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

State: Resolved (Closed)
Disclosed publicly: July 12, 2017 5:43pm -0700
Reported To: Uber
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

34.215.255.68

• 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

Top SSL Issuers

- Let's Encrypt
- Comodo
- GeoTrust
HTTP-BASED DOMAIN-VALIDATION
HTTP-BASED DOMAIN-VALIDATION

1. Request certificate

Client → ACME CA
HTTP-BASED DOMAIN-VALIDATION

1. Request certificate
2. Respond with challenge
HTTP-BASED DOMAIN-VALIDATION

1. Request certificate
2. Respond with challenge
3. Host challenge at http://example.com

Client → ACME CA

example.com Webserver
HTTP-BASED DOMAIN-VALIDATION

1. Request certificate
2. Respond with challenge
3. Host challenge at http://example.com
4. Verify challenge

ACME CA

Client

Webserver
e.g., example.com
HTTP-BASED DOMAIN-VALIDATION

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

Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates (NDSS 2018)

- 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?
• 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
• 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

---

**SCALE?**
• 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
PREVENTIVE HTTP-BASED DOMAIN-VALIDATION

1 Request certificate

Client → ACME CA
PREVENTIVE HTTP-BASED DOMAIN-VALIDATION

1. Request certificate
2. Check for existing certificates
PREVENTIVE HTTP-BASED DOMAIN-VALIDATION

1. Request certificate
2. Check for existing certificates
3. Respond with challenge
PREVENTIVE HTTP-BASED DOMAIN-VALIDATION

1. Request certificate
2. Check for existing certificates
3. Respond with challenge
4. Host challenge at https://example.com

Client

ACME CA

example.com Webserver

CT Logs
PREVENTIVE HTTP-BASED DOMAIN-VALIDATION

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

Client

ACME CA

example.com
Webserver

CT Logs
PREVENTIVE HTTP-BASED DOMAIN-VALIDATION

1. **Request certificate**
2. **Check for existing certificates**
3. **Respond with challenge**
4. **Host challenge at https://example.com**
5. **Verify challenge and existing certificate**

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

Client

ACME CA

CT Logs

Webserver

example.com

Kevin Borgolte

Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates (NDSS 2018)
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?

Kevinbo@cs.ucsb.edu
https://kevin.borgolte.me
Twitter: @caovc

I am looking for a faculty position!