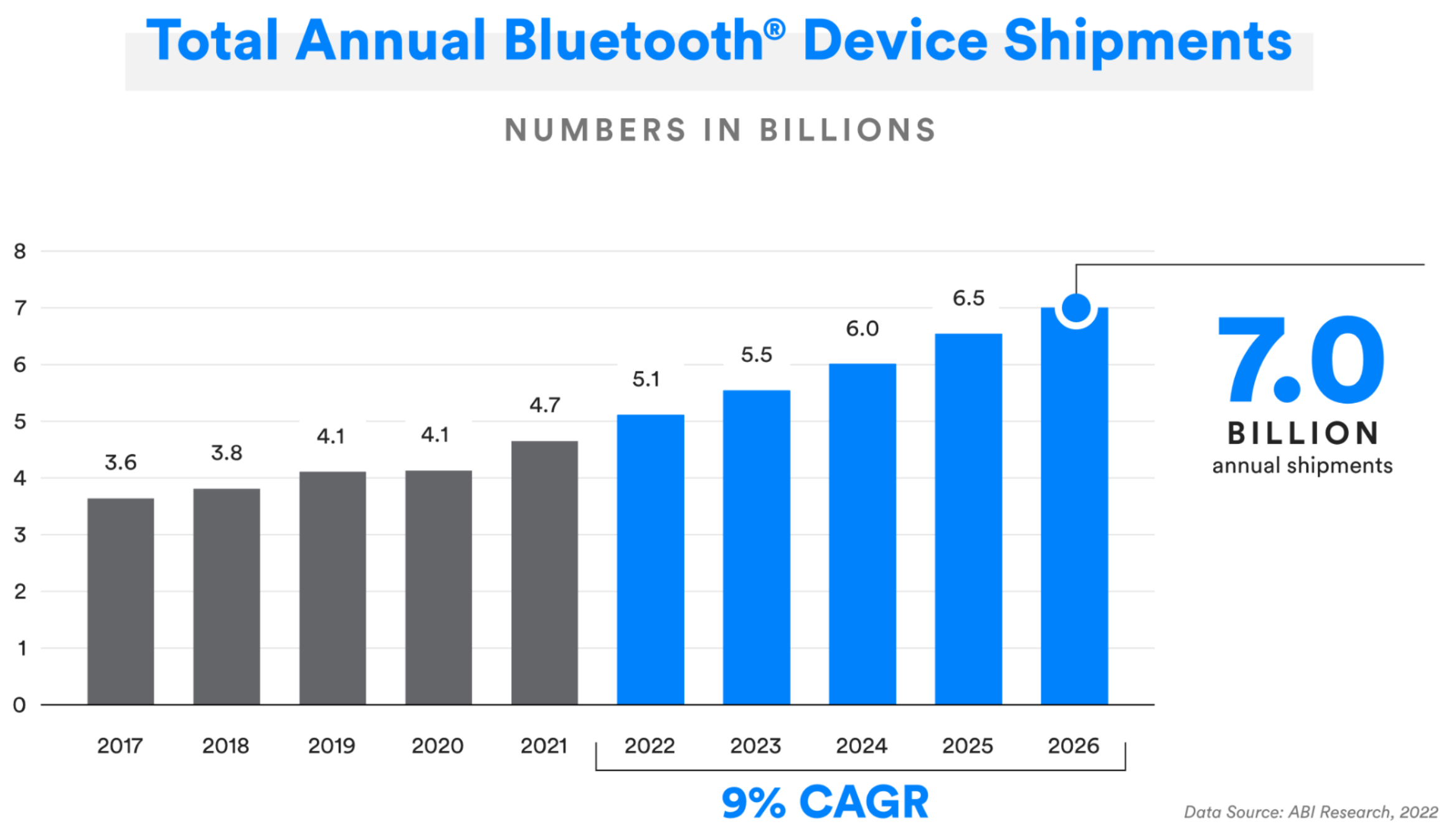
LIGHTBLUE: Automatic Profile-Aware Debloating of Bluetooth Stacks

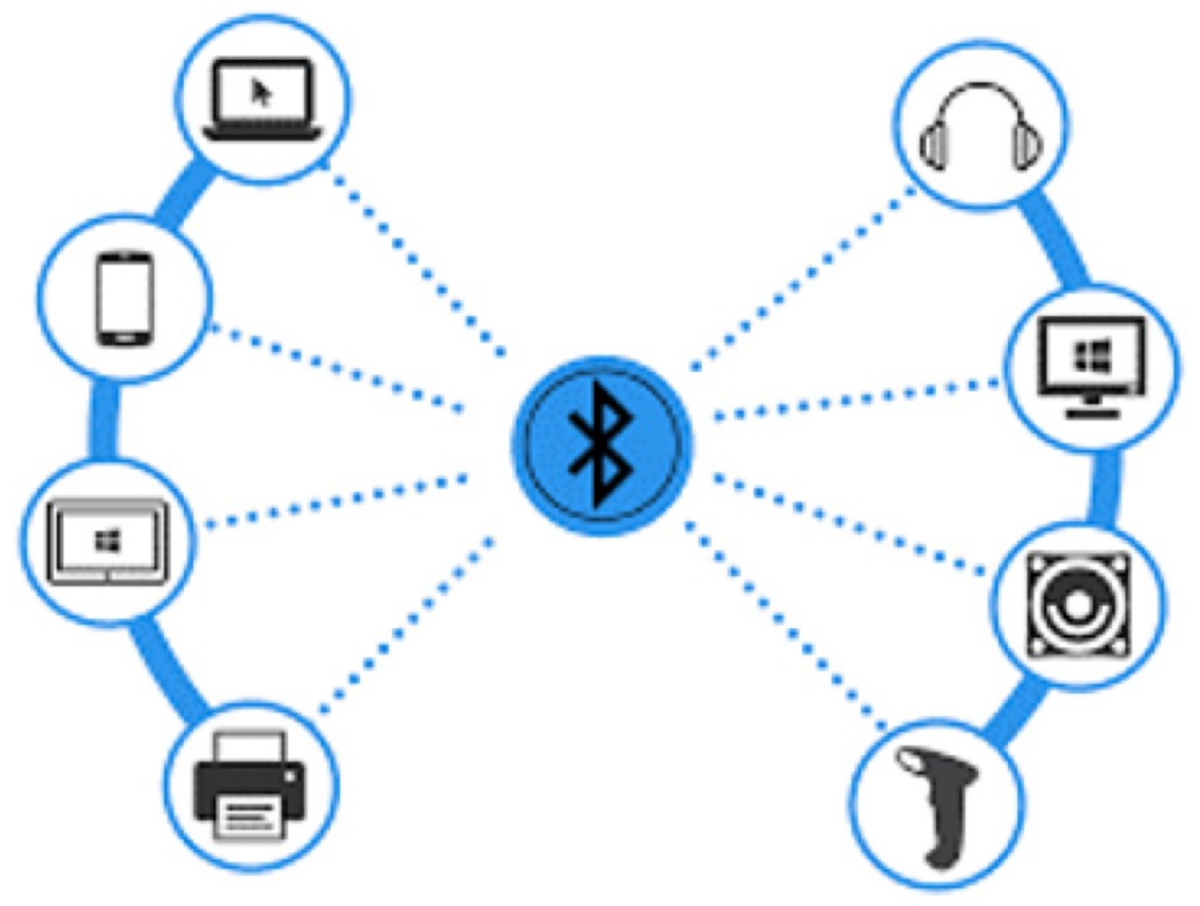
This project was supported in part by ONR under grants N00014-18-1-2674 and N00014-17-1-2513

Jianliang Wu, Ruoyu Wu, Daniele Antonioli, Mathias Payer, Nils Ole Tippenhauer, Dongyan Xu, Dave (Jing) Tian, Antonio Bianchi

Bluetooth Devices Are Everywhere

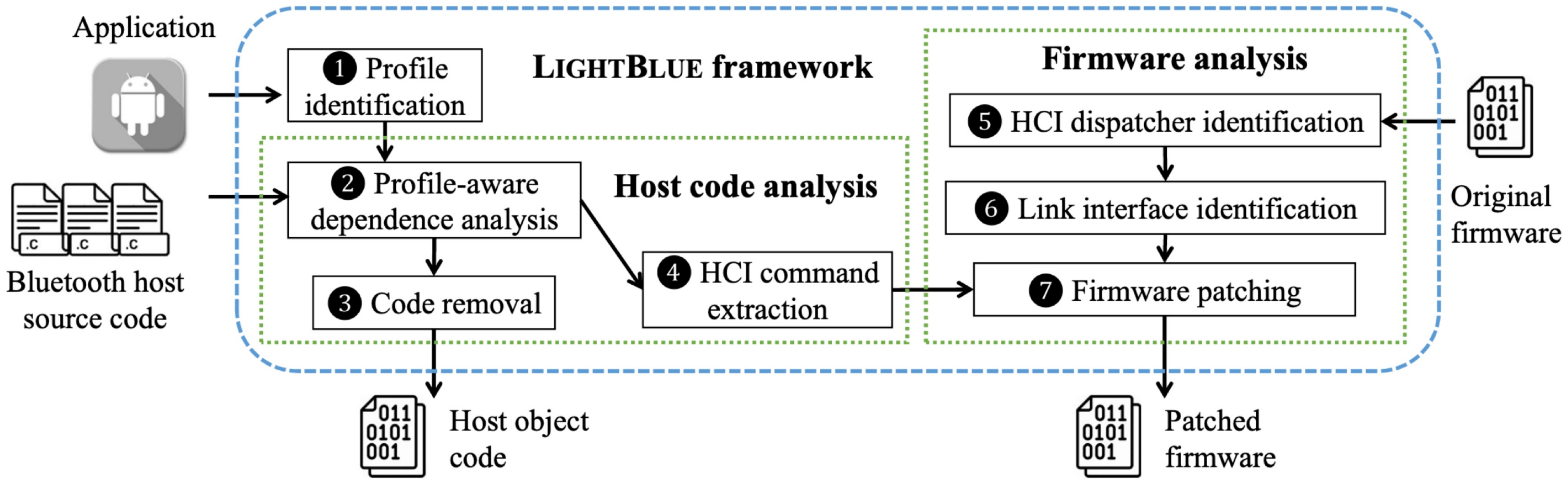


Source: https://www.bluetooth.com/2022-market-update/



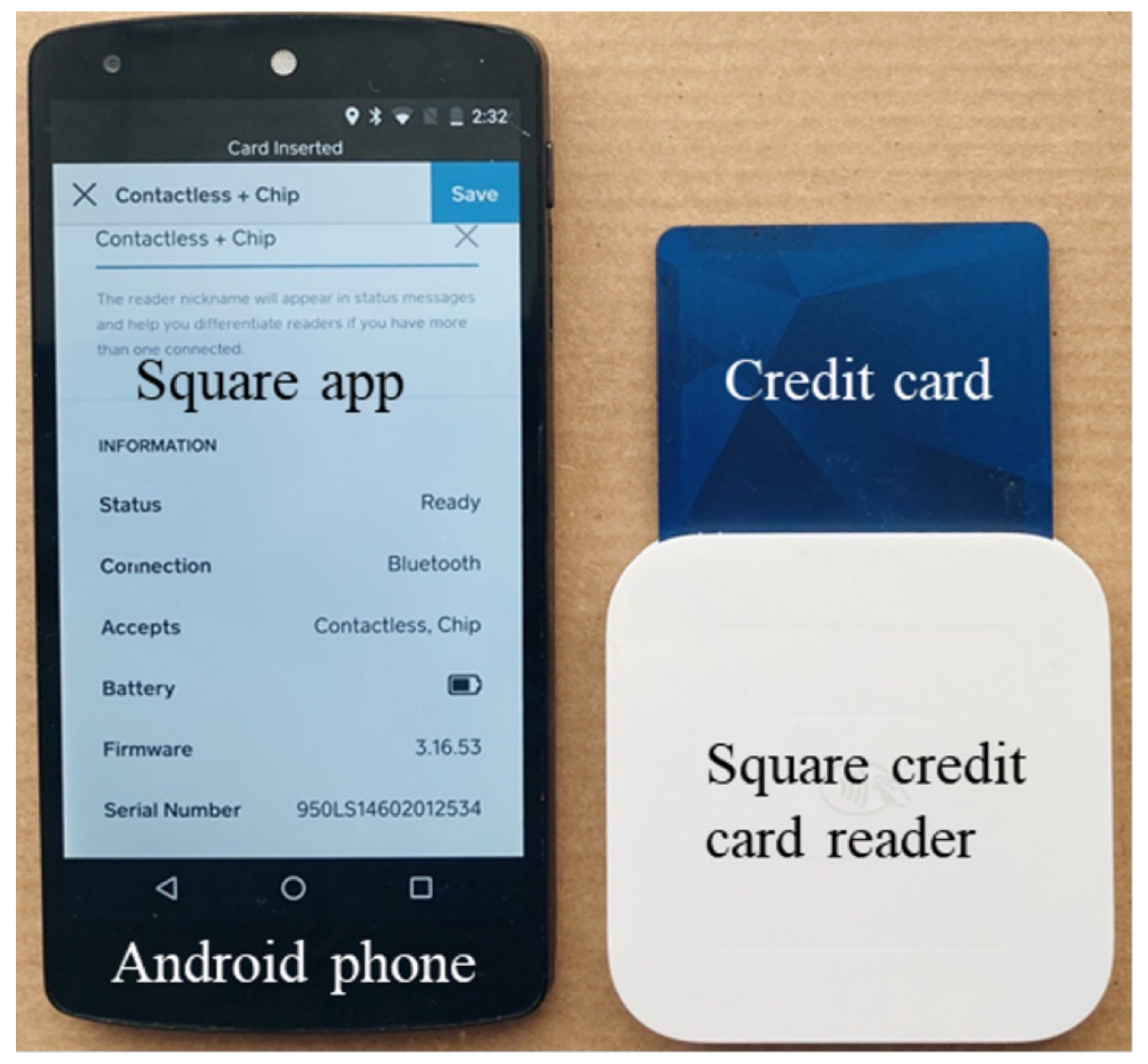
Headsets
Smartphones
IoT devices

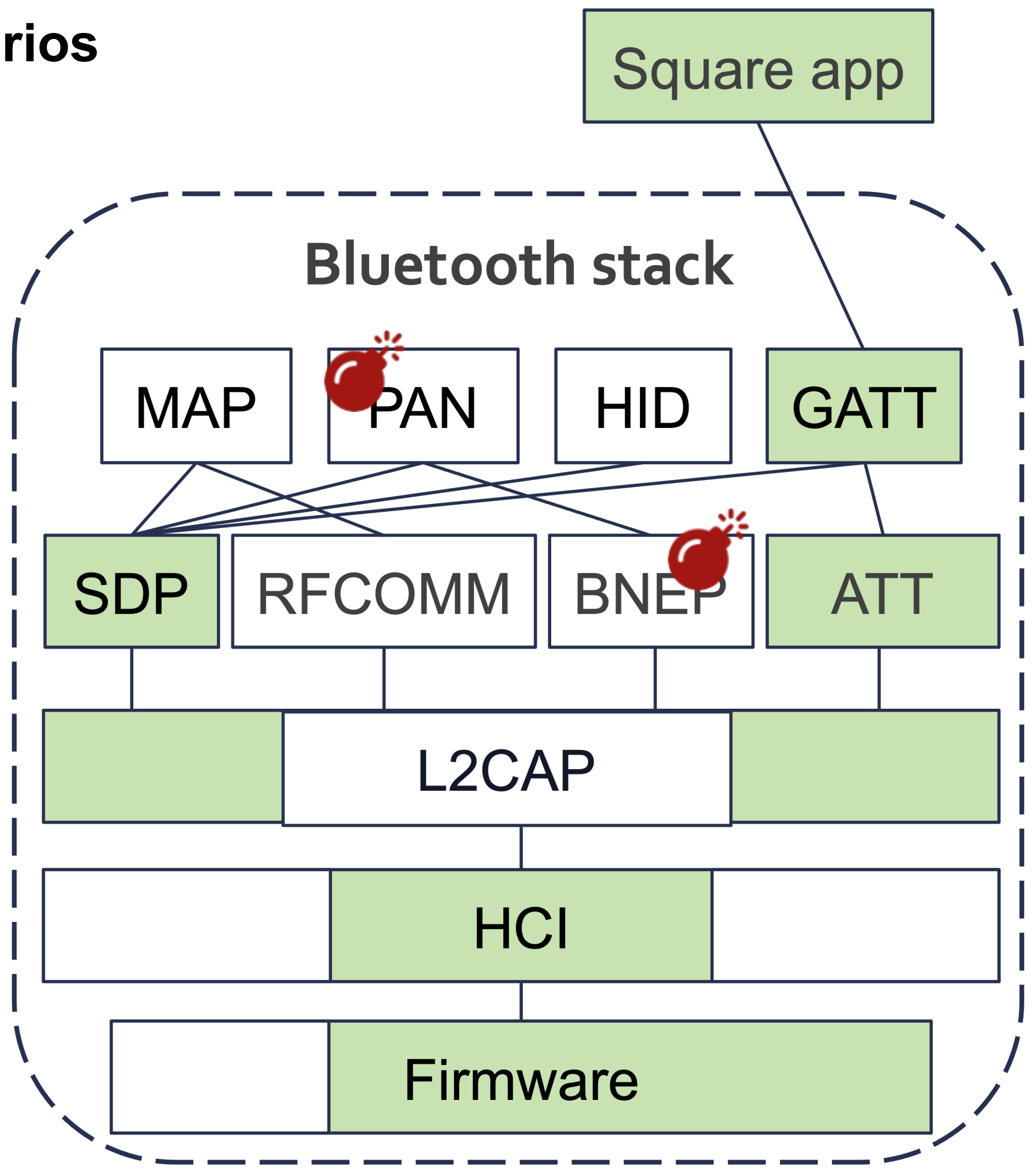
LightBlue Framework



Bluetooth Stack Is Bloated and Vulnerable

- **The host code supports multiple usage scenarios**
- **The firmware supports diverse functionalities**





In many use cases, limited functionality is needed while the nonessential functionalities may contain vulnerabilities [1]

Debloat the Bluetooth stack to reduce attack surface!

Existing Debloating Approaches Cannot Be Directly Applied

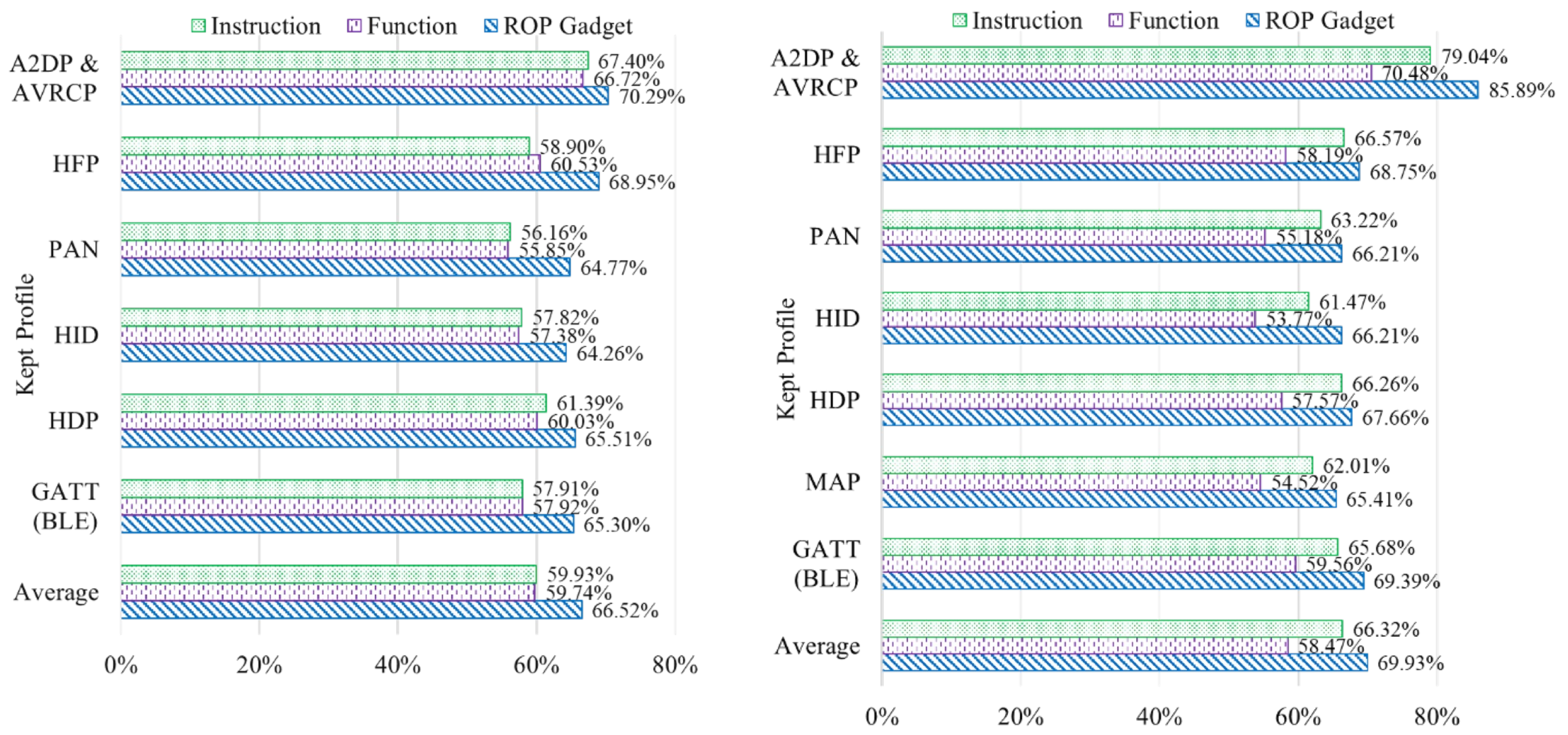
Existing debloating methods require that the program has a single entry point while the Bluetooth stack may have several entry points

The code of different functionalities are coupled together

The host code and firmware are two separated pieces of software that do not directly call each other and run on different CPUs

Evaluation

(a) Host Code Debloating



(b) Prevented CVEs

Vul. Loc.	Related Profile	Platform	# of Vul. Functions	CVE Number
HO	A2DP & (AVRCP)	Plt. 1	4	CVE-2018-9542* CVE-2018-9450* CVE-2017-13266* CVE-2018-9453
		Plt. 4	7	CVE-2019-2227* CVE-2018-9588* CVE-2018-9507* CVE-2018-9506* CVE-2019-2049
	PAN	Plt. 1	7	CVE-2017-0783* CVE-2017-0782* CVE-2017-0781* CVE-2018-9436* CVE-2018-9356* CVE-2018-9357 CVE-2017-13269
	MAP	Plt. 4	1	CVE-2018-9505*
	HSP/HFP	Plt. 4	5	CVE-2018-9583*
	N/A	Plt. 4	1	CVE-2019-2226
FM	GATT	Plt. 3	1	CVE-2019-13916*

*: CVEs that can be triggered by over-the-air attacks.

(c) Firmware Debloating

Platform	Plt. 1			Plt. 2			Plt. 3		
Host Code	BlueDroid			BlueZ			BlueKitchen		
Bluetooth Chip	BCM4339			BCM43430A1			CYW20735B1		
# of Cmds Processed by Firmware	310			299			423		
out of which vendor-specific	*135*			*93*			*174*		
# of Cmds Processed by Host Code	138			144			131		
Kept Profile	HFP	GATT	Others[1]	HFP	GATT	Others	HFP	GATT	Others
Needed Link(s)	ACL & SCO	LE ACL[2] & ADVB[3]	ACL	ACL & SCO	LE ACL & ADVB	ACL	ACL & SCO	LE ACL & ADVB	ACL
# of Cmds Processed by Firmware and Removed by Debloating	192	196	195	171	172	174	352	354	354
out of which vendor-specific	*125*	*125*	*125*	*88*	*88*	*88*	*171*	*171*	*171*
# of Cmds Processed by Host Code and Removed by Debloating	20	24	23	16	17	19	60	62	62
# of Cmds Removed by Debloating	192 (64.2%)	196 (65.6%)	195 (65.2%)	171 (57.2%)	172 (57.5%)	174 (58.2%)	352 (83.2%)	354 (83.7%)	354 (83.7%)

1. Other profiles supported on the platform. 2. Low Energy Asynchronous Connection. 3. LE Advertising Broadcast link.

Our paper [2], code [3], video tutorial, and virtual machine image are publicly available online!

[1]. BlueBorne, https://www.armis.com/research/blueborne/

[2]. LightBlue (USENIX SEC'21), https://www.usenix.org/conference/usenixsecurity21/presentation/wu-jianliang

[3]. LightBlue code, https://github.com/purseclab/lightblue