



## **The SPaCIoS Tool**

**property-driven and vulnerability-driven security testing for Web-based apps**

**Luca Compagna**, Product Security Research, SAP AG  
*(on behalf of SPaCIoS consortium)*

STREP Project number: 257876

Objective ICT-2009.1.4 c: Technology and Tools for Trustworthy ICT

01.10.10 – 31.01.14

[www.spacios.eu](http://www.spacios.eu)

## Research prototype

- model checking
- security testing
- penetration testing
- ...

## Complements state-of-the-art

## Targets industrially-relevant Security Protocols & Web Apps

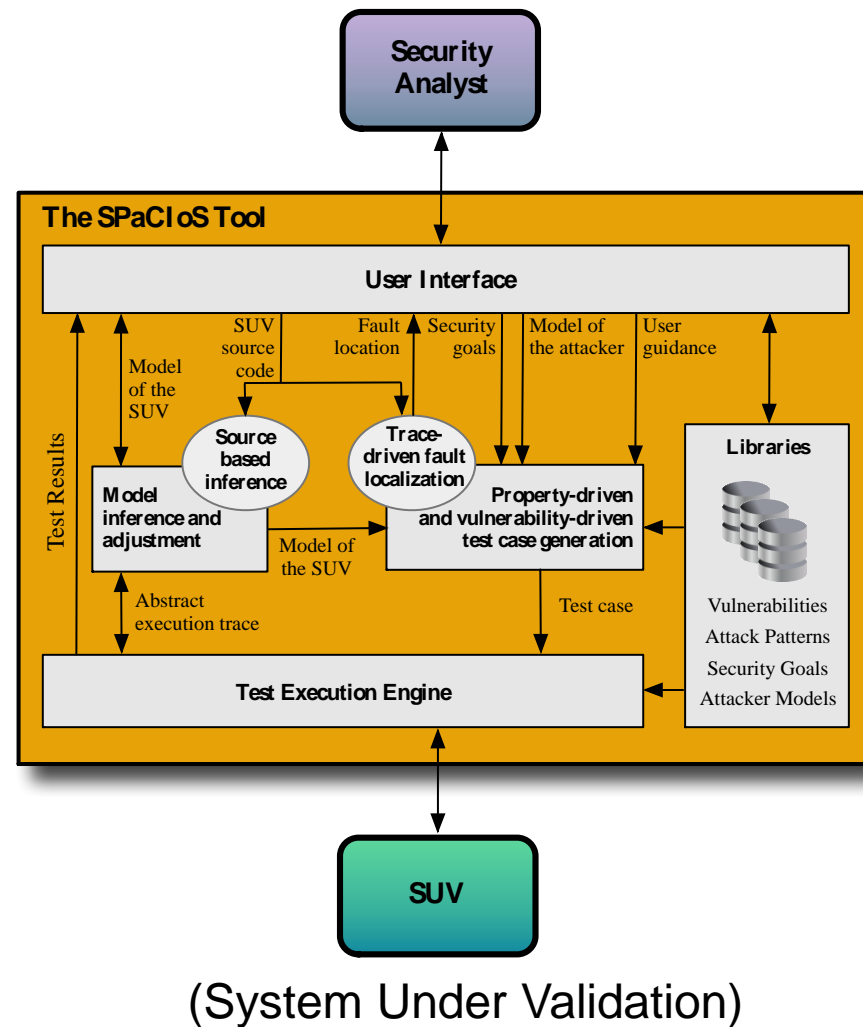
## Broad security range

- logic-flaws, injections, AC, ...
- good coverage of OWASP top 10

## Promising results

- SAML SSO, OAuth2, ..
- WebGoat, Shopping Cart, ..

## On-going transfers to SAP and SIEMENS



## Research prototype

- model checking
- security testing
- penetration testing
- ...

## Complements state-of-the-art

## Targets industrially-relevant Security Protocols & Web Apps

## Broad security range

- logic-flaws, injections, AC, ...
- good coverage of OWASP top 10

## Promising results

- SAML SSO, OAuth2, ..
- WebGoat, Shopping Cart, ..

## On-going transfers to SAP and SIEMENS

- Rigorous, formal
- Automated (at least most of it)
- Synergic combination of independent components
- Logic workflow of the SUV
- Discovering vulnerabilities that others do not find



## Research prototype

- model checking
- security testing
- penetration testing
- ...

## Complements state-of-the-art

## Targets industrially-relevant Security Protocols & Web Apps

## Broad security range

- logic-flaws, injections, AC, ...
- good coverage of OWASP top 10

## Promising results

- SAML SSO, OAuth2, ..
- WebGoat, Shopping Cart, ..

## On-going transfers to SAP and SIEMENS



	OWASP Top 10	The SPaCloS Tool
A1	Injection	WebGoat lesson: String SQL Injection WebGoat lesson: Numeric SQL Injection SIEMENS InfoBase and eHealth
A2	Broken Authentication & Session Management	SAML, OpenID, OAuth: e.g., authentication logic-flaws Password brute-forcing on SIEMENS InfoBase and eHealth
A3	Cross-Site Scripting	WebGoat lesson: Stored XSS WebGoat lesson: Reflected XSS SIEMENS InfoCase and eHealth
A4	Insecure Direct Object References	SIEMENS InfoBase and eHealth: File Enumeration and Path Traversal
A5	Security Misconfiguration	WebGoat lesson: Forced Browsing (File Enumeration)
A6	Sensitive Data Exposure	SAML, OpenID, OAuth: data confidentiality logic flaws
A7	Missing Function Level Access Control	WebGoat lesson: Bypass Business Layer Access Control, WebGoat lesson: Bypass Data Layer Access Control WebGoat lesson: Role Based Access Control SIEMENS eHealth
A8	CSRF	SIEMENS InfoBase and eHealth
A9	Using Components with Known Vulnerabilities	
A10	Unvalidated Redirects and Forwards	

# **The SPaCloS tool and what you can do with it**

**Use case 1**

**property-driven security  
testing**

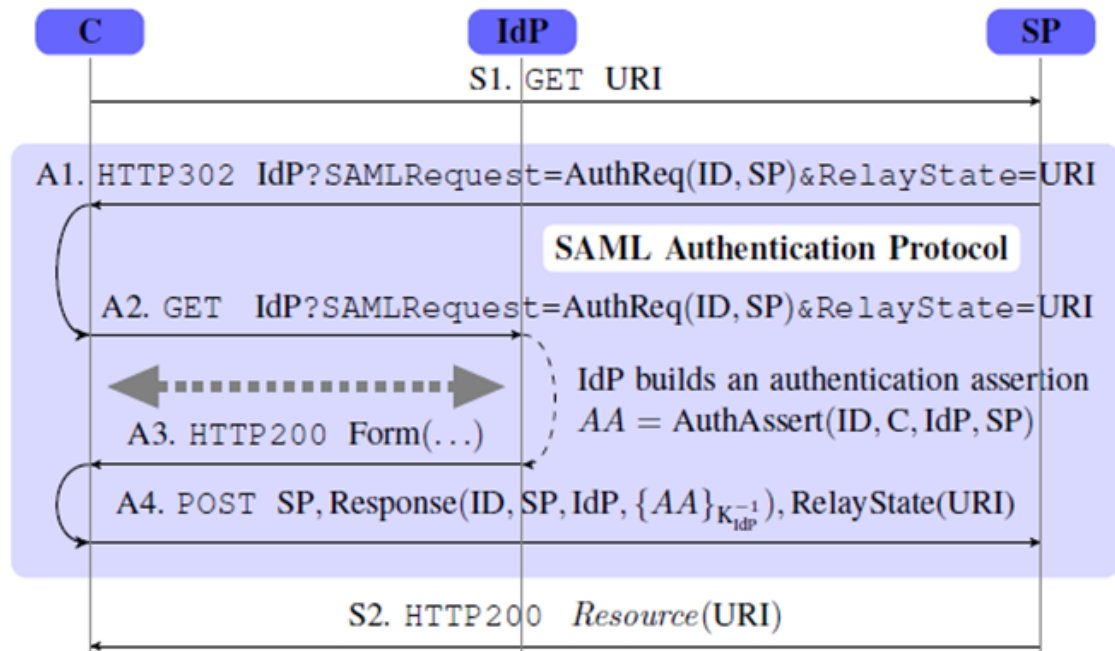
# One example

Company enriching its products with **security standards** (SAML SSO, OAuth2, ..)

- security standards are highly configurable → which **options** and recommendations?
- company's internal requirements → some **deviations** wrt standard?
- security **impact**?

## SAML SSO – SP-initiated profile

- TLS/SSL everywhere or only in certain places?
- Shall IdP require signed SAML requests?
- Is “SP checking ID” really necessary?



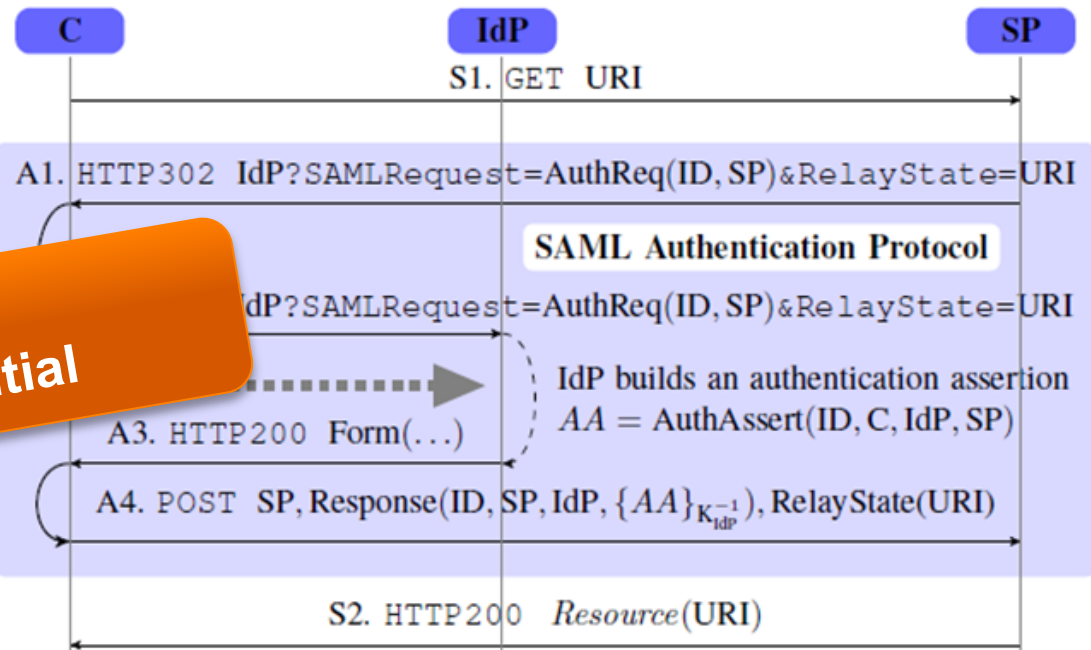
# One example

Company enriching its products with **security standards** (SAML SSO, OAuth2, ..)

- security standards are highly configurable → which **options** and recommendations?
- company's internal requirements → some **deviations** wrt standard?
- security **impact**?

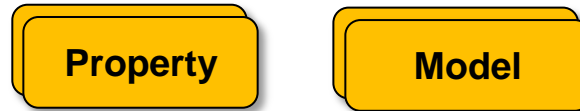
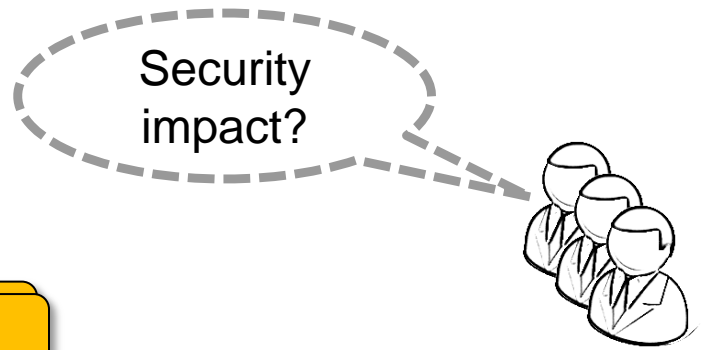
## SAML SSO – SP-initiated profile

- TLS/SSL everywhere or only in certain places?
- Shall IdP require signed SAML requests?
- Is “SP checking ID” really necessary?



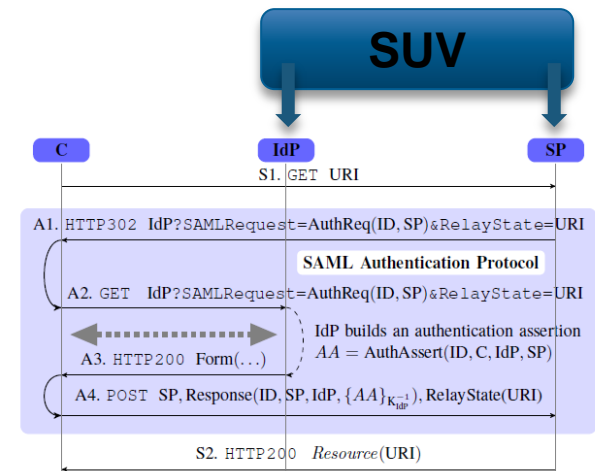
- SP shall authenticate C
- Resource shall be confidential



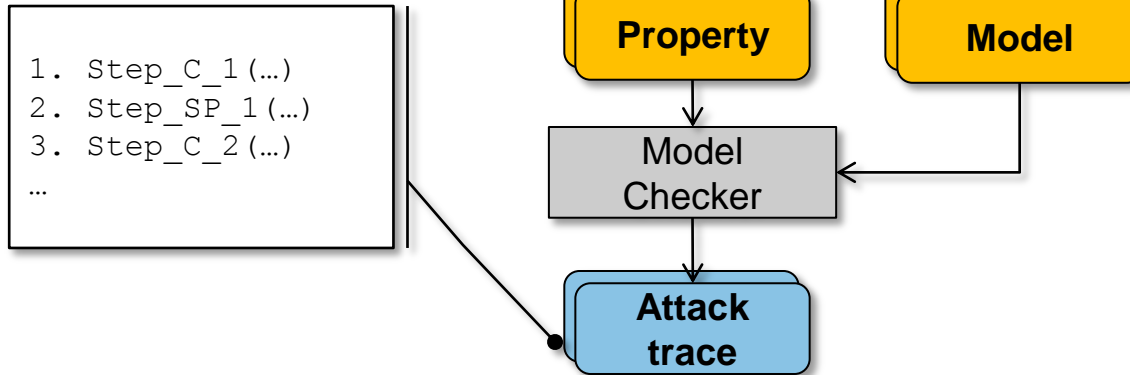
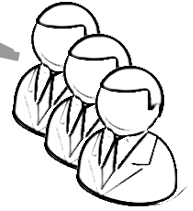


 Input

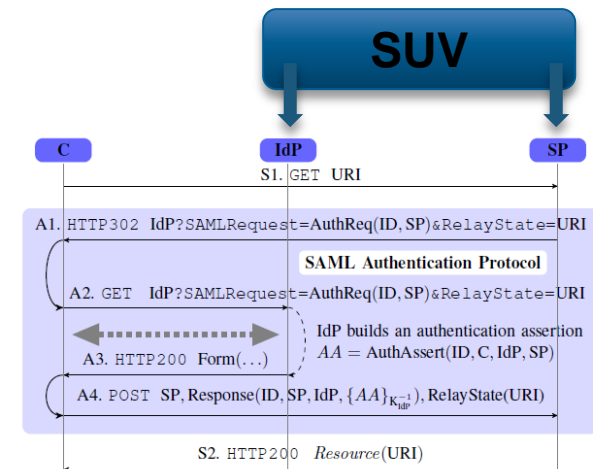
 Output



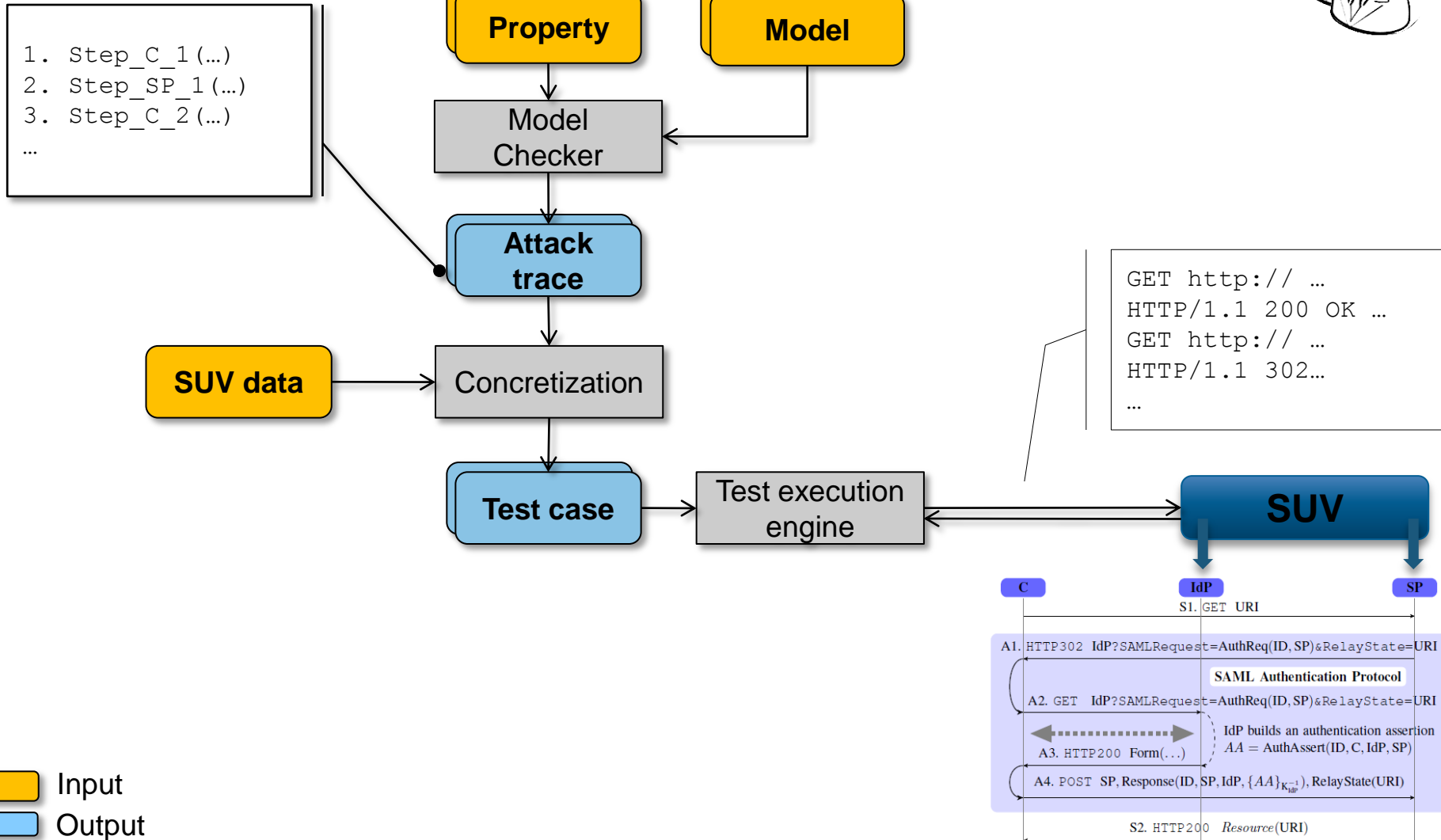
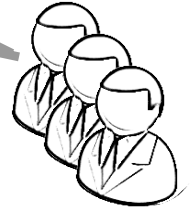
Security  
impact?



 Input  
 Output



Security  
impact?



# Demo

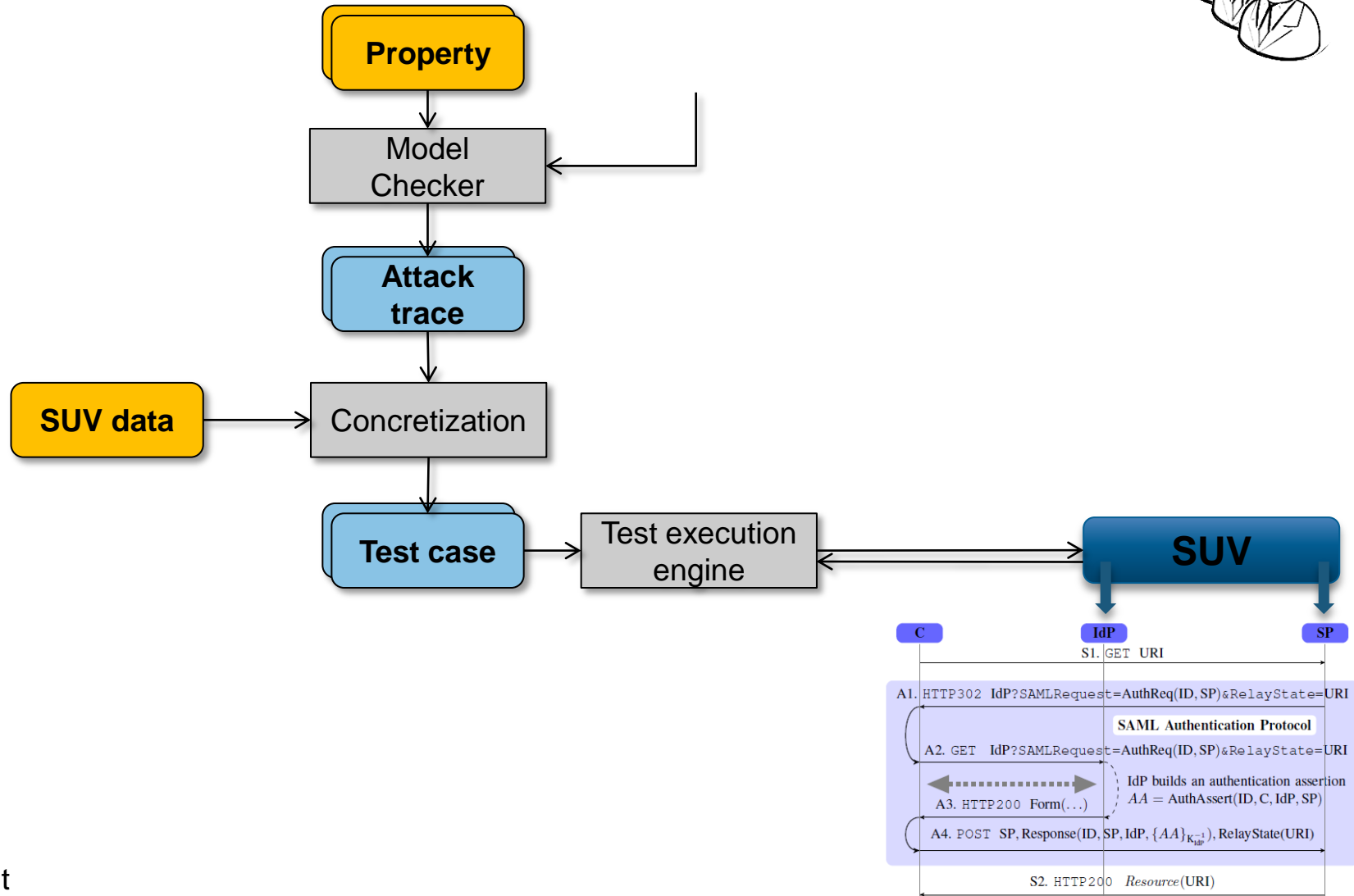
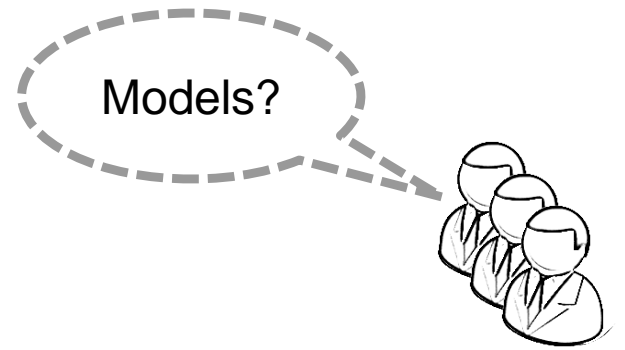


# **Use case 2**

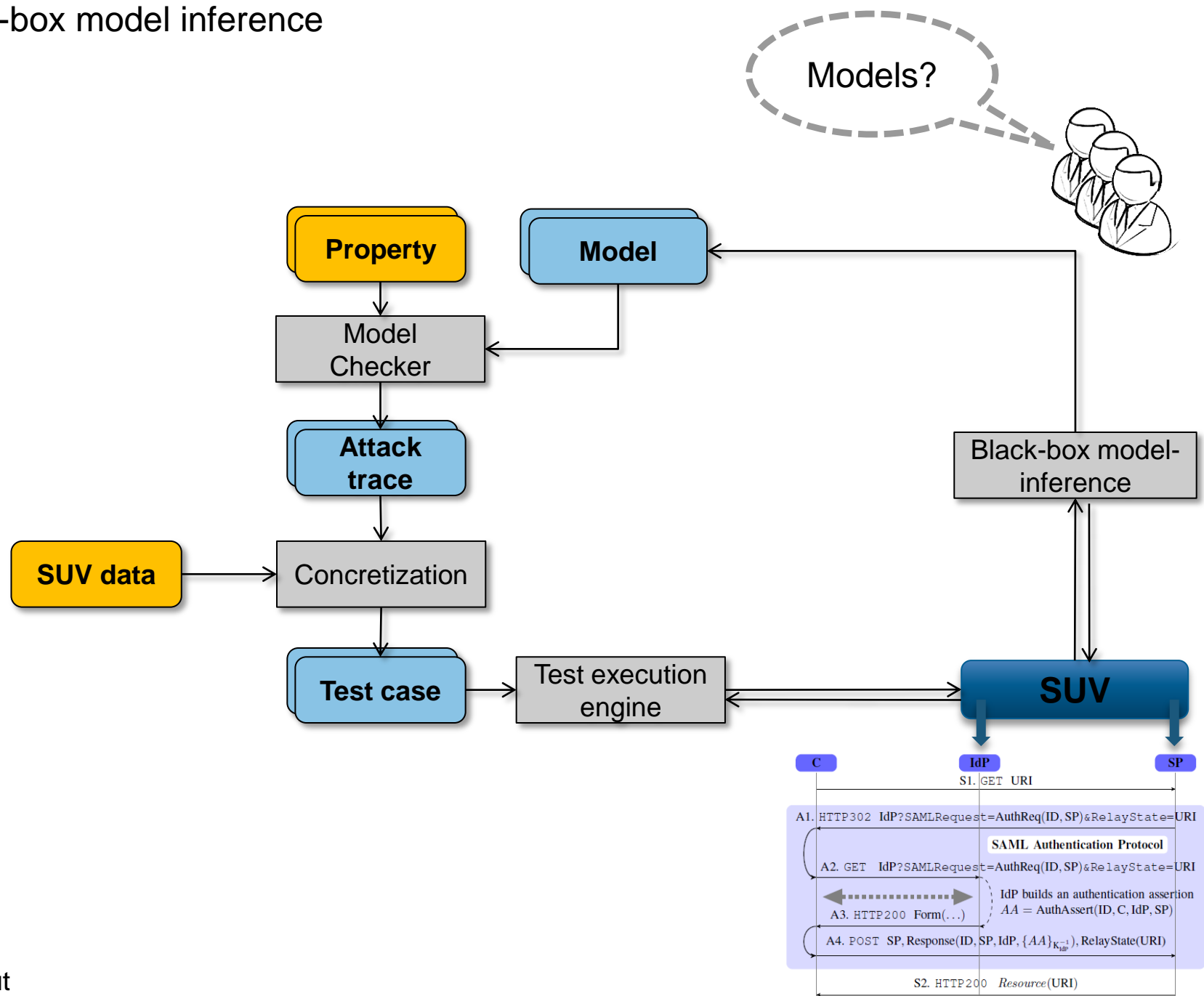
## **model-inference**

**If time, otherwise  
next time?**

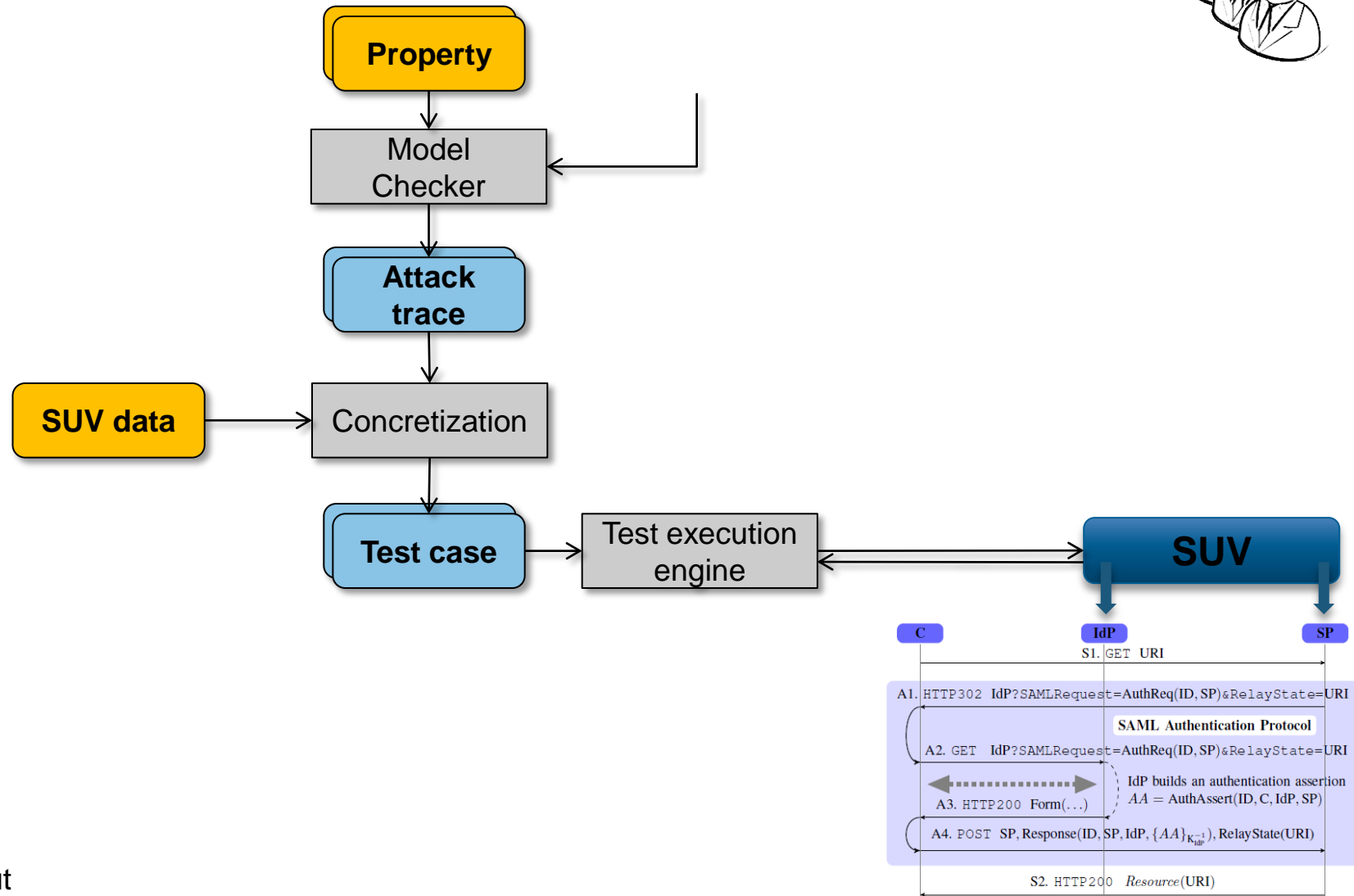




- Black-box model inference

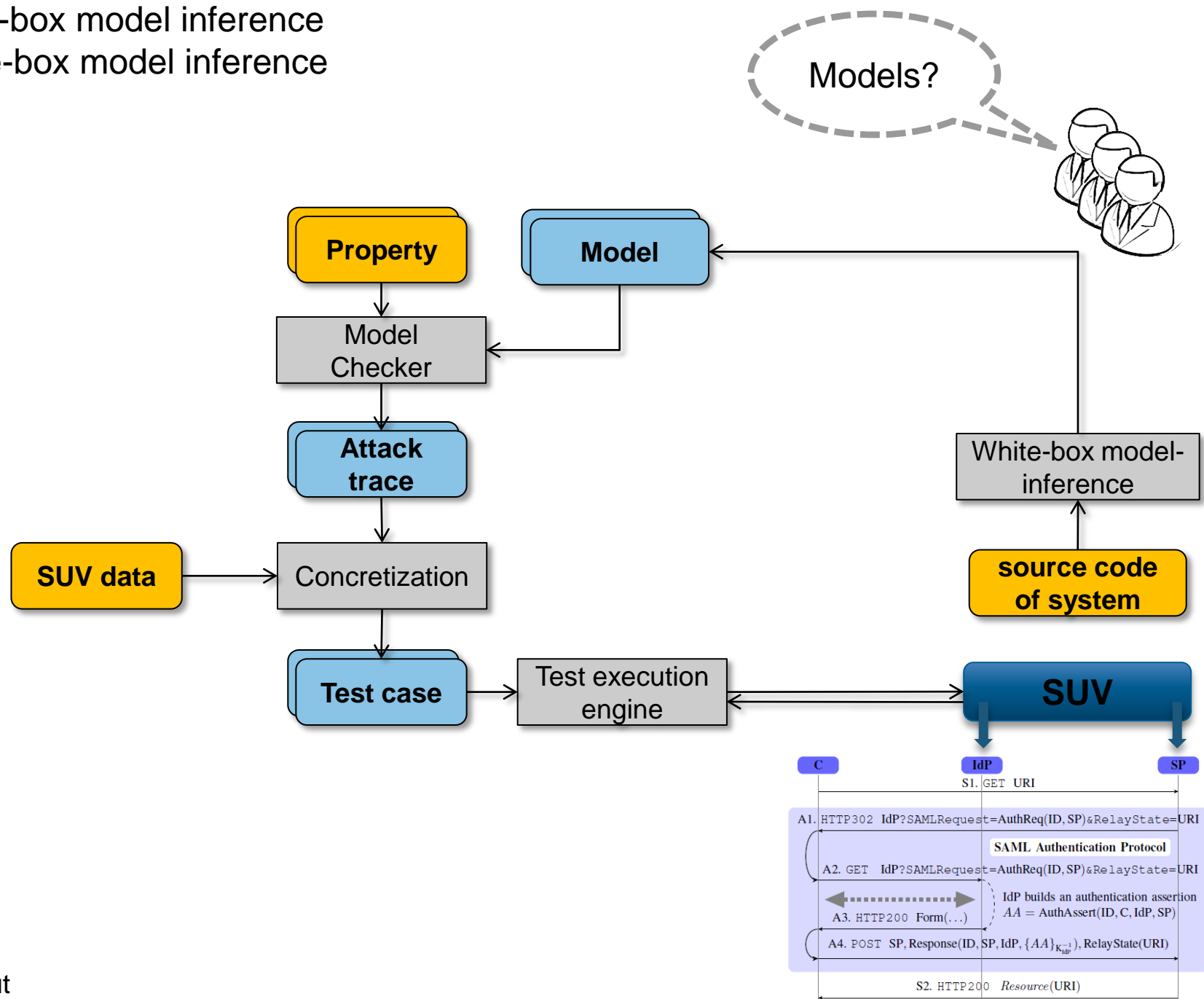


- Black-box model inference

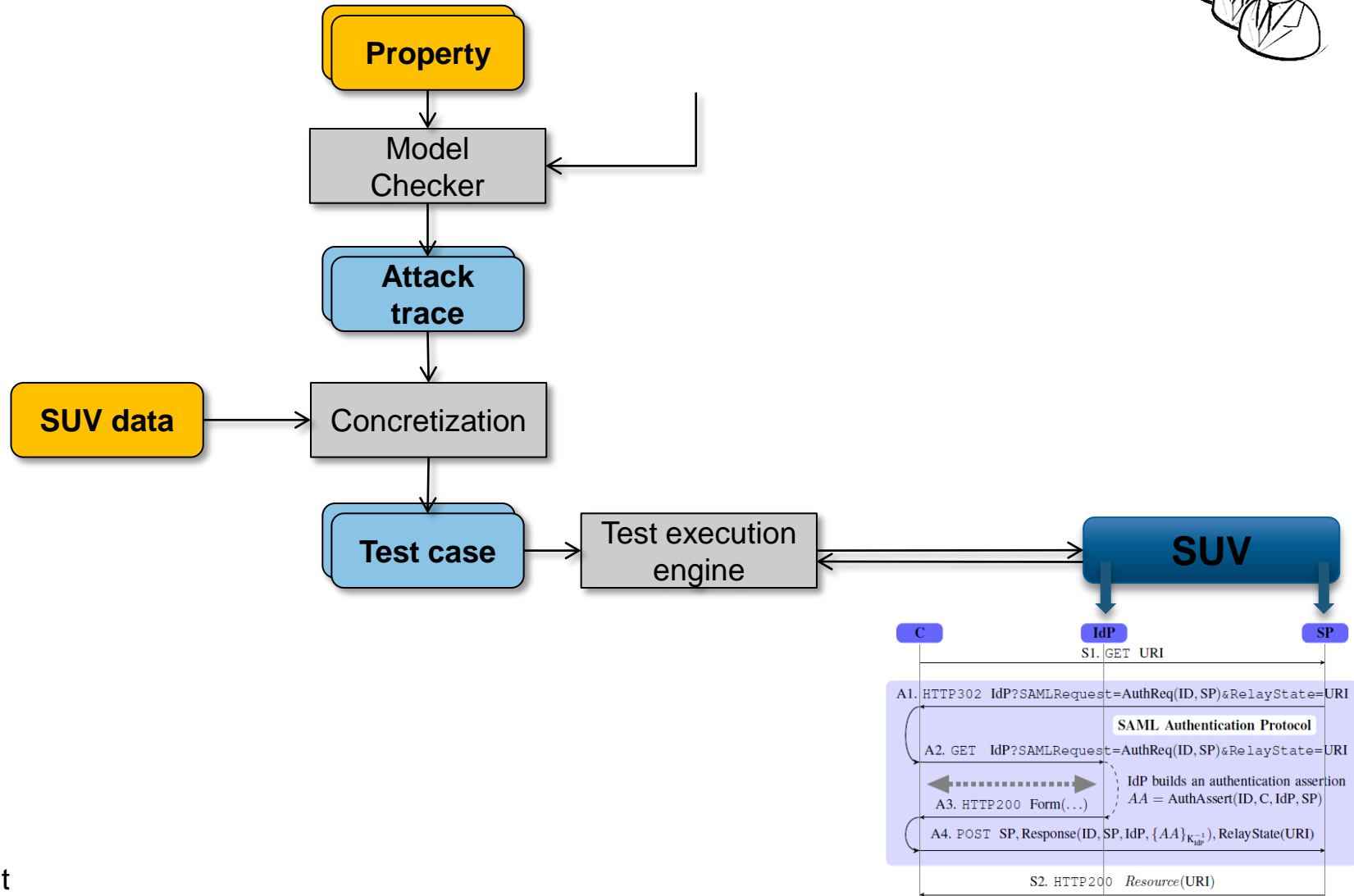
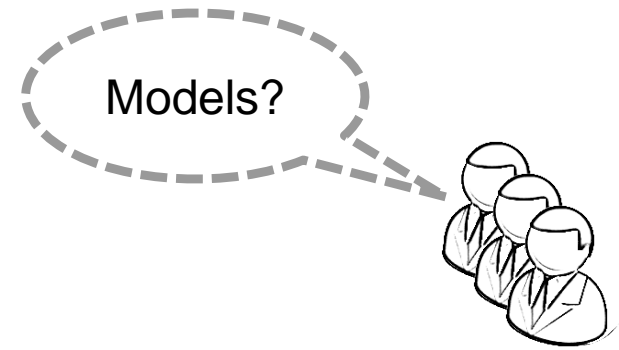




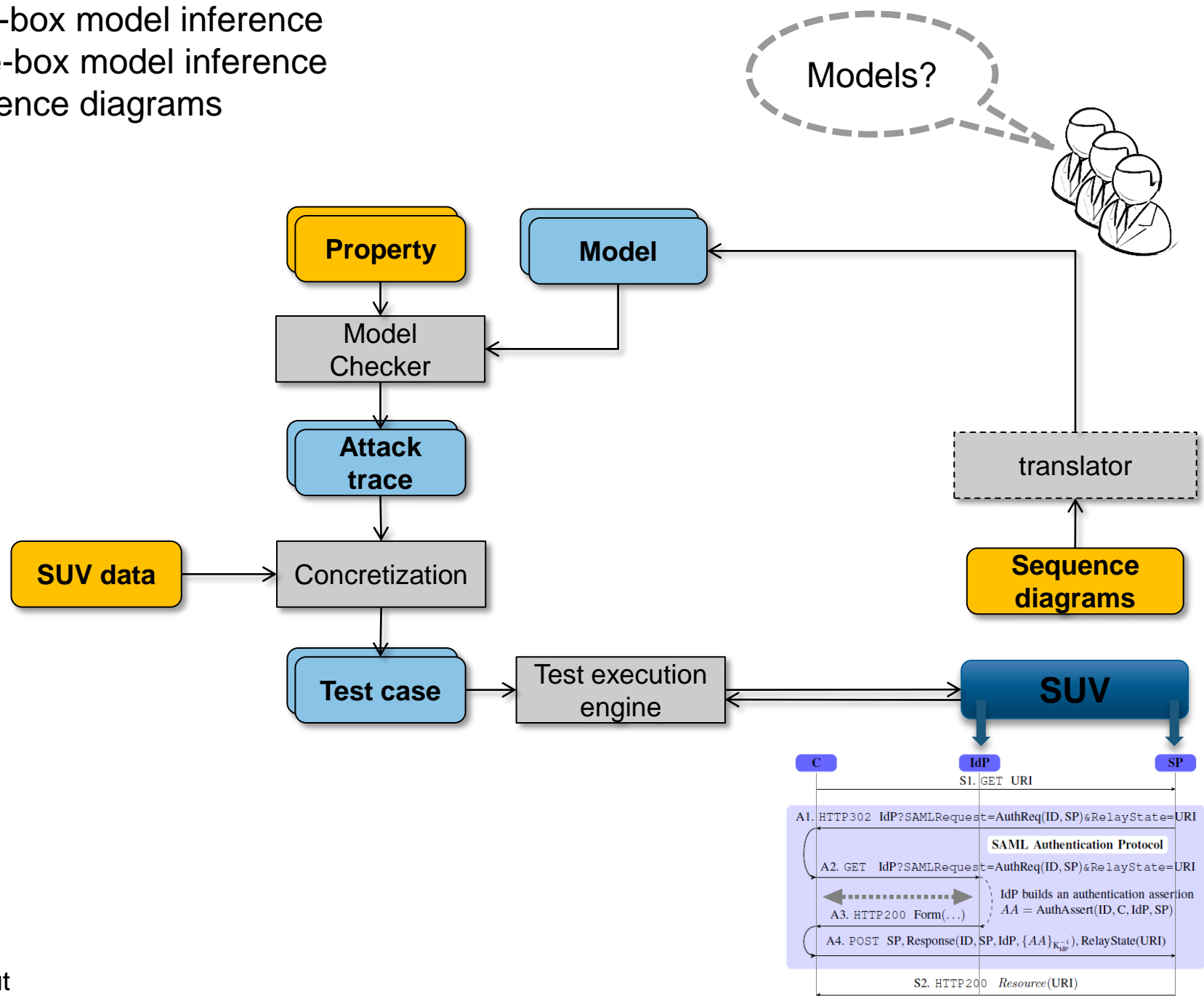
- Black-box model inference
- White-box model inference



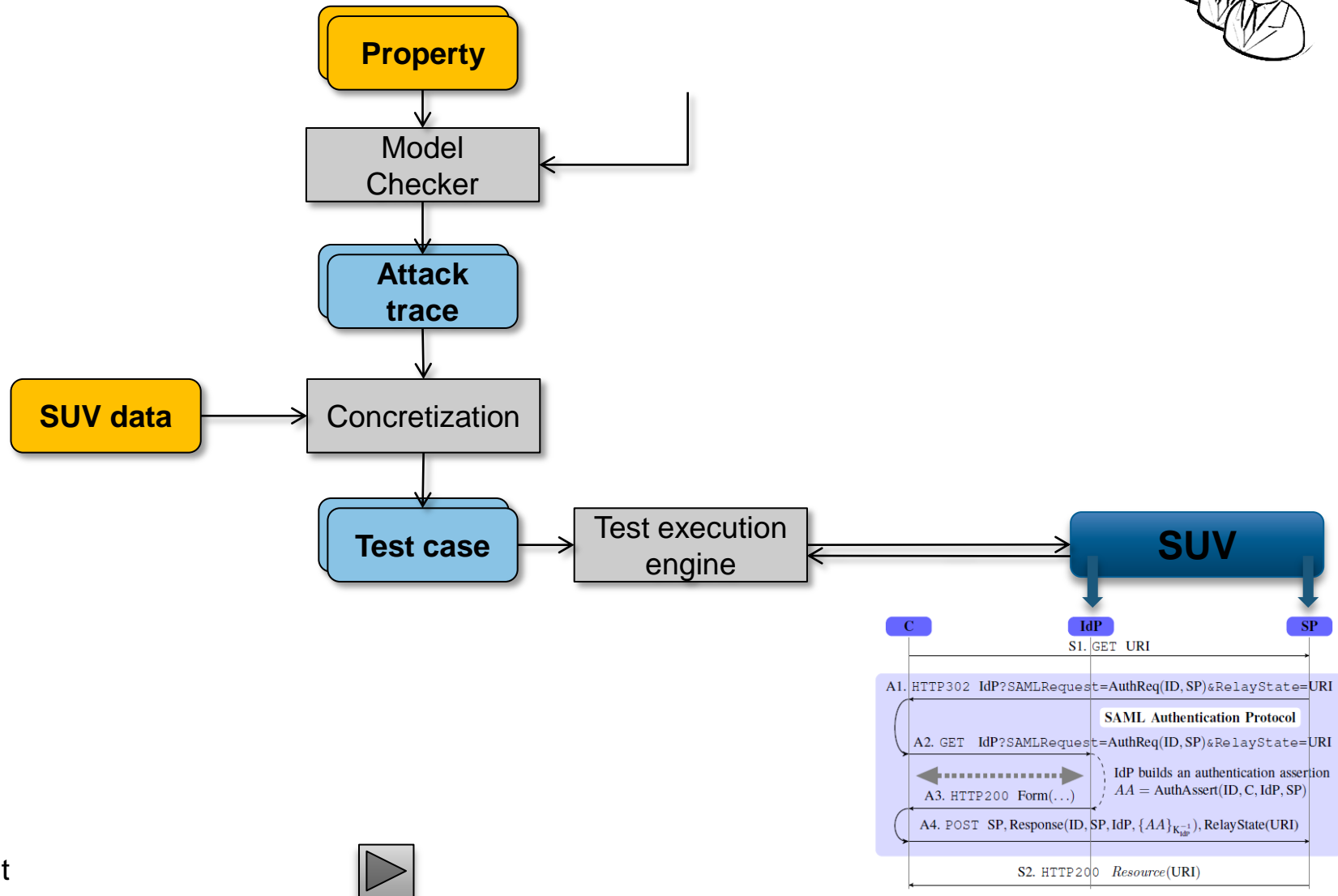
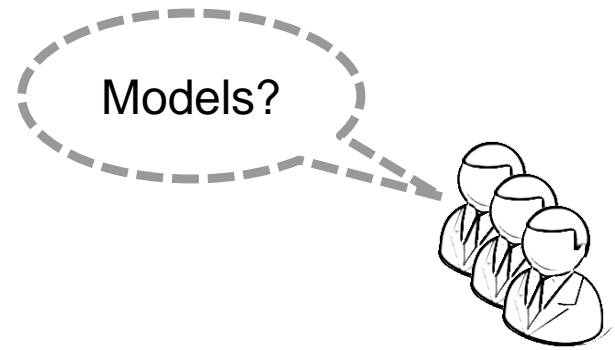
- Black-box model inference
- White-box model inference



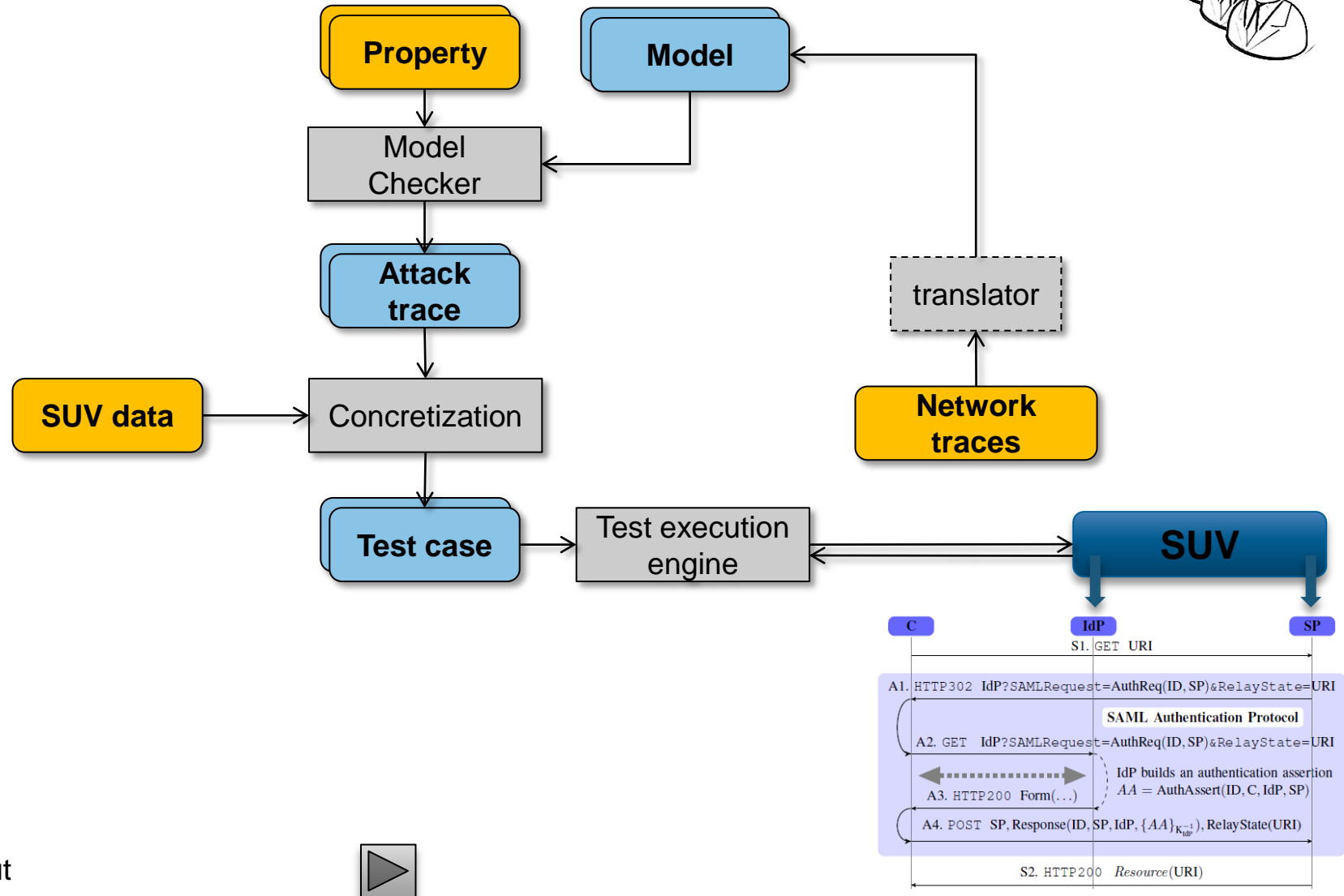
- Black-box model inference
- White-box model inference
- Sequence diagrams



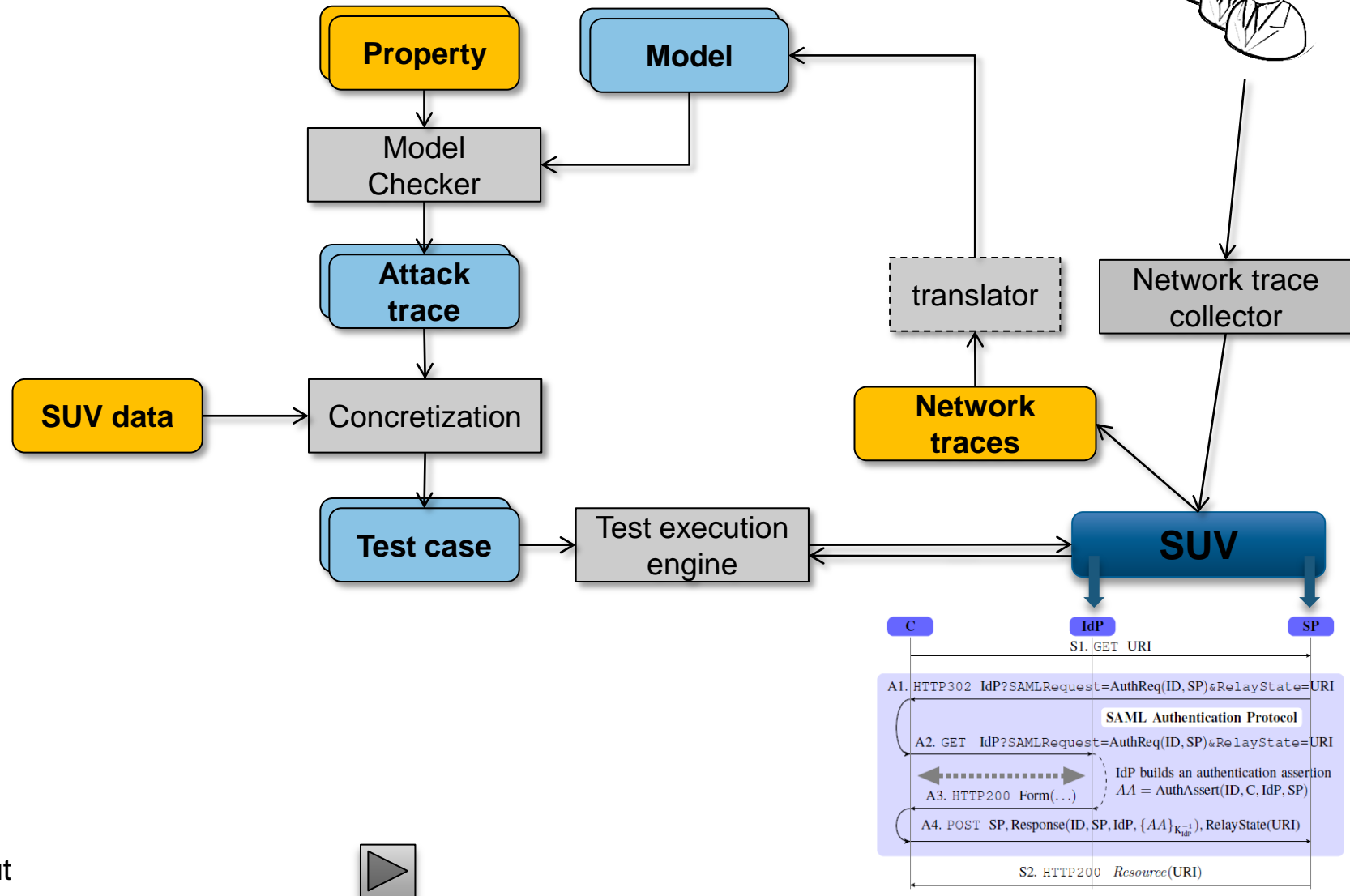
- Black-box model inference
- White-box model inference
- Sequence diagrams



- Black-box model inference
- White-box model inference
- Sequence diagrams
- Network traces

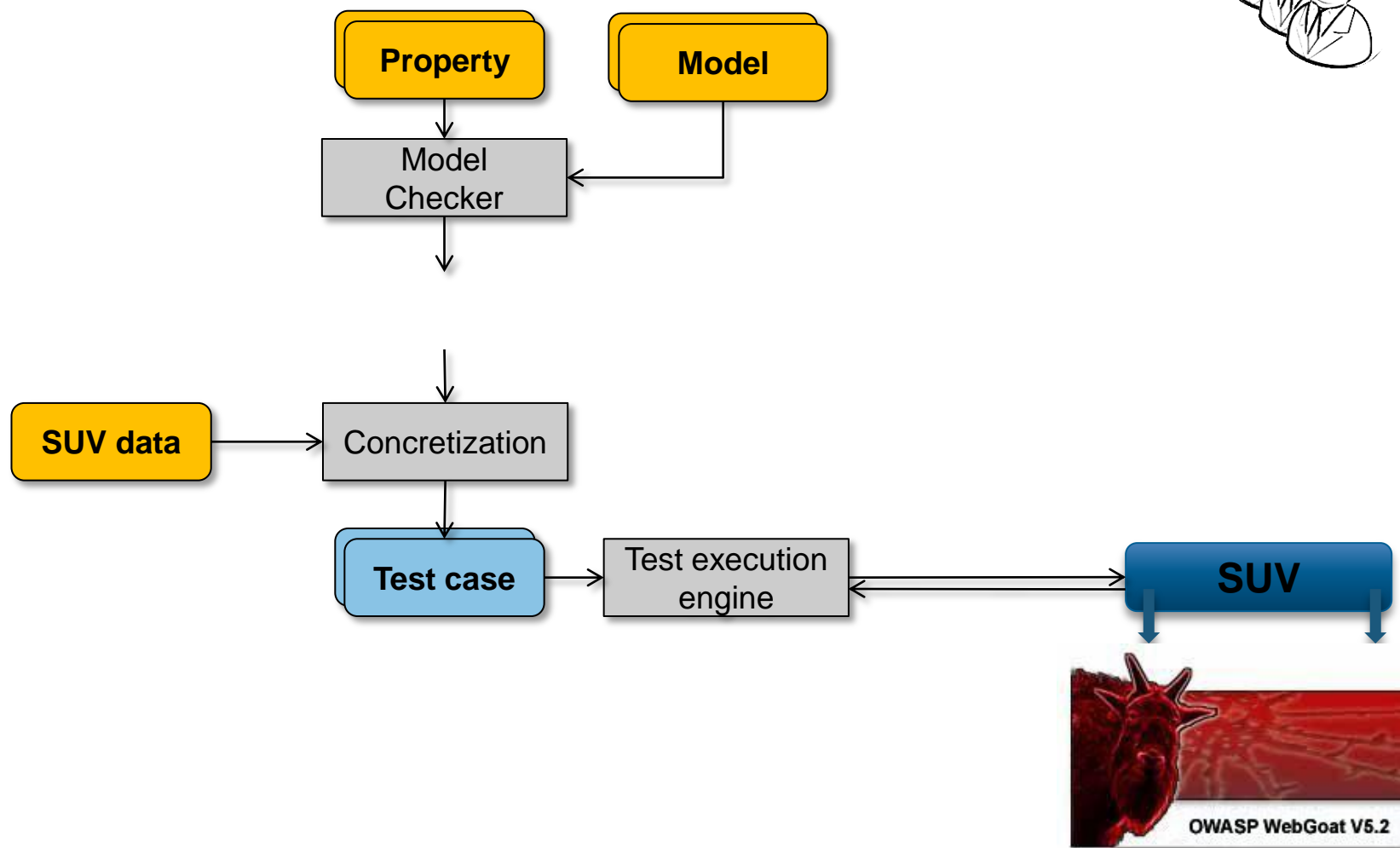
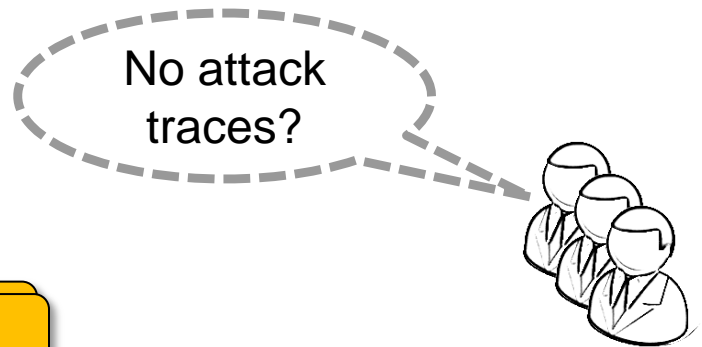



- Black-box model inference
- White-box model inference
- Sequence diagrams
- Network traces



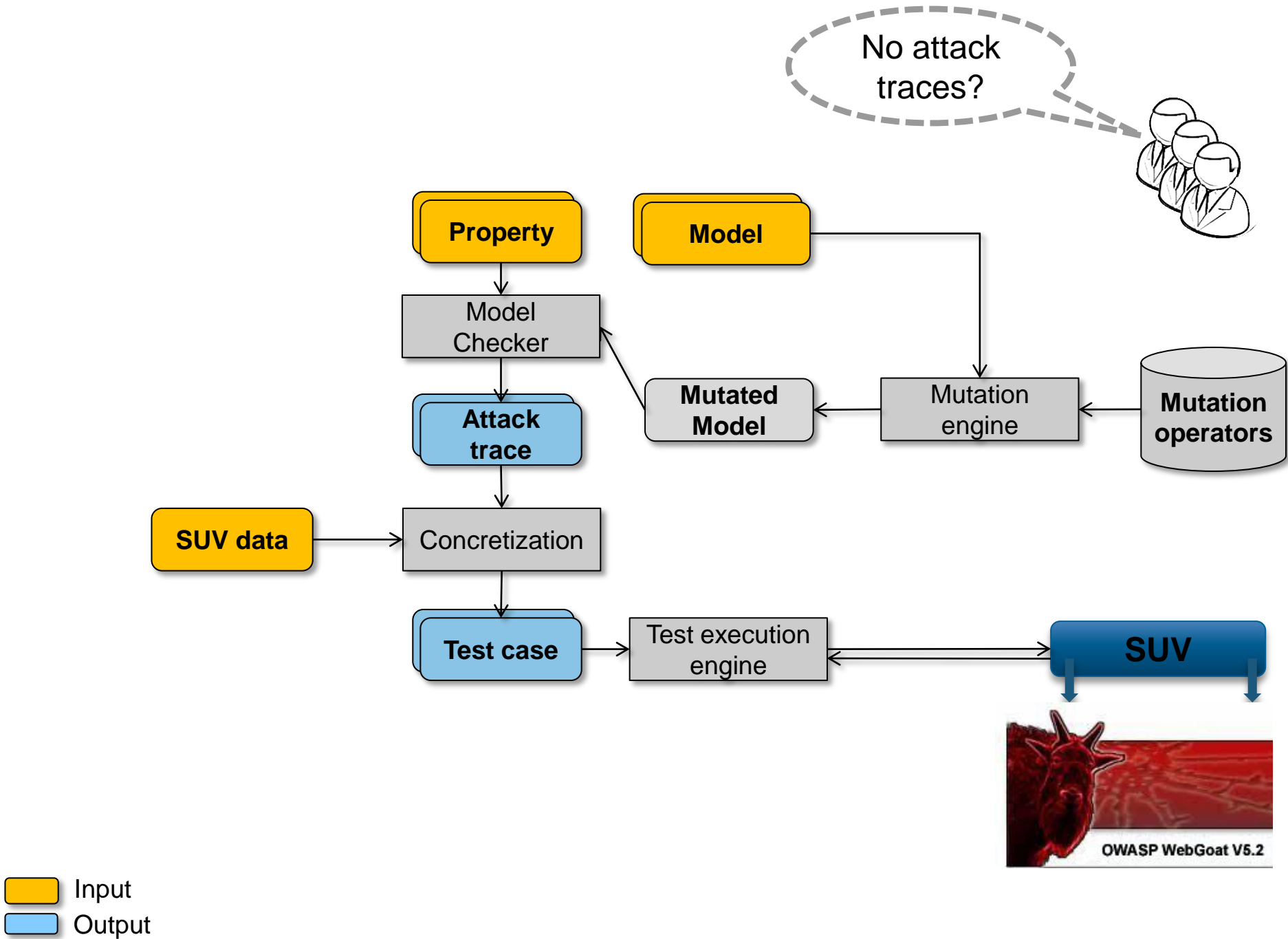
# **Use case 3**

**mutation-based testing**



 Input  
 Output



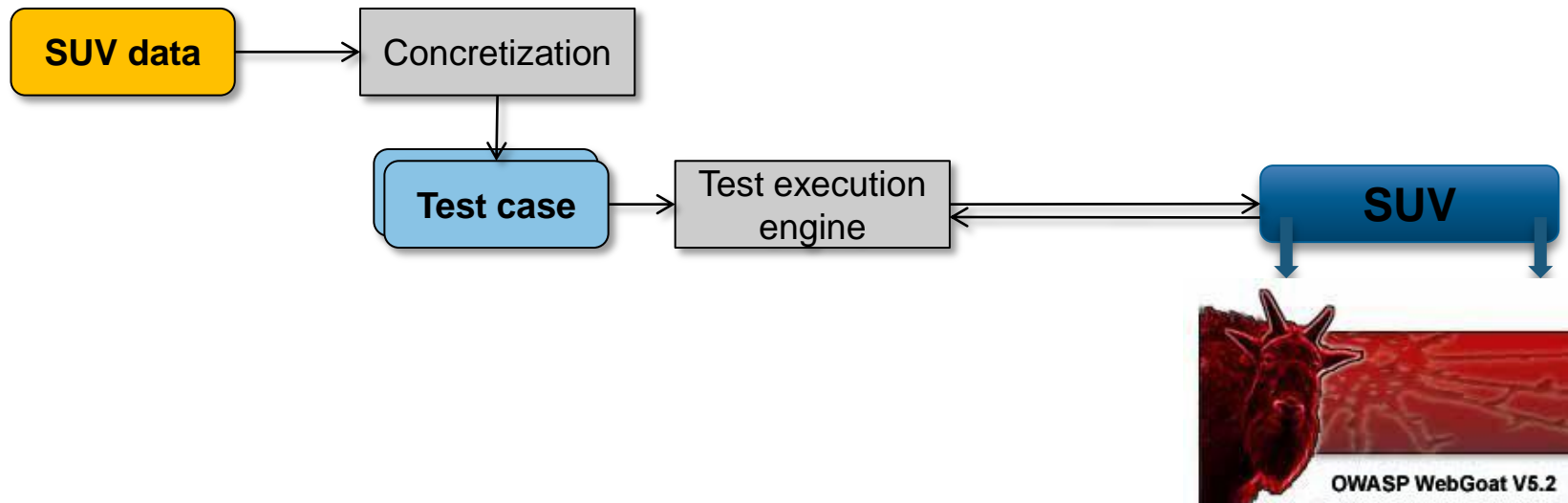
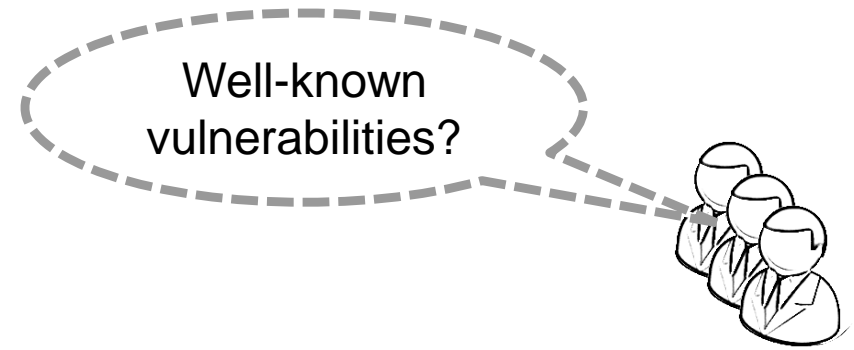


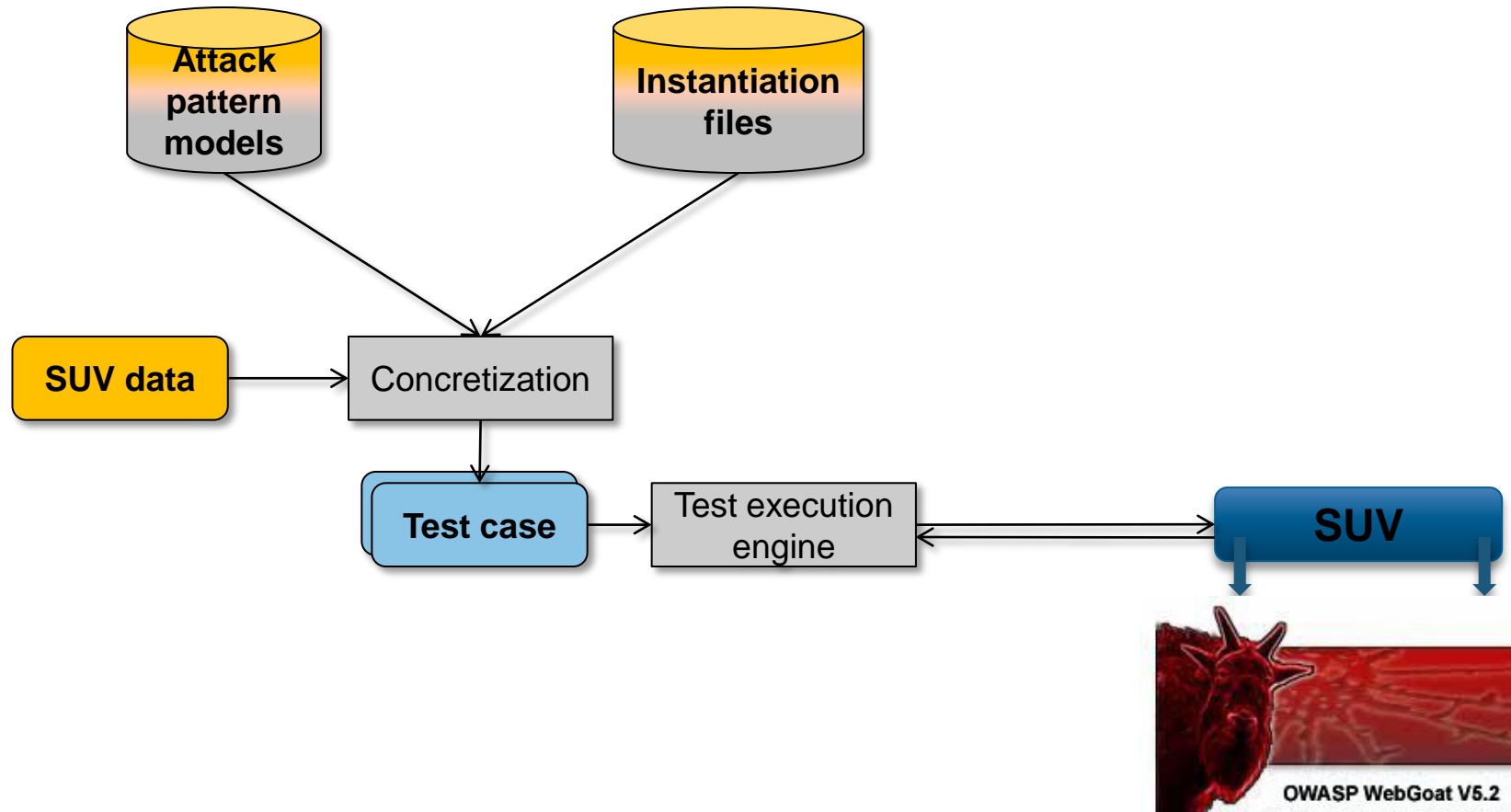
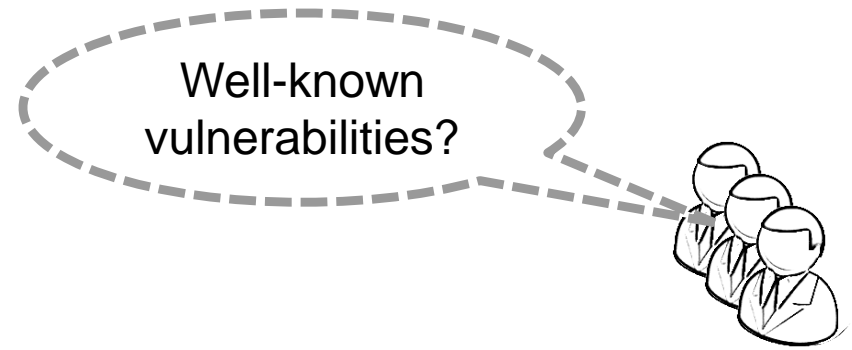
# Demo



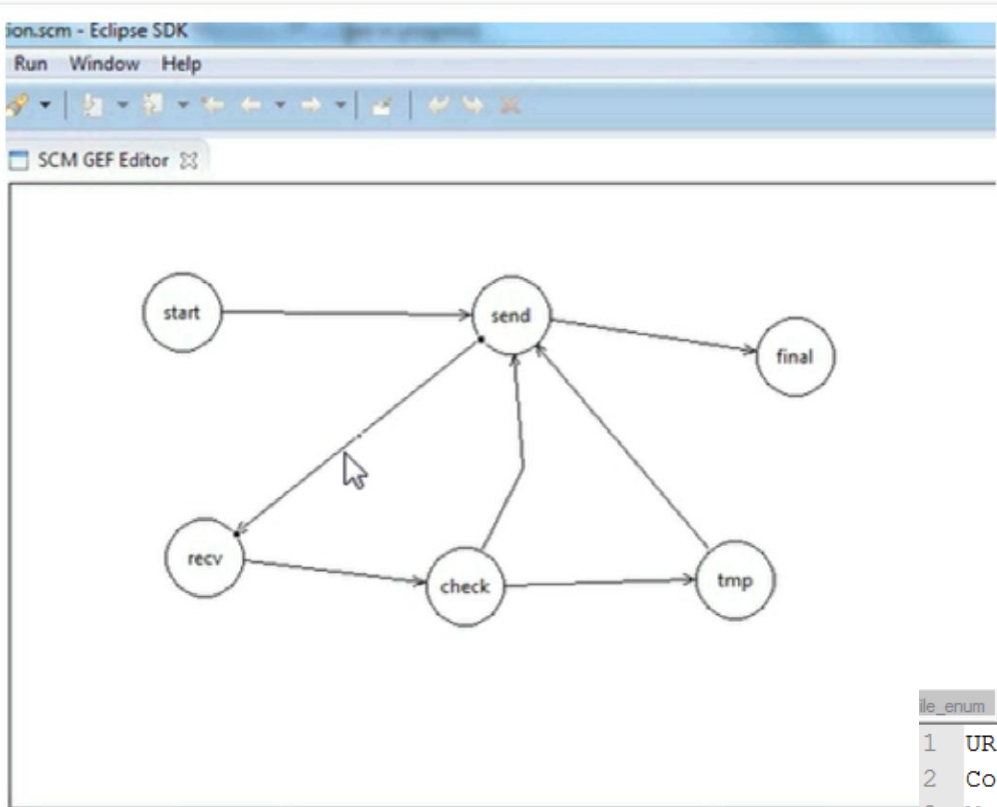
# **Use case 4**

## **vulnerability-driven testing**





# Attack Pattern + Instantiation file + SUV data



Properties

Property	Value
Guard	<code>i&amp;lt;i</code>
Input	
Output	<code>vHttp.snd(URL=IO[i].co</code>
Source	Node send
Target	Node recv

file\_enum

```
1 IO=[
2   ".htaccess",
3   ".htaccess.bak",
4   ".htpasswd",
5   ".meta",
6   ".web",
7   "conf",
8   "apache/logs/access.log ",
9   "apache/logs/access_log",
10  "apache/logs/error.log ",
11  "apache/logs/error_log",
12  "httpd/logs/access.log ",
13  "httpd/logs/access_log",
14  "httpd/logs/error.log ",
15  "httpd/logs/error_log",
16  "logs/access.log",
17  "logs/access.log ",
```

file\_enum webgoat.conf

```
1 URL="http://localhost:8086/WebGoat/attack?Screen=37&menu=20
2 Cookie="JSESSIONID=E6E32C706E8CC910AB0962DDE7FCC1FD"
3 Method="POST"
4 Fields1={'employee_id':'105', 'password':'tom', 'action':'L
5 Fields2={'action':'ViewProfile'}
6 Header1={'Content-Type': 'application/x-www-form-urlencoded
7 Header2={'Content-Type': 'application/x-www-form-urlencoded
8 # Bug in WebGoat: After complete the exercise, the success :
9 Control." will not be always showed, just when one load the
10 Check_Info=["Stage 4: Add Data Layer Access Control.", "Imp
11 Repeat stage 3. Verify that access to other employee's pro
```

# **Use case 5**

**Evolutionary fuzzing  
for filtered type-1 and 2 XSS**

**No time, next  
time?**

# Use case 6

## Testing based on Business logic patterns

No time, next  
time?





**Promising results**

	OWASP Top 10	The SPaCloS Tool
A1	Injection	WebGoat lesson: String SQL Injection WebGoat lesson: Numeric SQL Injection SIEMENS InfoBase and eHealth
A2	Broken Authentication & Session Management	SAML, OpenID, OAuth: e.g., authentication logic-flaws Password brute-forcing on SIEMENS InfoBase and eHealth
A3	Cross-Site Scripting	WebGoat lesson: Stored XSS WebGoat lesson: Reflected XSS SIEMENS InfoCase and eHealth
A4	Insecure Direct Object References	SIEMENS InfoBase and eHealth: File Enumeration and Path Traversal
A5	Security Misconfiguration	WebGoat lesson: Forced Browsing (File Enumeration)
A6	Sensitive Data Exposure	SAML, OpenID, OAuth: data confidentiality logic flaws
A7	Missing Function Level Access Control	WebGoat lesson: Bypass Business Layer Access Control, WebGoat lesson: Bypass Data Layer Access Control WebGoat lesson: Role Based Access Control SIEMENS eHealth
A8	CSRF	SIEMENS InfoBase and eHealth
A9	Using Components with Known Vulnerabilities	
A10	Unvalidated Redirects and Forwards	

# Some highlights

- SAML SSO authentication flaw and SAML ERRATA corrige
- Filtered type-1 and type-2 XSS that other scan tools were not able to find
- Shopping for free on several shopping cart web sites (to be published)
- Transfers to SAP and SIEMENS
  - Vulnerability-driven security testing approach applied on Web Apps at SIEMENS
  - Property- and vulnerability-driven approaches applied at SAP: on development of security standards and security core mechanisms

## Research prototype

- model checking
- security testing
- penetration testing
- ...

## Complements state-of-the-art

## Targets industrially-relevant Security Protocols & Web Apps

## Broad security range

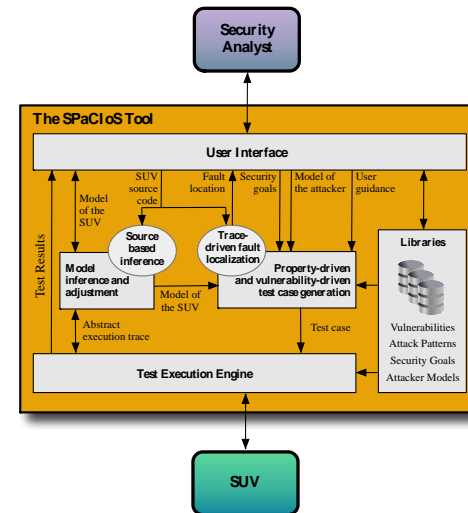
- logic-flaws, injections, AC, ...
- good coverage of OWASP top 10

## Promising results

- SAML SSO, OAuth2, ..
- WebGoat, Shopping Cart, ..

## On-going transfers to SAP and SIEMENS

# Thank you!



The SPaCloS Tool will be available for public download end of January 2013

<http://www.spacios.eu>