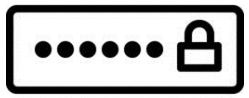
Reconciling Information-Flow Control and Database Access Control

Daniel Schoepe

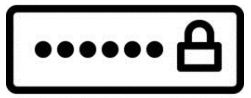
joint work with Marco Guarnieri, Musard Balliu, David Basin, Andrei Sabelfeld

(work in progress)

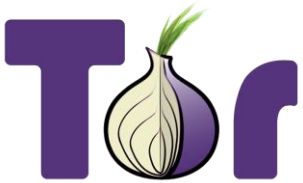
Sensitive data



Sensitive data

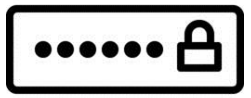


Untrusted code



Sensitive data

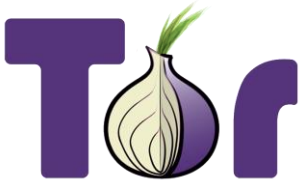





Untrusted code





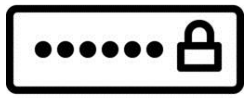




Public channels



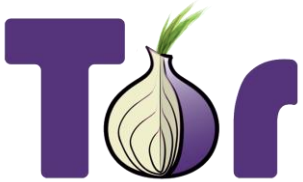
Sensitive data






Untrusted code




Private channels


Public channels

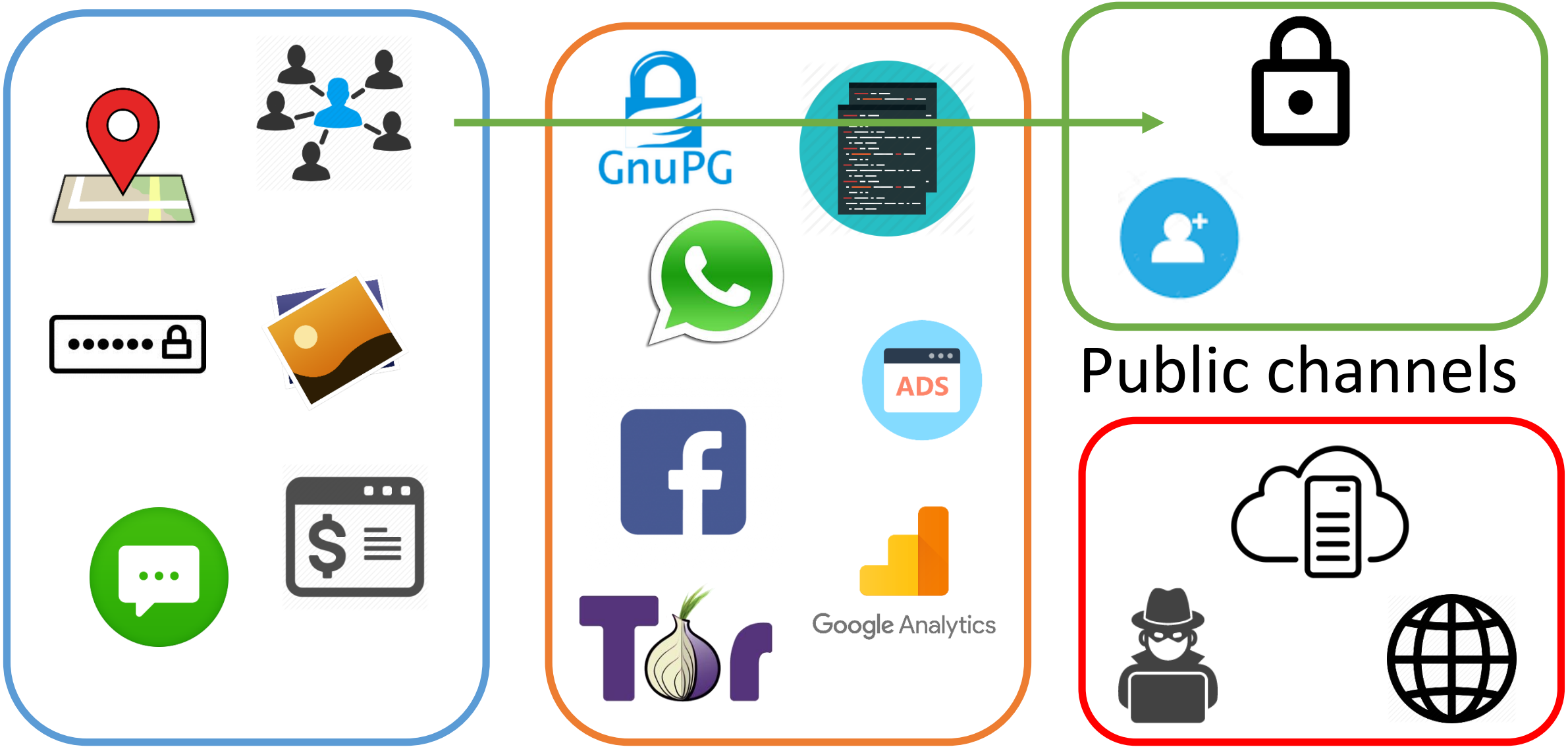


Sensitive data

Untrusted code

Private channels

Public channels

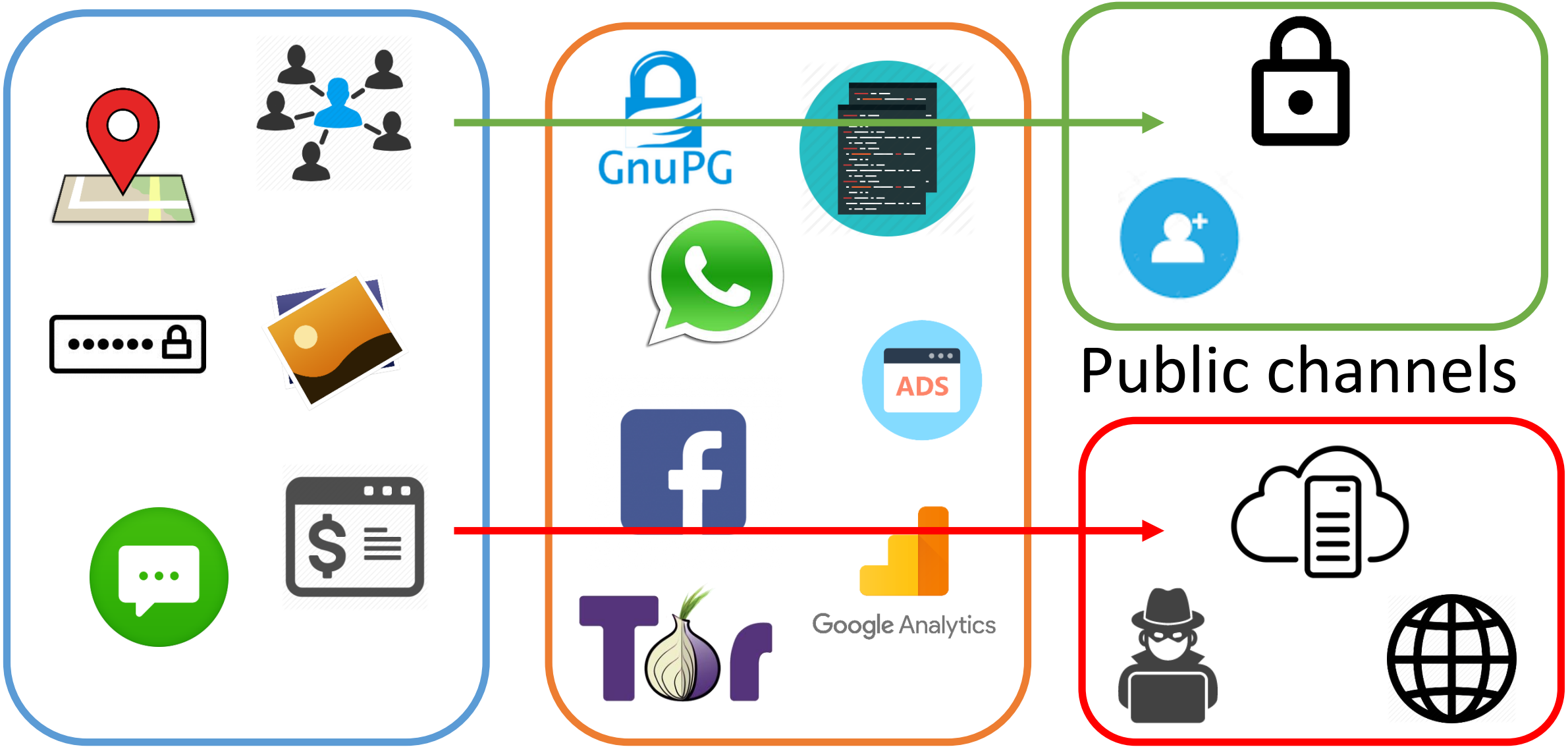


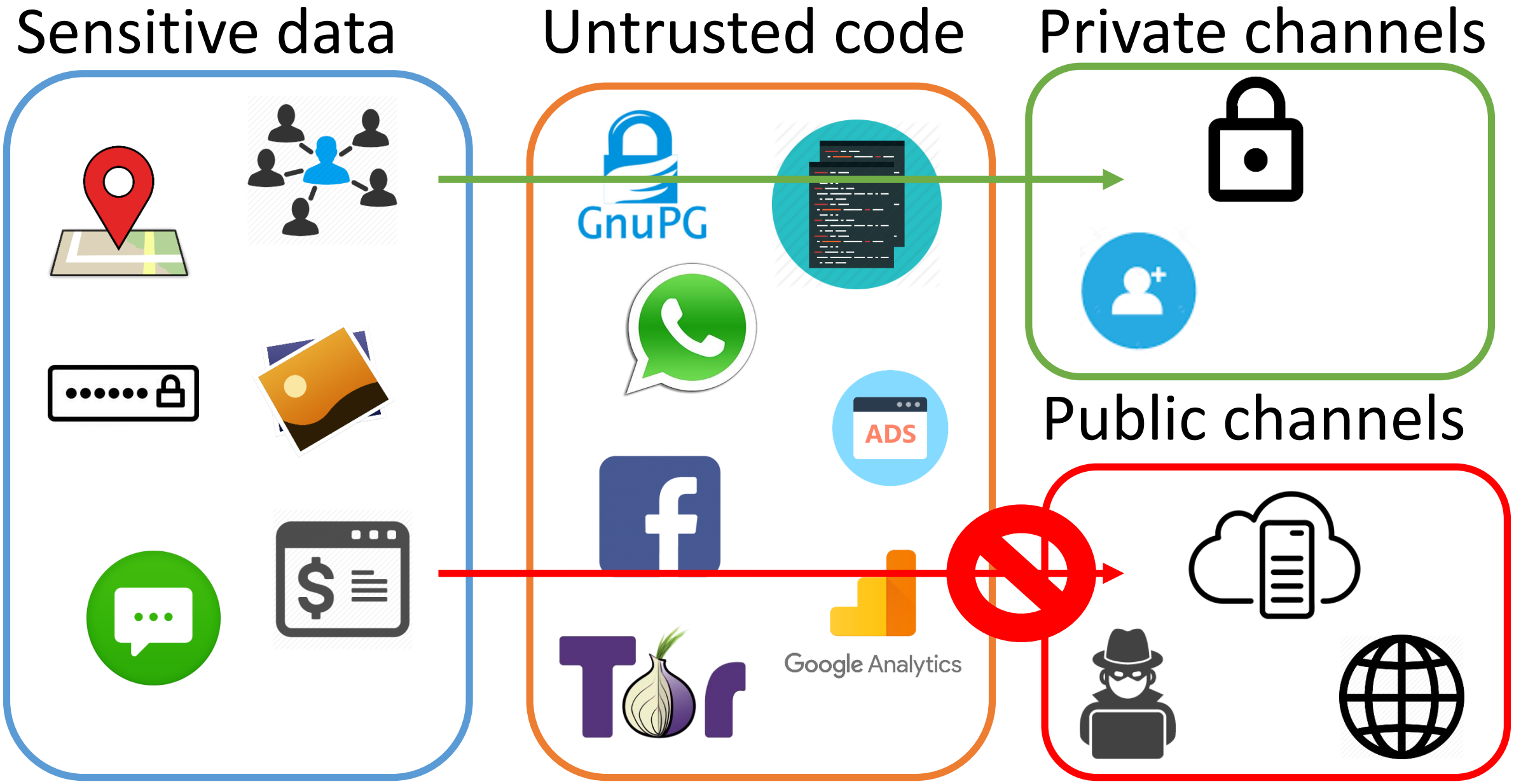
Sensitive data

Untrusted code

Private channels

Public channels




Sensitive data
Untrusted code
Private channels
GnuPG
ADS
Public channels
Google Analytics
Tor

Noninterference

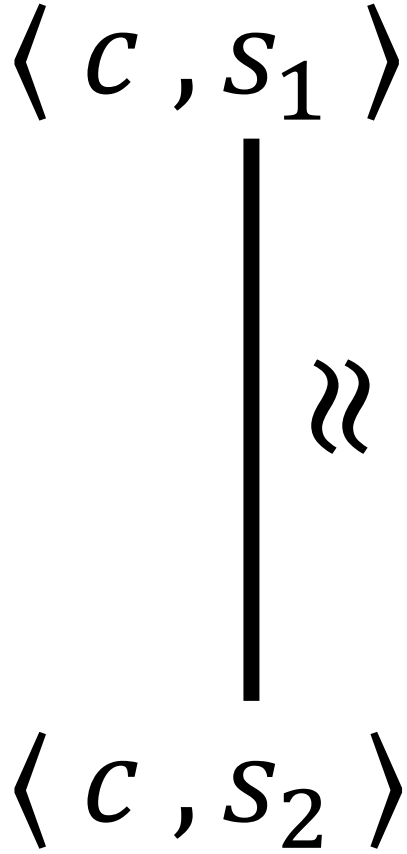
$\langle\, c\,, s_1\,\rangle$

Noninterference

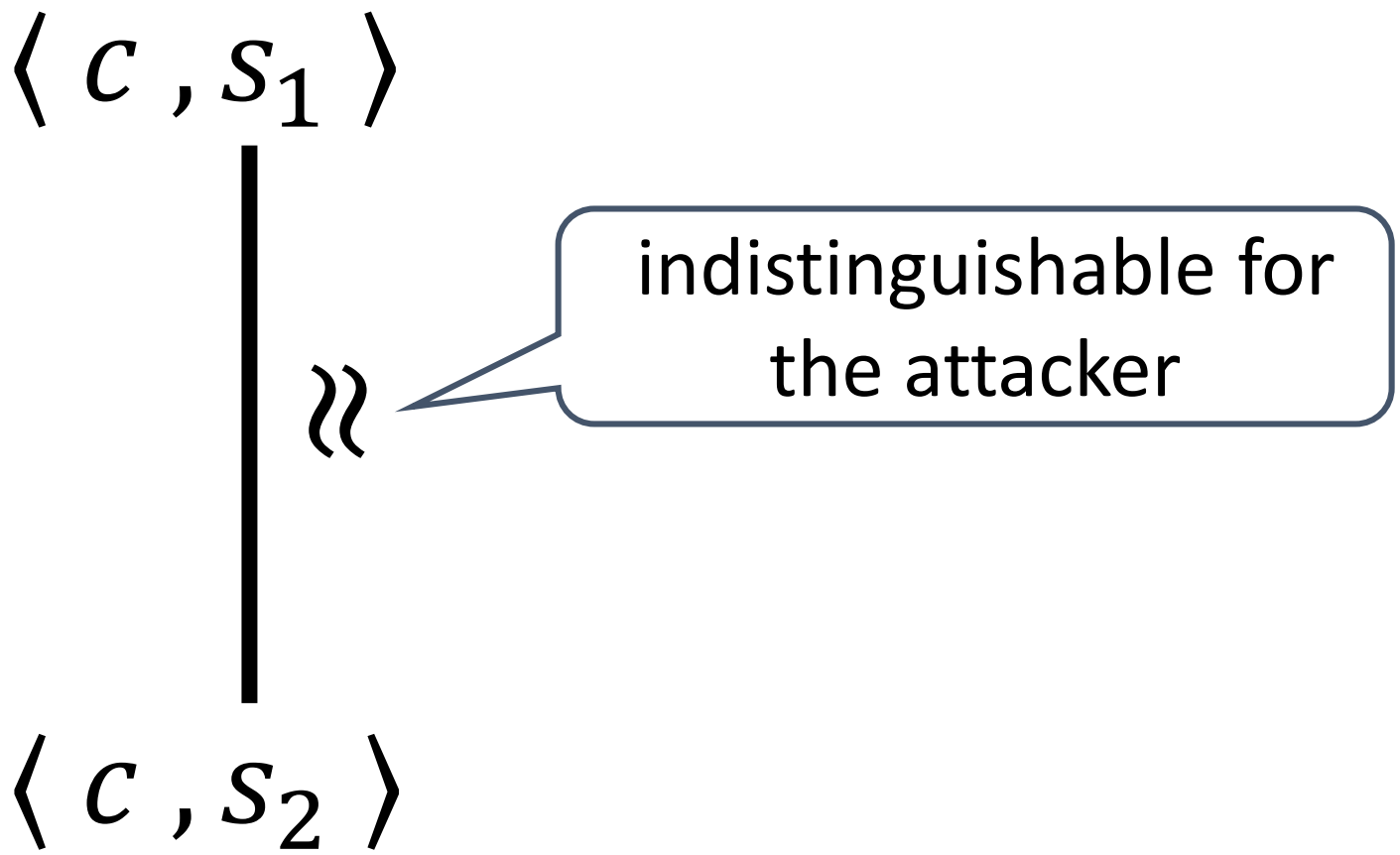
$\langle\, c\,, s_1\,\rangle$

$\langle\, c\,, s_2\,\rangle$

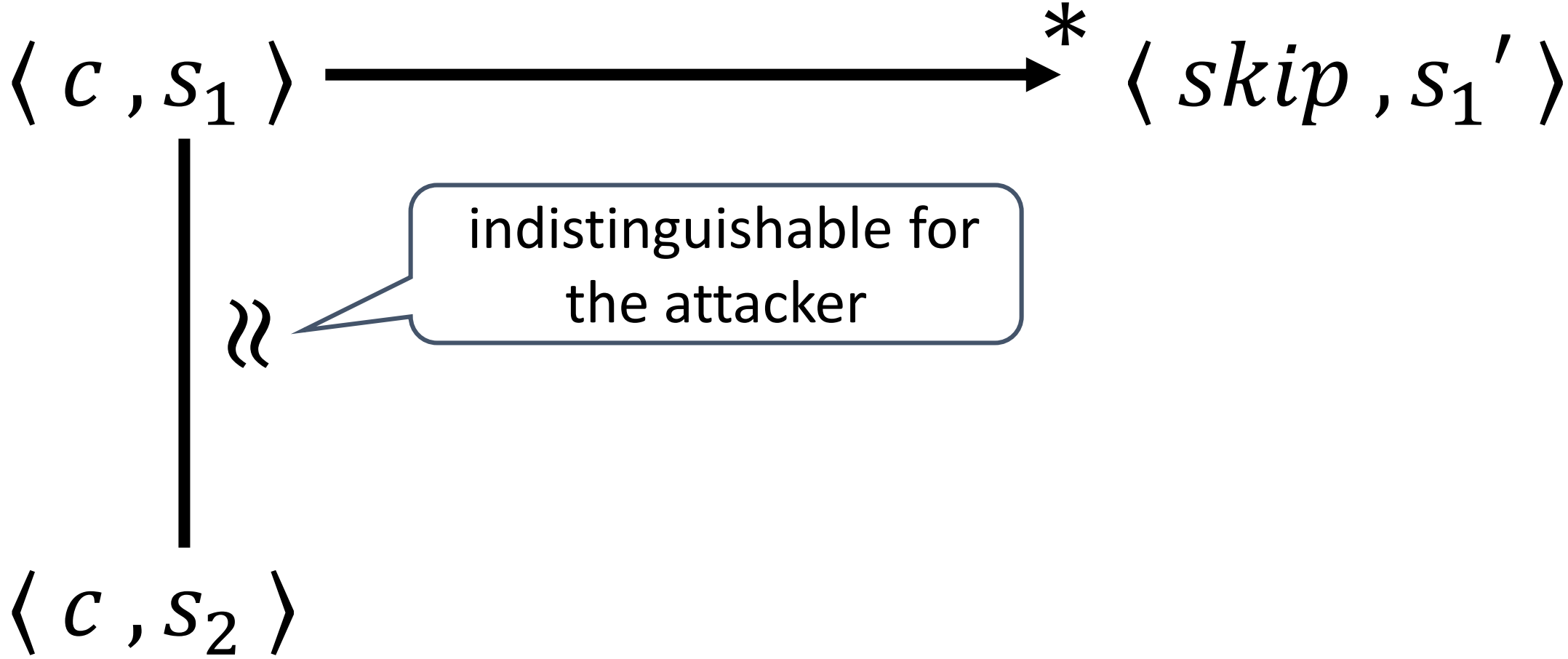
Noninterference



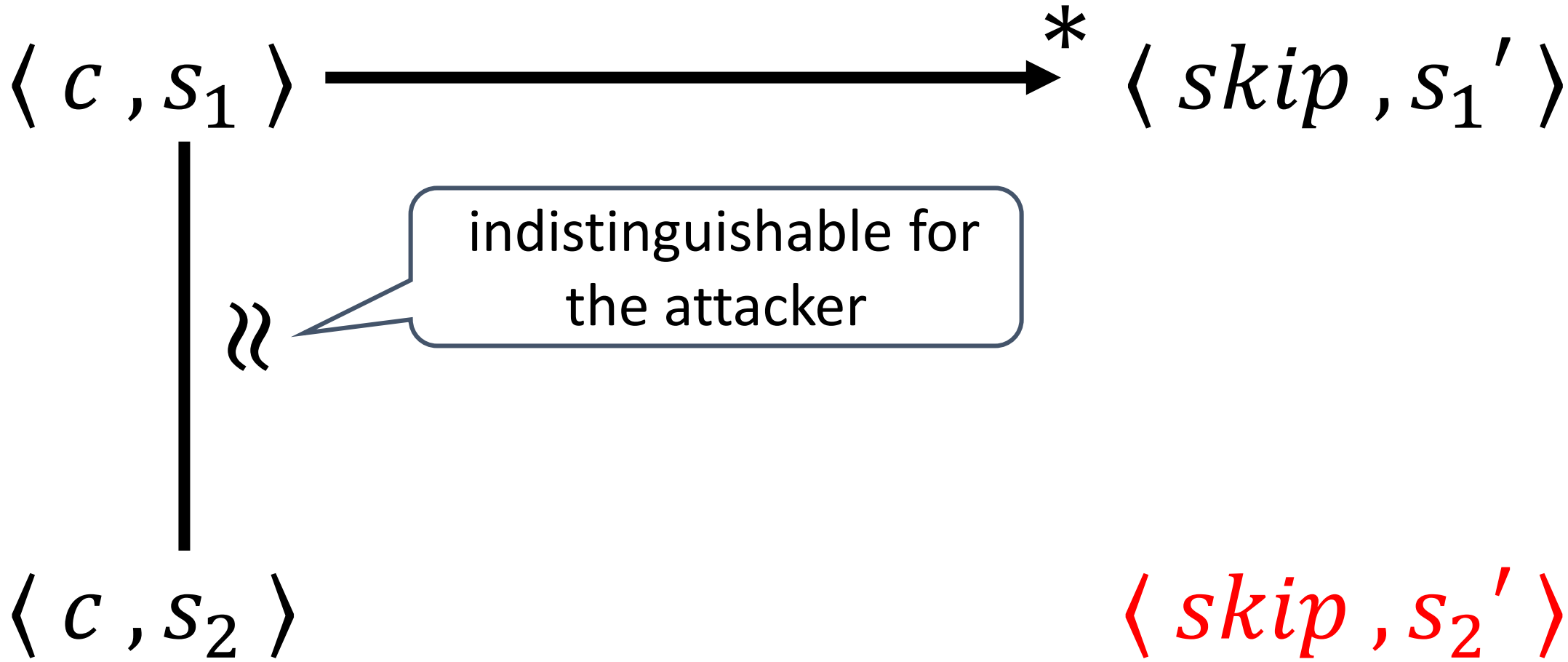
Noninterference



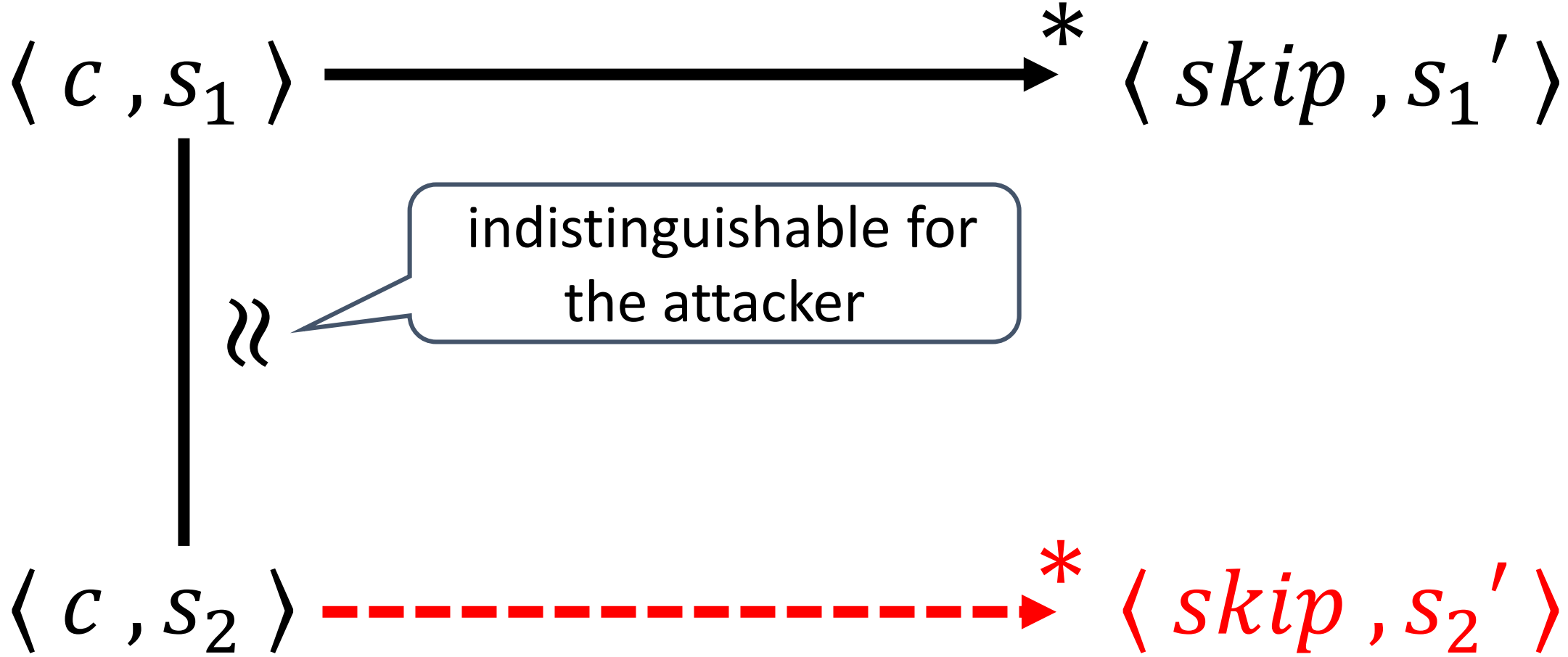
Noninterference



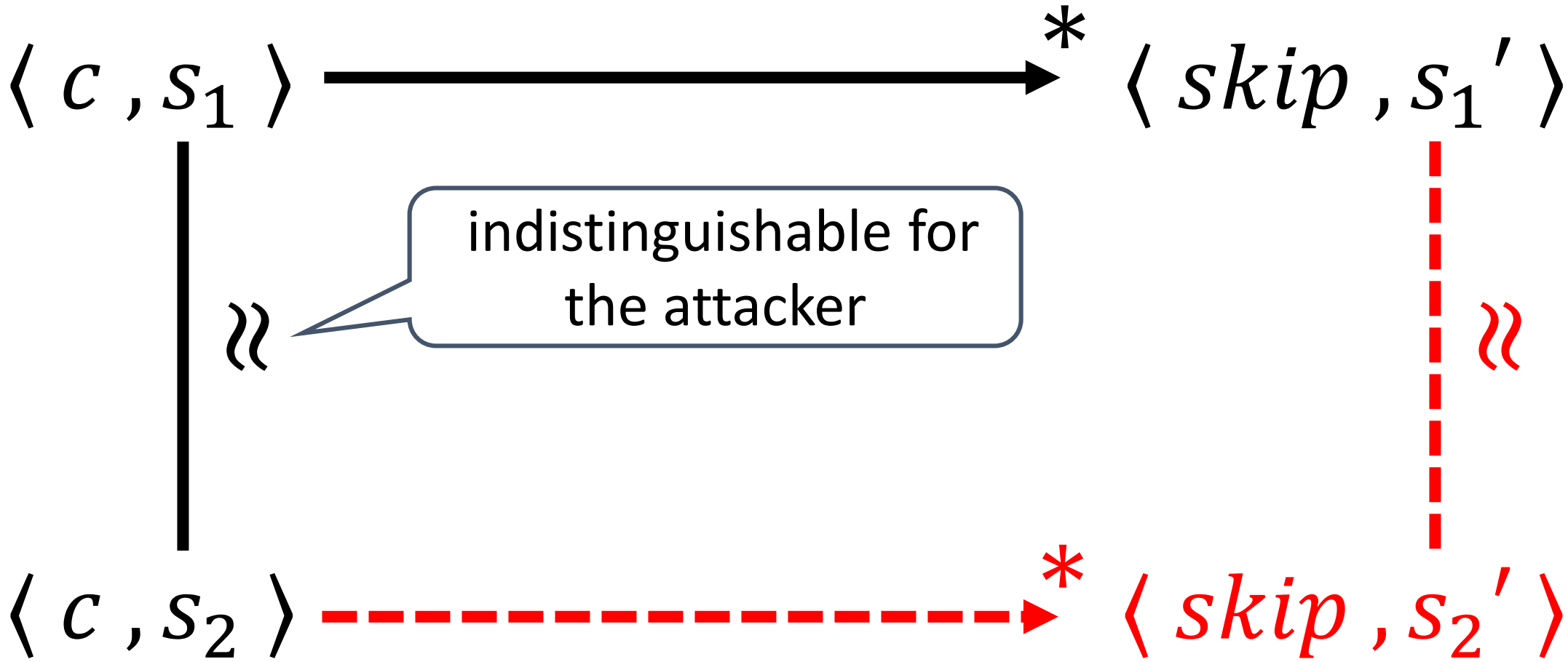
Noninterference



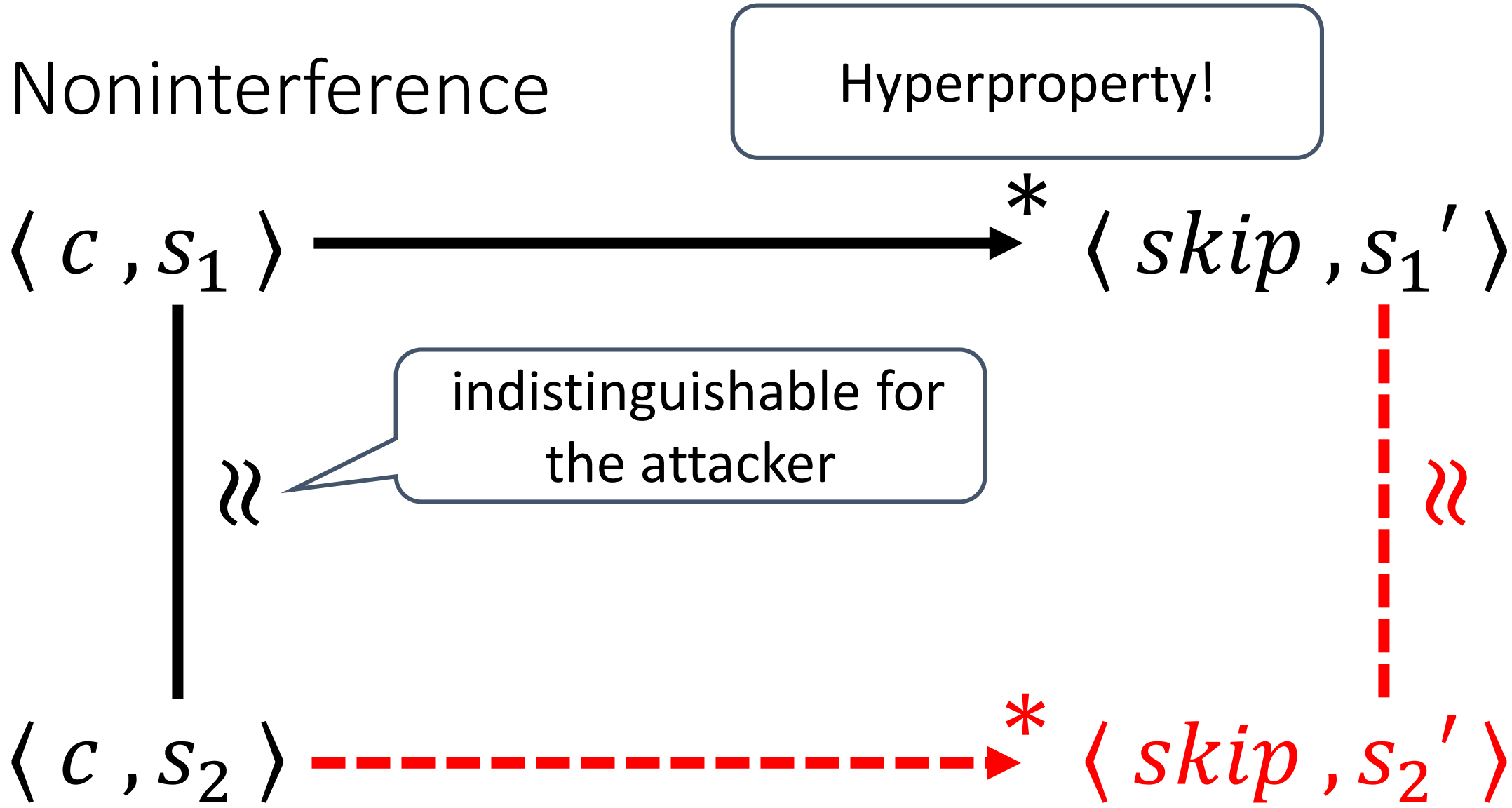
Noninterference



Noninterference



Noninterference

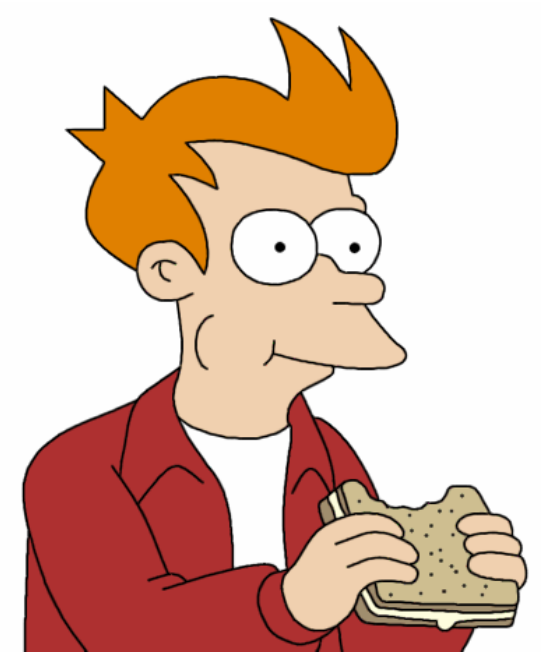


Database Access Control

User

Database

Database Access Control

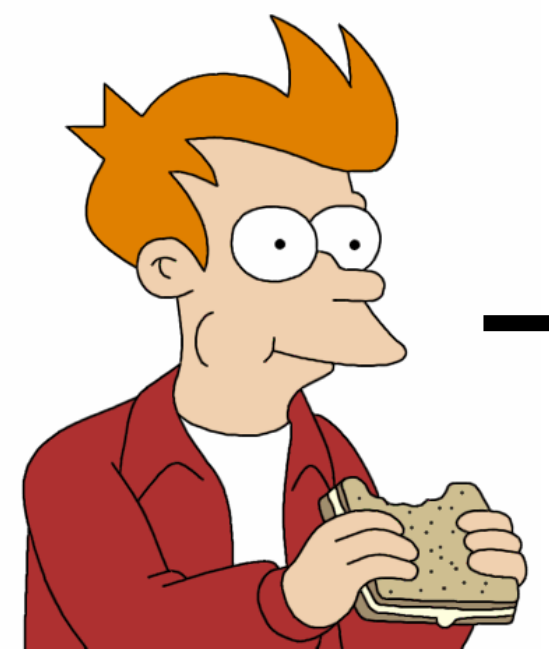


User

Access Control

Database

Database Access Control



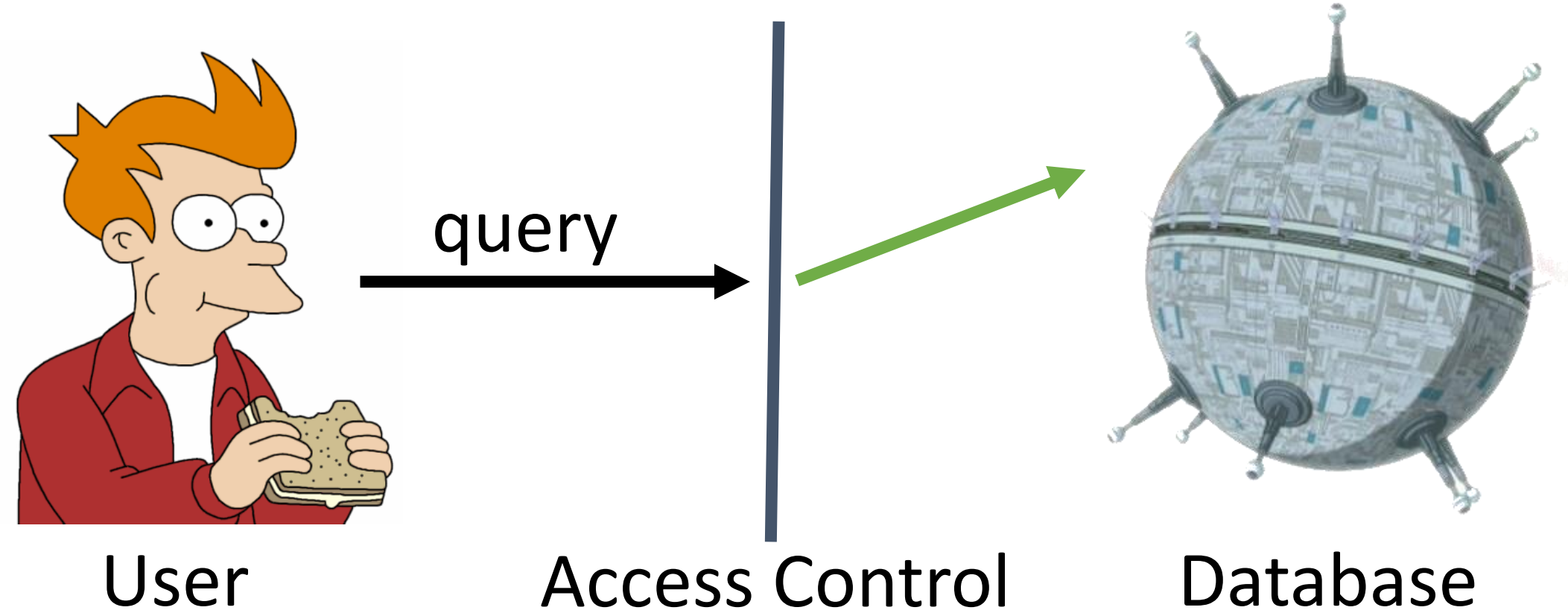
query

User

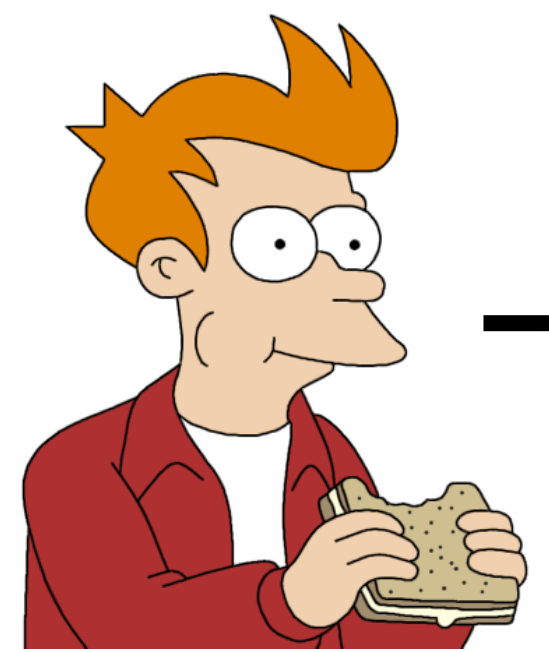
Access Control

Database

Database Access Control



Database Access Control



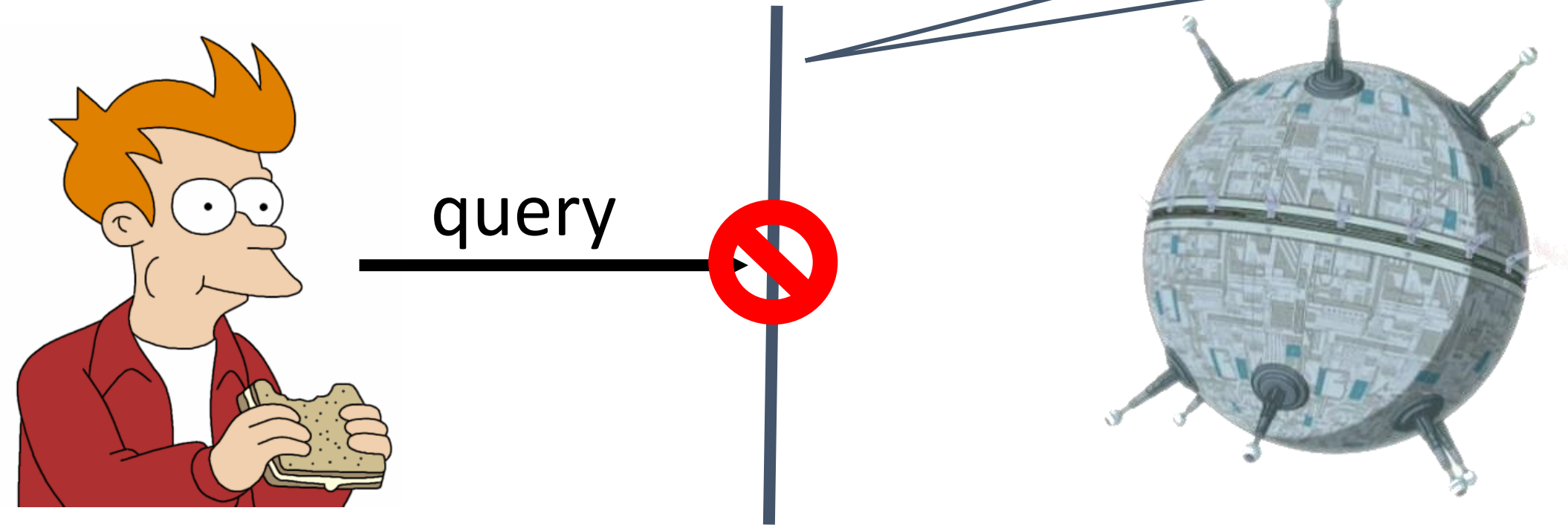
query

User

Access Control

Database

Database Access Control



Queries are programs

```
-- As admin:
CREATE TRIGGER foo AFTER INSERT ON public
  INSERT INTO public(x) VALUES (1)
  WHEN (SELECT * FROM secret) ;
```

Queries are programs

```
-- As admin:
CREATE TRIGGER foo AFTER INSERT ON public
  INSERT INTO public(x) VALUES (1)
  WHEN (SELECT * FROM secret) ;

-- As attacker
INSERT INTO public(x) VALUES (5) ;

SELECT * FROM public ;
```

Queries are programs

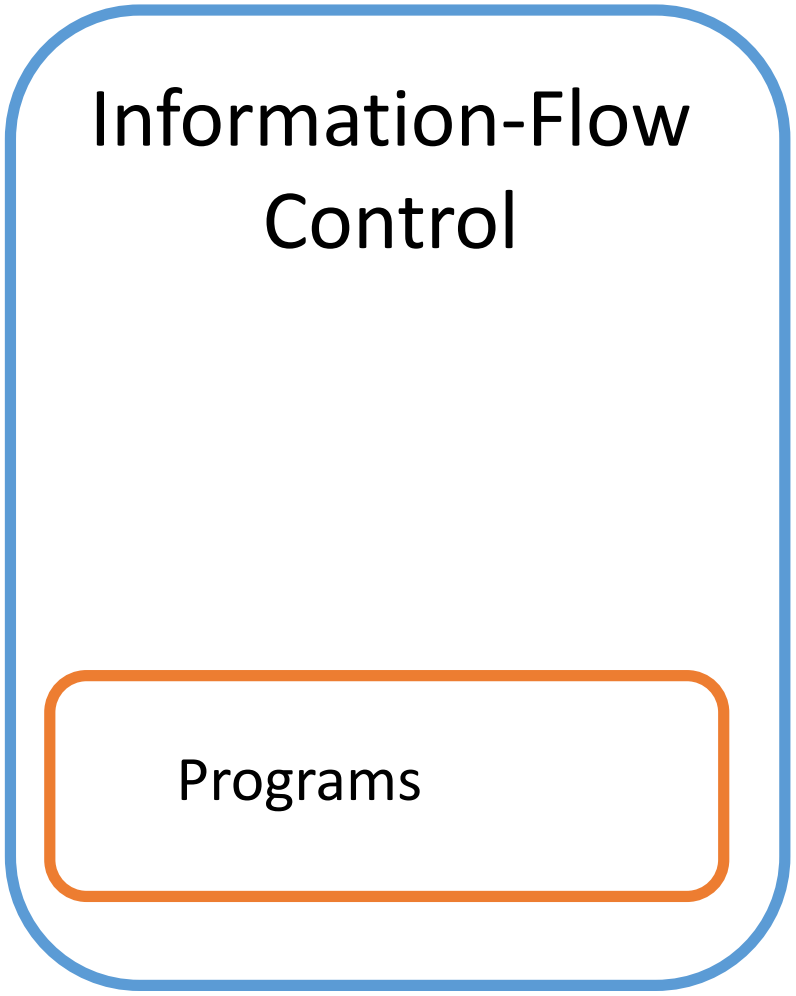
```
-- As admin:
CREATE TRIGGER foo AFTER INSERT ON public
  INSERT INTO public(x) VALUES (1)
  WHEN (SELECT * FROM secret) ;

-- As attacker
INSERT INTO public(x) VALUES (5) ;

SELECT * FROM public ;
```

Reveals if secret is empty

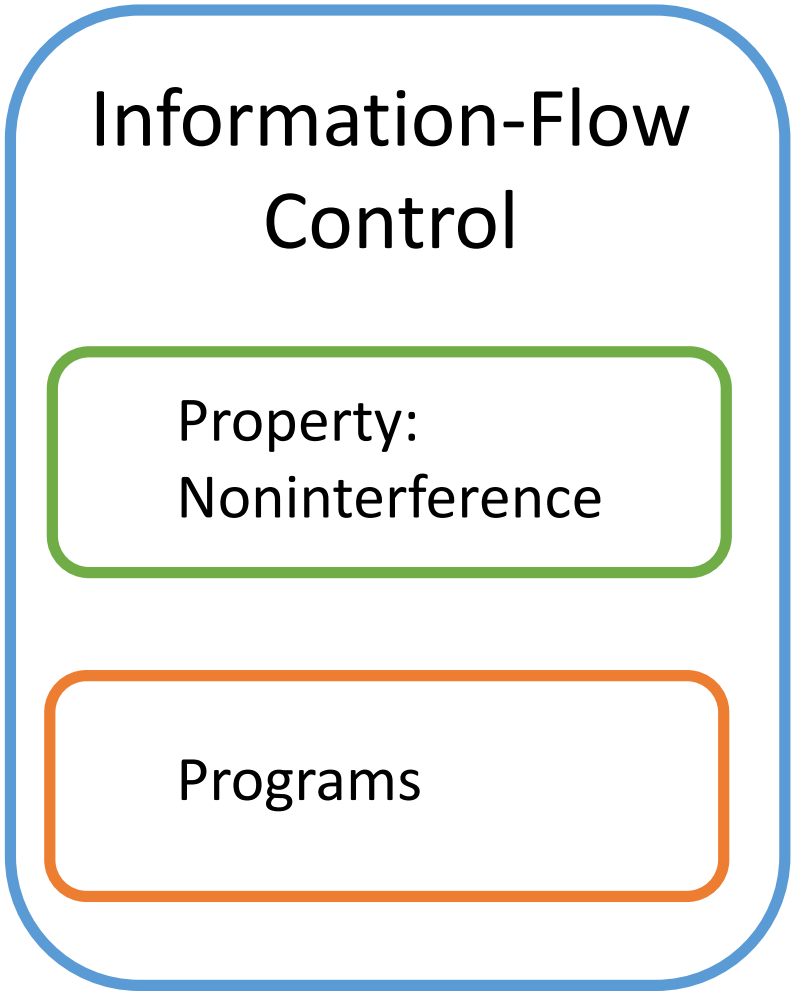
Summary

Information-Flow Control

Summary



Summary


Information-Flow Control
Property: Noninterference
Programs

Summary

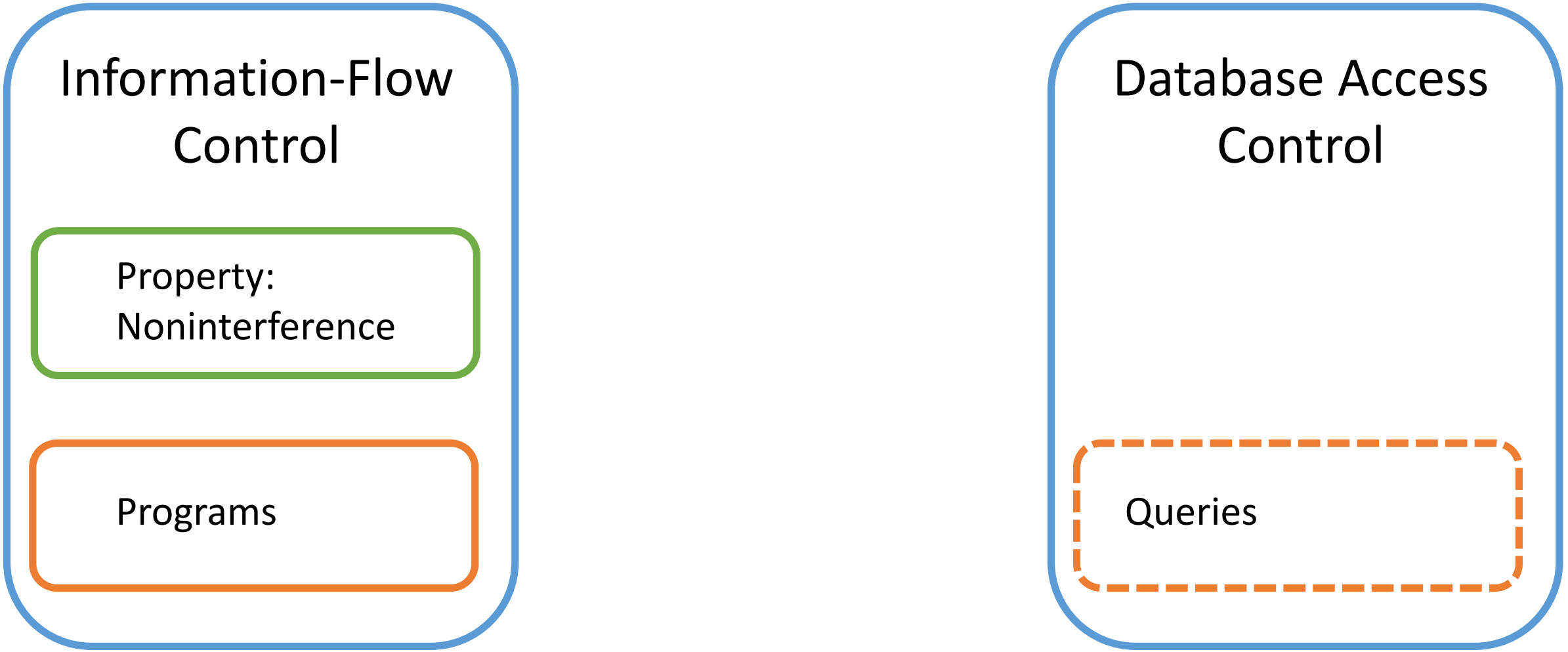
Information-Flow Control

Property: Noninterference

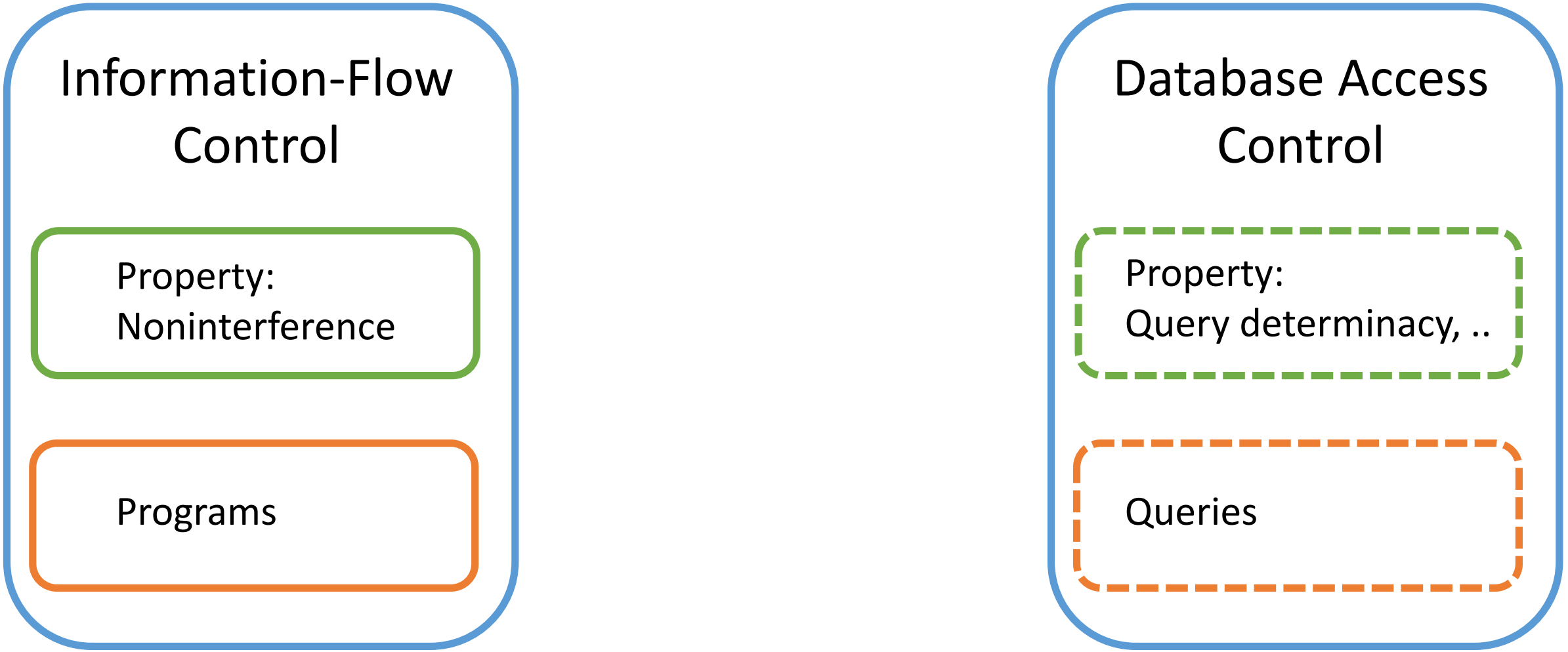
Programs

Database Access Control

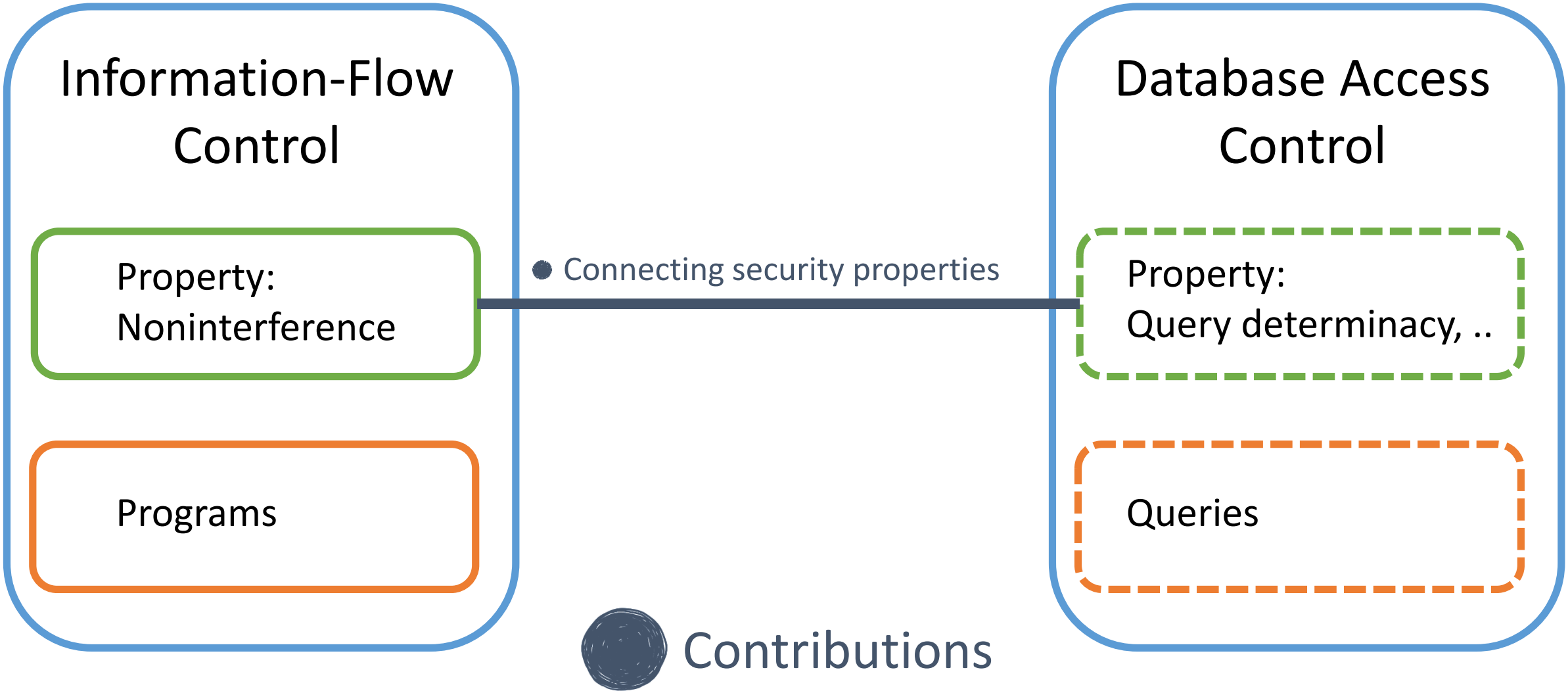
Summary


Information-Flow Control
Property: Noninterference
Programs
Database Access Control
Queries

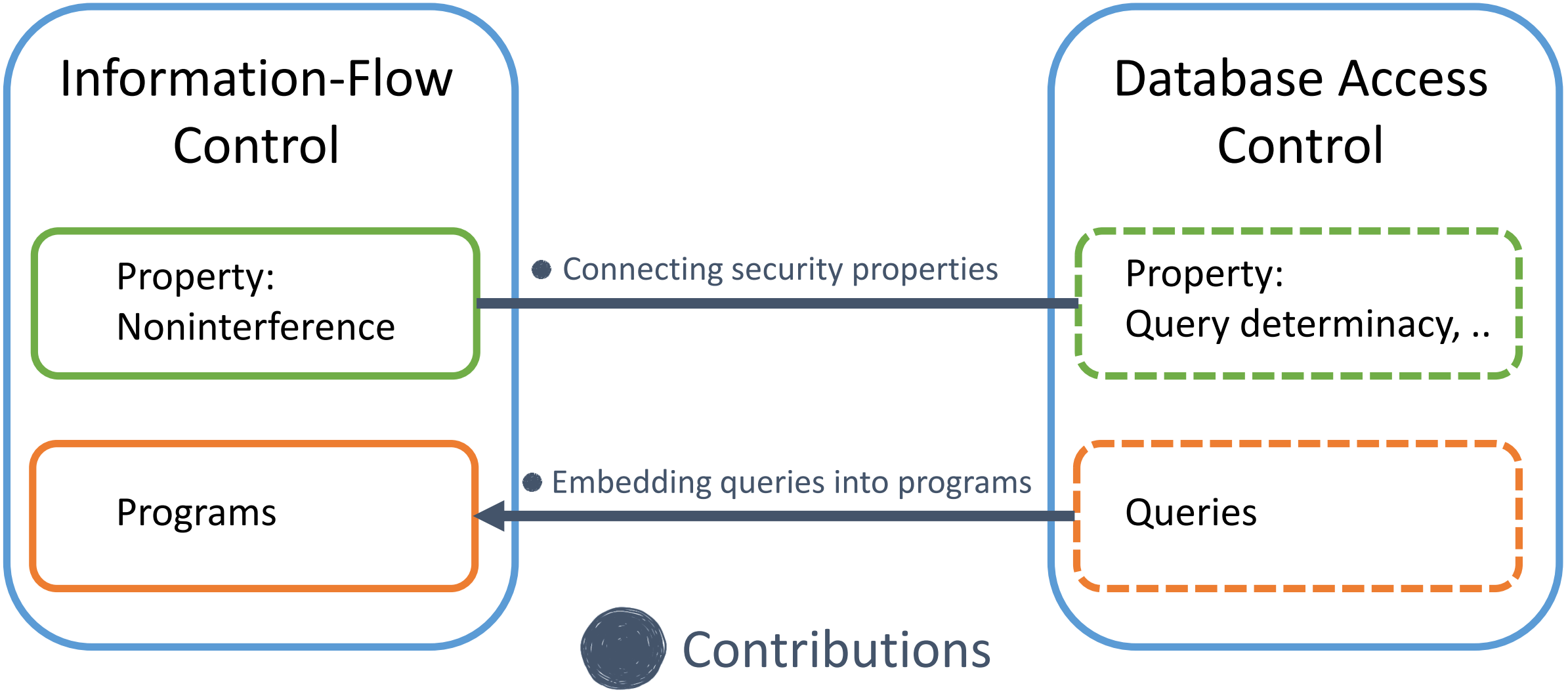
Summary


Information-Flow Control
Property: Noninterference
Programs
Database Access Control
Property: Query determinacy, ..
Queries

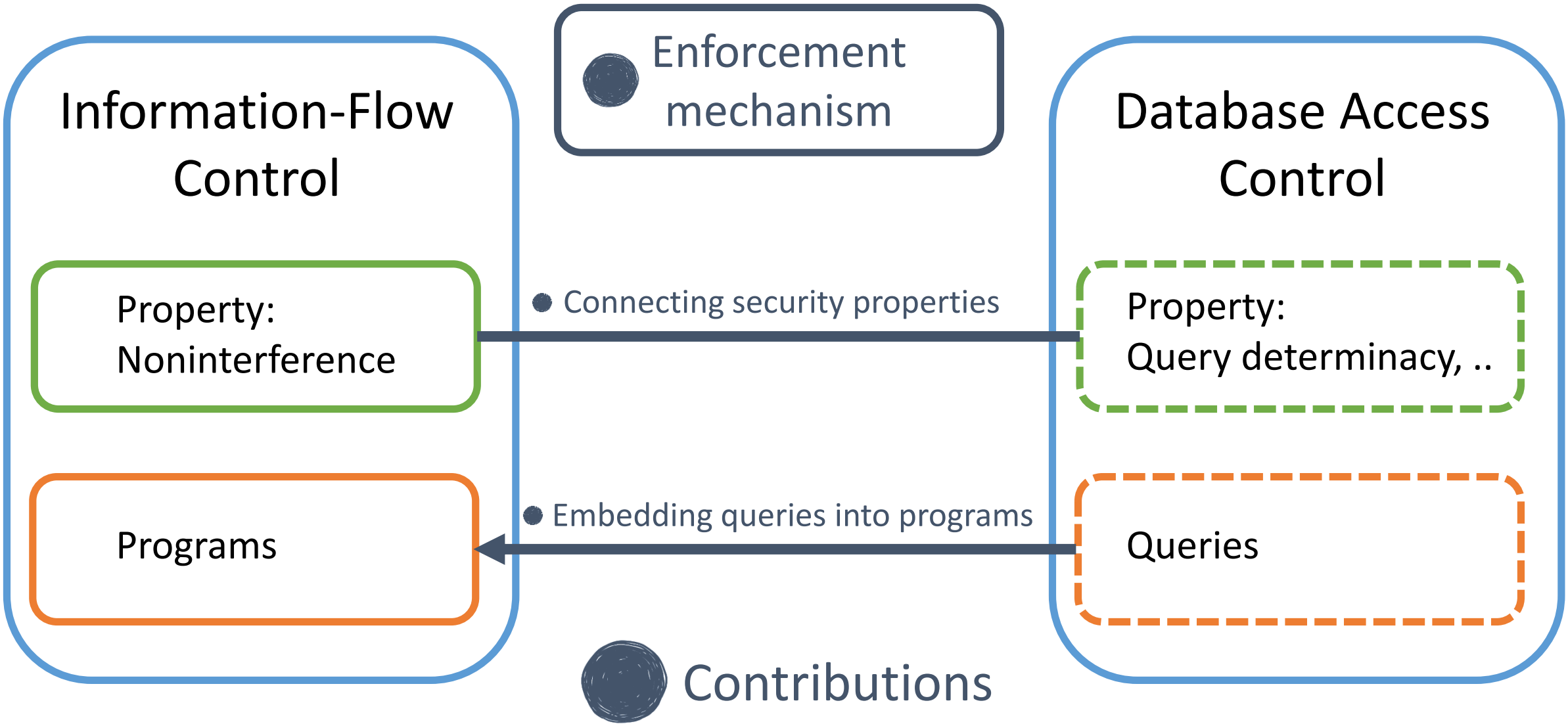
Summary


Information-Flow Control
Property: Noninterference
Programs
Connecting security properties
Database Access Control
Property: Query determinacy, ..
Queries
Contributions

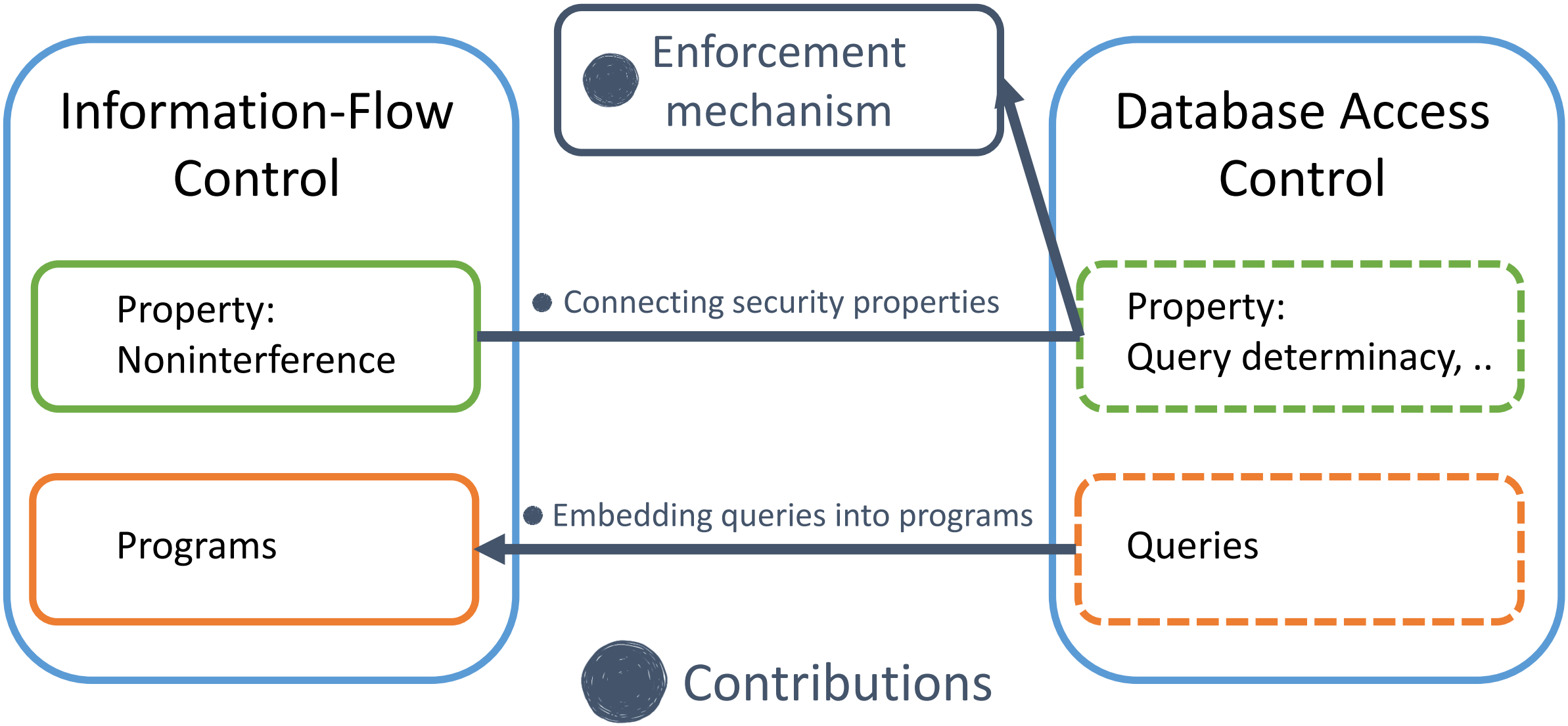
Summary


Information-Flow Control
Database Access Control
Property: Noninterference
Connecting security properties
Property: Query determinacy, ..
Programs
Embedding queries into programs
Queries
Contributions

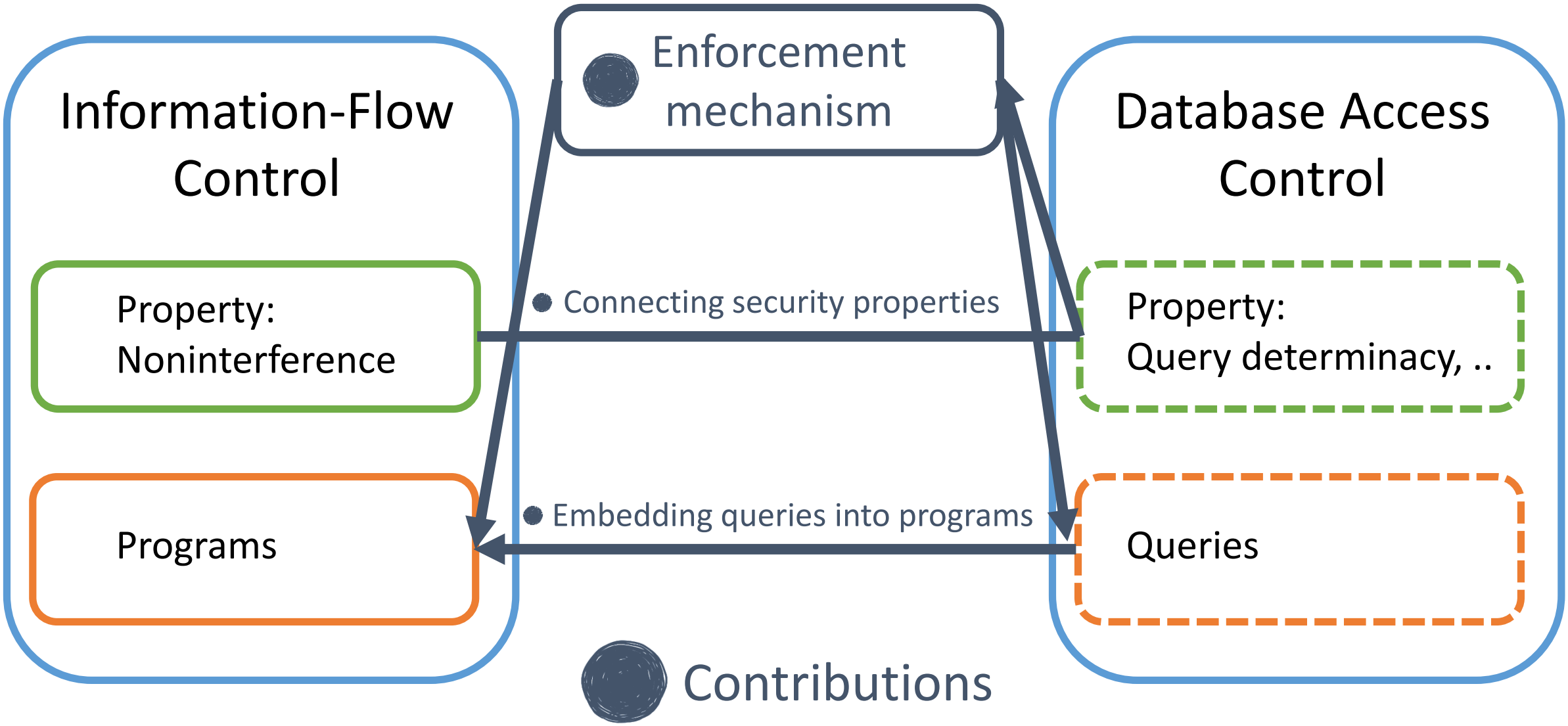
Summary


Enforcement mechanism
Information-Flow Control
Database Access Control
Property: Noninterference
Connecting security properties
Property: Query determinacy, ..
Programs
Embedding queries into programs
Queries
Contributions

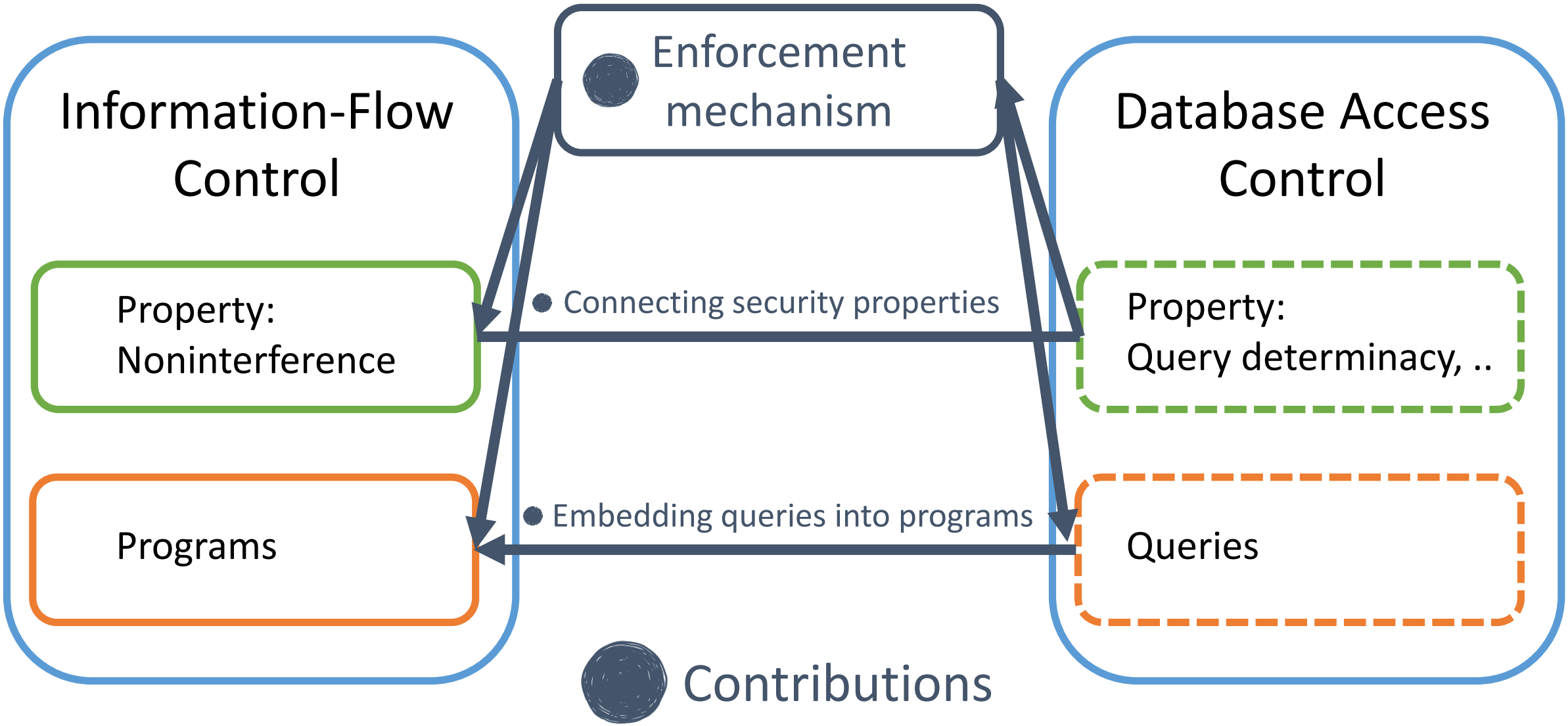
Summary


Information-Flow Control
Enforcement mechanism
Database Access Control
Property: Noninterference
Connecting security properties
Property: Query determinacy, ..
Programs
Embedding queries into programs
Queries
Contributions

Summary


Information-Flow Control
Enforcement mechanism
Database Access Control
Property: Noninterference
Connecting security properties
Property: Query determinacy, ..
Programs
Embedding queries into programs
Queries
Contributions

Summary


Information-Flow Control
Enforcement mechanism
Database Access Control
Property: Noninterference
Connecting security properties
Property: Query determinacy, ..
Programs
Embedding queries into programs
Queries
Contributions