NDSS

Network and Distributed System Security (NDSS) Symposium
26 February–1 March 2024, San Diego, California

Certificate Transparency Revisited: The Public Inspections on Third-party Monitors

Aozhuo Sun, Jingqiang Lin, Wei Wang, Zeyan Liu, Bingyu Li,
Shushang Wen, Qiongxiao Wang, Fengjun Li

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

中国科学院大学
University of Chinese Academy of Sciences

中国科学技术大学
University of Science and Technology of China

KU THE UNIVERSITY OF KANSAS

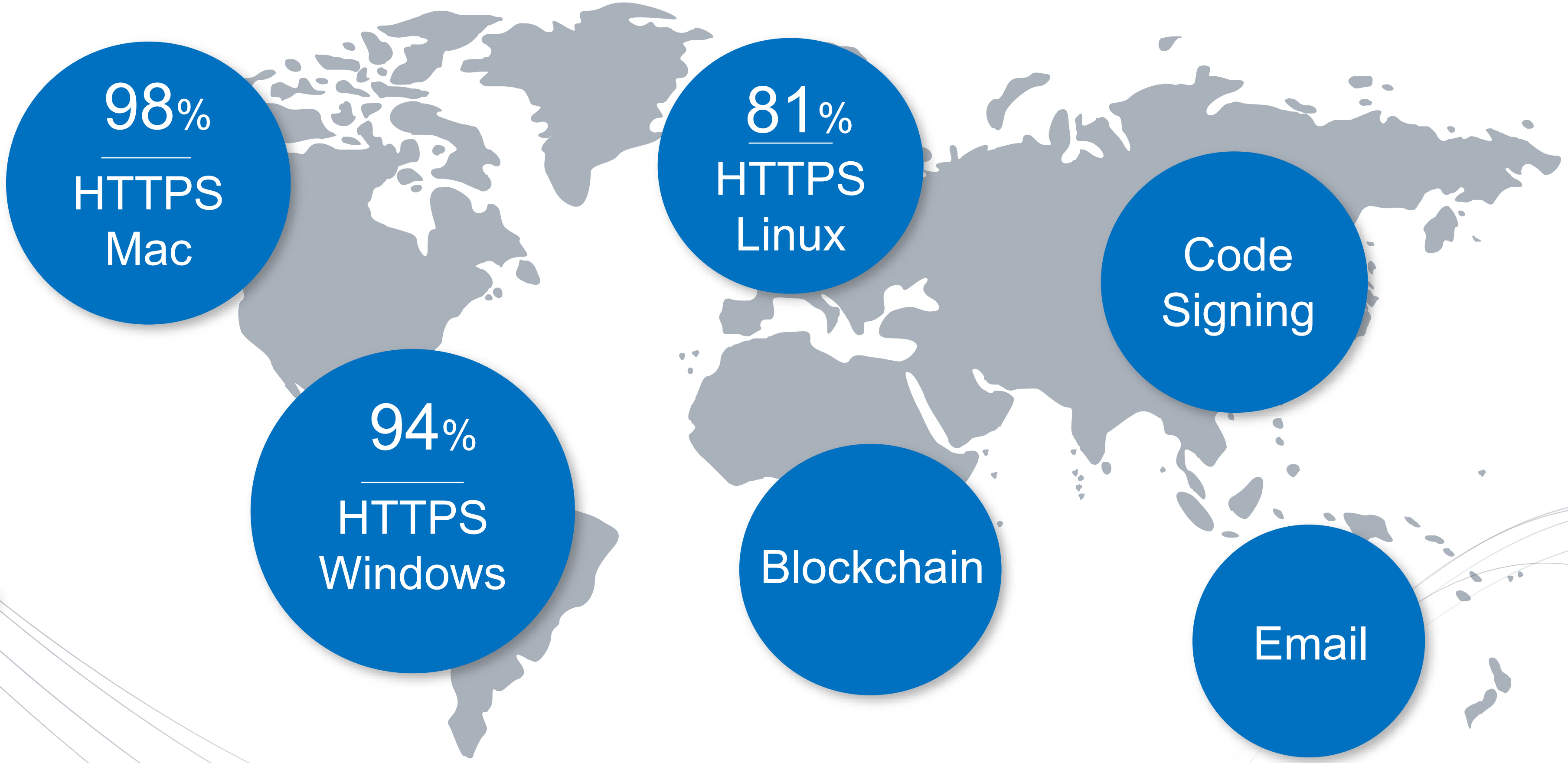
北京航空航天大學
BEIHANG UNIVERSITY

February 30, 2024

Outline

- **Problem and Motivation**
- CT Watcher Design
- Implementation and Evaluation
- Conclusions

PKI and Certificates



98%

HTTPS Mac

81%

HTTPS Linux

Code Signing

94%

HTTPS Windows

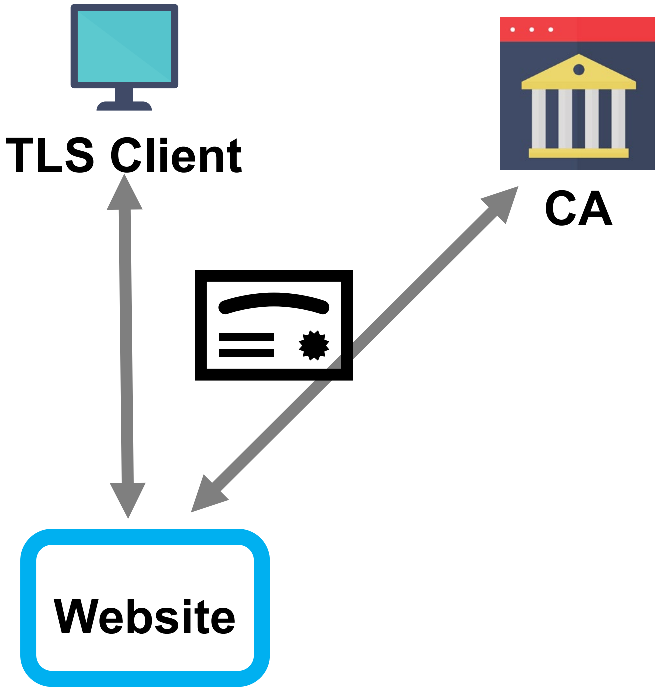
Blockchain

Email

PKI is one of the most important security services on the Internet!

Data from Google Transparency Report, accessed in January 2024

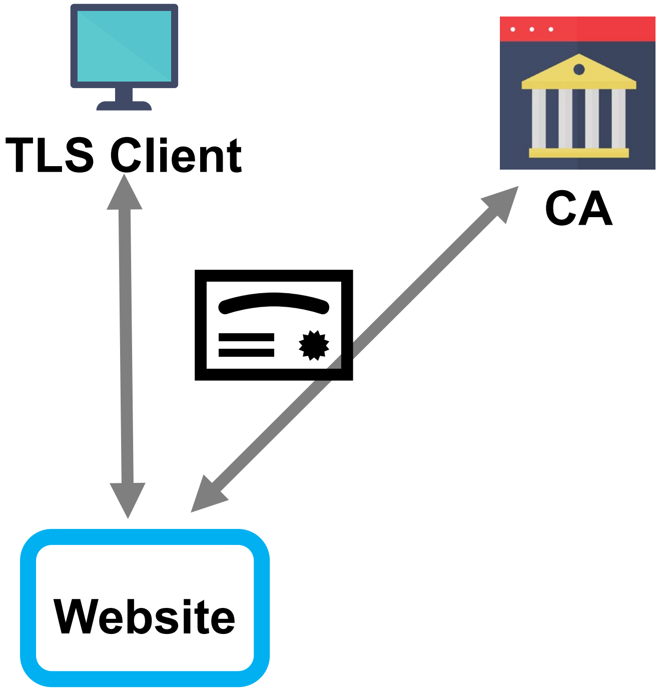
Trust is NOT assumed!

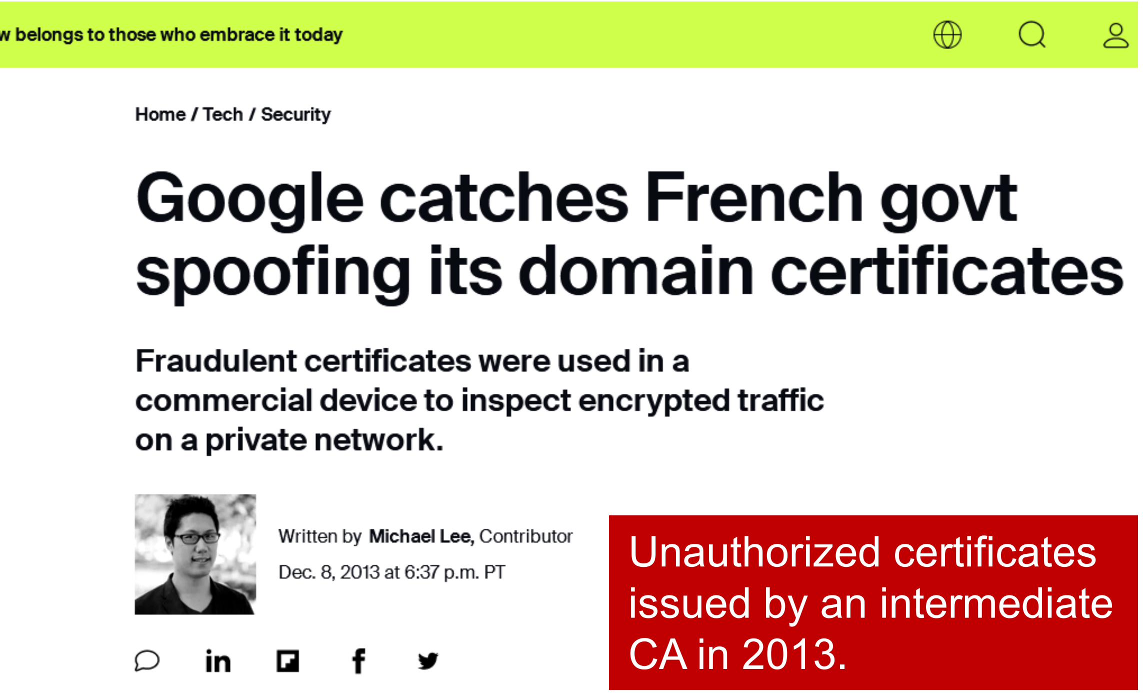


✓ **PKI shifts the trust to the CA**

***But* should we fully trust the CAs?**

Trust is NOT assumed!





tomorrow belongs to those who embrace it today

Home / Tech / Security

Google catches French govt spoofing its domain certificates

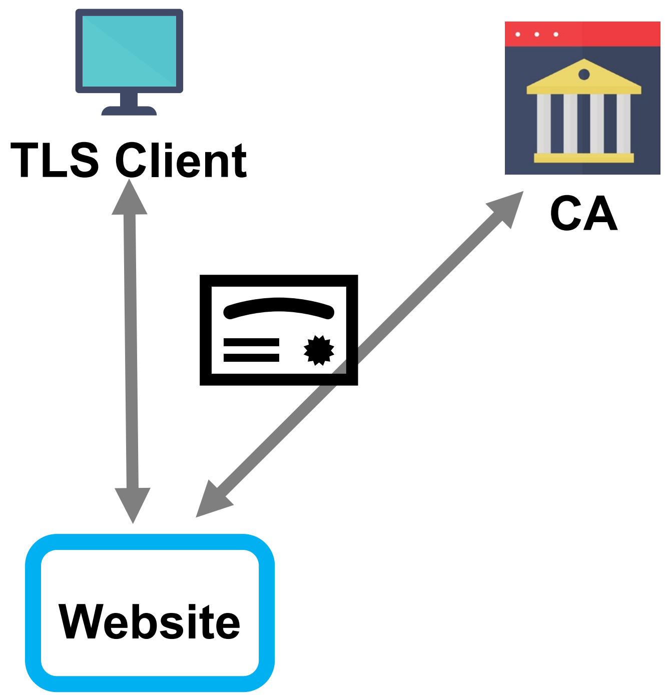
Fraudulent certificates were used in a commercial device to inspect encrypted traffic on a private network.

Written by **Michael Lee,** Contributor

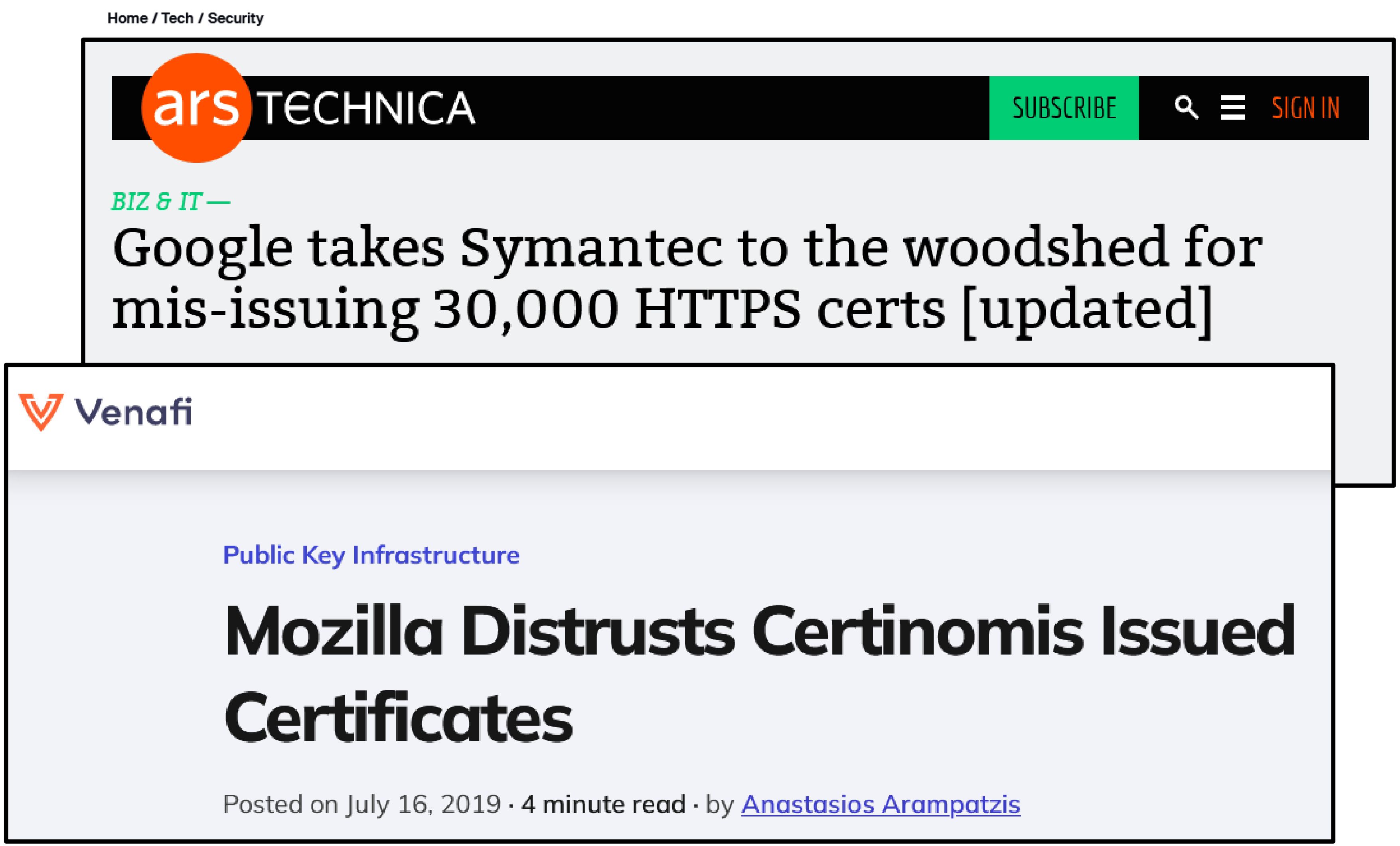
Dec. 8, 2013 at 6:37 p.m. PT

Unauthorized certificates issued by an intermediate CA in 2013.

Trust is NOT assumed!



/ tech



BIZ & IT —

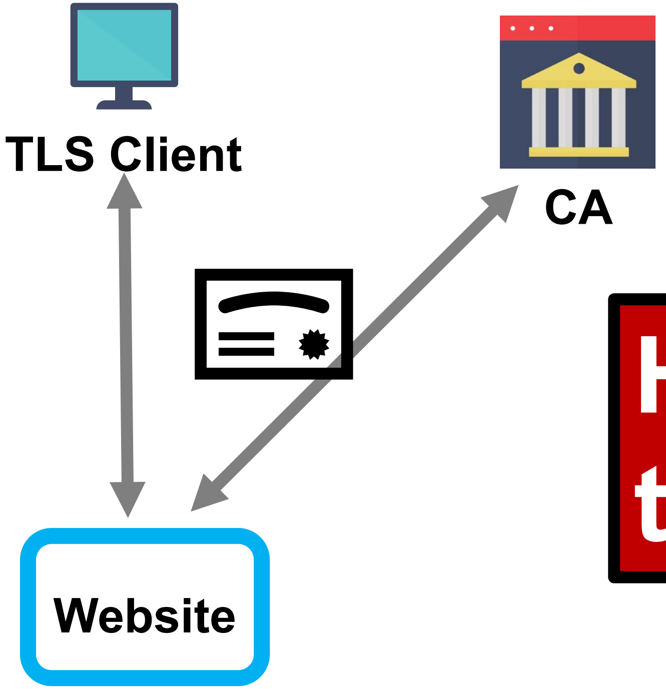
Google takes Symantec to the woodshed for mis-issuing 30,000 HTTPS certs [updated]

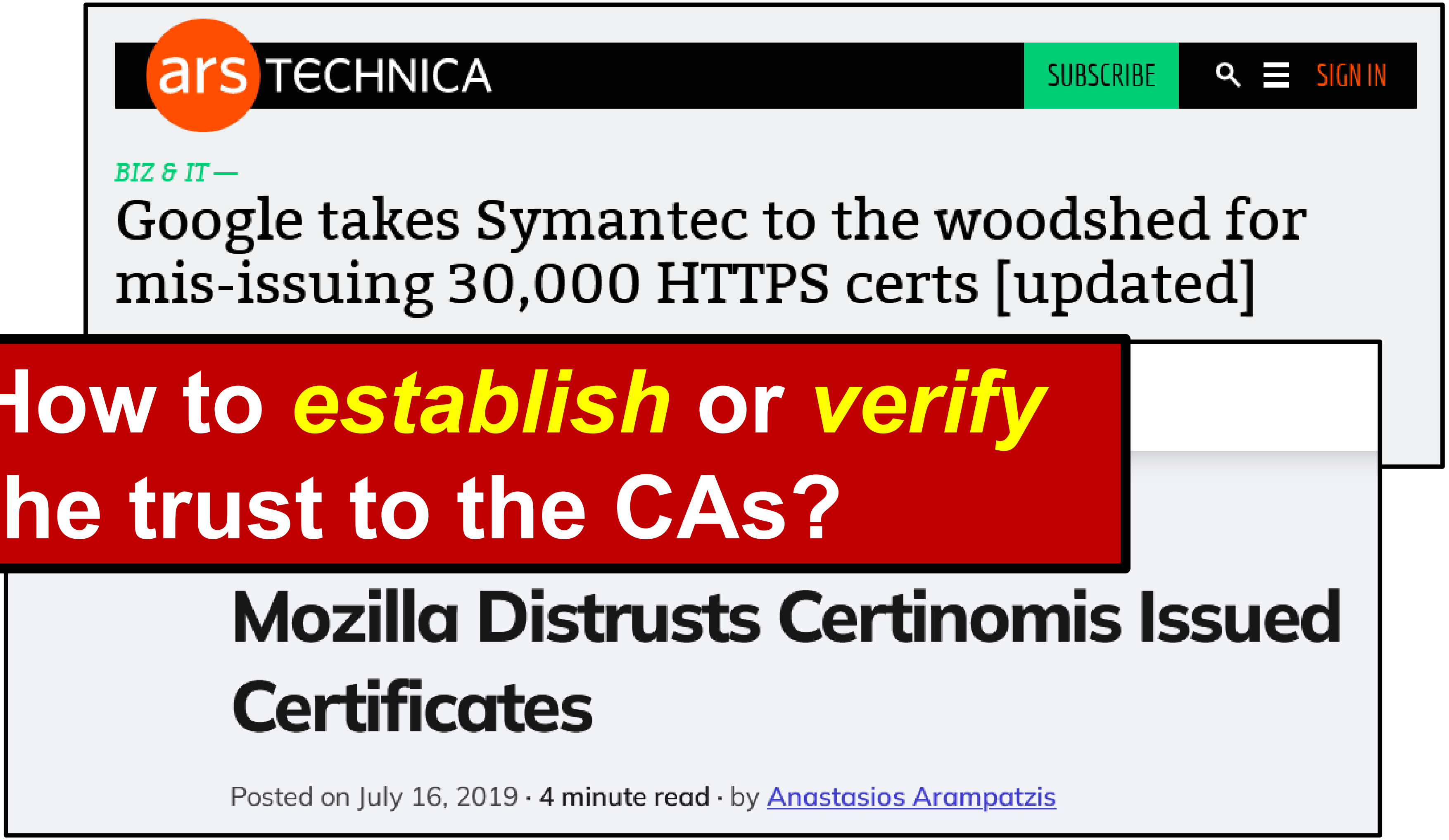
Public Key Infrastructure

Mozilla Distrusts Certinomis Issued Certificates

Posted on July 16, 2019 · 4 minute read · by Anastasios Arampatzis

Trust is NOT assumed!





BIZ & IT —

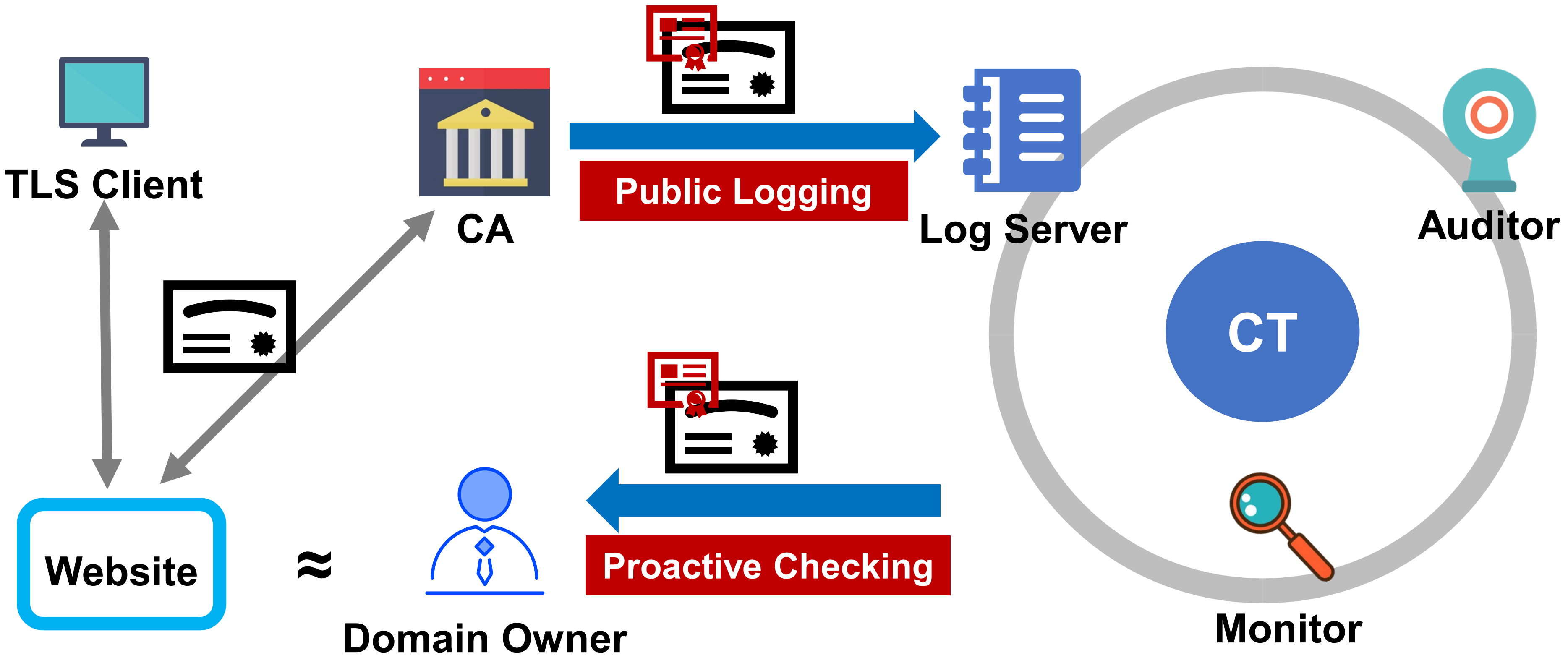
Google takes Symantec to the woodshed for mis-issuing 30,000 HTTPS certs [updated]

Mozilla Distrusts Certinomis Issued Certificates

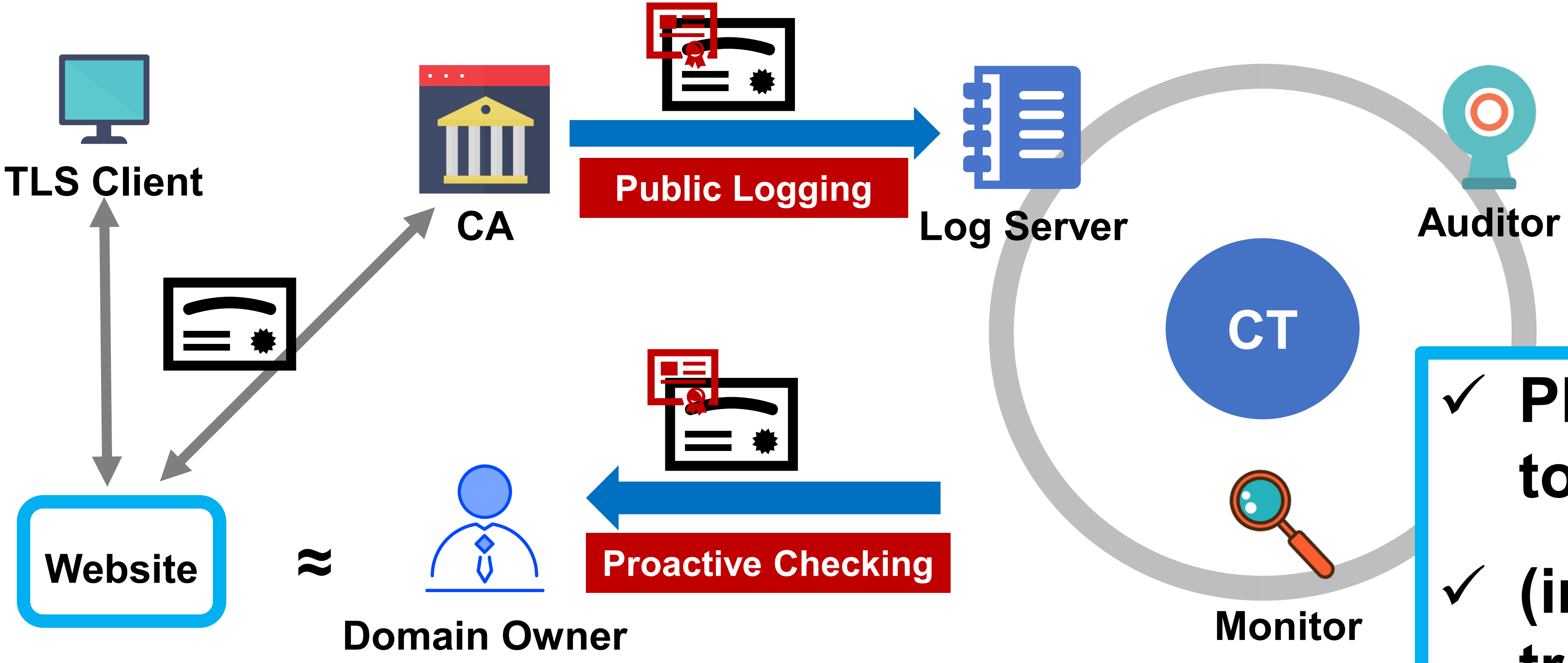
Posted on July 16, 2019 · 4 minute read · by Anastasios Arampatzis

How to *establish* or *verify* the trust to the CAs?

Certificate Transparency (CT)

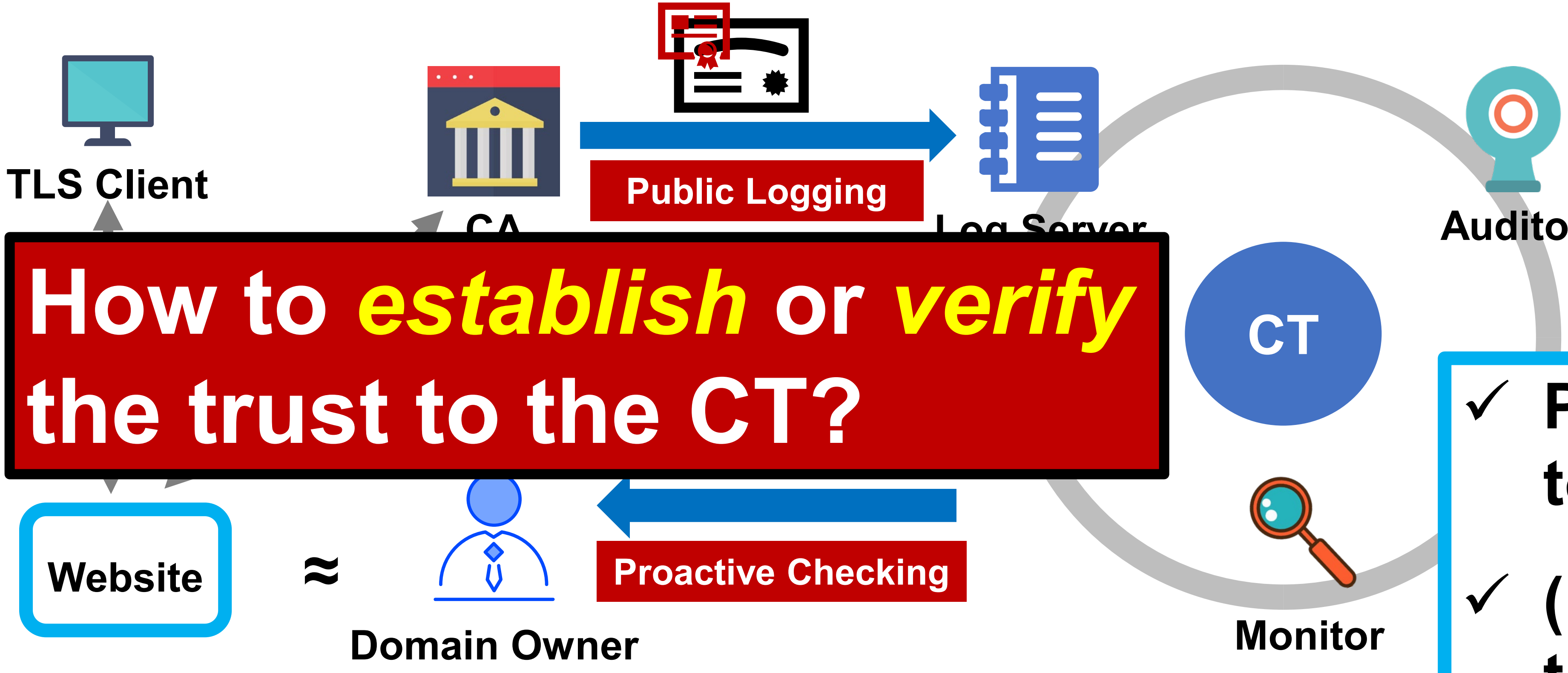


Certificate Transparency (CT)



- ✓ PKI shifts trust to the CAs
- ✓ (implicitly) shift trust to the CT

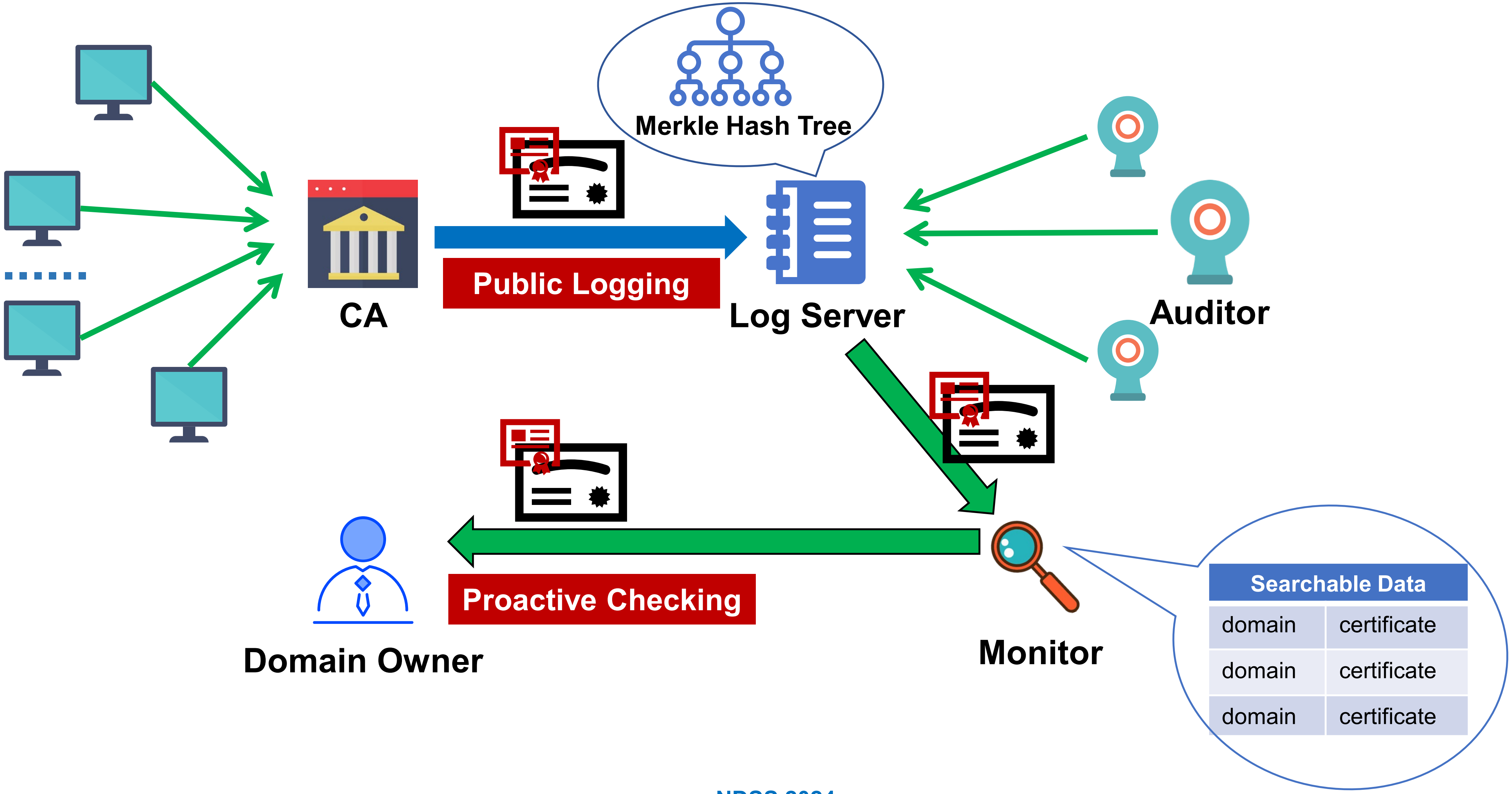
Certificate Transparency (CT)



How to *establish* or *verify* the trust to the CT?

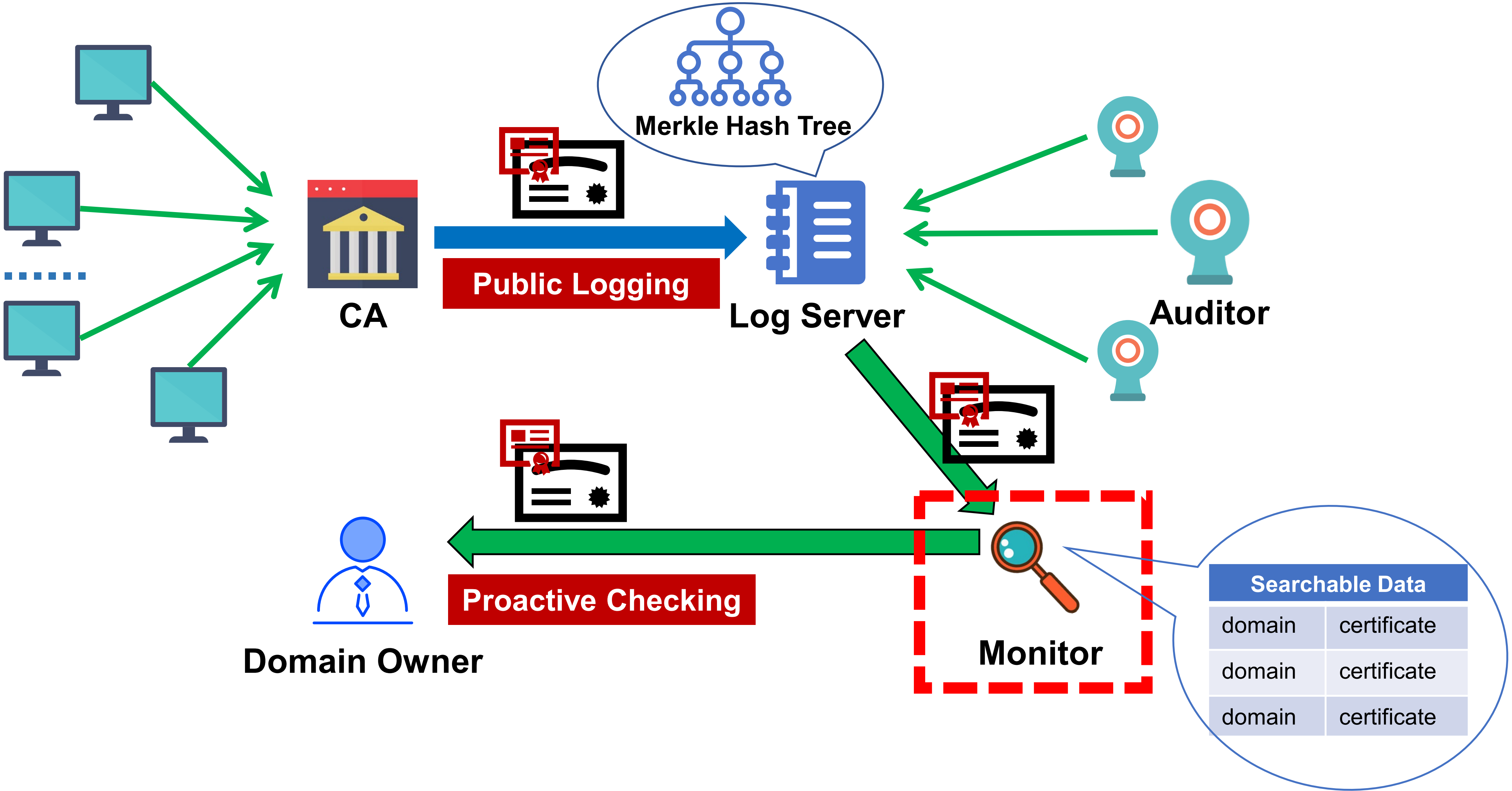
- ✓ **PKI shifts trust to the CAs**
- ✓ **(implicitly) shift trust to the CT**

CT Entities and the Trust Model



Searchable Data	
domain	certificate
domain	certificate
domain	certificate

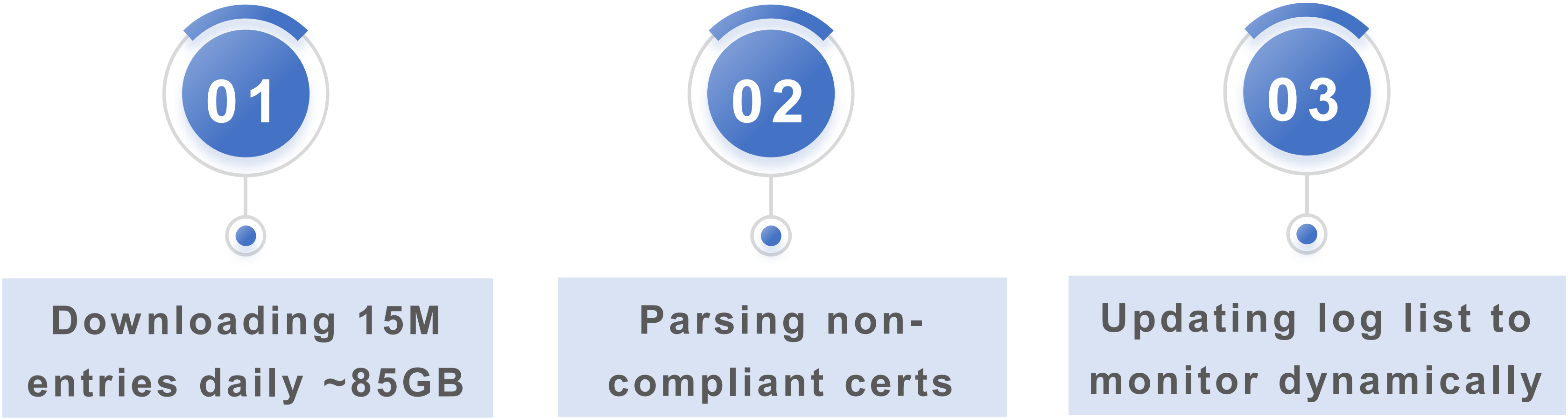
CT Entities and the Trust Model



Searchable Data	
domain	certificate
domain	certificate
domain	certificate

CT Monitors in the Wild

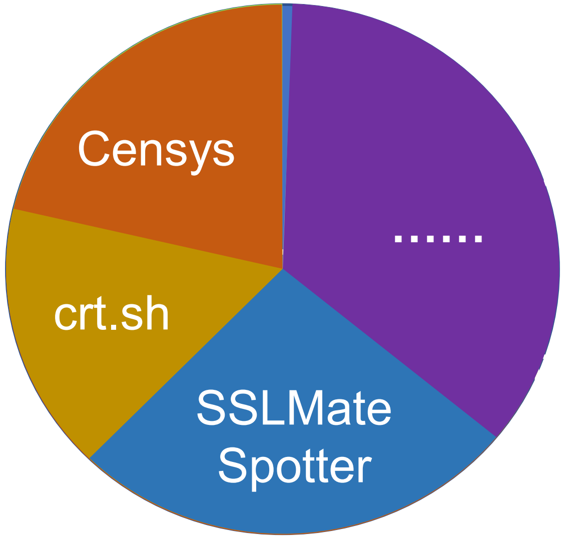
- Any party can serve as a CT Monitor [RFC9162]
  - Self-monitors operated by domain owners
  - Third-party monitors operated by service providers
- Impractical to operate self-monitors by ordinary domain owners [Li et al. CCS'19]



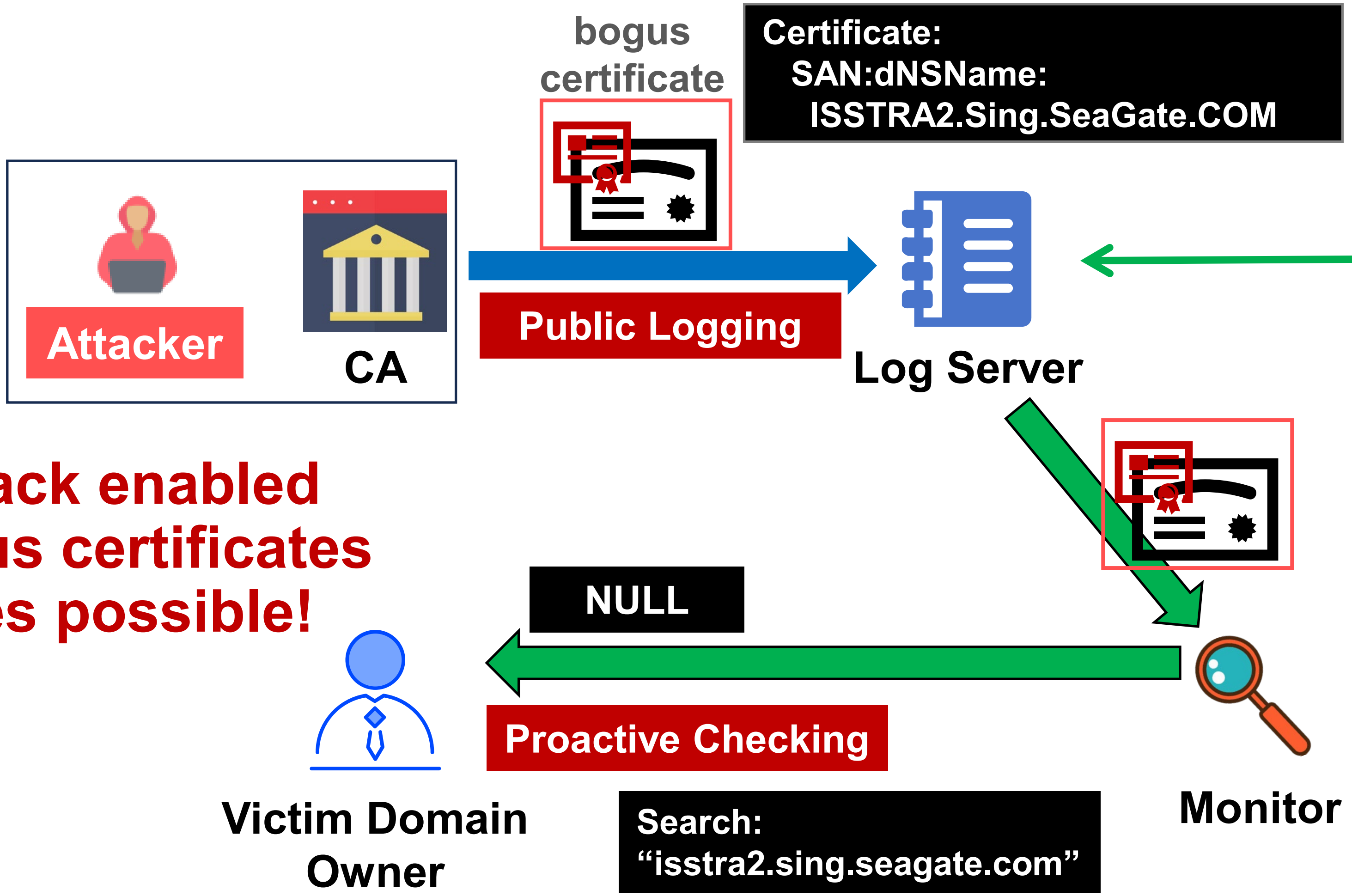
01 Downloading 15M entries daily ~85GB

02 Parsing non-compliant certs

03 Updating log list to monitor dynamically



What Could Possibly Go Wrong?



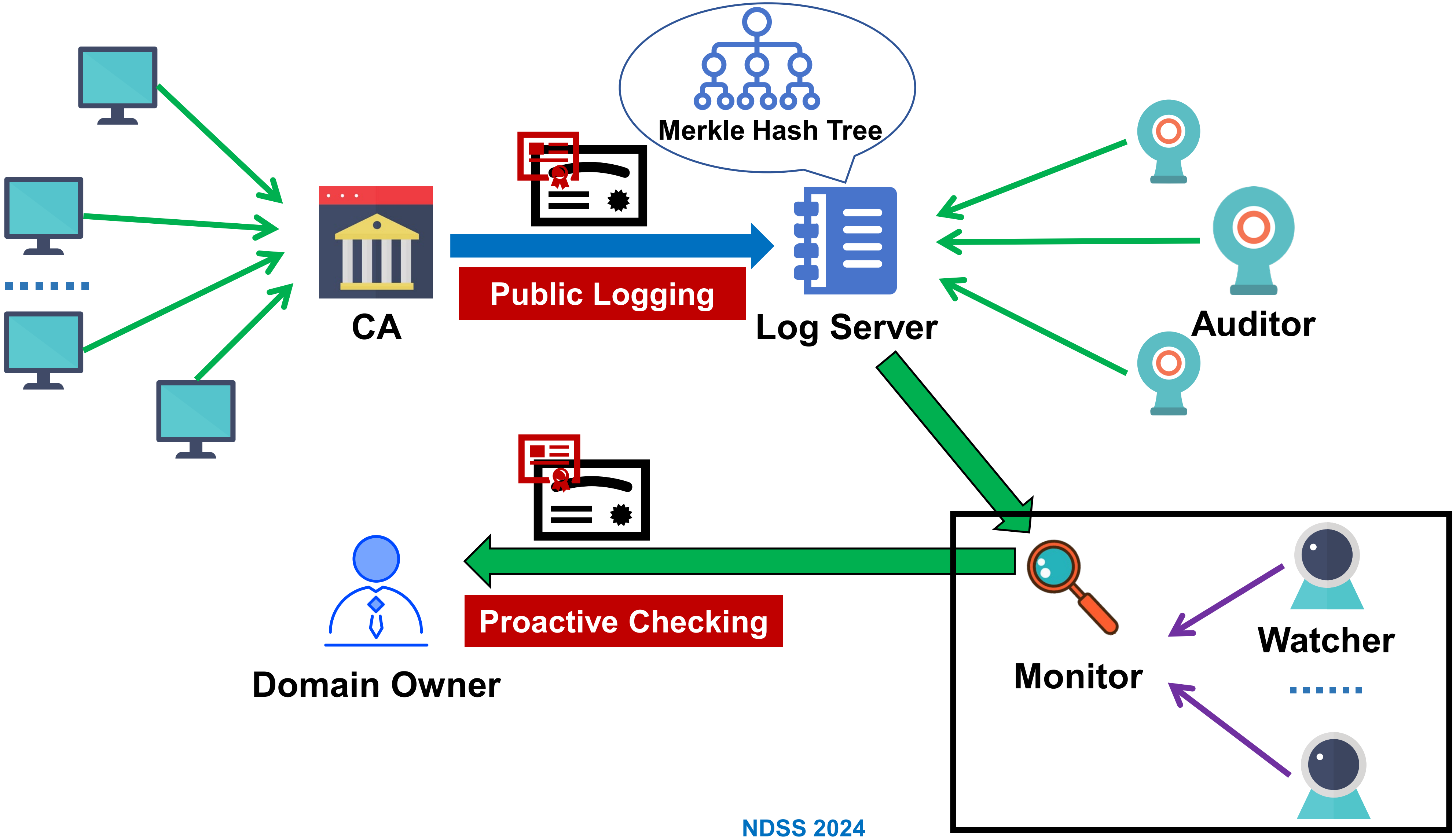
Certificate:
SAN:dNSName:
ISSTRA2.Sing.SeaGate.COM

Search:
“isstra2.sing.seagate.com”

Any attack enabled by bogus certificates becomes possible!

3rd-party Monitors are not as reliable as we expect [Li et al. CCS’19]

CT Watcher


Merkle Hash Tree
CA
Public Logging
Log Server
Auditor
Monitor
Watcher
Proactive Checking
Domain Owner

Outline

- Problem and Motivation
- **CT Watcher Design**
- Implementation and Evaluation
- Conclusions

Threat Model

Monitor

Benignly-faulty Monitor

- Has program flaw(s)
- Some flaws cause rhythmic and repeatitive misbehavior

Watcher

Watcher

- Can be benign or malicious
- If malicious, it can cause malicious disclosure
- Or intended hiding

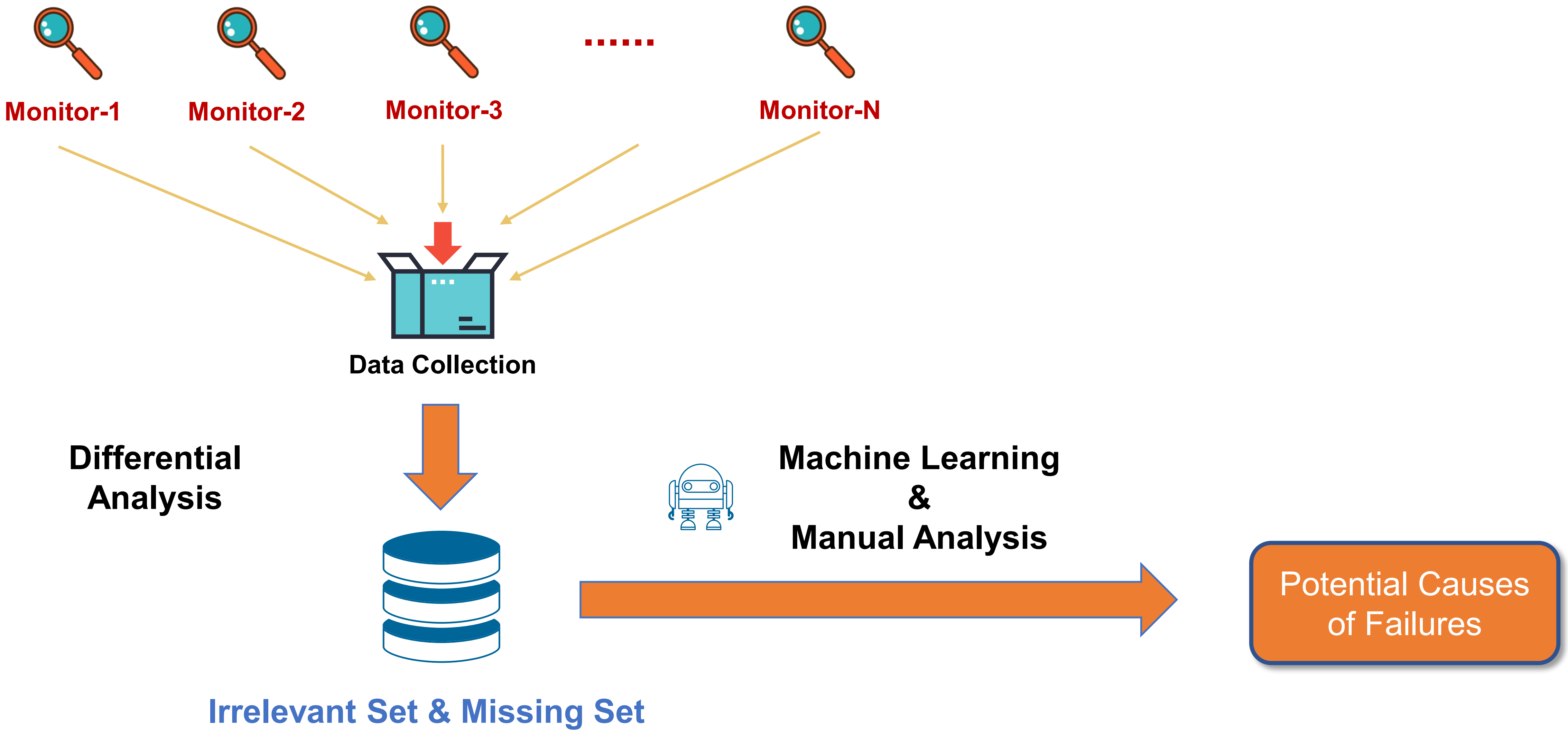
Malicious Monitor

- Misbehave unpredictably

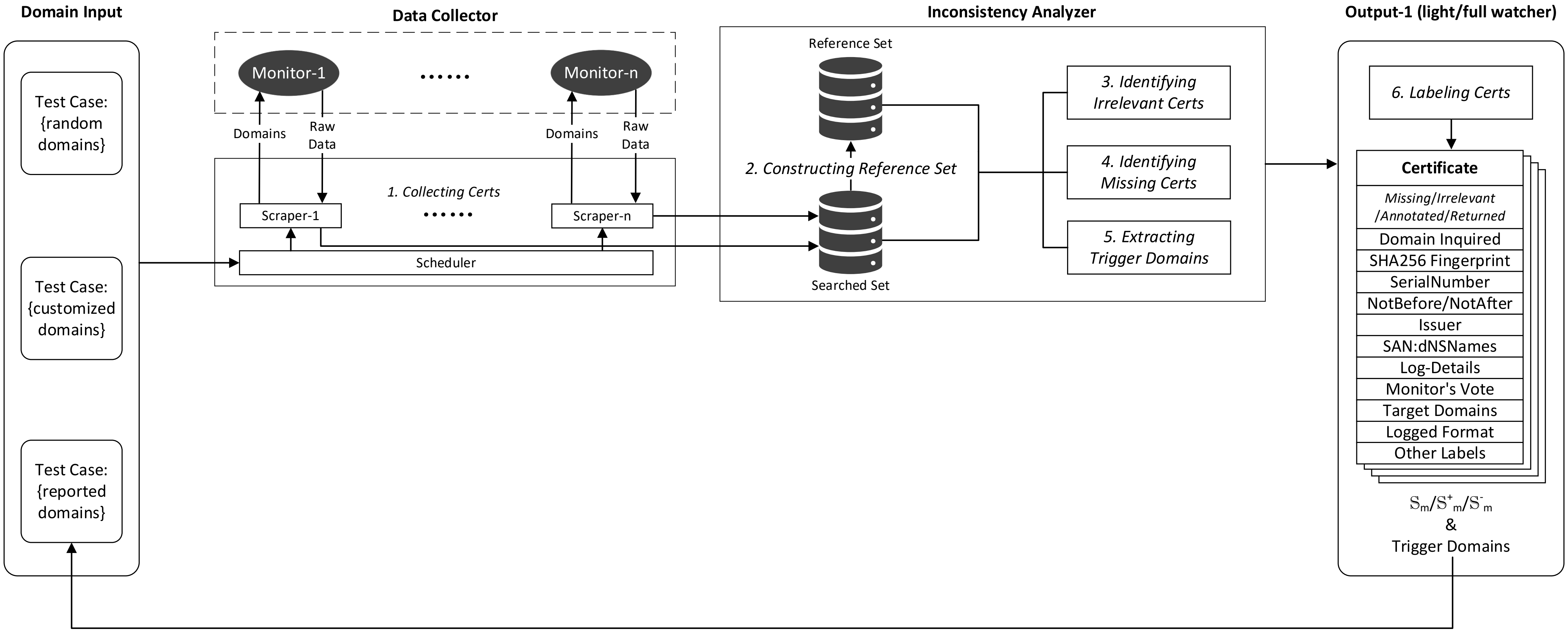
Challenges

- No ground truth about the “correct” result for any given domain
- Little knowledge about third-party monitors
- Need to watch all domains
- Monitor’s misbehavior may be caused by various, unknown reasons

CT Watcher Architecture


Monitor-1
Monitor-2
Monitor-3
......
Monitor-N
Data Collection
Differential Analysis
Machine Learning & Manual Analysis
Irrelevant Set & Missing Set
Potential Causes of Failures

Light Watcher



Domain Input

Test Case: {random domains}

Test Case: {customized domains}

Test Case: {reported domains}

Data Collector

Monitor-1 ...... Monitor-n

Domains

Raw Data

1. *Collecting Certs*

Scraper-1 ...... Scraper-n

Scheduler

Inconsistency Analyzer

Reference Set

2. *Constructing Reference Set*

Searched Set

3. *Identifying Irrelevant Certs*

4. *Identifying Missing Certs*

5. *Extracting Trigger Domains*

Output-1 (light/full watcher)

6. *Labeling Certs*

Certificate

Missing/Irrelevant /Annotated/Returned

Domain Inquired

SHA256 Fingerprint

SerialNumber

NotBefore/NotAfter

Issuer

SAN:dNSNames

Log-Details

Monitor's Vote

Target Domains

Logged Format

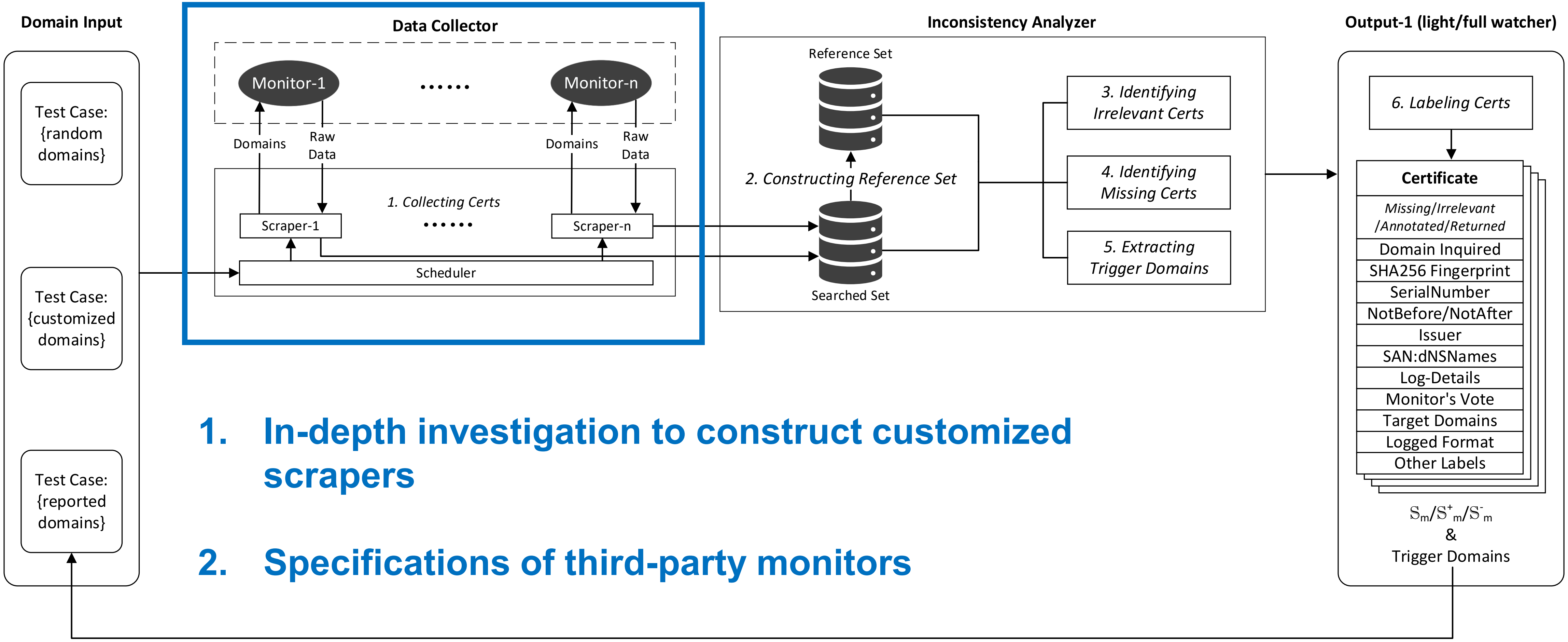
Other Labels

$S_m/S^+_m/S^-_m$

&

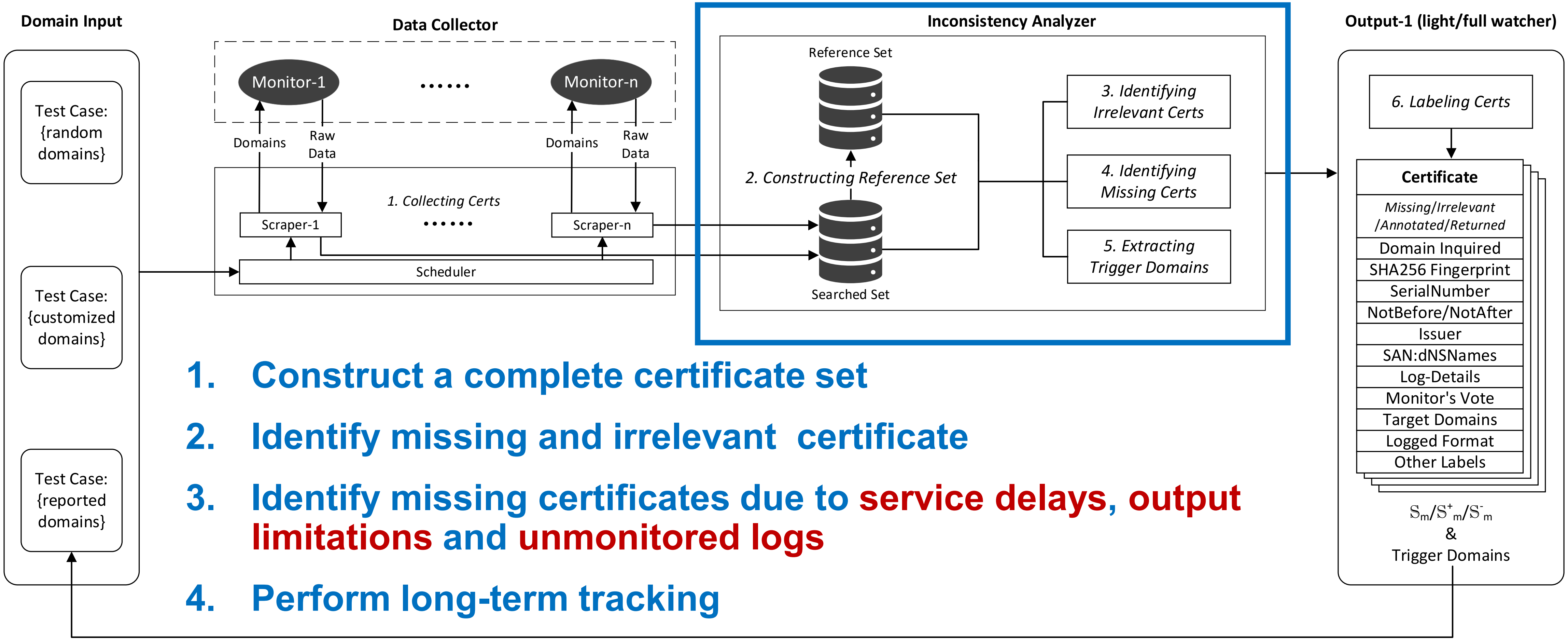
Trigger Domains

Light Watcher



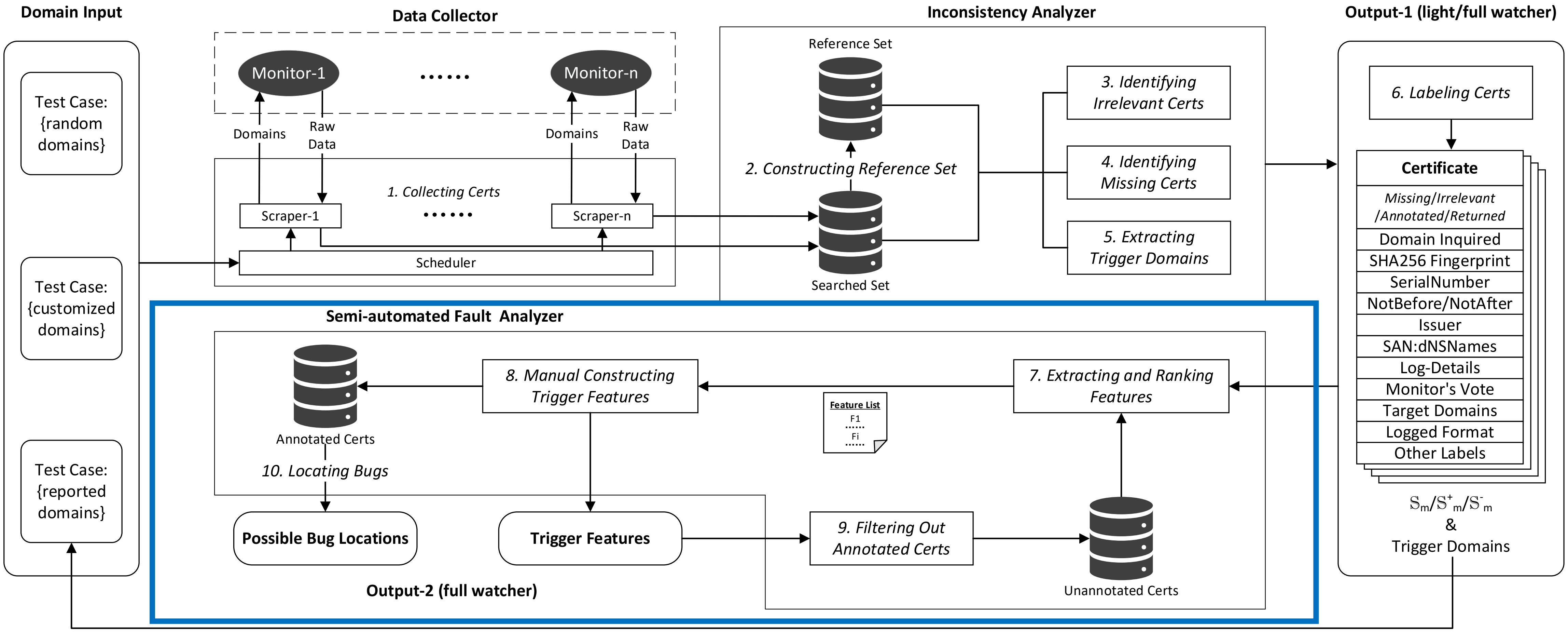
1. **In-depth investigation to construct customized scrapers**
2. **Specifications of third-party monitors**

Light Watcher



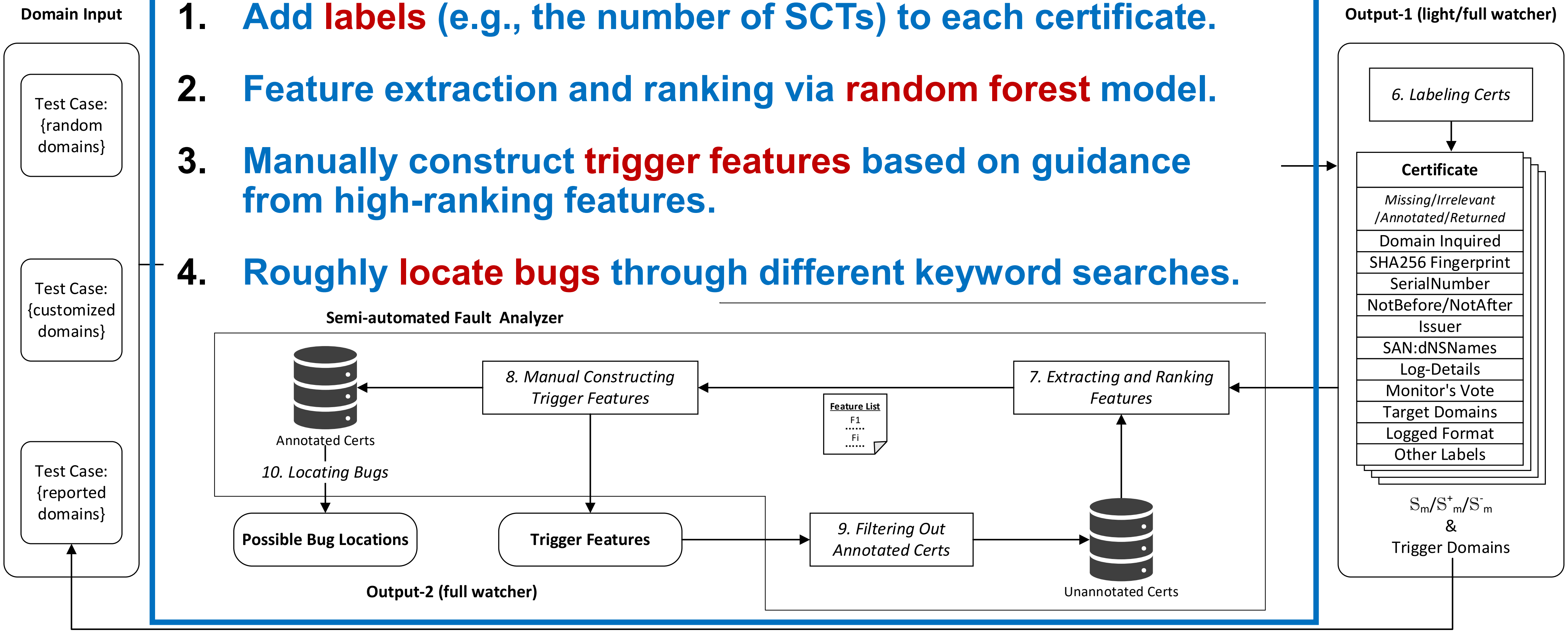
1. Construct a complete certificate set
2. Identify missing and irrelevant certificate
3. Identify missing certificates due to service delays, output limitations and unmonitored logs
4. Perform long-term tracking

Full Watcher

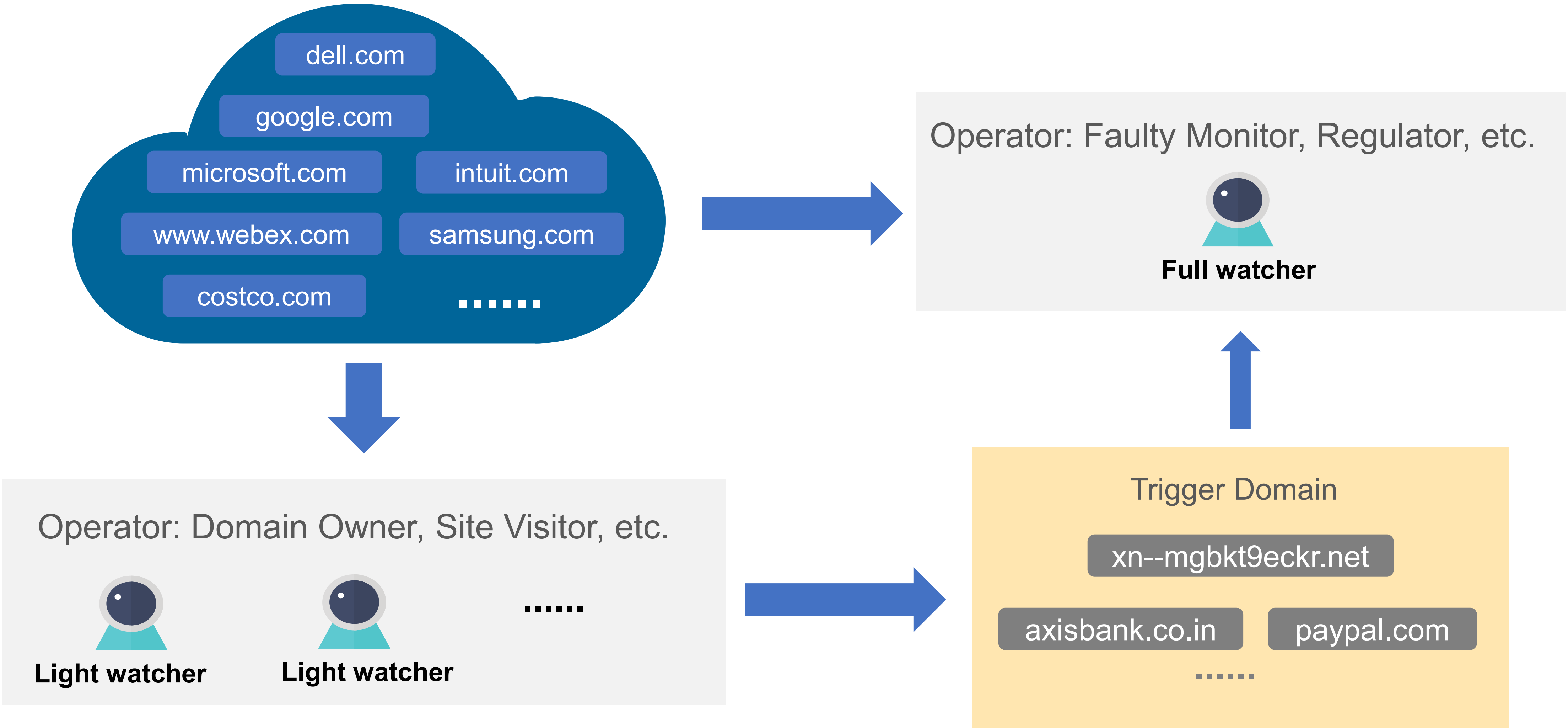


Full Watcher

1. Add **labels** (e.g., the number of SCTs) to each certificate.
2. Feature extraction and ranking via **random forest** model.
3. Manually construct **trigger features** based on guidance from high-ranking features.
4. Roughly **locate bugs** through different keyword searches.



Watcher Deployment



Outline

- Problem and Motivation
- CT Watcher Design
- **Implementation and Evaluation**
- Conclusions

Implementations and Experiments

6 popular third-party monitors

Censys, crt.sh, Entrust, Facebook Monitor, Google Monitor, SSLMate Spotter

52 days of tracking

January 25th – March 16th, 2020

4,000 domains

Randomly selected among Alexa Top1M sites

964K unique certificates

Keep one certificate and its precertificate for each domain

Overview of Inconsistent Certificates

	Censys	crt.sh	Entrust Search	Facebook Monitor	Google Monitor	SSLMate Spotter
Irrelevant Cert	-	52	5	42	-	-
Missing Cert	**206,037**	**80,841**	**621,520**	**633,605**	**95,527**	**310,078**
Service Delay	203,030	80,841	76,999	38,862	75,258	65,365
Output Limit	-	-	466,828	-	-	-
Log List	11	-	-	-	-	-
Informed Error	-	-	-	-	-	244,713
Service Bugs	2,973	-	65,447	594,737	19,939	-
Unknown Causes	23	-	12,246	6	330	-

Overview of Inconsistent Certificates

	Censys	crt.sh	Entrust Search	Facebook Monitor	Google Monitor	SSLMate Spotter
Irrelevant Cert	-	52	5	42	-	-
Missing Cert	206,037	80,841	621,520	633,605	95,527	310,078
Service Delay	**203,030**	**80,841**	**76,999**	**38,862**	**75,258**	**65,365**
Output Limit	**-**	**-**	**466,828**	**-**	**-**	**-**
Log List	**11**	**-**	**-**	**-**	**-**	**-**
Informed Error	-	-	-	-	-	244,713
Service Bugs	2,973	-	65,447	594,737	19,939	-
Unknown Causes	23	-	12,246	6	330	-

Overview of Inconsistent Certificates

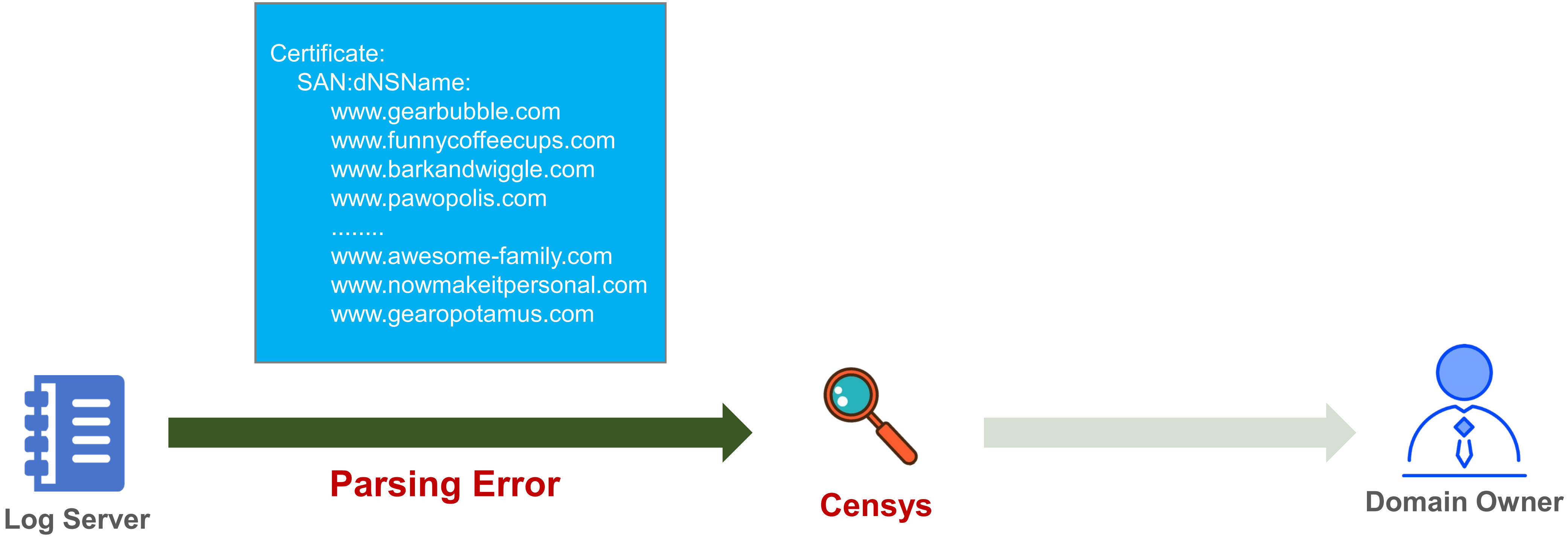
	Censys	crt.sh	Entrust Search	Facebook Monitor	Google Monitor	SSLMate Spotter
Irrelevant Cert	-	52	5	42	-	-
Missing Cert	206,037	80,841	621,520	633,605	95,527	310,078
Service Delay	203,030	80,841	76,999	38,862	75,258	65,365
Output Limit	-	-	466,828	-	-	-
Log List	11	-	-	-	-	-
Informed Error	-	-	-	-	-	244,713
Service Bugs	**2,973**	**-**	**65,447**	**594,737**	**19,939**	**-**
Unknown Causes	23	-	12,246	6	330	-

Overview of Inconsistent Certificates

	Censys	crt.sh	Entrust Search	Facebook Monitor	Google Monitor	SSLMate Spotter
Irrelevant Cert	-	52	5	42	-	-
Missing Cert	206,037	80,841	621,520	633,605	95,527	310,078
Service Delay	203,030	80,841	76,999	38,862	75,258	65,365
Output Limit	-	-	466,828	-	-	-
Log List	11	-	-	-	-	-
Informed Error	-	-	-	-	-	244,713
Service Bugs	2,973	-	65,447	594,737	19,939	-
Unknown Causes	**23**	**-**	**12,246**	**6**	**330**	**-**

Identified Faults

① **Censys may incorrectly parse a certificate with vast characters in its SAN:dNSNames**



```
Certificate:
    SAN:dNSName:
         www.gearbubble.com
         www.funnycoffeecups.com
         www.barkandwiggle.com
         www.pawopolis.com
         ........
         www.awesome-family.com
         www.nowmakeitpersonal.com
         www.gearopotamus.com
```

Log Server

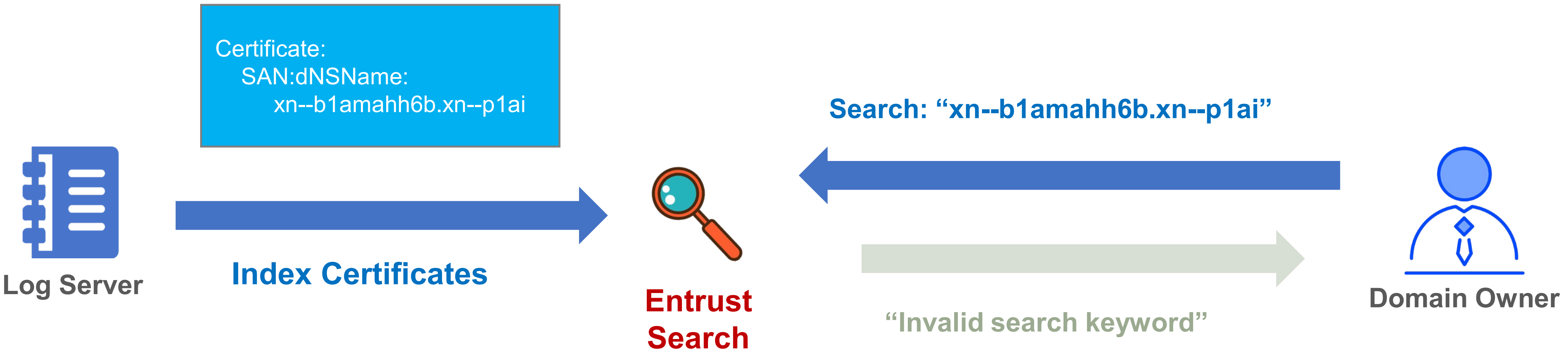
Parsing Error

Censys

Domain Owner

Identified Faults

② **Entrust Search and Facebook Monitor prohibited queries with IDN-ccTLD**

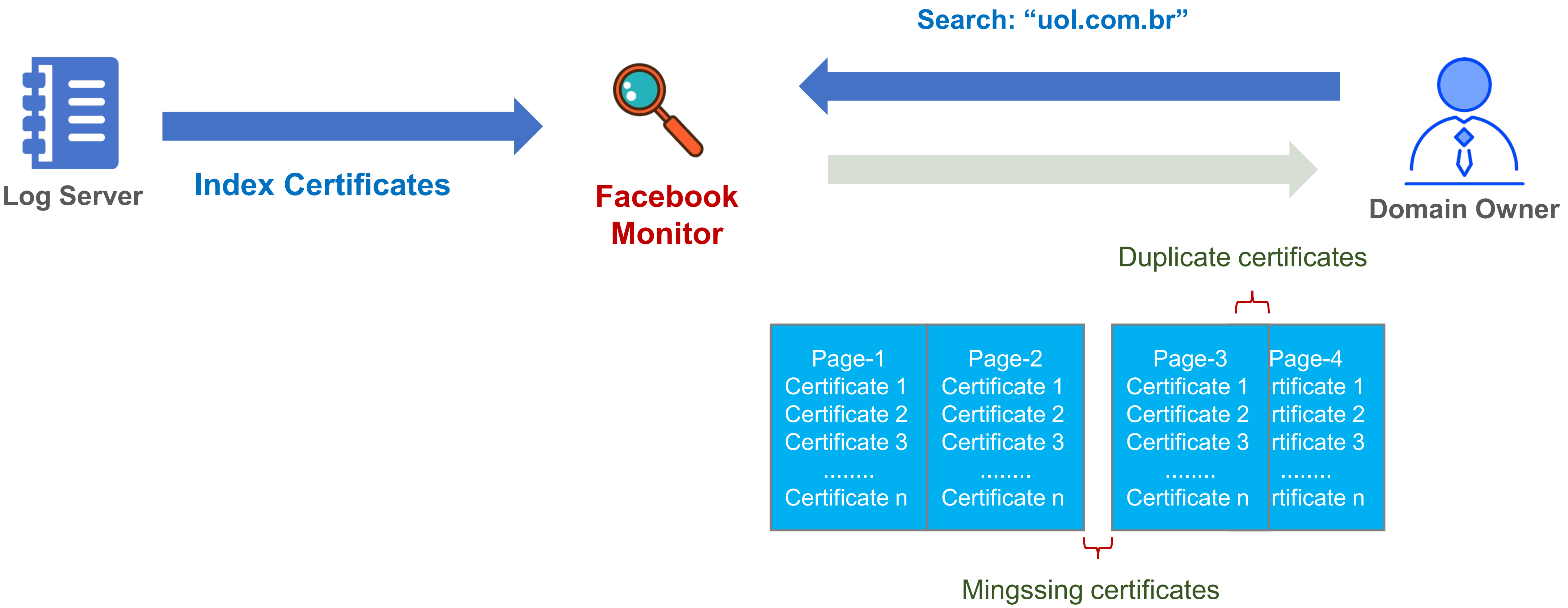


Certificate:
SAN:dNSName:
xn--b1amahh6b.xn--p1ai

Search: “xn--b1amahh6b.xn--p1ai”

Identified Faults

③ **Facebook Monitor may have error when returning certificates in multiple pages**



Search: “uol.com.br”

Log Server

Index Certificates

Facebook Monitor

Domain Owner

Duplicate certificates

Page-1	Page-2	Page-3	Page-4
Certificate 1	Certificate 1	Certificate 1	rtificate 1
Certificate 2	Certificate 2	Certificate 2	rtificate 2
Certificate 3	Certificate 3	Certificate 3	rtificate 3
....	....	....	....
Certificate n	Certificate n	Certificate n	rtificate n

Mingssing certificates

Operating Cost of Light Watchers

Average Cost for Processing a Domain Per Search Period

	Downloads	Storage	Time	Cost
Censys	0.16MB	0.19MB	-	Free/$0.04
crt.sh	0.23MB	0.26MB	5.21s	Free
Entrust Search	0.12MB	0.28MB	9.91s	Free
Facebook Monitor	0.16MB	0.28MB	14.1s	Free
Google Monitor	0.36MB	0.41MB	79.7s	Free
SSLMate Spotter	0.16MB	0.19MB	87.98s	Free/$0.002
Watcher	**1.19MB**	**1.97MB**	**163s**	△

Outline

- Problem and Motivation
- CT Watcher Design
- Implementation and Evaluation
- **Conclusions**

Conclusions

- We presented *CT Watcher* as a scalable inspecting service to detect and enhance the *reliability of third-party CT monitors*.
- We designed and implemented two types of watchers, i.e., automated *light watchers* and semiautomated *full watchers*.
- We conducted real-world experiments including a 52-day trial operation to validate the *effectiveness* of CT watchers.
- We discovered several design and implementation flaws and limitations in *six* commonly used third-party monitors.

Thank you for listening!

Q & A

Feel free to reach out to us if you have any questions:
fli@ku.edu, sunaozhuo@iie.ac.cn, linjq@ustc.edu.cn