CLOUD STRIFE

Mitigating the Security Risks of Domain-Validated Certificates

Kevin Borgolte kevinbo@cs.ucsb.edu
Tobias Fiebig t.fiebig@tudelft.nl
Shuang Hao shao@utdallas.edu
Christopher Kruegel chris@cs.ucsb.edu
Giovanni Vigna vigna@cs.ucsb.edu

Applied Networking Research Workshop (ANRW 2018) / IETF 102

Arne Swinnen (arneswinnen)

4002	76th	6.81	97th
Reputation	Rank	Signal	Percentile

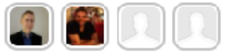
129

#219205

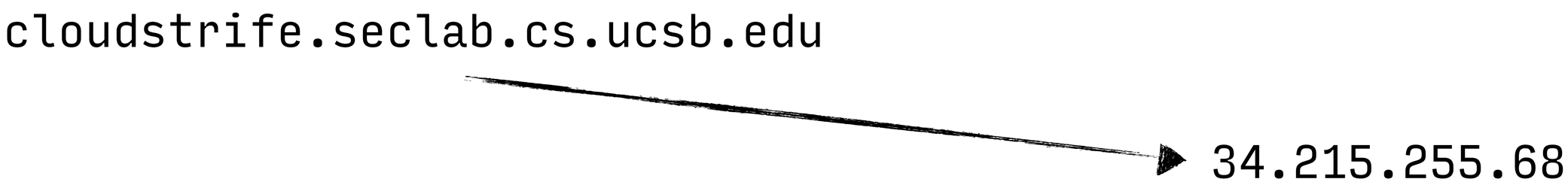
Authentication bypass on auth.uber.com via subdomain takeover of saostatic.uber.com

Share:

State	Resolved (Closed)
Disclosed publicly	July 12, 2017 5:43pm -0700
Reported To	Uber
Weakness	Improper Authentication - Generic
Bounty	$5,000

Severity	Critical (9.3)
Participants	
Visibility	Public (Full)

Stale DNS Records and IP Address Re-Use



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

Domain-Validated Certificates

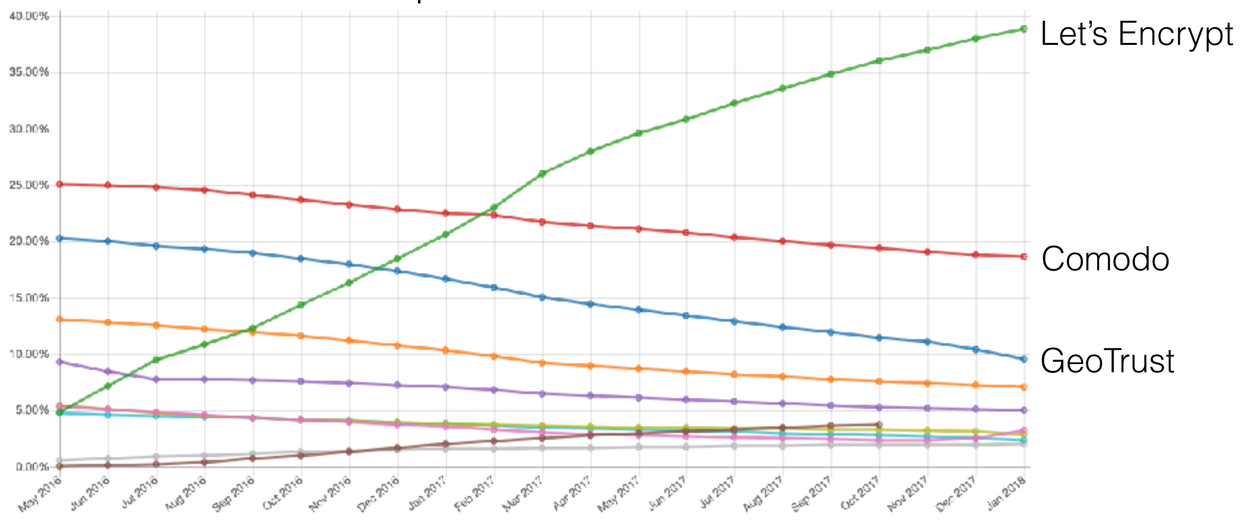
- Standard TLS certificate
- Trusted by major browsers and operating systems
- Credited for the rise in HTTPS adoption
- Cheap or free
- No identity verification

ELECTRONIC FRONTIER FOUNDATION

Let's Encrypt Hits 50 Million Active Certificates and Counting

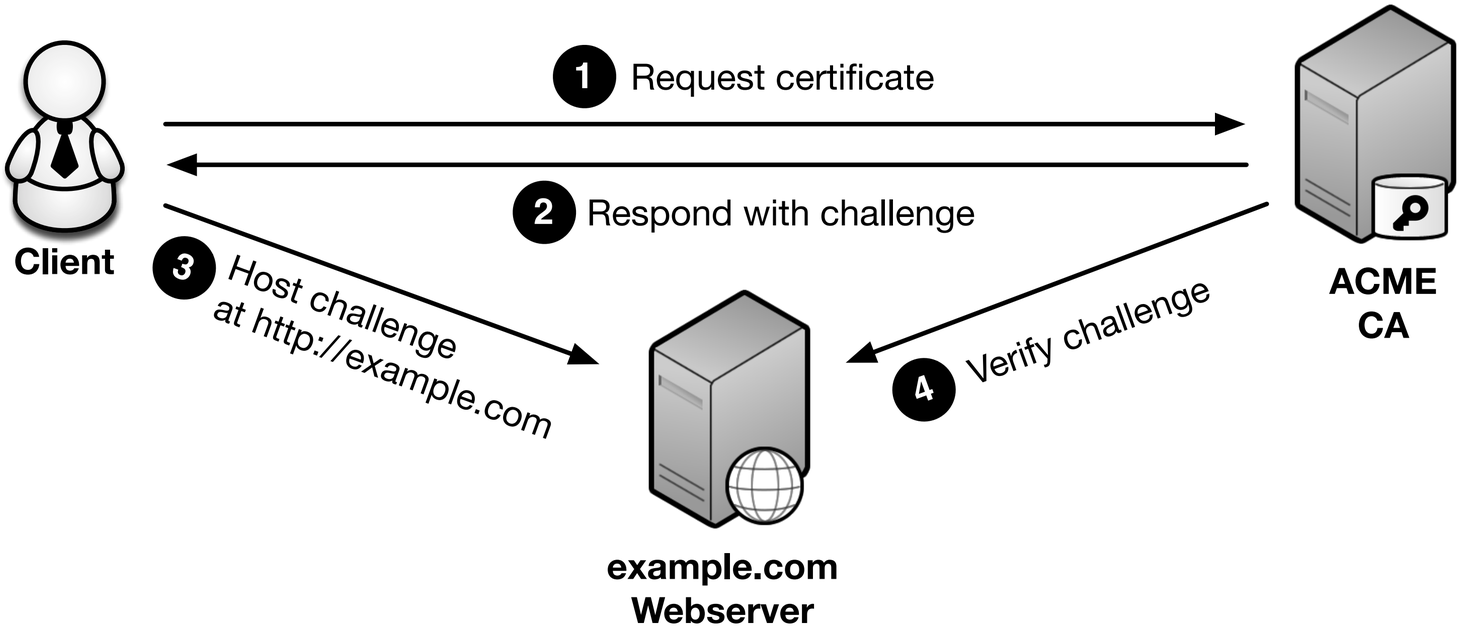
BY GENNIE GEBHART AND SETH SCHOEN | FEBRUARY 14, 2018

Top SSL Issuers



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

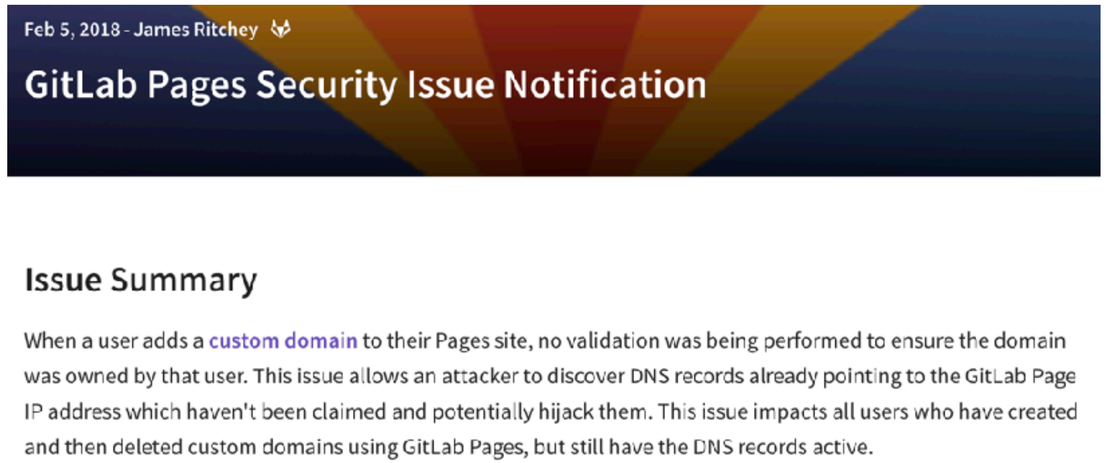
HTTP-Based Domain-Validation

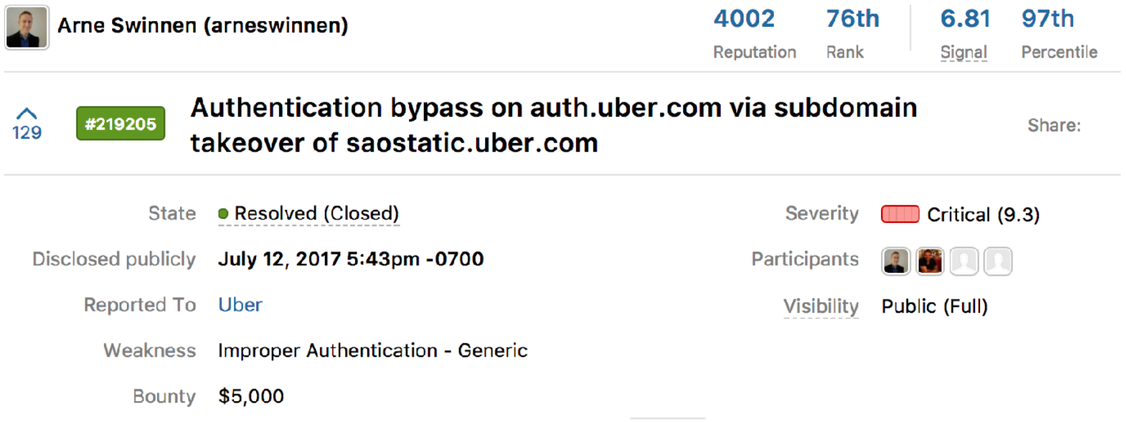


If you control the host behind the domain, then you can prove domain ownership successfully.

IMPACT?

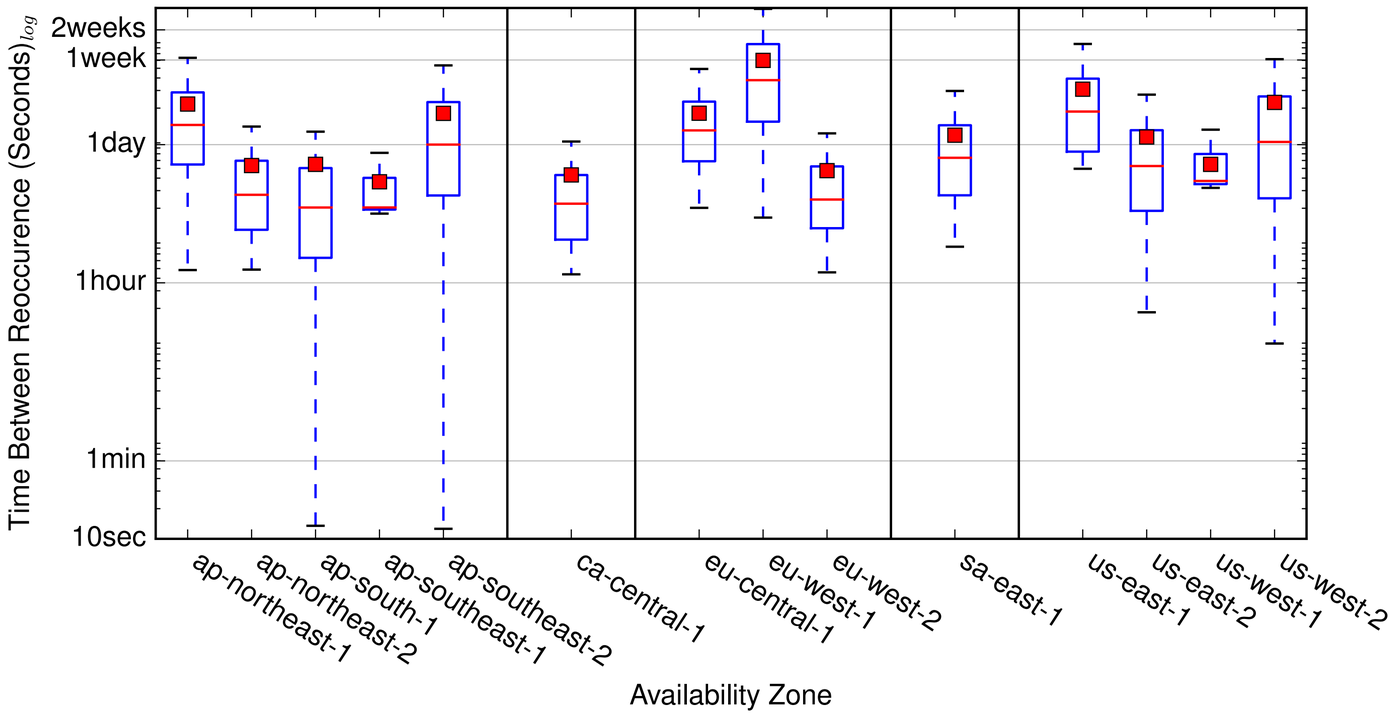
- Trusted TLS certificates (MitM)
- Malicious and remote code loading
- Subdomain attacks
- Email (no MX = A record)
- Spam & phishing (residual trust)





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 and 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~~ domain-validated certificates
  - HTTP Strict Transport Security
  - ~~HTTP Public Key Pinning~~ deprecated since 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 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

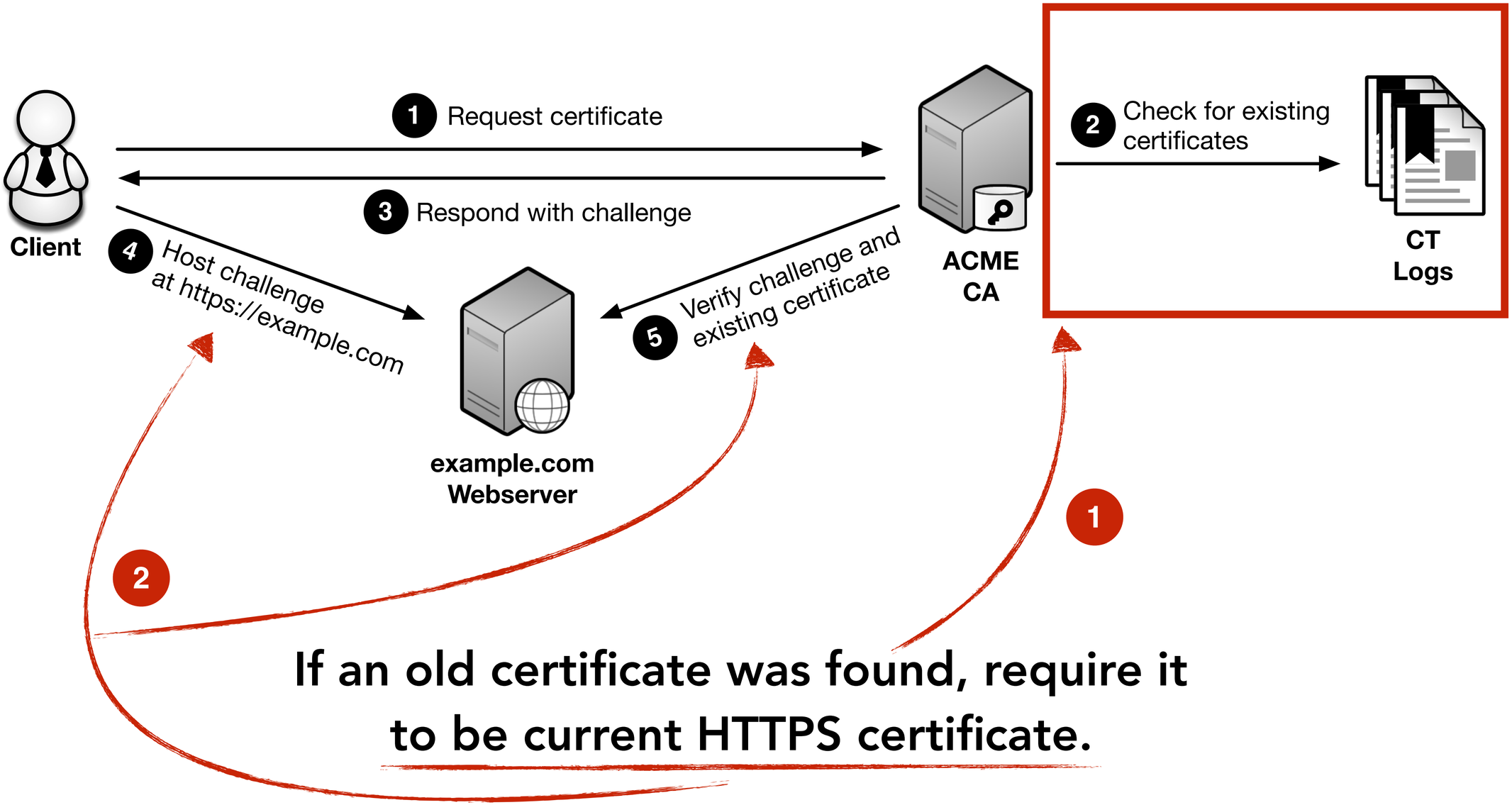
- Public append-only log for issued certificates
- Monitor for suspicious certificates
- Real-time(ish) audit trail

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



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
- ACME validation challenge draft next?

Thank you!

Questions?

seclab

THE COMPUTER SECURITY GROUP AT UC SANTA BARBARA

kevinbo@cs.ucsb.edu
https://kevin.borgolte.me
twitter: @caovc