@chelloway

Proving prior-key possession to mitigate IP-use-after-free attacks

Tobias Fiebig, Kevin Borgolte

TUDelft

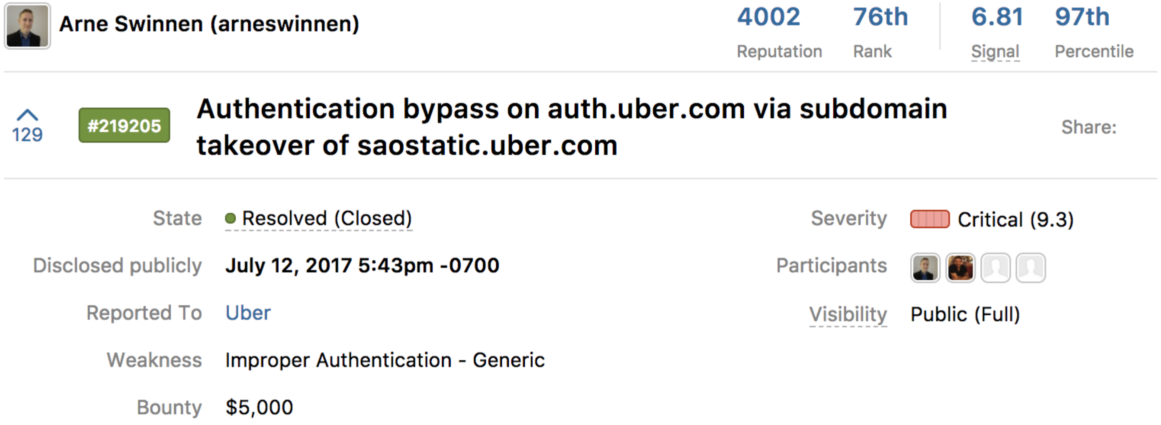
The Problem: IP-use-after-free

- Attackers can re-use IP addresses if a stale DNS record still point to them
  - Serious problem (found >700,000 Domains only with Amazon EC2)

- Problem for ACME: We are verifying the target (IP) to which a domain points as a proxy for verifying authority over a domain

The Problem: *-use-after-free

- Also hits other things we use to point domains at: Loadbalancer, BGP hijacks,…



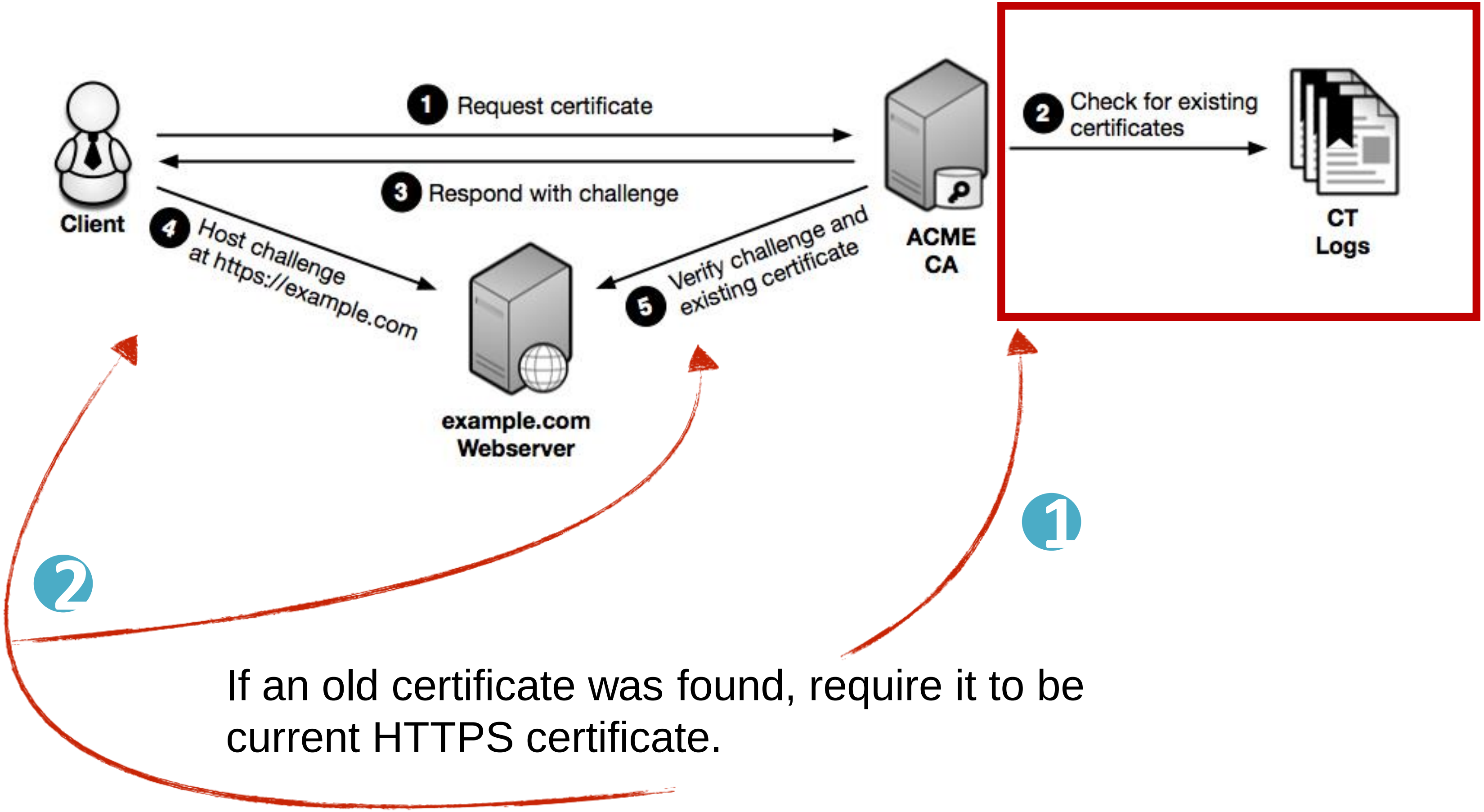
Arne Swinnen (arneswinnen)

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)	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		


1 Request certificate
3 Respond with challenge
Client
4 Host challenge at https://example.com
5 Verify challenge and existing certificate
ACME CA
2 Check for existing certificates
CT Logs
example.com Webserver
1
2

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

What to do when things fail

- When to fail: Expired certs?
- Proof of (prior) key possession originally planned (-00 §7.3)
- What to do when this fails?
  - Gracefully to DNS Challenge?
  - Corner cases: Lost keys, disaster, broken deployment processes

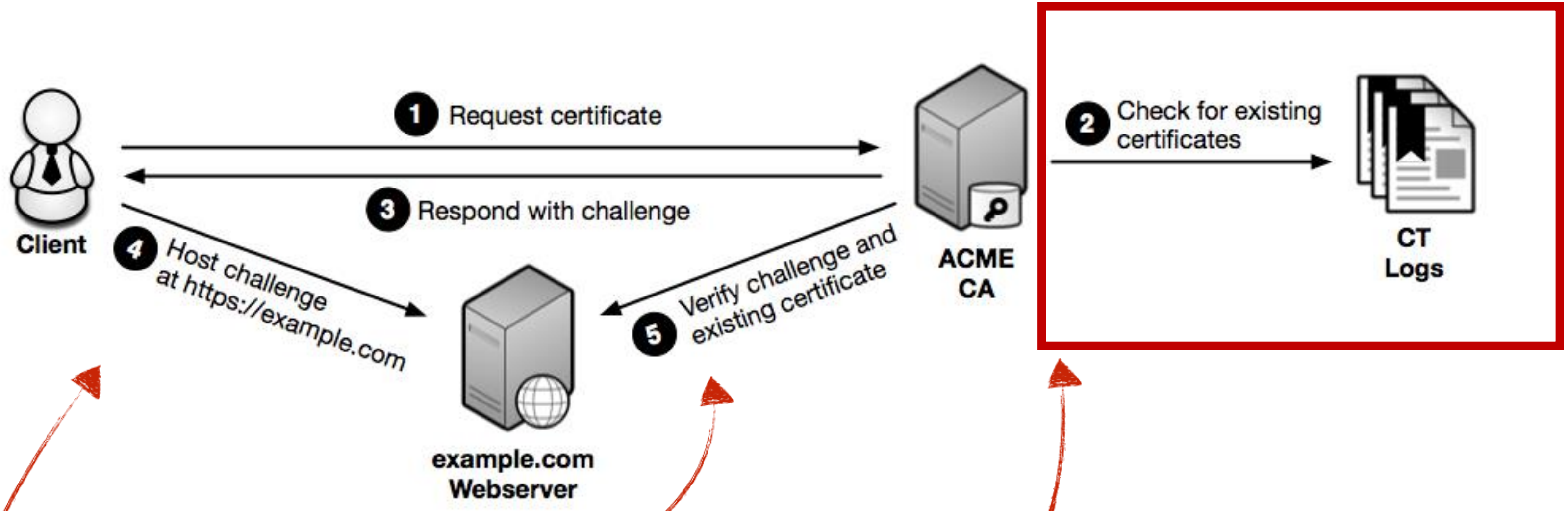
Problems to solve

- Problems with using HTTPS
  - Not allowed in base HTTP challenge (-12 §8.3)
  - Default vhosts
    - Not a problem here (can assume prior cert)

- Build a dedicated challenge format?
  - Rolling own crypto?
  - Using keys for non-original purpose

Next Steps

- Measurements:
  - Figure out corner cases
  - How many certs would be affected?
- Write a Draft next few weeks
  - Discussion in Bangkok?
- Write PRs to ACME client/server


1 Request certificate
3 Respond with challenge
Client
4 Host challenge at https://example.com
example.com Webserver
5 Verify challenge and existing certificate
ACME CA
2 Check for existing certificates
CT Logs

1

2

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