Security and Privacy Analysis of Tile's Location Tracking Protocol

Akshaya Kumar, Anna Raymaker, and Michael A. Specter

Usenix Security 2026

Georgia Tech

Crowdsourced location tracking protocols

Crowdsourced location tracking protocols



Finders



Tag

Crowdsourced location tracking protocols



Finders



Tag







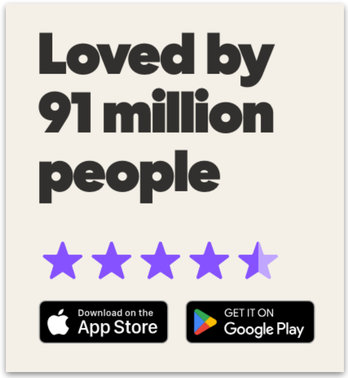




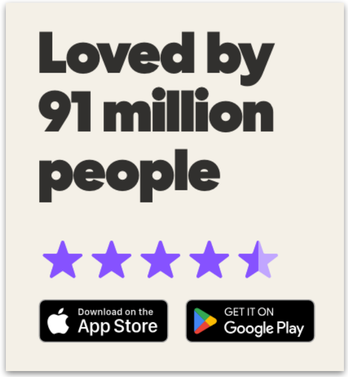




Security and privacy analysis of Tile's protocol



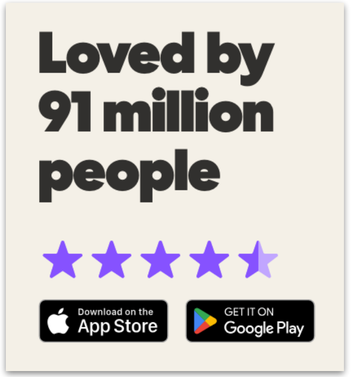
Security and privacy analysis of Tile’s protocol





Tag

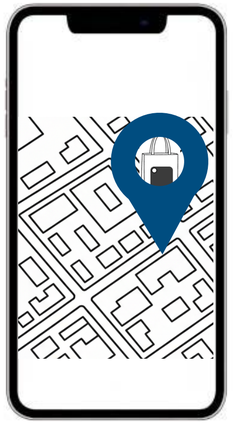
Security and privacy analysis of Tile’s protocol





Tag

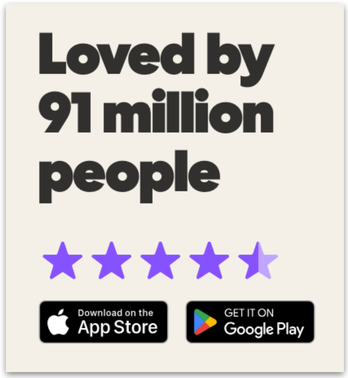
Track lost item using the network



Owner

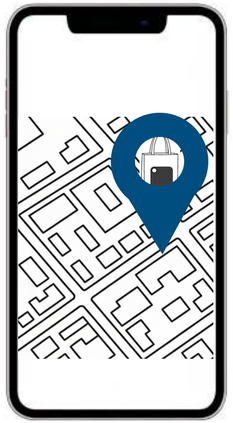
Helps users track their belongings

Security and privacy analysis of Tile's protocol

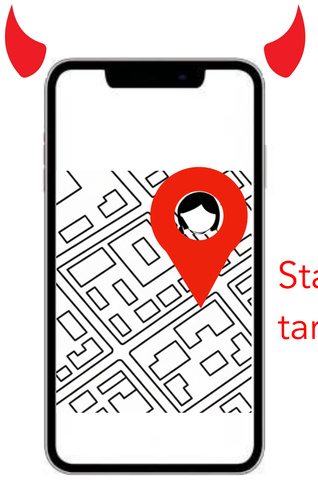


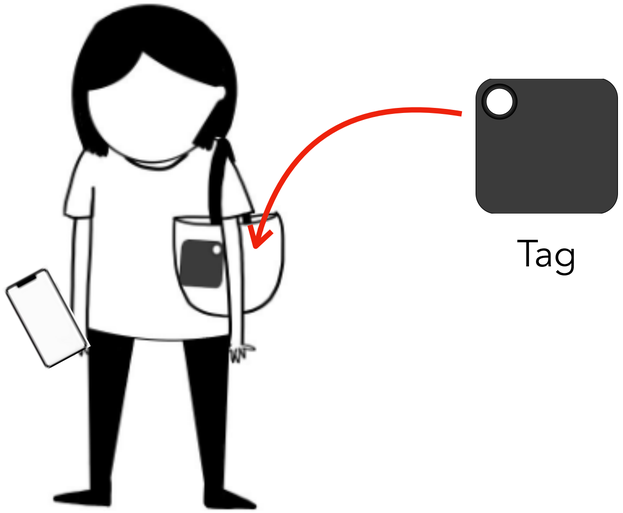


Track lost item using the network



Helps users track their belongings

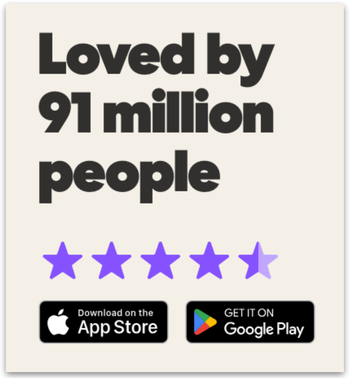




Stalk target by placing tag on target's person/belongings

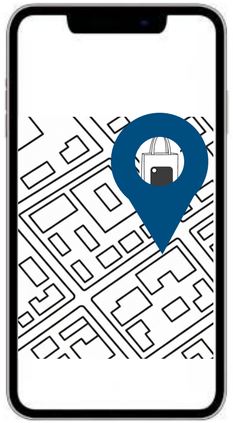
Helps users stalk other people

Security and privacy analysis of Tile's protocol

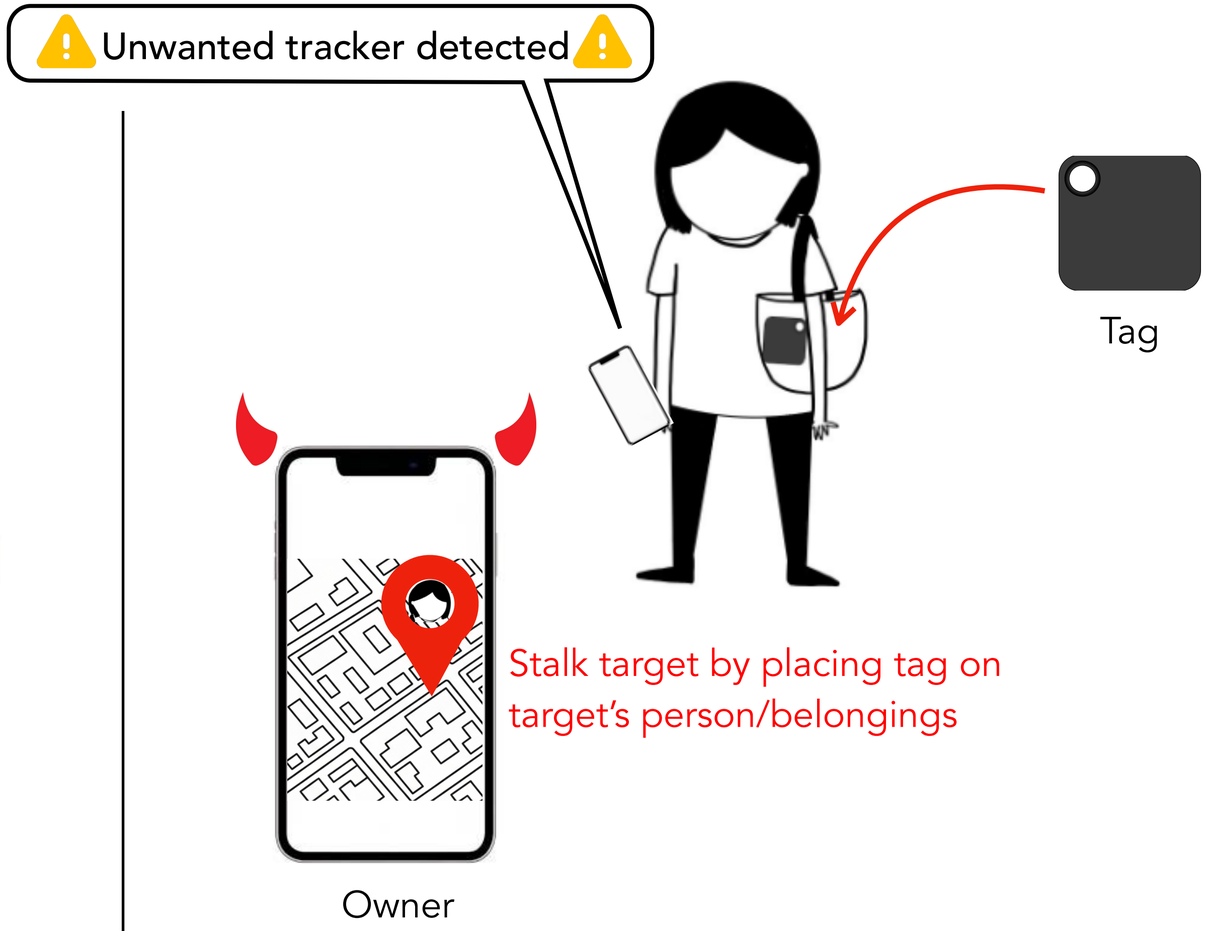




Track lost item using the network



Helps users track their belongings



Stalk target by placing tag on target's person/belongings

Helps users stalk other people

Tile’s AntiTheft mode and accountability claims

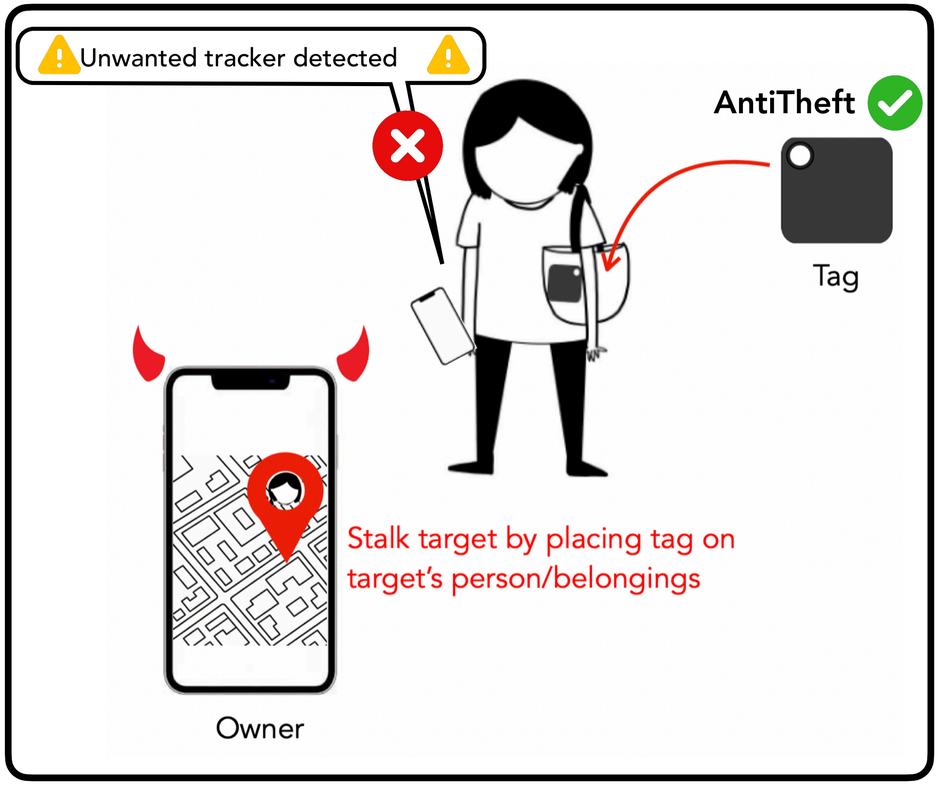
Tile Anti-Theft Mode



Tile’s AntiTheft mode and accountability claims

Tile Anti-Theft Mode

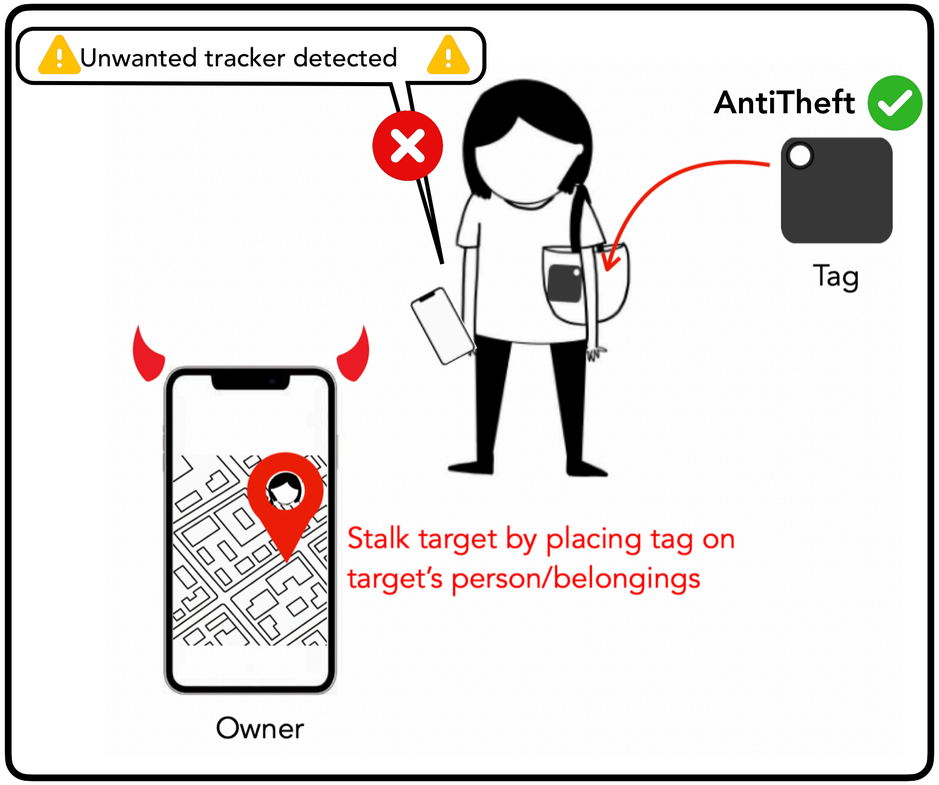




Tile’s AntiTheft mode and accountability claims

Tile Anti-Theft Mode



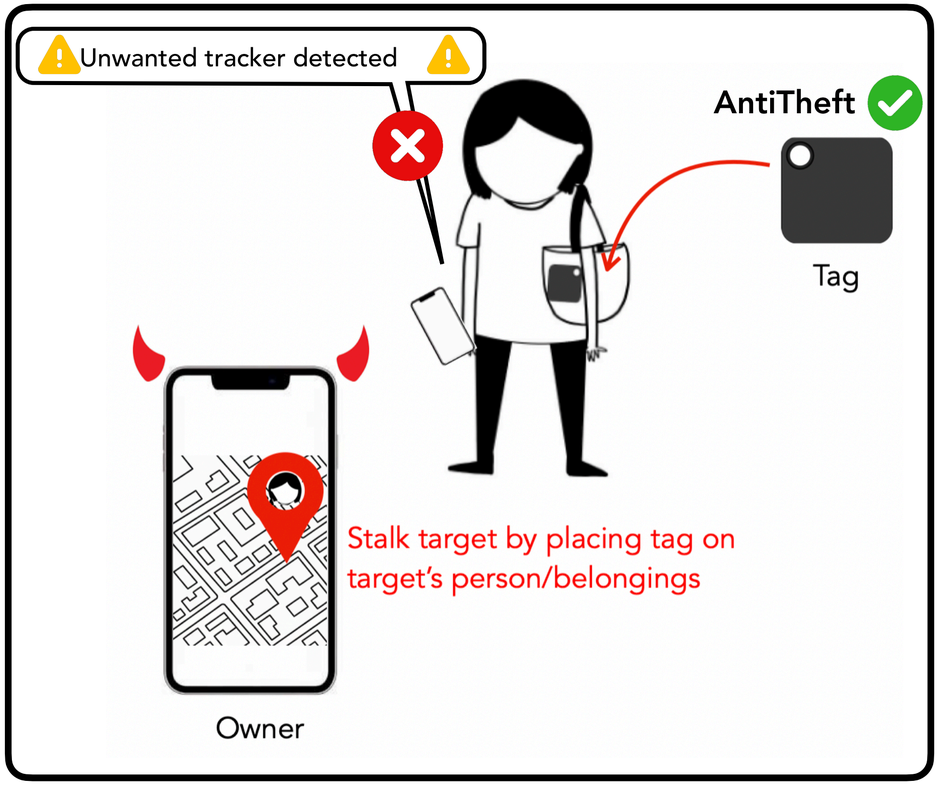


Antistalking		AntiTheft
Victims can detect tags	×	Tags invisible to scans

Tile’s AntiTheft mode and accountability claims

Tile Anti-Theft Mode





Tile’s accountability guarantees

“… personal information can and will be shared with law enforcement at our discretion, even without a subpoena, to aid in the investigation and prosecution of suspected stalking.”

Antistalking
Victims can detect tags

×

AntiTheft
Tags invisible to scans

Our contributions

Methodology: Reverse engineered Tile's Android application and reconstructed its protocol

Our contributions

Methodology: Reverse engineered Tile's Android application and reconstructed its protocol

Does Tile's AntiTheft mode provide the claimed functionality?
No, modified app sees all "hidden" tags

Our contributions

Methodology: Reverse engineered Tile's Android application and reconstructed its protocol

Does Tile's AntiTheft mode provide the claimed functionality?
No, modified app sees all "hidden" tags

Does Tile's accountability mechanism work?
No, trivially subvertible and enables a new class of "framing" attacks against honest users

Our contributions

Methodology: Reverse engineered Tile's Android application and reconstructed its protocol

Does Tile's AntiTheft mode provide the claimed functionality?
No, modified app sees all "hidden" tags

Does Tile's accountability mechanism work?
No, trivially subvertible and enables a new class of "framing" attacks against honest users

Does Tile's protocol guarantee location privacy?
No, Tile's servers collect unencrypted locations, essentially running a mass-surveillance network

Our contributions

Methodology: Reverse engineered Tile's Android application and reconstructed its protocol

Does Tile's AntiTheft mode provide the claimed functionality?
No, modified app sees all "hidden" tags

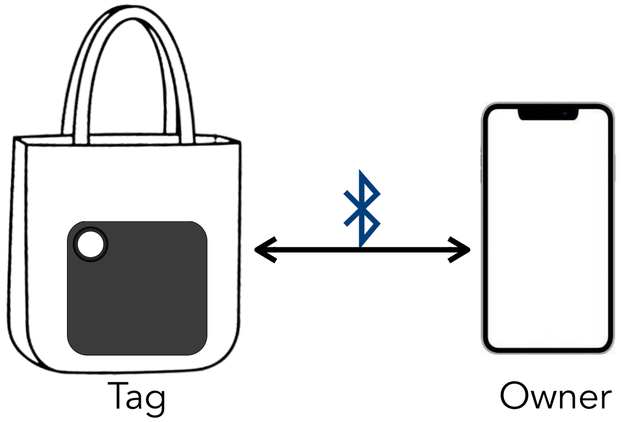
Does Tile's accountability mechanism work?
No, trivially subvertible and enables a new class of "framing" attacks against honest users

Does Tile's protocol guarantee location privacy?
No, Tile's servers collect unencrypted locations, essentially running a mass-surveillance network

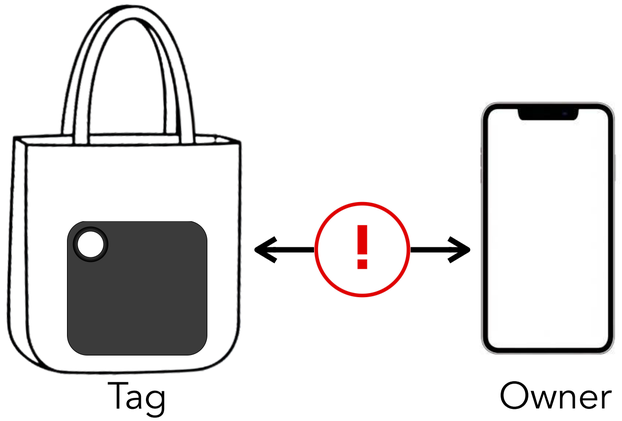
Does Tile's protocol guarantee other standard properties?
No, identified other attacks that break antistalking and unlinkability properties

Crowdsourced location tracking: An overview

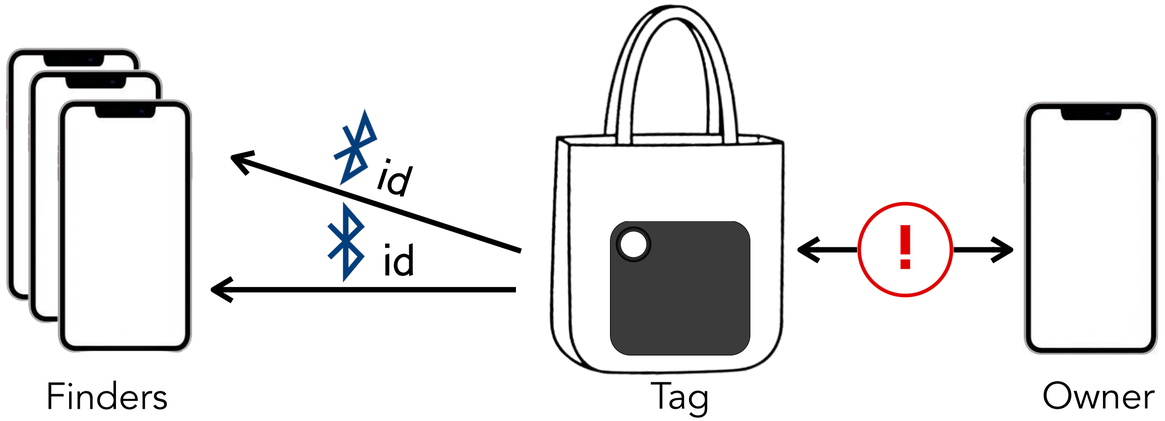
Crowdsourced location tracking: An overview



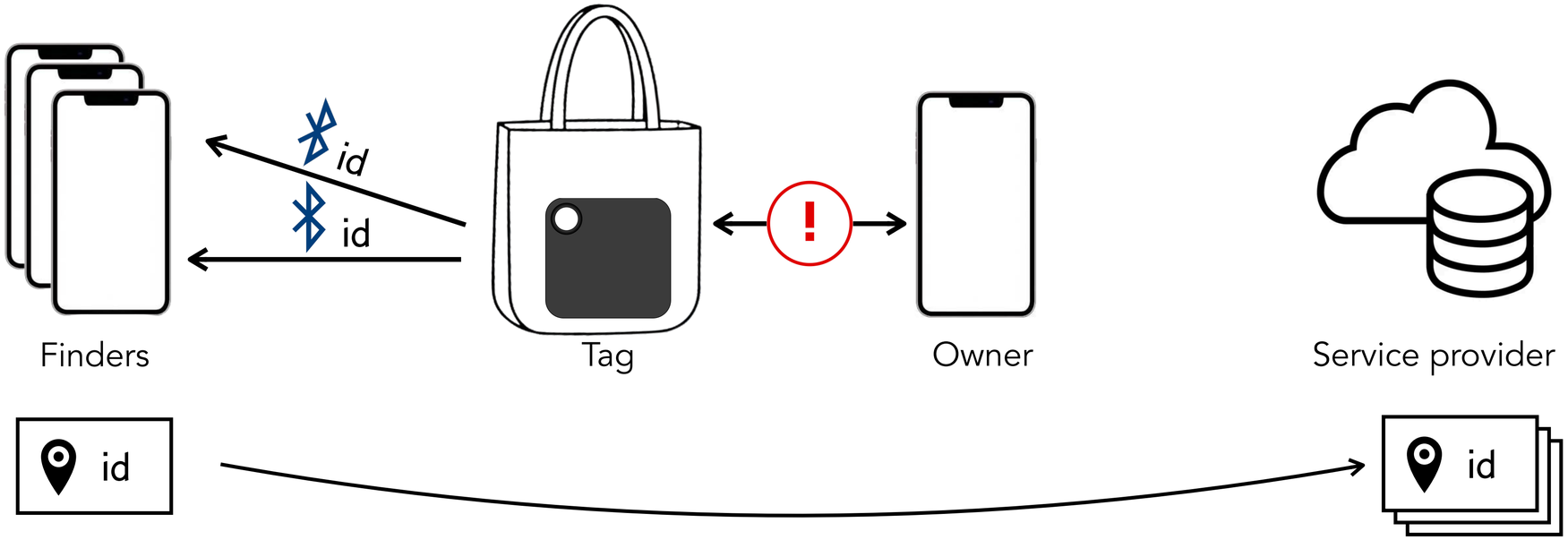
Crowdsourced location tracking: An overview



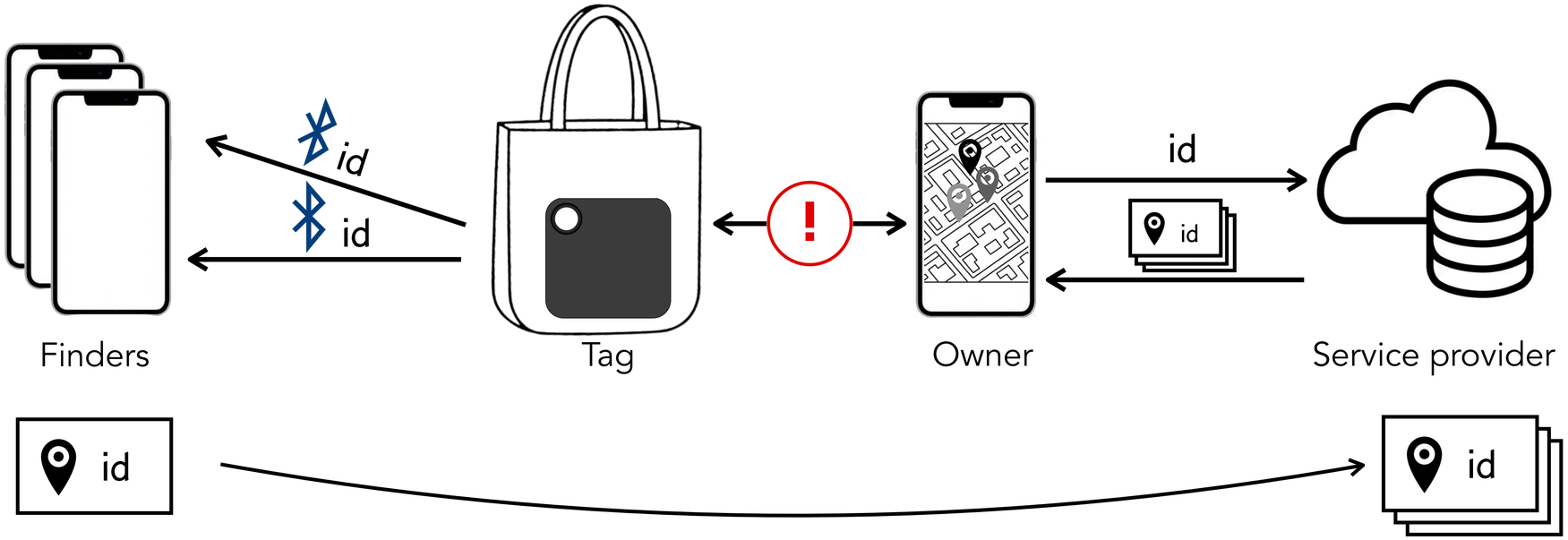
Crowdsourced location tracking: An overview



Crowdsourced location tracking: An overview

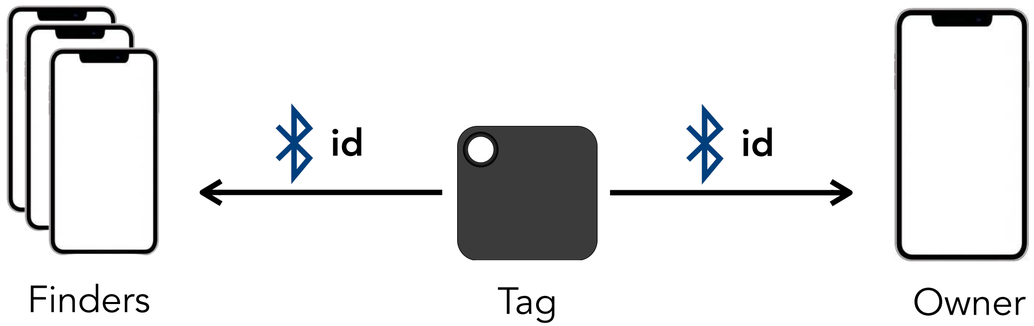


Crowdsourced location tracking: An overview

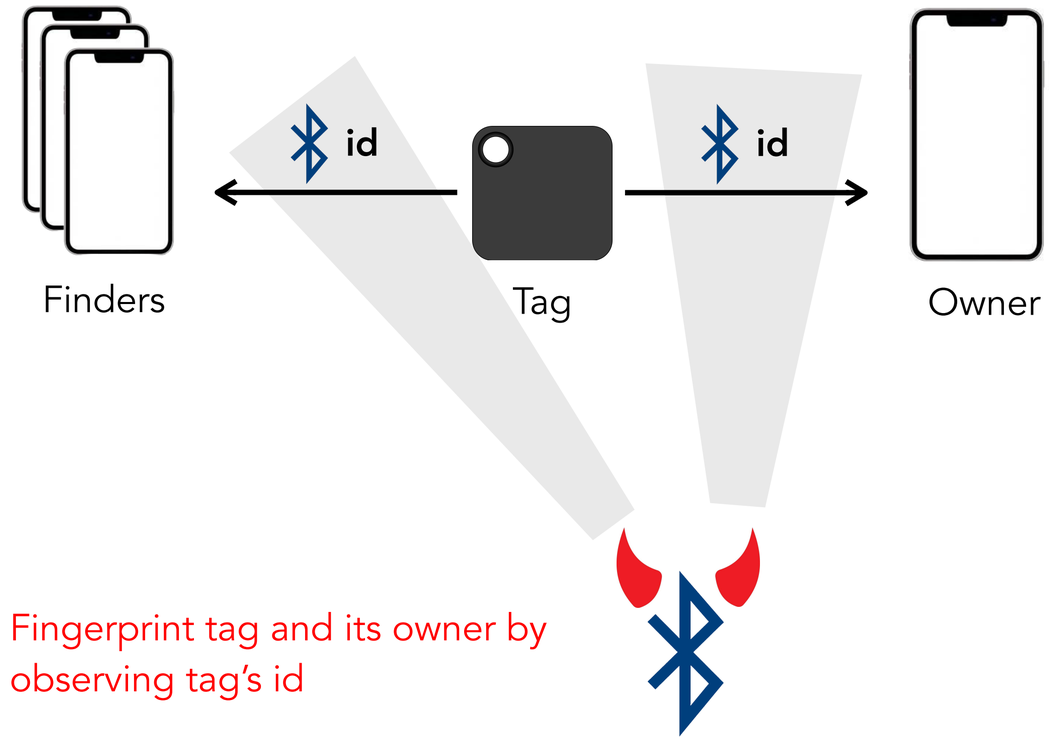


A complex cryptographic landscape: Privacy-antitheft-safety tensions

A complex cryptographic landscape: Privacy-antitheft-safety tensions

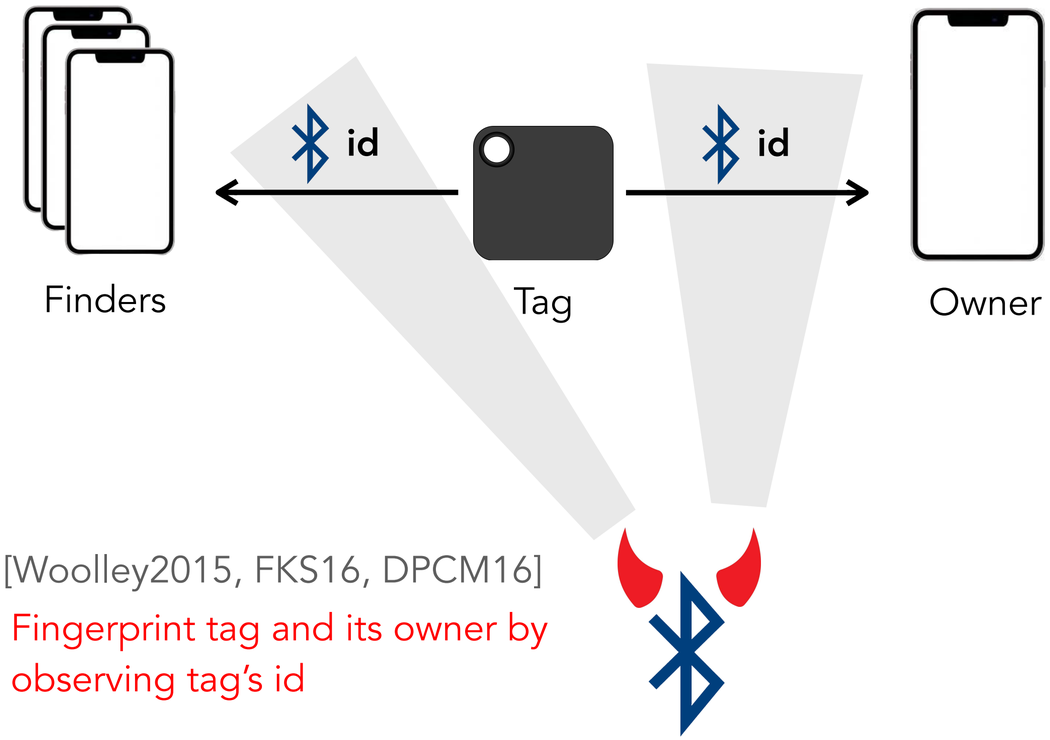


A complex cryptographic landscape: Privacy-antitheft-safety tensions



Fingerprint tag and its owner by observing tag's id

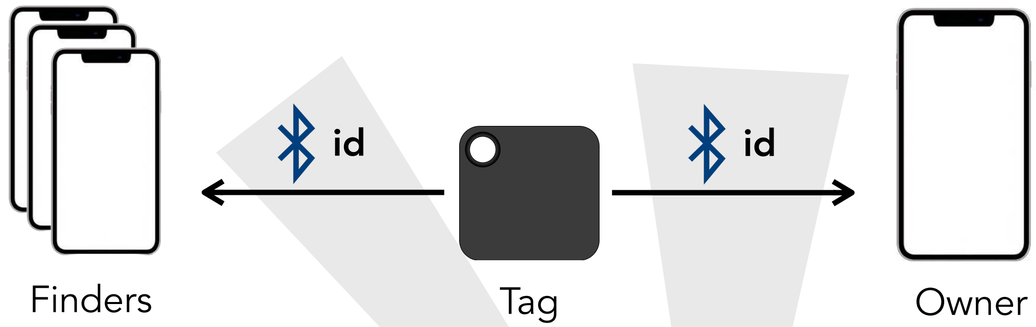
A complex cryptographic landscape: Privacy-antitheft-safety tensions



[Woolley2015, FKS16, DPCM16]

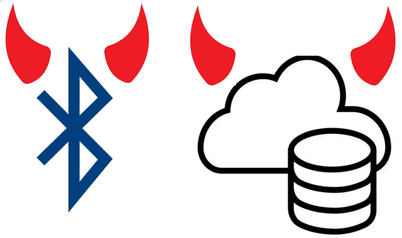
Fingerprint tag and its owner by observing tag's id

A complex cryptographic landscape: Privacy-antitheft-safety tensions

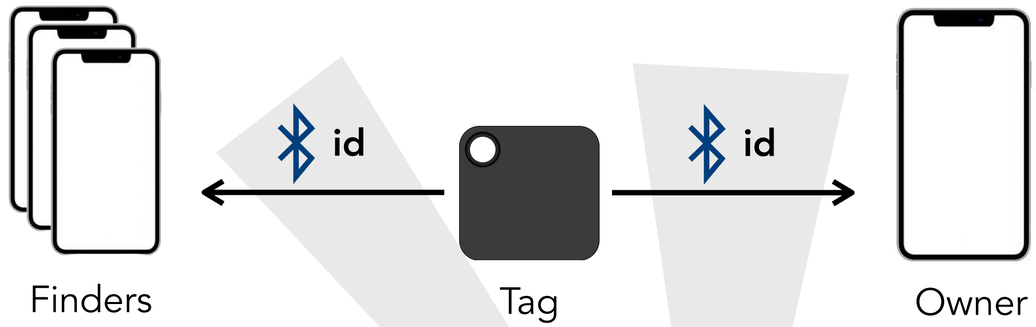


[Woolley2015, FKS16, DPCM16]

Fingerprint tag and its owner by observing tag's id

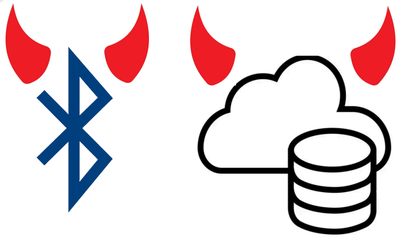


A complex cryptographic landscape: Privacy-antitheft-safety tensions



[Woolley2015, FKS16, DPCM16]

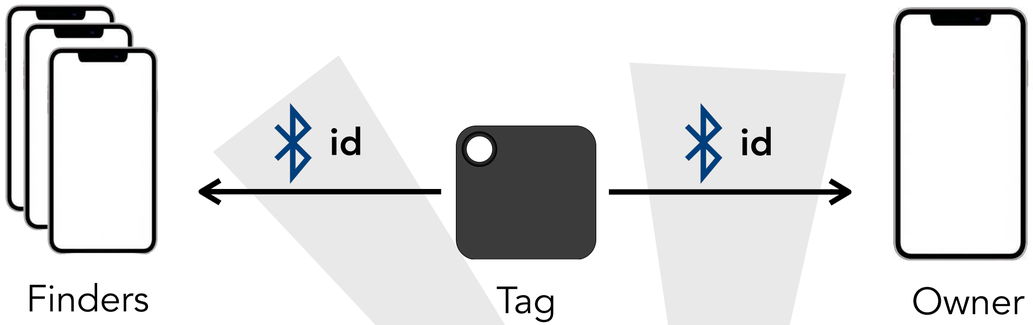
Fingerprint tag and its owner by observing tag's id



Goal: Unlinkability

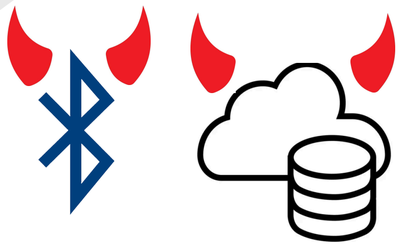
Hard for Bluetooth attacker and server to link identifiers broadcast by a tag

A complex cryptographic landscape: Privacy-antitheft-safety tensions



Woolley2015, FKS16, DPCM16

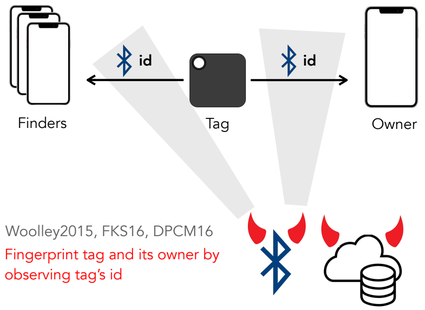
Fingerprint tag and its owner by observing tag's id



Goal: Unlinkability

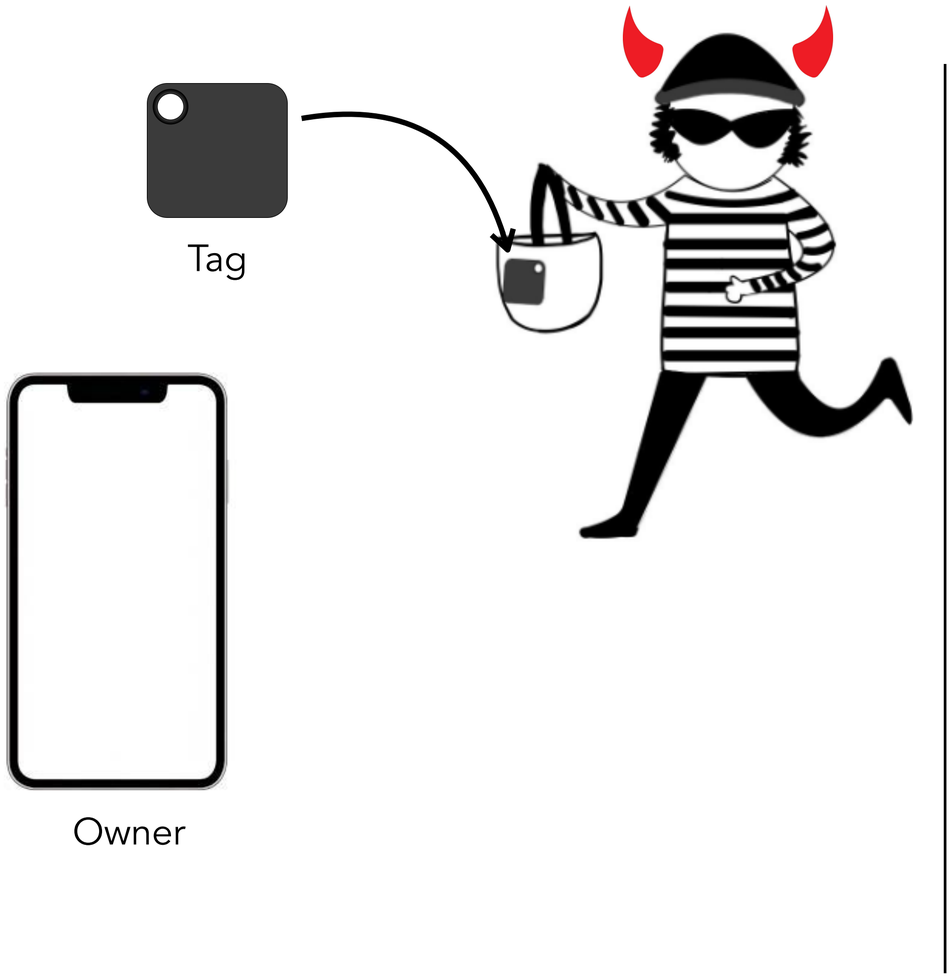
Hard for Bluetooth attacker and server to link identifiers broadcast by a tag

A complex cryptographic landscape: Privacy-antitheft-safety tensions



Woolley2015, FKS16, DPCM16

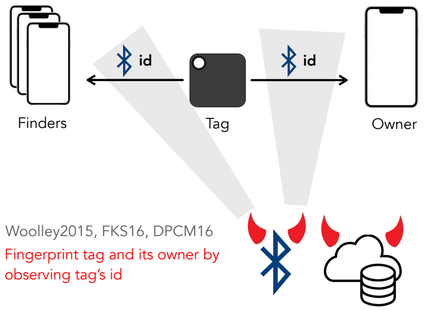
Fingerprint tag and its owner by observing tag's id



Goal: Unlinkability

Hard for Bluetooth attacker and server to link identifiers broadcast by a tag

A complex cryptographic landscape: Privacy-antitheft-safety tensions



Woolley2015, FKS16, DPCM16

Fingerprint tag and its owner by observing tag's id

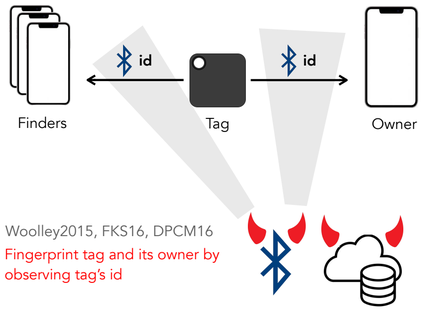


Track stolen item using the OF network

<u>Goal: Unlinkability</u>

Hard for Bluetooth attacker and server to link identifiers broadcast by a tag

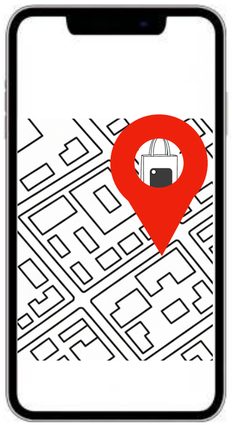
A complex cryptographic landscape: Privacy-antitheft-safety tensions



Woolley2015, FKS16, DPCM16

Fingerprint tag and its owner by observing tag's id





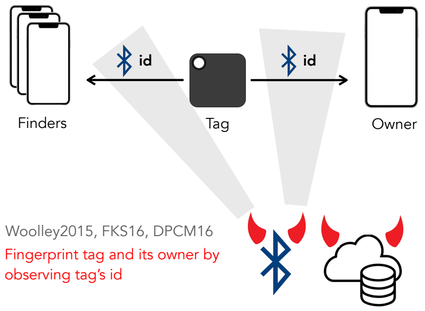
Owner

Track stolen item using the OF network

<u>Goal: Unlinkability</u>
Hard for Bluetooth attacker and server to link identifiers broadcast by a tag

<u>Goal: Undetectability</u>
Thief cannot link identifiers broadcast by a tag to detect it

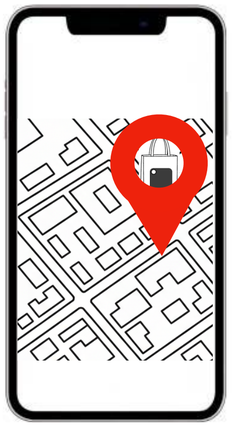
A complex cryptographic landscape: Privacy-antitheft-safety tensions



Woolley2015, FKS16, DPCM16

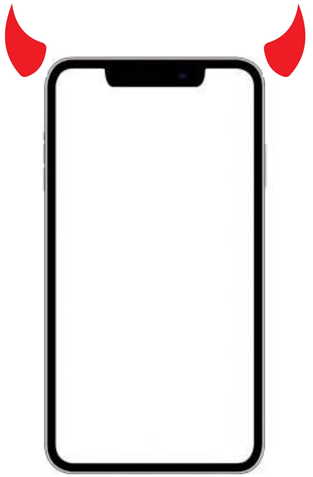
Fingerprint tag and its owner by observing tag's id



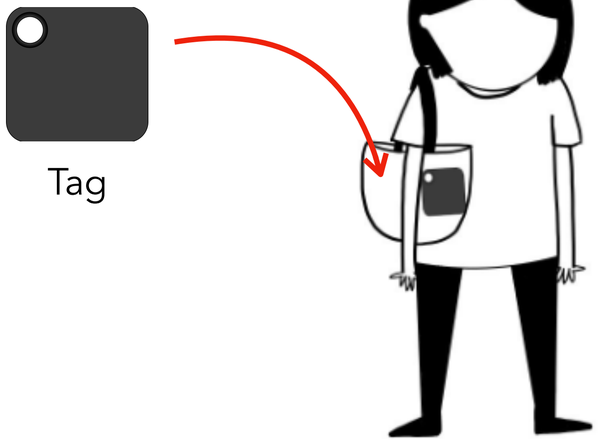


Owner

Track stolen item using the OF network



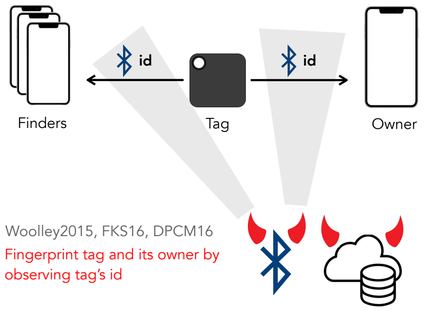
Owner



<u>Goal: Unlinkability</u>
Hard for Bluetooth attacker and server to link identifiers broadcast by a tag

<u>Goal: Undetectability</u>
Thief cannot link identifiers broadcast by a tag to detect it

A complex cryptographic landscape: Privacy-antitheft-safety tensions



Woolley2015, FKS16, DPCM16

Fingerprint tag and its owner by observing tag's id

Goal: Unlinkability

Hard for Bluetooth attacker and server to link identifiers broadcast by a tag



Track stolen item using the OF network

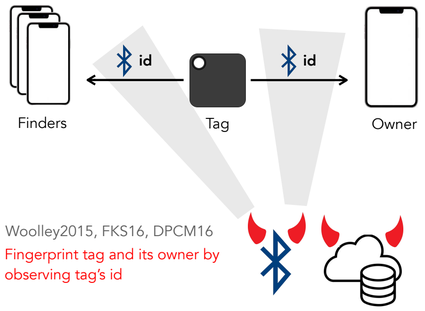
Goal: Undetectability

Thief cannot link identifiers broadcast by a tag to detect it



Stalk target by placing tag on target's person/belongings

A complex cryptographic landscape: Privacy-antitheft-safety tensions

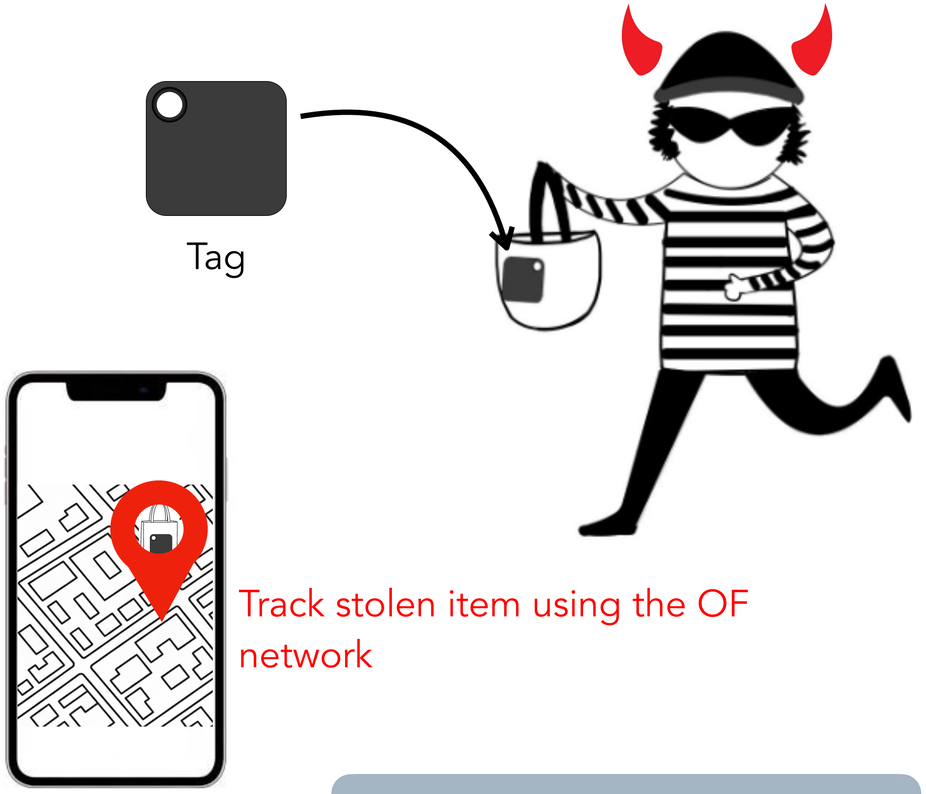


Woolley2015, FKS16, DPCM16

Fingerprint tag and its owner by observing tag's id

Goal: Unlinkability

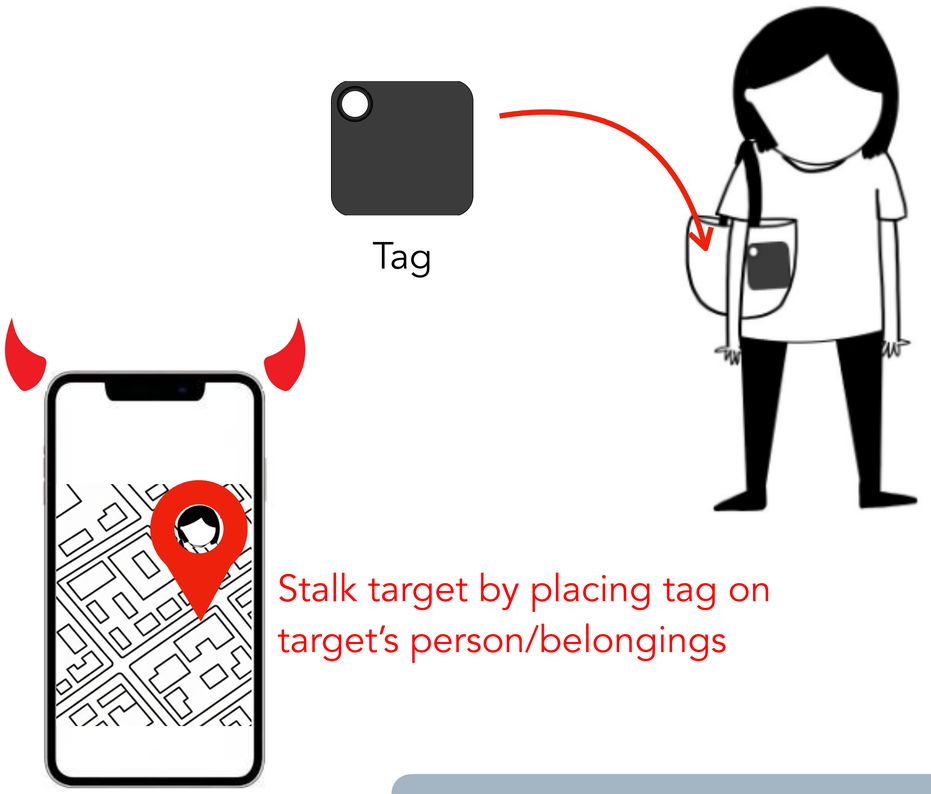
Hard for Bluetooth attacker and server to link identifiers broadcast by a tag



Track stolen item using the OF network

Goal: Undetectability

Thief cannot link identifiers broadcast by a tag to detect it



Stalk target by placing tag on target's person/belongings

Goal: Detectability

Stalking survivor can link tag identifiers across locations

A complex cryptographic landscape: Privacy-antitheft-safety tensions

A complex cryptographic landscape: Privacy-antitheft-safety tensions

Goal: Unlinkability
Hard for Bluetooth attacker and server to link identifiers broadcast by a tag

A complex cryptographic landscape: Privacy-antitheft-safety tensions

Goal: Unlinkability
Hard for Bluetooth attacker and server to link identifiers broadcast by a tag

Goal: Undetectability
Thief cannot link identifiers broadcast by a tag to detect it

A complex cryptographic landscape: Privacy-antitheft-safety tensions

Goal: Unlinkability
Hard for Bluetooth attacker and server to link identifiers broadcast by a tag

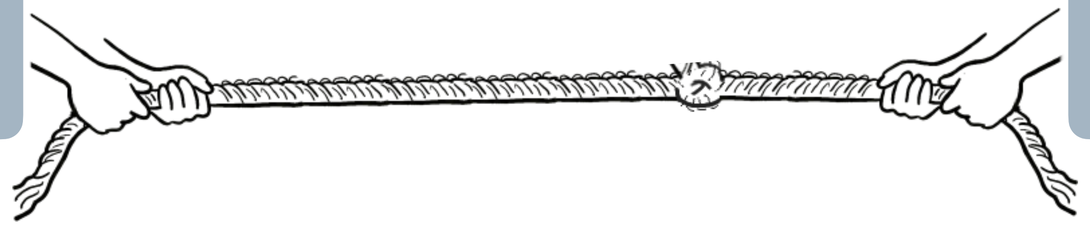
Goal: Undetectability
Thief cannot link identifiers broadcast by a tag to detect it

Goal: Detectability
Stalking survivor can link tag identifiers across locations

A complex cryptographic landscape: Privacy-antitheft-safety tensions

Goal: Unlinkability
Hard for Bluetooth attacker and server to link identifiers broadcast by a tag

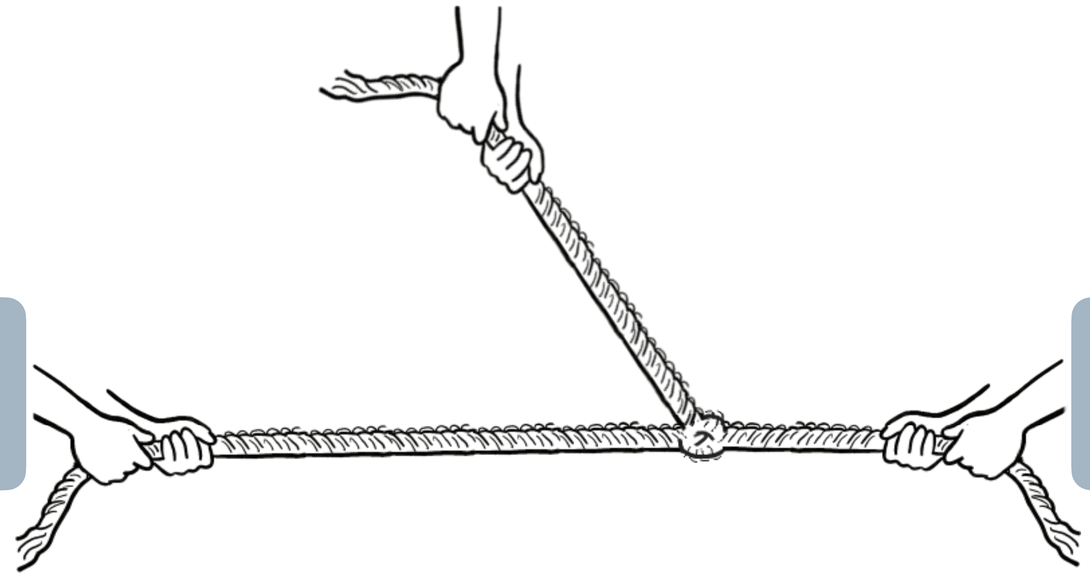
Goal: Undetectability
Thief cannot link identifiers broadcast by a tag to detect it



Goal: Detectability
Stalking survivor can link tag identifiers across locations

A complex cryptographic landscape: Privacy-antitheft-safety tensions

Goal: Unlinkability
Hard for Bluetooth attacker and server to link identifiers broadcast by a tag

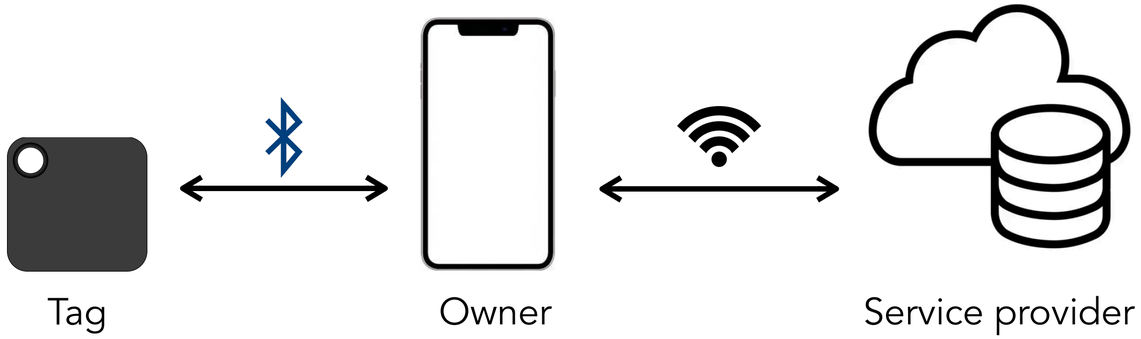


Goal: Undetectability
Thief cannot link identifiers broadcast by a tag to detect it

Goal: Detectability
Stalking survivor can link tag identifiers across locations

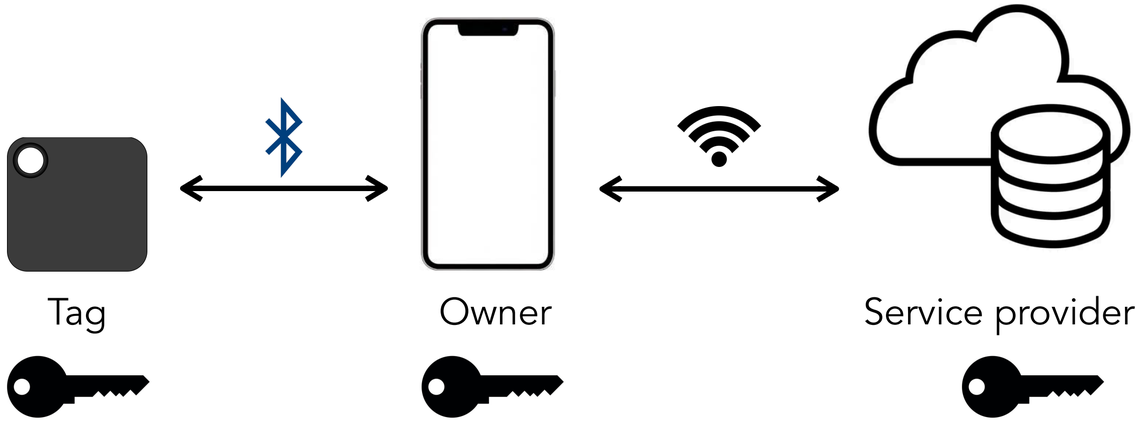
Tile’s protocol

1. **Registration and pairing**



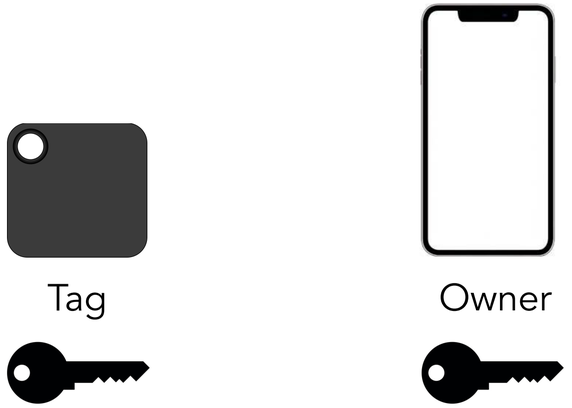
Tile’s protocol

1. **Registration and pairing**



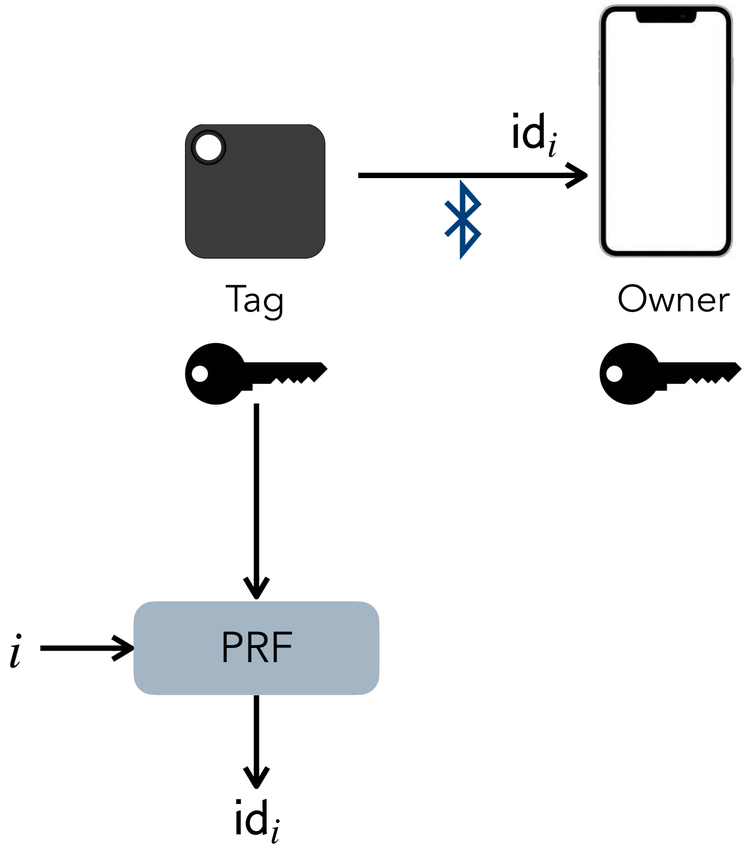
Tile’s protocol

2. Post-pairing interactions



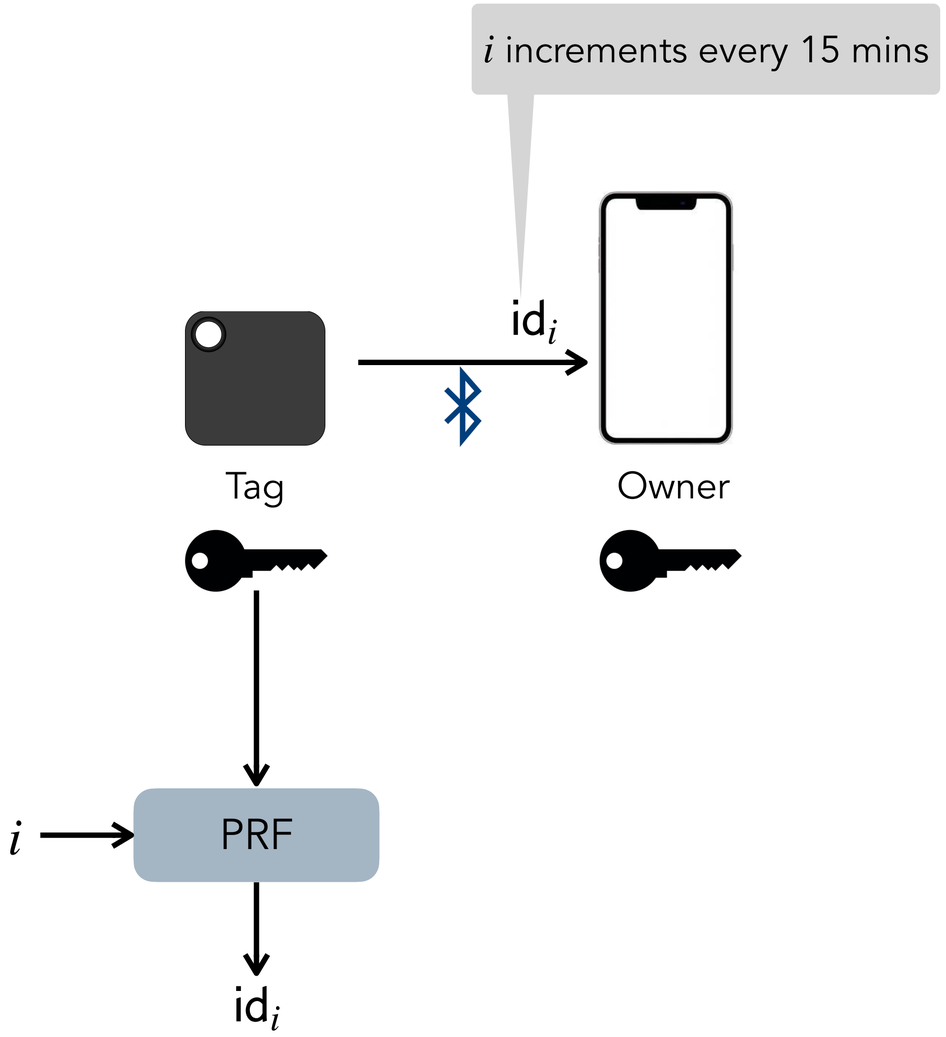
Tile’s protocol

2. Post-pairing interactions



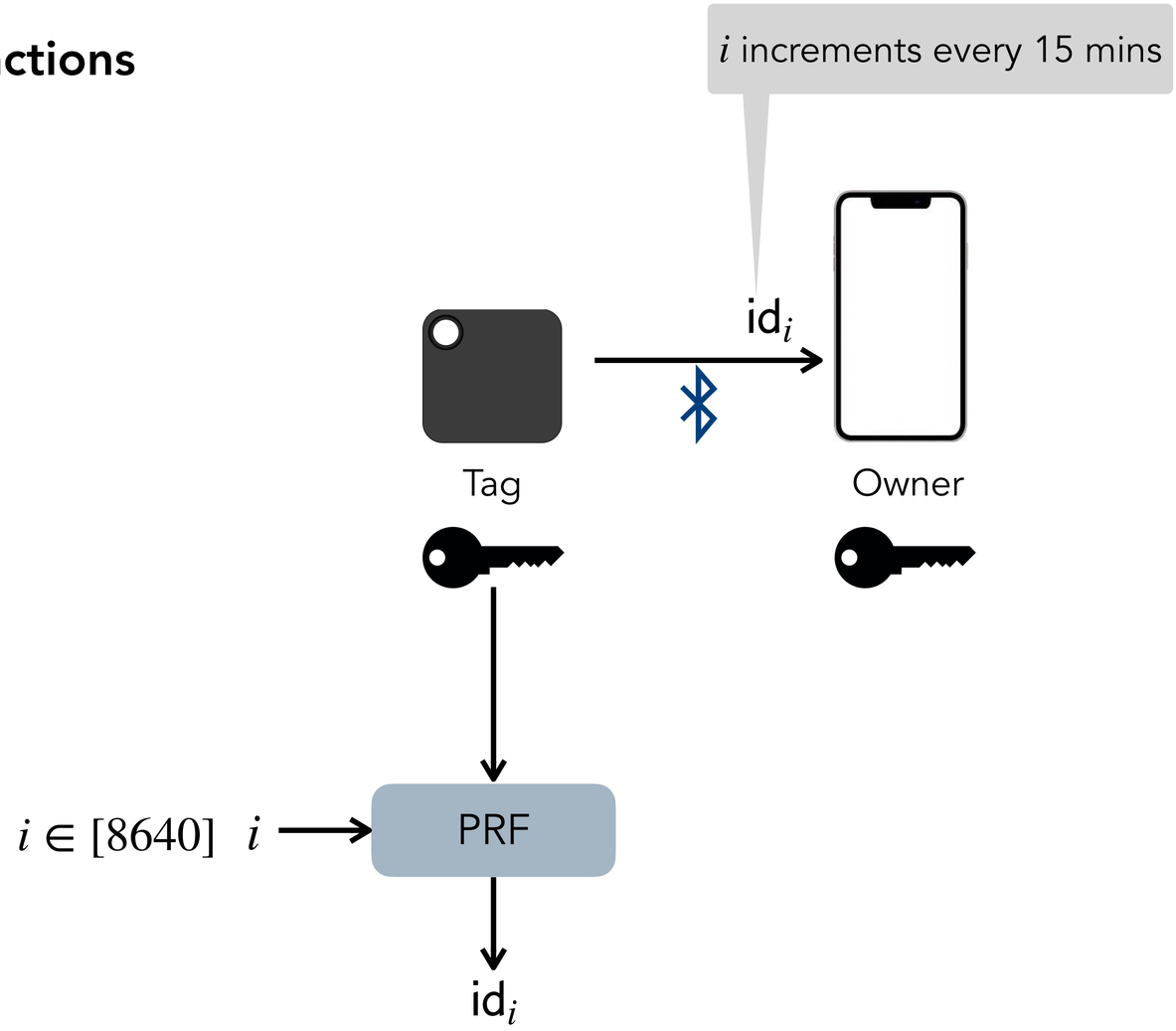
Tile’s protocol

2. Post-pairing interactions



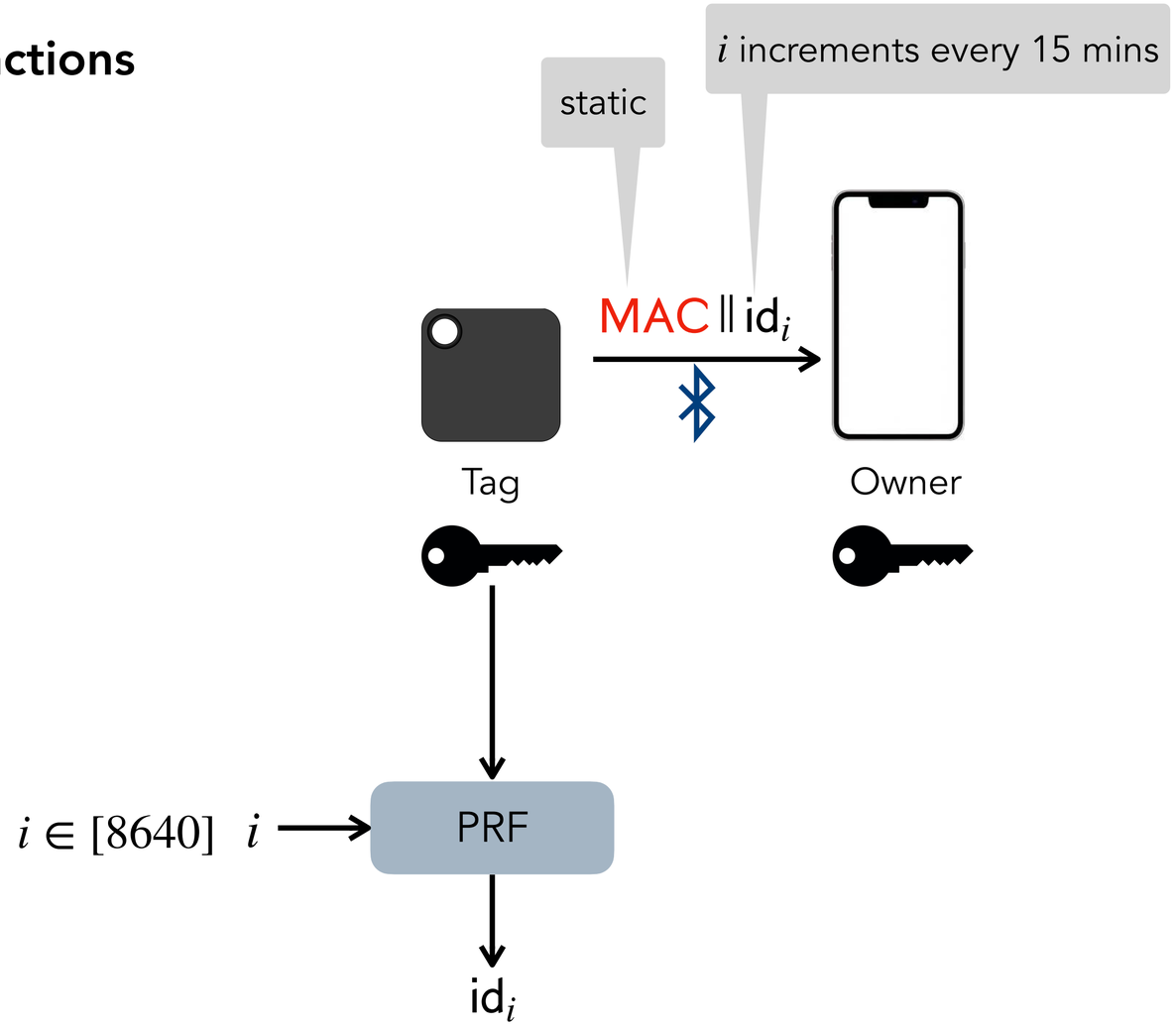
Tile's protocol

2. Post-pairing interactions



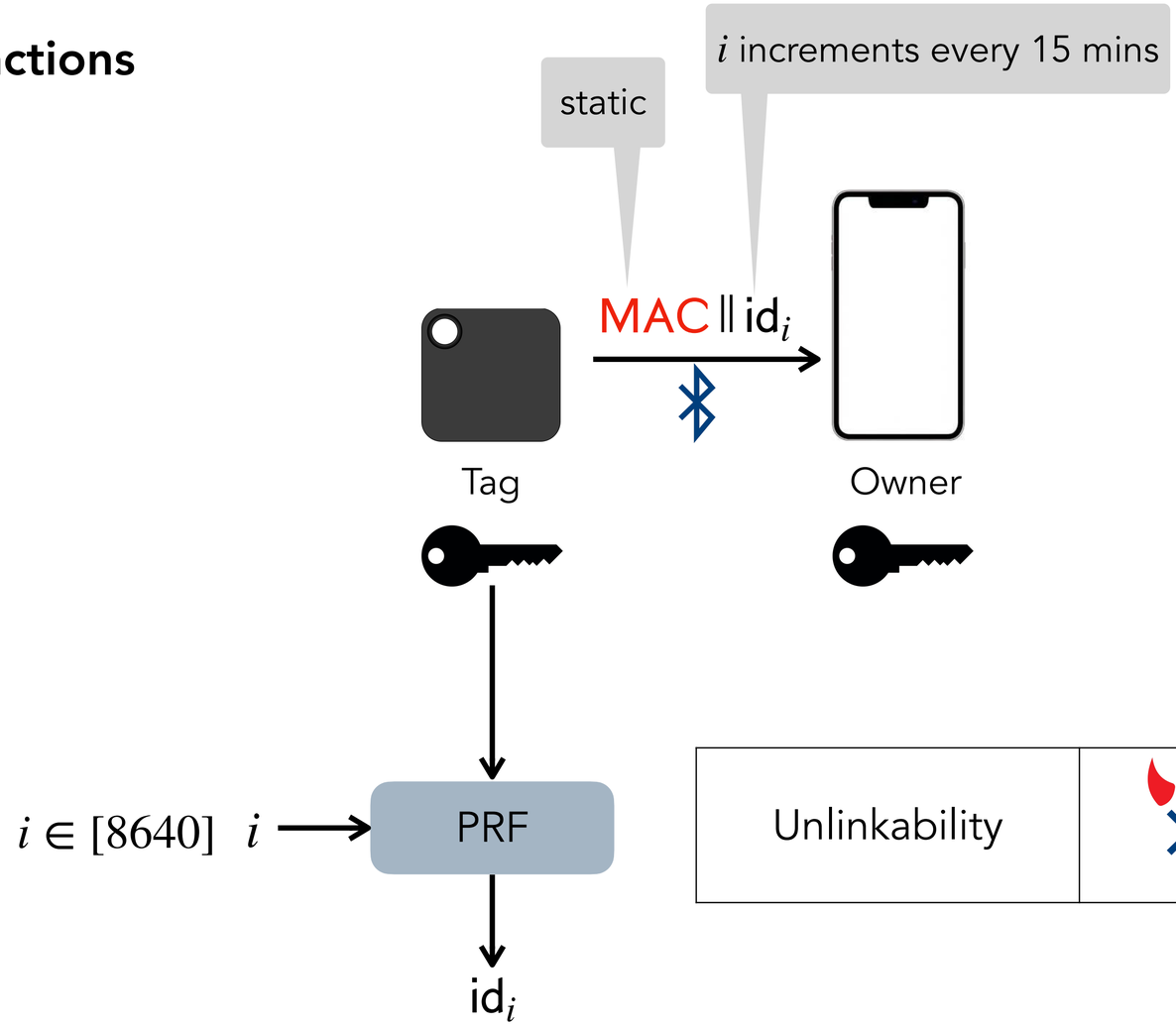
Tile's protocol

2. Post-pairing interactions



Tile's protocol

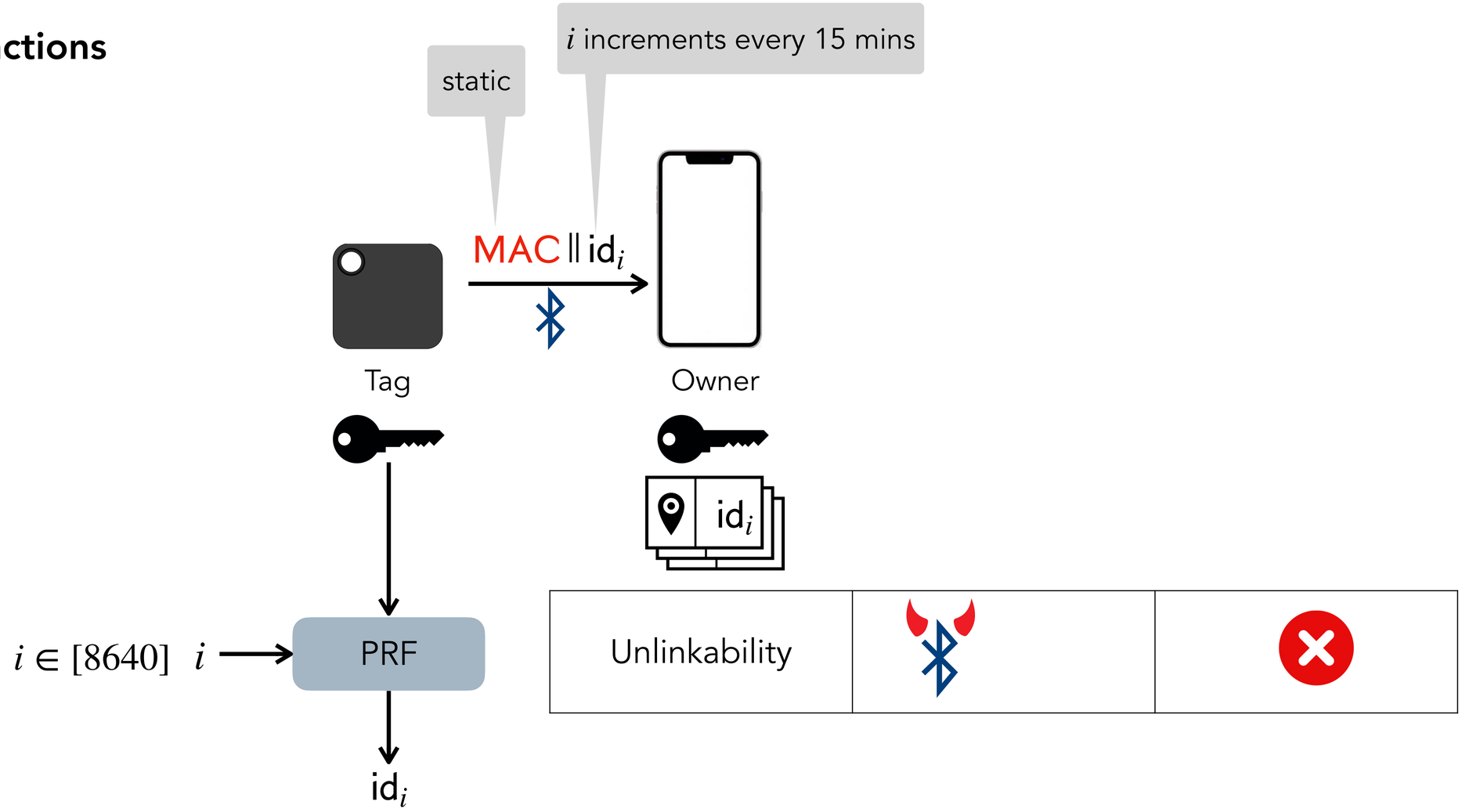
2. Post-pairing interactions



Unlinkability		

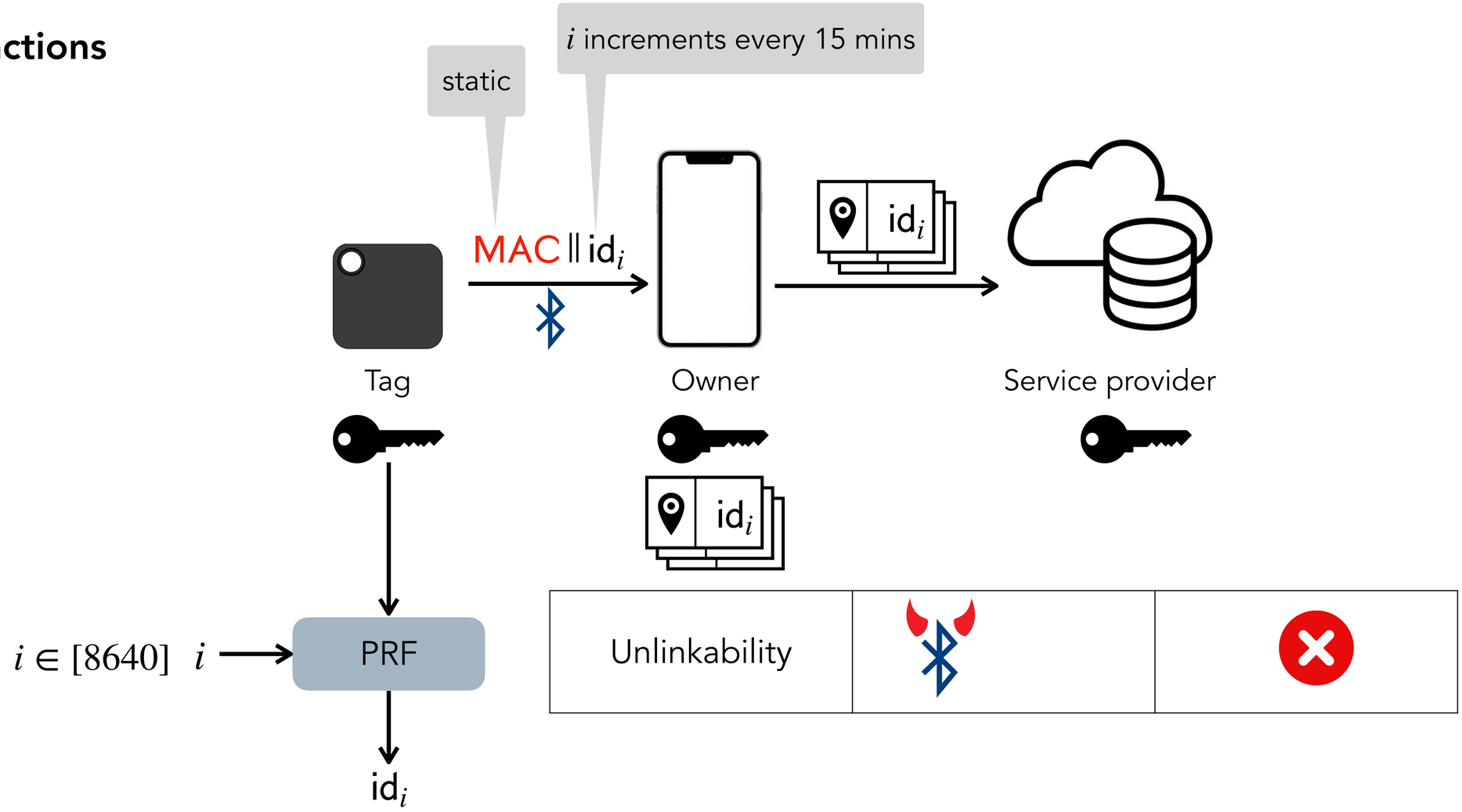
Tile's protocol

2. Post-pairing interactions



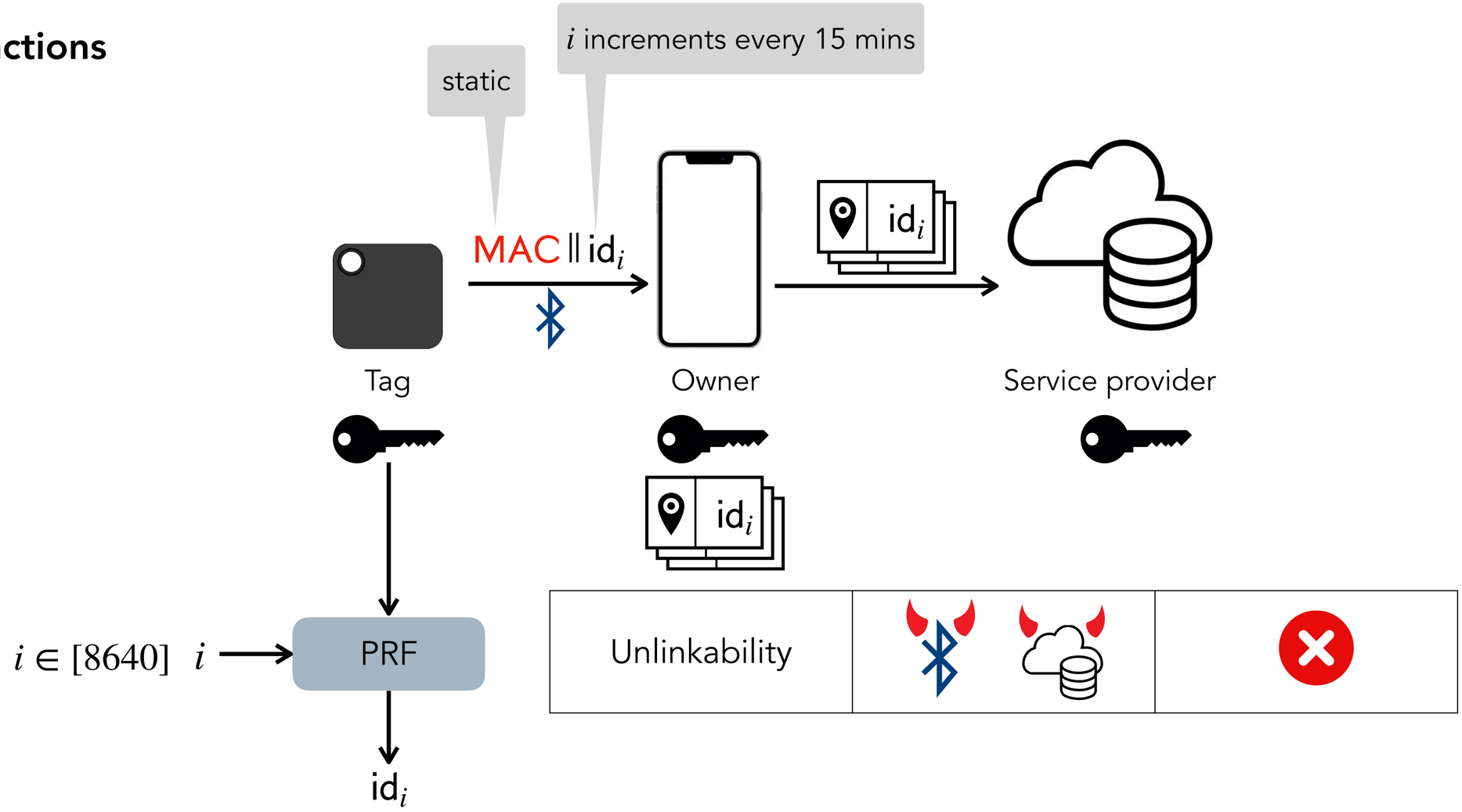
Tile's protocol

2. Post-pairing interactions



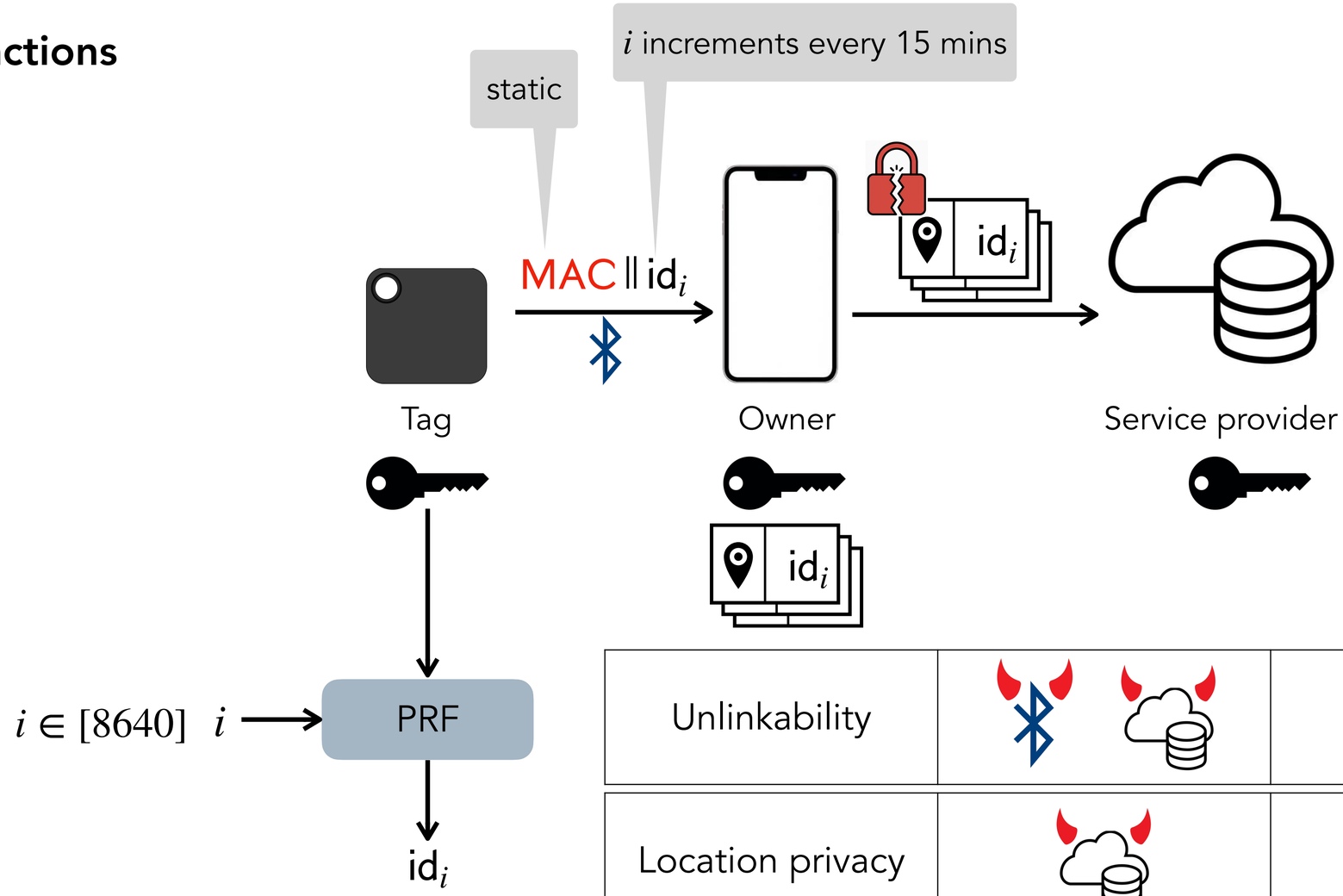
Tile's protocol

2. Post-pairing interactions



Tile's protocol

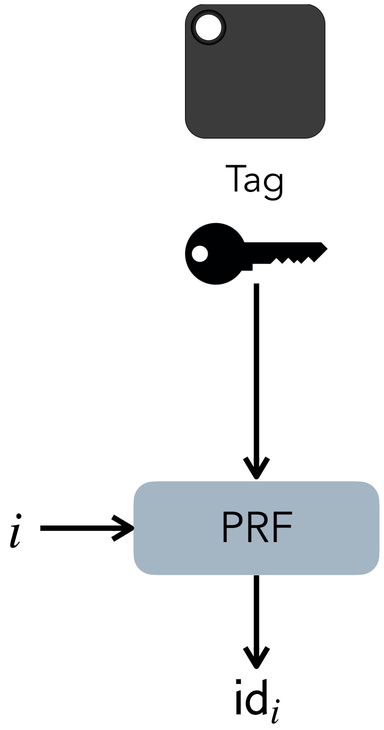
2. Post-pairing interactions



Unlinkability		
Location privacy		

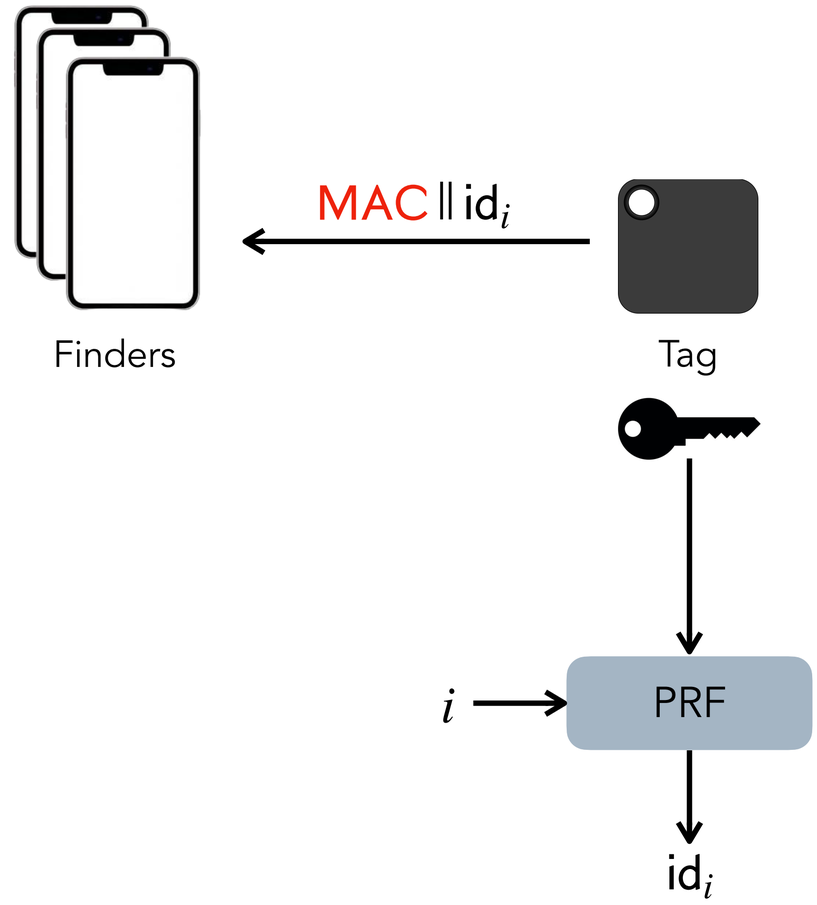
Tile’s protocol

2. Post-pairing interactions



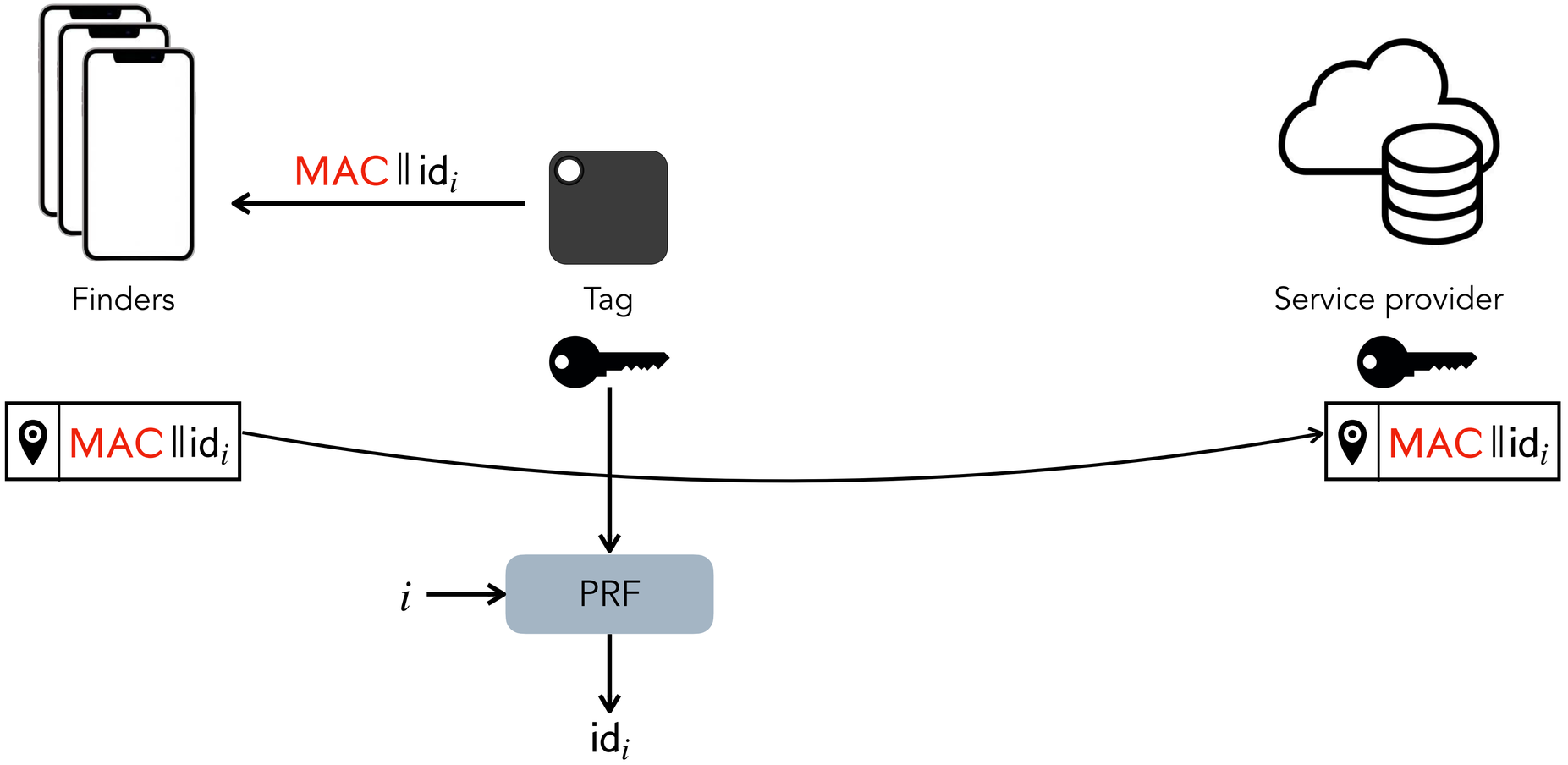
Tile’s protocol

2. Post-pairing interactions



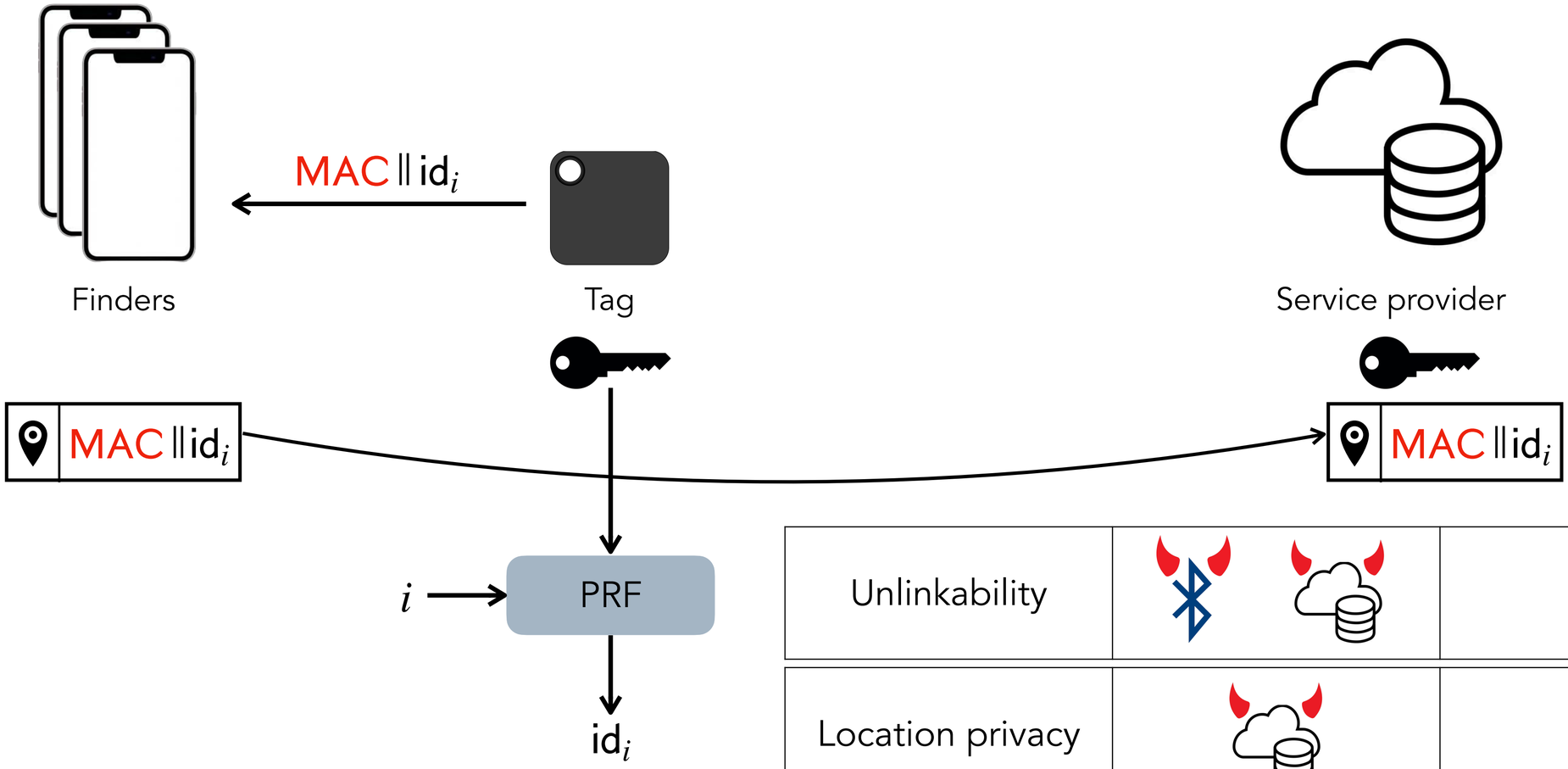
Tile's protocol

2. Post-pairing interactions



Tile's protocol

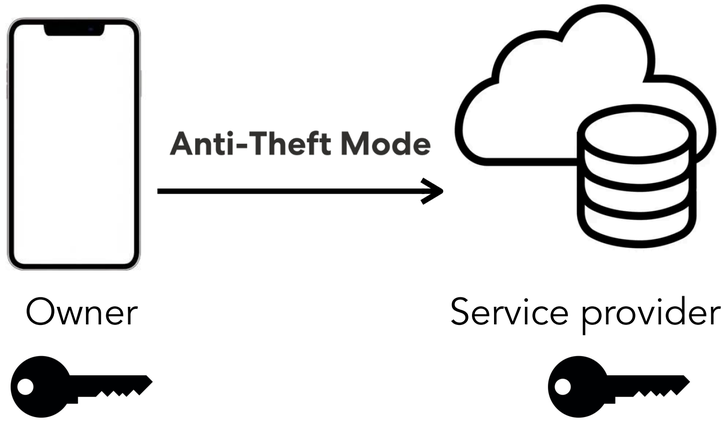
2. Post-pairing interactions



Unlinkability		
Location privacy		

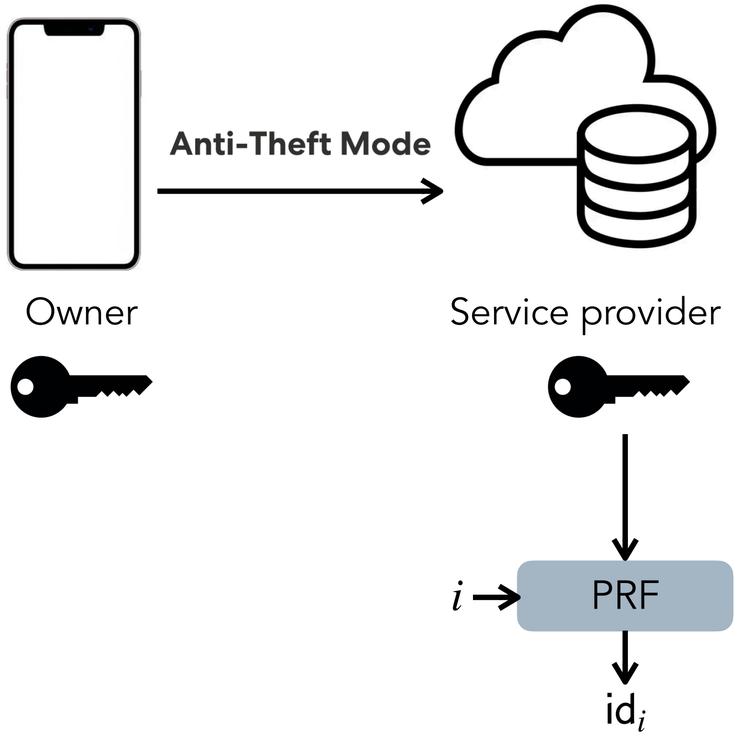
Tile’s protocol

3. The Anti-Theft mode



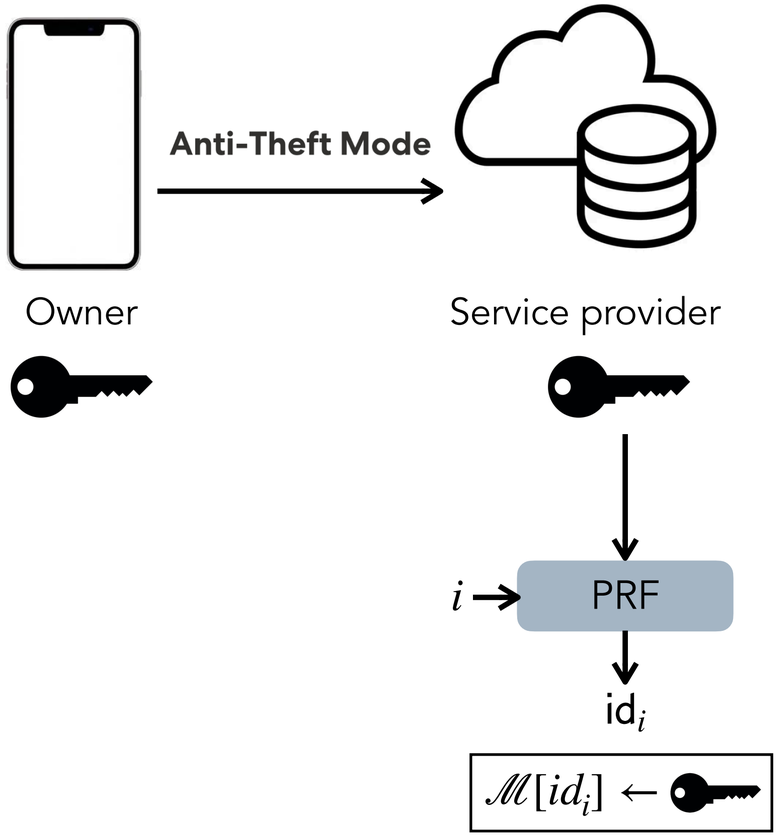
Tile’s protocol

3. The Anti-Theft mode



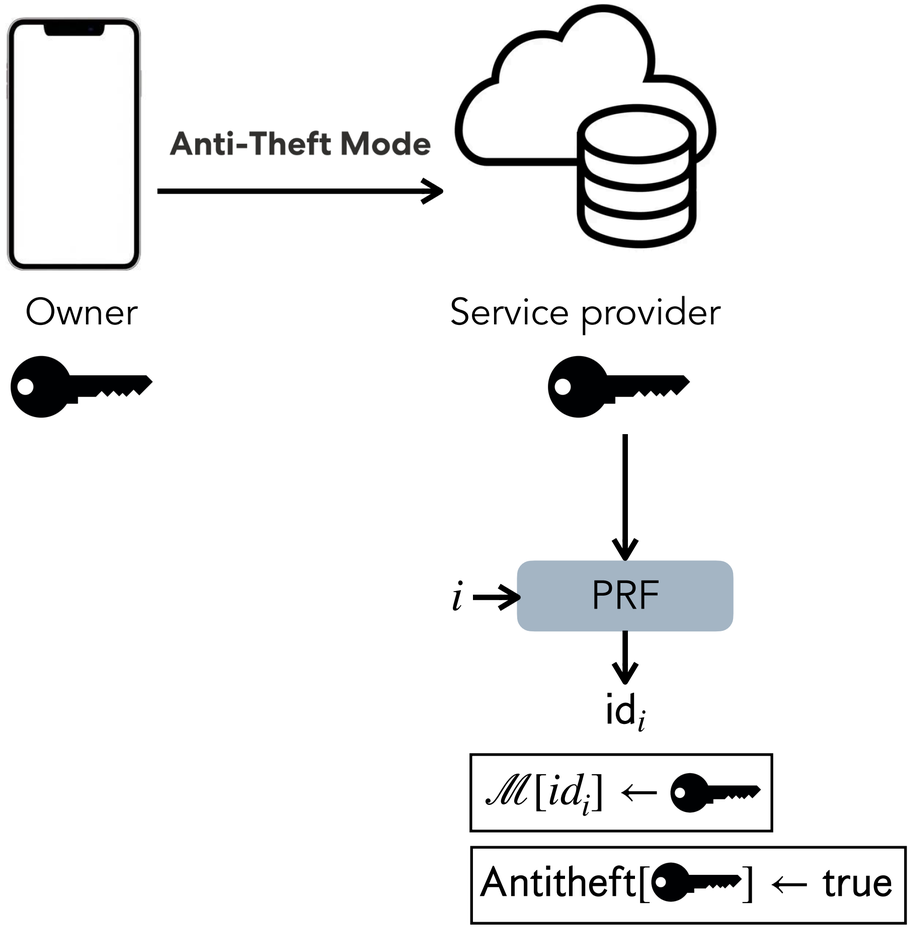
Tile’s protocol

3. The Anti-Theft mode



Tile’s protocol

3. The Anti-Theft mode



Tile’s protocol

4. Stalking detection



Tile’s protocol

4. Stalking detection

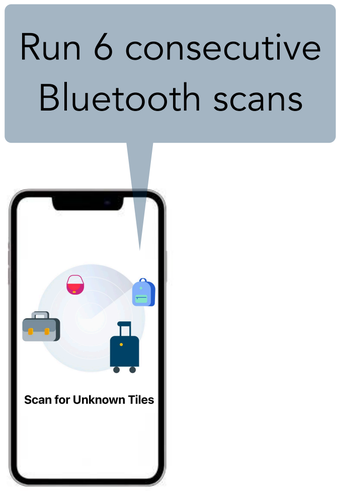




Tile’s protocol

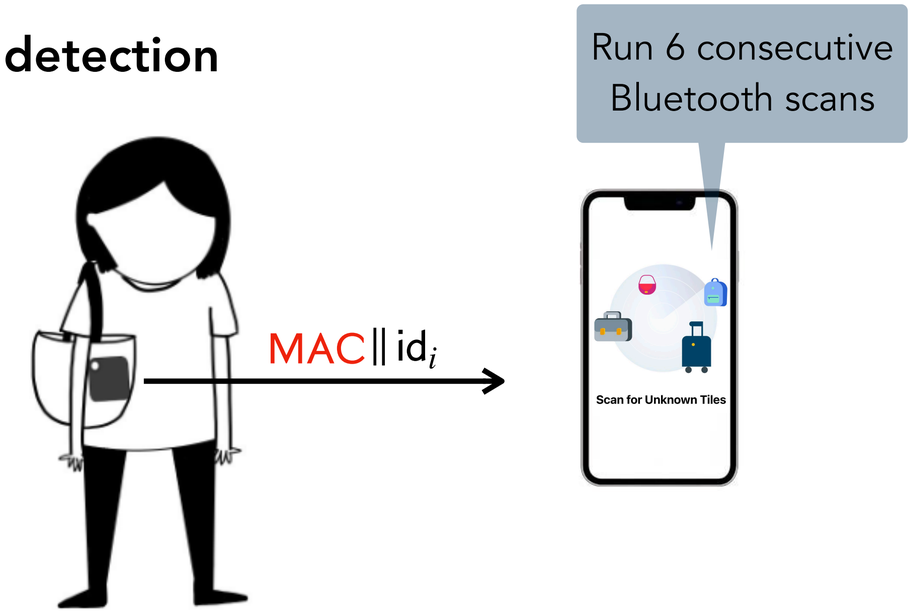
4. Stalking detection





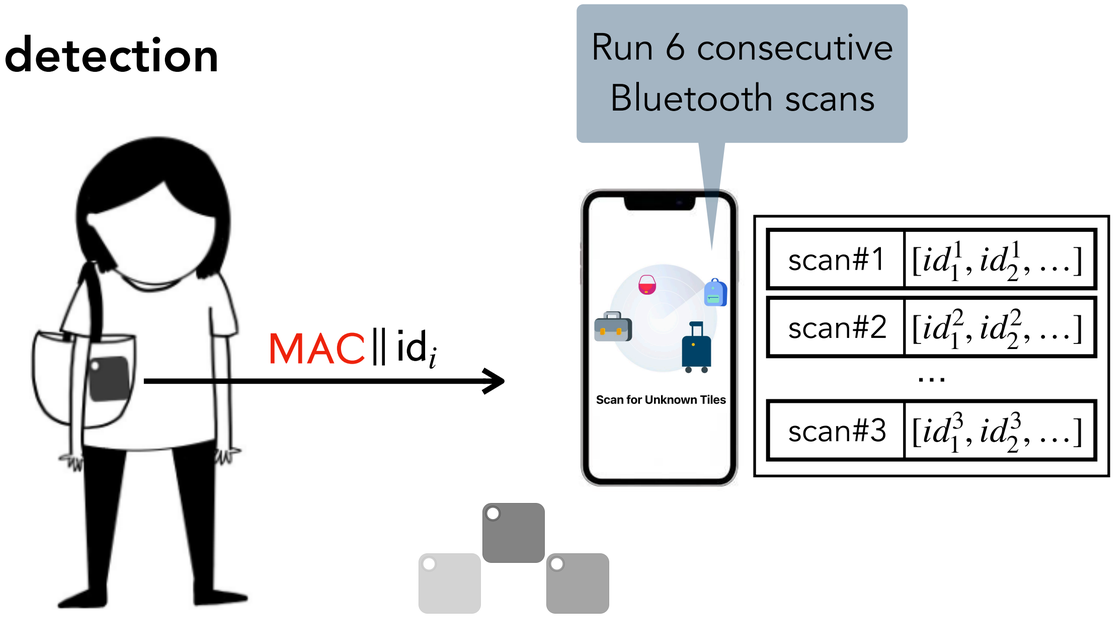
Tile’s protocol

4. Stalking detection



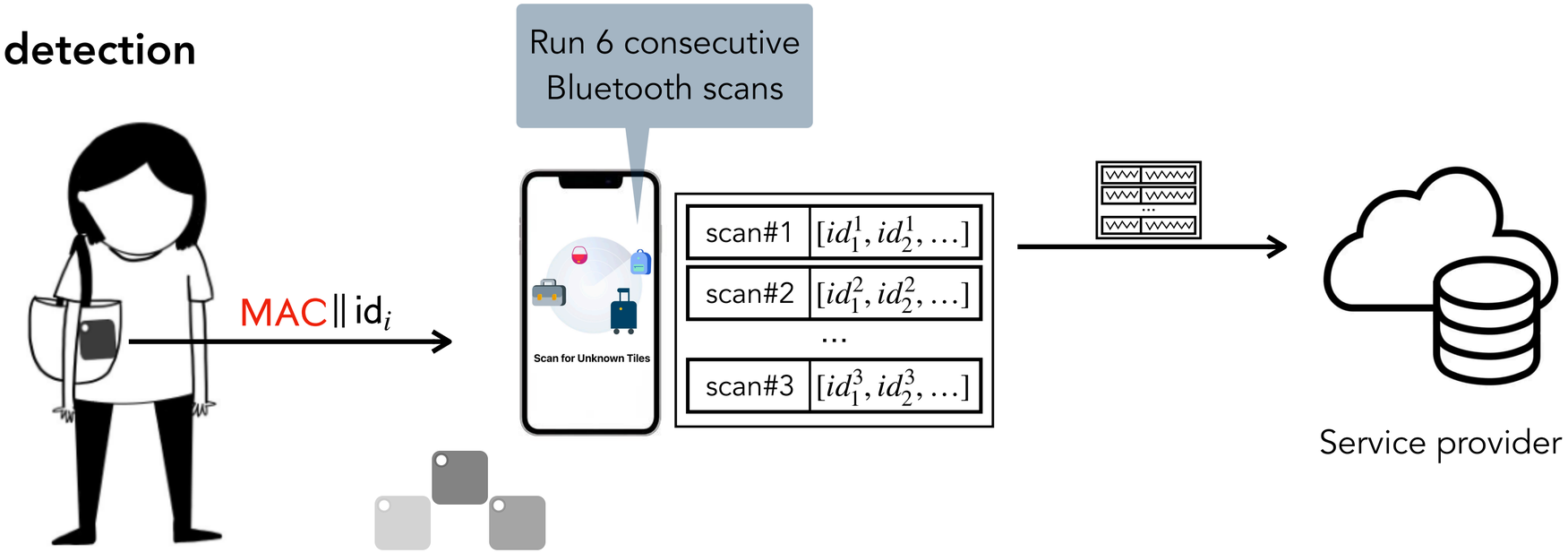
Tile’s protocol

4. Stalking detection



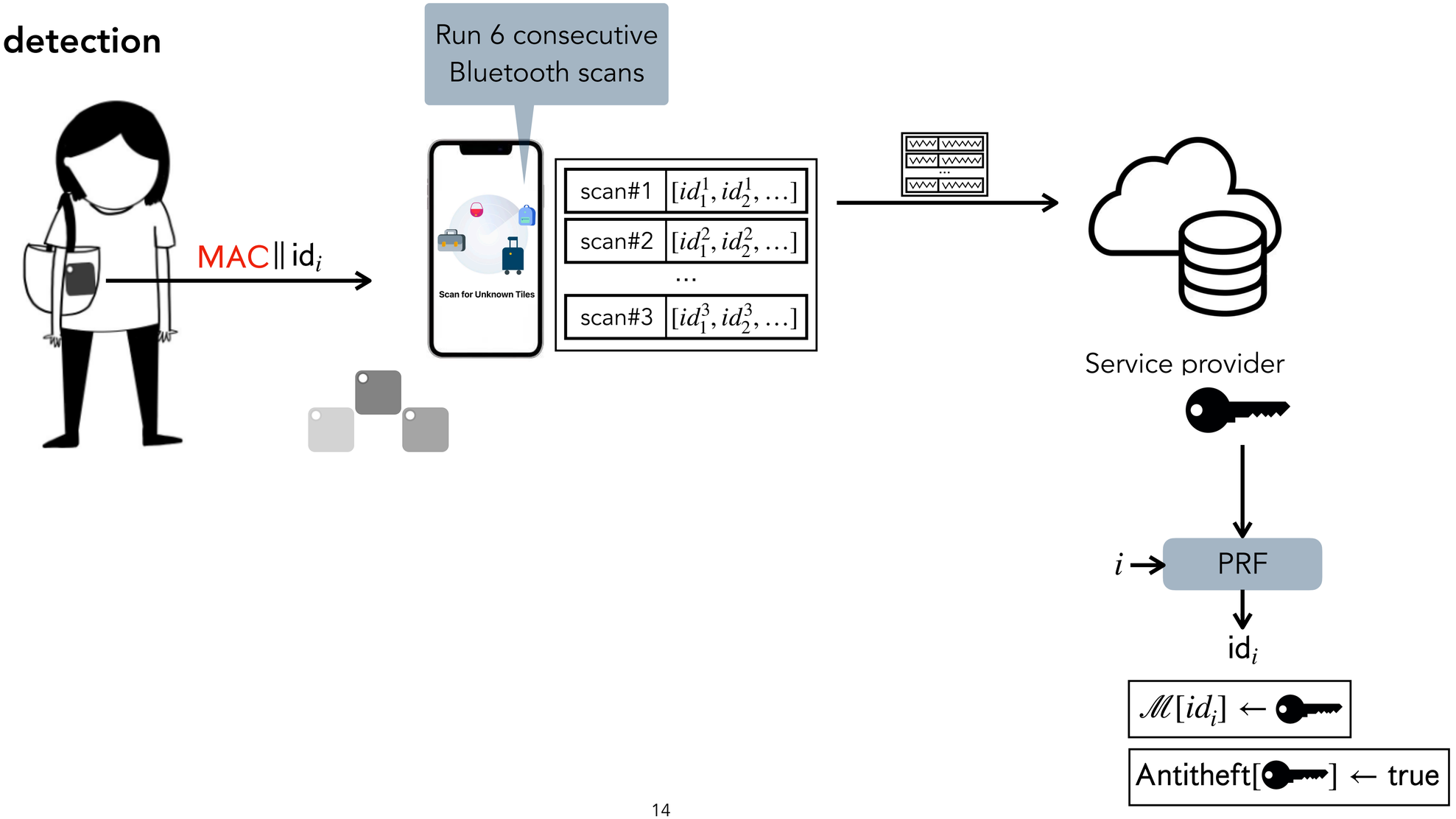
Tile’s protocol

4. Stalking detection



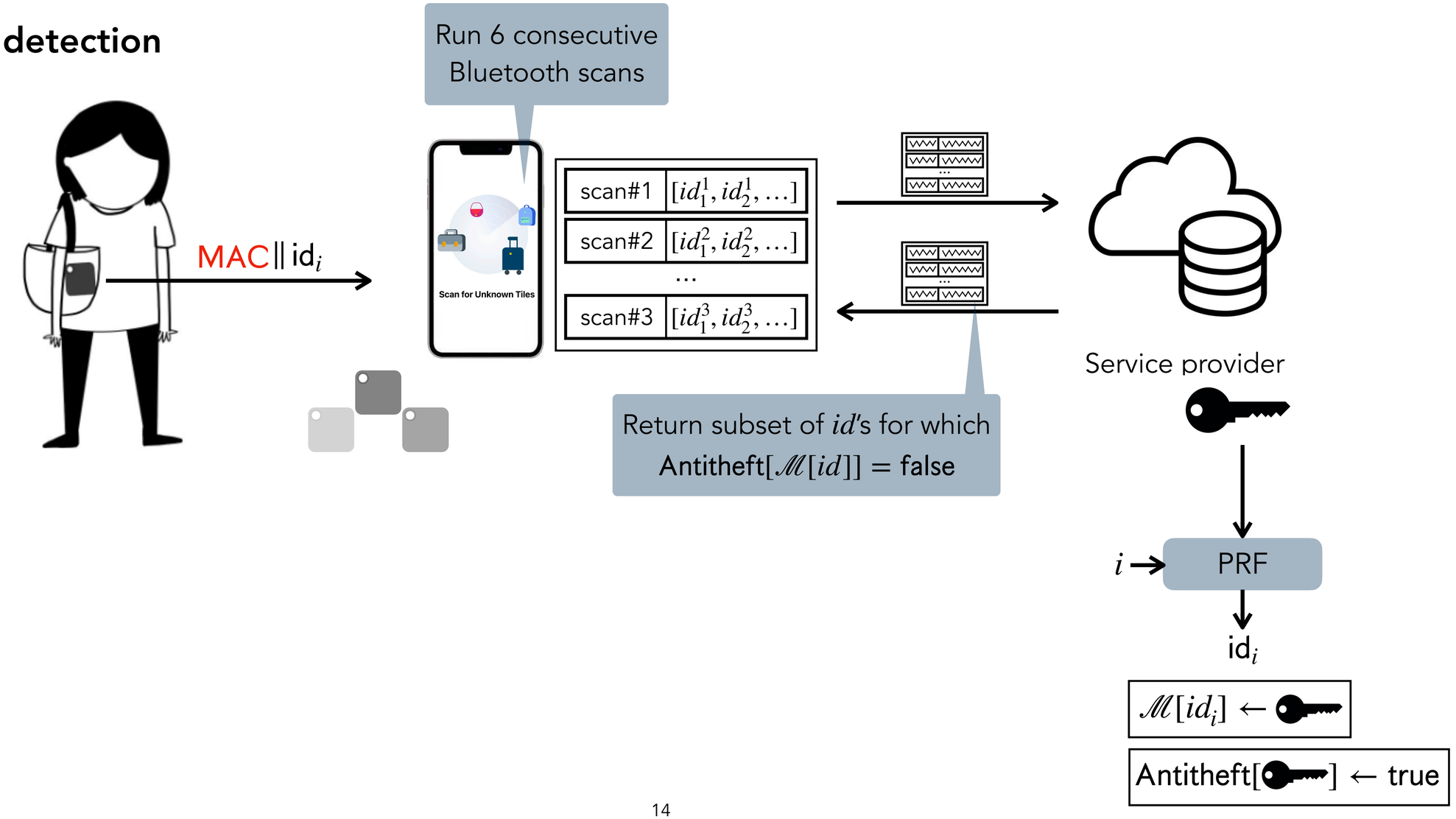
Tile's protocol

4. Stalking detection



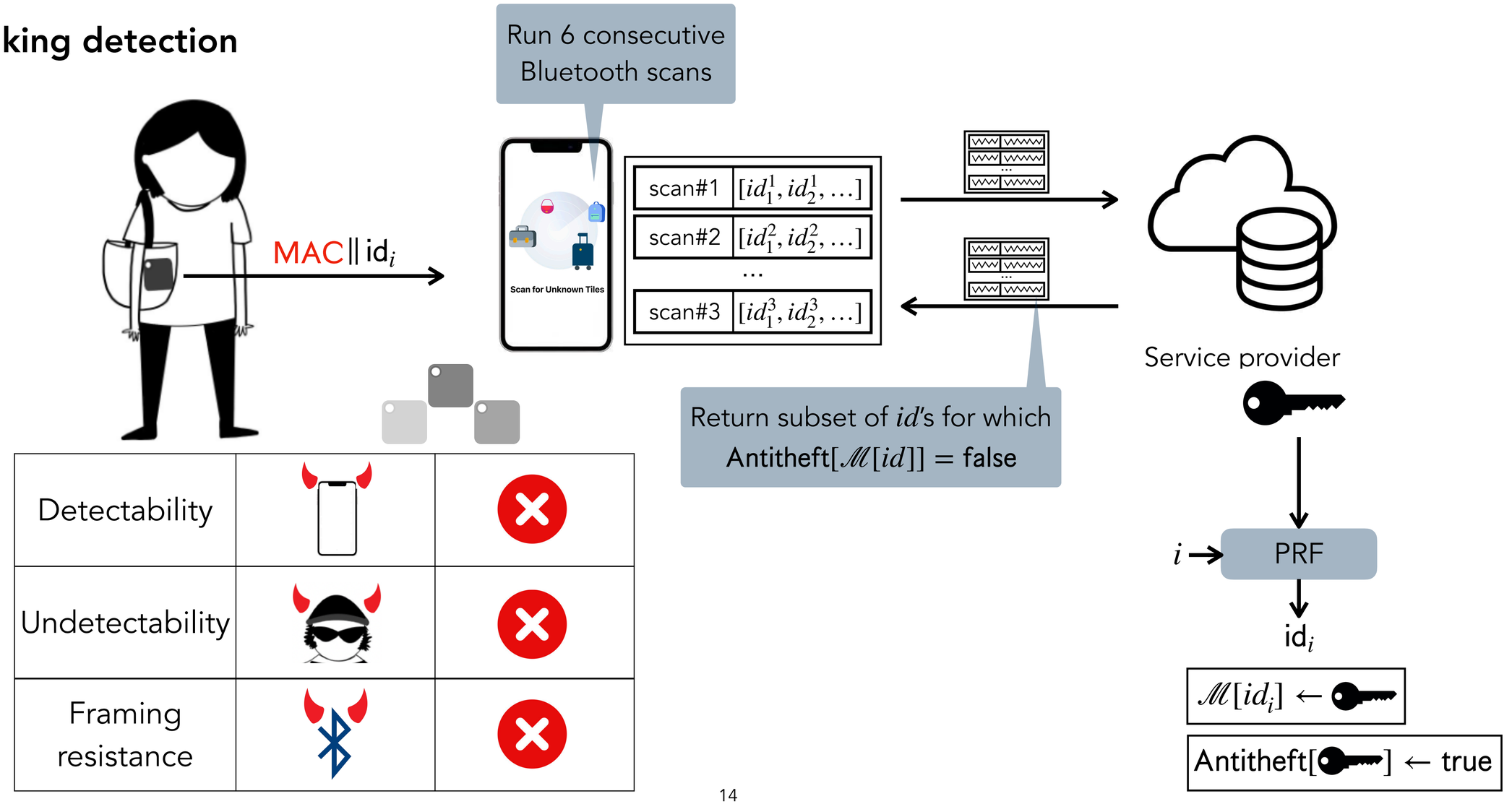
Tile's protocol

4. Stalking detection



Tile's protocol

4. Stalking detection



Detectability		
Undetectability		
Framing resistance		

Summary of Tile’s analysis

Privacy ✗

No unlinkability

No location privacy

Safety ✗

Usability concerns with detectability

Detectability relies on lack of privacy

No way to locate detected Tiles

Summary of Tile's analysis

Privacy ✗

No unlinkability

No location privacy

Safety ✗

Usability concerns with detectability

Detectability relies on lack of privacy

No way to locate detected Tiles

Insecurities arise from failure to balance conflicting goals:
(i) unlinkability x detectability
(ii) undetectability x detectability
(Many other things go wrong; details in the paper!)

Takeaways

Takeaways

1. Bluetooth-based location tracking is an important topic area particularly given widespread use for stalking

Takeaways

1. Bluetooth-based location tracking is an important topic area particularly given widespread use for stalking

2. Tile case study shows what can go wrong

Takeaways

1. Bluetooth-based location tracking is an important topic area particularly given widespread use for stalking

2. Tile case study shows what can go wrong

3. **Prioritize people over stuff:** Anti-theft directly opposed to anti-stalking; should be dropped as a goal

Takeaways

1. Bluetooth-based location tracking is an important topic area particularly given widespread use for stalking

2. Tile case study shows what can go wrong

3. **Prioritize people over stuff:** Anti-theft directly opposed to anti-stalking; should be dropped as a goal

4. **Accountability is important:** Providing accountability mechanisms to deter abuse in these systems remains an interesting open problem

Takeaways

1. Bluetooth-based location tracking is an important topic area particularly given widespread use for stalking
2. Tile case study shows what can go wrong
3. **Prioritize people over stuff:** Anti-theft directly opposed to anti-stalking; should be dropped as a goal
4. **Accountability is important:** Providing accountability mechanisms to deter abuse in these systems remains an interesting open problem

Akshaya Kumar, Anna Raymaker, Michael A. Specter

akshayakumar@gatech.edu

https://tinyurl.com/TileAnalysis

USENIX Security 2026