

SZCZEGÓŁOWY SPIS TREŚCI

PRZEDMOWA	xix
------------------------	-----

PODZIĘKOWANIA	xxi
----------------------------	-----

WPROWADZENIE	xxiii
---------------------------	-------

Jak wyglądają urządzenia wbudowane	xxv
--	-----

Sposoby hakowania urządzeń wbudowanych	xxv
--	-----

Co oznacza atak sprzętowy?	xxvi
----------------------------------	------

Kto powinien przeczytać tę książkę?	xxvii
---	-------

O książce	xxvii
-----------------	-------

1

HIGIENA JAMY USTNEJ. WPROWADZENIE DO ZABEZPIECZEŃ WBUDOWANYCH	1
--	---

Komponenty sprzętu	2
--------------------------	---

Komponenty oprogramowania	5
---------------------------------	---

Początkowy kod rozruchu	5
-------------------------------	---

Program rozruchowy	6
--------------------------	---

Środowisko zaufanego uruchamiania systemu operacyjnego (TEE)
--

i zaufane aplikacje	7
---------------------------	---

Obrazy oprogramowania układowego	7
--	---

Główne jądro systemu operacyjnego i aplikacje	8
---	---

Modelowanie zagrożeń sprzętowych	8
--	---

Czym jest bezpieczeństwo?	9
---------------------------------	---

Drzewo ataków	12
---------------------	----

Profilowanie atakujących	12
--------------------------------	----

Typy ataków	14
-------------------	----

Ataki programowe na sprzęt	15
----------------------------------	----

Ataki na poziomie PCB	17
-----------------------------	----

Ataki logiczne	19
----------------------	----

Ataki nieinwazyjne	21
--------------------------	----

Ataki inwazyjne na chipy	21
--------------------------------	----

Zasoby i cele bezpieczeństwa	26
------------------------------------	----

Poufność i integralność kodu binarnego	27
--	----

Poufność i integralność kluczy	27
--------------------------------------	----

Zdalna atestacja rozruchu	28
---------------------------------	----

Poufność i integralność danych osobowych	29
--	----

Integralność i poufność danych z sensorów	30
---	----

Ochrona poufności treści	30
--------------------------------	----

Odpowiedzialność i odporność	31
------------------------------------	----

Środki zapobiegawcze	31
Chronienie	31
Wykrywanie	32
Odpowiadanie	32
Przykładowe drzewo ataku	32
Identyfikacja vs. eksploatacja	36
Skalowalność	36
Analizowanie drzewa ataku	36
Ocenianie ścieżek ataków sprzętowych	37
Ujawnianie kwestii związanych z bezpieczeństwem	39
Podsumowanie	41

2

NAWIĄZYWANIE KONTAKTU, POŁĄCZ SIĘ ZE MNA, POŁĄCZ SIĘ Z TOBĄ. SPRZĘTOWE INTERFEJSY PERYFERYJNE

Podstawy elektryki	44
Napięcie	44
Natężenie	45
Rezystancja	45
Prawo Ohma	45
AC/DC	45
Rozbieranie rezystancji	46
Moc	47
Interfejs z użyciem elektryczności	48
Poziomy logiczne	48
Wysoka impedancja, podciąganie i ściąganie	50
Push-pull vs. tristate vs. otwarty kolektor albo otwarty dren	51
Komunikacja asynchroniczna vs. synchroniczna vs. taktowanie wbudowane	53
Sygnały różnicowe	54
Interfejsy szeregowo o niskiej prędkości	55
Uniwersalna, asynchroniczna komunikacja szeregowo	56
Szeregowy interfejs urządzeń peryferyjnych	58
Interfejs IIC	60
Secure Digital Input/Output oraz Embedded Multimedia Cards	64
Magistrala CAN	66
JTAG i inne interfejsy debugowania	67
Interfejsy równoległe	71
Interfejsy pamięci	72
Szybkie interfejsy szeregowo	73
Uniwersalna Magistrala Szeregowo	74
PCI Express	75
Ethernet	76
Miernictwo	76
Multimetr: napięcie	76
Multimetr: ciągłość	77
Oscyloskop cyfrowy	78
Analityzator stanów logicznych	82
Podsumowanie	83

3

OBSERWOWANIE. IDENTYFIKACJA KOMPONENTÓW I ZBIERANIE INFORMACJI

Zbieranie informacji	86
Zgłoszenia w Federalnej Komisji Łączności	86
Patenty	89
Karty katalogowe i schematy	92
Przykład wyszukiwania informacji: urządzenie USB Armory	94
Otwieranie obudowy	102
Identyfikowanie układów scalonych na płytce	102
Małe obudowy z wystającymi wyprowadzeniami: SOIC, SOP i QFP	105
Obudowy bez wystających wyprowadzeń: SO i QFN	107
Ball grid array	108
Chip scale packaging	111
DIP, przewlekane i inne	111
Przykładowe obudowy układów scalonych na PCB	112
Identyfikowanie innych komponentów na płycie	115
Mapowanie PCB	120
Użycie do mapowania skanowania ścieżką krawędziową JTAG	125
Odtwarzanie informacji z oprogramowania układowego	127
Uzyskiwanie obrazu oprogramowania układowego	128
Analizowanie obrazu oprogramowania układowego	130
Podsumowanie	138

4

SŁOŃ W SKLEPIE Z PORCELANĄ.

WPROWADZENIE DO WSTRZYKIWANIA BŁĘDÓW

Wprowadzanie błędów do mechanizmów bezpieczeństwa	140
Obchodzenie weryfikacji podpisu oprogramowania układowego	141
Uzyskiwanie dostępu do zablokowanej funkcjonalności	142
Odtwarzanie kluczy kryptograficznych	142
Ćwiczenie z wstrzykiwaniem błędów do OpenSSH	143
Wstrzykiwanie błędów do kodu w C	143
Wstrzykiwanie błędów do kodu maszynowego	144
Słoń wstrzykiwania błędów	146
Urządzenie cel oraz rezultat błędu	147
Narzędzia do wstrzykiwania błędów	147
Przygotowanie i kontrola celu	149
Metody wyszukiwania błędów	154
Odkrywanie prymitywów błędów	154
Poszukiwanie skutecznych błędów	158
Strategie poszukiwań	166
Analizowanie rezultatów	169
Podsumowanie	171

5

NIE LIŻ PRÓBNIKA. JAK WSTRZYKIWAĆ BŁĘDY 173

Wstrzykiwanie błędu zegara	174
Metastabilność	178
Analiza wrażliwości na błędy	181
Ograniczenia	181
Wymagany sprzęt	182
Parametry wstrzykiwania błędu zegara	184
Wstrzykiwanie błędu napięcia	185
Generowanie zakłóceń napięcia	186
Budowanie wstrzykiwacza wykorzystującego przełączanie	186
Wstrzykiwanie błędów typu crowbar	191
Atakowanie błędami Raspberry Pi z użyciem crowbara	193
Poszukiwanie parametrów wstrzykiwania błędu napięcia	200
Wstrzykiwanie błędów elektromagnetycznych	200
Generowanie błędów elektromagnetycznych	202
Architektury do wstrzykiwania błędów elektromagnetycznych	204
Kształty i szerokości impulsów EMFI	206
Poszukiwanie parametrów wstrzykiwania błędu elektromagnetycznego	207
Wstrzykiwanie błędów optycznych	208
Przygotowywanie chipa	208
Ataki z przodu i z tyłu	210
Źródła światła	212
Konfiguracja wstrzykiwania błędów optycznych	213
Konfigurowalne parametry wstrzykiwania błędów optycznych	213
Wstrzykiwanie body biasing	214
Parametry dla wstrzykiwania body biasing	216
Wyzwalanie błędów w sprzęcie	217
Postępowanie z nieprzewidywalnymi czasami celu	218
Podsumowanie	219

6

CZAS NA BADANIA. LABORATORIUM WSTRZYKIWANIA BŁĘDÓW 221

Akt 1: prosta pętla	222
Grillowa zapalniczka bólu	225
Akt 2: wstawianie przydatnych zakłóceń	227
Zakłócenie crowbar powodujące błąd w danych konfiguracyjnych	228
Wstrzykiwanie błędów multipleksacją	244
Akt 3: różnicowa analiza błędów	250
Niecو matematyki dotyczącej RSA	250
Zdobywanie prawidłowego podpisu z celu	254
Podsumowanie	258

7

TO JEST TO MIEJSCE. ZRZUT PAMIĘCI PORTFELA TREZOR ONE . . . 259

Wprowadzenie do ataku	260
Wewnętrzne elementy portfela Trezor One	261
Wprowadzanie błędu do żądania odczytu USB	262
Deasemblacja kodu	264
Budowanie oprogramowania układowego i walidowanie zakłócenia	266
Wyzwalanie i określanie odpowiedniego momentu	270
Zakłócanie przez obudowę	274
Konfigurowanie	274
Przegląd kodu do wstrzykiwania błędów	275
Uruchomienie kodu	278
Potwierdzanie zrzutu	280
Dostrajanie impulsu EM	280
Dostrajanie momentu błędu na podstawie komunikatów USB	281
Podsumowanie	282

8

MAM MOC. WPROWADZENIE DO ANALIZY MOCY 285

Ataki czasowe	287
Atak czasowy na dysk twardy	290
Pomiary mocy dla ataków czasowych	293
Prosta analiza mocy	294
Zastosowanie SPA od RSA	295
Zastosowanie SPA do RSA, ponownie	297
SPA na ECDSA	300
Podsumowanie	306

9

CZAS NA BADANIA. PROSTA ANALIZA MOCY 307

Domowe laboratorium	308
Budowanie podstawowego środowiska sprzętowego	308
Kupowanie narzędzi	312
Przygotowywanie kodu celu	313
Budowanie konfiguracji	315
Zbieranie wszystkiego razem: atak SPA	317
Przygotowanie celu	318
Przygotowanie oscyloskopu	320
Analiza sygnału	321
Oskryptowanie komunikacji i analizy	322
Oskryptowanie ataku	325
Przykład z ChipWhisperer-Nano	328
Budowanie i ładowanie oprogramowania układowego	328
Pierwsze spojrzenie na komunikację	329
Przechwytywanie śladu	330
Od śladu do ataku	331
Podsumowanie	335

10

DZIELENIE RÓŻNIC. RÓŻNICOWA ANALIZA MOCY	337
Wewnątrz mikrokontrolera	338
Zmiana napięcia na kondensatorze	339
Od mocy do danych i na odwrót	341
Przykład seksownych XOR-ów	343
Atak z użyciem różnicowej analizy mocy	345
Przewidywanie poboru mocy na podstawie założenia dotyczącego wycieków	346
Atak DPA w Pythonie	349
Poznaj swojego wroga: standardowy kurs łamania zaawansowanego szyfrowania	353
Atakowanie AES-128 z użyciem DPA	355
Korelacja w ataku z analizą mocy	357
Współczynnik korelacji	358
Atakowanie AES-128 z użyciem CPA	362
Komunikacja z urządzeniem celem	368
Szybkość przechwytywania oscyloskopu	368
Podsumowanie	369

11

SKUP SIĘ NA TYM. ZAAWANSOWANA ANALIZA MOCY	371
Główne przeszkody	372
Potężniejsze ataki	374
Mierzenie powodzenia	375
Metryki oparte na wskaźniku powodzenia	375
Metryki oparte na entropii	376
Progresja pików korelacji	378
Wysokość pików korelacji	379
Pomiary na rzeczywistych urządzeniach	380
Działanie urządzenia	380
Sonda pomiarowa	383
Określanie wrażliwych sieci zasilania	387
Automatyczne skanowanie z użyciem sondy	388
Konfiguracja oscyloskopu	389
Analiza i przetwarzanie zbiorów śladów	392
Techniki analizy	393
Techniki przetwarzania	404
Głębokie uczenie z wykorzystaniem spłotowych sieci neuronowych ..	407
Podsumowanie	410

12

CZAS NA BADANIA. RÓŻNICOWA ANALIZA MOCY	413
Środowisko programu rozruchowego	414
Protokół komunikacyjny programu rozruchowego	414
Szczegóły AES-256 CBC	416
Atakowanie AES-256	417

Pozyskanie i budowa kodu programu rozruchowego	418
Uruchamianie celu i przechwytywanie śladów	419
Obliczanie CRC	419
Komunikacja z programem rozruchowym	420
Przechwytywanie ogólnych śladów	421
Przechwytywanie szczegółowych śladów	422
Analiza	423
Klucz rundy 14	423
Klucz rundy 13	424
Odtwarzanie IV	427
Co należy przechwycić	428
Generowanie pierwszego śladu	428
Generowanie reszty śladów	430
Analiza	430
Atakowanie podpisu	434
Teoria ataku	434
Ślady mocy	435
Analiza	435
Wszystkie cztery bajty	437
Podglądanie kodu źródłowego programu rozruchowego	437
Moment sprawdzania podpisu	439
Podsumowanie	440

13

BEZ ŻARTÓW. PRZYKŁADY Z ŻYCIA 443

Ataki z wstrzykiwaniem błędów	443
Nadzorca w PlayStation 3	444
Xbox 360	448
Hakowanie z analizą mocy	451
Hakowanie żarówek Philips Hue	451
Podsumowanie	456

14

POMYŚL O DZIECIACH. ŚRODKI ZAPOBIEGAWCZE, CERTYFIKATY I DALSZE KROKI 461

Środki zapobiegawcze	462
Wdrażanie środków zapobiegawczych	463
Weryfikacja środków zapobiegawczych	481
Certyfikaty branżowe	485
Zwiększanie umiejętności	488
Podsumowanie	489

A

CZAS ZAKUPÓW. WYPOSAŻENIE LABORATORIUM TESTOWEGO 491

Sprawdzanie połączeń i napięcia: od \$50 do \$500	492
Lutowanie precyzyjne: od 50\$ do 1500\$	494
Odlutowywanie: od 30\$ do 500\$	496

Lutowanie i odlutowywanie elementów montowanych powierzchniowo:	
od 100\$ do 500\$	498
Modyfikowanie PCB: od \$5 do \$700	502
Mikroskopy optyczne: od \$200 do \$2,000	503
Fotografowanie płyt: od \$50 do \$2,000	504
Zasilanie: od \$10 do \$1 000	505
Podgląd przebiegów analogowych (oscylloskopy): od \$300 do \$25 000	505
Głębokość pamięci	507
Częstotliwość próbkowania	508
Szerokość pasma	510
Inne parametry	512
Podgląd przebiegów logicznych: od \$300 do \$8000	512
Wyzwalanie w magistralach szeregowych: od \$300 do \$8000	514
Dekodowanie protokołów szeregowych: od \$50 do \$8000	515
Podsluchiwanie i wyzwalanie magistrali CAN: od \$50 do \$5000	516
Podsluchiwanie Ethernetu: \$50	517
Interakcja przez JTAG: od \$20 do \$10,000	517
Ogólny JTAG i skanowanie granic	517
Debugowanie JTAG	518
Komunikacja PCIe: od \$100 do \$1,000	519
Podsluchiwanie USB: od \$100 do \$6,000	520
Wyzwalanie USB: od \$250 do \$6,000	522
Emulacja USB: \$100	523
Połączenia Flash SPI: od \$25 do \$1000	523
Pomiary w analizie mocy: od \$300 do \$50000	524
Wyzwalanie na podstawie przebiegów analogowych: powyżej \$3800	528
Mierzenie pól magnetycznych: od \$25 do \$10,000	528
Wstrzykiwanie błędów zegara: od \$100 do \$30000	531
Wstrzykiwanie błędów napięcia: od \$25 do \$30000	532
Wstrzykiwanie błędów elektromagnetycznych: od \$100 do \$50000	533
Wstrzykiwanie błędów optycznych: od \$1000 do \$250000	534
Pozycjonowanie sond: od \$100 do \$50000	535
Urządzenia docelowe: od \$10 do \$10000	535

B

CAŁA TWOJA BAZA NALEŻY DO NAS.

POPULARNE UKŁADY PINÓW	539
SPI Flash	539
Konektory 0,1 cala	540
Arm JTAG z 20 pinami	540
PowerPC JTAG z 14 pinami	541
Konektory 0,05 cala	542
Arm Cortex JTAG/SWD	542
Konektor Ember Packet Trace Port	542