RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: CMI-W06

Jigsaw Puzzle Attack: A New Attack Method for Platform APPs

Yao Yao

Security Engineer of Ant Financial & Alipay Tian Chen Security Lab

Weiting Chen

Senior Security Researcher of Ant Financial & Alipay Tian Chen Security Lab

Agenda

- What is a platform app?
- What is a Jigsaw puzzle attack?
- How to conduct a Jigsaw puzzle attack on a platform app?
- How to defend against the jigsaw puzzle attack？

RSAConference2020 APJ

A Virtual Learning Experience

Platform App

Several Mainstream Platform Apps

2.6 billion+
Number of users

1.16 billion+
Number of users

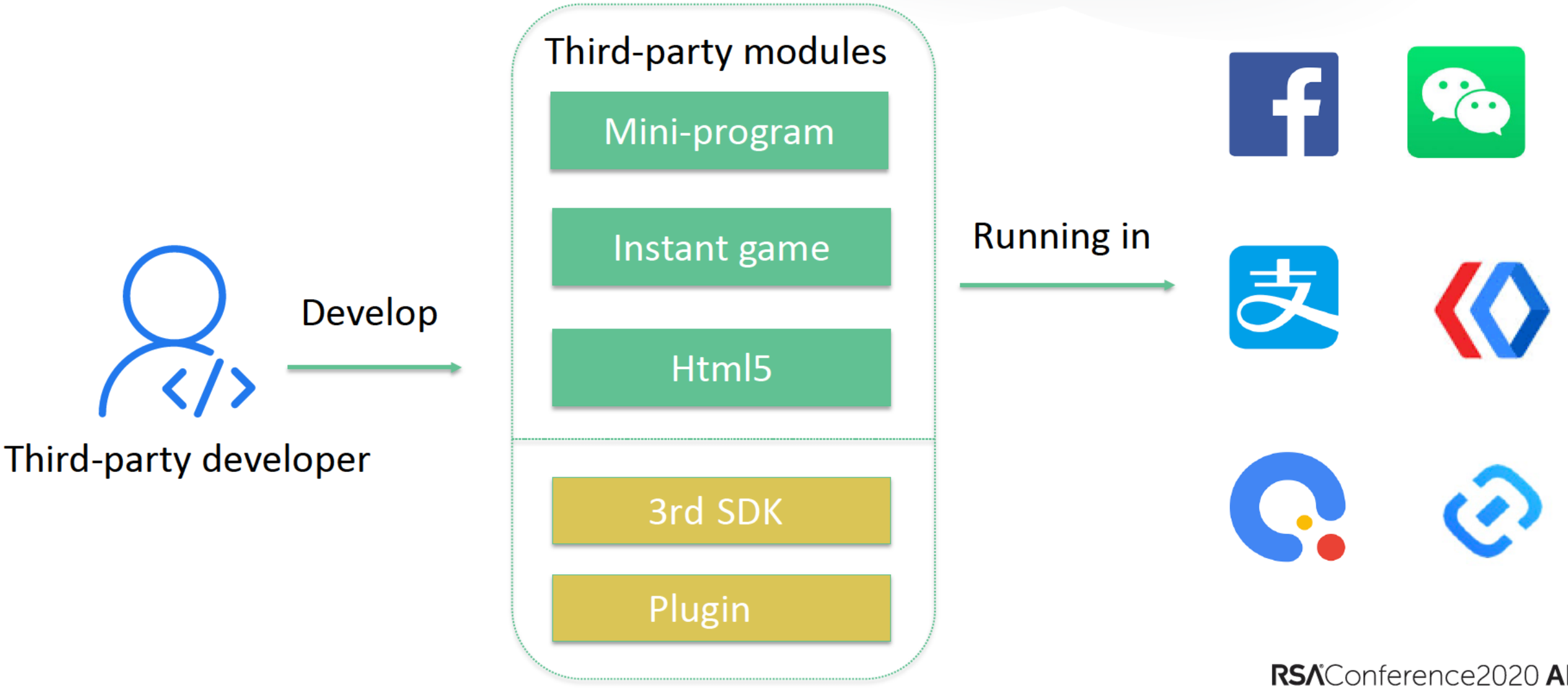
Mini-Programs

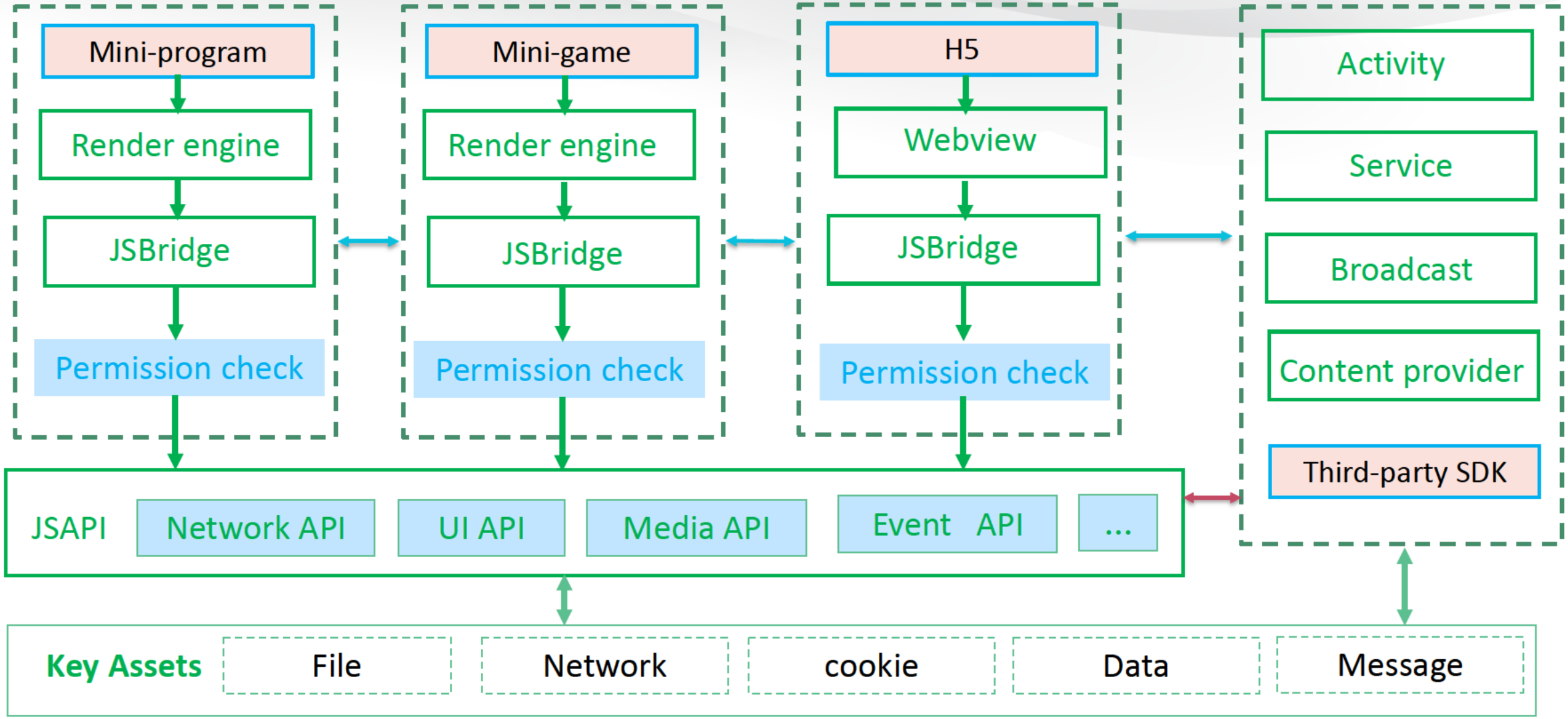
Instant Games

1.2 billion+
Number of users

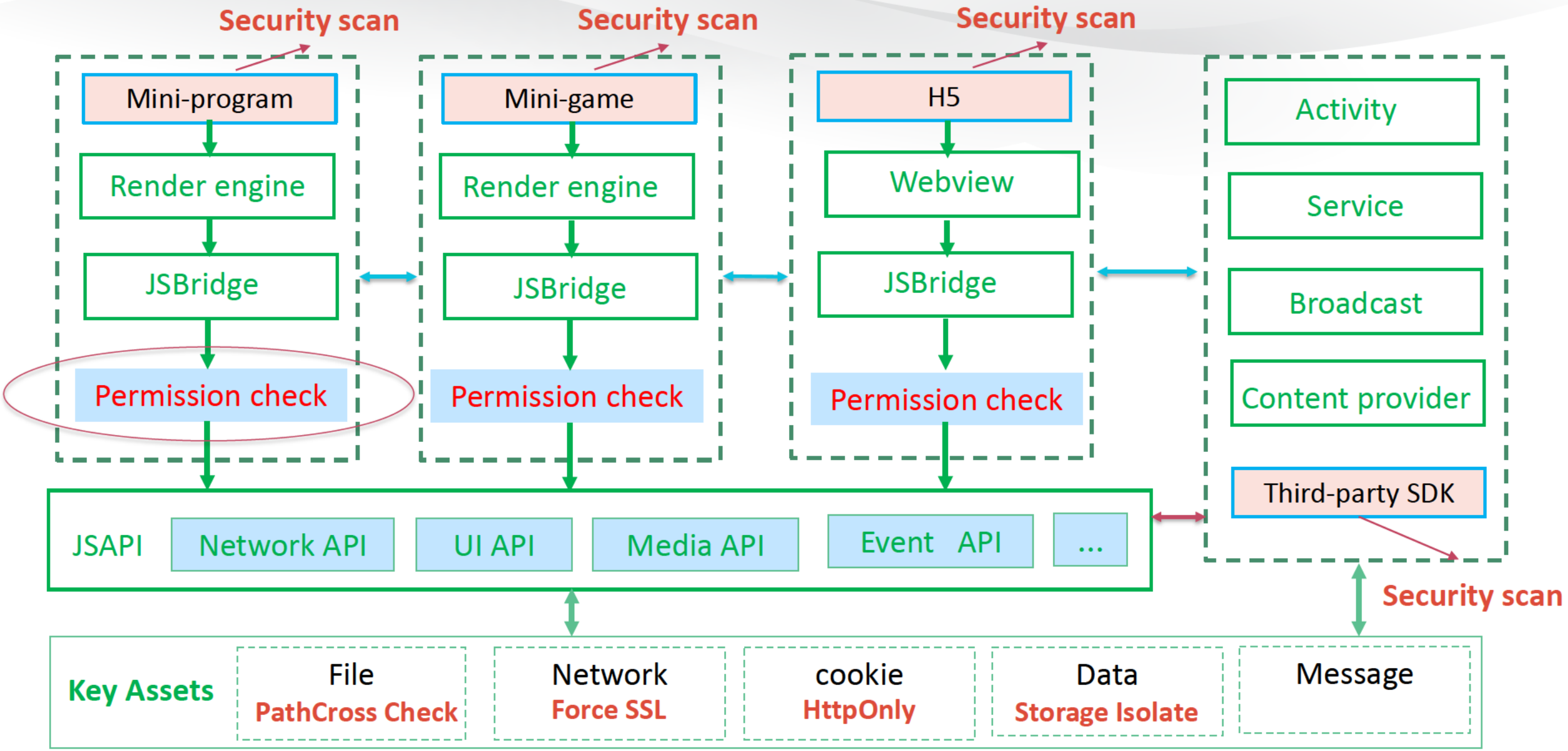
800 million+
Number of users

Like an operating system





Common Architecture of Platform Apps



Security Mechanism of Platform Apps

What is a Jigsaw puzzle attack?

Jigsaw Puzzle in the Platform App

A Puzzle Piece

Tabs

Can send https request

Can download a file

Can ...

Blanks

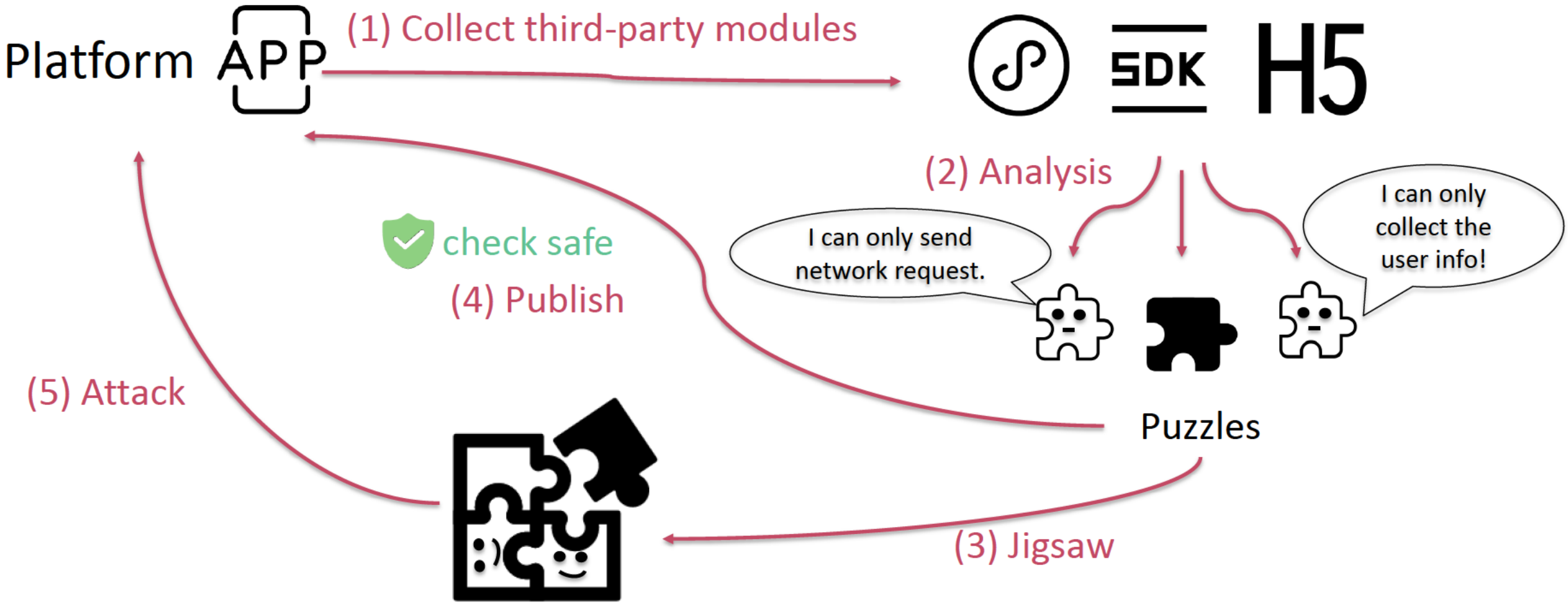
Cannot access local network

Cannot get cookie

Cannot ...

Jigsaw methods

Jigsaw Puzzle Attack Model



Jigsaw Puzzle Attack Type

- Common
  - Malicious developers can introduce low-level risks codes into platform apps and combine these low-risk vulnerabilities into high-risk by taking advantage of different third-party modules.
- Novel
  - Malicious developers could develop flawless and scan-safe code to conduct attacks based on existing capabilities of different third-party modules.

RSAConference2020 APJ
A Virtual Learning Experience

How to conduct a Jigsaw puzzle attack on a platform app?

Identify explicit tabs and blanks of third-party modules

Download

Demo

Instrumentation


```
console.log({'api_name':'httpRequest'});
console.log({'param_type_list':['url','method','da
console.log({'param_value_list':{'url':'https://t
console.log({'return_type_list':['res']})
Call.httpRequest({
  url: 'http://test.com',
  method: 'POST',
  data: {
    from: 'test',
    production: 'test_demo',
  },
  dataType: 'json',
  success: function(res) {
    console.log('success',res);
  },
  fail: function(res) {
    console.log('fail',res);
  }
});
```

Instrumentation

Instrumentation

Output: Error

Blanks

Output: Success

Tabs

Identify explicit tabs and blanks of third-party modules

```
...
Call.request({
url: 'https://test.com',
method: 'POST',
...
```

Success

Tabs: send https network data

```
...
Call.saveFile({
filePath: tempFilePath,
...
```

Success

Tabs: write file into sdcard

Transform the key parameter value

- url
- filepath
- data
- db

```
...
Call.request({
url: 'http://192.168.XX',
method: 'POST',
...
```

Success

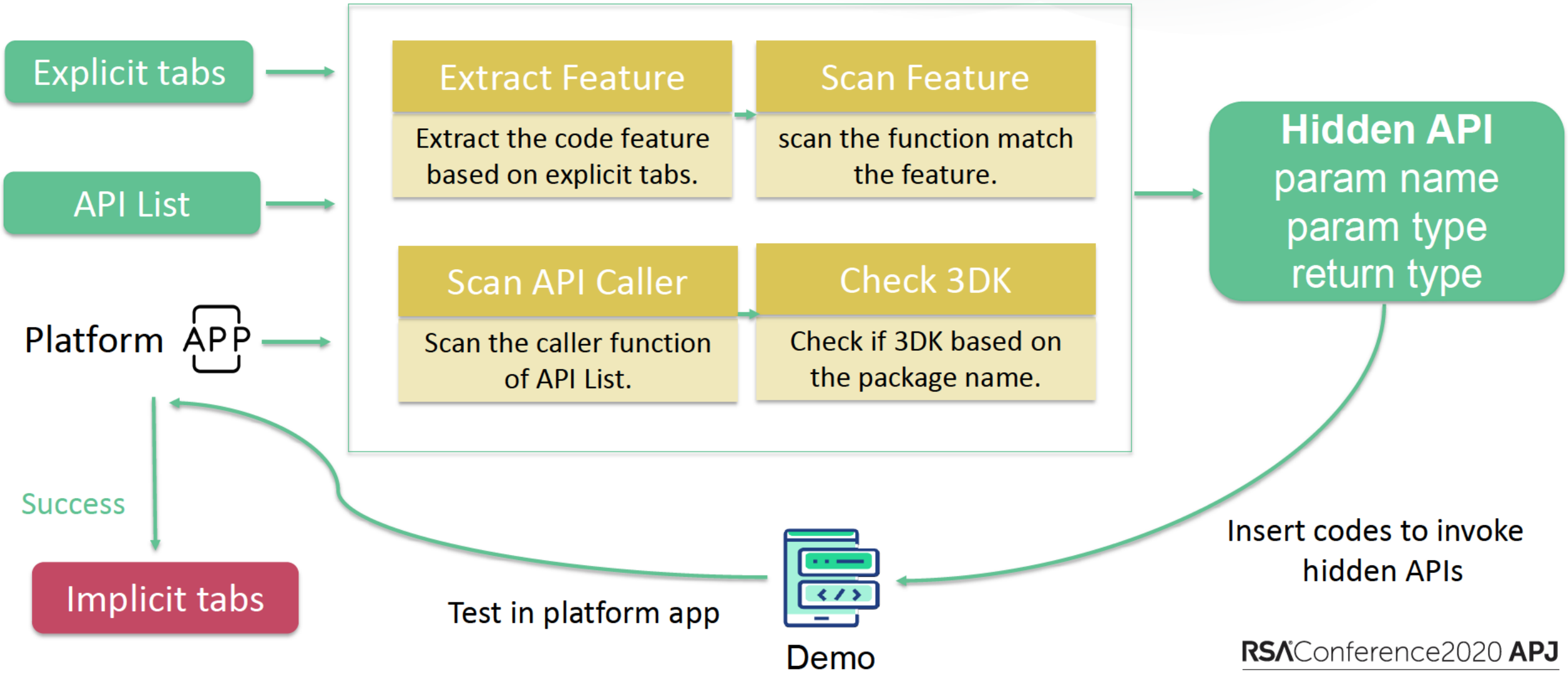
Tabs: access local network

```
...
Call.saveFile({
filePath:'/data/data/...',
...
```

Success

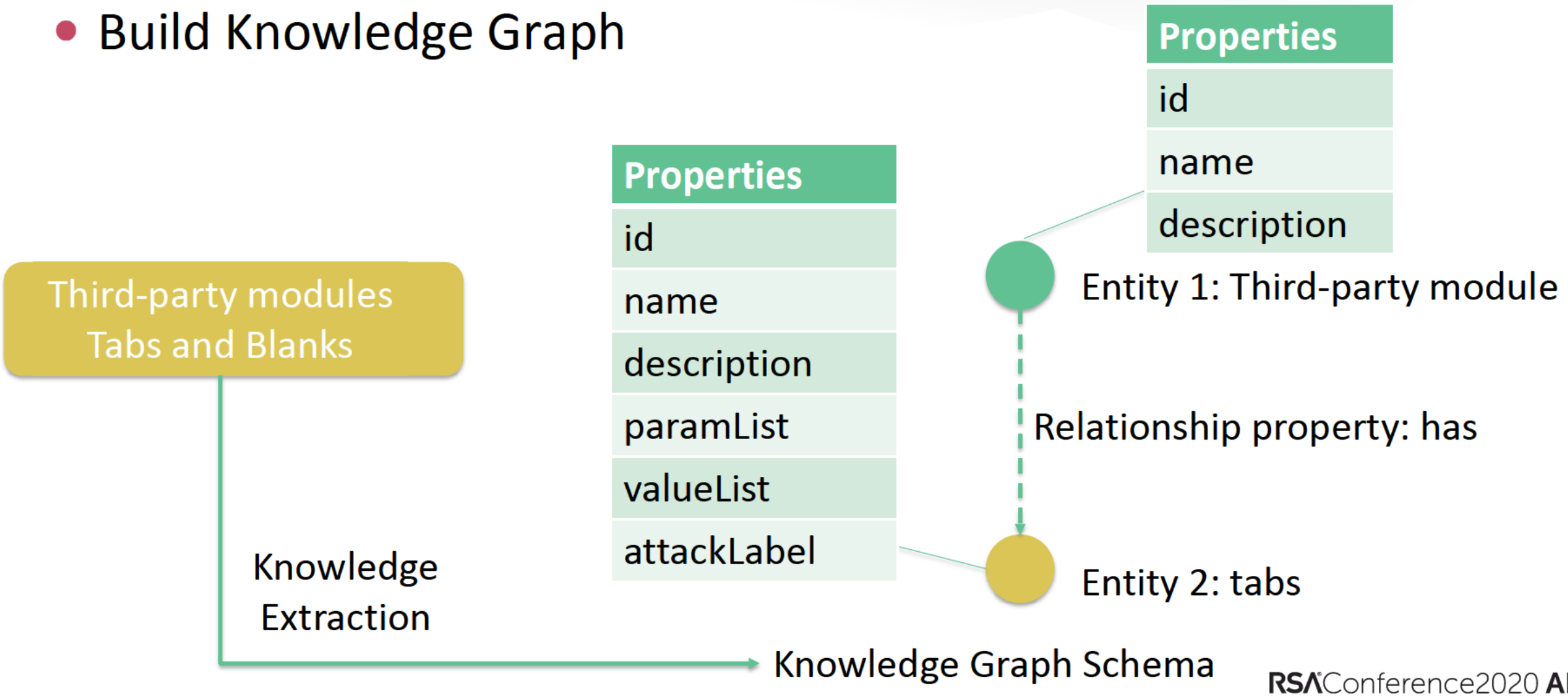
Tabs: write file into private dir

Identify implicit tabs of third-party modules



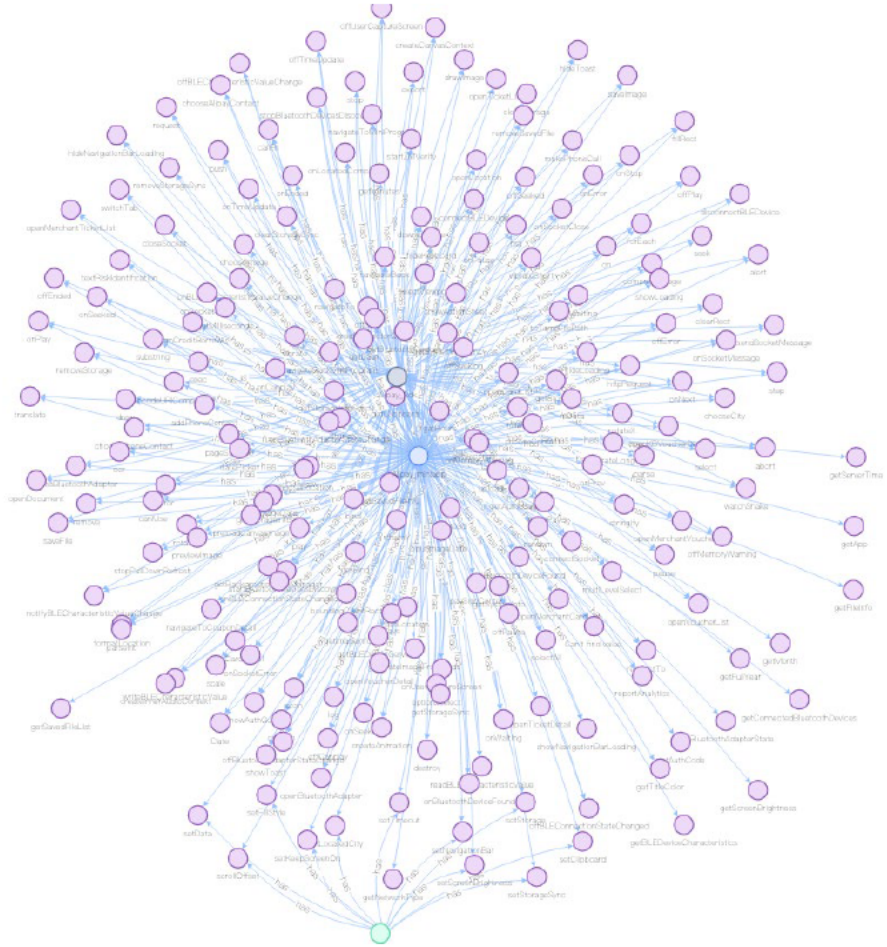
Infer the jigsaw methods leading to an attack

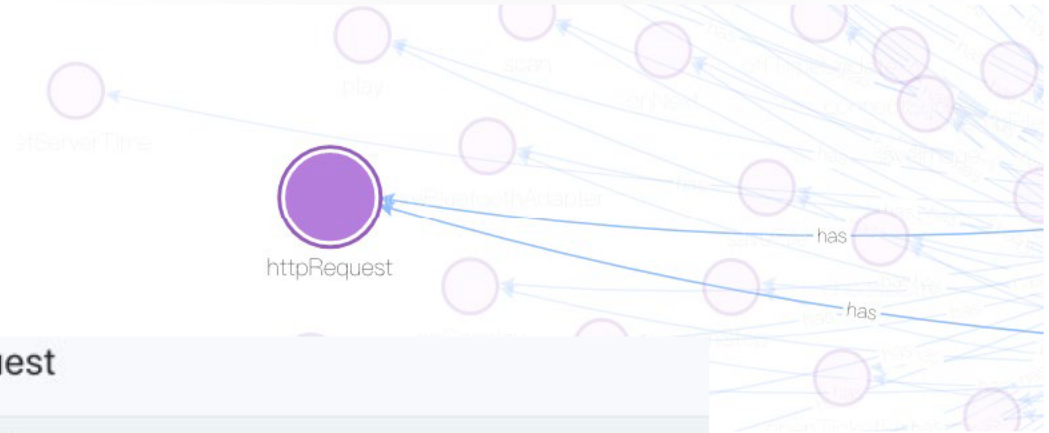
- Build Knowledge Graph



Infer the jigsaw methods leading to an attack

- Build Knowledge Graph





httpRequest

▼ Basic info

type: ASC.Tabs(Tabs)

▼ Attribute

name(名称)	httpRequest
attackLabel(攻击标识)	['Exfiltration']
id(实体主键)	httpRequest
paramList(参数)	['success', 'url', 'dataType', 'fail', '
retList(返回值)	[]

Infer the jigsaw methods leading to an attack

- What attacks can tabs be used for?

MITRE | ATT&CK®

A Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

ATT&CK Matrix for Enterprise

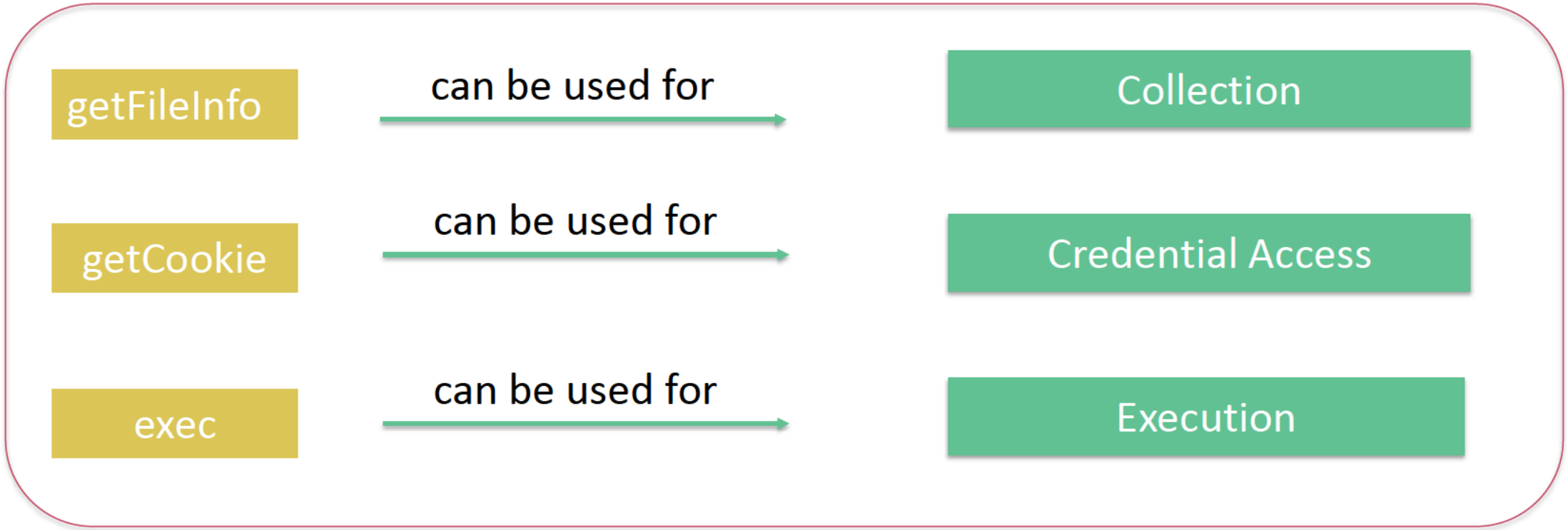
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement

Attack Tactics

- Execution
- Credential Access
- Collection
- Command and Control
- Exfiltration

Infer the jigsaw methods leading to an attack

- We label the tabs with attack tactics.

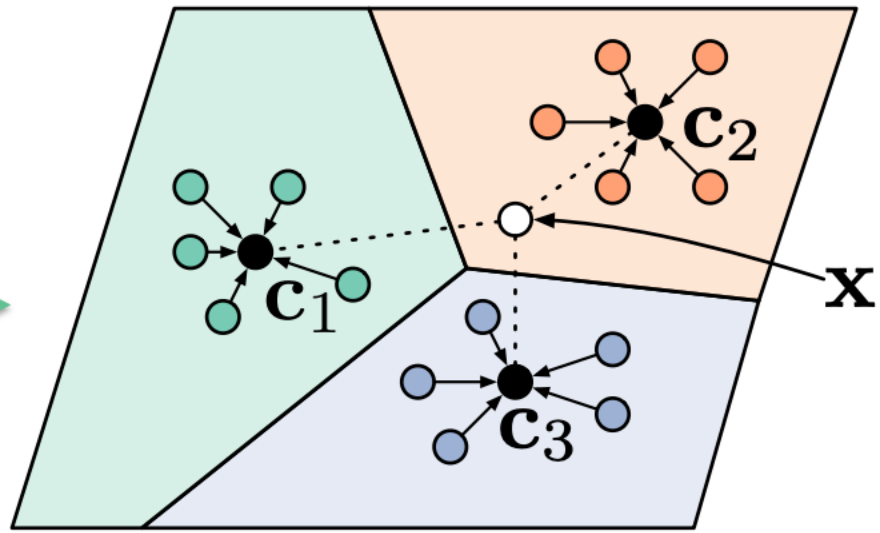


Infer the jigsaw methods leading to an attack

- Label tabs with attack tactics

(name,param,ret)

embed



label

Attack Tactics

Tabs -> X

Attack Tactic -> c

$$\mathbf{c}_k = \frac{1}{|S_k|} \sum_{(\mathbf{x}_i, y_i) \in S_k} f_{\phi}(\mathbf{x}_i) \qquad p_{\phi}(y = k \mid \mathbf{x}) = \frac{\exp(-d(f_{\phi}(\mathbf{x}), \mathbf{c}_k))}{\sum_{k'} \exp(-d(f_{\phi}(\mathbf{x}), \mathbf{c}_{k'}))}$$

Prototypical Networks for Few-shot Learning

Infer the jigsaw methods leading to an attack

- Rule-based Reasoning
- An inference rule for discovering privacy leaks：

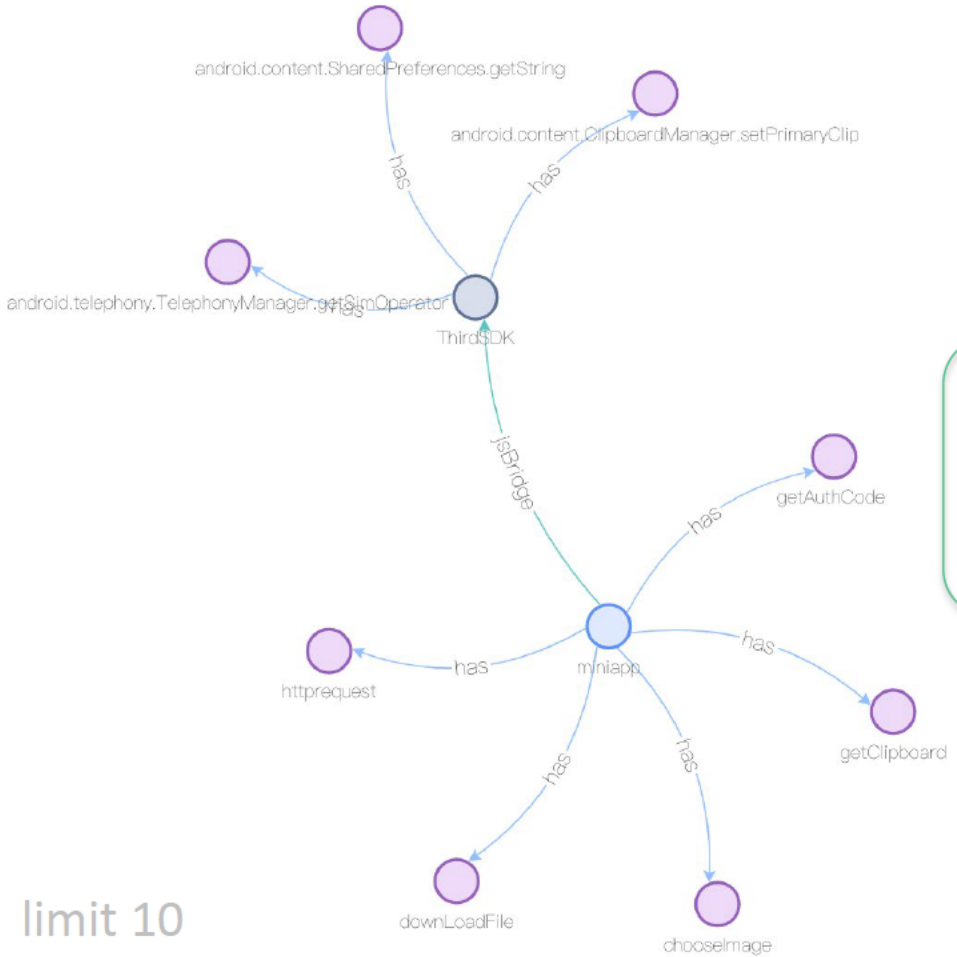
```
GraphStructure {
  A, B [Tabs]
  C [Miniapp]
  D [ThirdSDK]
  C->A [has]
  D->B [has]
  C->D [jsBridge]
}
```

```
Rule{
  R1: A.attackLabel in ["['Collection']", "['Exfiltration']" ]
  R2: B.attackLabel in ["['Collection']", "['Exfiltration']" ]
}

Action{
  get(A.name,B.name)
}
```

Infer the jigsaw methods leading to a vulnerability

- Data characteristics correlation analysis of different tabs



limit 10

Mini app
[chooseImage(param,ret), getClipboard(param,ret)...]

3DK
android.telephony.TelephonyManager.getSimOperator

query

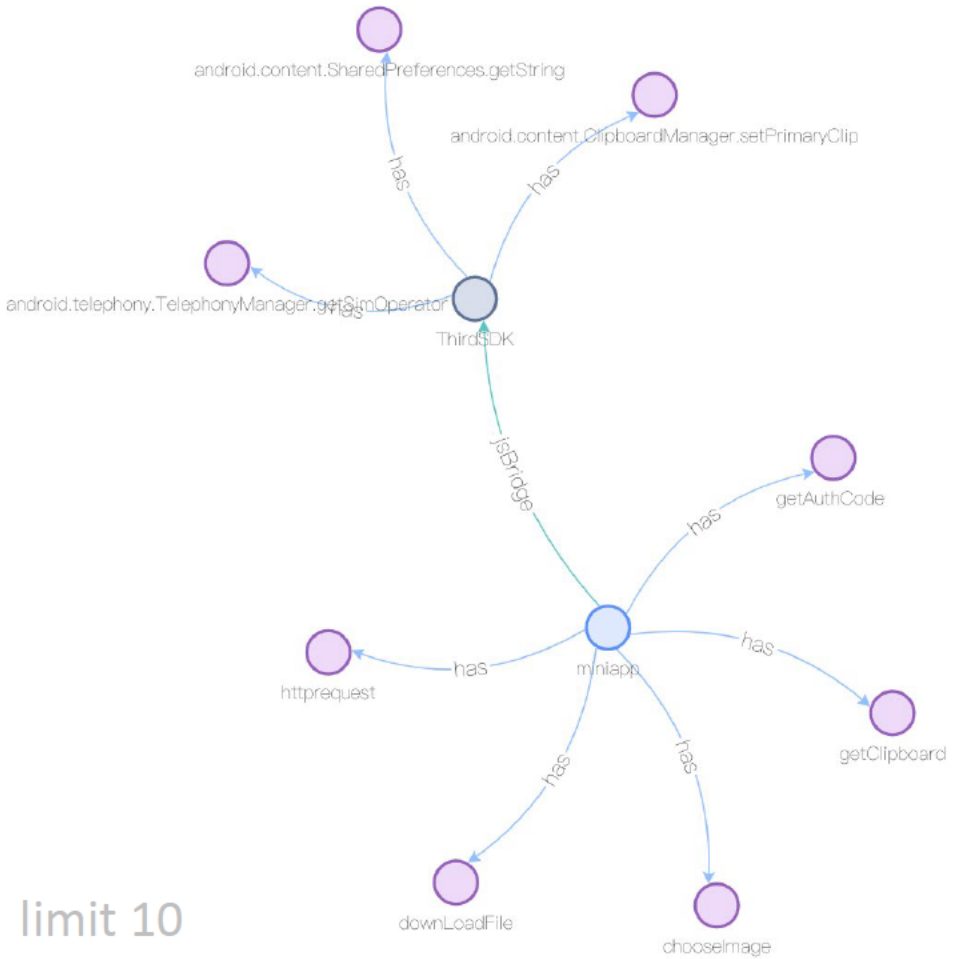
BM25-Ant Algorithm

Get most relevant

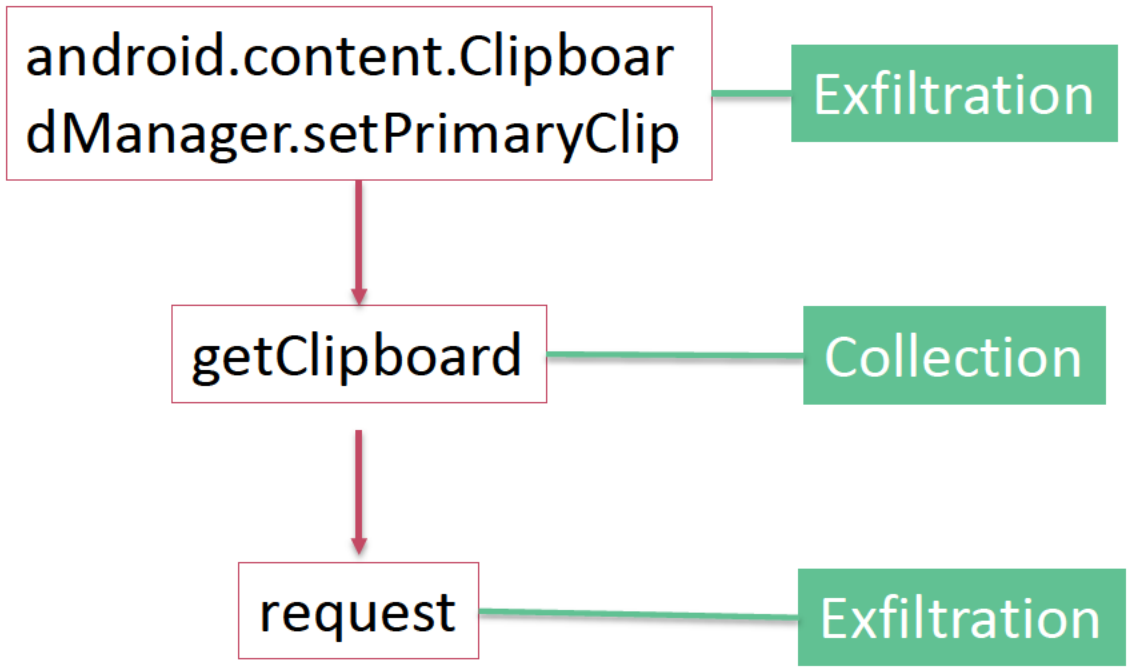
[getClipboard(param,ret)]

Infer the jigsaw methods leading to an attack

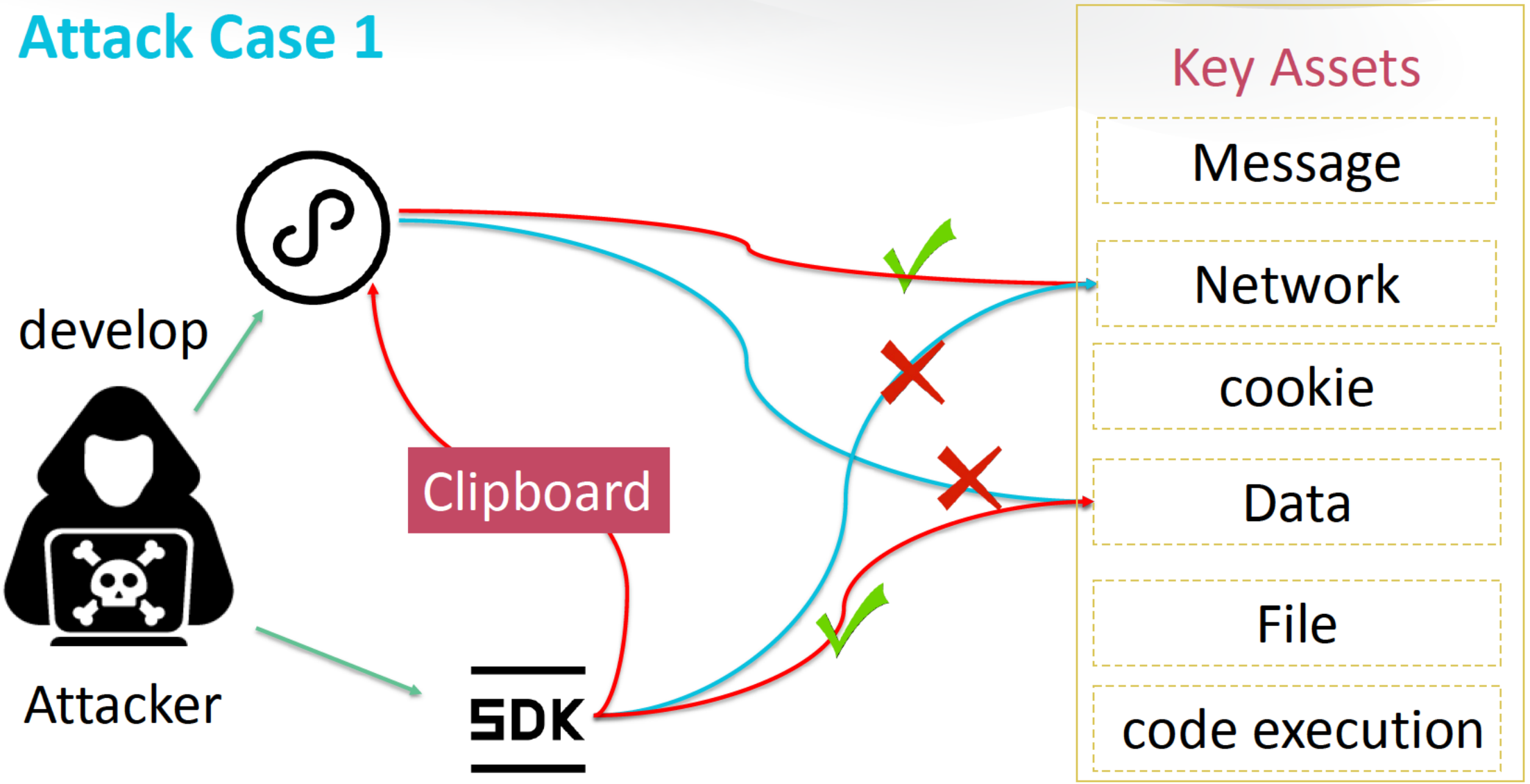
- Rule-based Reasoning



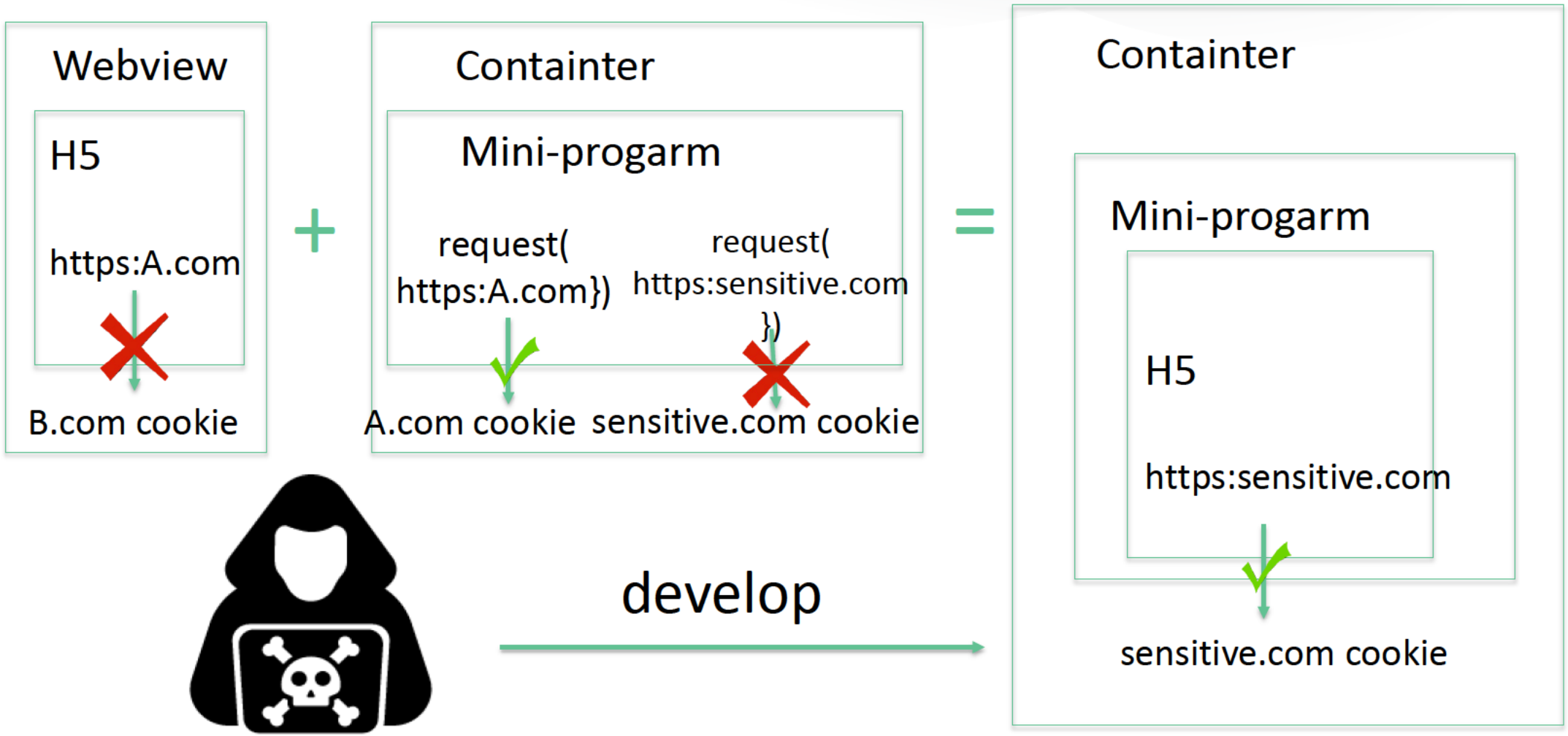
limit 10



Attack Case 1



Attack Case 2



RSAConference2020 APJ
A Virtual Learning Experience

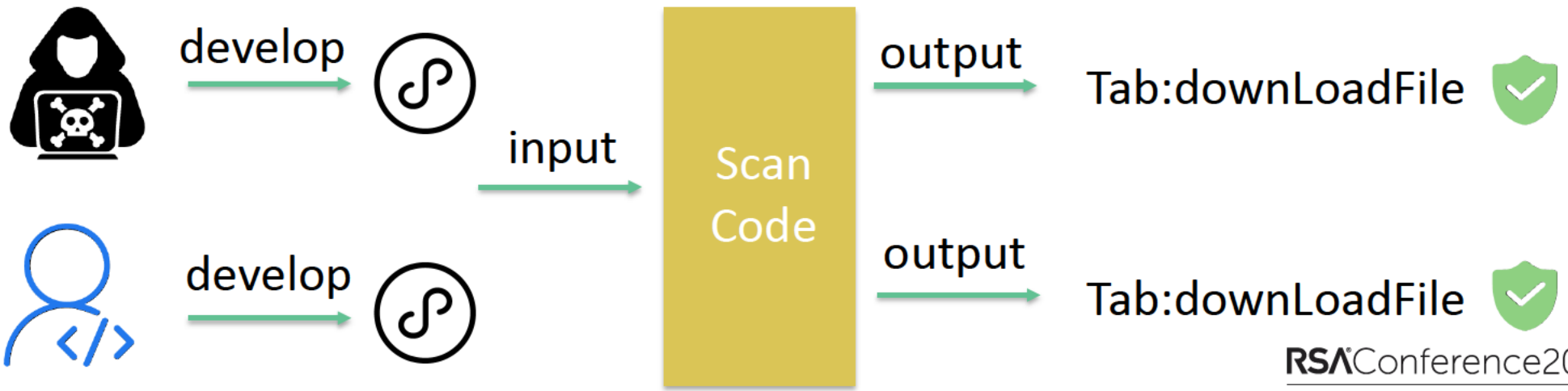
How to defend against the jigsaw puzzle attack?

Key notes

- The security mechanism of the operating system is also applicable on the platform app：
  - Principle of Least Privilege.
  - Access control.
  - Security audit mechanism.
  - Secure transmission and storage of sensitive data.

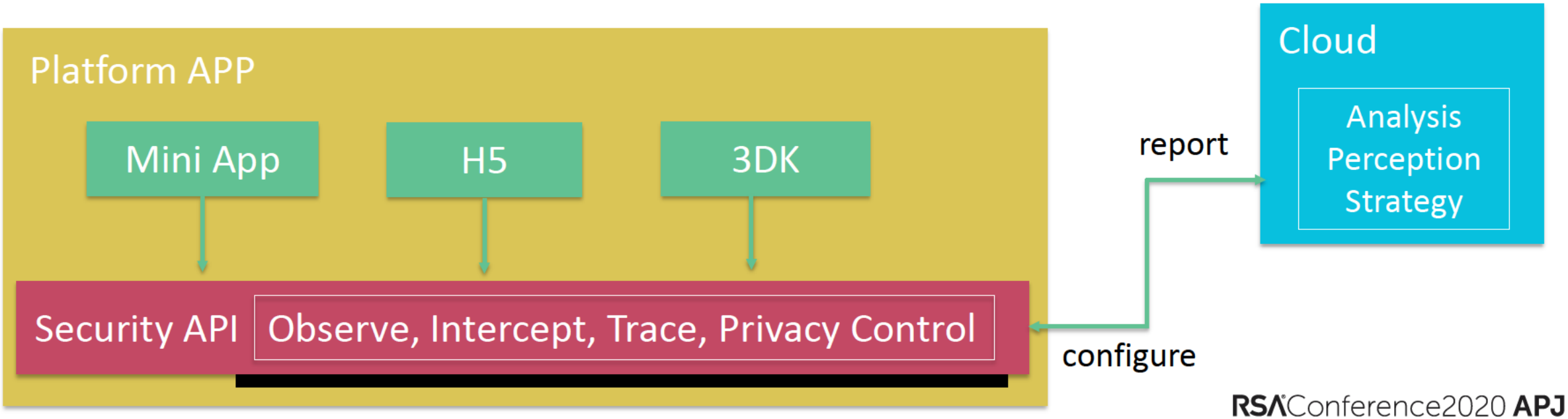
Defense scheme for jigsaw puzzle attack

- It is difficult to statically identifying this type of risks.
- Reasons:
  - It is hard to distinguish between unintentional jigsaw and intentional jigsaw.
  - It is hard to obtain the dynamic parameters.



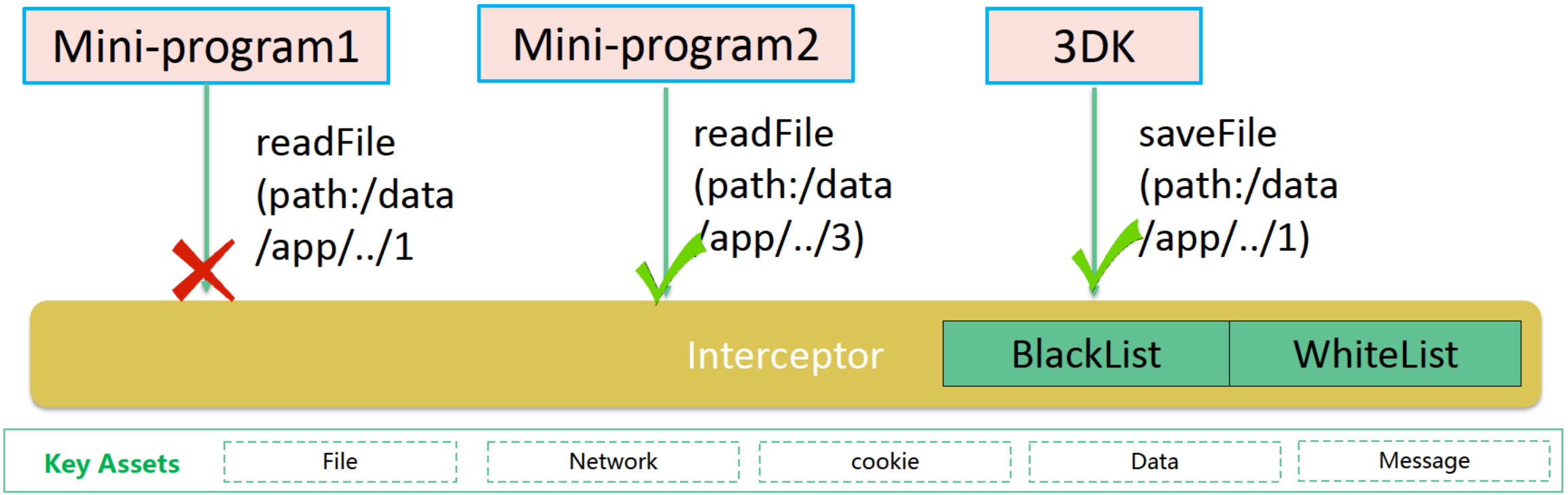
Defense scheme for jigsaw puzzle attack

- Ant Security Aspect Defense System
  - Based on AOP (Aspect Oriented Programming)
  - Inside observe each fine-grained invoke chain of API.
  - Intercept the attack behaviors in real time.



Defense scheme for jigsaw puzzle attack

- Security policy + Dynamic interception



Apply What You Have Learned Today

- Next week you should:
  - Identify all third-party modules within your application.
- In the first three months following this presentation you should:
  - Sort out the "tabs" and "blanks" of each third-party module within your application.
  - Use Security Experience and Machine Learning to identify the jigsaw methods that maybe lead to a vulnerability.
  - Learn to adopt the AOP to implement a comprehensive security defense scheme to protect against the harm brought from third-party code.

Thank you !