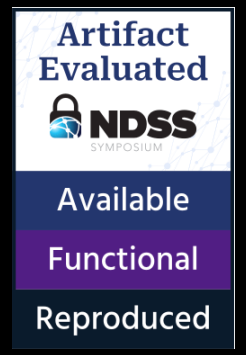


WCDCAnalyzer: Scalable Security Analysis of Wi-Fi Certified Device Connectivity Protocols

Zilin Shen, Imtiaz Karim, Elisa Bertino

Wi-Fi Device Connectivity is Everywhere

Wi-Fi Direct
3+ billion devices

EasyConnect (DPP)
Secure provisioning

EasyMesh
Multi-AP networks

PURDUE UNIVERSITY

The Problem

WCDC = Wi-Fi Certified Device Connectivity (DPP, P2P, WPS, etc.)

Prior research focused on WPA2/WPA3...
But WCDC protocols remain largely unstudied

Can we formally verify the security of WCDC protocols?

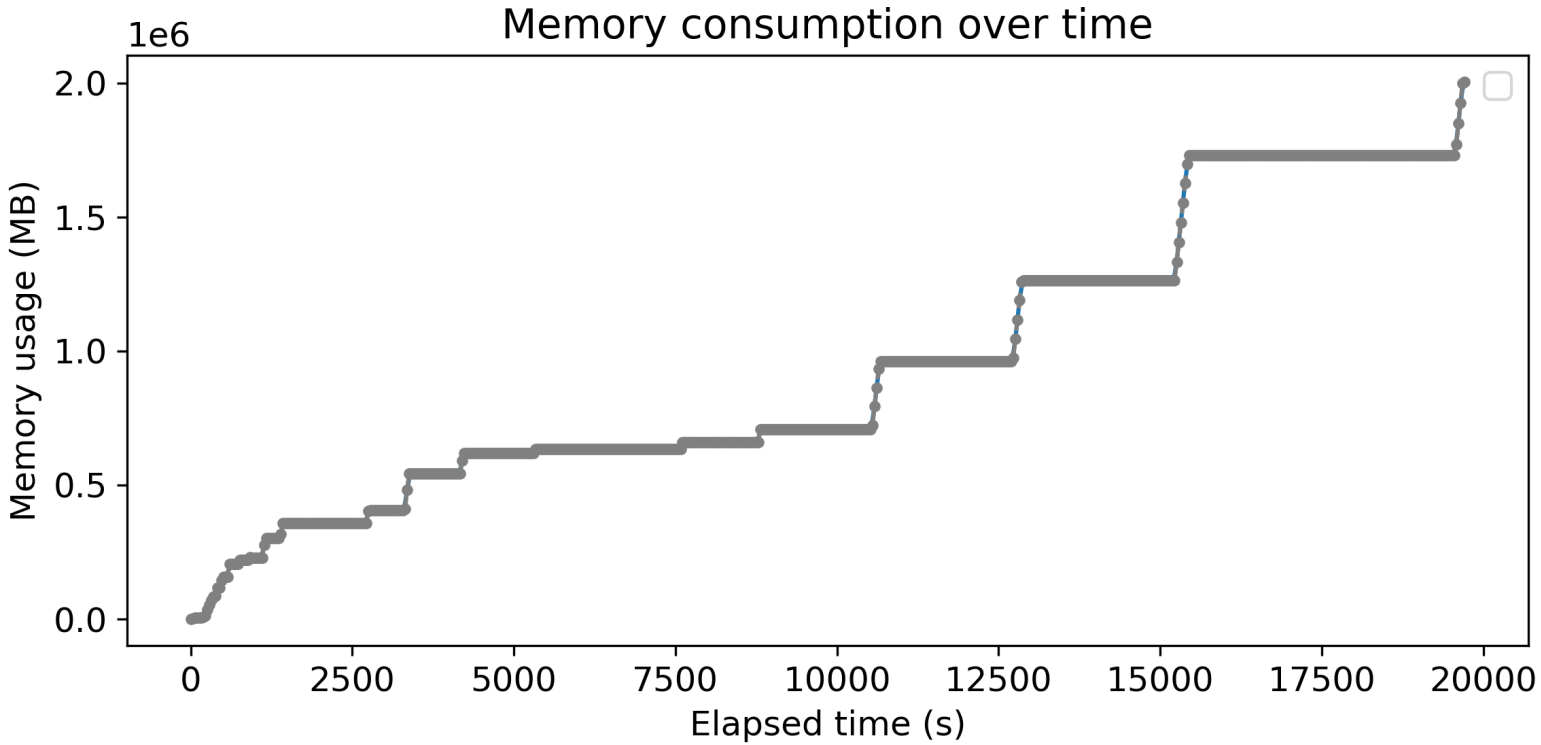
Challenge: Protocol complexity causes state explosion in formal verification

PURDUE UNIVERSITY

Challenge: State Explosion

192 cores, 2TB RAM

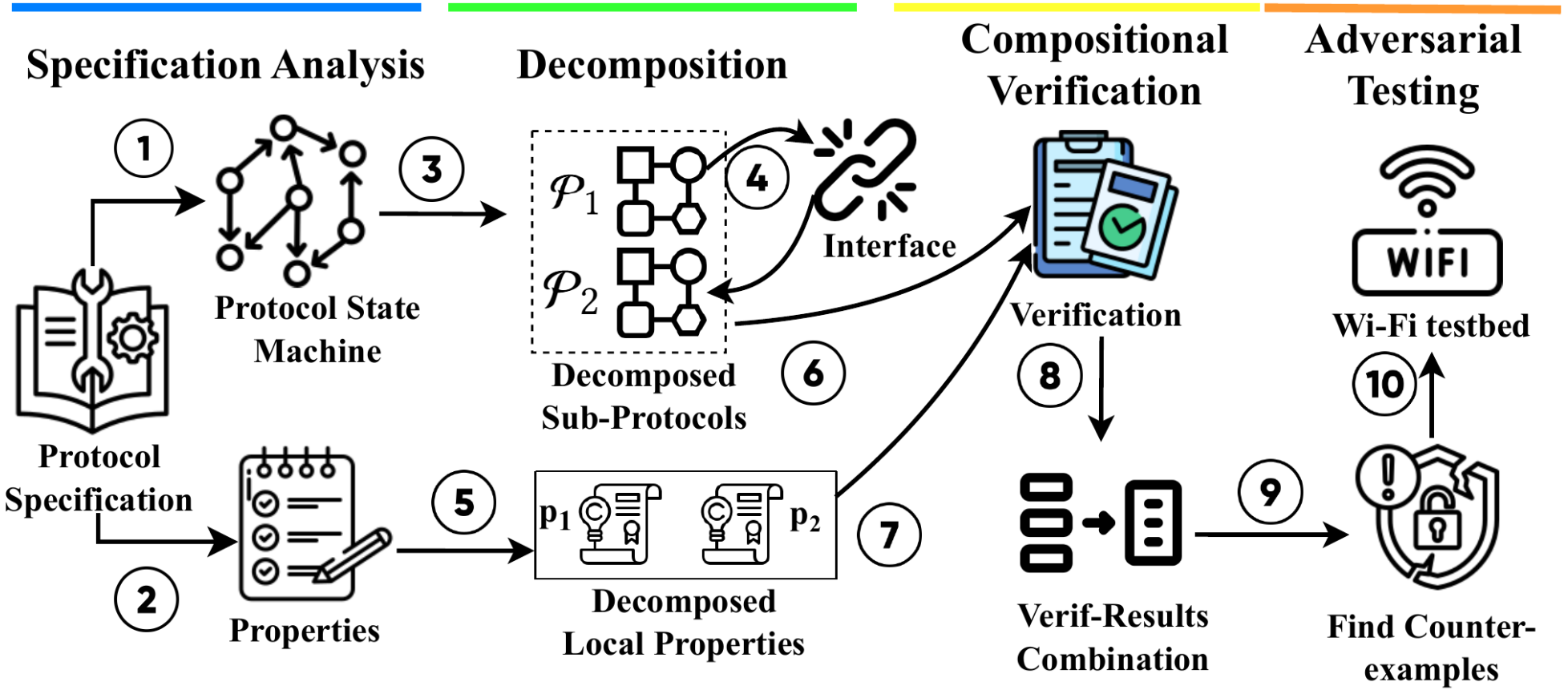
- Wi-Fi Direct too large for Tamarin
- 50+ terms sent to public channel
- States grow exponentially
- Verification killed after hours



PURDUE UNIVERSITY

Our Solution: WCDCAnalyzer

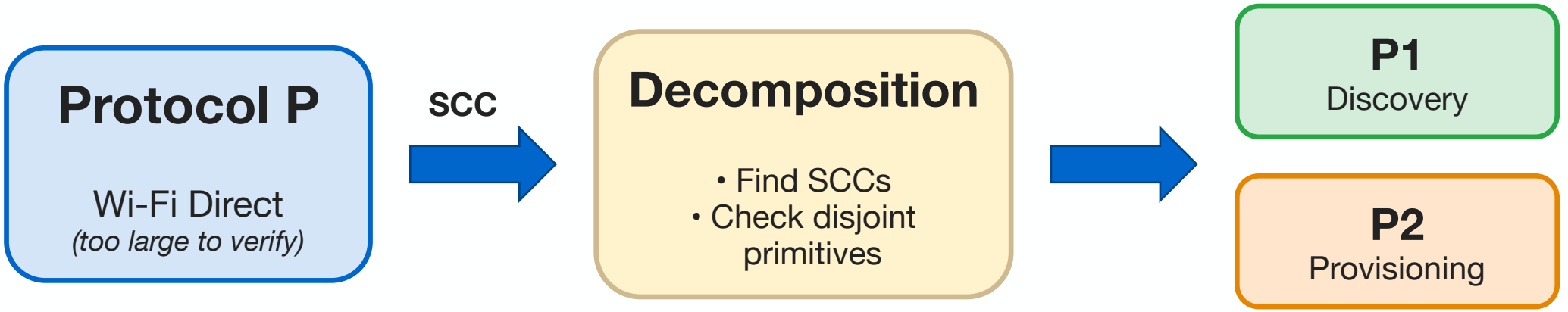
First comprehensive formal analysis framework with automatic decomposition



PURDUE UNIVERSITY

Key Technique: Protocol Decomposition

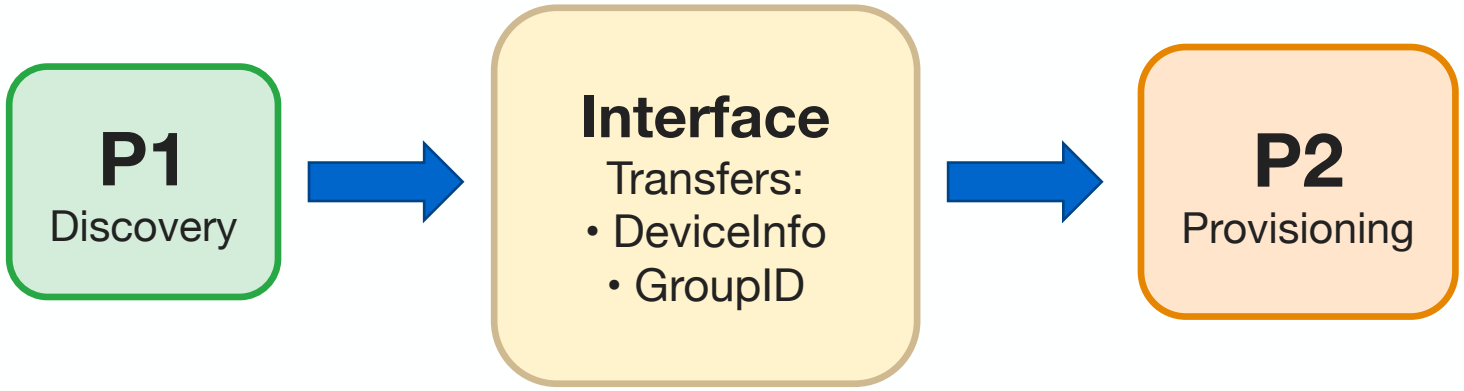
Break complex protocol into manageable sub-protocols using SCC algorithm



Theoretical basis: Compositional reasoning with disjoint cryptographic primitives

If sub-protocols are secure → whole protocol is secure

Interface: Bridging Sub-Protocols



Challenge:
Sub-protocols share terms (e.g., DeviceInfo from P1)

Solution:
Interface state transfers dependent terms

Soundness: Verify secrecy to determine attacker knowledge
• Secret term → fresh(t) • Public term → fresh(t) + send(t)

Soundness:
• Secret term → fresh(t)
• Public term → send(t)

PURDUE UNIVERSITY

Compositional Verification

Global Property p

Defined over entire protocol:

- Executability
- Secrecy
- Authentication
- Privacy

Local Properties

p1 for P1 (Discovery)
p2 for P2 (Provisioning)

Verify independently,
combine results

p holds $\iff$ p1 $\wedge$ p2 hold

Scalability Results

Property	$\mathcal{P}$		$\mathcal{P}_1$		$\mathcal{P}_2$		$\mathcal{P}_1 + \mathcal{P}_2$	
	Mem	Time	Mem	Time	Mem	Time	Mem	Time
Executability	191 G✗	80 m	195.3 M	3.7 s	156 G	494 m	156.2 G	494 m
PrivKey Secrecy	211.2G✗	110 m	*None*	*None*	336.7 M	19.9 s	336.7 M	19.9 s
Addr Privacy	189.5G✗	90 m	178 M	3.5 s	269.5 M	19.6 s	447.5 M	23.1 s
Provision Authentication	189.8 G✗	350 m	*None*	*None*	4.59 G	774 s	4.59 G	774 s
DevPwdID Integrity	190 G✗	105 m	198.7 M	3.4 s	336.8 M	17.6 s	535.5 M	20.9 s

Without Decomposition

191 GB+ ✗

With Decomposition

156 GB ✓

PURDUE UNIVERSITY

Security Findings: 10 New Vulnerabilities

Wi-Fi Direct

D1: Downgrade Attack
→ Auth Bypass

D2-D3: UUID/MAC Leak
→ Privacy

D4-D5: DoS Attacks

EasyConnect

EC1: Bootstrap Key Exposure

EC2: MAC Address Leakage

→ Device Tracking

EasyMesh

EM1-EM3:
Key & Address Exposure

→ Device Tracking

✓ All validated on 19 commercial devices **✓ Acknowledged by Wi-Fi Alliance**

PURDUE UNIVERSITY

Attack: Authentication Bypass

Direct Downgrade Attack on DPP

Attack Steps:

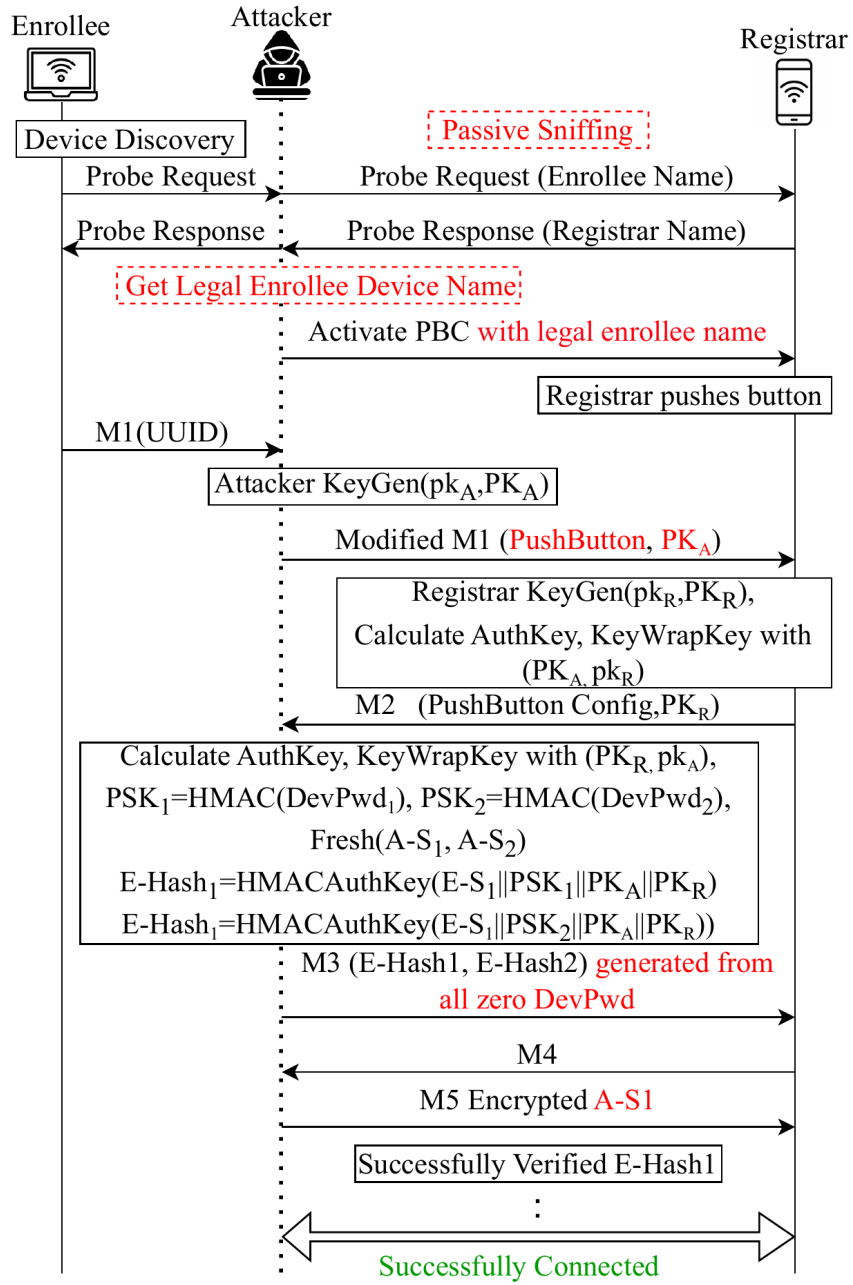
1. Attacker passively sniffs Enrollee's probe request
2. Impersonates Enrollee using captured device name
3. Activates PBC with legal enrollee name
4. Generates malicious M1 with attacker's public key
5. Registrar accepts and establishes session

Root Cause:

- DPP lacks proper device authentication
- Public key exchange has no binding to identity

Impact:

- Attacker gains full network access
- Legitimate device is excluded



PURDUE UNIVERSITY

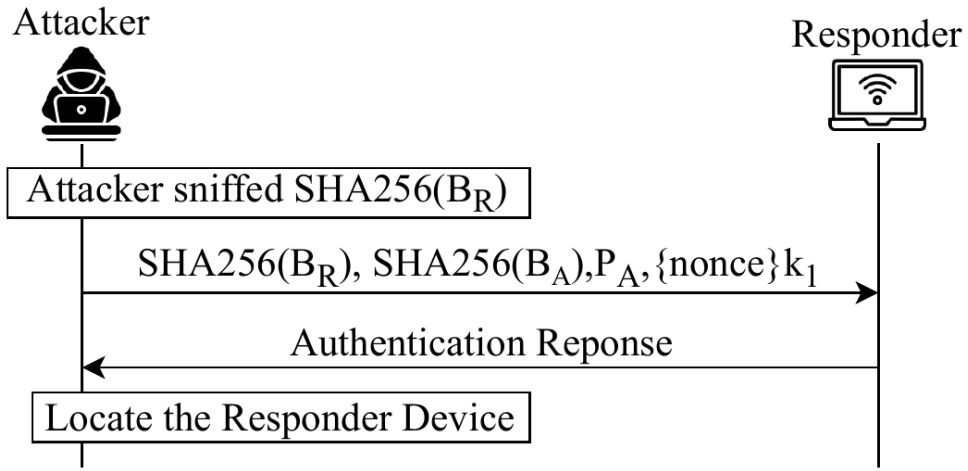
Attack: Privacy Leakage

UUID Leakage (D2)

- UUID in M1 message
- Transmitted in plaintext
- No rotation required

Bootstrapping Key Information Exposure (EC1)

- Bootstrapping key static
- Attacker sniffed in discovery
- Enables active tracking



PURDUE UNIVERSITY

Real-World Validation

19 Devices Tested

Coverage:

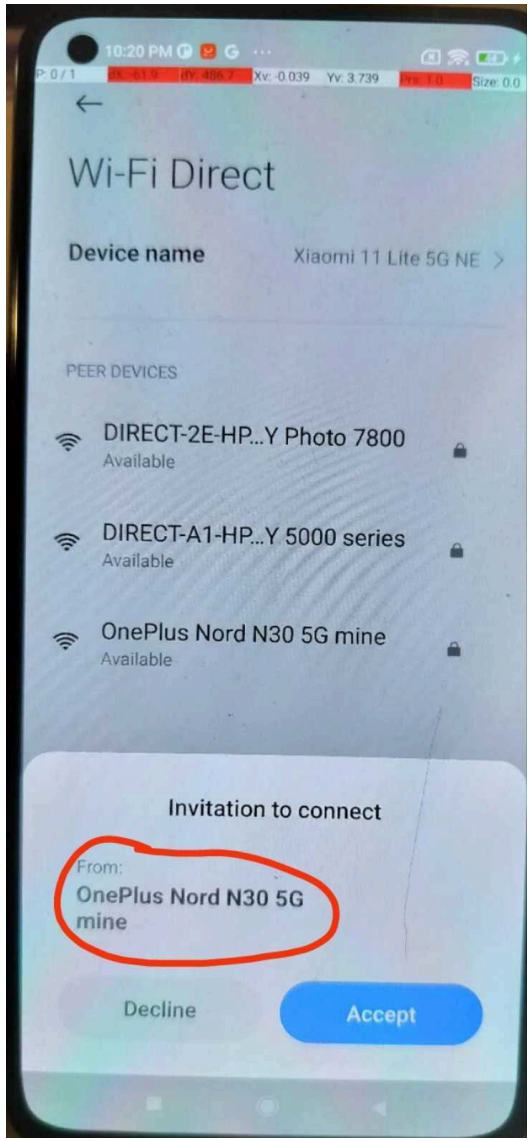
- Wi-Fi 4 to Wi-Fi 6E
- 10 phones, 8 network cards
- 1 development board

Results:

- 100% affected by vulnerabilities
- 9/11 Direct devices: all 5 issues

Disclosure:

- Wi-Fi Alliance acknowledged
- Fix in next spec version



ID	Device Name
P1	OnePlus Nord N30
P2	Xiaomi 11 Lite
P3	OnePlus 8T+
P4	OnePlus 9 Pro
P5	OnePlus 7T
P6	REVVL 4+
P7	Oneplus Nord
P8	Motorola Edge30 Pro
P9	Xiaomi 12T
P10	Honor 8X
N1	Alfa AWUS036ACM
N2	TL-WN722N
N3	BrosTrend AC3L
N4	Netgear A8000
N5	EDUP EP-AX1672
N6	Alfa AWUS036ACU
N7	Realtek rtl8812bu
N8	Intel AC 8265
B1	ESP32

PURDUE UNIVERSITY

Contributions

1

First Formal Analysis

Comprehensive framework
for WCDC protocols

2

Decomposition Method

SCC-based automatic
decomposition + interface

3

Vulnerabilities

Real-world impact
19 devices validated

Open-source: github.com/Zilinlin/WCDCAnalyzer

PURDUE UNIVERSITY

Thank You!

Questions?

Zilin Shen | shen624@purdue.edu

github.com/Zilinlin/WCDCAnalyzer

PURDUE UNIVERSITY

github.com/Zilinlin/WCDCAnalyzer