Deanonymizing Device Identities via Side-Channel Attacks in Exclusive-use IoTs & Mitigation

Christopher Ellis*, Yue Zhang†, Mohit Kumar Jangid*, Shixuan Zhao*, and Zhiqiang Lin*

*The Ohio State University, †Drexel University

Network and Distributed System Security - 2025

Bottom Line Up Front

Our research reveals a historically overlooked, **fundamental flaw** in ubiquitous wireless technologies enabling **tracking attacks** that we introduce as **IDBleed.**

Bottom Line Up Front

Our mitigation, **Anonymization Layer**, removes data flow directionality, context, and provides pseudo-responses with an **approximate 2% overhead** to throughput and power consumption.

Motivation

Inspiration

- Packets are observable
- Exclusively paired devices exhibit different communication patterns
- Side-channel effect: boolean indicator of relationship

What does this mean?

- Deanonymizing **exclusive-use devices** via side-channel observation
- Enabling **tracking attacks**

Motivation

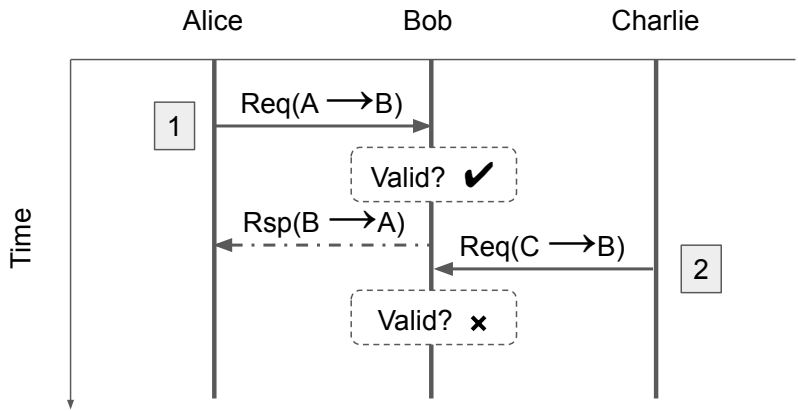
Inspiration

- Packets are observable
- Exclusively paired devices exhibit different communication patterns
- Side-channel effect: boolean indicator of relationship

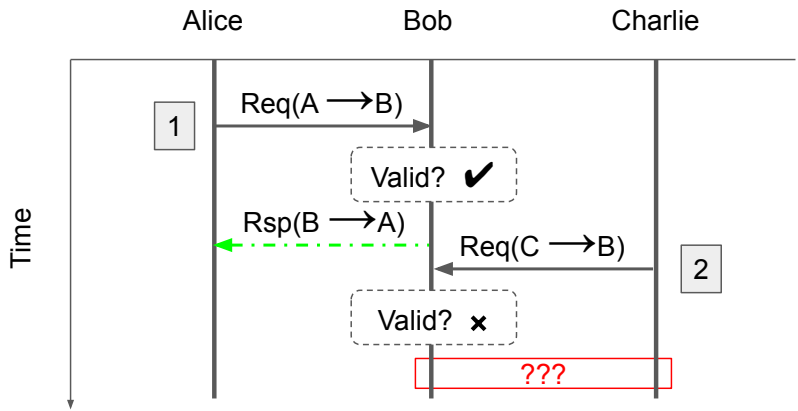
What does this mean?

- Deanonymizing **exclusive-use devices** via side-channel observation
- Enabling **tracking attacks**

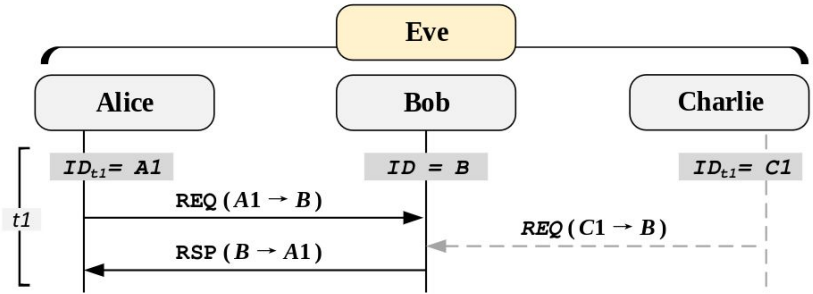
Observable Side-channel



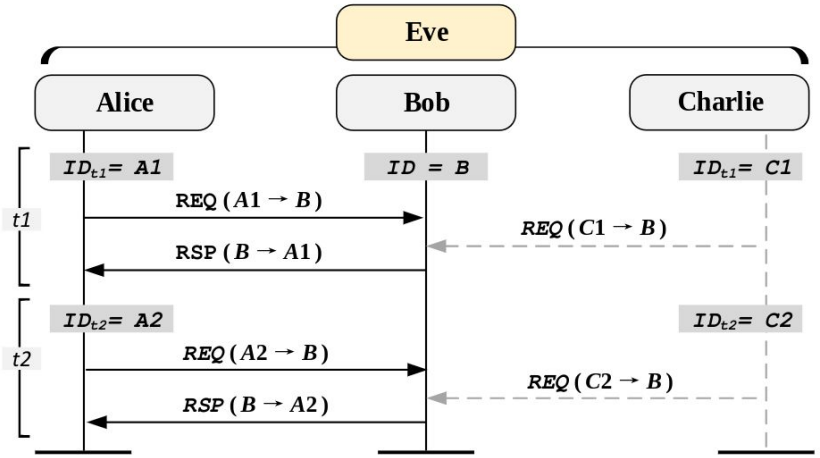
Exclusive-Use



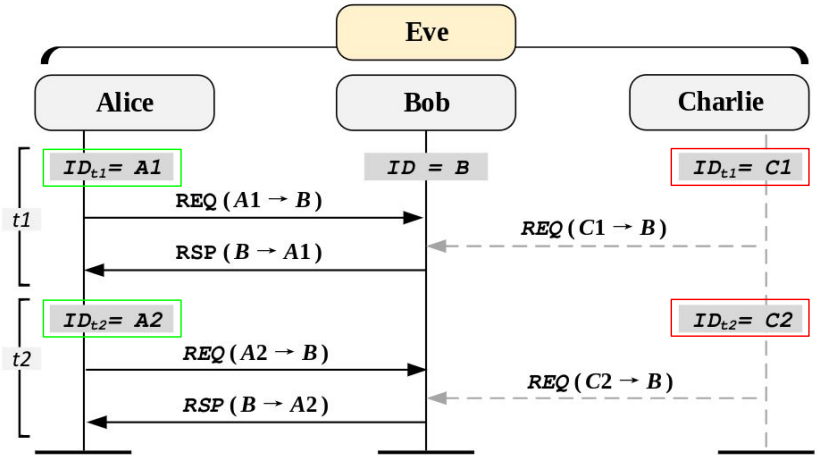
Passive Deanonymization



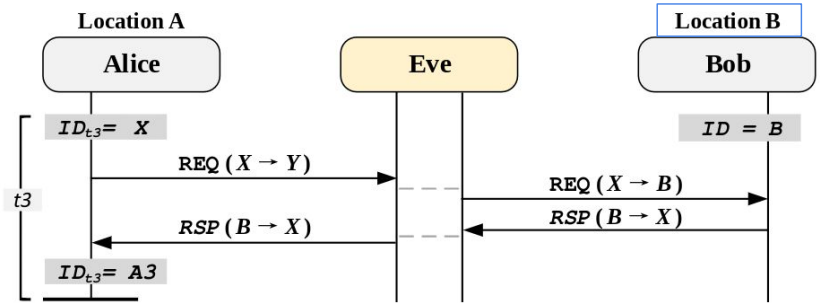
Passive Deanonymization



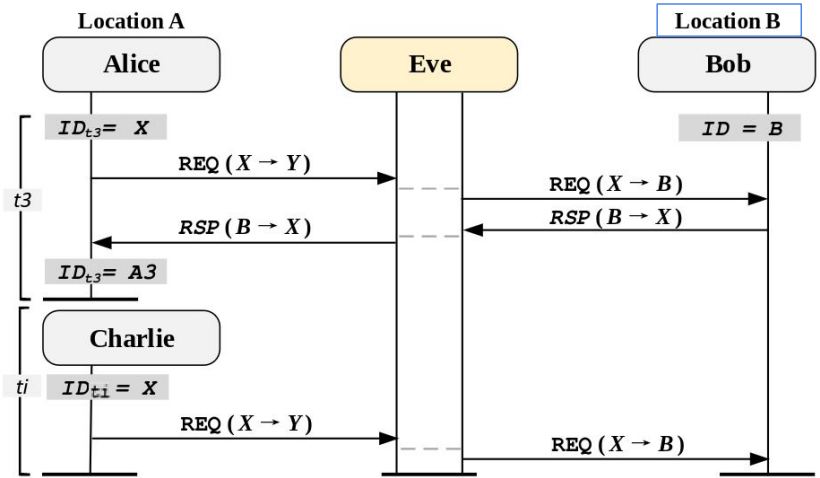
Passive Deanonymization



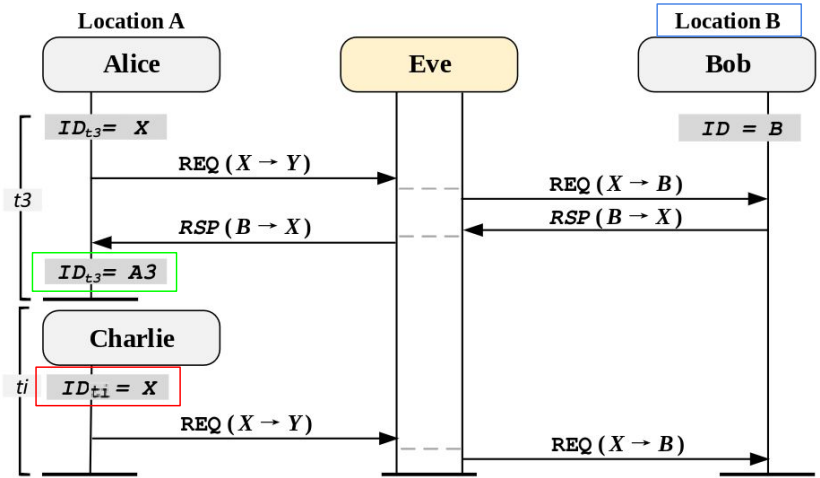
Active Deanonymization



Active Deanonymization



Active Deanonymization

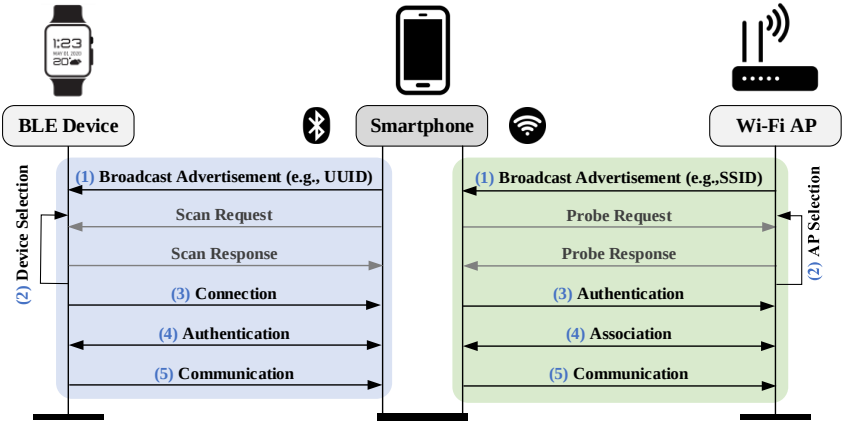


Protocol Investigations

Confidentiality, Integrity, Authentication, Auto-connection

1. BLE: Secure Connections (Confidentiality)
2. BLE: Connection Data Signing Procedure (Verification)
3. Wi-Fi: Authentication and Auto-connection
4. IoT smarthome companion apps / devices

Wireless Workflows

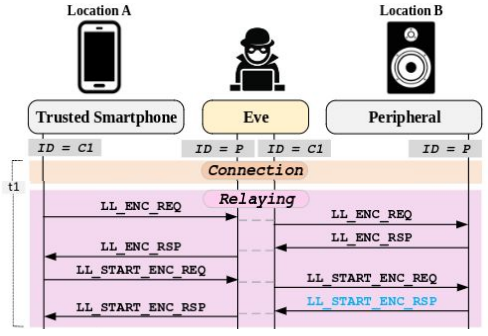


Typical BLE and Wi-Fi workflows.

BLE Confidentiality: Passive Attack

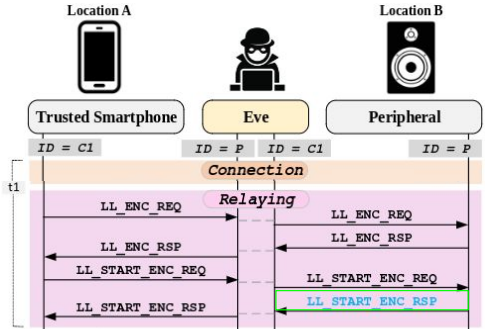
No.	Time	Source ID	Destination ID	PDU Type
	t0 = 0 min, C0 = ad:d8:3e:a9:ba:52 (Passive attacker)			
1	00:00:36	58:d7:8e:c7:8e:31	Broadcast	ADV_IND
2	00:00:40	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	SCAN_REQ
3	00:00:44	58:d7:8e:c7:8e:31	Broadcast	SCAN_RSP
4	00:00:48	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	CONNECT_REQ
5	00:01:00	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	LL_ENC_REQ
6	00:01:04	58:d7:8e:c7:8e:31	ad:d8:3e:a9:ba:52	LL_ENC_RSP
7	00:01:12	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	LL_START_ENC_REQ
8	00:01:16	58:d7:8e:c7:8e:31	ad:d8:3e:a9:ba:52	LL_START_ENC_RSP

BLE Confidentiality: Active Attack



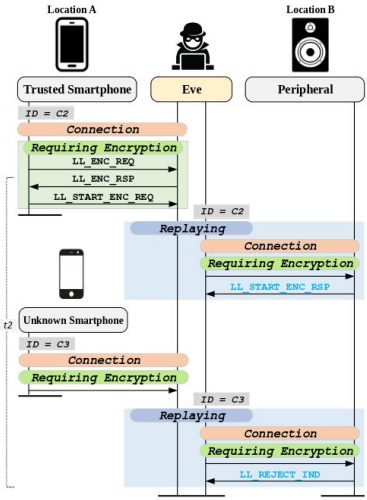
No.	Time	Source ID	Destination ID	PDU Type
t0 = 0 min, C0 = `ad:d8:3e:a9:ba:52` **(Passive attacker)**				
1	00:00:36	58:d7:8e:c7:8e:31	Broadcast	ADV_IND
2	00:00:40	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	SCAN_REQ
3	00:00:44	58:d7:8e:c7:8e:31	Broadcast	SCAN_RSP
4	00:00:48	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	CONNECT_REQ
5	00:01:00	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	LL_ENC_REQ
6	00:01:04	58:d7:8e:c7:8e:31	ad:d8:3e:a9:ba:52	LL_ENC_RSP
7	00:01:12	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	LL_START_ENC_REQ
8	00:01:16	58:d7:8e:c7:8e:31	ad:d8:3e:a9:ba:52	LL_START_ENC_RSP
t1 = 15 min, C1 = `be:a4:4e:dd:af:ee` **(Active Attacker Using Relaying)**				
101	00:15:36	58:d7:8e:c7:8e:31	Broadcast	ADV_IND
102	00:15:40	be:a4:4e:dd:af:ee	58:d7:8e:c7:8e:31	SCAN_REQ
103	00:15:44	58:d7:8e:c7:8e:31	Broadcast	SCAN_RSP
104	00:15:48	be:a4:4e:dd:af:ee	58:d7:8e:c7:8e:31	CONNECT_REQ
105	00:16:00	be:a4:4e:dd:af:ee	58:d7:8e:c7:8e:31	LL_ENC_REQ
106	00:16:04	58:d7:8e:c7:8e:31	be:a4:4e:dd:af:ee	LL_ENC_RSP
107	00:16:12	be:a4:4e:dd:af:ee	58:d7:8e:c7:8e:31	LL_START_ENC_REQ
108	00:16:16	58:d7:8e:c7:8e:31	be:a4:4e:dd:af:ee	LL_START_ENC_RSP

BLE Confidentiality: Active Attack



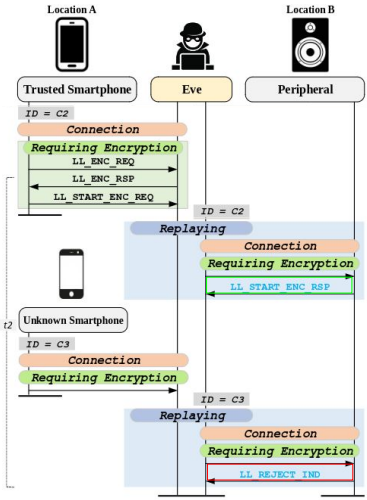
No.	Time	Source ID	Destination ID	PDU Type
		t0 = 0 min, C0 = ad:d8:3e:a9:ba:52 **(Passive attacker)**		
1	00:00:36	58:d7:8e:c7:8e:31	Broadcast	ADV_IND
2	00:00:40	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	SCAN_REQ
3	00:00:44	58:d7:8e:c7:8e:31	Broadcast	SCAN_RSP
4	00:00:48	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	CONNECT_REQ
5	00:01:00	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	LL_ENC_REQ
6	00:01:04	58:d7:8e:c7:8e:31	ad:d8:3e:a9:ba:52	LL_ENC_RSP
7	00:01:12	ad:d8:3e:a9:ba:52	58:d7:8e:c7:8e:31	LL_START_ENC_REQ
8	00:01:16	58:d7:8e:c7:8e:31	ad:d8:3e:a9:ba:52	LL_START_ENC_RSP
		t1 = 15 min, C1 = be:a4:4e:dd:af:ee **(Active Attacker Using Relaying)**		
101	00:15:36	58:d7:8e:c7:8e:31	Broadcast	ADV_IND
102	00:15:40	be:a4:4e:dd:af:ee	58:d7:8e:c7:8e:31	SCAN_REQ
103	00:15:44	58:d7:8e:c7:8e:31	Broadcast	SCAN_RSP
104	00:15:48	be:a4:4e:dd:af:ee	58:d7:8e:c7:8e:31	CONNECT_REQ
105	00:16:00	be:a4:4e:dd:af:ee	58:d7:8e:c7:8e:31	LL_ENC_REQ
106	00:16:04	58:d7:8e:c7:8e:31	be:a4:4e:dd:af:ee	LL_ENC_RSP
107	00:16:12	be:a4:4e:dd:af:ee	58:d7:8e:c7:8e:31	LL_START_ENC_REQ
108	00:16:16	58:d7:8e:c7:8e:31	be:a4:4e:dd:af:ee	LL_START_ENC_RSP

BLE Confidentiality: Active Attack



No.	Time	Source ID	Destination ID	PDU Type
		t2 = 30 min (Active Attacker Using Replay)		
		C2 = ae:f4:3f:d9:aa:12		
201	00:30:36	58:d7:8e:c7:8e:31	Broadcast	ADV_IND
202	00:30:40	ae:f4:3f:d9:aa:12	58:d7:8e:c7:8e:31	SCAN_REQ
203	00:30:44	58:d7:8e:c7:8e:31	Broadcast	SCAN_RSP
204	00:30:48	ae:f4:3f:d9:aa:12	58:d7:8e:c7:8e:31	CONNECT_REQ
205	00:31:00	ae:f4:3f:d9:aa:12	58:d7:8e:c7:8e:31	LL_ENC_REQ
206	00:31:04	58:d7:8e:c7:8e:31	ae:f4:3f:d9:aa:12	LL_ENC_RSP
207	00:31:12	ae:f4:3f:d9:aa:12	58:d7:8e:c7:8e:31	LL_START_ENC_REQ
208	00:31:16	58:d7:8e:c7:8e:31	ae:f4:3f:d9:aa:12	LL_START_ENC_RSP
		C3 = cf:ad:34:fe:ab:ee		
211	00:30:36	58:d7:8e:c7:8e:31	Broadcast	ADV_IND
212	00:30:40	cf:ad:34:fe:ab:ee	58:d7:8e:c7:8e:31	SCAN_REQ
213	00:30:44	58:d7:8e:c7:8e:31	Broadcast	SCAN_RSP
214	00:30:48	cf:ad:34:fe:ab:ee	58:d7:8e:c7:8e:31	CONNECT_REQ
215	00:31:00	cf:ad:34:fe:ab:ee	58:d7:8e:c7:8e:31	LL_ENC_REQ
216	00:31:04	58:d7:8e:c7:8e:31	cf:ad:34:fe:ab:ee	LL_ENC_RSP
217	00:31:12	cf:ad:34:fe:ab:ee	58:d7:8e:c7:8e:31	LL_START_ENC_REQ
218	00:31:16	58:d7:8e:c7:8e:31	cf:ad:34:fe:ab:ee	LL_REJECT_IND

BLE Confidentiality: Active Attack



No.	Time	Source ID	Destination ID	PDU Type
		t2 = 30 min (Active Attacker Using Replay)		
		C2 = ae:f4:3f:d9:aa:12		
201	00:30:36	58:d7:8e:c7:8e:31	Broadcast	ADV_IND
202	00:30:40	ae:f4:3f:d9:aa:12	58:d7:8e:c7:8e:31	SCAN_REQ
203	00:30:44	58:d7:8e:c7:8e:31	Broadcast	SCAN_RSP
204	00:30:48	ae:f4:3f:d9:aa:12	58:d7:8e:c7:8e:31	CONNECT_REQ
205	00:31:00	ae:f4:3f:d9:aa:12	58:d7:8e:c7:8e:31	LL_ENC_REQ
206	00:31:04	58:d7:8e:c7:8e:31	ae:f4:3f:d9:aa:12	LL_ENC_RSP
207	00:31:12	ae:f4:3f:d9:aa:12	58:d7:8e:c7:8e:31	LL_START_ENC_REQ
208	00:31:16	58:d7:8e:c7:8e:31	ae:f4:3f:d9:aa:12	LL_START_ENC_RSP
		C3 = cf:ad:34:fe:ab:ee		
211	00:30:36	58:d7:8e:c7:8e:31	Broadcast	ADV_IND
212	00:30:40	cf:ad:34:fe:ab:ee	58:d7:8e:c7:8e:31	SCAN_REQ
213	00:30:44	58:d7:8e:c7:8e:31	Broadcast	SCAN_RSP
214	00:30:48	cf:ad:34:fe:ab:ee	58:d7:8e:c7:8e:31	CONNECT_REQ
215	00:31:00	cf:ad:34:fe:ab:ee	58:d7:8e:c7:8e:31	LL_ENC_REQ
216	00:31:04	58:d7:8e:c7:8e:31	cf:ad:34:fe:ab:ee	LL_ENC_RSP
217	00:31:12	cf:ad:34:fe:ab:ee	58:d7:8e:c7:8e:31	LL_START_ENC_REQ
218	00:31:16	58:d7:8e:c7:8e:31	cf:ad:34:fe:ab:ee	LL_REJECT_IND

Wi-Fi: Passive and Active Attack

No.	Time	Source ID	Destination ID	Type
t0 = 0 min, C0 = `0e:8d:ae:c7:1e:50` (Passive Attacker)				
1	00:00:16	`0e:8d:ae:c7:1e:50`	`ff:ff:ff:ff`	PROBE_REQ
2	00:00:40	`12:df:a9:ef:fb:52`	`0e:8d:ae:c7:1e:50`	PROBE_RSP
3	00:00:44	`0e:8d:ae:c7:1e:50`	`12:df:a9:ef:fb:52`	INVITATION_REQ
4	00:00:48	`12:df:a9:ef:fb:52`	`0e:8d:ae:c7:1e:50`	INVITATION_RSP
5	00:00:54	`0e:8d:ae:c7:1e:50`	`12:df:a9:ef:fb:52`	PROBE_REQ
6	00:00:58	`12:df:a9:ef:fb:52`	`0e:8d:ae:c7:1e:50`	PROBE_RSP
7	00:01:00	`0e:8d:ae:c7:1e:50`	`12:df:a9:ef:fb:52`	AUTH
8	00:01:04	`12:df:a9:ef:fb:52`	`0e:8d:ae:c7:1e:50`	AUTH
9	00:01:12	`0e:8d:ae:c7:1e:50`	`12:df:a9:ef:fb:52`	ASSOC_REQ
10	00:01:16	`12:df:a9:ef:fb:52`	`0e:8d:ae:c7:1e:50`	ASSOC_RSP
t1 = 15 min, C1 = `0f:9e:fe:c2:2e:23` (Active Attacker Using Relay)				
201	00:15:16	`0f:9e:fe:c2:2e:23`	`ff:ff:ff:ff`	PROBE_REQ
202	00:15:40	`12:df:a9:ef:fb:52`	`0f:9e:fe:c2:2e:23`	PROBE_RSP
203	00:15:44	`0f:9e:fe:c2:2e:23`	`12:df:a9:ef:fb:52`	INVITATION_REQ
204	00:15:48	`12:df:a9:ef:fb:52`	`0f:9e:fe:c2:2e:23`	INVITATION_RSP
205	00:15:54	`0f:9e:fe:c2:2e:23`	`12:df:a9:ef:fb:52`	PROBE_REQ
206	00:15:58	`12:df:a9:ef:fb:52`	`0f:9e:fe:c2:2e:23`	PROBE_RSP
207	00:16:00	`0f:9e:fe:c2:2e:23`	`12:df:a9:ef:fb:52`	AUTH
208	00:16:04	`12:df:a9:ef:fb:52`	`0f:9e:fe:c2:2e:23`	AUTH

Wi-Fi: Passive and Active Attack

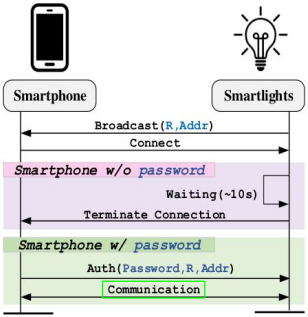
No.	Time	Source ID	Destination ID	Type
t0 = 0 min, C0 = `0e:8d:ae:c7:1e:50` (Passive Attacker)				
1	00:00:16	`0e:8d:ae:c7:1e:50`	`ff:ff:ff:ff`	PROBE_REQ
2	00:00:40	`12:df:a9:ef:fb:52`	`0e:8d:ae:c7:1e:50`	PROBE_RSP
3	00:00:44	`0e:8d:ae:c7:1e:50`	`12:df:a9:ef:fb:52`	INVITATION_REQ
4	00:00:48	`12:df:a9:ef:fb:52`	`0e:8d:ae:c7:1e:50`	INVITATION_RSP
5	00:00:54	`0e:8d:ae:c7:1e:50`	`12:df:a9:ef:fb:52`	PROBE_REQ
6	00:00:58	`12:df:a9:ef:fb:52`	`0e:8d:ae:c7:1e:50`	PROBE_RSP
7	00:01:00	`0e:8d:ae:c7:1e:50`	`12:df:a9:ef:fb:52`	AUTH
8	00:01:04	`12:df:a9:ef:fb:52`	`0e:8d:ae:c7:1e:50`	AUTH
9	00:01:12	`0e:8d:ae:c7:1e:50`	`12:df:a9:ef:fb:52`	ASSOC_REQ
10	00:01:16	`12:df:a9:ef:fb:52`	`0e:8d:ae:c7:1e:50`	ASSOC_RSP
t1 = 15 min, C1 = `0f:9e:fe:c2:2e:23` (Active Attacker Using Relay)				
201	00:15:16	`0f:9e:fe:c2:2e:23`	`ff:ff:ff:ff`	PROBE_REQ
202	00:15:40	`12:df:a9:ef:fb:52`	`0f:9e:fe:c2:2e:23`	PROBE_RSP
203	00:15:44	`0f:9e:fe:c2:2e:23`	`12:df:a9:ef:fb:52`	INVITATION_REQ
204	00:15:48	`12:df:a9:ef:fb:52`	`0f:9e:fe:c2:2e:23`	INVITATION_RSP
205	00:15:54	`0f:9e:fe:c2:2e:23`	`12:df:a9:ef:fb:52`	PROBE_REQ
206	00:15:58	`12:df:a9:ef:fb:52`	`0f:9e:fe:c2:2e:23`	PROBE_RSP
207	00:16:00	`0f:9e:fe:c2:2e:23`	`12:df:a9:ef:fb:52`	AUTH
208	00:16:04	`12:df:a9:ef:fb:52`	`0f:9e:fe:c2:2e:23`	AUTH

BLE Companion Apps

Device	Type	Channel	Exclusive-Use	Passive Attacks	Active Attacks
AppLights Standards	Light	BLE	❸ ❹	✓	✓
AppLights C9	Light	BLE	❶ ❸ ❹	✓	✓
AppLights Strings	Light	BLE	❶ ❸ ❹	✓	✓
i-Health Labs	Medical	BLE	❸ ❹	✓	✓
Ultraloq	Lock	BLE	❶ ❷ ❸ ❹	✓	✓
Kasa Plug	Plug	Wi-Fi	❸ ❹	✓	✓

Tested IoT devices. ❶ Verification, ❷ Encryption, ❸ Authentication, ❹ Auto-connection

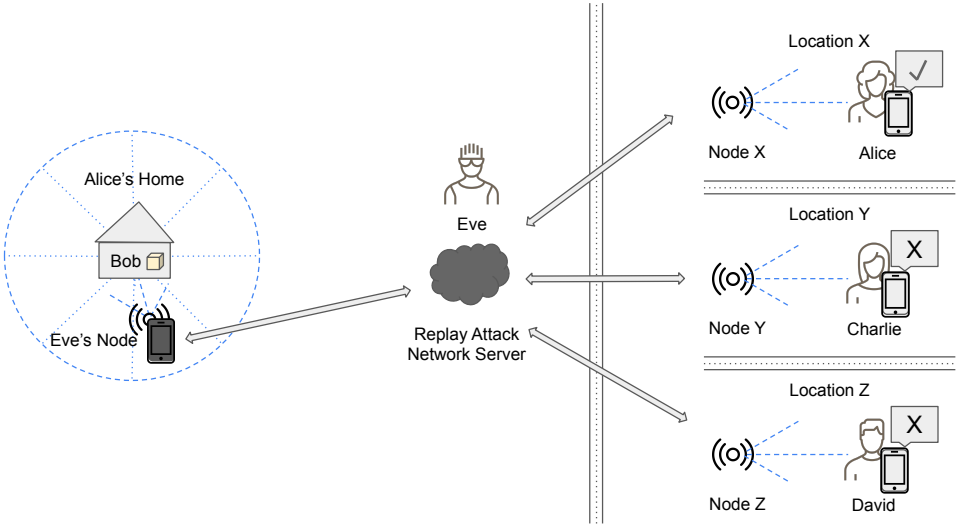
BLE Companion Apps



No.	Time	Source ID	Destination ID	PDU Type	PDU Playload
		Smartphone w/o Password			
1	00:36	98:7b:f3:78:d0:ad	Broadcast	ADV_IND	ADDR
2	00:40	ad:d8:3e:a9:ba:52	98:7b:f3:78:d0:ad	SCAN_REQ	EMPTY
3	00:44	98:7b:f3:78:d0:ad	Broadcast	SCAN_RSP	RAND
4	00:48	ad:d8:3e:a9:ba:52	98:7b:f3:78:d0:ad	CONNECT_REQ	EMPTY
5	01:00	ad:d8:3e:a9:ba:52	98:7b:f3:78:d0:ad	ATT_WRITE	DISCOVER_SERVICES
6	01:04	98:7b:f3:78:d0:ad	ad:d8:3e:a9:ba:52	ATT_READ	0xFFF1
7	01:12	ad:d8:3e:a9:ba:52	98:7b:f3:78:d0:ad	EMPTY_PDU	EMPTY
8	01:22	98:7b:f3:78:d0:ad	ad:d8:3e:a9:ba:52	LL_TERMINATE_IND	EMPTY
		Smartphone w/ Password			
1	00:36	98:7b:f3:78:d0:ad	Broadcast	ADV_IND	ADDR
2	00:40	ad:d8:3e:a9:ba:52	98:7b:f3:78:d0:ad	SCAN_REQ	EMPTY
3	00:44	98:7b:f3:78:d0:ad	Broadcast	SCAN_RSP	RAND
4	00:48	ad:d8:3e:a9:ba:52	98:7b:f3:78:d0:ad	CONNECT_REQ	EMPTY
5	01:00	ad:d8:3e:a9:ba:52	98:7b:f3:78:d0:ad	ATT_WRITE	DISCOVER_SERVICES
6	01:04	98:7b:f3:78:d0:ad	ad:d8:3e:a9:ba:52	ATT_READ	0xFFF1
7	01:12	ad:d8:3e:a9:ba:52	98:7b:f3:78:d0:ad	ATT_WRITE	AUTH(PASS, RAND, ADDR)
8	01:16	98:7b:f3:78:d0:ad	ad:d8:3e:a9:ba:52	ATT_READ	NOTIFY(OK)

Packet capture excerpt from AppLights

Distributed Relay/Replay Attack Network



Mitigation: Introducing *Anonymization Layer*

A defense against *IDBleed* must provide:

1. Indistinguishable Transmission Direction
2. Hide Context / Provide Entropy
3. Provide Untrusted Responses
4. No Modifications - Separate / Additional Layer

Mitigation: Introducing *Anonymization Layer*

A defense against *IDBleed* must provide:

1. Indistinguishable Transmission Direction
2. Hide Context / Provide Entropy
3. Provide Untrusted Responses
4. No Modifications - Separate / Additional Layer

Mitigation: Introducing *Anonymization Layer*

A defense against *IDBleed* must provide:

1. Indistinguishable Transmission Direction
2. Hide Context / Provide Entropy
3. Provide Untrusted Responses
4. No Modifications - Separate / Additional Layer

Mitigation: Introducing *Anonymization Layer*

A defense against *IDBleed* must provide:

1. Indistinguishable Transmission Direction
2. Hide Context / Provide Entropy
3. Provide Untrusted Responses
4. No Modifications - Separate / Additional Layer

Anonymization Layer: Features

1. **Broadcast**: Random addresses removes linkability
2. **Encryption**: Removes meta information and context
3. **Pseudo Response**: Indistinguishable, tunable random responses
4. **Self-Contained**: Transparent to adjacent layers (eBPF, kernel modules)

Anonymization Layer: Features

1. **Broadcast**: Random addresses removes linkability
2. **Encryption**: Removes meta information and context
3. **Pseudo Response**: Indistinguishable, tunable random responses
4. **Self-Contained**: Transparent to adjacent layers (eBPF, kernel modules)

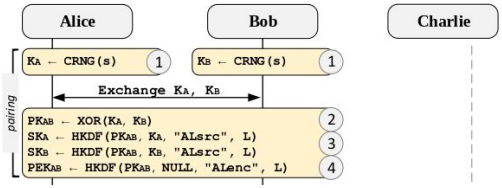
Anonymization Layer: Features

1. **Broadcast**: Random addresses removes linkability
2. **Encryption**: Removes meta information and context
3. **Pseudo Response**: Indistinguishable, tunable random responses
4. **Self-Contained**: Transparent to adjacent layers (eBPF, kernel modules)

Anonymization Layer: Features

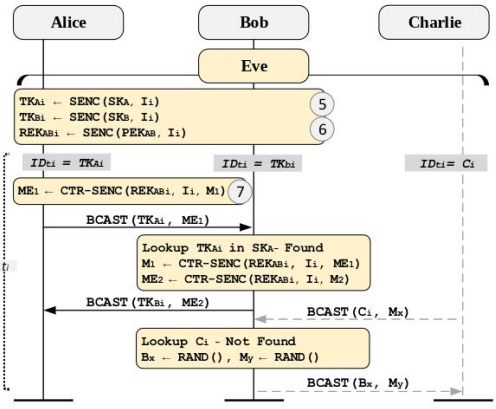
1. **Broadcast**: Random addresses removes linkability
2. **Encryption**: Removes meta information and context
3. **Pseudo Response**: Indistinguishable, tunable random responses
4. **Self-Contained**: Transparent to adjacent layers (eBPF, kernel modules)

Anonymization Layer



1. Generate random keys and exchange
2. XOR keys for Pairing Key
3. Use result to generate Source Keys
4. Use Pairing Key to generate Paired Encryption Key

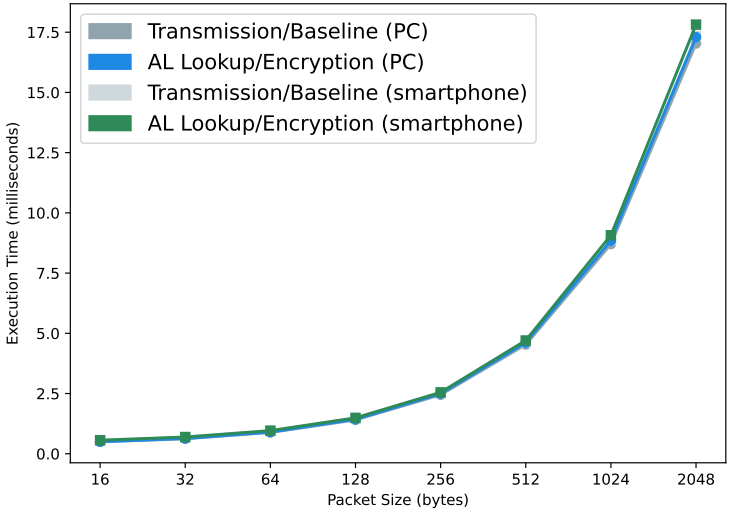
Anonymization Layer



5. Generate set of ephemeral Transmission Keys (TK)
6. Generate ephemeral set of Encryption Keys (REK)
7. Randomly select a TK/REK pair and encrypt Message

An AL packet is now formed using M_e and the corresponding Transmission Key and broadcasted over the communication medium.

Anonymization Layer: Overall Overhead

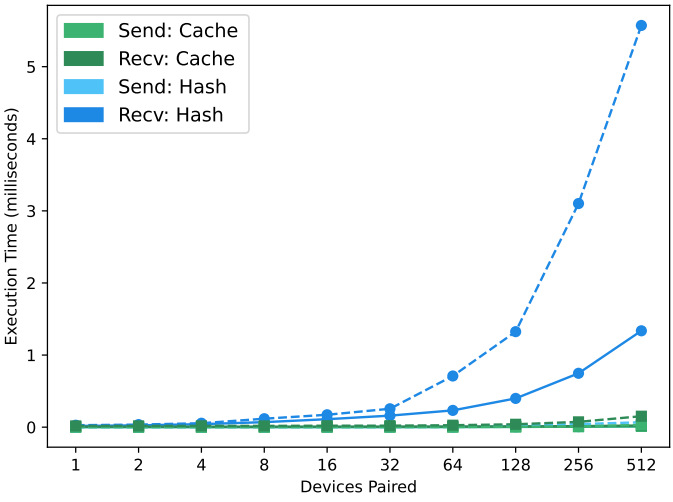


Anonymization Layer: Encryption Overhead

Size (B)	Enc. (ms)	Dec. (ms)	Total (ms)	Base (ms)	Δ
Pixel 7 Smartphone					
16	0.00487	0.00506	0.00993	0.54841	1.81%
32	0.00551	0.00551	0.01102	0.68064	1.62%
64	0.00717	0.00736	0.01453	0.94310	1.54%
128	0.01074	0.01085	0.02159	1.46606	1.47%
256	0.01805	0.01852	0.03657	2.50955	1.46%
512	0.03887	0.03993	0.07880	4.62103	1.71%
1024	0.09839	0.10140	0.19979	8.86632	2.25%
2048	0.22943	0.24132	0.47076	17.33921	2.71%
PC Laptop					
16	0.00330	0.00483	0.00814	0.49123	1.66%
32	0.00385	0.00622	0.01007	0.62184	1.62%
64	0.00543	0.00934	0.01477	0.88302	1.67%
128	0.00870	0.01576	0.02446	1.40463	1.74%
256	0.01495	0.02752	0.04247	2.44767	1.74%
512	0.02619	0.04943	0.07562	4.53251	1.67%
1024	0.04908	0.09395	0.14304	8.70166	1.64%
2048	0.08932	0.17213	0.26145	17.03093	1.54%

Average encryption overhead per packet, shown over various sizes

Anonymization Layer: Key Resolution Overhead

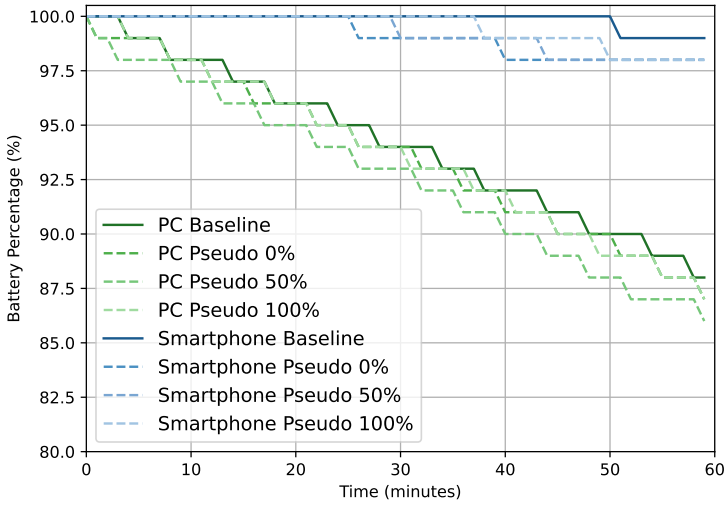


Anonymization Layer: Key Resolution Overhead

	Hash (ms)			Cache (ms)		
Pairs	**Send**	**Recv.**	**Δ**	**Send**	**Recv.**	**Δ**
Pixel 7 Smartphone						
1	0.00117	0.02700	1.12%	0.00109	0.01742	0.74%
4	0.00139	0.05475	2.24%	0.00126	0.01842	0.78%
16	0.00188	0.17209	6.93%	0.00144	0.02014	0.86%
128	0.02821	1.32464	53.91%	0.00425	0.04013	1.77%
512	0.06770	5.57161	224.71%	0.03129	0.15183	7.30%
PC Laptop						
1	0.00099	0.01677	0.73%	0.00095	0.00619	0.29%
4	0.00100	0.04178	1.75%	0.00100	0.00606	0.29%
16	0.00114	0.11065	4.57%	0.00121	0.00645	0.31%
128	0.00361	0.39888	16.44%	0.00358	0.01080	0.59%
512	0.00975	1.33669	55.01%	0.01050	0.02280	1.36%

Key resolution overhead for packet of varied sizes

Anonymization Layer: Power Overhead



Prior Research

Attack Vectors/Impact	IDBleed	BAT
Generalized	✓	✗
Encryption	✓	✗
Authentication	✓	✗
Auto-Connection	✓	✗
Data-Verification	✓	✗
BLE	✓	✓
Wi-Fi	✓	✗
Replay	✓	✓
Relay	✓	✗
Hard to Patch	✓	✗

Comparison between *IDBleed* and motivating *BAT* attacks.

Conclusion

1. *Exclusive-use*: Inherent flaw in communication patterns reveals device association
2. *IDBleed*: Deanonymize devices despite modern countermeasures
3. *Anonymization Layer*: Mitigation that removes observable boolean side-channel

Anonymization Layer source code publicly available at:
`https://github.com/OSUSecLab/AnonymizationLayer`

Thank You!