Misdirection of Trust: Demystifying the Abuse of Dedicated URL Shortening Service

Zhibo Zhang, Lei Zhang, Zhangyue Zhang, Geng Hong,
Yuan Zhang, Min Yang

Fudan University

URL Shortening Service (USS)

- Purpose
  - Simplifies **link sharing** and enables **user tracking**
- Popularity of USS
  - Case 1 [Bitly]: serves over **100 million URLs**
  - Case 2 [google firebase link]: Powers over **30% of mobile apps**

Benefit

- fit the limited mobile screen
- memorable, recognizable

Shared ? Dedicated !

Option 1

Shared URL Shortening Service (SUSS)

- **Low cost**: free, fixed domain name(e.g., *bit.ly*)
- **Low security**: no limit on users

becomes notorious:

Option 2

Dedicated URL Shortening Service (DUSS)

- **High reputation**: a brand domain name
- **High security**: only serves trusted URLs

a popular trend:

walmrt.us	*amzn.to*	… …	*go.shell.com*

Shared ? Dedicated !

Option 1

Shared URL Shortening Service (SUSS)

- **Low cost**: free, fixed domain name(e.g., *bit.ly*)
- **Low security**: no limit on users

becomes notorious:

Option 2

Dedicated URL Shortening Service (DUSS)

- **High reputation**: a brand domain name
- **High security**: only serves trusted URLs

a popular trend:

walmrt.us	*amzn.to*	… …	*go.shell.com*
… …	… …	… …	… …

Crucial question:
whether DUSSs implement adequate security measures?

Misdirection Attack

- Definition
  - Misdirection attacks **redirect security focus** from an untrusted entity to one perceived as trustworthy, compromising
    - online social network users
    - applications with domain-based checker (e.g., mobile applink verification)
- Threat Model
  - **Web Attacker**: Compromises vulnerable DUSS to serve **malicious URLs**
  - **Victim Users**: Online users or those using impacted applications

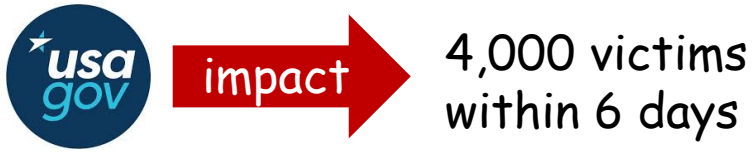

Home / News / Security News

NEWS

Spammers abuse .gov URL shortener service in work-at-home scams

By Lucian Constantin

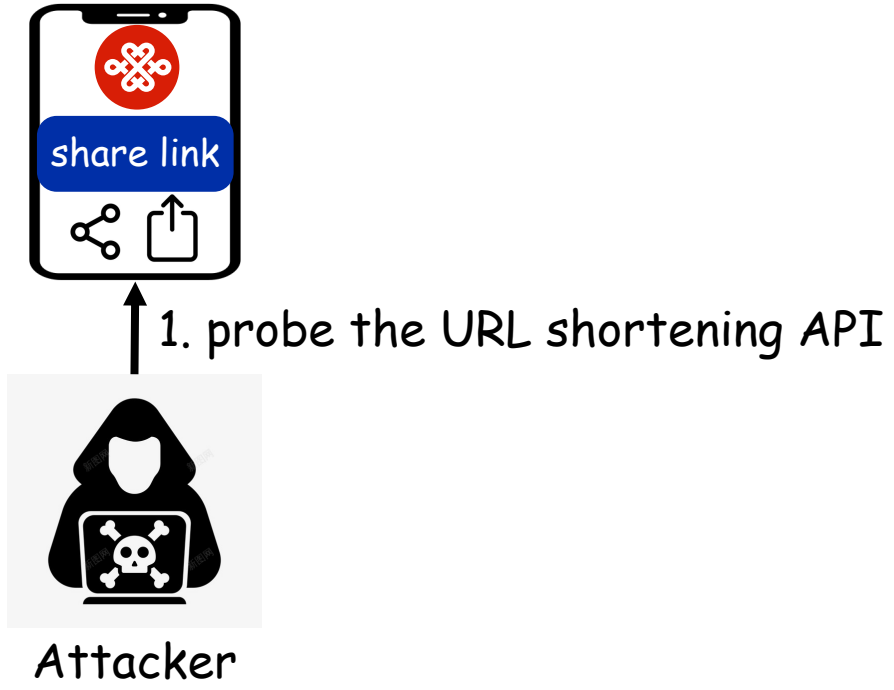
OCT 22, 2012 10:55 AM PDT



Motivating Example

1. Gather intelligence about DUSS

- Identify the entry point
  - e.g., network traffic analysis



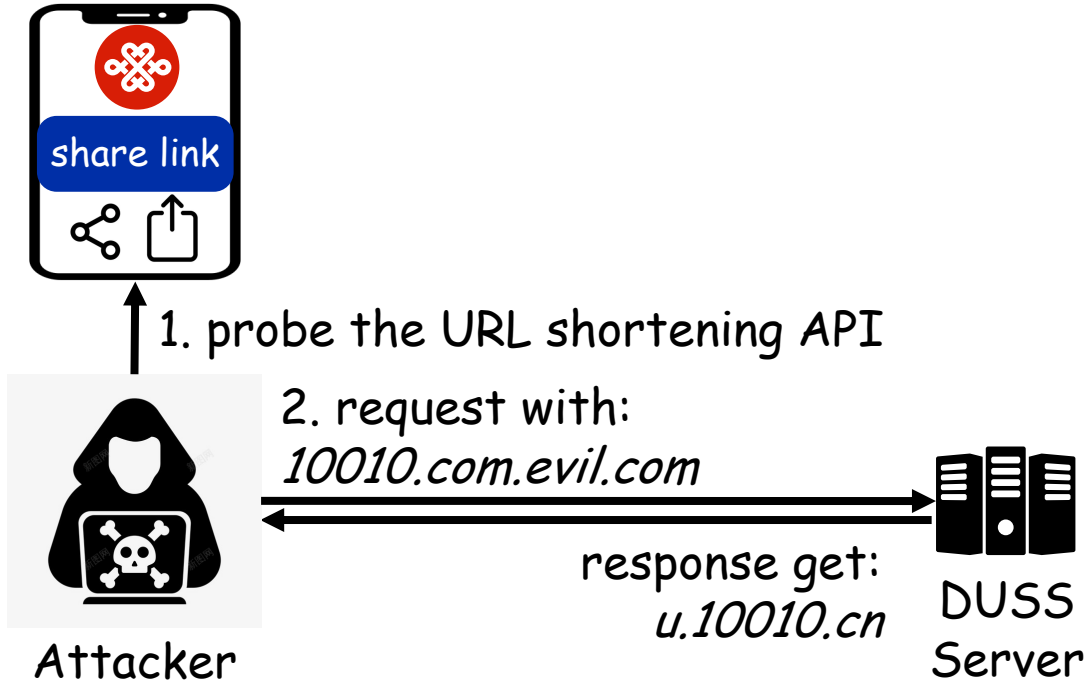
Motivating Example

1. Gather intelligence about DUSS

- Identify the entry point
  - e.g., network traffic analysis

2. Compromise and abuse DUSS

- DUSS only check if "10010.com" in host

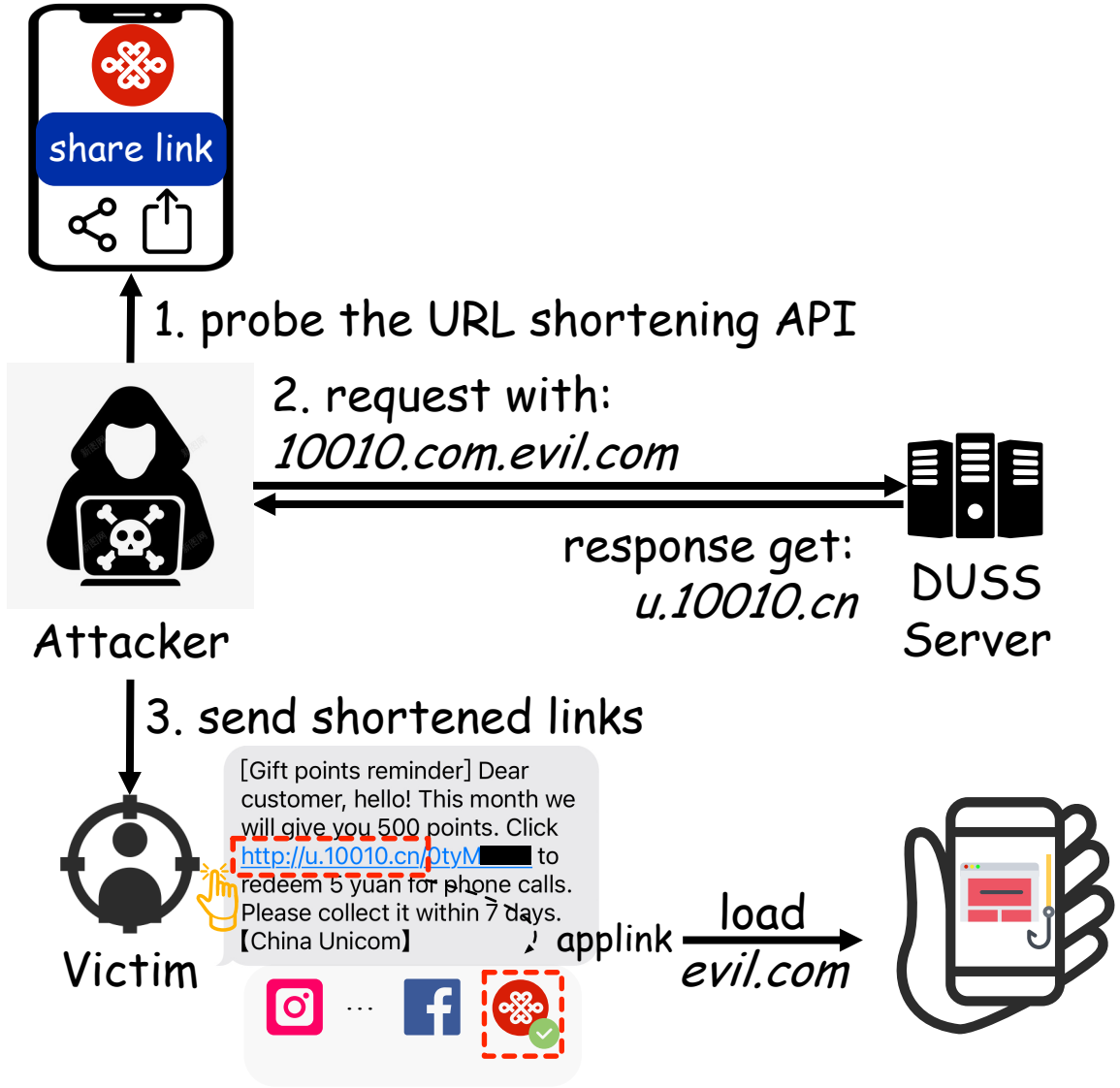


Motivating Example

1. Gather intelligence about DUSS
- Identify the entry point
  - e.g., network traffic analysis

2. Compromise and abuse DUSS
- DUSS only check if "10010.com" in host

3. Launch stealthy attacks
- Phishing
- Remote code injection
  - e.g., install malicious app, steal photos

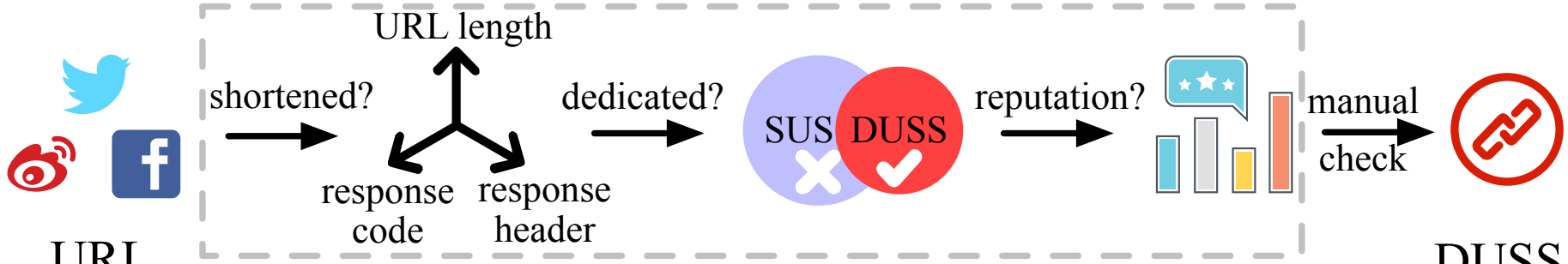


Our Work

- First systematic study about the entire attack surface, detection, and security impacts of Misdirection Attack
  - RQ1. What are the security design of DUSSs and their potential attack surfaces?
  - RQ2. How do we automatically detect whether existing DUSSs are robust to the Misdirection Attack?
  - RQ3. What security implication does the Misdirection Attack have on social network users and domain-based checkers?

Building DUSS Data Set

- Key Insight: follow the shortened links to get the DUSSs



URL Collector

To collect URLs
- in social media posts

Binary Classification Module

To identify DUSS-shortened link
- short length<17
- has redirection (e.g., "30x" code)
- good reputation (e.g., not SUSS, SLD rank in Tranco top 1M)

DUSS-Links

Manual verification
- find 88 unique DUSSs

RQ1: DUSS Architecture

- Deployment Model

Self-developed (65/88)

- developer owns the server
- domain DNS binds to server directly

#	DUSS Corporation	Link Domain	Tranco Rank
1	Baidu	j.map.baidu.com	8
2	Reddit	www.reddit.com	35
3	Youtube	youtu.be	40
4	Google Map	goo.gl	57
5	Wangyi	u.163.com	61
6	TikTok	www.tiktok.com	68
7	Skype	join.skype.com	87
8	Aliexpress	a.aliexpress.com	122
9	Booking.com	www.booking.com	166
10	Huawei	url.cloud.huawei.com	295

Third-party hosted (23/88)

- commercial USS provides the server
- domain DNS binds to third-party server
- example: Carousell, Adidas, Starbucks……

#	Commercial Service	# of Users	Charge
1	Bitly	500,000+	paid
2	TinyURL	102,035+	paid
3	Rebrandly	30,000+	paid
4	Branch IO	100,000+	paid
5	AppsFlyer	12,000+	paid

- Customized security checks on URL scheme/domain/path

RQ1: DUSS Security Analysis

- Attack Vectors
  - summarize researches/blogs about "URL check bypass":
    - flawed scheme check — e.g., javascript://allowed.com/%0aalert(1)
    - flawed domain check
      - for domain parsing: — e.g., https://allowed.com:x@malicious.com
      - for domain matching: — e.g., endsWith("allowed.com") -> aaaallowed.com
      - for domain asset: — e.g., XSS, open-redirection … …
    - flawed path check

- Attack Surface
  - wildly exposed shortening API in client-side apps(8/15)

RQ2: Vulnerable DUSSs in The Wild

- Goal
  - Identify and test the security of link-shortening APIs from client-side apps

- Technique Challenge
  - Difficult to recognize customized link-shortening APIs of different DUSSs
  - Challenging to bypass API encryption for legitimate testing requests
  - Hard to create comprehensive and effective security tests

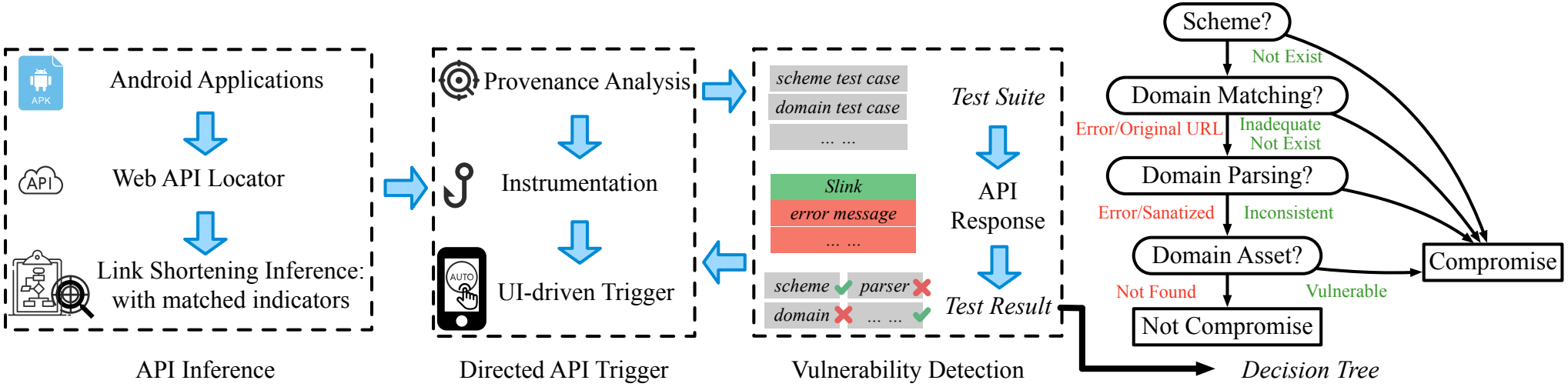
API Identification

Legal API request

Ethical problem

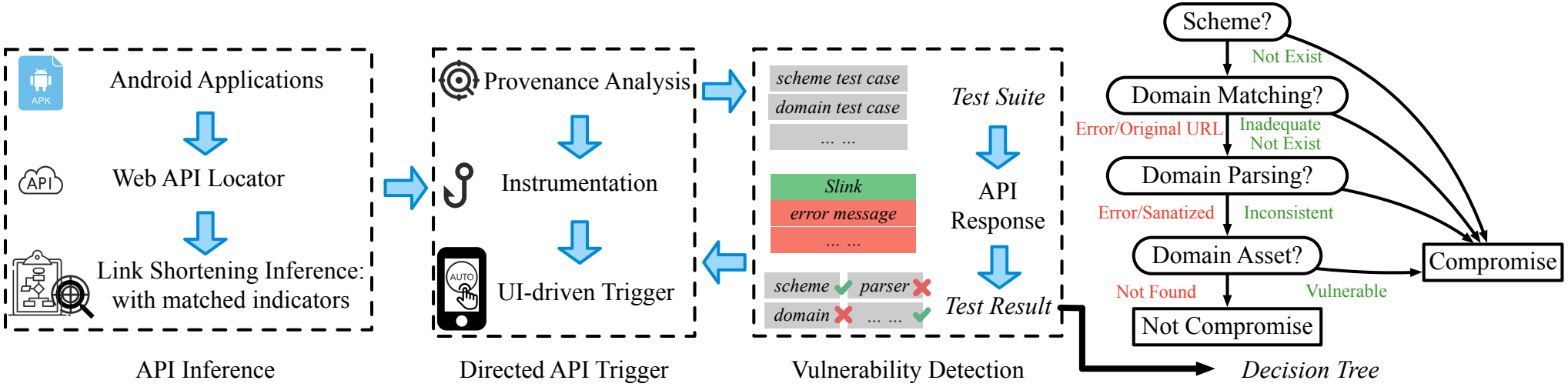
RQ2: Overview

- DUSS Interface Testing Tool (Ditto)
  - API Inference
  - Directed API Trigger
  - Vulnerability Detection



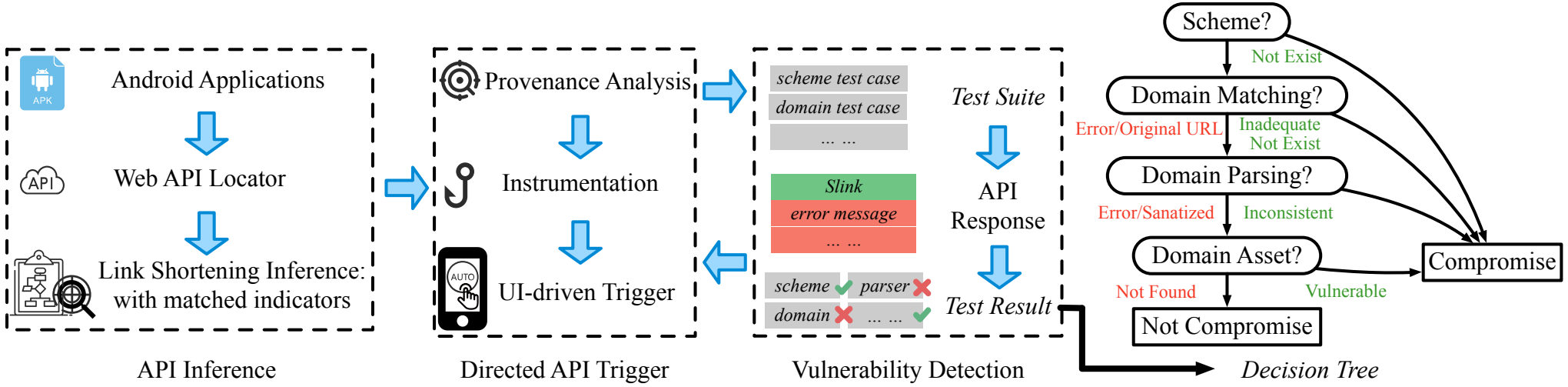
Ditto Design

- API Inference
  - **Insight:** find **potential** link-shortening API by analyzing client-side Web API implementation logic
  - Two key indicators
    - **URL Objects**: Both **request** and **response** data contain **URL-type-objects**
    - **SDK Calls**: The API is called from a **commercial service SDK**



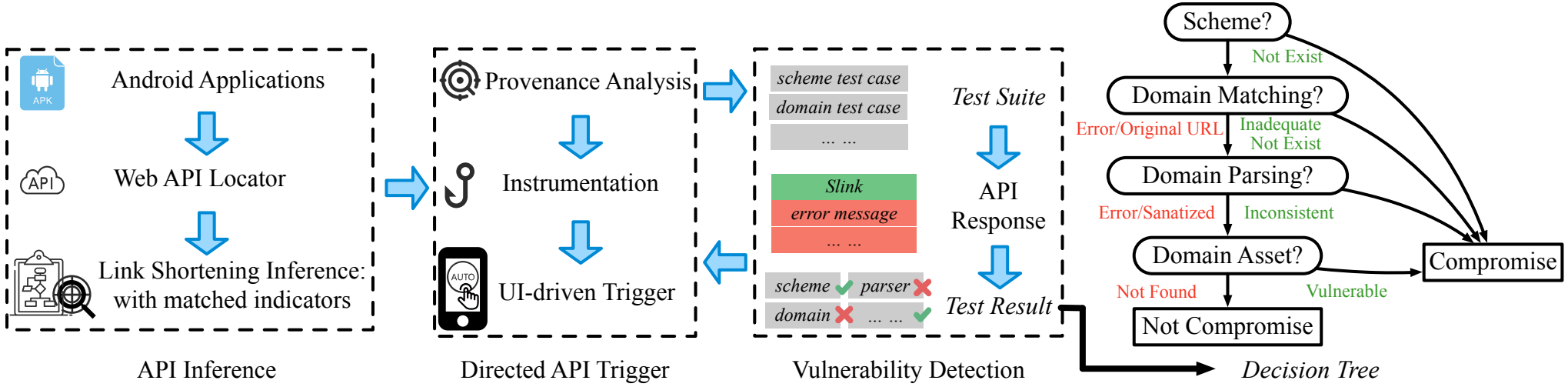
Ditto Design

- Directed API Trigger
  - **Insight**: Ditto dynamically triggers legal API requests and modifies the URL source before API encryption
  - Core Techniques
    - Provenance Analysis: traces the source of the URL to identify modifiable elements
    - Instrumentation: instruments apps for convenient URL modification
    - UI-driven API Trigger: uses UI interactions to trigger API calls (also verify it)



Ditto Design

- Vulnerability Detection
  - **Insight**: uses a decision tree to guide test suites, optimize their sequence, remove unnecessary tests, improve efficiency
    - **Test Suites**
      - the least PoC URLs that exploit most known URL check vulnerabilities
      - provide unique templates for test case generation
    - **Decision Tree Guidance**
      - Validates consequences before preconditions, preventing redundant validations



RQ2: Evaluation

- Experimental Setup
  - Analyzed **377 APKs** developed by **DUSS corporations**
- Results
  - Identified **50 link-shortening APIs**
  - Verified **22 vulnerable APIs** after **373 tests**

TABLE I

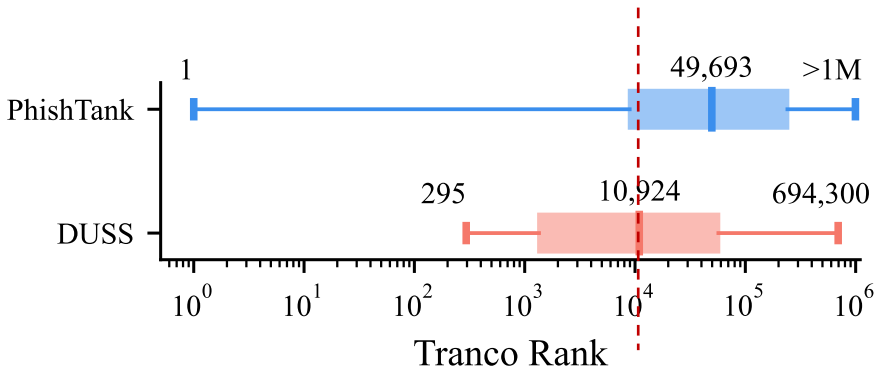
VULNERABILITY BREAKDOWN IN THE TOP 15 VULNERABLE DUSSS. SYMBOL "✔" MEANS THE DUSS IS COMPROMISED IN THIS URL CHECK SCENARIO. "-" MEANS NO VULNERABILITY IS FOUND IN THIS CATEGORY. "M/P/A" STANDS FOR VULNERABLE MATCHING/PARSING/ASSET.

#	Corporation	Website	# Visiting	Brand Domain	Visiting	Tranco Rank	Development	Scheme	Domain(M/P/A)
1	Huawei	huawei.com	92.9M	url.cloud.huawei.com	-	295	Self-developed	-	✔(A)
2	Lazada	lazada.com	1.6M	s.lazada.sg	231.6K	6k	Self-developed	-	✔(P)
3	CastBox	castbox.fm	1.2M	castbox.fm	1.2M	6k	Self-developed	✔	✔(M)
4	Sina	sina.cn	107.7M	t.cn	1.4M	8k	Self-developed	-	✔(M)
5	Amazon	amazon.com	2.4B	a.co	17.3M	8k	Self-developed	✔	✔(M)
6	ixigo	ixigo.com	12.3M	f.ixigo.com	188.7K	13k	Self-developed	-	✔(M)
7	Weilai	nio.cn	345.6K	l.nio.com	2.8K	22k	Self-developed	-	✔(M)
8	Flipboard	flipboard.com	4.5M	flip.it	852.6K	42k	Self-developed	✔	✔(M)
9	YamiBuy	yamibuy.com	1.1M	u.yamibuy.com	-	56k	Self-developed	✔	✔(M)
10	Yelp	yelp.com	134.8M	yelp.to	1.6M	183k	Self-developed	-	✔(P)
11	Xiaohongshu	xiaohongshu.com	162.1M	xhslink.com	928.9K	295k	Self-developed	✔	✔(M)
12	China Unicom	10010.com	3.4M	u.10010.cn	58.9K	526k	Self-developed	-	✔(P)
13	momo shopping	momoshop.com.tw	33.6M	momo.dm	237.8K	694k	Self-developed	-	✔(M)
14	flipp	flipp.com	2.8M	click.flipp.com	124.8K	14k	Third-party Hosted	-	✔(M)
15	TubiTv	tubitv.com	36.3M	link.tubi.tv	202.8K	49k	Third-party Hosted	-	✔(M)

RQ3: Security Impact

on Social Users

Fact: Users prefer to trust well-known domain name



Misdirection Attack is **more deceptive** than traditional phishing URLs

on Domain-based Checkers

- Experimental group: Misdirection Attack
  - Tested using 22 vulnerable DUSS
- Control group: Traditional Attack
  - Tested using standard URLs (i.e., evil.com)

Result: **11 apps/webs** are vulnerable **only to Misdirection Attack**, leading to *remote code injection*, *privacy leakage*, impacting **3 billion** users…

xhslink.com *u.10010.cn* *url.cloud.huawei.com* *flip.it* … …

Security checkers (i.e., mobile applinks, OAuth allowlists, and link warning services … …) can be deceived

Conclusion

- Conduct the first systematic analysis of **DUSS**, uncovering **88 high-profile DUSSs** used by real-world corporations and examining their security design and attack surfaces

- Propose an automated analysis framework Ditto for identifying vulnerable DUSSs susceptible to Misdirection Attack, and identify 22 exploitable DUSSs with high precision and efficiency

- Our findings highlight the **wide-ranging security implications** of such attacks, including **phishing** and bypassing **domain-based checkers**, which could compromise critical app functions and lead to significant privacy risks for millions of users

Thanks !

Q&A