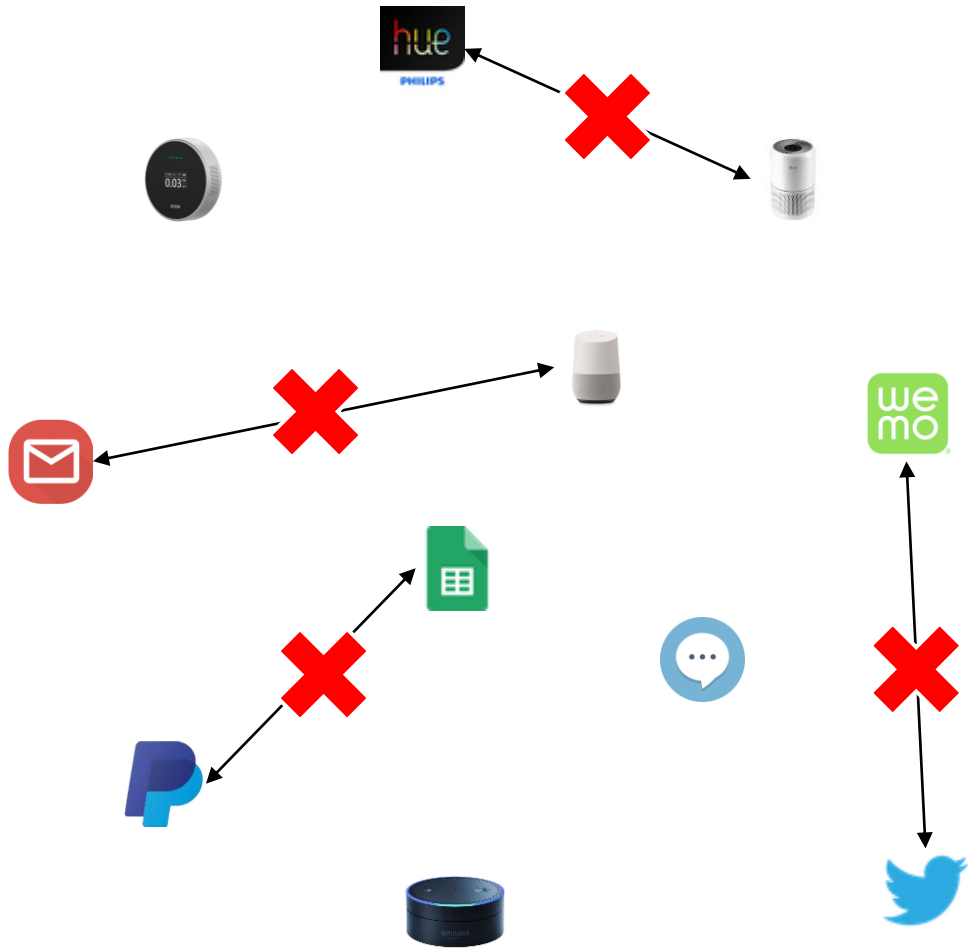


Practical Data Access Minimization in Trigger-Action Platforms

Yunang Chen, Mohannad Alhanahnah,
Andrei Sabelfeld, Rahul Chatterjee, Earlence Fernandes*

*work done while at UW-Madison

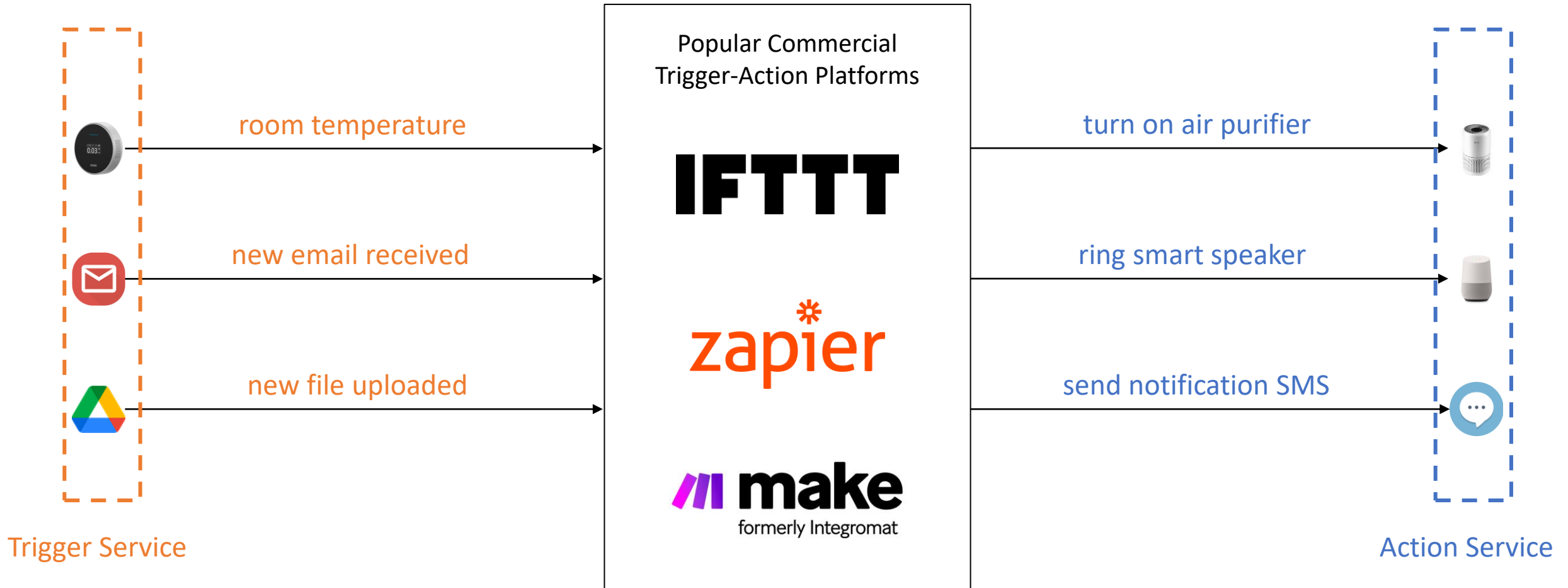




Working across different services is difficult...



Trigger-Action Platforms (TAPs) empower automation rules



Overview

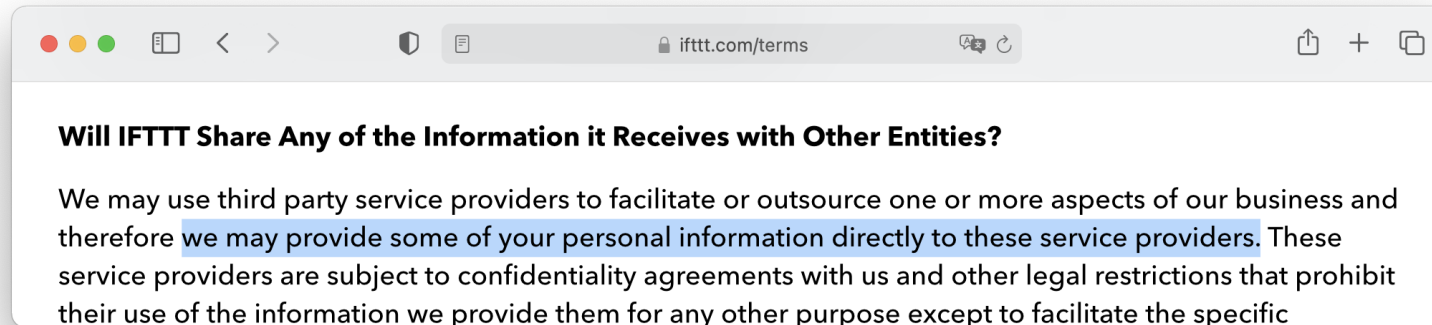
- Privacy concerns in **Trigger-Action Platforms (TAPs)**
 - Token-level Overprivilege
 - Attribute-level Overprivilege
- Design of minTAP -- leveraging language-based techniques to track dependencies
- Evaluation on current TAP -- privacy benefits of deploying minTAP

Privacy Concerns in TAPs: IFTTT as an example

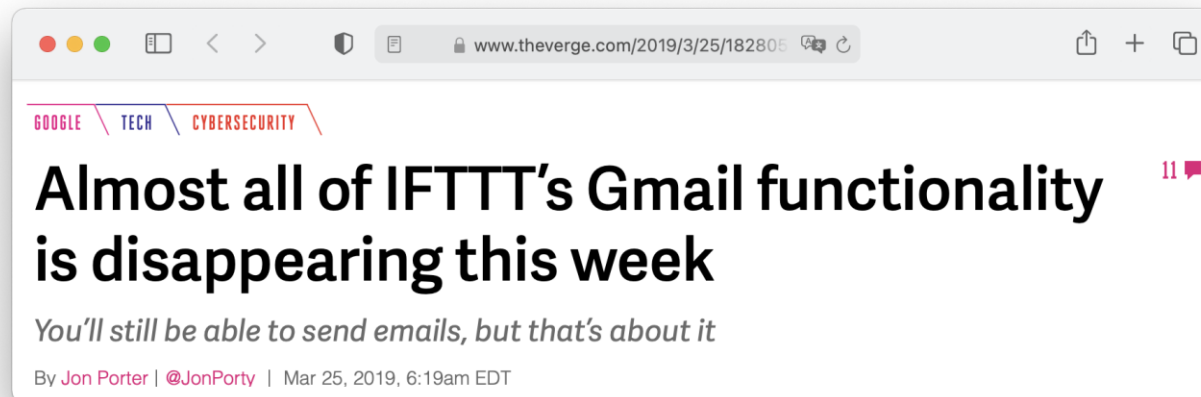
600+ services

20M+ users

- IFTTT's Term of Use states...



- Gmail removed its triggers from IFTTT due to privacy concern



Privacy Concerns in TAPs: Token-level Overprivilege

IF  new file uploaded THEN do ...




IFTTT

I want an access token  that can ...


- read files
- modify files
- delete files
-

Privacy Concerns in TAPs: Token-level Overprivilege



IF  new

IFTTT

IFTTT wants to access your Google Account

 uwmadnsp@gmail.com

This will allow IFTTT to:

-  See, edit, create, and delete all of your Google Drive files 

Make sure you trust IFTTT


You may be sharing sensitive info with this site or app. You can always see or remove access in your [Google Account](#).

Learn how Google helps you [share data safely](#).

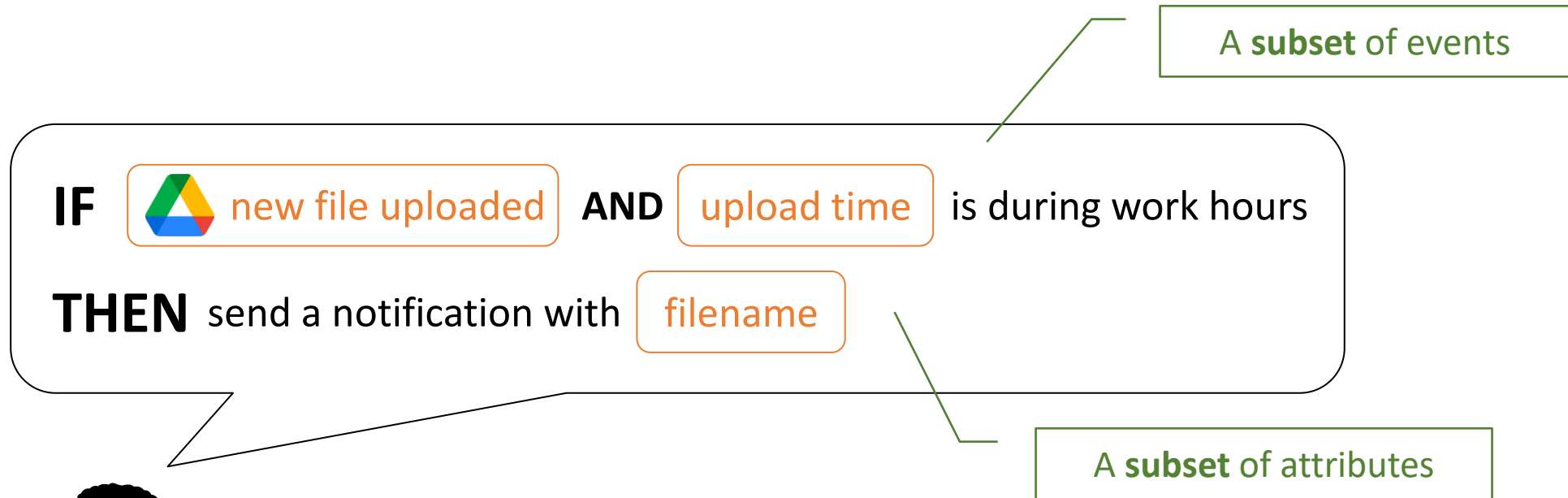
See IFTTT's [Privacy Policy](#) and [Terms of Service](#).

Cancel Allow

IFTTT

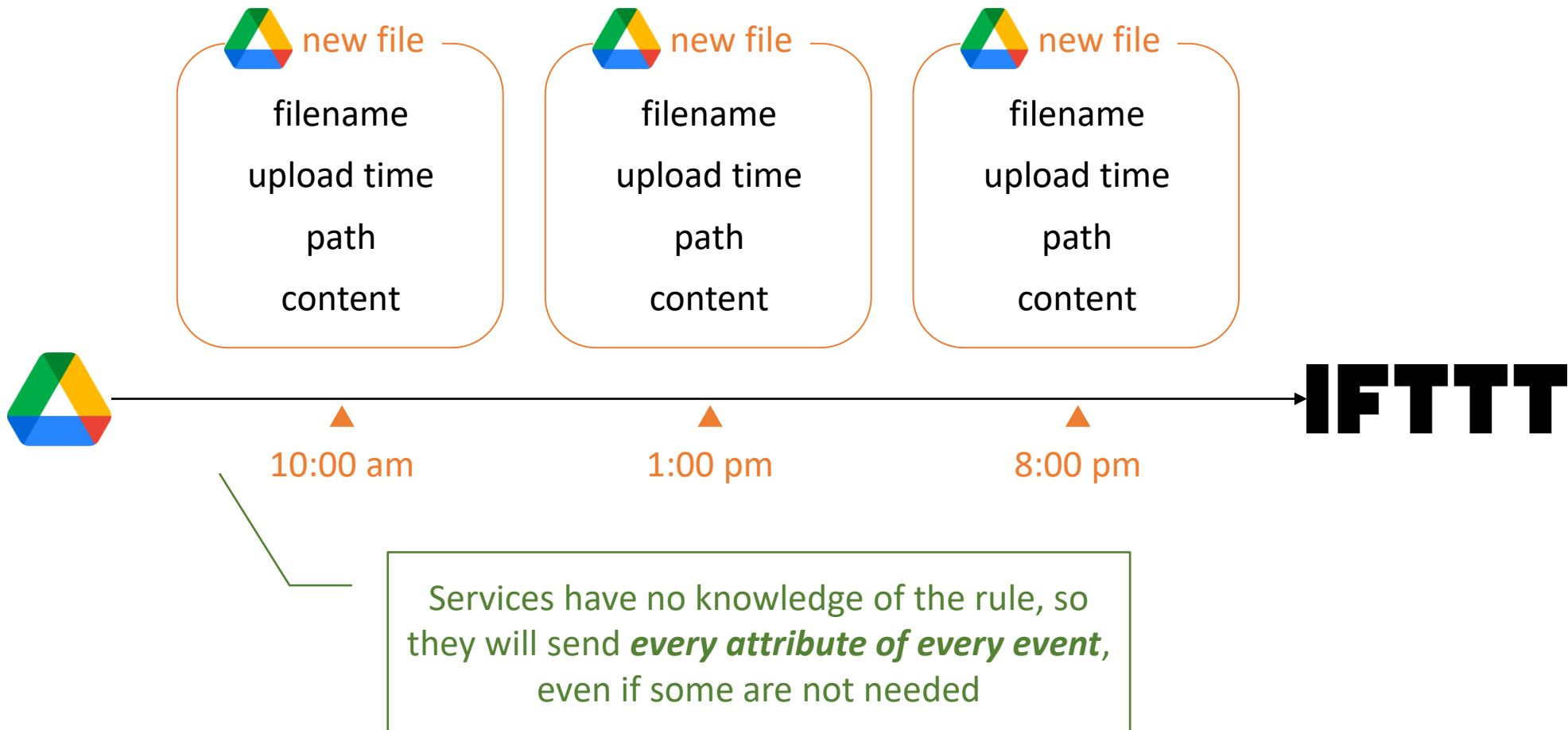
 that can ...

Privacy Concerns in TAPs: Attribute-level Overprivilege

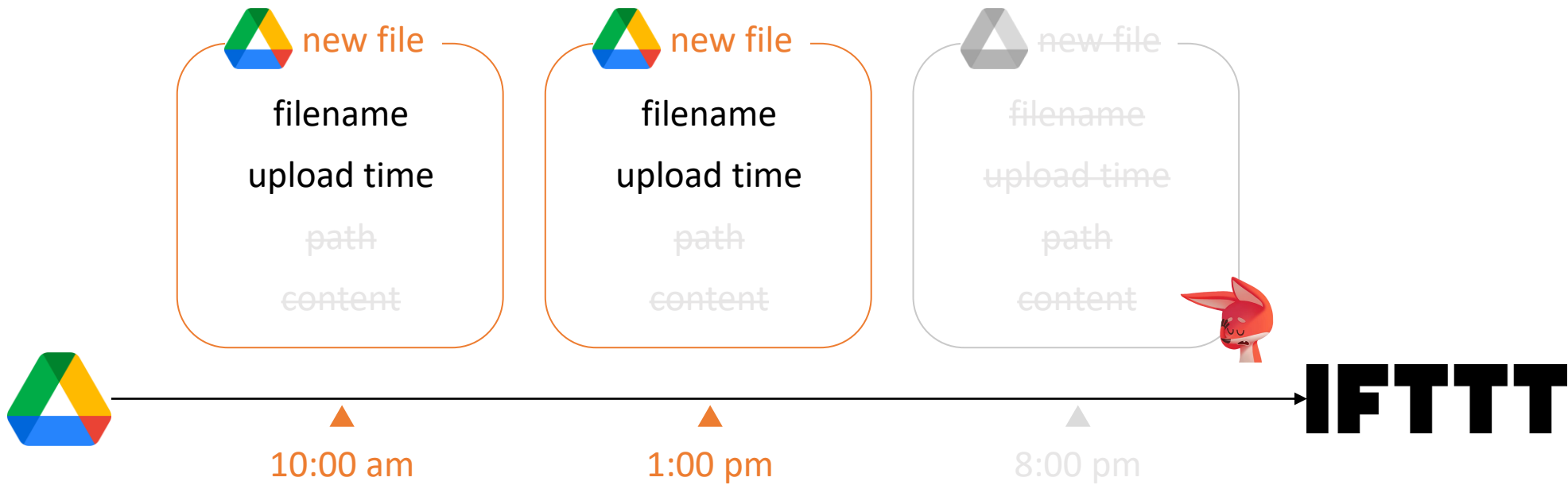



IFTTT

Privacy Concerns in TAPs: Attribute-level Overprivilege



Privacy Concerns in TAPs: Attribute-level Overprivilege



IF  new file uploaded **AND** upload time is during work hours
THEN send a notification with filename



minTAP: Trigger-Action Platform with minimized data access



Data Minimization

Trigger service should only send data that are necessary for rule execution



Allows for Computation

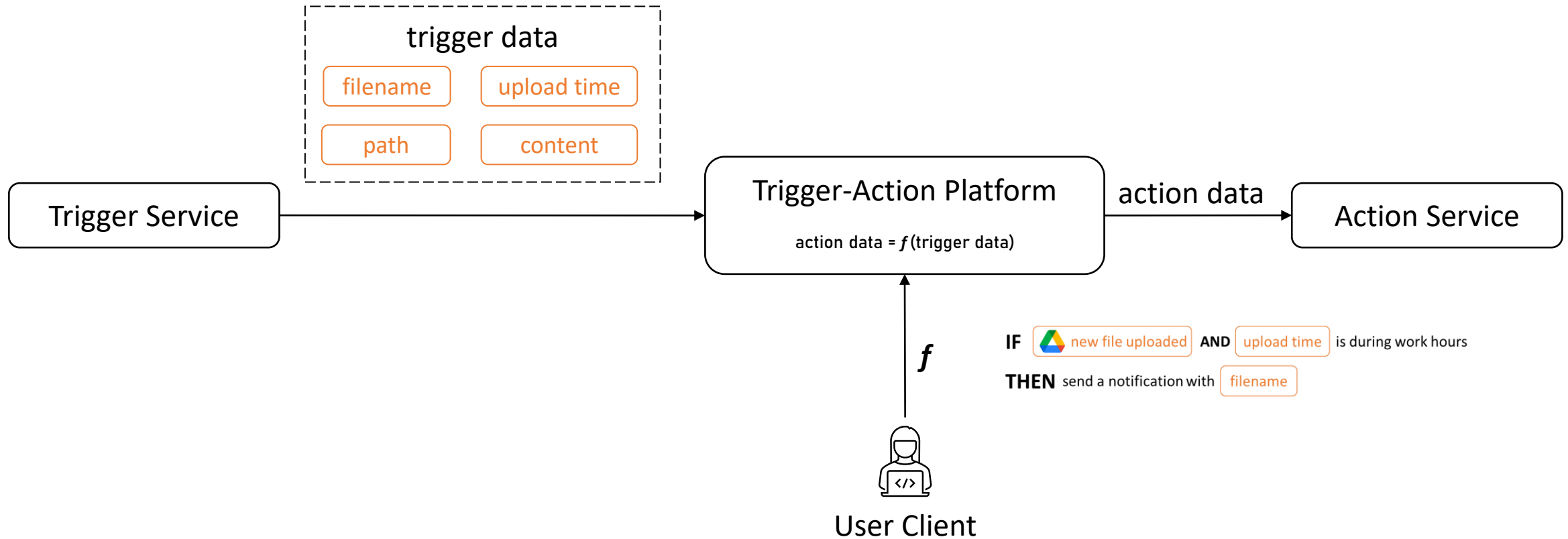
Users should be able to program complex rule conditions (using languages like JavaScript)



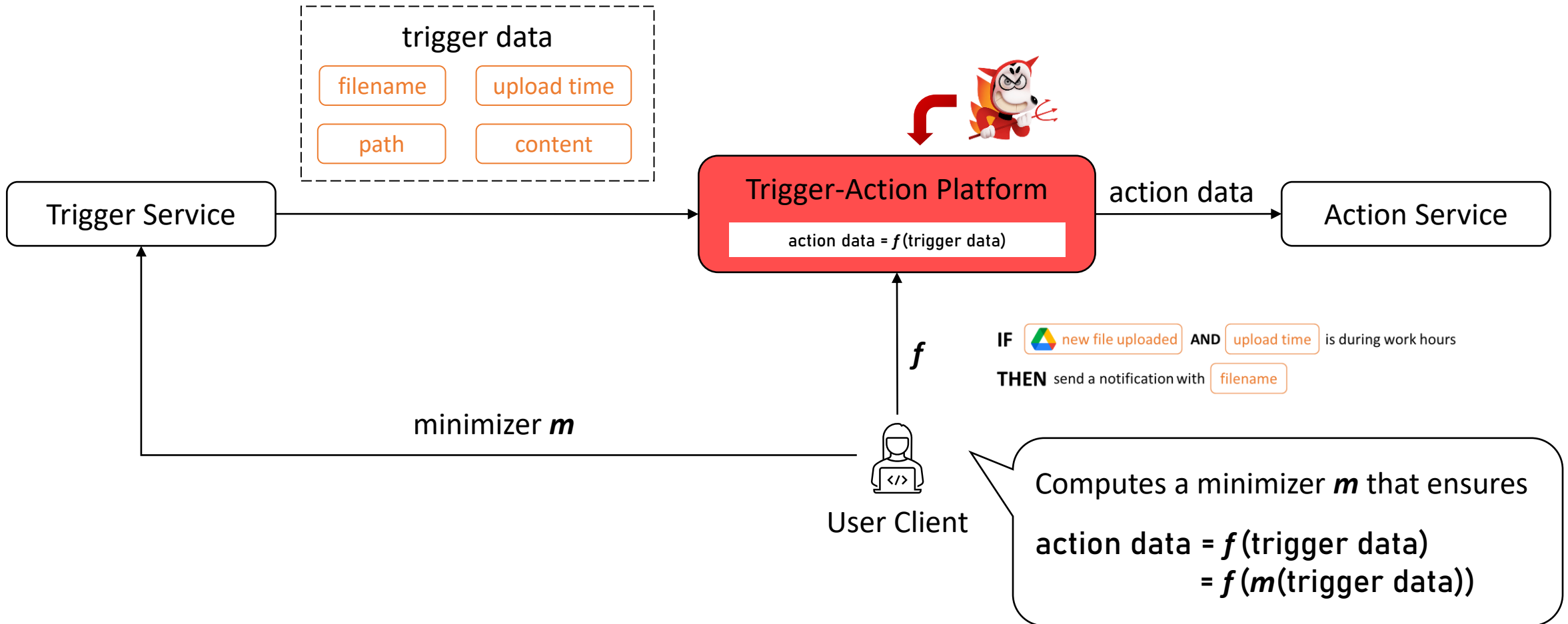
Works with Current Infrastructure

The design should only require changes in service's existing compatibility layer and be fully compatible with IFTTT with minimal affections in user experience

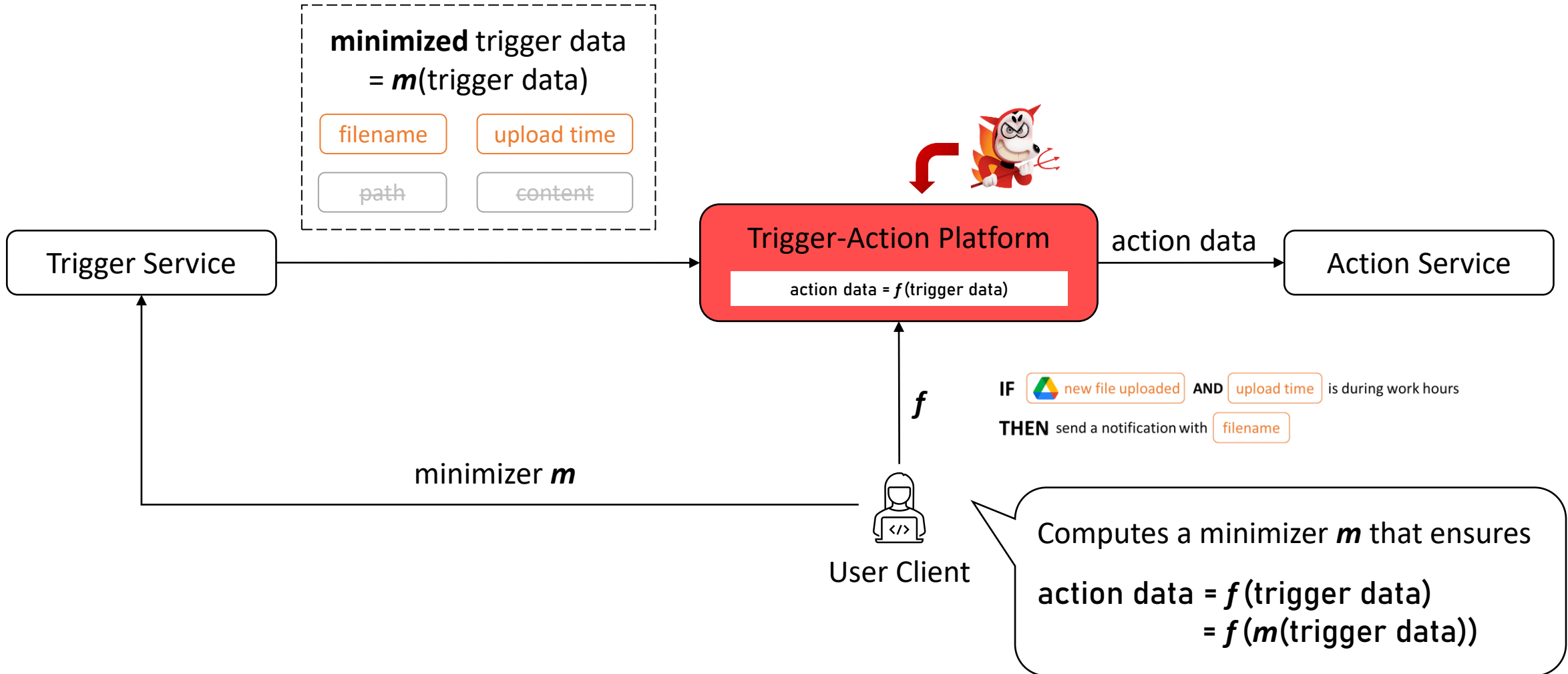
Current TAP Design



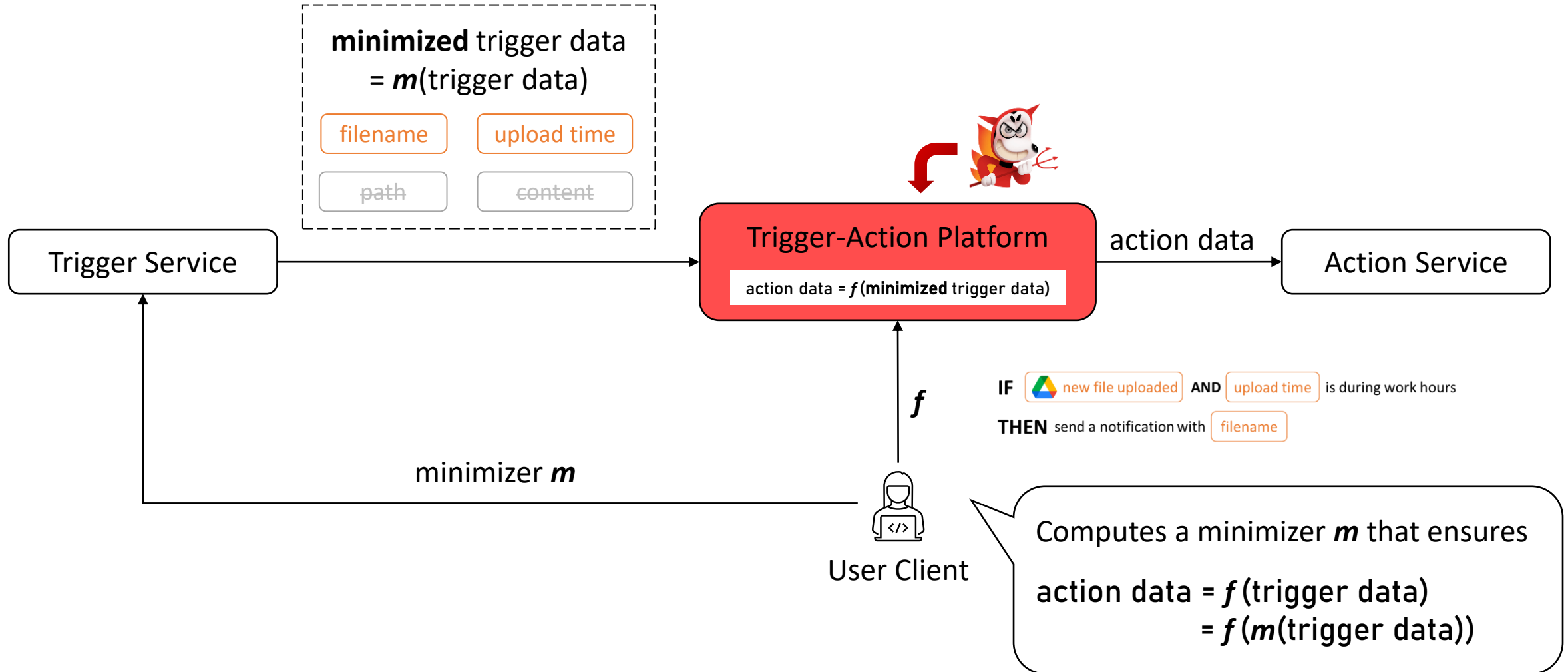
minTAP Design Overview



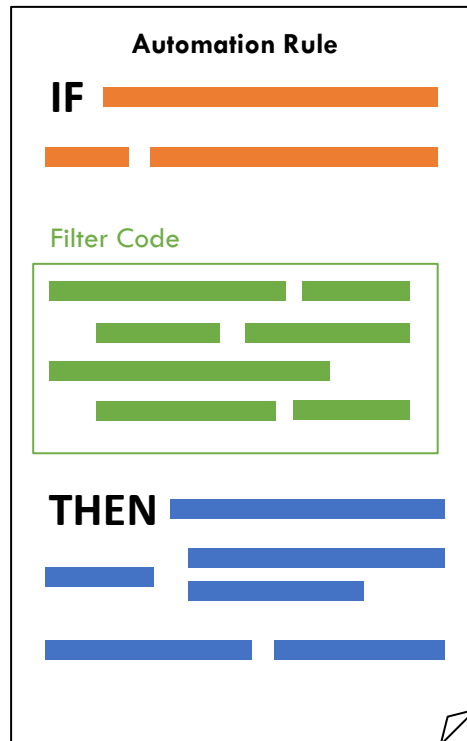
minTAP Design Overview



minTAP Design Overview



Minimizer in automation rules



Minimizer in automation rules

Automation Rule

IF Google Drive: New File in ...

Drive

Filter Code

██████████

██████████

██████████

██████████

THEN Notification: Send ...

Message

Attachment

Minimizer in automation rules

Automation Rule

IF Google Drive: New File in ...

Drive

Filter Code

```
if time before 9am / after 5pm:  
  skip action  
if filename ends with .jpg:  
  set Attachment to content
```

THEN Notification: Send ...

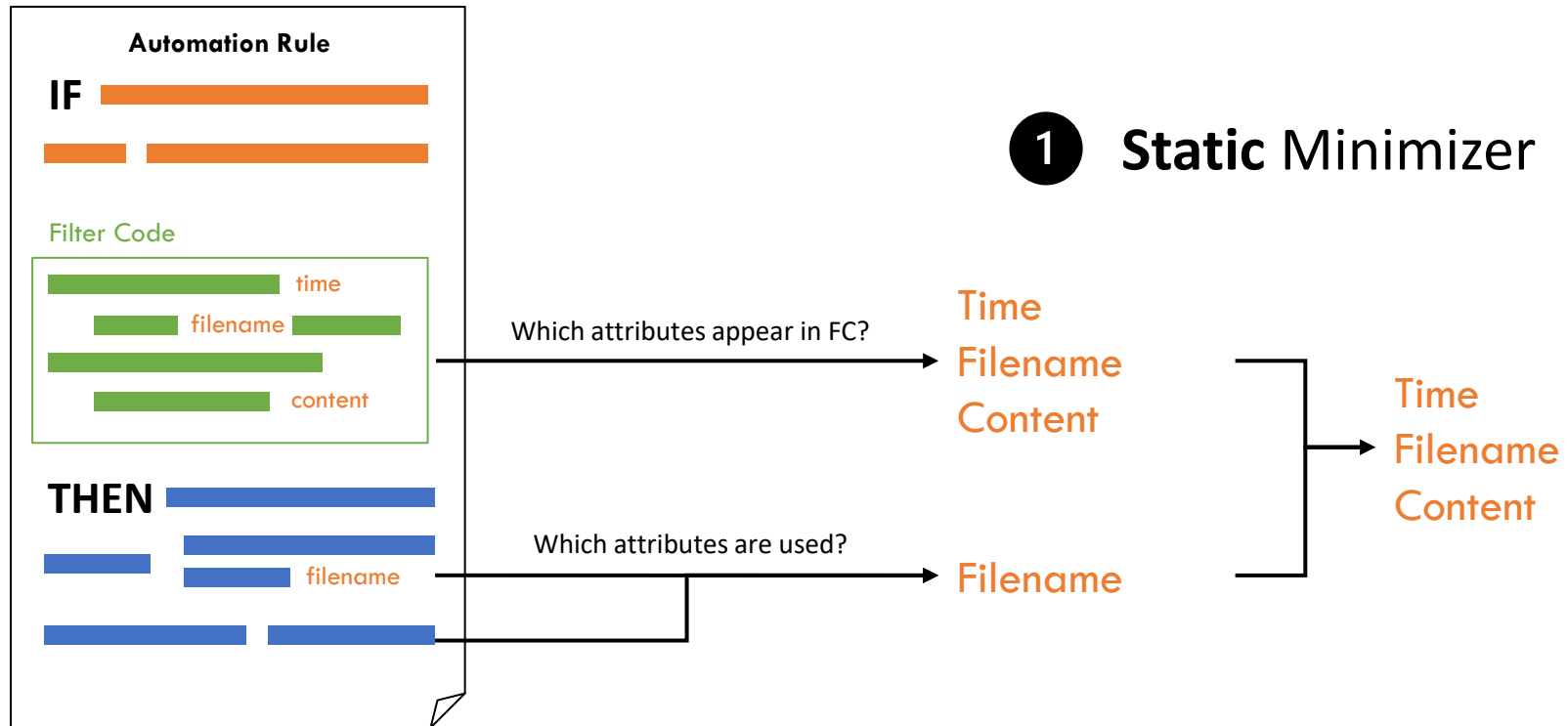
Message

Attachment

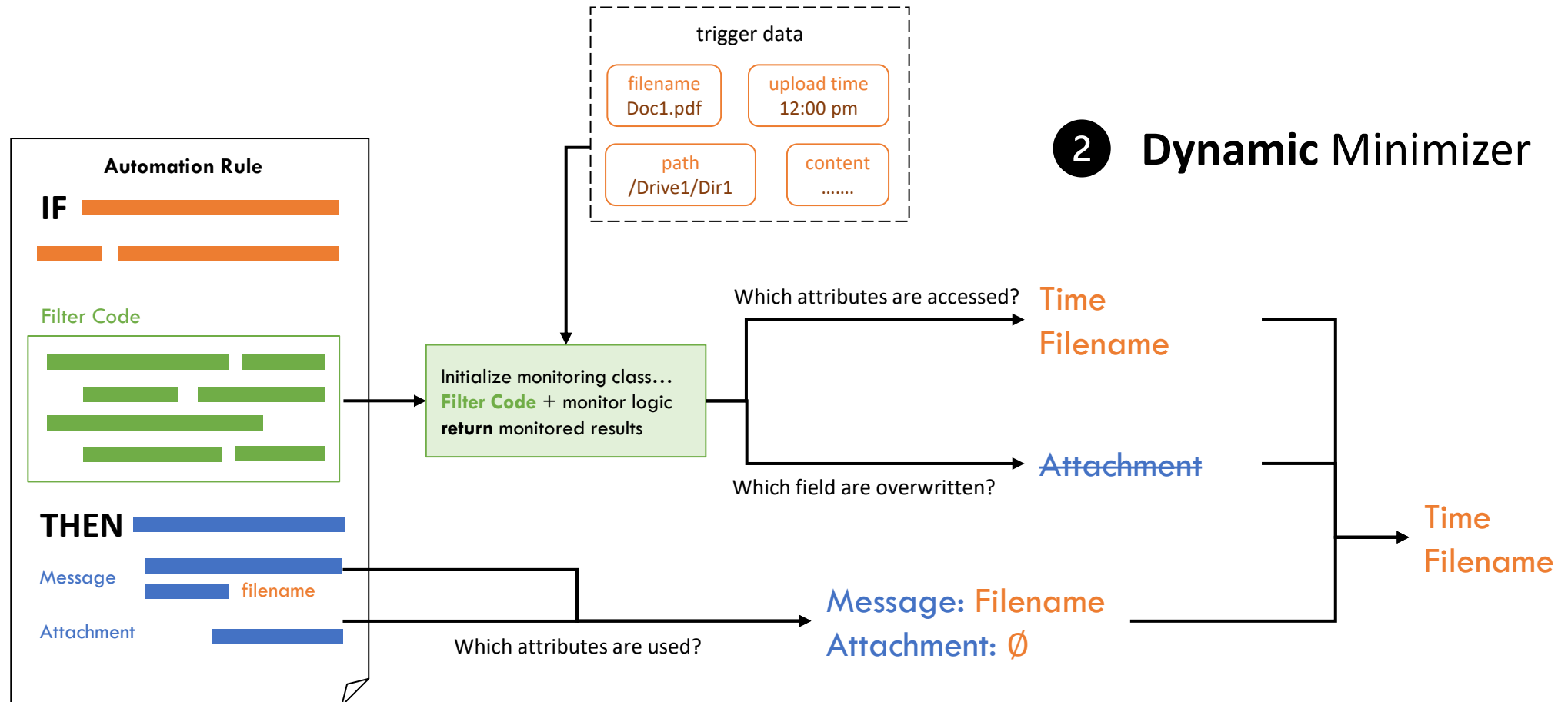
OPTION 1 : Static Minimizer

OPTION 2 : Dynamic Minimizer

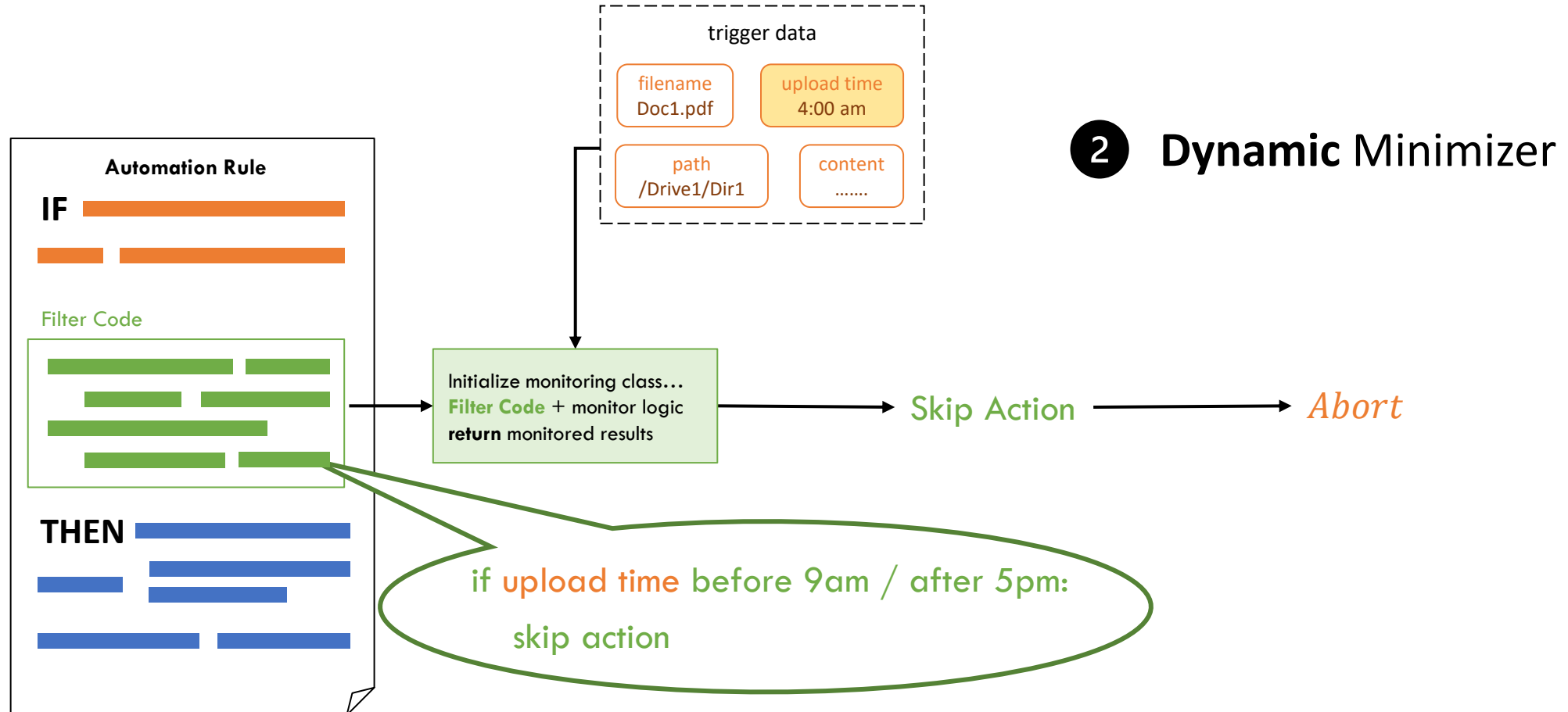
Minimizer in automation rules



Minimizer in automation rules



Minimizer in automation rules



Minimizer in automation rules

Automation Rule

IF Google Drive: New File in ...

Drive

Filter Code

```
if time before 9am / after 5pm:  
  skip action  
if filename ends with .jpg:  
  set Attachment to content
```

THEN Notification: Send ...

Message

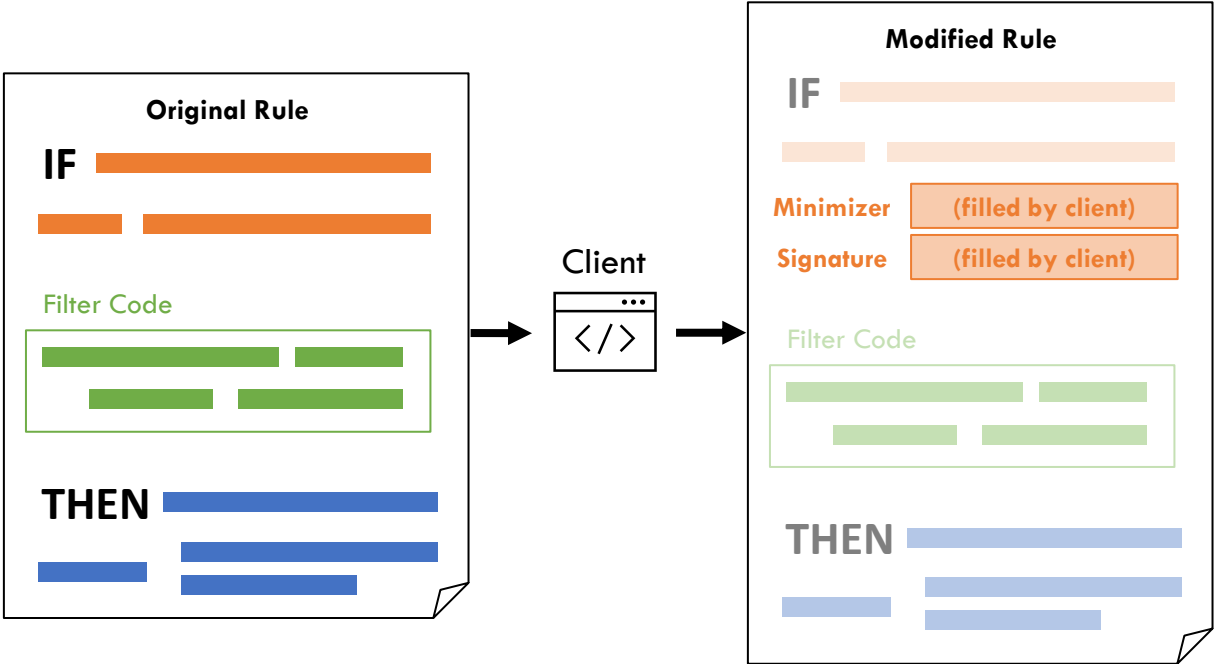
Attachment

OPTION 1: Static Minimizer

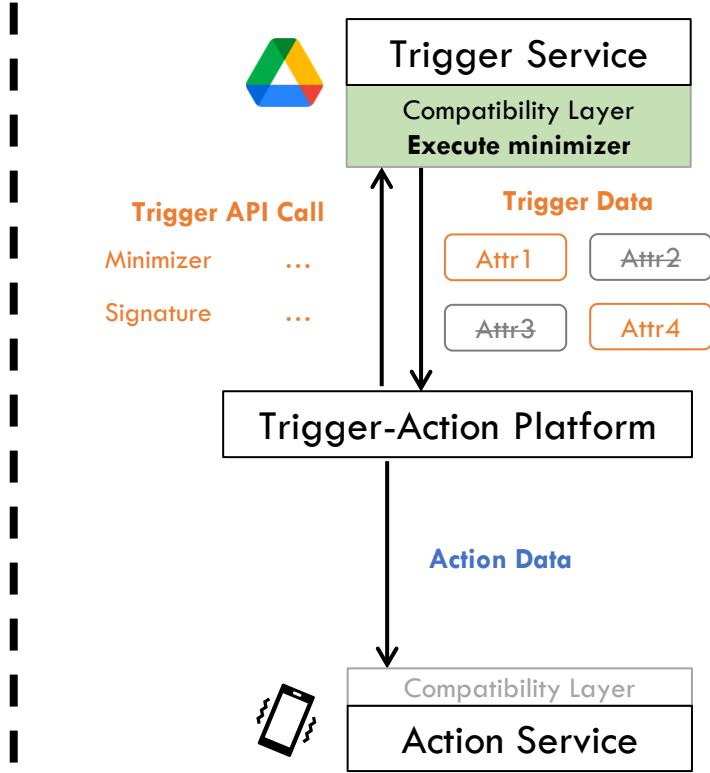
OPTION 2: Dynamic Minimizer

- + high precision, especially when branching exists in filter code
- extra latency overhead due to runtime execution: ≈ 6 milliseconds

minTAP Execution Flow

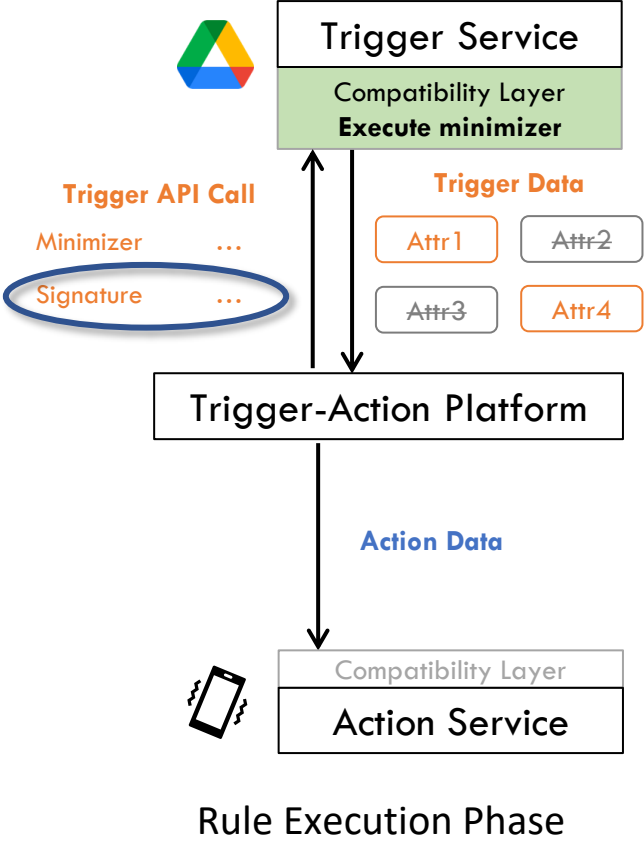
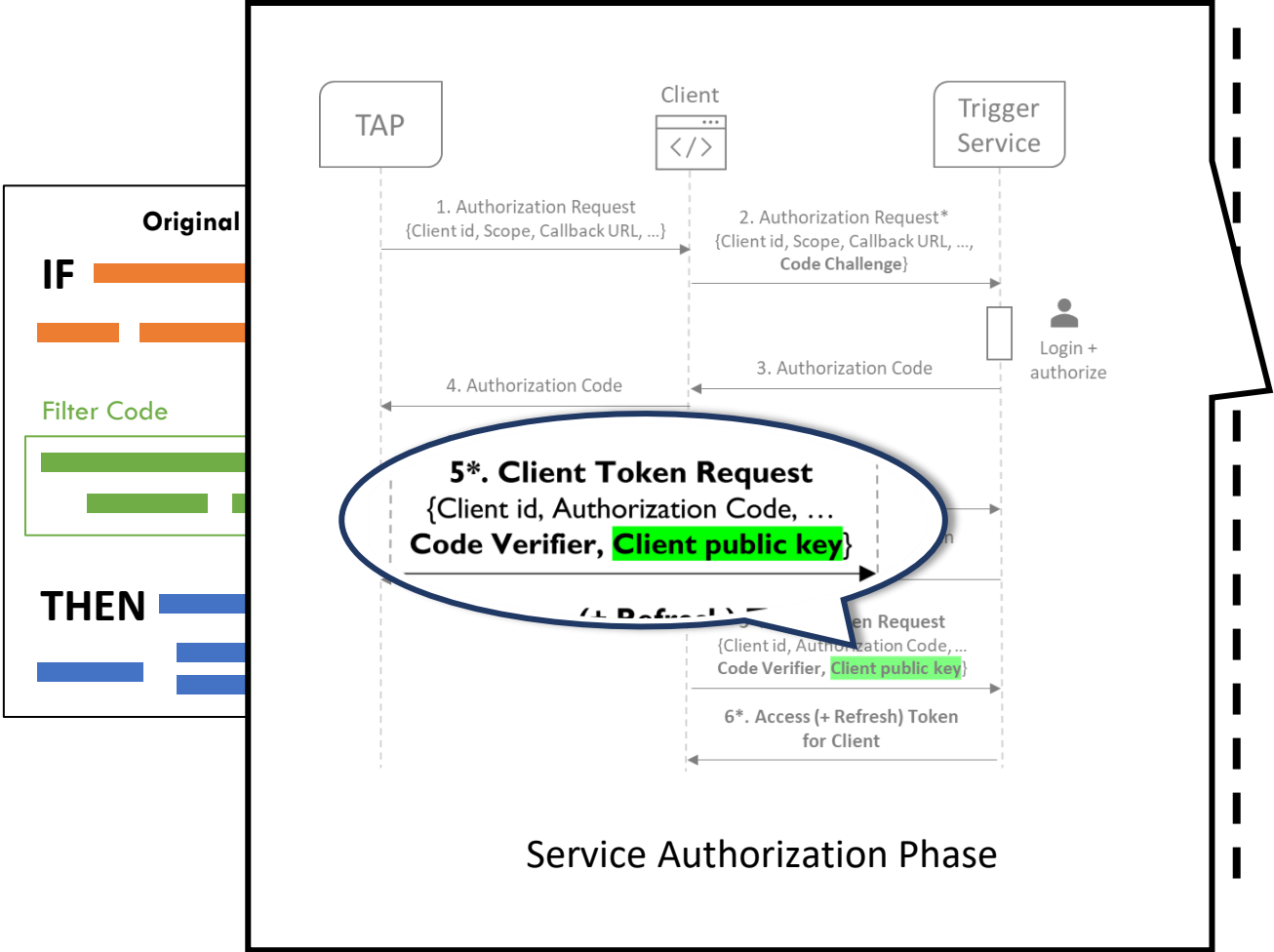


Rule Setup Phase



Rule Execution Phase

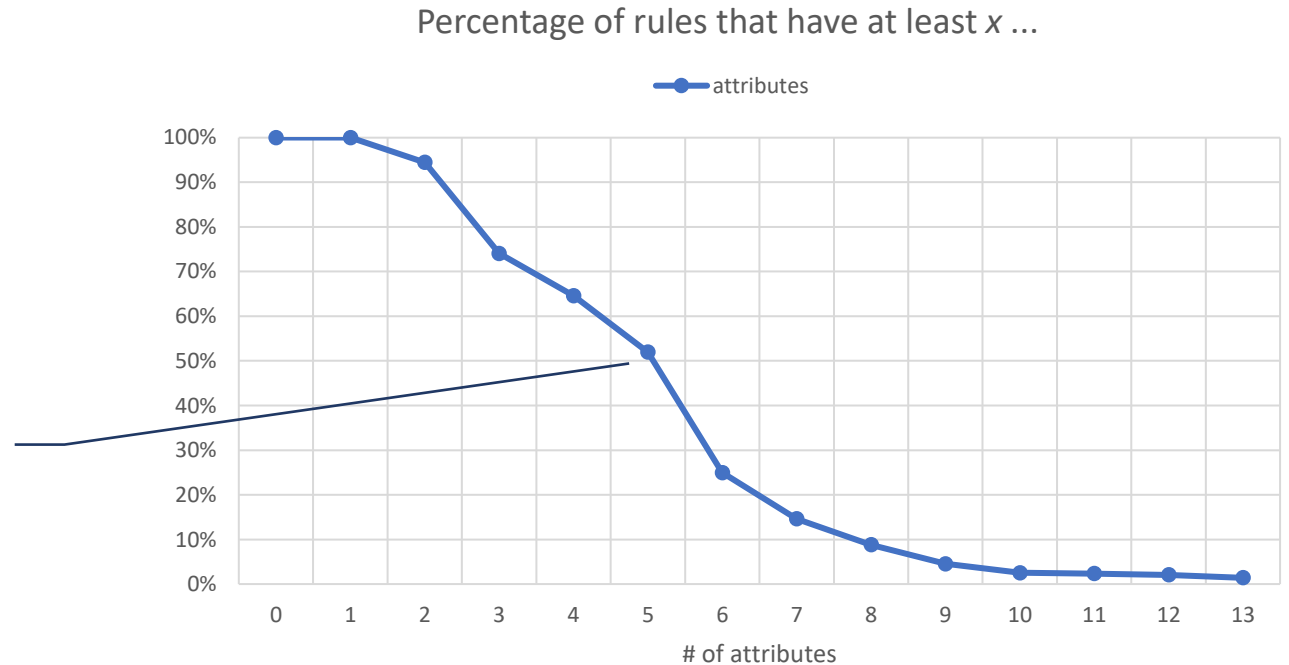
minTAP Execution Flow



Study of Overprivileges in IFTTT

- Collected **34,419** IFTTT rules connected to **private** triggers
 - Including detailed configuration (e.g., filter code)!

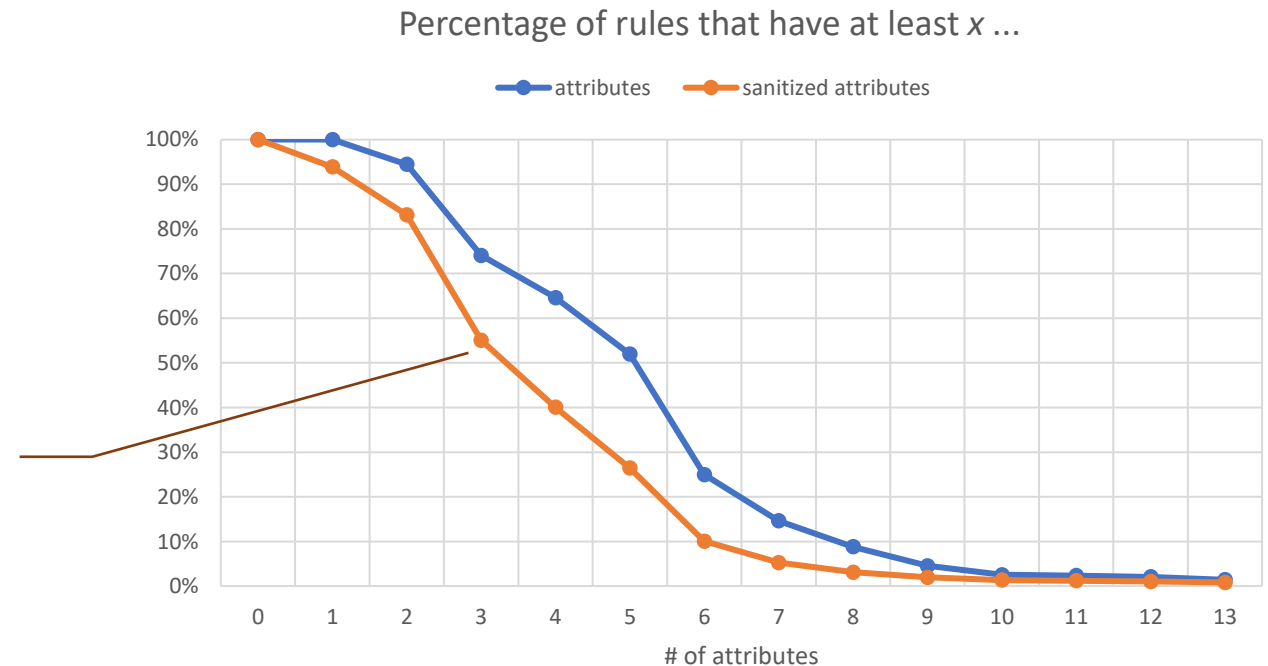
50% of these IFTTT rules have access to 5+ attributes



Study of Overprivileges in IFTTT

- Collected **34,419** IFTTT rules connected to private triggers
 - Including detailed configuration (e.g., filter code)!
- On average **3.6** attributes are not needed

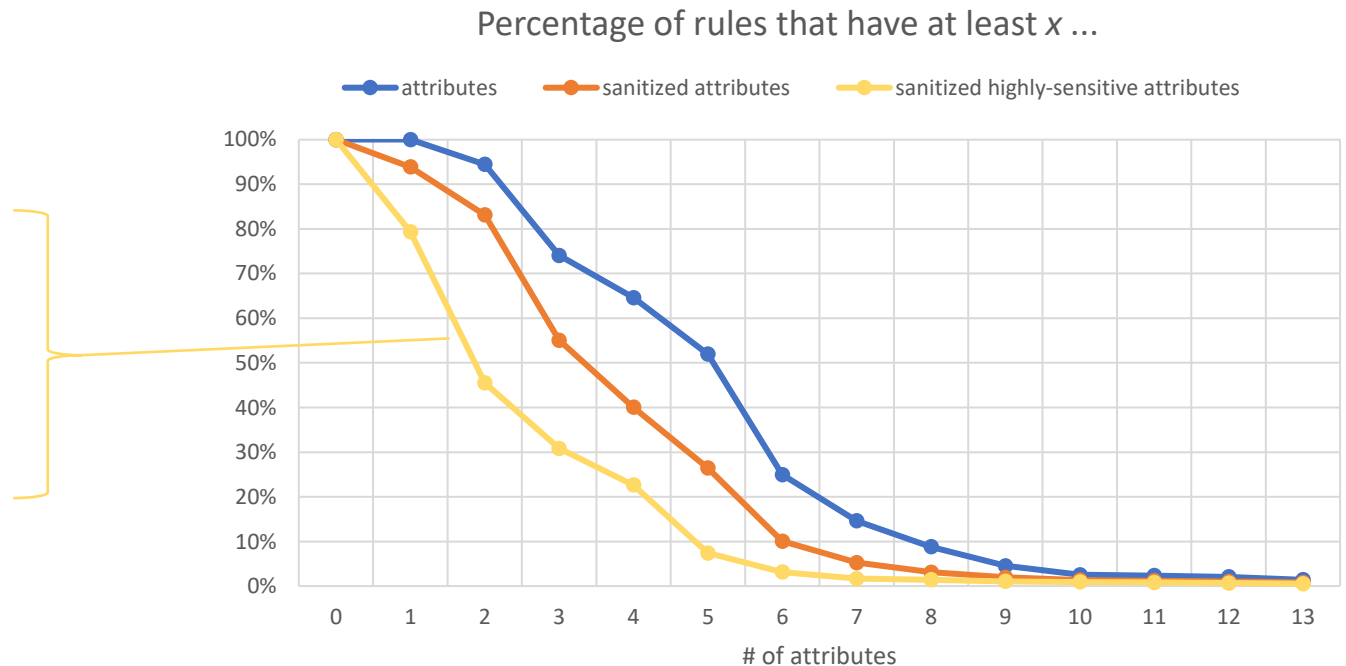
50% of these IFTTT rules have access to 3+ attributes **that are not needed and will be sanitized by minTAP**



Study of Overprivileges in IFTTT

- Collected **34,419** IFTTT rules connected to private triggers
 - Including detailed configuration (e.g., filter code)!
- On average **3.6** attributes are not needed

Attribute Type	%
Timestamp	26.7%
Event description	23%
User's personal info	13%
Location	9%
Downloadable link	7%
Access-controlled link	2.2%



Thank you!

minTAP: Trigger-Action Platform
with minimized data access



Leveraging static and dynamic analysis to
sanitize unnecessary data attributes



Works with user-created filter code



Only lightweight changes to existing TAP
compatibility layer required, while sanitizing
3.6 attributes per automation rule



Yunang Chen
yc@cs.wisc.edu



[https://github.com/
EarlMadSec/minTAP](https://github.com/EarlMadSec/minTAP)