.4. Żądanie Żegnaj	312
Sekcja 7. Projekt interfejsu użytkownika	313
Sekcja 8. Projekt techniczny	314
Sekcja 9. Konfiguracja	315
Sekcja 10. Odwołania	316
 B	
SŁOWNICZEK	317
 C	
ĆWICZENIA	326
 D	
ŚCIĄGI	332