



Fail-Secure Access Control

Petar Tsankov, Srdjan Marinovic,
Mohammad Torabi Dashti, David Basin

Institute of Information Security
ETH Zurich

Access Control + Failures

All access control systems must operate in the presence of failures



Access control in
web applications

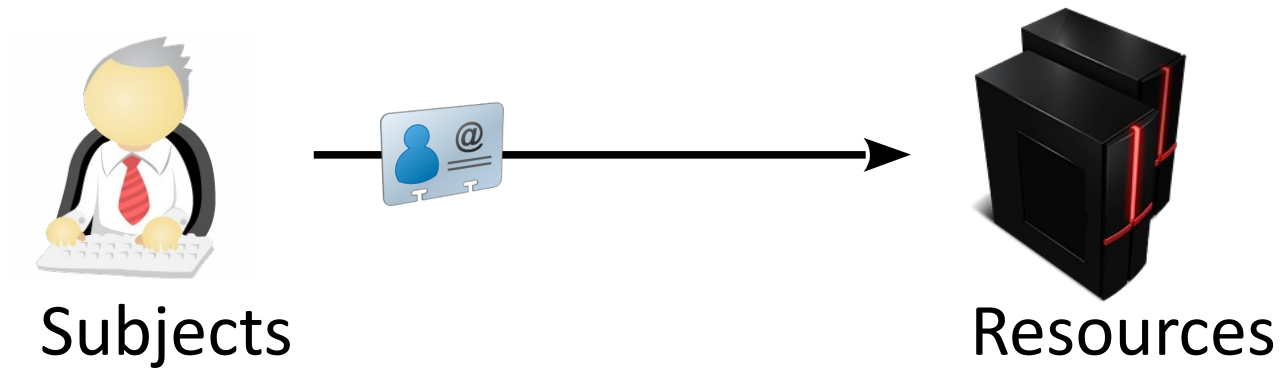


Firewalls

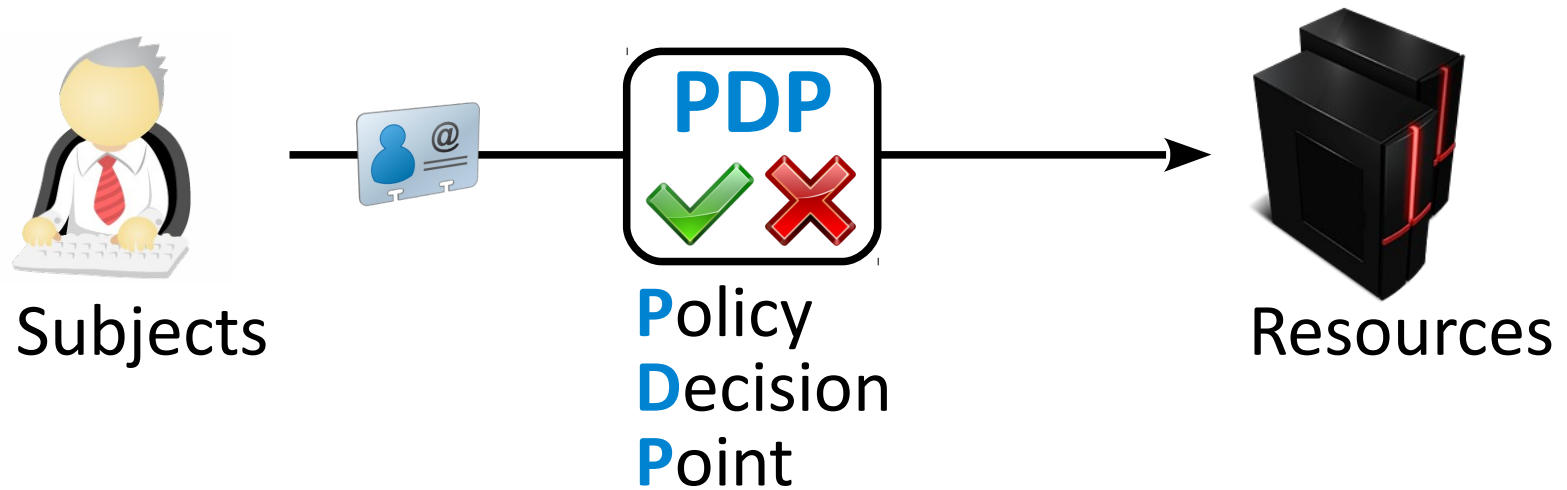


Physical access
control

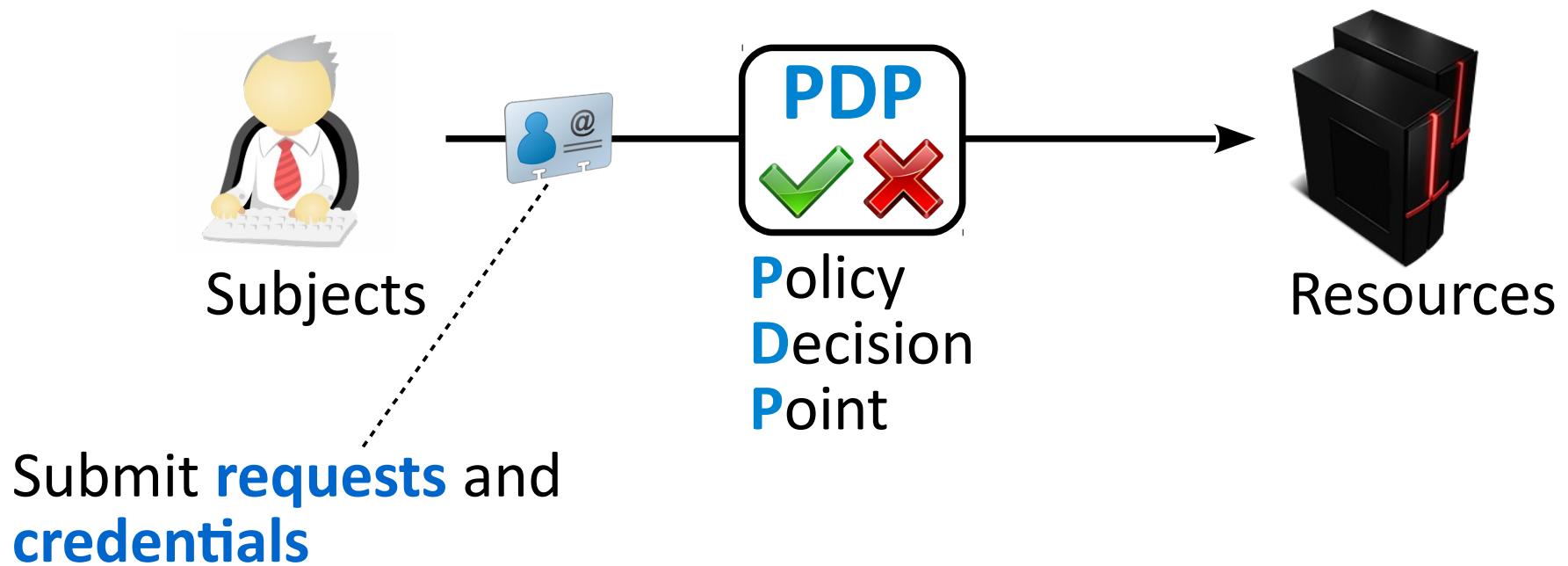
System Model



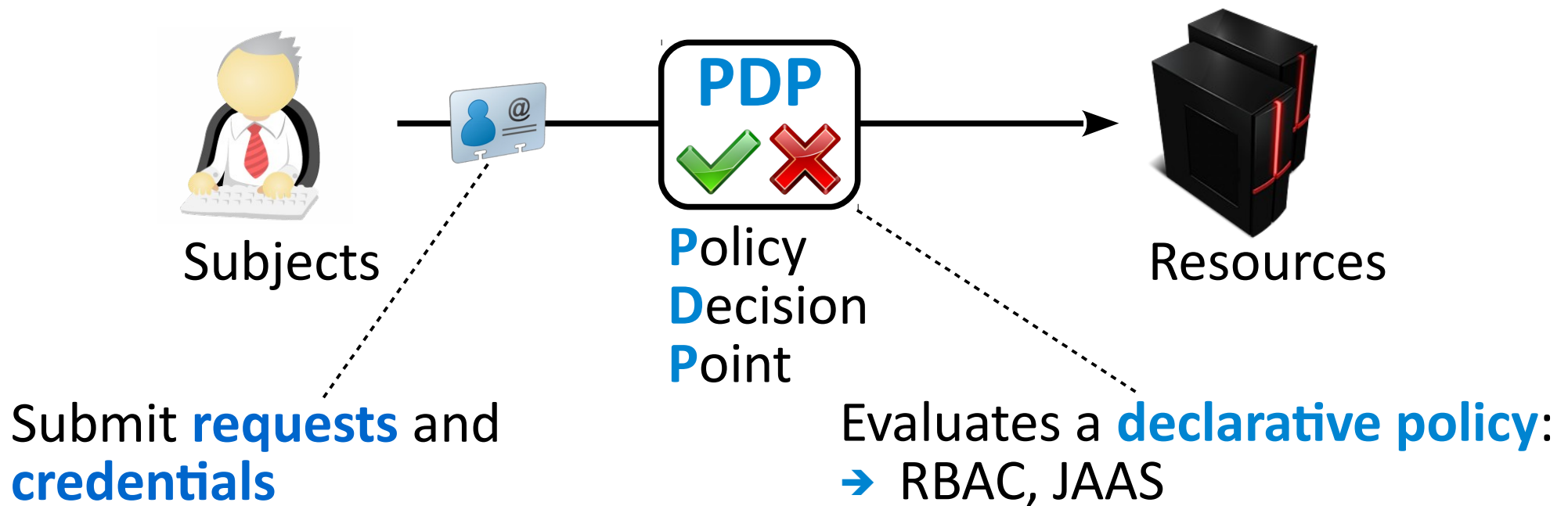
System Model



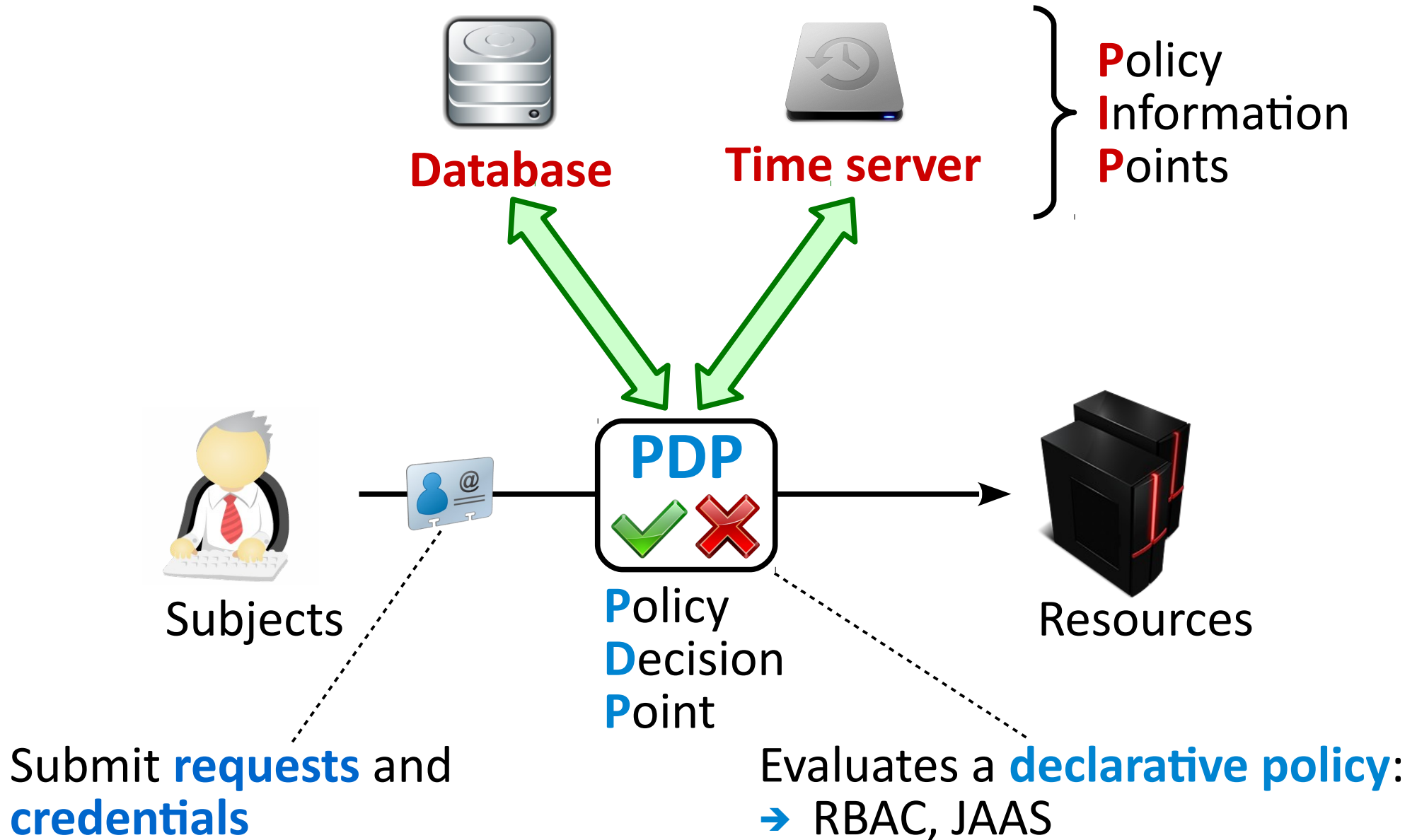
System Model



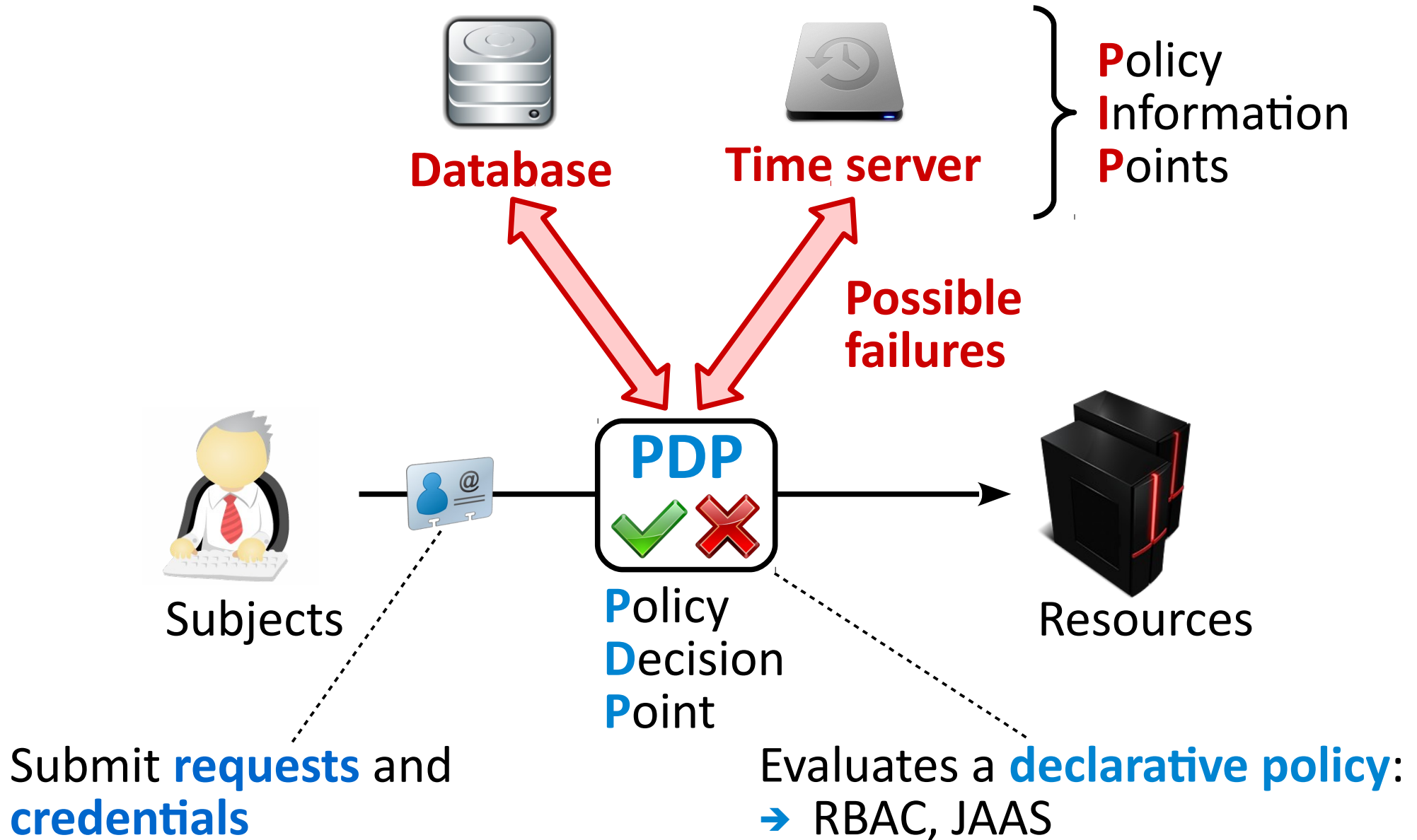
System Model



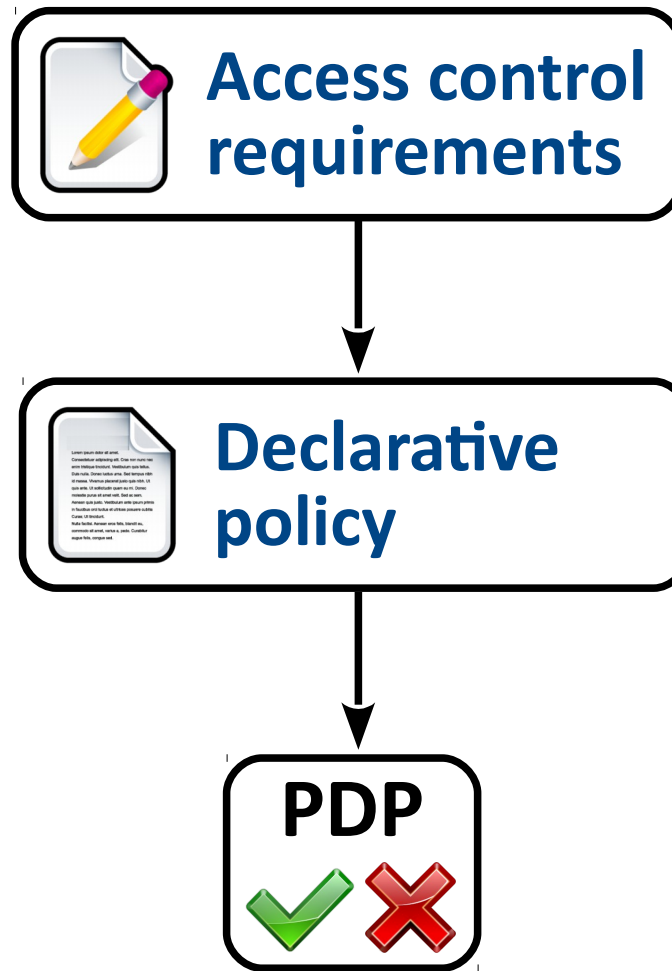
System Model



System Model

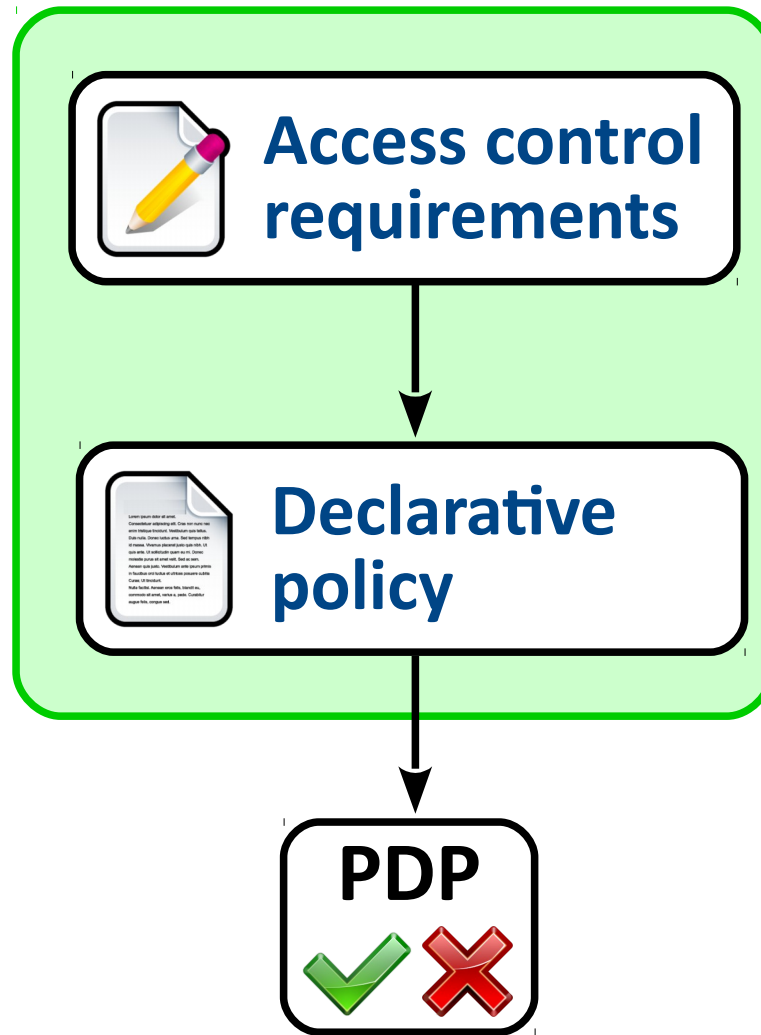


The Problem with Failure Handling



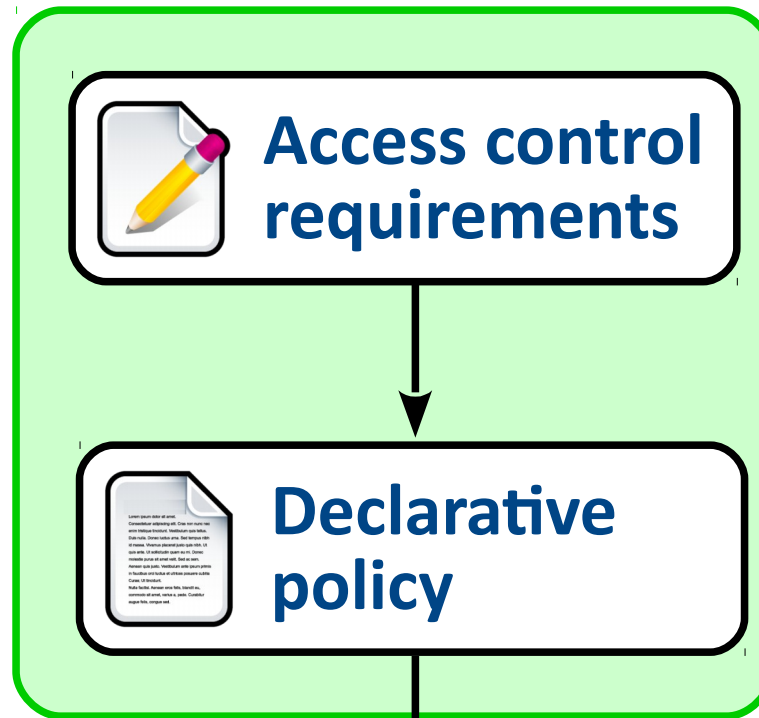
The Problem with Failure Handling

Policy Analysis



The Problem with Failure Handling

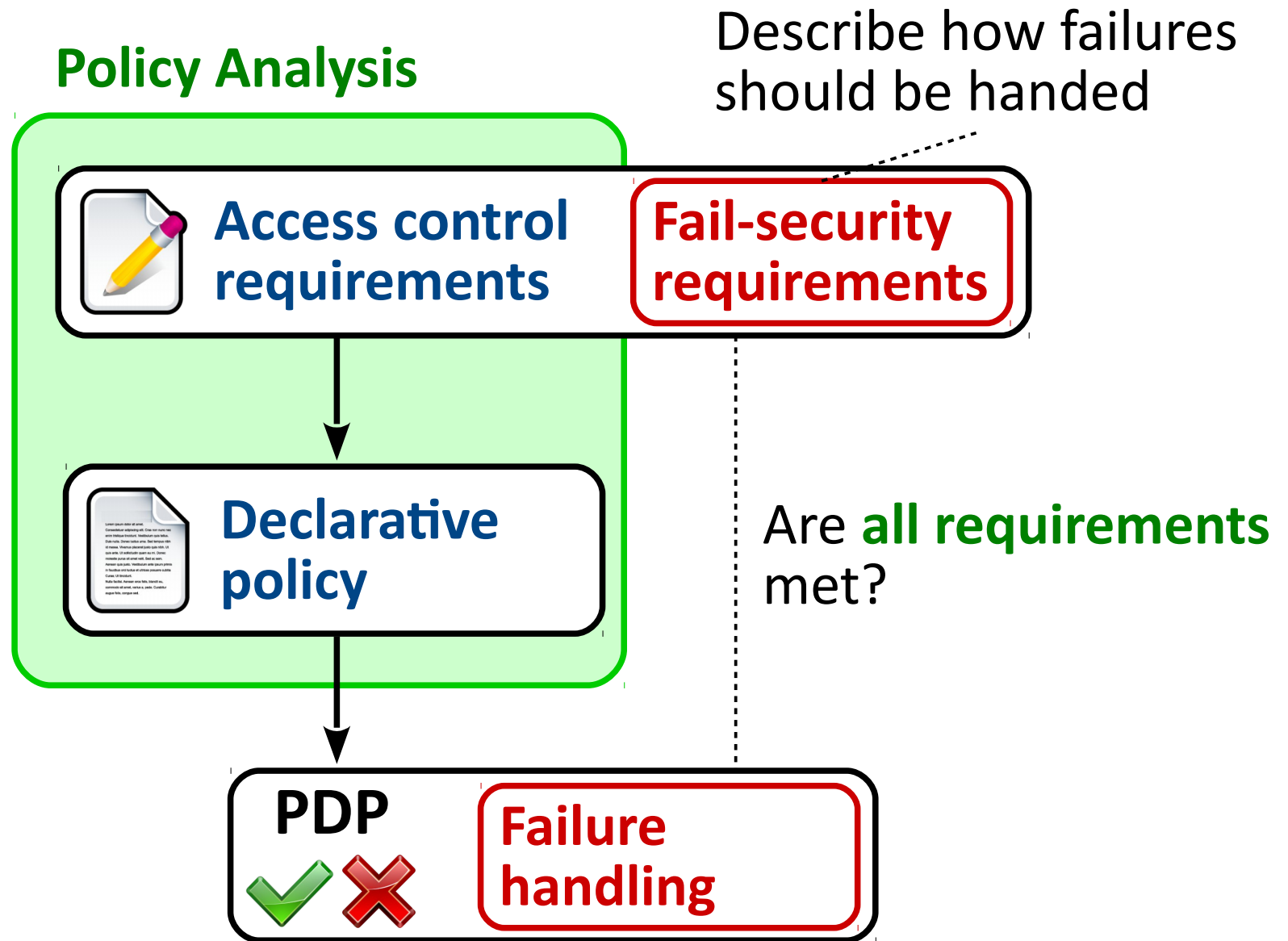
Policy Analysis



Affects how access decisions are made

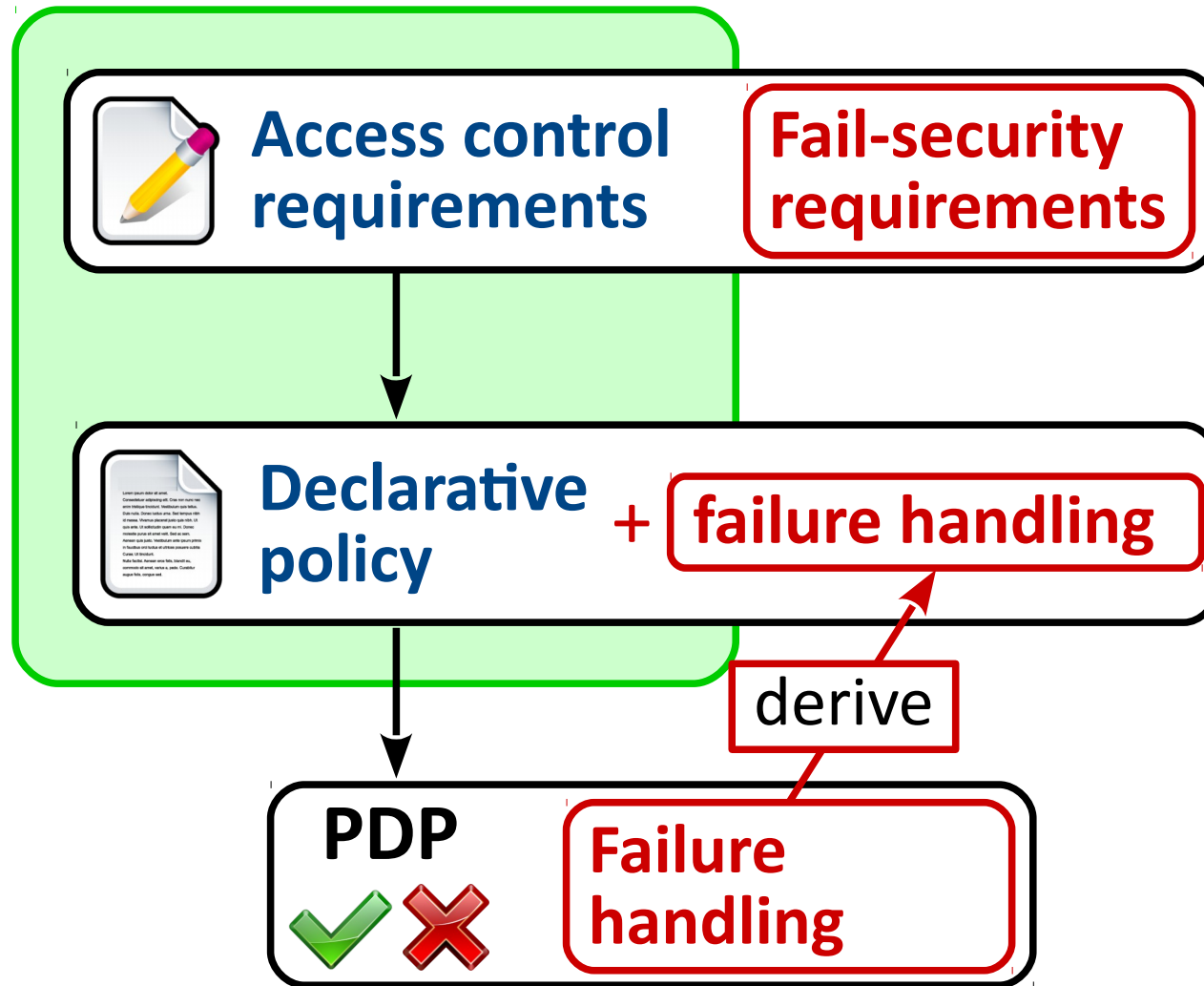


The Problem with Failure Handling

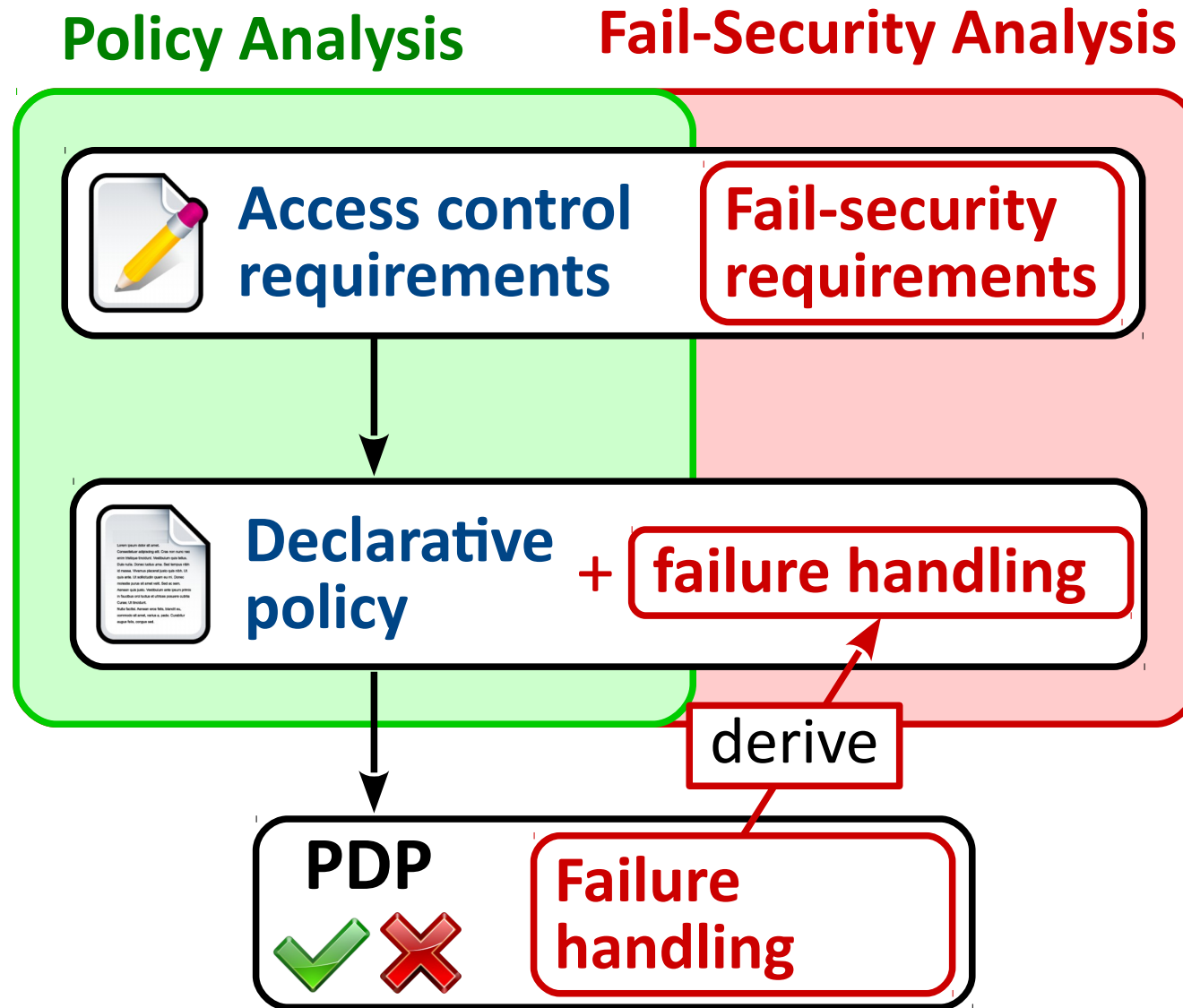


The Problem with Failure Handling

Policy Analysis



The Problem with Failure Handling



Contributions



Defining attacker model



**Specifying access policy
with failure handling**

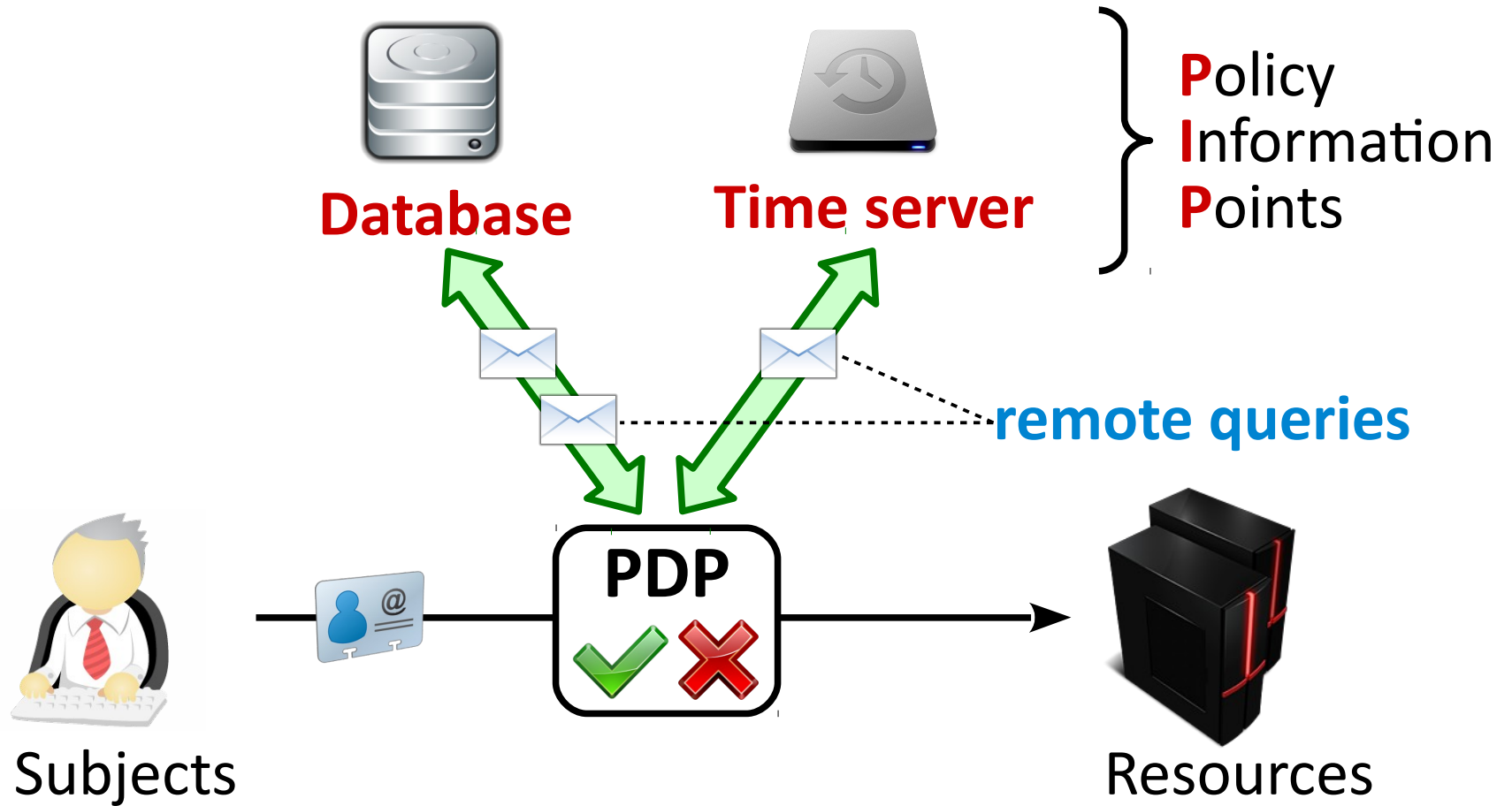


**Verifying fail-security
requirements**

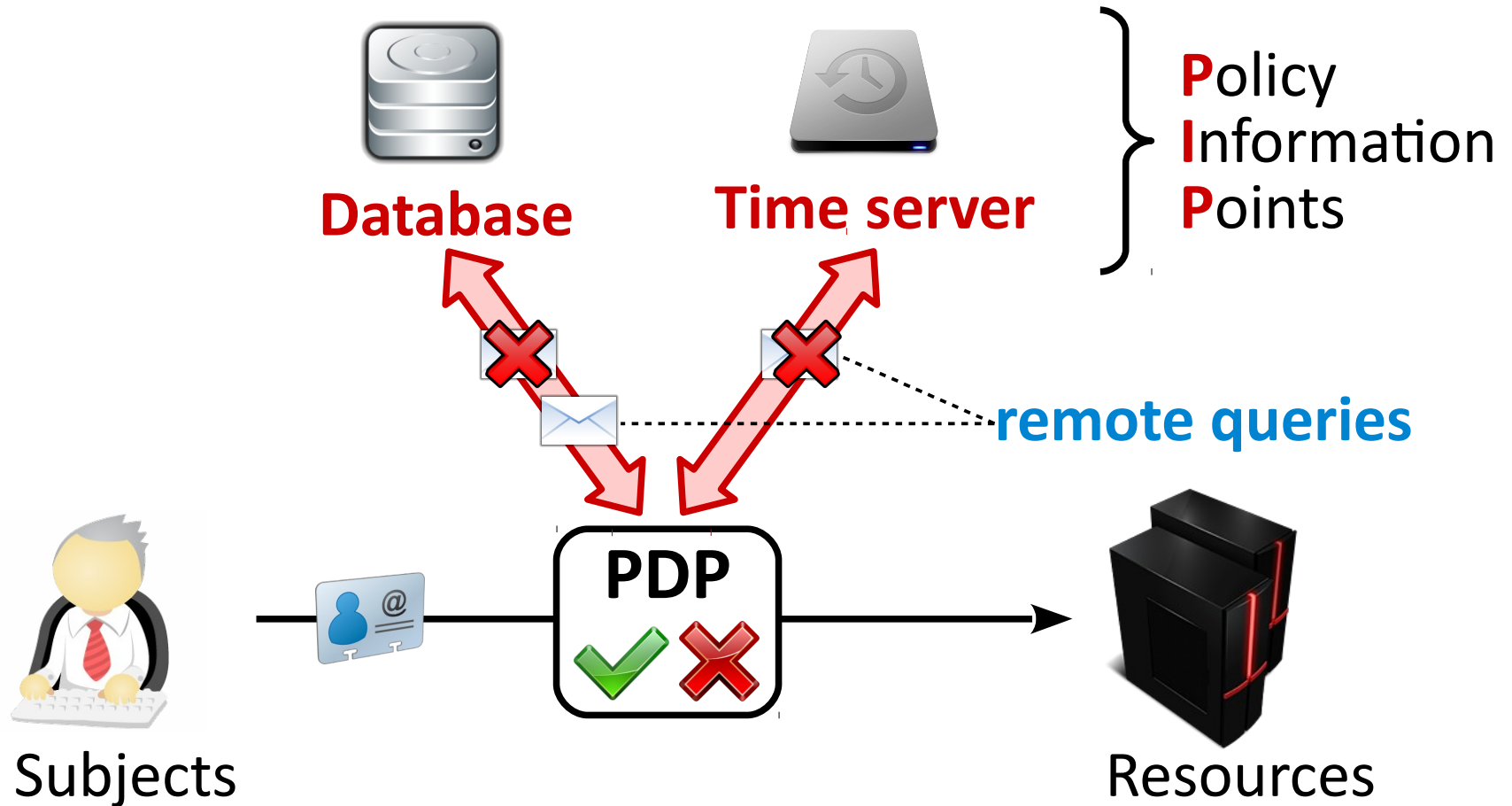


Attacker Model

System and Attacker Model



Attacker Model



The attacker can selectively cause any **remote query** to fail



Contributions



Defining attacker model



**Specifying access policy
with failure handling**

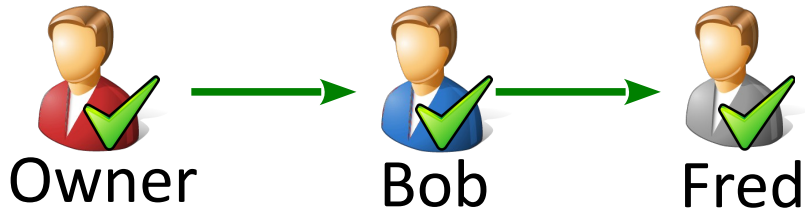


**Verifying fail-security
requirements**

Running Example

Running Example

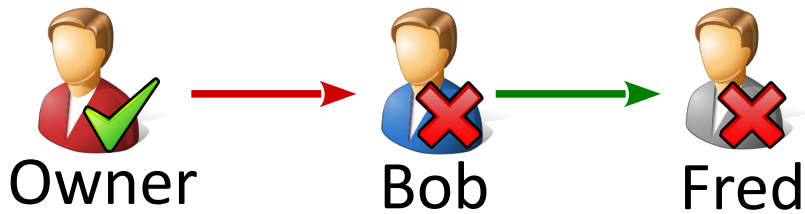
Authorizations in Grids



→ Valid delegation

Running Example

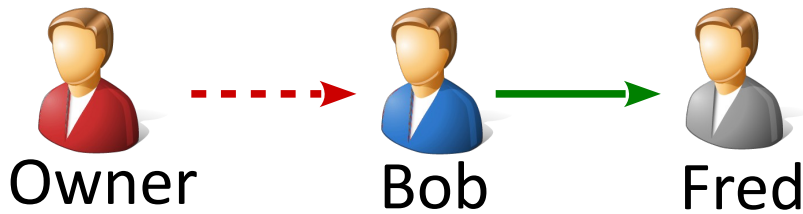
Authorizations in Grids



→ Valid delegation
→ Revoked delegation

Running Example

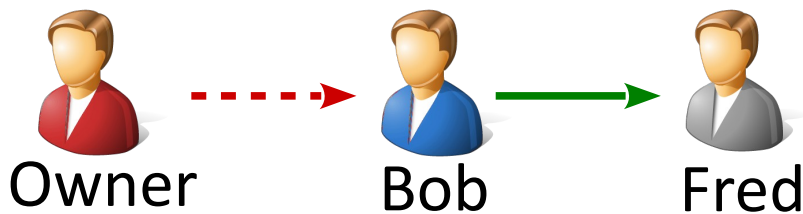
Authorizations in Grids



- Valid delegation
- Revoked delegation
- - -> The PDP fails to check if the delegation is revoked

Running Example

Authorizations in Grids



- Valid delegation
- Revoked delegation
- The PDP fails to check if the delegation is revoked

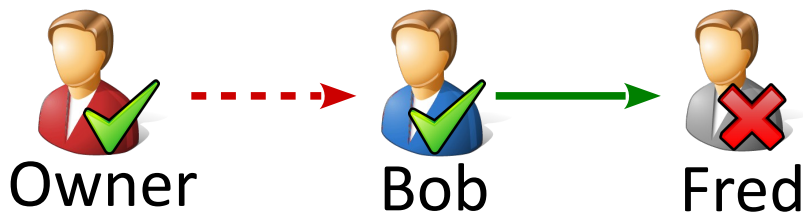
Fail-security requirement



If the PDP fails to check whether a delegation chain is valid, grant access iff the subject is a direct delegate

Running Example

Authorizations in Grids



- Valid delegation
- Revoked delegation
- - -> The PDP fails to check if the delegation is revoked

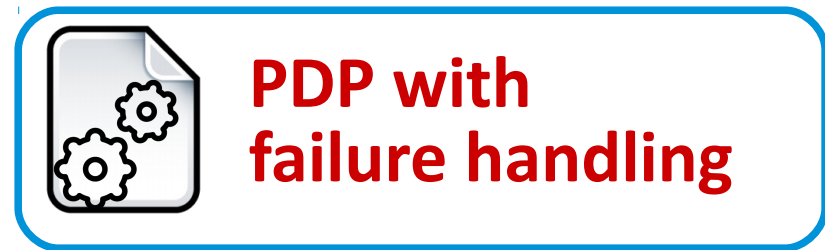
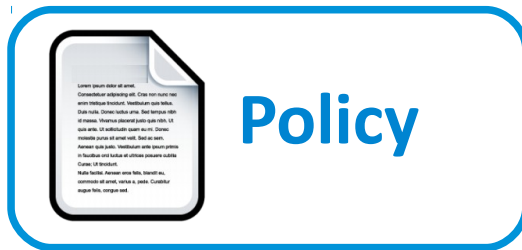
Fail-security requirement



If the PDP fails to check whether a delegation chain is valid, grant access iff the subject is a direct delegate

Building a Grid PDP

The **policy** and **the failure handling** are split



Building a Grid PDP

The **policy** and **the failure handling** are split

Policy

```
auth(X) :- owner(X)
auth(X) :- auth(Y), del(Y,X)
```

PDP with failure handling

```
auth(User user, List delegations):
    policyEngine.add(Policy)
    for del in delegations:
        try:
            if server.isNotRevoked(del):
                policyEngine.add(del)
        catch (Exception e):
            if del.issuer == owner:
                policyEngine.add(del)
    return policyEngine.auth(user)
```

Building a Grid PDP

The **policy** and **the failure handling** are split

Policy

```
auth(X) :- owner(X)
auth(X) :- auth(Y), del(Y,X)
```

PDP with failure handling

```
auth(User user, List delegations):
  policyEngine.add(Policy)
  for del in delegations:
    try:
      if server.isNotRevoked(del):
        policyEngine.add(del)
    catch (Exception e):
      if del.issuer == owner:
        policyEngine.add(del)
  return policyEngine.auth(user)
```

**Is this failure
handler correct?**

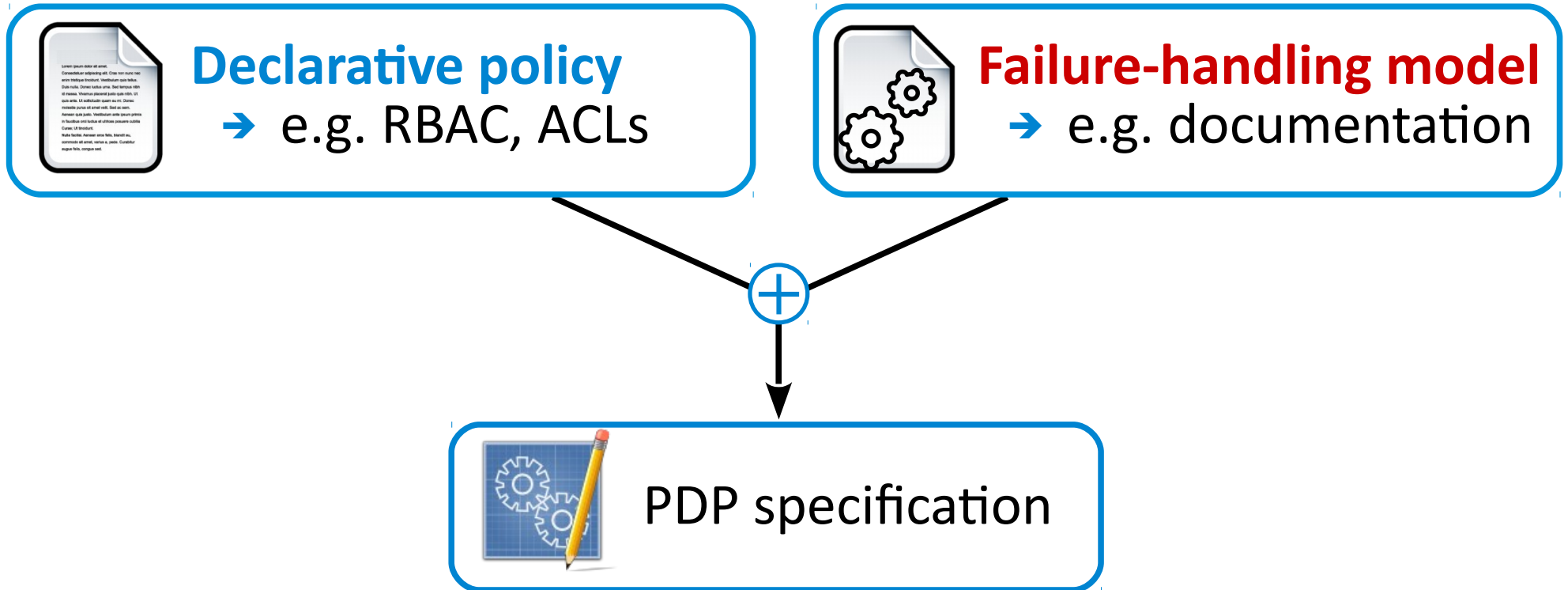


Does the PDP (**policy** + **failure handling**)
meet the **fail-security requirement**?

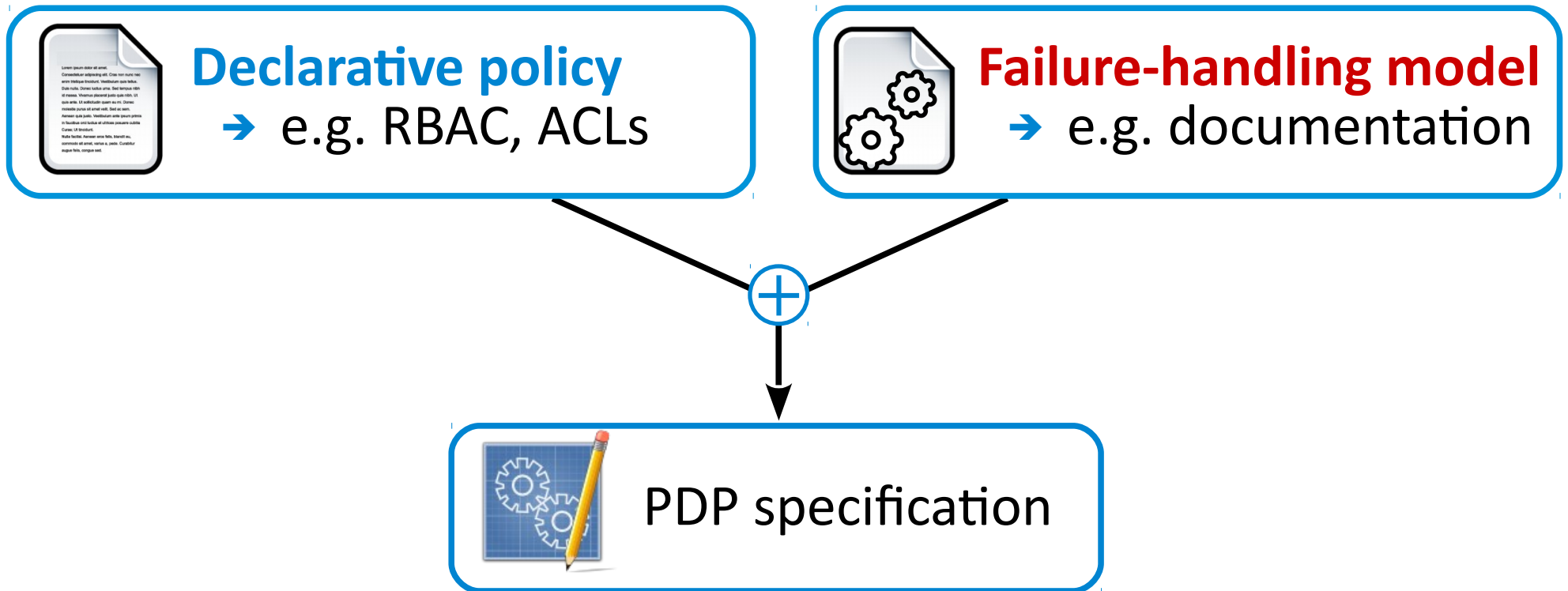


Specifying Access Control With Failure Handling

PDP Specification



PDP Specification



How to write this?

BelLog

A many-valued logic-programming language



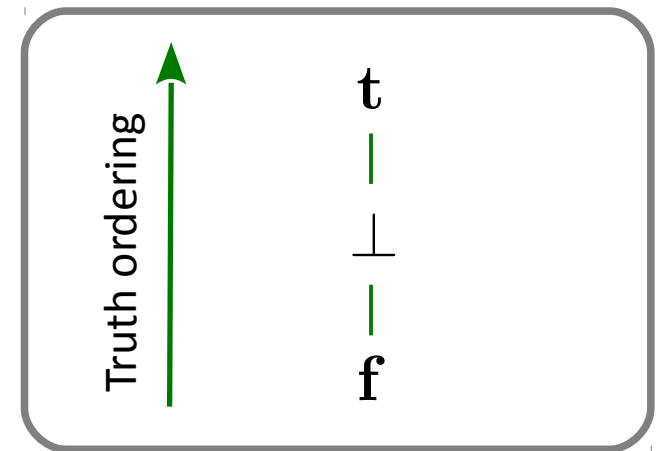
Can encode the state-of-the-art policy languages



Can encode failure handling:

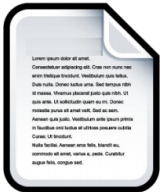
- **Denote failures** with $\perp$
- Derive failure-handling operators

Truth space



BelLog

A many-valued logic-programming language

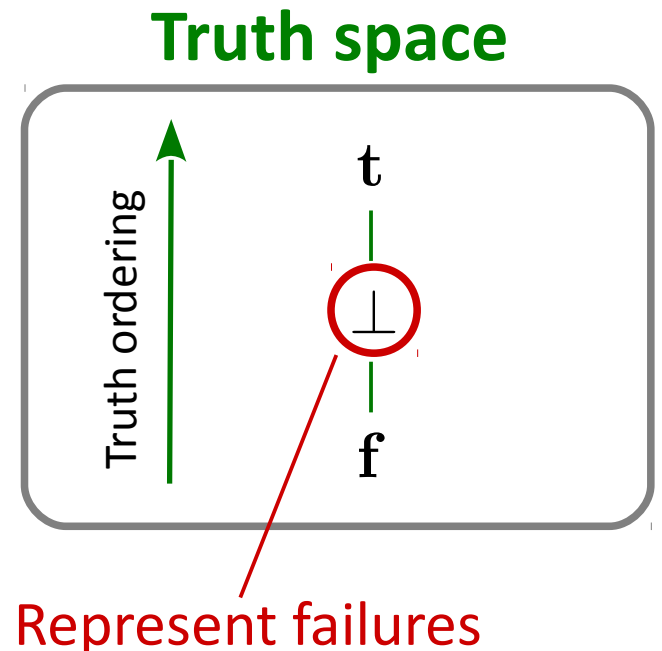


Can encode the state-of-the-art policy languages



Can encode failure handling:

- **Denote failures** with $\perp$
- Derive failure-handling operators



Specifying the Running Example

Policy

```
pol(X) :- owner(X)
pol(X) :- pol(Y), valid-del(Y,X)
```

to BelLog

```
pol(X) ← owner(X)
pol(X) ← pol(Y) ∧ valid-del(Y, X)
```

Failure handling

```
try:
    ...
catch (Exception e)
    if del.issuer == owner:
        policyEngine.add(del)
```

to BelLog

```
valid-del(X, Y) ← (del(X, Y) ► owner(X))
```

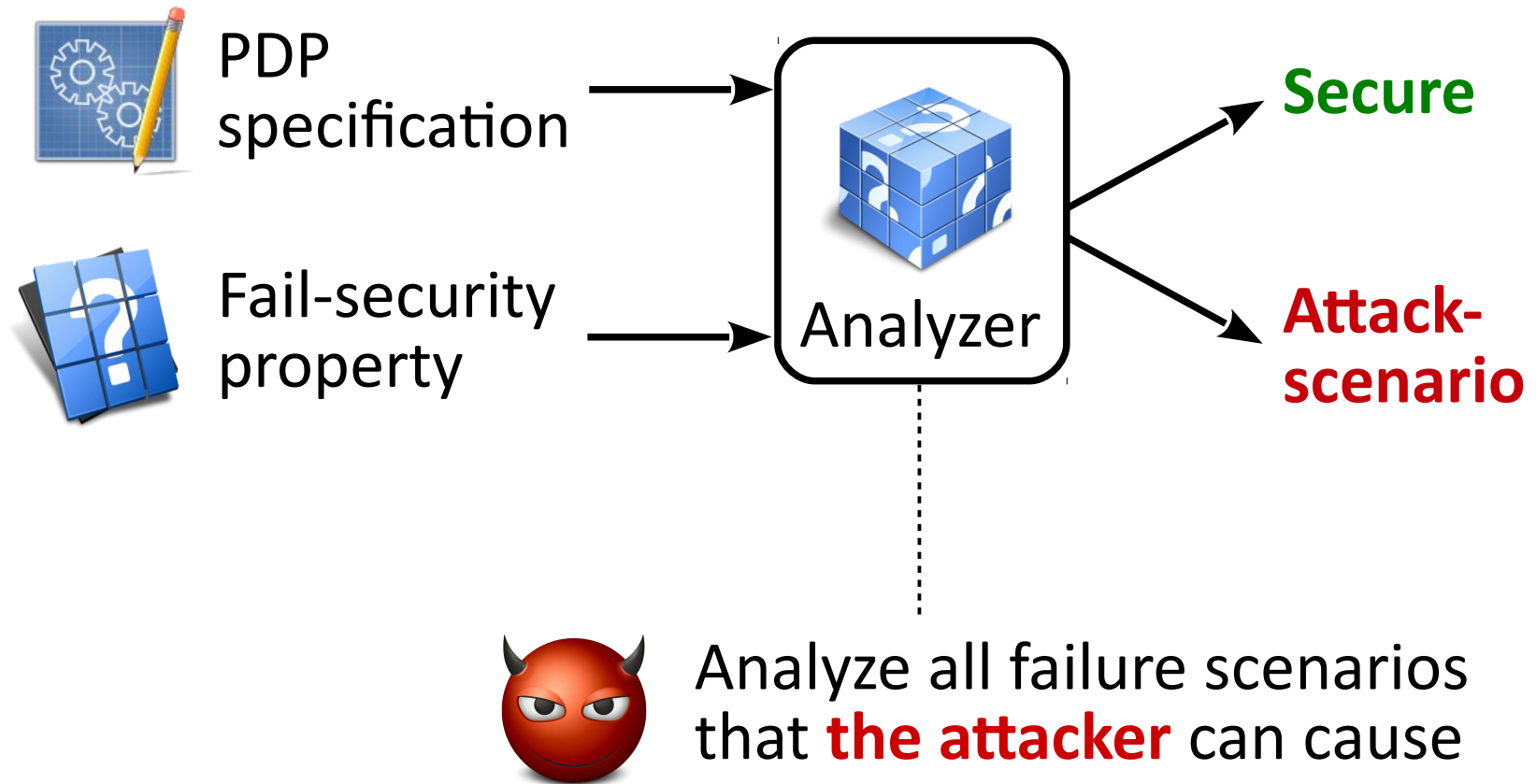
Common failure-handling idioms:

→ Catch → Fallback → Propagate

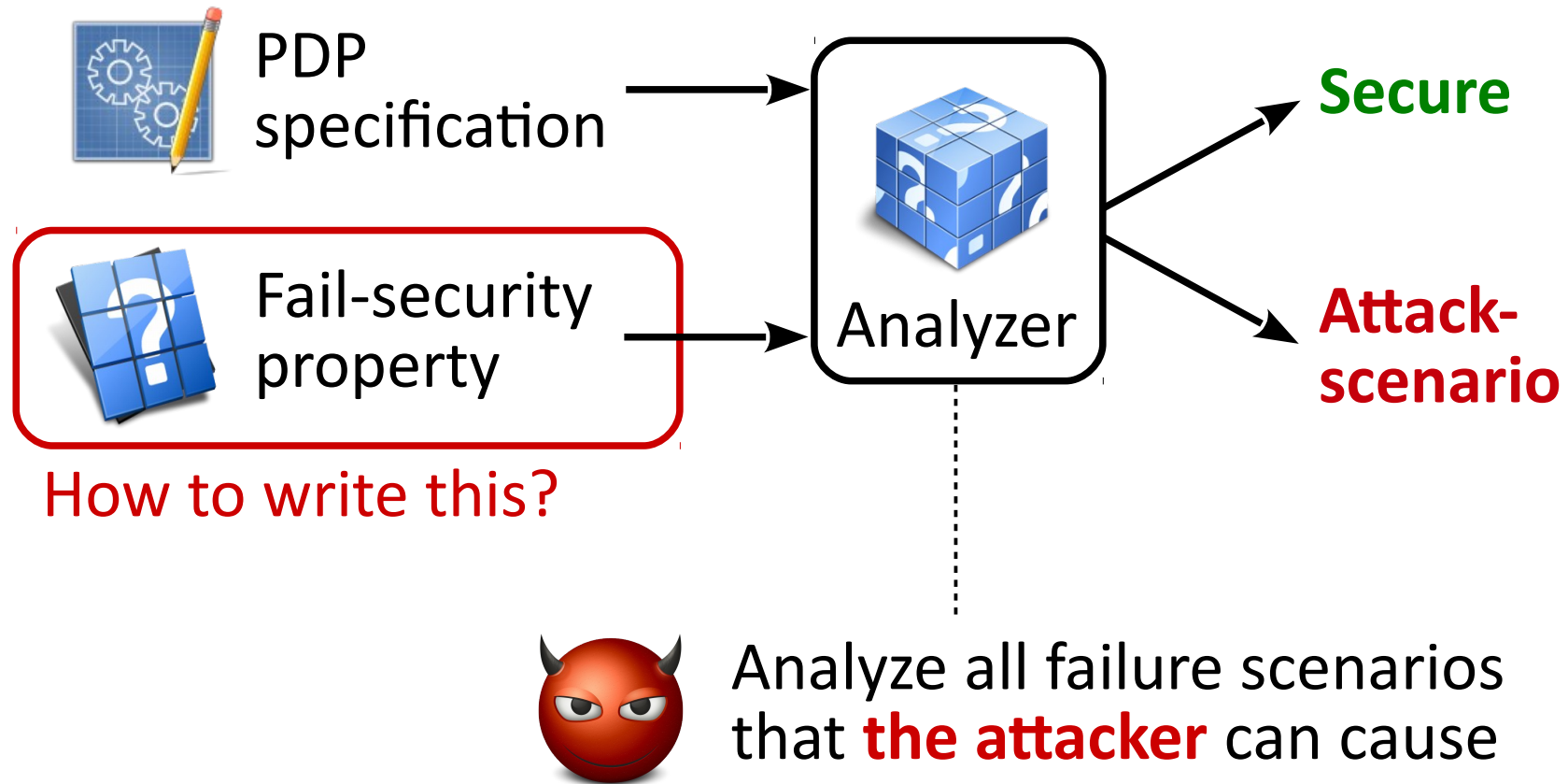


Verifying Fail-Security Requirements

Verifying Fail-Security Properties



Verifying Fail-Security Properties



Fail-Security Properties

Fail-security requirement

If the PDP fails to check whether a delegation chain is valid, grant access iff the subject is a direct delegate

Fail-Security Properties

Fail-security requirement

If the PDP fails to check whether a delegation chain is valid, grant access iff the subject is a direct delegate

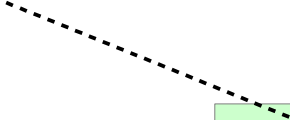
$$\varphi \rightarrow (S_{\text{pdp}} \Leftrightarrow S)$$

Fail-Security Properties

Fail-security requirement

If the PDP fails to check whether a delegation chain is valid, grant access iff the subject is a direct delegate

A condition that defines
failure-scenarios


$$\varphi \rightarrow (S_{\text{pdp}} \Leftrightarrow S)$$

Fail-Security Properties

Fail-security requirement

If the PDP fails to check whether a delegation chain is valid, grant access iff the subject is a direct delegate

A condition that defines
failure-scenarios

$$\varphi \rightarrow (S_{\text{pdp}} \Leftrightarrow S)$$

PDP specification

Fail-Security Properties

Fail-security requirement

If the PDP fails to check whether a delegation chain is valid,
grant access iff the subject is a direct delegate

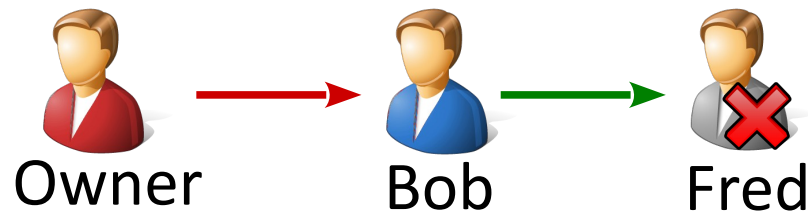
A condition that defines
failure-scenarios

PDP behavior described by
the fail-security requirement



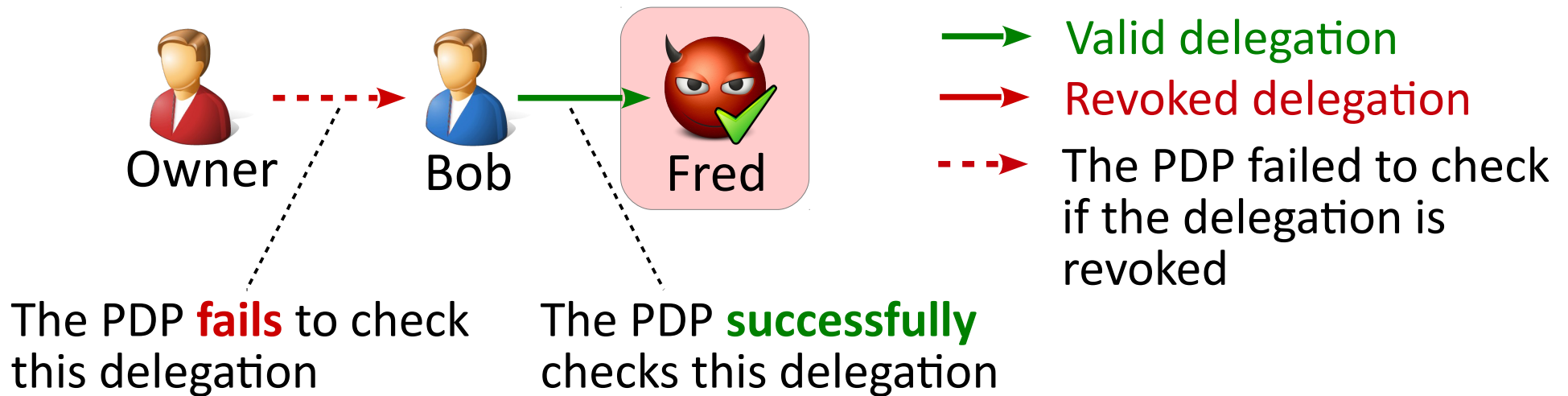
PDP specification

Running Example Attack

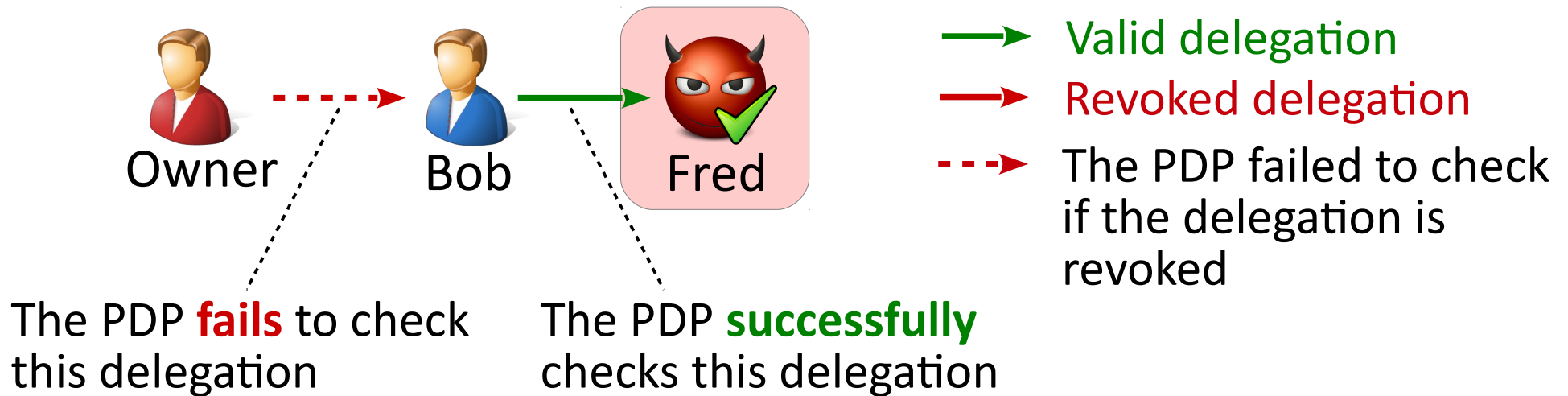


- Valid delegation
- Revoked delegation
- - - → The PDP failed to check if the delegation is revoked

Running Example Attack



Running Example Attack



```
try:  
    ...  
catch (Exception e)  
    if del.issuer == owner:  
        policyEngine.add(del)
```

**Incorrect
Failure
Handler**

What I Skipped Today



- Failure-handling idioms
- Algorithmic complexity
- Tools:
 - PDP Simulator (<http://bellog.org>)
 - PDP Analyzer (<http://goo.gl/JzKKxk>)
- More examples

Summary of Contributions

Summary of Contributions



Raised the problem of failure handling in access control

Summary of Contributions



Raised the problem of failure handling in access control



Defined an attacker that can selectively cause failures

Summary of Contributions



Raised the problem of failure handling in access control



Defined an attacker that can selectively cause failures



Defined idioms for specifying PDPs with failure handling

Summary of Contributions



Raised the problem of failure handling in access control



Defined an attacker that can selectively cause failures



Defined idioms for specifying PDPs with failure handling



Developed tools for automated analysis of fail-security properties