

Inżynieria zabezpieczeń : przewodnik po budowaniu niezawodnych systemów rozproszonych. Tom 2 / Ross Anderson. – Wydanie I. – Warszawa, 2024

Spis treści

Rozdział 15 Nadzór nad bronią jądrową	599
15.1. Wprowadzenie	599
15.2. Ewolucja dowodzenia i nadzoru	602
15.2.1. Memorandum Kennedy’ego	603
15.2.2. Autoryzacja, otoczenie, zamiar	604
15.3. Bezwarunkowo bezpieczne uwierzytelnianie	605
15.4. Schematy współdzielonego nadzoru	607
15.5. Odporność na manipulacje i zabezpieczenia PAL	609
15.6. Weryfikacja zachowania traktatów	611
15.7. Co idzie nie tak	612
15.7.1. Zdarzenia jądrowe	612
15.7.2. Związek z cyberwojną	613
15.7.3. Porażki techniczne	615
15.8. Tajność czy jawność?	616
15.9. Podsumowanie	617
Problemy badawcze	618
Materiały uzupełniające	618
 Rozdział 16 Zabezpieczenia drukarskie, plomby i pieczęcie	 621
16.1. Wprowadzenie	621
16.2. Historia	622
16.3. Zabezpieczenia drukarskie	623
16.3.1. Model zagrożeń	624
16.3.2. Techniki zabezpieczeń drukarskich	625
16.4. Opakowania i plomby	630
16.4.1. Właściwości podłoża	631
16.4.2. Problemy z klejem	632
16.4.3. Przesyłki z PIN-em	633
16.5. Systemowe luki w zabezpieczeniach	634
16.5.1. Specyfika modelu zagrożeń	635
16.5.2. Środki przeciwko nieuczciwości	636
16.5.3. Skutki przypadkowych uszkodzeń	637
16.5.4. Nadzór nad materiałami	638
16.5.5. Brak ochrony właściwych rzeczy	639
16.5.6. Koszt i charakter kontroli	640
16.6. Metodyka oceny	641
16.7. Podsumowanie	643
Problemy badawcze	643
Materiały uzupełniające	644

Rozdział 17 Biometria	647
17.1. Wprowadzenie	647
17.2. Podpisy odręczne	648
17.3. Rozpoznawanie twarzy	651
17.4. Odciski palców	657
17.4.1. Pozytywna i negatywna weryfikacja tożsamości	658
17.4.2. Techniki śledcze na miejscu przestępstwa	662
17.5. Kod tęczówki	666
17.6. Rozpoznawanie i przekształcanie głosu	669
17.7. Inne systemy	670
17.8. Co idzie nie tak	672
17.9. Podsumowanie	676
Problemy badawcze	677
Materiały uzupełniające	677
 Rozdział 18 Odporność na fizyczną penetrację sprzętu	 679
18.1. Wprowadzenie	679
18.2. Historia	681
18.3. Sprzętowe moduły zabezpieczeń	682
18.4. Ocena	688
18.5. Karty inteligentne i inne chipy zabezpieczające	690
18.5.1. Historia	690
18.5.2. Architektura	691
18.5.3. Ewolucja zabezpieczeń	692
18.5.4. Generatory liczb losowych i funkcje fizycznie nieklonowalne	704
18.5.5. Większe chipy	707
18.5.6. Aktualny stan wiedzy	712
18.6. Ryzyko rezydualne	714
18.6.1. Problem z zaufanym interfejsem	714
18.6.2. Konflikty	716
18.6.3. Rynek bubli, dumping ryzyka i gry w ocenianie	716
18.6.4. Zabezpieczanie przez zaciemnianie	717
18.6.5. Zmieniające się środowiska	718
18.7. Co zatem należy chronić?	719
18.8. Podsumowanie	721
Problemy badawcze	721
Materiały uzupełniające	721
 Rozdział 19 Ataki przez boczny kanał	 723
19.1. Wprowadzenie	723
19.2. Zabezpieczanie emisji	724
19.2.1. Historia	725
19.2.2. Techniczna inwigilacja i środki zaradcze	726
19.3. Ataki pasywne	729
19.3.1. Wycieki przez przewody zasilające i sygnałowe	730
19.3.2. Wycieki przez sygnały częstotliwości radiowych	730

19.3.3. Co idzie nie tak	735
19.4. Ataki między komputerami i wewnątrz nich	736
19.4.1. Analiza czasowa	737
19.4.2. Analiza mocy	737
19.4.3. Zakłócanie i różnicowa analiza błędów	741
19.4.4. Rowhammer, CLKScrew i Plundervolt	742
19.4.5. Meltdown, Spectre i inne ataki przez boczny kanał na enklawy	744
19.5. Środowiskowe wycieki przez boczny kanał	746
19.5.1. Akustyczne wycieki przez boczny kanał	746
19.5.2. Optyczne wycieki przez boczny kanał	748
19.5.3. Inne wycieki przez boczny kanał	749
19.6. Społecznościowe wycieki przez boczny kanał	750
19.7. Podsumowanie	751
Problemy badawcze	751
Materiały uzupełniające	752
Rozdział 20 Zaawansowana inżynieria kryptograficzna	755
20.1. Wprowadzenie	755
20.2. Szyfrowanie całego dysku	757
20.3. Signal	759
20.4. Tor	763
20.5. HSM-y	766
20.5.1. Atak XOR-em prowadzący do klucza z samych zer	767
20.5.2. Ataki wykorzystujące kompatybilność wsteczną i analizę czasowo-pamięciową	768
20.5.3. Różnicowa analiza protokołów	769
20.5.4. Atak na EMY	771
20.5.5. Hakowanie modułów HSM w urządzeniach certyfikacji i w chmurze	771
20.5.6. Zarządzanie ryzykiem HSM	772
20.6. Enklawy	772
20.7. Łańcuchy bloków	776
20.7.1. Portfele kryptowalutowe	779
20.7.2. Górnicy	780
20.7.3. Smart kontrakty	781
20.7.4. Mechanizmy płatności poza głównym łańcuchem	782
20.7.5. Giełdy, kryptoprzestępczość i regulacje	783
20.7.6. Współdzielone bazy danych o strukturach łańcuchów bloków	787
20.8. Kryptomarzenia, które upadły	788
20.9. Podsumowanie	788
Problemy badawcze	790
Materiały uzupełniające	791
Rozdział 21 Ataki i obrona w sieci	793
21.1. Wprowadzenie	793
21.2. Protokoły sieciowe i odmowa usług	795
21.2.1. Zabezpieczenia BGP	796
21.2.2. Zabezpieczenia DNS	798

21.2.3. UDP, TCP, SYN flood i SYN reflection	799
21.2.4. Inne ataki z powielaniem pakietów	800
21.2.5. Inne rodzaje ataków polegających na odmowie usługi	801
21.2.6. E-mail - od szpiegów do spamerów	802
21.3. Menażeria złośliwego oprogramowania - trojany, robaki i RAT	804
21.3.1. Wczesna historia złośliwego oprogramowania	805
21.3.2. Robak internetowy	806
21.3.3. Dalsza ewolucja złośliwego oprogramowania	807
21.3.4. Jak działa złośliwe oprogramowanie	809
21.3.5. Środki zapobiegawcze	810
21.4. Obrona przed atakami sieciowymi	812
21.4.1 Filtrowanie: zapory sieciowe, kontrolowanie treści i podsłuchy	814
21.4.1.1. Filtrowanie pakietów	814
21.4.1.2. Bramy transmisyjne	815
21.4.1.3. Pośrednicy aplikacji	815
21.4.1.4. Filtrowanie ruchu przychodzącego i wychodzącego	816
21.4.1.5. Architektura	816
21.4.2. Wykrywanie włamań	819
21.4.2.1. Rodzaje metod wykrywania włamań	820
21.4.2.2. Ogólne ograniczenia związane z wykrywaniem włamań	821
21.4.2.3. Specyficzne problemy związane z wykrywaniem ataków sieciowych	821
21.5. Kryptografia: poszarpana granica	823
21.5.1. SSH	823
21.5.2. Sieci bezprzewodowe na krańcach	824
21.5.2.1. Wi-fi	825
21.5.2.2. Bluetooth	826
21.5.2.3. HomePlug	826
21.5.2.4. Sieci VPN	827
21.6. Urzędy certyfikacji i PKI	827
21.7. Topologia	831
21.8. Podsumowanie	832
Problemy badawcze	833
Materiały uzupełniające	833

Rozdział 22 Telefony **835**

22.1. Wprowadzenie	835
22.2. Ataki na sieci telefoniczne	836
22.2.1. Ataki na systemy poboru opłat za połączenia	837
22.2.2. Ataki na przesyłanie sygnałów sterujących	840
22.2.3. Ataki na łącznice i konfiguracje	841
22.2.4. Niezabezpieczone systemy końcowe	843
22.2.5. Interakcja funkcji	846
22.2.6. VOIP	847
22.2.7. Oszustwa firm telekomunikacyjnych	848
22.2.8. Ekonomia zabezpieczeń w telekomunikacji	849
22.3. Idąc w mobilność	850

22.3.1. GSM	851
22.3.2. 3G	856
22.3.3. 4G	858
22.3.4. 5G i dalej	859
22.3.5. Główne problemy operatorów sieci komórkowych	861
22.4. Zabezpieczenia platformy	863
22.4.1. Ekosystem aplikacji na Androida	865
22.4.1.1. Rynki aplikacji i programiści	866
22.4.1.2. Kiepskie implementacje Androida	867
22.4.1.3. Uprawnienia	868
22.4.1.4. Androidowe złośliwe oprogramowanie	870
22.4.1.5. Reklamy i usługi stron trzecich	872
22.4.1.6. Preinstalowane aplikacje	873
22.4.2. Ekosystem aplikacji Apple'a	874
22.4.3. Problemy przekrojowe	878
22.5. Podsumowanie	879
Problemy badawcze	880
Materiały uzupełniające	881
Rozdział 23 Wojny elektroniczne i informacyjne	883
23.1. Wprowadzenie	883
23.2. Podstawy	884
23.3. Systemy komunikacyjne	885
23.3.1. Techniki rozpoznania elektromagnetycznego	887
23.3.2. Ataki na łączność	890
23.3.3. Techniki ochrony	892
23.3.3.1. Skokowe zmiany częstotliwości	893
23.3.3.2. DSSS	894
23.3.3.3. Transmisja paczkowa	896
23.3.3.4. Łączenie skrytości i odporności na zakłócanie	896
23.3.4. Interakcja między zastosowaniami cywilnymi i wojskowymi	898
23.4. Inwigilacja i namierzanie celu	899
23.4.1. Rodzaje radarów	900
23.4.2. Techniki zakłócania	901
23.4.3. Zaawansowane radary i przeciwdziałania	904
23.4.4. Kwestie związane z innymi czujnikami i multiczujnikami	905
23.5. Systemy identyfikacji swój-obcy	907
23.6. Improwizowane urządzenia wybuchowe	910
23.7. Broń o ukierunkowanej energii	912
23.8. Wojna informacyjna	914
23.8.1. Ataki na systemy sterowania	916
23.8.2. Ataki na inną infrastrukturę	919
23.8.3. Ataki na wybory i stabilność polityczną	920
23.8.4. Doktryna	922
23.9. Podsumowanie	923
Problemy badawcze	924
Materiały uzupełniające	924

Rozdział 24 Prawa autorskie i zarządzanie prawami cyfrowymi	927
24.1. Wprowadzenie	927
24.2. Prawa autorskie	929
24.2.1. Oprogramowanie	930
24.2.2. Wolne oprogramowanie, wolna kultura?	936
24.2.3. Książki i muzyka	941
24.2.4. Wideo i płatna telewizja	942
24.2.4.1. Architektura typowego systemu	943
24.2.4.2. Techniki szyfrowania sygnału wizyjnego	944
24.2.4.3. Ataki na hybrydowe systemy szyfrujące	946
24.2.4.4. DVB	950
24.2.5. DVD	951
24.3. DRM na komputerach ogólnego przeznaczenia	953
24.3.1. Zarządzanie prawami do multimediów w systemie Windows	953
24.3.2. FairPlay, HTML5 i inne systemy DRM	955
24.3.3. Zaciemnianie oprogramowania	956
24.3.4. Gry, oszustwa i DRM	958
24.3.5. Systemy peer-to-peer	960
24.3.6. Zarządzanie prawami do projektów sprzętu	962
24.4. Ukrywanie informacji	963
24.4.1. Zarządzanie znakami wodnymi i kopiowaniem	965
24.4.2. Główne techniki ukrywania informacji	965
24.4.3. Ataki na schematy znakowania prawami autorskimi	968
24.5. Polityka	971
24.5.1. Lobby związane z własnością intelektualną	974
24.5.2. Kto na tym korzysta?	977
24.6. Kontrola akcesoriów	978
24.7. Podsumowanie	980
Problemy badawcze	980
Materiały uzupełniające	981
 Rozdział 25 Nowe kierunki?	 983
25.1. Wprowadzenie	983
25.2. Autonomiczne i zdalnie sterowane pojazdy	984
25.2.1. Drony	985
25.2.2. Pojazdy autonomiczne	986
25.2.3. Poziomy automatyzacji i jej granice	988
25.2.4. Jak zhakować autonomiczny samochód	991
25.3. Sztuczna inteligencja/uczenie się maszyn	994
25.3.1. Uczenie się maszyn a bezpieczeństwo	995
25.3.2. Ataki na systemy z uczeniem się maszyn	996
25.3.3. Uczenie się maszyn i społeczeństwo	999
25.4. Technologie wspierające prywatność oraz bezpieczeństwo operacyjne	1003
25.4.1. Urządzenia umożliwiające anonimową komunikację	1006
25.4.2. Wsparcie społeczne	1009

25.4.3. Żyjąc z zasobów naturalnych	1012
25.4.4. Łącząc wszystko w całość	1014
25.4.5. Nazywa się Bond. James Bond	1016
25.5. Wybory	1017
25.5.1. Historia maszyn do głosowania	1019
25.5.2. Wiszące skrawki papieru	1019
25.5.3. Skanowanie optyczne	1021
25.5.4. Niezależność od oprogramowania	1023
25.5.5. Dlaczego wybory elektroniczne są trudne	1024
25.6. Podsumowanie	1028
Problemy badawcze	1029
Materiały uzupełniające	1030

Część III **1031**

Rozdział 26 Inwigilacja czy prywatność **1033**

26.1. Wprowadzenie	1033
26.2. Inwigilacja	1036
26.2.1. Historia źródeł rządowych	1037
26.2.2. Zapisy szczegółów połączeń (CDR-y)	1041
26.2.3. Warunki wyszukiwania i dane o lokalizacji	1045
26.2.4. Przetwarzanie algorytmiczne	1046
26.2.5. Dostawcy usług internetowych i dostawcy usług telekomunikacyjnych	1047
26.2.6. System systemów Sojuszu Pięciorga Oczu	1048
26.2.7. Wojny kryptograficzne	1051
26.2.7.1. Tło polityki dotyczącej kryptografii	1052
26.2.7.2. DES i badania kryptograficzne	1053
26.2.7.3. Pierwsza wojna kryptograficzna - układ Clipper	1054
26.2.7.4. Druga wojna kryptograficzna - niespójność	1058
26.2.8. Kontrola eksportu	1061
26.3. Terroryzm	1063
26.3.1. Przyczyny przemocy politycznej	1064
26.3.2. Psychologia przemocy politycznej	1064
26.3.3. Rola instytucji	1066
26.3.4. Demokratyczna reakcja	1068
26.4. Cenzura	1069
26.4.1. Cenzura w reżimach autorytarnych	1070
26.4.2. Filtrowanie, mowa nienawiści i radykalizacja	1072
26.5. Kryminalistyka i prawa dotyczące dowodów	1076
26.5.1. Kryminalistyka	1076
26.5.2. Dopuszczalność dowodów	1078
26.5.3. Co idzie nie tak	1080
26.6. Prywatność i ochrona danych	1082
26.6.1. Europejska ochrona danych	1083
26.6.2. Przepisy dotyczące prywatności w Stanach Zjednoczonych	1086
26.6.3. Fragmentacja?	1088

26.7. Wolność dostępu do informacji	1090
26.8. Podsumowanie	1091
Problemy badawcze	1093
Materiały uzupełniające	1093

Rozdział 27 Rozwój bezpiecznych systemów

1095

27.1. Wprowadzenie	1095
27.2. Zarządzanie ryzykiem	1097
27.3. Nauka z systemów krytycznych dla bezpieczeństwa	1100
27.3.1. Metodologie inżynierii bezpieczeństwa	1100
27.3.2. Analiza zagrożeń	1101
27.3.3. Drzewa błędów i drzewa zagrożeń	1102
27.3.4. Analiza trybów awaryjnych i analiza skutków	1103
27.3.5. Modelowanie zagrożeń	1104
27.3.6. Ilościowa ocena ryzyka	1106
27.4. Określanie priorytetów celów zabezpieczeń	1109
27.5. Metodologia	1111
27.5.1. Projektowanie z góry na dół	1113
27.5.2. Podejście iteracyjne: od spirali do zwinności	1115
27.5.3. Bezpieczny cykl życia rozwoju produktu	1117
27.5.4. Projektowanie z bramkami	1119
27.5.5. Oprogramowanie jako usługa	1121
27.5.6. Od DevOps do DevSecOps	1124
27.5.6.1. Ekosystem Azure	1124
27.5.6.2. Ekosystem Googlea	1125
27.5.6.3. Tworzenie systemu uczącego się	1127
27.5.7. Cykl życia podatności na zagrożenia	1128
27.5.7.1. System CVE	1130
27.5.7.2. Skoordynowane ujawnianie	1131
27.5.7.3. Zarządzanie incydentami i zdarzeniami z zakresu zabezpieczeń	1132
27.5.8. Złe zarządzanie ryzykiem w organizacji	1134
27.6. Zarządzanie zespołem	1138
27.6.1. Elita inżynierów	1138
27.6.2. Różnorodność	1140
27.6.3. Pielęgnowanie umiejętności i postaw	1141
27.6.4. Wyłaniające się cechy	1142
27.6.5. Ewolucja naszego przepływu pracy	1143
27.6.6.1 wreszcie	1144
27.7. Podsumowanie	1145
Problemy badawcze	1145
Materiały uzupełniające	1146

Rozdział 28 Zapewnienie bezpieczeństwa i odporność

1149

28.1. Wprowadzenie	1149
28.2. Ocena	1152
28.2.1. Alarmy i zamki	1153

28.2.2. Reżimy oceny bezpieczeństwa	1154
28.2.3. Bezpieczeństwo urządzeń medycznych	1155
28.2.4. Bezpieczeństwo w lotnictwie	1158
28.2.5. Pomarańczowa księga	1160
28.2.6. FIPS 140 i HSM-y	1161
28.2.7. Common Criteria	1162
28.2.7.1. Drastyczne szczegóły	1163
28.2.7.2. Co jest nie tak z Common Criteria	1165
28.2.7.3. Wspólne profile ochrony	1167
28.2.8. „Zasada maksymalnego samozadowolenia"	1167
28.2.9. Kolejne kroki	1170
28.3. Miary niezawodności i jej dynamika	1172
28.3.1. Modele wzrostu niezawodności	1173
28.3.2. Wroga ocena	1175
28.3.3. Oprogramowanie bezpłatne i open-source	1177
28.3.4. Zapewnienie bezpieczeństwa procesu	1179
28.4. Splątanie bezpieczeństwa i zabezpieczeń	1181
28.4.1. Elektroniczne bezpieczeństwo i zabezpieczenie samochodów	1183
28.4.2. Modernizowanie przepisów dotyczących bezpieczeństwa i zabezpieczeń	1187
28.4.3. Ustawa o cyberbezpieczeństwie z 2019 roku	1188
28.5. Odporność	1189
28.5.1. Dyrektywa o sprzedaży towarów	1190
28.5.2. Nowe kierunki badań	1191
28.6. Podsumowanie	1194
Problemy badawcze	1195
Materiały uzupełniające	1196

Rozdział 29 Poza obszarem, gdzie „komputer mówi nie" 1197

Bibliografia B-1

oprac. BPK