Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates

Kevin Borgolte
UC Santa Barbara
kevinbo@cs.ucsb.edu

Tobias Fiebig
TU Delft
t.fiebig@tudelft.nl

Shuang Hao
UT Dallas
shao@utdallas.edu

Christopher Kruegel
UC Santa Barbara
chris@cs.ucsb.edu

Giovanni Vigna
UC Santa Barbara
vigna@cs.ucsb.edu

ABSTRACT

Infrastructure-as-a-Service (IaaS), more generally the "cloud," changed the landscape of system operations on the Internet. Clouds' elasticity allow operators to rapidly allocate and use resources as needed, from virtual machines, to storage, to IP addresses, which is what made clouds popular. We show that the dynamic component paired with developments in trust-based ecosystems (e.g., TLS certificates) creates so far unknown attacks. We demonstrate that it is practical to allocate IP addresses to which stale DNS records point. Considering the ubiquity of domain validation in trust ecosystems, like TLS, an attacker can then obtain a valid and trusted certificate. The attacker can then impersonate the service, exploit residual trust for phishing, or might even distribute malicious code. Even worse, an aggressive attacker could succeed in less than 70 seconds, well below common time-to-live (TTL) for DNS. In turn, she could exploit normal service migrations to obtain a valid certificate, and, worse, she might not be bound by DNS records being (temporarily) stale. We introduce a new authentication method for trust-based domain validation, like IETF's automated certificate management environment (ACME), that mitigates staleness issues without incurring additional certificate requester effort by incorporating the existing trust of a name into the validation process.

Based on previously published work [1].

[1] Kevin Borgolte, Tobias Fiebig, Shuang Hao, Christopher Kruegel, Giovanni Vigna. February 2018. Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates. In Proceedings of the 25th Network and Distributed Systems Security Symposium (NDSS '18). Internet Society (ISOC). DOI: 10.14722/ndss.2018.23327. URL: https://doi.org/10.14722/nd

CCS CONCEPTS

• **Security and privacy** → **Security protocols**; • **Networks** → **Naming and addressing**; **Network security**; **Cloud computing**; • **Computer systems organization** → **Cloud computing**;

KEYWORDS

Domain Name System (DNS); Transport Layer Security (TLS); Secure Sockets Layer (SSL); Certificate Issuance; Domain Validation; Certificate Authority; Automated Certificate Management Environment (ACME); Certificate Transparency; Cloud Computing; Misconfiguration; Trust-based Ecosystem; IP Address Re-Use; Use After Free (UAF).

ACM Reference Format:
Kevin Borgolte, Tobias Fiebig, Shuang Hao, Christopher Kruegel, and Giovanni Vigna. 2018. Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates. In *ANRW '18: Applied Networking Research Workshop, July 16, 2018, Montreal, QC, Canada.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3232755.3232859

ANRW '18, July 16, 2018, Montreal, QC, Canada

ACM ISBN 978-1-4503-5585-8/18/07.
https://doi.org/10.1145/3232755.3232859