



THE COMPUTER SECURITY GROUP AT UC SANTA BARBARA

CLOUD STRIFE

Mitigating the Security Risks of Domain-Validated Certificates

Kevin Borgolte

Tobias Fiebig

Shuang Hao

Christopher Kruegel

Giovanni Vigna

`kevinbo@cs.ucsb.edu`

`t.fiebig@tudelft.nl`

`shao@utdallas.edu`

`chris@cs.ucsb.edu`

`vigna@cs.ucsb.edu`



Arne Swinnen (arneswinnen)

4002

Reputation

76th

Rank

6.81

Signal

97th

Percentile

129

#219205

Authentication bypass on auth.uber.com via subdomain takeover of saostatic.uber.com

Share:

State ● Resolved (Closed)

Severity ■ Critical (9.3)

Disclosed publicly July 12, 2017 5:43pm -0700

Participants

Reported To [Uber](#)

Visibility Public (Full)

Weakness Improper Authentication - Generic

Bounty \$5,000

STALE DNS RECORDS AND IP ADDRESS RE-USE

`cloudstrife.seclab.cs.ucsb.edu`

STALE DNS RECORDS AND IP ADDRESS RE-USE

`cloudstrife.seclab.cs.ucsb.edu`



`34.215.255.68`

STALE DNS RECORDS AND IP ADDRESS RE-USE

`cloudstrife.seclab.cs.ucsb.edu`



`34.215.255.68`

- How to migrate DNS gracefully?

STALE DNS RECORDS AND IP ADDRESS RE-USE

`cloudstrife.seclab.cs.ucsb.edu`



- How to migrate DNS gracefully?
- When to release 34.215.255.68? TTL? Longer?

STALE DNS RECORDS AND IP ADDRESS RE-USE

`cloudstrife.seclab.cs.ucsb.edu`

 `34.215.255.68`

- How to migrate DNS gracefully?
- When to release `34.215.255.68`? TTL? Longer?
- What about failure and automatic scaling?

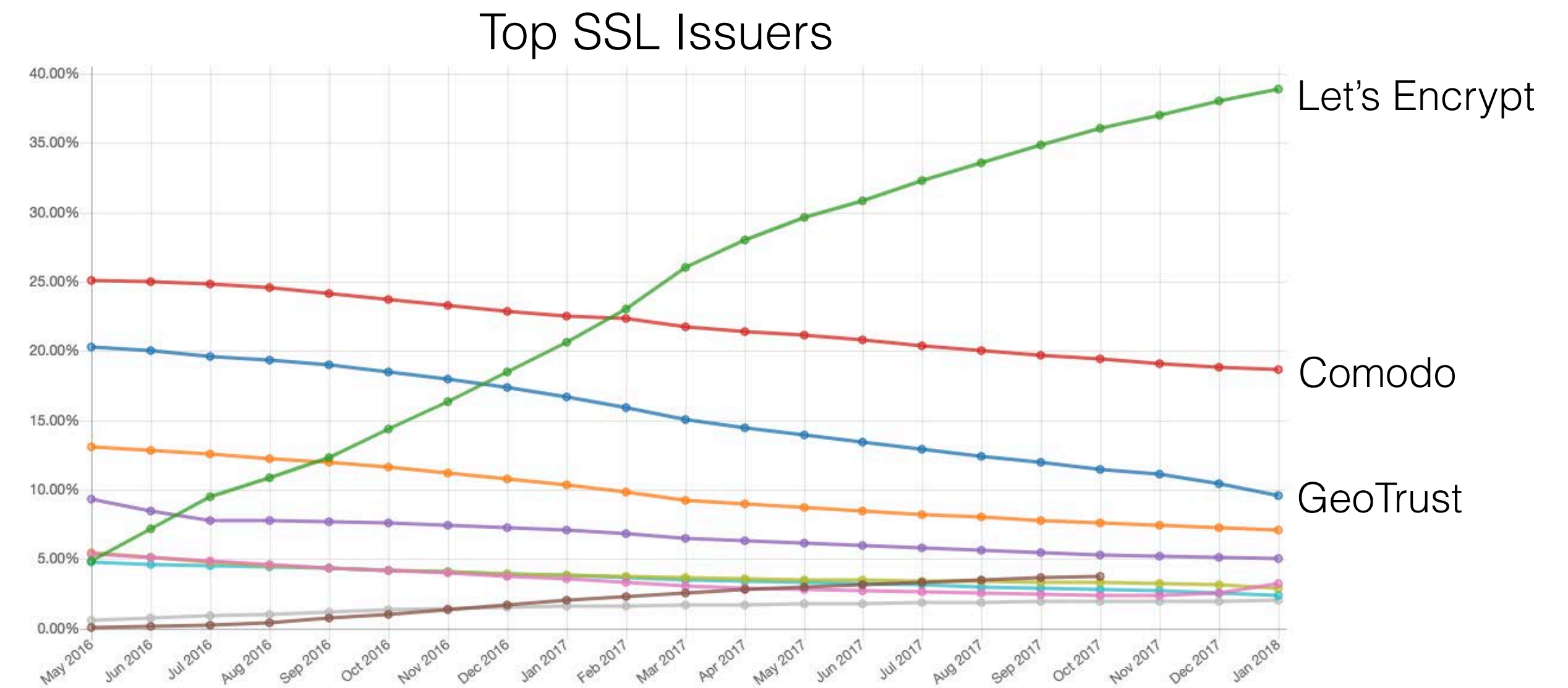
DOMAIN-VALIDATED CERTIFICATES

- Standard TLS certificate
- Trusted by major browsers and operating systems
- Credited for the rise in HTTPS adoption
- Cheap or free
- No identity verification



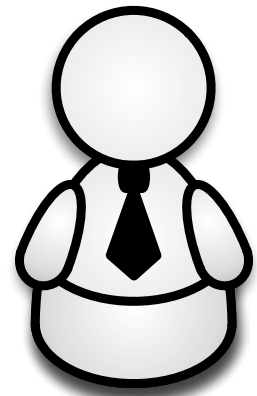
Let's Encrypt Hits 50 Million Active Certificates and Counting

BY GENNIE GEBHART AND SETH SCHOEN | FEBRUARY 14, 2018



via https://nettrack.info/ssl_certificate_issuers.html

HTTP-BASED DOMAIN-VALIDATION

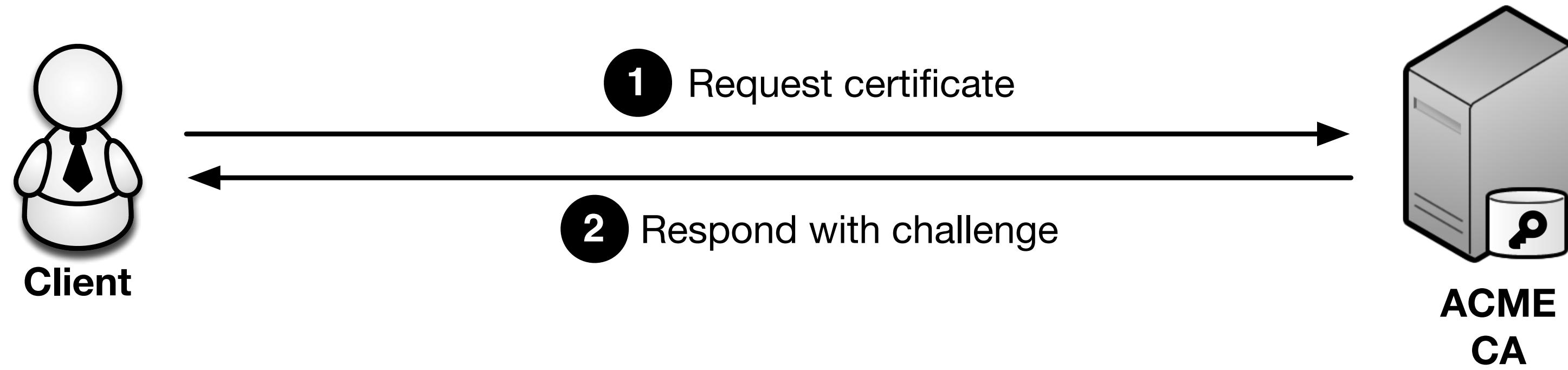


Client

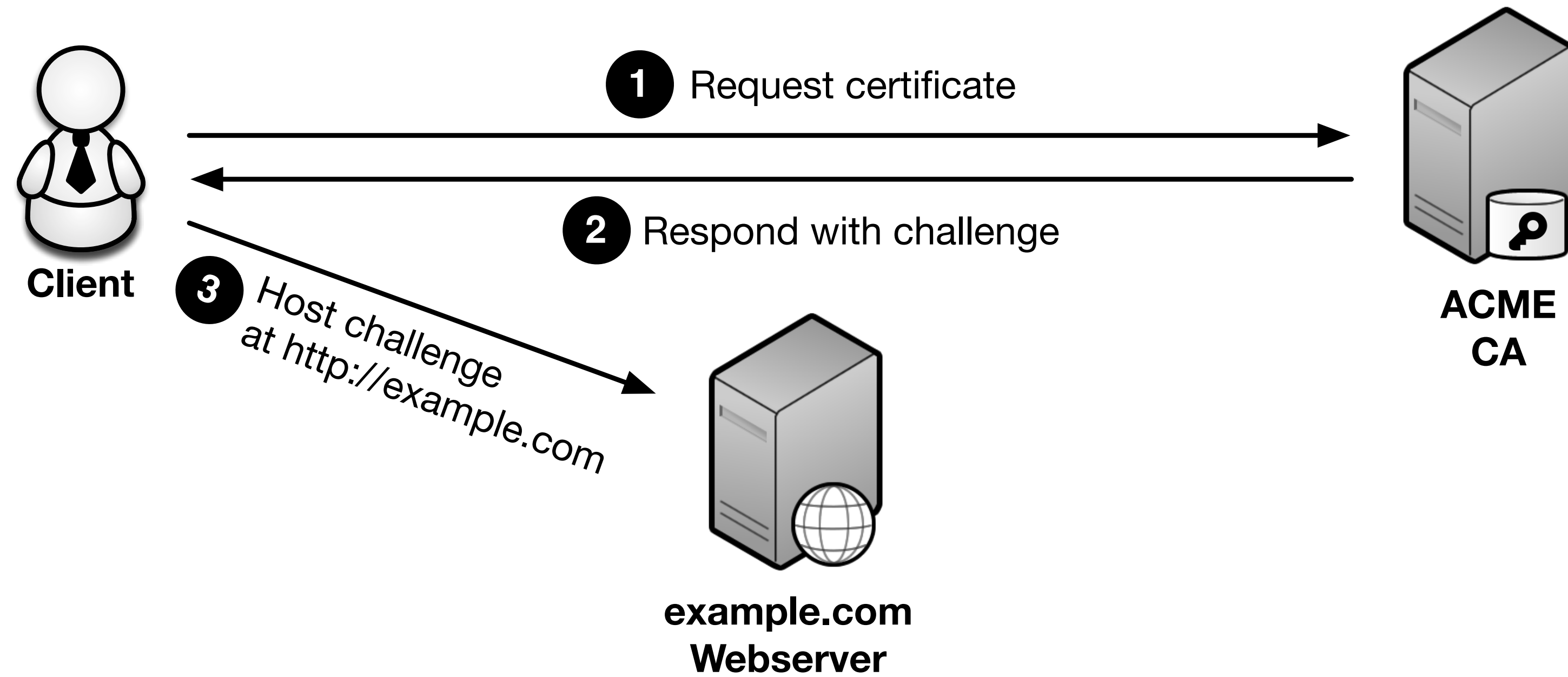
HTTP-BASED DOMAIN-VALIDATION



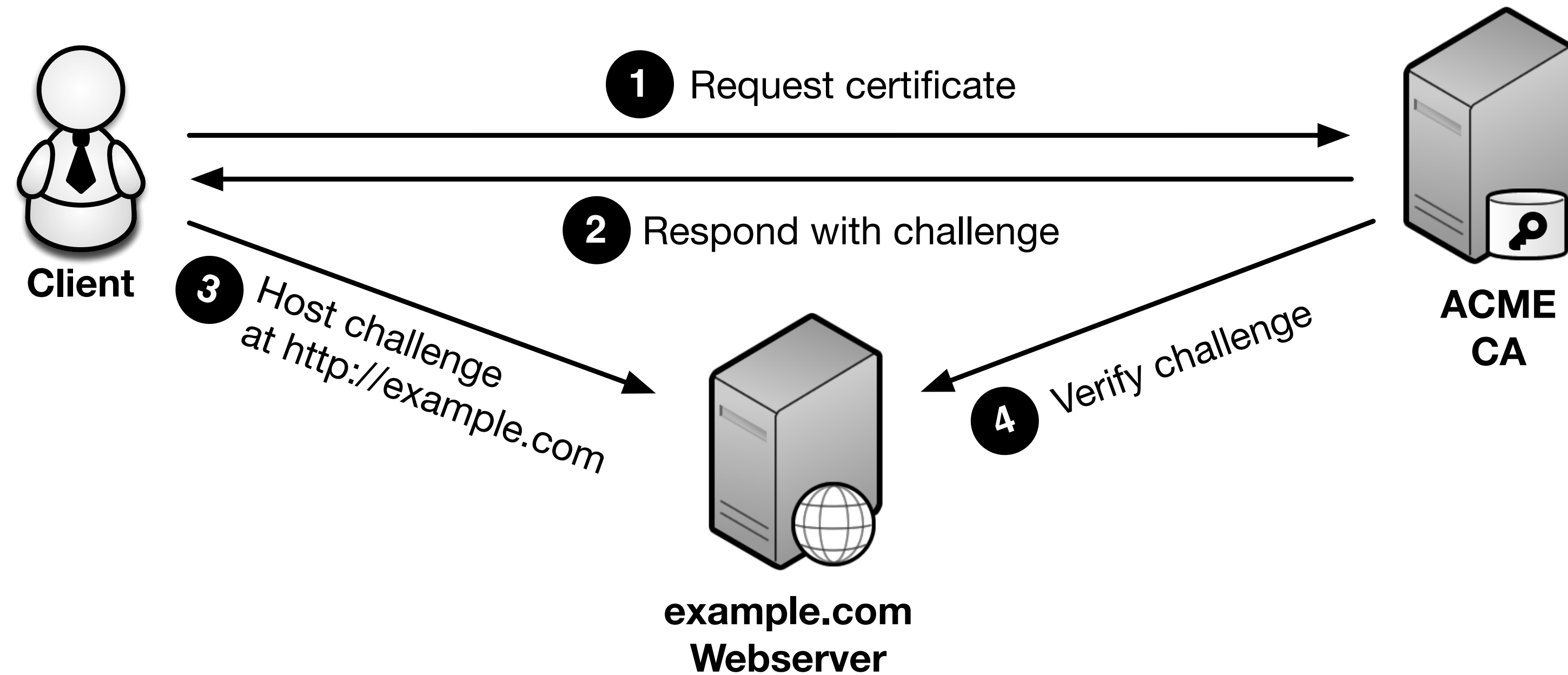
HTTP-BASED DOMAIN-VALIDATION



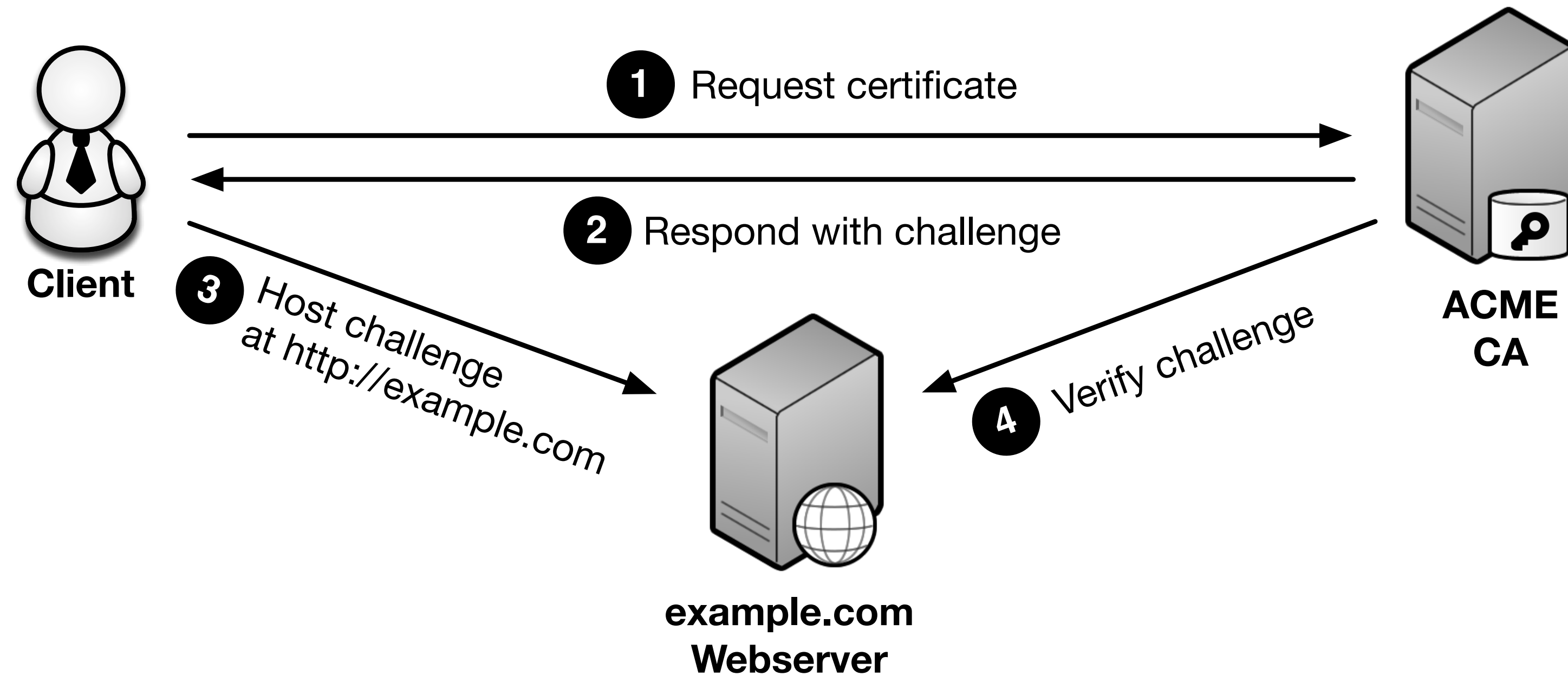
HTTP-BASED DOMAIN-VALIDATION



HTTP-BASED DOMAIN-VALIDATION



HTTP-BASED DOMAIN-VALIDATION



If you control the host behind the domain, then you can prove domain ownership successfully.

IMPACT?

- Trusted TLS certificates (MitM)
- Malicious and remote code loading
- Subdomain attacks
- Email (no MX = A record)
- Spam & phishing (residual trust)

Comodo SSL > Wildcard SSL Certificate

Wildcard SSL Certificate

- Best combination of flexibility, compatibility, and value -

🔒 Get Comodo SSL if you want:

- ✓ Multiple subdomains
- ✓ Multiple servers
- ✓ Fast online validation

1 Yr: \$449.95 /yr
2 Yrs: \$427.95 /yr - save 5%
✓ 3 Yrs: \$404.95 /yr - save 10%


ADD TO CART

Feb 5, 2018 - James Ritchey

GitLab Pages Security Issue Notification

Issue Summary


When a user adds a **custom domain** to their Pages site, no validation was being performed to ensure the domain was owned by that user. This issue allows an attacker to discover DNS records already pointing to the GitLab Page IP address which haven't been claimed and potentially hijack them. This issue impacts all users who have created and then deleted custom domains using GitLab Pages, but still have the DNS records active.

 Arne Swinnen (arneswinnen)

4002 Reputation | 76th Rank | 6.81 Signal | 97th Percentile

#219205 Authentication bypass on auth.uber.com via subdomain takeover of saostatic.uber.com

State: Resolved (Closed) | Severity: Critical (9.3)

Disclosed publicly: July 12, 2017 5:43pm -0700 | Participants: 

Reported To: Uber | Visibility: Public (Full)

Weakness: Improper Authentication - Generic

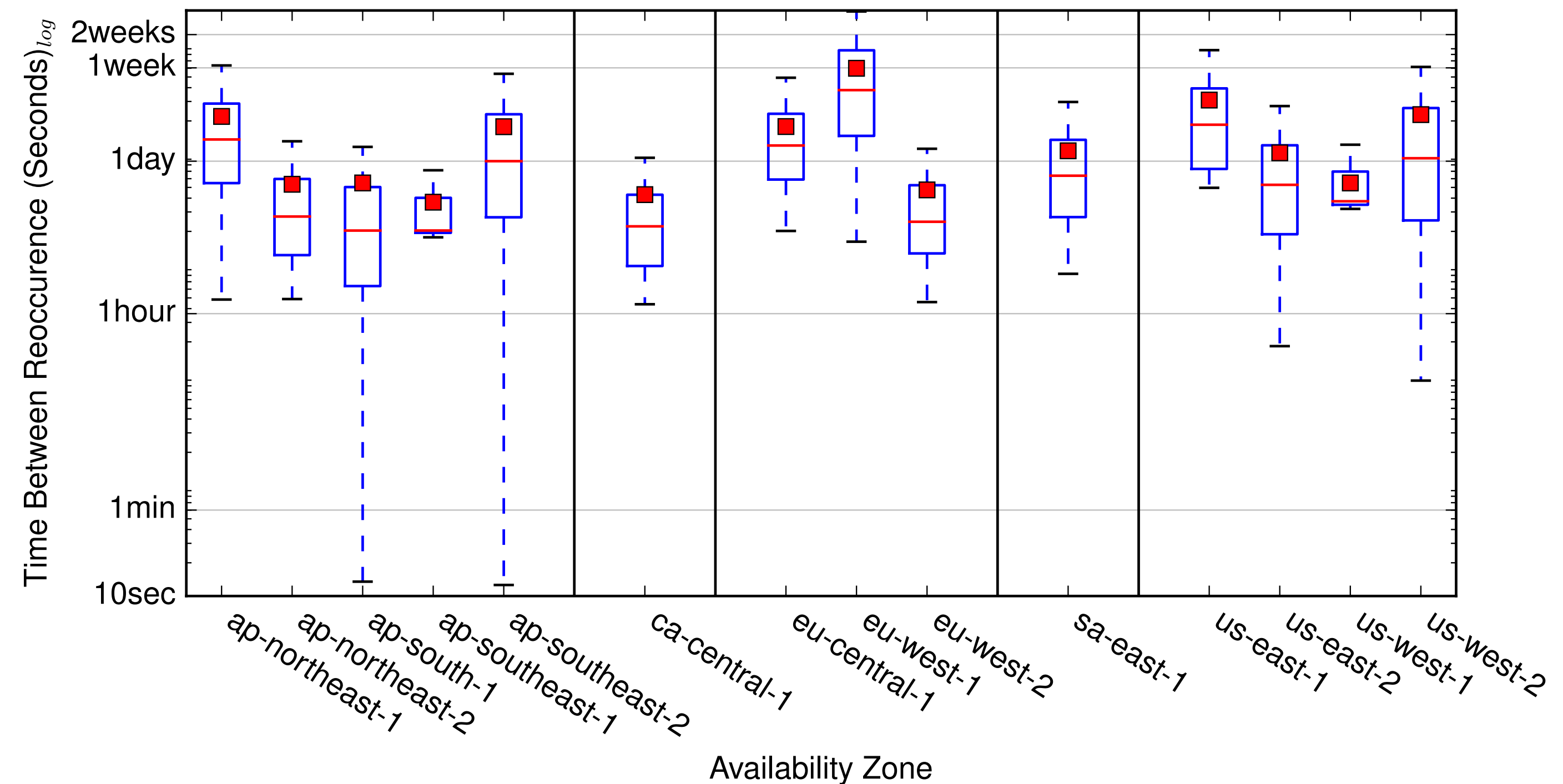
Bounty: \$5,000

SCALE?

- How many **active** domains point to free IPs?

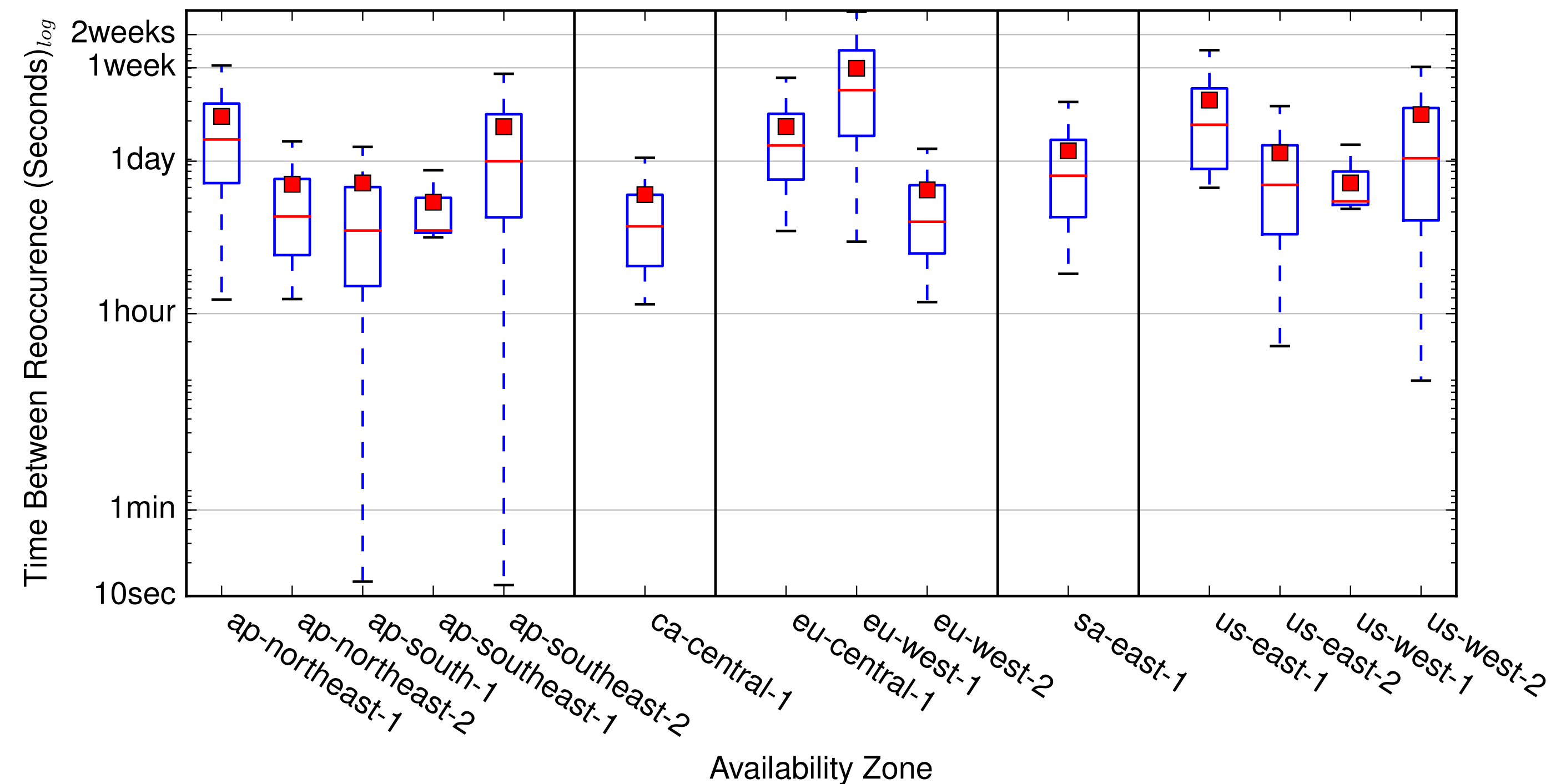
SCALE?

- How many **active** domains point to free IPs?
- Looking at cloud IP address (AWS, Azure)
- 1.6 million unique IPs, 14 million allocations
- 130 million unique domains



SCALE?

- How many **active** domains point to free IPs?
- Looking at cloud IP address (AWS, Azure)
- 1.6 million unique IPs, 14 million allocations
- 130 million unique domains
- >700,000 domains can be taken over within minutes by attacker



CLOUD STRIFE

- Assume takeovers can or will happen in the future
- Major changes to DNS or deployment impractical
- Aim to prevent attacks higher up

CLOUD STRIFE

- Assume takeovers can or will happen in the future
- Major changes to DNS or deployment impractical
- Aim to prevent attacks higher up

- Focus on TLS services
- Leverage existing standards when possible

MITIGATING TAKEOVER ATTACKS

- HTTP, simple idea:
 - HTTPS with trusted certificates
 - HTTP Strict Transport Security
 - HTTP Public Key Pinning

MITIGATING TAKEOVER ATTACKS

- HTTP, simple idea:
 - HTTPS with trusted certificates
 - HTTP Strict Transport Security
 - HTTP Public Key Pinning

Takeover attacks now require pinned certificate.

Reduces takeover attacks to denial of service attacks

MITIGATING TAKEOVER ATTACKS

- HTTP, simple idea:
 - HTTPS with trusted certificates
 - HTTP Strict Transport Security
 - HTTP Public Key Pinning

Takeover attacks now require pinned certificate.

Reduces takeover attacks to denial of service attacks

Doesn't work for SMTP etc. though

MITIGATING TAKEOVER ATTACKS

- HTTP, simple idea:
 - ~~HTTPS with trusted certificates~~ domain-validated certificates
 - HTTP Strict Transport Security
 - ~~HTTP Public Key Pinning~~ to be deprecated in Chrome 67

Takeover attacks now require pinned certificate.

Reduces takeover attacks to denial of service attacks

Doesn't work for SMTP etc. though

MITIGATING TAKEOVER ATTACKS

- HTTP, better idea:
 - HTTPS with trusted certificates
 - Prevent certificate issuance via HTTP-based domain-validation for domains (likely) taken over
 - HTTP Strict Transport Security

MITIGATING TAKEOVER ATTACKS

- HTTP, better idea:
 - HTTPS with trusted certificates
 - Prevent certificate issuance via HTTP-based domain-validation for domains (likely) taken over
 - HTTP Strict Transport Security

No trusted certificate = also works for SMTP etc.

MITIGATING TAKEOVER ATTACKS

- HTTP, better idea:
 - HTTPS with trusted certificates
 - Prevent certificate issuance via HTTP-based domain-validation for domains (likely) taken over
 - HTTP Strict Transport Security

No trusted certificate = also works for SMTP etc.

How do you prevent certificate issuance?

CERTIFICATE TRANSPARENCY LOGS

- Public append-only log for issued certificates
- Monitor for suspicious certificates
- Real-time(ish) audit trail

CERTIFICATE TRANSPARENCY LOGS

- Public append-only log for issued certificates
- Monitor for suspicious certificates
- Real-time(ish) audit trail

In itself:

- Reactive: attacker's window of opportunity remains
- Must be actively monitored (by domain owners)

CERTIFICATE TRANSPARENCY LOGS

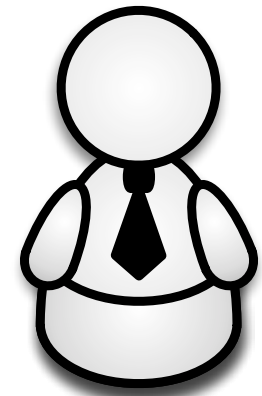
- Public append-only log for issued certificates
- Monitor for suspicious certificates
- Real-time(ish) audit trail

In itself:

- Reactive: attacker's window of opportunity remains
- Must be actively monitored (by domain owners)

Can be used for historic lookups

PREVENTIVE HTTP-BASED DOMAIN-VALIDATION

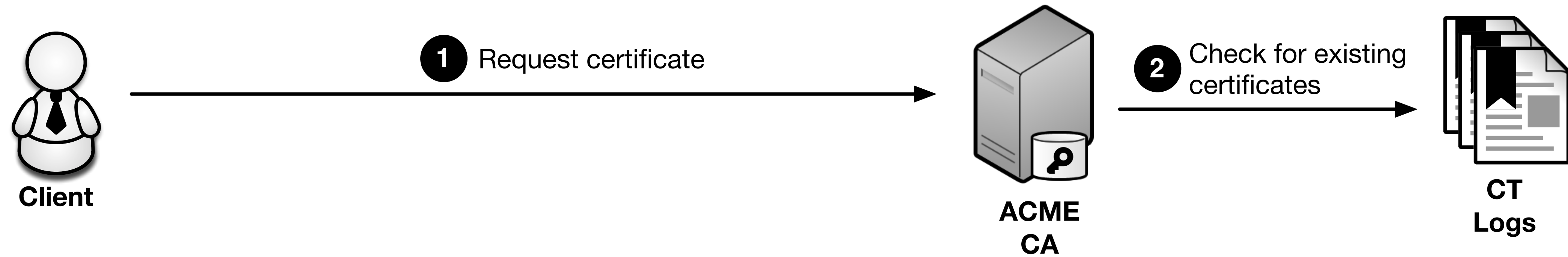


Client

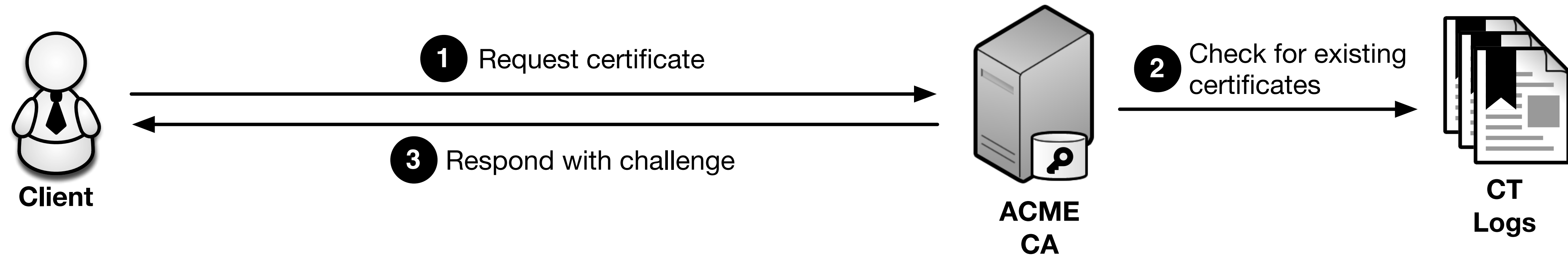
PREVENTIVE HTTP-BASED DOMAIN-VALIDATION



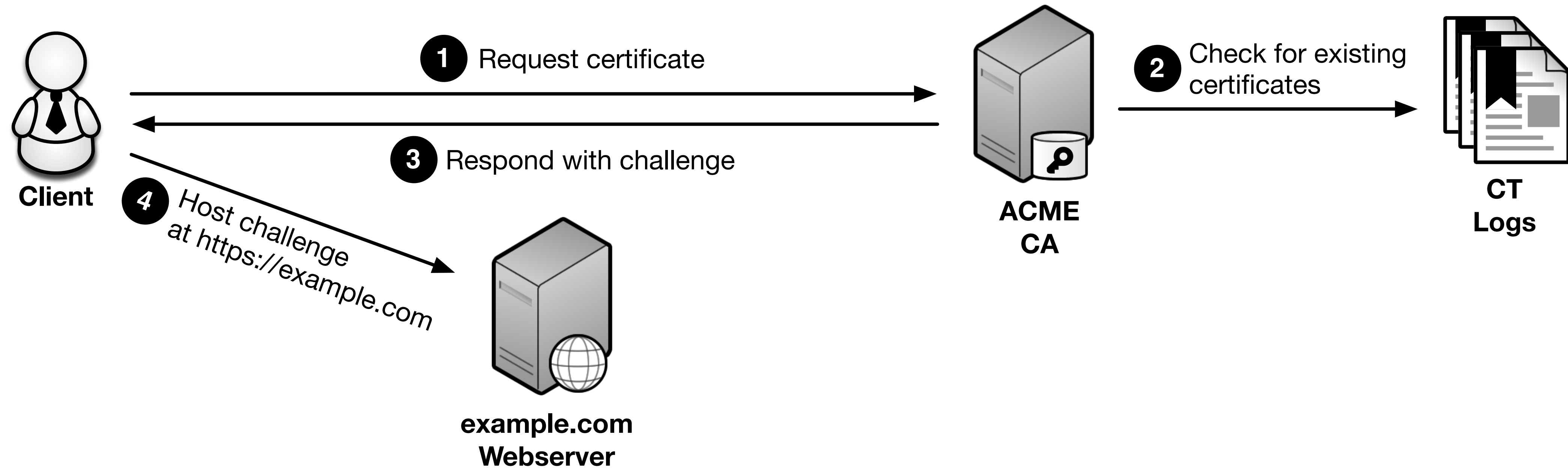
PREVENTIVE HTTP-BASED DOMAIN-VALIDATION



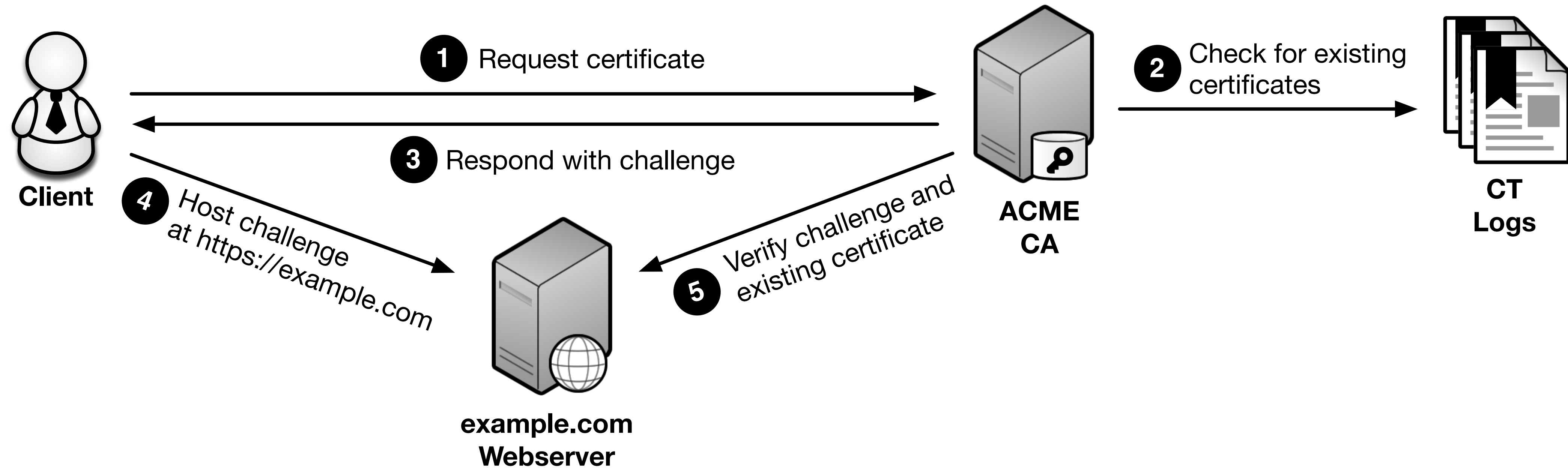
PREVENTIVE HTTP-BASED DOMAIN-VALIDATION



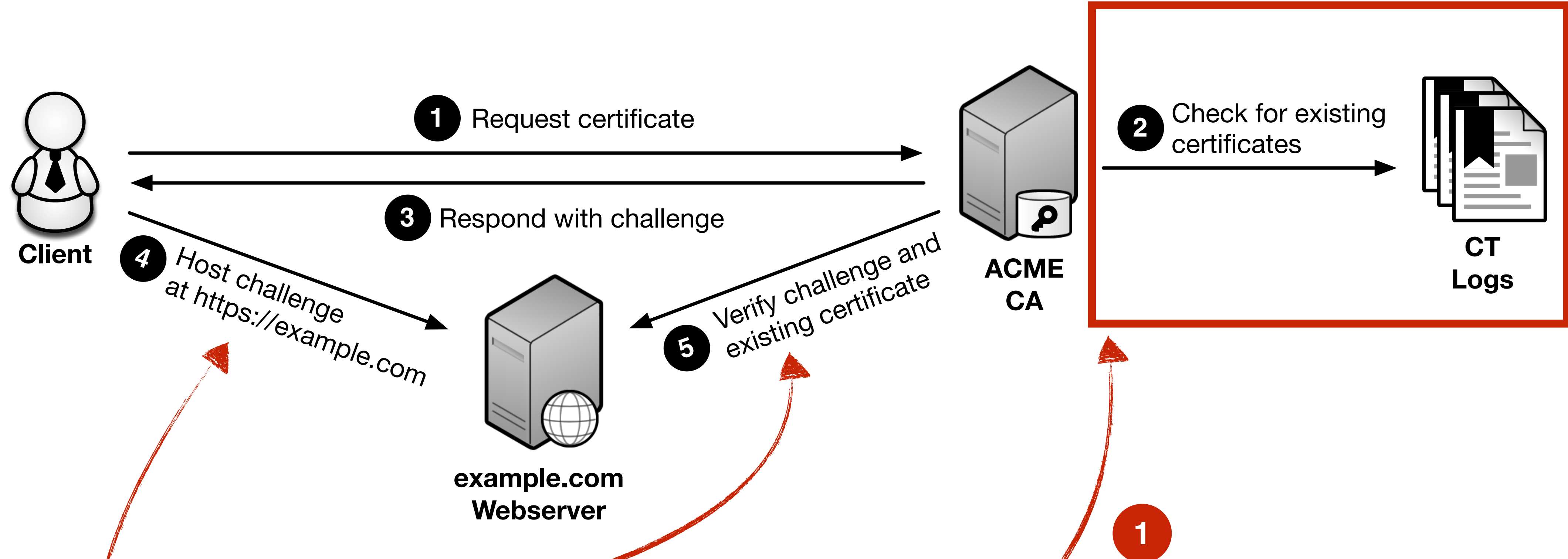
PREVENTIVE HTTP-BASED DOMAIN-VALIDATION



PREVENTIVE HTTP-BASED DOMAIN-VALIDATION



PREVENTIVE HTTP-BASED DOMAIN-VALIDATION



If an old certificate was found, require it to be current HTTPS certificate.

CLOUD STRIFE

- Prevents TLS certificates to be issued for takeovers
- No certificate = takeover attacks less useful (= DoS)
- Drawbacks for users only for disaster recovery
 - Re-bootstrap chain of trust
- ACMEv2 challenge RFC being drafted

Thank you!

Questions?



I am looking for a faculty position!