



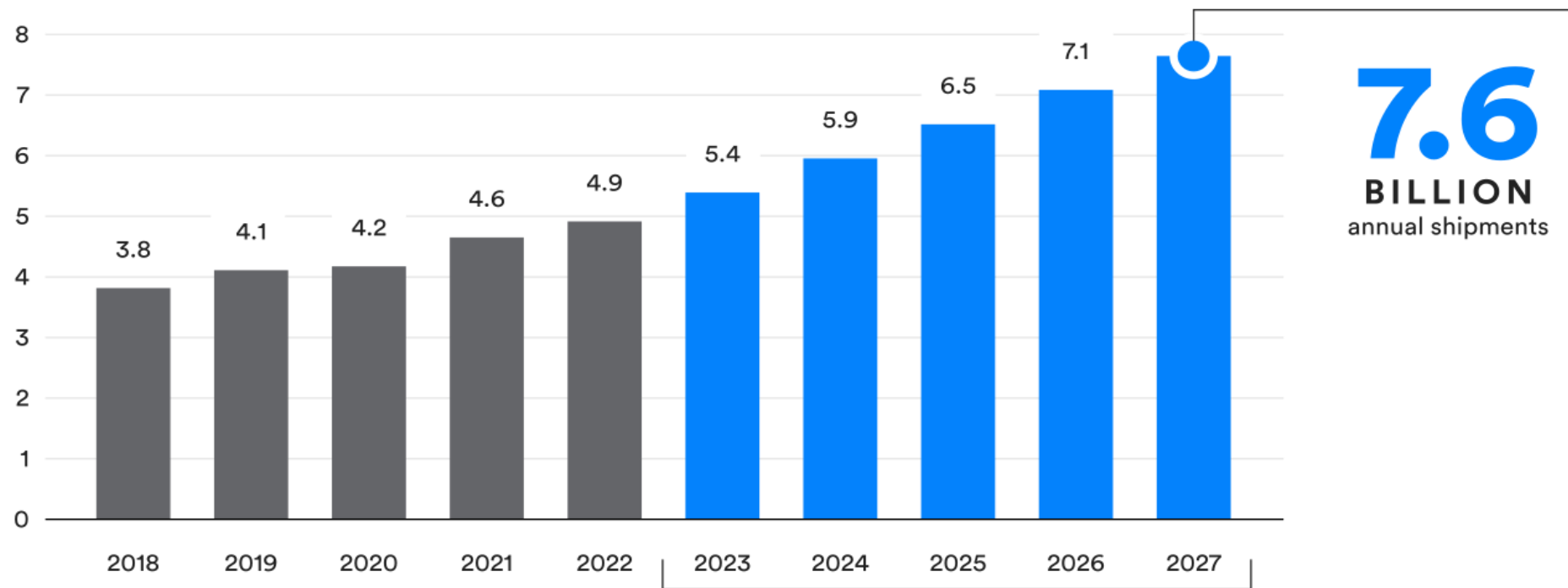
Atskats uz *Bluetooth* *Fuzzing* izpētes progresu

Temats: «Bluetooth protokola drošības novērtēšana,
izmantojot nejaušdatu testēšanu»
Eduards Blumbergs / 24.01.2024

Bluetooth tirgus

Total Annual Bluetooth® Device Shipments

NUMBERS IN BILLIONS



9% CAGR

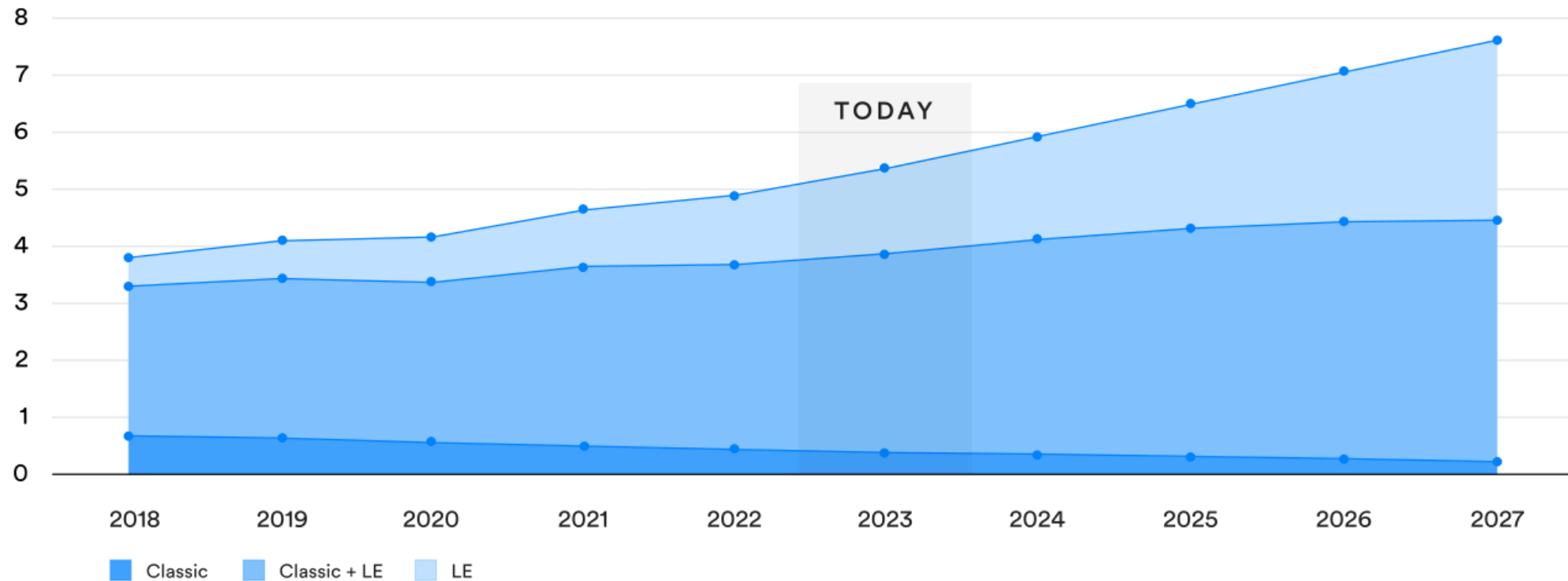
Data Source: ABI Research, 2023

<https://www.bluetooth.com/2023-market-update/>

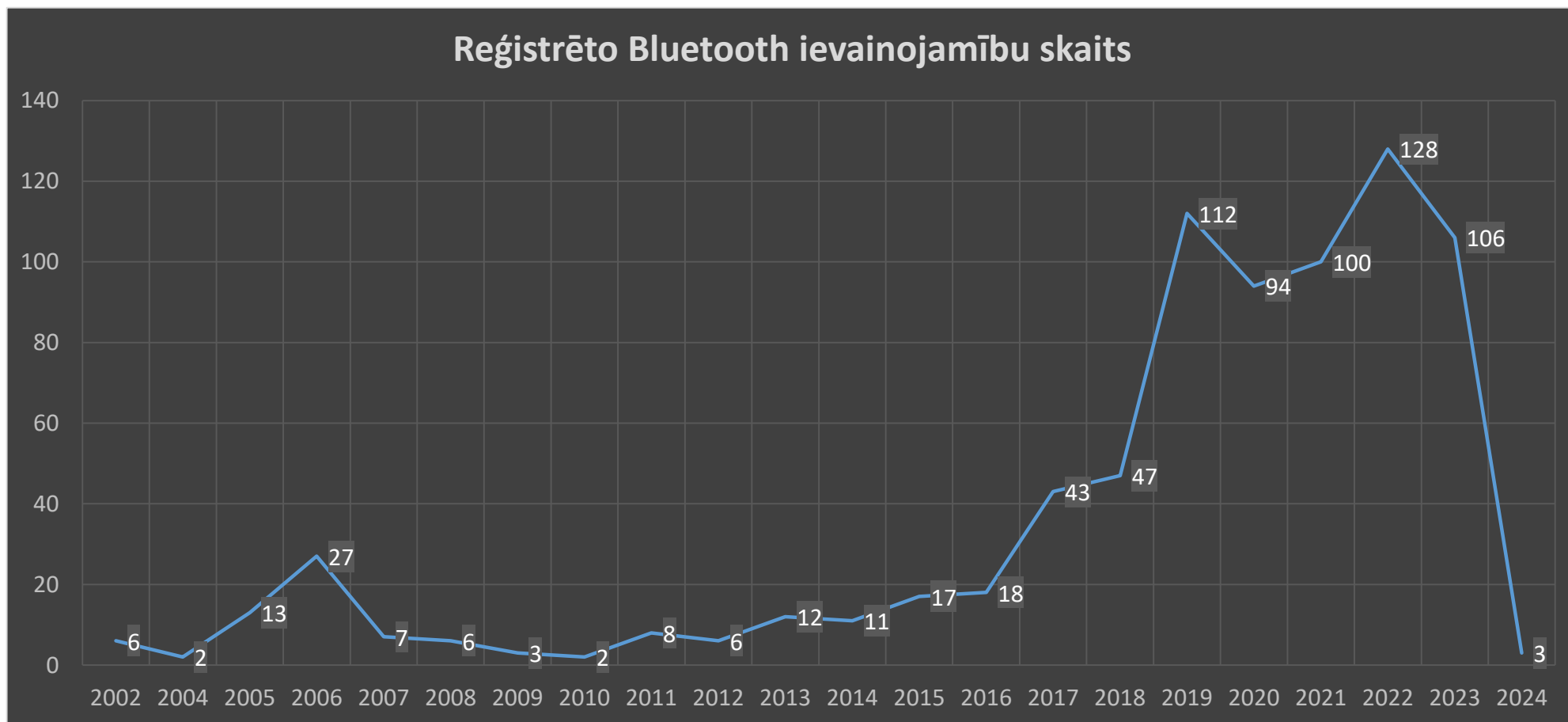
Bluetooth versijas

Bluetooth® Enabled Device Shipments by Radio Version

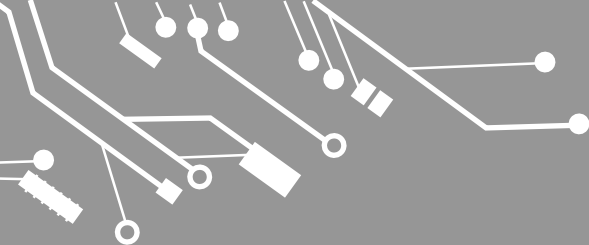
NUMBERS IN BILLIONS



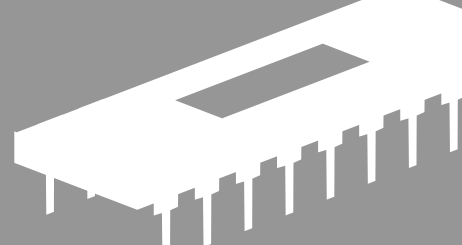
Ievainojamību skaits



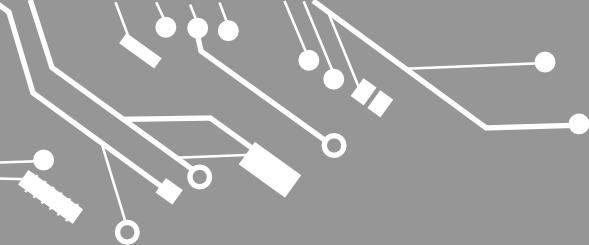
<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=bluetooth>



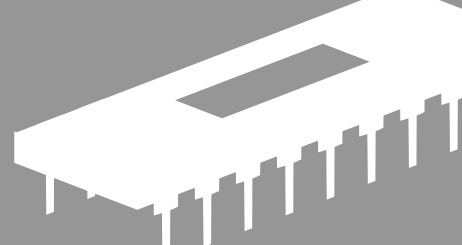
Ievainojamību veidi



- *Bluejacking* – nevēlamo «reklāmas» ziņu sūtīšana.
- *Bluesnarfing, BlueBugging* – pieslēgšanās bez atļaujas.
- *Malware on a Bluetooth device* – izplatīšanas kanāls.
- ***Fuzzing*** – meklējam ***0-day Bluesnarfing, DoS u.c.***
- *Car Whisperer* – ievainojamības automašīnas *Bluetooth*.
- *DoS* – bateriju tērēšana, savienojumu traucēšana.
- *Pairing Eavesdropping* – atslēgu vākšana pārošanas laikā.
- *Secure Simple Pairing* – izlikšanās par jau sapārotu ierīci.

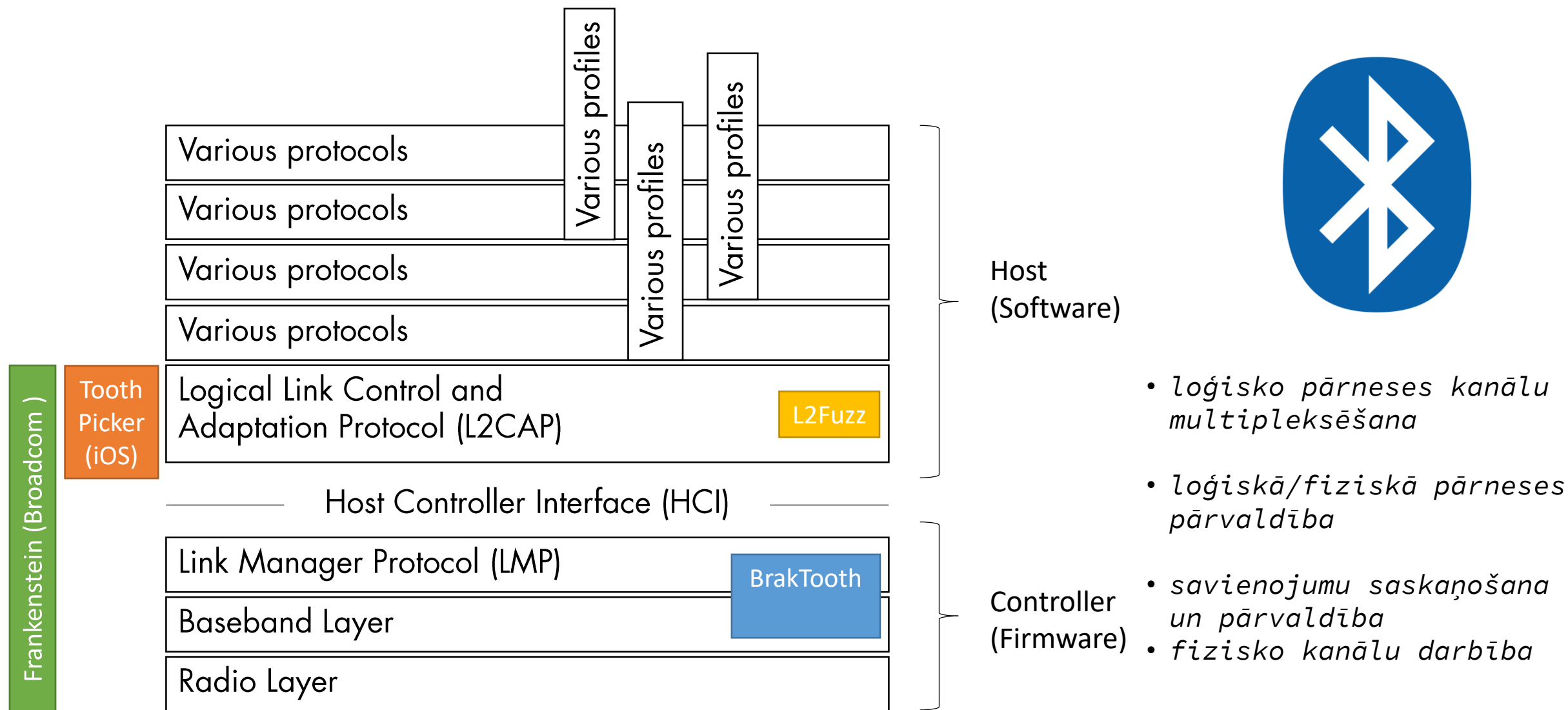
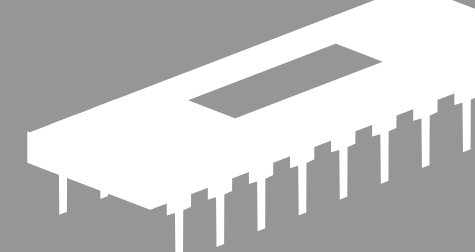


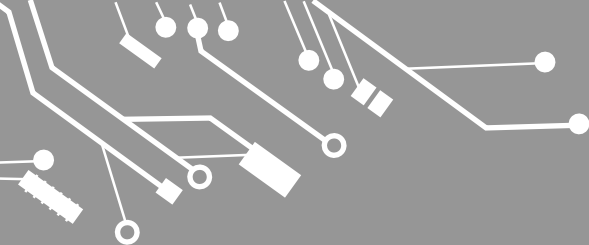
Motivācija



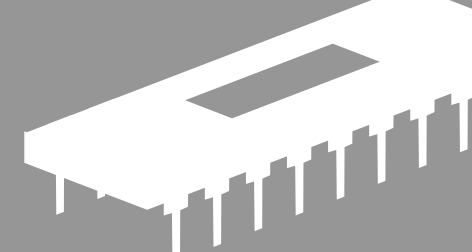
- Vairākslāņu protokols, kas atbalsta mantotas perifērās ierīces un apgrūtināts ar lielu savietojamības bagāžu (protokola līmeņa programmaparatūras ievainojamības).
- Grūti vai neiespējami izplatīt atjauninājumus.
- Pašreizējā kvalitātes nodrošināšana un sertifikācija nepilnvērtīgi un neviendabīgi pārbauda ļaunprātīgu datu apstrādes iespējamību ierīcēs.
- Ar programmaparatūru un draiveri var apiet operētājsistēmas drošību.

Protokola arhitektūra

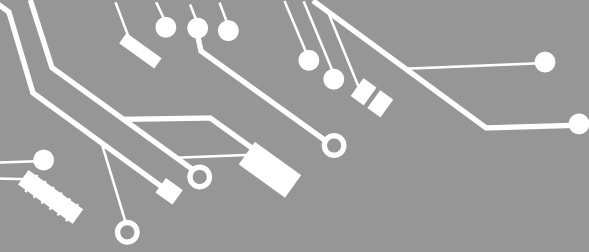




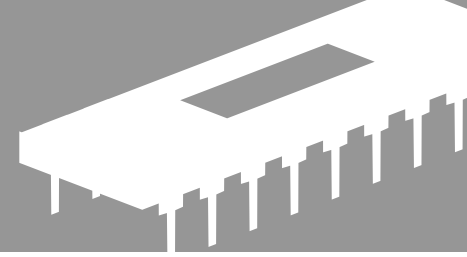
Nejaušdatu testēšana



- Fuzz testēšana ir Melnās kastes automātiska testēšanas metode, kas izmanto nejaušus vai daļēji nejaušus testēšanas datus, lai pārbaudītu strādājošu protokolu, meklējot tajā jaunas ievainojamības vai neparedzētu uzvedību. Parasti *fuzzing* rezultāts ir ierīces avārija, traucējumi vai apstāšanās.
- Mērķa protokols un kā līdz tam nonākt. *Bluetooth* daudzpakāpju stāvokļi nepieļauj uzreiz «fuzēt», piemēram, zemāko aparātprogrammatūras slāni. Nepieciešama plānošana uz izpratne par protokola darbību dažādās ierīcēs!
- Testa datu veidošanas metode. Pilnīgi nederīgus datus kvalitatīva aparātprogramma var nepieņemt apstrādei. Tas atkarīgs no ražotāja ieguldījuma un kvalitātes prasībām!



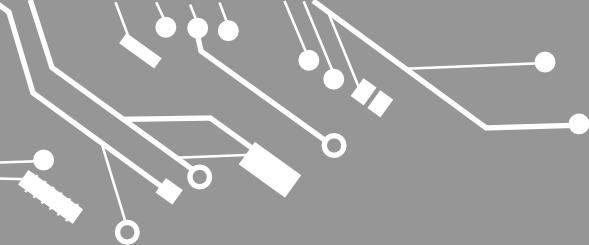
Testēšanas paņēmieni



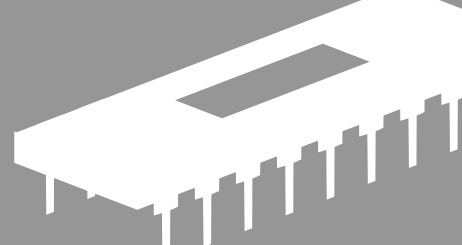
- Ģeneratīva pieeja – ģenerē datus no nulles pēc specifikācijas (meklē negaidītu derīgu ievadi).
- Mutāciju pieeja – ģenerē, modificējot zināmus derīgus datus (meklē robežgadījumus).

Modernos rīkos parasti izmanto abas pieejas, bet unikālā veidā, piemēram:

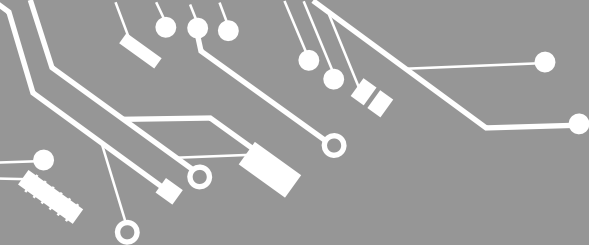
- *L2Fuzz* koncentrējas uz L2CAP slāni, izmanto ģeneratīvu pieeju, lai radītu jaunas paketes, un var atklāt ievainojamības draiveros bez pārošanas.
- *BrakTooth* izmanto mutāciju pieeju, lai modificētu esošās paketes aparātprogrammatūrā (LMP un *Baseband* slānī).
- *ToothPicker* ir vērsts uz *iOS 13*, ģenerē modeļus.
- *Frankenstein* izmanto ģeneratīvu pieeju un simboliskas mainīgo vērtības bez reāliem ievaddatiem, emulē *Broadcom* mikroshēmu un meklē atmiņas bojājumus.



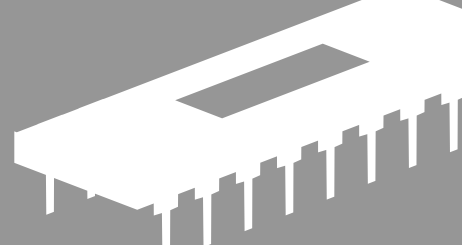
Zinātniskais darbs



- Literatūras izpēte un *fuzzing* pētniecības jomā izmantoto metožu apkopošana, aprobēšana, salīdzināšana un dokumentēšana.
- Modernu atvērtā koda *fuzzing* rīku izpēte.
- Dalība 2 publikāciju veidošanā LZP projektā (2. autors un 1. autors)
 - *“Wearable Device RF Fingerprinting: an Experimental Study Using COTS Hardware”* konferencei *“International workshop on Embedded Digital Intelligence (IWoeDI'2023)”* (2.autors)
 - *“Bluetooth Classic Protocol Fuzzing Practices”* publicēšanai žurnālā *“Baltic Journal of Modern Computing”* (1.autors), raksts ir izskatīšanas procesā un nav vēl apstiprināts publicēšanai.



Eksperimenti



- *Fuzzing* eksperimenti ar bezvadu audio ierīcēm.
- *Fuzzing* eksperimenti ar *Windows Bluetooth* draiveriem.
- Automatizācijas skriptu veidošana ierīču inventarizācijai un vieglākai *fuzzing* rīku apkalpošanai.
- Ierīču izjaukšana un salikšana – mikroshēmu dokumentēšana.

Skripti (1)

```
Found blue_hydra database. Do you want try to use it instead of a new run? (yes/no):
Backing up database...
Database backed up as /home/ejus/bt/runner/dbackups/dbackups-          -nr-0.db
The blue_hydra folder already exists. Do you want to force clone? (yes/no): yes
Deleting existing repository /home/ejus/bt/runner/blue_hydra using sudo privileges...
Cloning blue_hydra repository from https://github.com/ZeroChaos-/blue_hydra.git...

Multiple Bluetooth interfaces found. Please select one:
1. hci1 8C:88:2B:          :8F, LMP: 5.1, Realtek Semiconductor Corporation
2. hci0 18:5E:0F:          :82, LMP: 4.2, Intel Corp.
Enter the number of the interface to use: 1
Bringing down Bluetooth interface hci0...
Bringing up Bluetooth interface hci1...
Interface hci1 is up.

blue_hydra configuration file created at /home/ejus/bt/runner/blue_hydra/blue_hydra.yml.

Selected interface hci1 information:
hci1:  Type: Primary  Bus: USB
       BD Address: 8C:88:2B:          :8F  ACL MTU: 1021:5  SCO MTU: 255:11
       HCI Version: 5.1 (0xa)  Revision: 0xd99
       LMP Version: 5.1 (0xa)  Subversion: 0x646b
       Manufacturer: Realtek Semiconductor Corporation (93)
       Unsupported manufacturer
       Name: 'ejus-Latitude #2'

Starting blue_hydra scan process for 60 seconds...
```

Skripti (2)

Interface hci1 is up.

Data saved to /home/ejus/bt/runner/reports/bh_run_2024

1.json and /home/ejus/bt/runner/reports/bh_run_2024

741.csv

THE SUMMARY

Found 28 devices:

0	CA:99:A6:9D:	1	BTC/BLE: f/t	Seen: 2024-01-
1	E0:8E:A6:DA:	4	BTC/BLE: f/t	Seen: 2024-01-
2	4A:0F:F6:BF:	D	BTC/BLE: f/t	Seen: 2024-01-
3	E3:71:23:BF:	F	BTC/BLE: f/t	Seen: 2024-01-
4	DA:CE:97:0E:	E	BTC/BLE: f/t	Seen: 2024-01-
5	CB:41:1D:1F:	6	BTC/BLE: f/t	Seen: 2024-01-
6	EF:CC:21:F8:	1	BTC/BLE: f/t	Seen: 2024-01-
7	7C:C2:94:2F:	1	BTC/BLE: f/t	Seen: 2024-01-
8	F9:9B:73:CE:	5	BTC/BLE: f/t	Seen: 2024-01-
9	77:4F:BC:79:	E	BTC/BLE: f/t	Seen: 2024-01-
10	22:22:92:AB:	E	BTC/BLE: t/f	Seen: 2024-01-
11	E0:9D:13:89:	9	BTC/BLE: f/t	Seen: 2024-01-
12	42:00:00:20:	0	BTC/BLE: f/t	Seen: 2024-01-
13	FE:28:61:B5:	3	BTC/BLE: f/t	Seen: 2024-01-
14	DE:2E:C9:49:	4	BTC/BLE: f/t	Seen: 2024-01-
15	00:1B:66:05:	C	BTC/BLE: f/t	Seen: 2024-01-
16	78:80:D2:BE:	5	BTC/BLE: f/t	Seen: 2024-01-
17	51:89:F0:3D:	0	BTC/BLE: f/t	Seen: 2024-01-
18	6D:8B:FC:ED:	1	BTC/BLE: f/t	Seen: 2024-01-
19	5B:6C:DC:69:	A	BTC/BLE: f/t	Seen: 2024-01-
20	57:CB:56:D7:	E	BTC/BLE: f/t	Seen: 2024-01-
21	00:D5:11:BE:	9	BTC/BLE: f/t	Seen: 2024-01-
22	59:8E:32:09:	E	BTC/BLE: f/t	Seen: 2024-01-
23	80:2B:F9:D1:	2	BTC/BLE: f/t	Seen: 2024-01-
24	DB:1F:45:87:	A	BTC/BLE: f/t	Seen: 2024-01-
25	65:EB:56:9D:	A	BTC/BLE: f/t	Seen: 2024-01-
26	DA:87:C4:FD:	9	BTC/BLE: f/t	Seen: 2024-01-
27	6B:8E:E5:7E:	8	BTC/BLE: f/t	Seen: 2024-01-

58:23	Random BDA - Apple, Inc. (76)	Random	(Static)
58:21	Random BDA - Apple, Inc. (76)	Random	(Static)
58:20	Unknown - Apple, Inc. (76)	(Resolvable)	
58:06	Unknown - Apple, Inc. (76)	(Static)	
58:06	Random BDA - Apple, Inc. (76)	Random	(Static)
58:06	Random BDA - Apple, Inc. (76)	Random	(Static)
58:05	Random BDA - Apple, Inc. (76)	Random	(Static)
58:04	Beijing Xiaomi Mobile Software Co., Ltd - Xiaomi Inc. (911)	Public	
58:04	Random BDA - Apple, Inc. (76)	Random	(Static)
58:03	Random BDA - Apple, Inc. (76)	Random	(Resolvable)
58:03	Set-top box "TriaPlayBox" : Unknown		
58:03	Samsung Electronics Co.,Ltd - Samsung Electronics Co. Ltd. (117)	Public	
58:03	Random BDA - Apple, Inc. (76)	Random	(Resolvable)
58:03	Random BDA - Apple, Inc. (76)	Random	(Static)
58:03	Random BDA - Apple, Inc. (76)	Random	(Static)
58:02	"HD 450SE" : Sennheiser electronic GmbH & Co. KG	Public	
58:02	Unknown - Apple, Inc. (76)	(Resolvable)	
58:02	Random BDA	Random	(Resolvable)
58:02	Random BDA	Random	(Resolvable)
58:02	Random BDA - Apple, Inc. (76)	Random	(Resolvable)
58:02	Random BDA - Apple, Inc. (76)	Random	(Resolvable)
58:02	Random BDA - Microsoft (6)	Random	(Non-Resolvable)
58:02	Random BDA - Apple, Inc. (76)	Random	(Resolvable)
58:02	Hon Hai Precision Ind. Co.,Ltd. - Apple, Inc. (76)	(Hon Hai Precision Ind. Co.,Ltd.)	
58:02	"Mi Band 3" : Random BDA - Anhui Huami Information Technology Co., Ltd.	(Random BDA)	
58:01	Random BDA - Apple, Inc. (76)	Random	(Resolvable)
58:01	Random BDA - Apple, Inc. (76)	Random	(Static)
58:01	Random BDA - Apple, Inc. (76)	Random	(Resolvable)

Enter the number of the Bluetooth device to fuzz: |

Skripti (3)

Choose an option:

- 1 - List of 24 BrakTooth Exploits
- 2 - BrakTooth Fuzzer GUI
- 3 - l2fuzz-custom2 (Crash Windows)
- 4 - l2fuzz-custom (Find BT Profile to Fuzz)
- 5 - List of 24 BrakTooth Exploits v2
- 6 - BrakTooth Exploit invalid_timing_accuracy 30sec - for Apple AirPods Pro Gen 2
- 7 - BrakTooth Exploit lmp_max_slot_overflow 1min - for Apple AirPods Pro Gen 2
- 8 - BrakTooth Exploit duplicated_encapsulated_payload - for Lidl Sound Spot, Model HG09049C Version 05/2022
- q - Quit

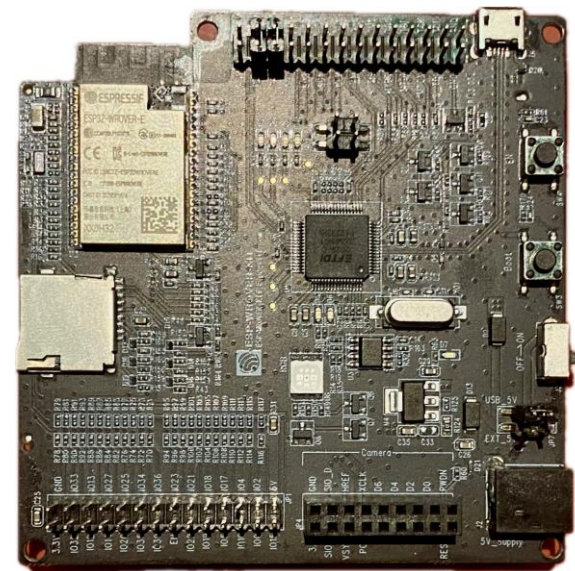
Enter your choice: 1

BrakTooth Exploit List:

- 0. paging_scan_disable
- 1. lmp_invalid_transport
- 2. noncompliance_duplicated_encryption_request
- 3. duplicated_encapsulated_payload
- 4. repeated_host_connection
- 5. lmp_auto_rate_overflow
- 6. au_rand_flooding
- 7. knob
- 8. wrong_encapsulated_payload
- 9. invalid_setup_complete
- 10. sdp_unknown_element_type
- 11. truncated_lmp_accepted
- 12. invalid_timing_accuracy
- 13. noncompliance_invalid_stop_encryption
- 14. lmp_max_slot_overflow
- 15. truncated_sco_link_request
- 16. feature_response_flooding
- 17. invalid_max_slot
- 18. sdp_oversized_element_size
- 19. lmp_overflow_dm1
- 20. duplicated_iocap
- 21. invalid_feature_page_execution

Izmantotās ierīces

PAREK Ubertooth One
eksperimentiem un
ierīču inventarizācijai



ESP32-WROVER-E KIT
darbam ar *BrakTooth*

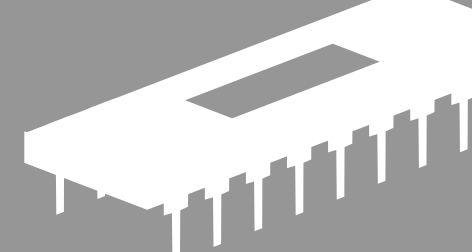


Realtek & TP-Link
Winows draiveru testi
un ierīču inventarizācijai



nRF52840
BLE4.2/5.0
inventarizācijai
un potenciāliem
eksperimentiem
ar *SweynTooth*
un *Automata Learning*

Interesanti atklājumi (1)



- *TP-Link & Realtek Windows 8–11 draivera sabrukums (BSOD vai pilnīga apstāšanās) caur Service Discovery Protocol, fazojot ar gadījuma datiem L2Fuzz Protocol/Service Multiplexer 1. portu (Izlaisti 2023.08. atjauninājumi, bet Windows 8.1 < joprojām ievainojams). – Prezētēts konferencē «Kiberšahs 2023», Rīgā.*



Novērotās kļūdas:

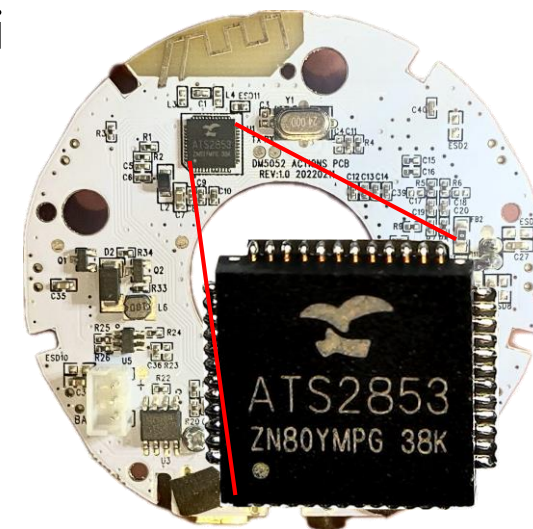
- *PAGE_FAULT_IN_NONPAGED_AREA (nederīga piekļuve atmiņai RtkBtfilter.sys).*
- *SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (izraisa BTHAvrcp.sys audio/video tālvadība).*
- *WDF_VIOLATION (izraisa USBXHCI.SYS, kad ierīce ir pievienota, izmantojot USB3).*
- *DRIVER_IRQL_NOT_LESS_OR_EQUAL (izraisa Wdf01000.sys neparedzēta atmiņas piekļuve draiverī, kas palīdz palaist citus draiverus).*

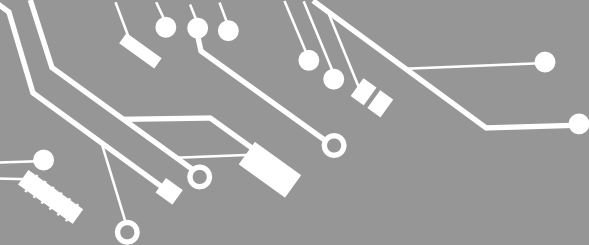
Interesanti atklājumi (2)

```
# List of available BrakTooth exploits
exploits = [
    "paging_scan_disable",
    "lmp_invalid_transport",
    "noncompliance_duplicated_encryption_request",
    "duplicated_encapsulated_payload",
    "repeated_host_connection",
    "lmp_auto_rate_overflow",
    "au_rand_flooding",
    "knob",
    "wrong_encapsulated_payload",
    "invalid_setup_complete",
    "sdp_unkown_element_type",
    "truncated_lmp_accepted",
    "invalid_timing_accuracy",
    "noncompliance_invalid_stop_encryption",
    "lmp_max_slot_overflow",
    "truncated_sco_link_request",
    "feature_response_flooding",
    "invalid_max_slot",
    "sdp_oversized_element_size",
    "lmp_overflow_dm1",
    "duplicated_iocap",
    "invalid_feature_page_execution",
    "lmp_overflow_2dh1",
    "feature_req_ping_pong",
]
```

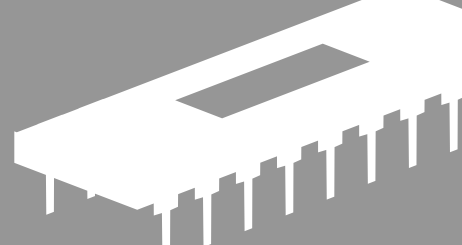
- *Apple AirPods Pro 2* H2 mikroshēmas patvaļīga pārstartēšanas (*BrakTooth* invalid_timing_accuracy & lmp_max_slot_overflow) – kļūdas joprojām nav novērstas, nepieciešams turpināt eksperimentus.
- Daudzu mazbudžeta un lielveikala zīmolu bezvadu audio ierīču patvaļīga pārstartēšanās, skaņas raustīšanās vai izslēgšanās pie kāda no 24 *BrakTooth* mūķiem (*exploit*). Piemēram, *Lidl* «Sound Spot» skaļruņa RISC 32bit mikroshēma ATS2853 izslēdzas ar mūķi duplicated_encapsulated_payload. Uz iepakojuma apgalvo BT5.3, bet ATS2853 specifikācija*: BT5.3 compatible with BT4.2/4.2 LE/4.0/2.1 + EDR system... :)

*) <https://www.i-lexia.com/productinfo/1031204.html>
<https://fccid.io/YMX-ATS2853/User-Manual/Users-Manual-6967840.pdf>

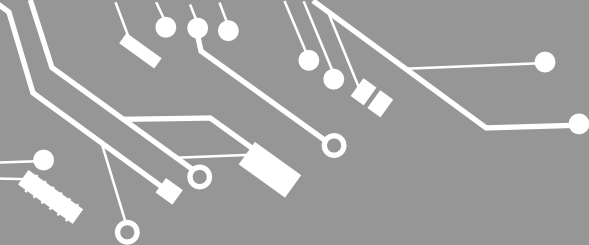




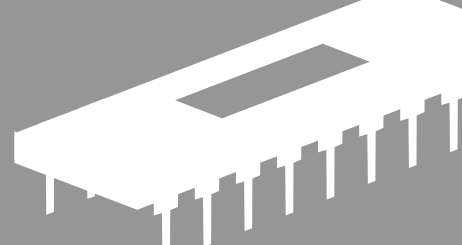
Tuvākie plāni



- Automatizācijas skriptu papildināšana, atklūdošana un dokumentēšana.
- Populārāko *Bluetooth* audio ierīču eksperimentu apkopošana, jauna(u) CVE koda(u) pieteikšana.
- Disertācijas melnraksts un struktūras skice (apskatītā literatūra, veiktie eksperimenti un publikācijas, ierobežojumi).
- *Bluetooth fuzzing* metodoloģijas aprakstīšana.



Tālākie plāni



- Jauna mūķa vai *BrakTooth* moduļa izveidošana.
- *BrakTooth* pielāgošana darbam ar jaunākiem *Linux* kodoliem.
- Eksperimenti ar *ToothPicker* (pielāgot jaunākai *iOS*, github.com/seemoo-lab/toothpicker).
- Eksperimenti ar *Frankenstein* (nepieciešama *Infineon* CYW20735 ierīce, github.com/seemoo-lab/frankenstein).
- Eksperimenti ar *SwaynTooth* (github.com/Matheus-Garbelini/sweyntooth_bluetooth_low_energy_attacks un git.ist.tugraz.at/apferscher/ble-fuzzing).



PALDIES

Jautājumi?