

Inżynieria zabezpieczeń : przewodnik po budowaniu niezawodnych systemów rozproszonych. Tom 1 / Ross Anderson. – Wydanie I. – Warszawa, 2024

Spis treści

Przedmowa do wydania trzeciego	XXVII
Przedmowa do wydania drugiego	XXXI
Przedmowa do wydania pierwszego	XXXIII
Dla mojej córki oraz innych prawników	XXXIX
Wstęp	XLI
Część I	1
Rozdział 1 Czym jest inżynieria zabezpieczeń?	3
1.1. Wprowadzenie	3
1.2. Schemat pojęciowy	4
1.3. Przykład 1: bank	6
1.4. Przykład 2: baza wojskowa	8
1.5. Przykład 3: szpital	10
1.6. Przykład 4: dom	11
1.7. Definicje	13
1.8. Podsumowanie	18
Rozdział 2 Kim jest przeciwnik?	21
2.1. Wprowadzanie	21
2.2. Szpiedzy	23
2.2.1. Sojusz Pięciorga Oczu	24
2.2.1.1. Prism	24
2.2.1.2. Tempora	25
2.2.1.3. Muscular	26
2.2.1.4. Program SCS	27
2.2.1.5. Bullrun i Edgehill	28
2.2.1.6. Xkeyscore	29
2.2.1.7. Longhaul	30
2.2.1.8. Quantum	31
2.2.1.9. CNE	31
2.2.1.10. Z punktu widzenia analityka	33
2.2.1.11. Operacje ofensywne	34

2.2.1.12. Skalowanie ataku	35
2.2.2. Chiny	36
2.2.3. Rosja	42
2.2.4. Pozostali	46
2.2.5. Przypisywanie	49
2.3. Oszuści	50
2.3.1. Infrastruktura przestępcza	51
2.3.1.1. Pasterze botów	52
2.3.1.2. Twórcy złośliwego oprogramowania	54
2.3.1.3. Osoby rozsyłające spam	55
2.3.1.4. Włamania do kont na dużą skalę	55
2.3.1.5. Osoby zajmujące się atakami na konkretne cele	56
2.3.1.6. Gangi zajmujące się zamianą na gotówkę	56
2.3.1.7. Ransomware	57
2.3.2. Ataki na bankowość i systemy płatnicze	58
2.3.3. Sektorowe ekosystemy cyberprzestępczości	59
2.3.4. Ataki wewnętrzne	60
2.3.5. Przestępstwa prezesów	60
2.3.6. Sygnaliści	62
2.4. Maniacy komputerowi	64
2.5. Bagno	65
2.5.1. Haktywizm i kampanie nienawiści	65
2.5.2. Materiały przedstawiające seksualne wykorzystywanie dzieci	68
2.5.3. Nękanie w szkole i w miejscu pracy	69
2.5.4. Nadużycia w związkach intymnych	70
2.6. Podsumowanie	72
Problemy badawcze	73
Materiały uzupełniające	74
Rozdział 3 Psychologia i użyteczność	75
3.1. Wprowadzenie	75
3.2. Spostrzeżenia z badań psychologicznych	77
3.2.1. Psychologia poznawcza	77
3.2.2. Płeć, różnorodność i zmienność interpersonalna	81
3.2.3. Psychologia społeczna	84
3.2.3.1. Autorytet i jego nadużywanie	84
3.2.3.2. Efekt obojętnego przechodnia	85
3.2.4. Teoria mózgu społecznego a oszustwa	86
3.2.5. Heurystyki, tendencyjność i ekonomia behawioralna	91
3.2.5.1. Teoria perspektywy i błędna percepcja ryzyka	91
3.2.5.2. Skłanianie się ku stanowi obecnemu i hiperboliczne obniżenie wartości	93
3.2.5.3. Domyślne warunki i impulsy	93
3.2.5.4. Domyślna intencjonalność	94
3.2.5.5. Heurystyka afektu	95

3.2.5.6. Dysonans poznawczy	96
3.2.5.7. Termostatyczny model ryzyka	96
3.3. Oszustwa w praktyce	97
3.3.1. Sprzedawca i oszust	97
3.3.2. Socjotechnika	100
3.3.3. Phishing	102
3.3.4. Zabezpieczenie operacyjne	105
3.3.5. Badanie oszustw	107
3.4. Hasła	108
3.4.1. Odzyskiwanie haseł	109
3.4.2. Wybór hasła	112
3.4.3. Trudności z niezawodnym wprowadzaniem haseł	112
3.4.4. Trudności z zapamiętaniem hasła	113
3.4.4.1. Naiwny wybór	114
3.4.4.2. Umiejętności użytkowników i ich szkolenie	115
3.4.4.3. Błędy projektowe	117
3.4.4.4. Zaniedbania operacyjne	119
3.4.4.5. Ataki wykorzystujące socjotechnikę	120
3.4.4.6. Edukowanie klientów	121
3.4.4.7. Ostrzeżenie przed phishingiem	122
3.4.5. Problemy systemowe	123
3.4.6. Czy można odmówić dostępu do usługi?	124
3.4.7. Chronić siebie czy innych?	125
3.4.8. Ataki związane z wprowadzaniem hasła	126
3.4.8.1. Projekt interfejsu	126
3.4.8.2. Zaufana ścieżka i fałszywe terminale	126
3.4.8.3. Techniczne porażki liczników prób wprowadzenia hasła	127
3.4.9. Ataki na miejsca przechowywania hasła	128
3.4.9.1. Szyfrowanie jednokierunkowe	129
3.4.9.2. Łamanie haseł	129
3.4.9.3. Zdalne sprawdzanie haseł	130
3.4.10. Bezwzględne granice	130
3.4.11. Korzystanie z menedżera haseł	132
3.4.12. Czy kiedykolwiek pozbędziemy się haseł?	133
3.5. CAPTCHA	136
3.6. Podsumowanie	137
Problemy badawcze	138
Materiały uzupełniające	139

Rozdział 4 Protokoły **141**

4.1. Wprowadzenie	141
4.2. Ryzyko związane z podsłuchiowaniem haseł	143
4.3. „Stać, kto idzie?!”, czyli proste uwierzytelnianie	144
4.3.1. Wyzwanie i odpowiedź	147
4.3.2. Uwierzytelnianie dwuskładnikowe	151

4.3.3. Atak z MIG-iem jako pośrednikiem	153
4.3.4. Ataki metodą odbicia lustrzanego	156
4.4. Manipulowanie wiadomościami	158
4.5. Zmiana środowiska	158
4.6. Ataki na wybrany protokół	159
4.7. Zarządzanie kluczami szyfrującymi	161
4.7.1. „Ożywianie kaczątka"	161
4.7.2. Zdalne zarządzanie kluczami	162
4.7.3. Protokół Needhama-Schroedera	163
4.7.4. Kerberos	164
4.7.5. Praktyczne zarządzanie kluczami	166
4.8. Zapewnienie bezpieczeństwa projektu	167
4.9. Podsumowanie	168
Problemy badawcze	169
Materiały uzupełniające	169

Rozdział 5 Kryptografia **171**

5.1. Wprowadzenie	171
5.2. Tło historyczne	173
5.2.1. Szyfr Vigenère'a jako przykład wczesnego szyfru strumieniowego	174
5.2.2. Szyfr z kluczem jednorazowym	175
5.2.3. Szyfr Playfair - wczesny szyfr blokowy	177
5.2.4. Funkcje skrótu	179
5.2.5. Podstawowe elementy asymetryczne	181
5.3. Modele bezpieczeństwa	182
5.3.1. Funkcje losowe - funkcje skrótu	184
5.3.1.1. Własności	185
5.3.1.2. Twierdzenie o dniu urodzin	185
5.3.2. Generatory losowe - szyfry strumieniowe	187
5.3.3. Losowe permutacje - szyfry blokowe	189
5.3.4. Szyfrowanie z kluczem publicznym i jednokierunkowe permutacje z zapadką	191
5.3.5. Podpisy cyfrowe	192
5.4. Symetryczne algorytmy kryptograficzne	193
5.4.1. Sieci SP	194
5.4.1.1. Rozmiar bloku	195
5.4.1.2. Liczba rund	195
5.4.1.3. Dobór S-boksów	196
5.4.1.4. Kryptoanaliza liniowa	196
5.4.1.5. Kryptoanaliza różnicowa	196
5.4.2. AES	198
5.4.3. Szyfry Feistela	200
5.4.3.1. Wyniki Luby'ego-Rackoffa	202
5.4.3.2. DES	202
5.5. Tryby działania	205

5.5.1. Jak nie używać szyfru blokowego	205
5.5.2. Wiązanie bloków zaszyfrowanych	207
5.5.3. Szyfrowanie z licznikiem	208
5.5.4. Starsze tryby szyfrów strumieniowych	209
5.5.5. Kod uwierzytelniania wiadomości	209
5.5.6. Tryb licznika Galois	210
5.5.7. XTS	211
5.6. Funkcje skrótu	211
5.6.1. Powszechnie stosowane funkcje skrótu	212
5.6.2. Zastosowania funkcji skrótu - HMAC, zobowiązania i aktualizowanie	214
5.7. Asymetryczne podstawowe elementy kryptograficzne	216
5.7.1. Kryptografia oparta na faktoryzacji (rozkładzie na czynniki pierwsze)	216
5.7.2. Kryptografia oparta na logarytmach dyskretnych	220
5.7.2.1. Jednokierunkowe szyfrowanie przemienne	220
5.7.2.2. Wymiana klucza Diffiego-Hellmana	221
5.7.2.3. Podpis cyfrowy ElGamala i DSA	224
5.7.3. Kryptografia oparta na krzywych eliptycznych	225
5.7.4. Urzędy certyfikacji	226
5.7.5. TLS	228
5.7.5.1. Zastosowania TLS	229
5.7.5.2. Zabezpieczenia TLS	229
5.7.5.3. TLS 1.3	230
5.7.6. Inne protokoły z kluczem publicznym	230
5.7.6.1. Podpisywanie kodu	230
5.7.6.2. PGP/GPG	231
5.7.6.3. QUIC	232
5.7.7. Elementy podstawowe specjalnego przeznaczenia	232
5.7.8. Jak mocne są asymetryczne podstawowe elementy kryptograficzne?	234
5.7.9. Co jeszcze idzie nie tak	236
5.8. Podsumowanie	237
Problemy badawcze	238
Materiały uzupełniające	238
Rozdział 6 Kontrola dostępu	241
6.1. Wprowadzenie	241
6.2. Kontrola dostępu systemu operacyjnego	243
6.2.1. Grupy i role	245
6.2.2. Listy kontroli dostępu	246
6.2.3. Zabezpieczenia systemu operacyjnego Unix	247
6.2.4. Możliwości dostępu	249
6.2.5. DAC oraz MAC	250
6.2.6. MacOS firmy Apple	252

6.2.7. iOS	253
6.2.8. Android	254
6.2.9. Windows	255
6.2.10. Oprogramowanie pośredniczące	258
6.2.10.1. Środki kontroli dostępu do bazy danych	259
6.2.10.2. Przeglądarki	260
6.2.11. Sandboxing (piaskownicowanie)	261
6.2.12. Wirtualizacja	261
6.3. Ochrona sprzętu	264
6.3.1. Procesory Intela	265
6.3.2. Procesory ARM	267
6.4. Co idzie nie tak	269
6.4.1. Przepełnienie bufora na stosie	271
6.4.2. Inne ataki techniczne	272
6.4.3. Usterki interfejsu użytkownika	275
6.4.4. Środki zaradcze	276
6.4.5. Pełzanie środowiska	278
6.5. Podsumowanie	279
Problemy badawcze	279
Materiały uzupełniające	280

Rozdział 7 Systemy rozproszone **283**

7.1. Wprowadzenie	283
7.2. Współbieżność	284
7.2.1. Użycie starych danych a płacenie za propagację stanu	285
7.2.2. Blokowanie w celu zapobieżenia niespójnym aktualizacjom	287
7.2.3. Kolejność aktualizacji	288
7.2.4. Zakleszczenie	289
7.2.5. Stan niezbieżny	290
7.2.6. Bezpieczny czas	291
7.3. Odporność na uszkodzenia i odzyskiwanie danych po awarii	292
7.3.1. Modele awarii	293
7.3.1.1. Awaria bizantyjska	293
7.3.1.2. Interakcja z odpornością na awarie	294
7.3.2. Czemu służy odporność?	296
7.3.3. Na jakim poziomie jest redundancja?	297
7.3.4. Ataki polegające na odmowie usługi	299
7.4. Nazewnictwo	300
7.4.1. Zasady nazewnictwa Needhama	302
7.4.2. Co jeszcze idzie nie tak	305
7.4.2.1. Nazewnictwo i tożsamość	306
7.4.2.2. Przesłanki kulturowe	307
7.4.2.3. Semantyczna zawartość nazw	310
7.4.2.4. Niepowtarzalność nazw	310
7.4.2.5. Stabilność nazw i adresów	311

7.4.2.6. Restrykcje w używaniu nazw	312
7.4.3. Rodzaje nazw	313
7.5. Podsumowanie	314
Problemy badawcze	315
Materiały uzupełniające	316

Rozdział 8 Ekonomia **317**

8.1. Wprowadzenie	317
8.2. Ekonomia klasyczna	319
8.2.1. Monopol	320
8.3. Ekonomia informacji	323
8.3.1. Dlaczego rynki informacji są inne?	324
8.3.2. Wartość uzależnienia od dostawcy	325
8.3.3. Asymetria informacji	327
8.3.4. Dobra publiczne	328
8.4. Teoria gier	329
8.4.1. Dylemat więźnia	331
8.4.2. Gry powtarzalne i ewolucyjne	332
8.5. Teoria aukcji	334
8.6. Ekonomia bezpieczeństwa i niezawodności	337
8.6.1. Dlaczego system Windows jest tak słabo zabezpieczony?	338
8.6.2. Zarządzanie cyklem wprowadzania poprawek	340
8.6.3. Modele strukturalne ataku i obrony	343
8.6.4. Ekonomia uzależnień od dostawcy, sprzedaży związanej i DRM	345
8.6.5. Regulacje antymonopolowe i polityka konkurencji	347
8.6.6. Przewrotnie zmotywowana ochrona	350
8.6.7. Ekonomia prywatności	351
8.6.8. Zachowania organizacji i ludzi	354
8.6.9. Ekonomia cyberprzestępczości	355
8.7. Podsumowanie	357
Problemy badawcze	357
Materiały uzupełniające	358

Część II **361**

Rozdział 9 Zabezpieczenia wielopoziomowe **363**

9.1. Wprowadzenie	363
9.2. Czym jest model polityki bezpieczeństwa?	364
9.3. Polityka zabezpieczeń wielopoziomowych	366
9.3.1. Raport Andersona	368
9.3.2. Model Bella-LaPaduli	369
9.3.3. Standardowa krytyka modelu Bella-LaPaduli	370
9.3.4. Ewolucja polityk zabezpieczeń wielopoziomowych (MLS)	372
9.3.5. Model Biby	374
9.4. Historyczne przykłady systemów zabezpieczeń wielopoziomowych	376

9.4.1. SCOMP	376
9.4.2. Diody danych	377
9.5. MAC: od zabezpieczeń wielopoziomowych (MLS) do kontroli przepływu informacji (IFC) i integralności	380
9.5.1. Windows	380
9.5.2. SELinux	380
9.5.3. Systemy wbudowane	381
9.6. Co idzie nie tak	382
9.6.1. Możliwość komponowania	382
9.6.2. Problem kaskady	383
9.6.3. Ukryte kanały	383
9.6.4. Zagrożenia złośliwym oprogramowaniem	384
9.6.5. Wieloinstancyjność	385
9.6.6. Praktyczne problemy z zabezpieczeniami wielopoziomowymi	386
9.7. Podsumowanie	389
Problemy badawcze	389
Materiały uzupełniające	391

Rozdział 10 Granice przestrzeni osobistej 393

10.1. Wprowadzenie	393
10.2. Przedzielanie i model kratowy	396
10.3. Prywatność dla tygrysów	399
10.4. Prywatność dokumentacji medycznej	402
10.4.1. Model zagrożeń	405
10.4.2. Polityka bezpieczeństwa BMA	407
10.4.3. Pierwsze kroki praktyczne	410
10.4.4. Co faktycznie idzie nie tak	411
10.4.4.1. Opieka w nagłych wypadkach	413
10.4.4.2. Odporność	414
10.4.4.3. Wykorzystanie wtórne	414
10.4.5. Poufność - przyszłość	418
10.4.6. Etyka	420
10.4.7. Opieka społeczna i edukacja	423
10.4.8. Model chińskiego muru	425
10.5. Podsumowanie	427
Problemy badawcze	428
Materiały uzupełniające	429

Rozdział 11 Kontrola wnioskowania 431

11.1. Wprowadzenie	431
11.2. Początki kontroli wnioskowania	433
11.2.1. Podstawowa teoria kontroli wnioskowania	434
11.2.1.1. Kontrola rozmiaru zbioru dla zapytań	435
11.2.1.2. Trackery	435
11.2.1.3. Ukrywanie komórek	435

11.2.1.4. Inne mechanizmy kontroli ujawniania danych statystycznych	437
11.2.1.5. Bardziej zaawansowana kontrola zapytań	438
11.2.1.6. Randomizacja	439
11.2.2. Granice klasycznych zabezpieczeń statystycznych	439
11.2.3. Ataki aktywne	441
11.2.4. Kontrola wnioskowania przy obszernych danych medycznych	442
11.2.5. Trzecia tura: preferencje i wyszukiwanie	446
11.2.6. Czwarta tura: lokalizacja i społeczeństwo	447
11.3. Prywatność różnicowa	450
11.4. Co zrobić z tą luką?	452
11.4.1. Anonimowość taktyczna i jej problemy	454
11.4.2. Pobudki	457
11.4.3. Możliwości	458
11.4.4. Ciemna strona	459
11.5. Podsumowanie	461
Problemy badawcze	462
Materiały uzupełniające	462

Rozdział 12 Bankowość i księgowość 465

12.1. Wprowadzenie	465
12.2. Systemy księgowe	467
12.2.1. Reguła podwójnego zapisu	468
12.2.2. Księgowość w bankach	469
12.2.3. Model polityki zabezpieczeń Clarka-Wilsona	470
12.2.4. Projektowanie kontroli wewnętrznych	471
12.2.5. Oszustwa wewnętrzne	476
12.2.6. Oszustwa na szczeblu dyrekcji	477
12.2.6.1. Przypadek poczty	479
12.2.6.2. Inne awarie	480
12.2.6.3. Ekologiczna zasadność	481
12.2.6.4. Dostrajanie kontroli i rządy korporacyjne	482
12.2.7. Znajdowanie słabych punktów	483
12.3. Międzybankowe systemy płatności	485
12.3.1. Historia e-handlu w telegraficznym skrócie	485
12.3.2. SWIFT	486
12.3.3. Co idzie nie tak	488
12.4. Bankomaty	491
12.4.1. Podstawy bankomatów	492
12.4.2. Co idzie nie tak	494
12.4.3. Pobudki i niesprawiedliwość	499
12.5. Karty kredytowe	500
12.5.1. Oszustwa związane z kartami kredytowymi	501
12.5.2. Internetowe oszustwa związane z kartami	503
12.5.3. 3DS	506
12.5.4. Mechanizmy wykrywania oszustw	506

12.6. Karty płatnicze EMV	508
12.6.1. Karty chipowe	508
12.6.1.1. Statyczne uwierzytelnianie danych	509
12.6.1.2. ICW, DDA i CDA	514
12.6.1.3. Atak typu No-PIN	515
12.6.2. Atak typu preplay	516
12.6.3. Płatności zbliżeniowe	518
12.7. Bankowość internetowa	521
12.7.1. Phishing	521
12.7.2. CAP	523
12.7.3. Złośliwe oprogramowanie bankowe	523
12.7.4. Telefon jako drugi czynnik	524
12.7.5. Odpowiedzialność	525
12.7.6. Oszustwa związane z autoryzowanymi płatnościami inicjowanymi przez płatnika	526
12.8. Płatności pozabankowe	528
12.8.1. M-Pesa	528
12.8.2. Inne telefoniczne systemy płatności	529
12.8.3. Sofort i otwarta bankowość	529
12.9. Podsumowanie	531
Problemy badawcze	531
Materiały uzupełniające	533
Rozdział 13 Zamki i alarmy	535
13.1. Wprowadzenie	535
13.2. Zagrożenia i bariery	536
13.2.1. Model zagrożenia	537
13.2.2. Odstraszanie	538
13.2.3. Ściany i bariery	541
13.2.4. Zamki mechaniczne	542
13.2.5. Zamki elektroniczne	547
13.3. Alarmy	550
13.3.1. Jak nie chronić obrazu	551
13.3.2. Pokonywanie czujników	552
13.3.3. Współdziałanie różnych elementów	555
13.3.4. Ataki na komunikację	556
13.3.5. Wnioski	559
13.4. Podsumowanie	560
Problemy badawcze	561
Materiały uzupełniające	562
Rozdział 14 Monitorowanie i pomiary	563
14.1. Wprowadzenie	563
14.2. Tokeny przedpłatowe	565
14.2.1. Pomiary zużycia mediów	566

14.2.2. Jak działa system STS	567
14.2.3. Co idzie nie tak	569
14.2.4. Inteligentne liczniki i inteligentne sieci	571
14.2.5. Oszustwa związane z biletami	575
14.3. Taksometry tachografy i ograniczniki prędkości dla ciężarówek	576
14.3.1. Tachograf	577
14.3.2. Co idzie nie tak	579
14.3.2.1. Jak dokonuje się większości manipulacji tachografem	579
14.3.2.2. Majstrowanie przy zasilaniu	580
14.3.2.3. Majstrowanie przy przyrządzie	581
14.3.2.4. Zaawansowane ataki technologicznie	581
14.3.3. Tachografy cyfrowe	582
14.3.3.1. Problemy systemowe	583
14.3.3.2. Inne problemy	584
14.3.4. Ataki na czujniki i urządzenia trzeciej generacji	586
14.3.5. Czwarta generacja - inteligentne tachografy	587
14.4. Elektroniczne lokalizatory: GPS jako policjant	588
14.5. Frankownice	592
14.6. Podsumowanie	596
Problemy badawcze	597
Materiały uzupełniające	597

Bibliografia

B-1

oprac. BPK