ACME Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 24, 2019
T. Fiebig
TU Delft
K. Borgolte
Princeton University
October 21, 2018

Extended Security Considerations for the Automatic Certificate Management Environment (ESecACME)
draft-fiebig-acme-esecacme-00

Abstract

By now, most Public Key Infrastructure X.509 (PKIX) certificates are issued via the ACME protocol. Recently, several attacks against domain validation (DV) have been published, including IP-use-after-free, (forced) on-path attacks, and attacks on protocols used for validation. In general, these attacks can be mitigated by (selectively) requirering additional challenges, e.g., DNS validation, proof of prior-key-ownership, or in severe cases even extended validation (EV) instead of DV. This document provides a list of critical cases and describes which mitigations can be used to reduce the threat of issuing a certificate to an unauthorized party.

Table of Contents

1. Introduction

By now, most Public Key Infrastructure X.509 (PKIX) certificates are issued via the ACME protocol. The automated nature of ACME and its heavy use of Domain Validation (DV) make it susceptible to a variety of attacks. These include IP-use-after-free [CSTRIFE], (forced) on-path attacks [BAMBOO], and attacks on protocols used for validation [DVP], e.g., DNS. In general, these attacks can be mitigated by (selectively) requirering additional challenges, e.g., DNS validation, proof of prior-key-ownership, or in severe cases even extended validation (EV) instead of DV.

This document provides a list of potential attacks and how they can be detected. In addition, it describes which mitigations can be used to reduce the threat of issuing a certificate to an unauthorized party in case a potential attack has been detected. This section also holds information on how these mitigations may impact the usability of CAs using ACME to issue certificates.

2. Attacks

In this section we describe common attacks against DV, how they can be detected, and which additional verification methods should be used in case they are detected.

2.1. IP/Resource-use-after-free

IP- and Resource-use-after-free attacks occur if a domain owner points a DNS record to a resource, which they later vacate without deleting the DNS record. The resource, usually in cloud scenarios, can then be allocated by another party.

For example, one might run a service for www.example.com on a virtual machine hosted with a cloud provider. One then points the AAAA record of www.example.com to the IPv6 address of that virtual machine, 2001:DB8:1234:1234::1. However, when the operator discontinues the service, they do not delete this DNS record, leading to a stale record. If another client of the cloud provider now allocates a virtual machine, and receives the same IPv6 address, they can proof ownership of www.example.com to an ACME compliant CA. These observations similarly hold for DNS records pointing to legacy IPv4 resources (A records), mail servers in case of email verification using the ACME protocol (MX records), http and https delegations (SRV records), and DNS delegations if DNSSEC is not being used (NS records).

2.1.1. Detection

This attack type is difficult to detect from the CAs site, without operators taking precautions themselves, which we describe in the following section. Heuristics CAs could use depend on the availability of cooperation from operators, or require proof of prior key ownership.

Ideally, operators will use TLSA records to pin the TLS public key for a name, allowing a CA to match the TLSA record to the key for which a certificate is requested.

If a DNS challenge is used, failed DNSSEC validation may point at a resource-use-after-free attack.

A heuristic which does not require prior cooperation by operators is using Certificate Transparency (CT) logs to identify prior certificate issuances. Furthermore, CAA records could be used to limit the number of CT logs which have to be searched by the ACME compliant CA. Furthermore, if the CA with which a certificate has been requested is also the only CA allowed in the CAA, it could check the ACME account ID of prior requests vs. the one used in the current request.

2.1.2. Defense

On a mismatch between the TLSA public key and the public key used in the request, the CA must deny the requested certificate. In case of pre-existing certificates, or a mismatch in the ACME account ID, the operator should use an additional validation technique. If DNSSEC is being used, the DNS challenge is an option. Given that NS and MX records may also suffer from resource-use-after-free attacks, unauthenticated DNS and email challenges are not an option.

Due to the usability implications of the available defense options a CA may opt to only perform mitigation on high-risk resources, e.g., known cloud operators and operators with a high customer churn.

2.2. (Forced)-on-path Attacks

If an attacker can perform a Monkey-in-the-Middle (MitM) attack by controlling a part of the network path between the CA and the resource used for validation, they can also impersonate an operator and illegitimately obtain a certificate for a domain. Attackers may force this on-path situation, e.g., using BGP shorter-prefix attacks [BAMBOO].

2.2.1. Detection

To detect on-path attacks, CAs should validate challenges from multiple vantage points. For this purpose, the CA should operate a geographically and topologically distributed system for verification. This system should contain at least one validator per IP region (AfriNIC, APNIC, ARIN, LACNIC, RIPE). Similarly, a CA may monitor the BGP prefix from which it received a request with a service similar to https://bgpmon.net [1]. Note that, depending how close the attacker is to the victim, no path without malicious activity may remain, generalizing the detection issue to that outlined for resource-use-after-free attacks.

2.2.2. Defense

The same defense options as for resource-use-after-free attacks apply.

2.3. DNS Cache Poisoning Attacks

Paper just appeared; will be included in the next version of this draft.

2.3.1. Detection

2.3.2. Defense

3. Summary Indicators for Additional Validation

In this section, we summarize indicators for using an extended validation machanism.

3.1. High-Resource-Reuse Source / Cloud Provider

If the validation target for a challenge (A/AAAA/NS/MX) is located in a network with a high resources churn, e.g., a cloud or hosting provider, or a residential ISP, extended validation requirements should be considered.

3.2. Multi-Vantagepoint Validation Mismatch

If at least one of an CAs validation notes does not match the results of the other nodes, the CA must consider the requested domain to be under attack, necessitating either DNSSEC signed DNS validation, proof of prior-key-ownership or EV.

3.3. BGP monitoring

If any prefix for either the A, AAAA, MX, or NS records (or intermediate names and CNAMEs) is considered to be under a BGP MitM attack by a service similar to https://bgpmon.net [2], the CA must consider the requested domain to be under attack, necessitating either DNSSEC signed DNS validation, proof of prior-key-ownership or EV.

3.4. DNS Fragmentation

Paper just appeared; will be included in the next version of this draft.

3.5. Failed DNSSEC Validation

If DNSSEC validation for a domain for which a certificate is requested fails, the CA must consider the domain to be under attack, necessitating either proof of prior-key-ownership or EV.

3.6. Recent Domain Transfer

If a domain has been transfered during the last 72 hours, the CA should consider the domains ownership-state as insufficiently defined, and reuire either proof of prior-key-ownership or EV.

3.7. High-Risk Domains

If a domain is a high-risk domain, CAs should only offer DNSSEC signed DNS validation, proof of prior-key-ownership DV, or EV. Domains are high risk domains if they are part of the Alexa top 10,000, belong to a CA, a software or hardware vendor, or a payment provider.

4. Additional Validation Options

If one or multiple of the indicators above are detected by a CA, it can employ one of the following additional validation options.

4.1. Proof of Prior Key Ownership

If a CA detects an attack, it can require the requesting party to proof that it has access to the private key for a previously issued certificate. This can be done implicitly, by requirering DV over HTTPS, using a validating certificate, or, explicitly, by using a dedicated ACME-challenge.

4.1.1. Limitations

This option has several operational challenges. An operator's infrastructure may not be design in a way that preserves prior private keys, for example in large container setups. Similarly, the prior key might have been lost due to data-loss, or because the systems holding it have been discontinued. Similarly, prior certificates may have expired.

Furthermore, an attacker may have obtained a prior private key by compromising a system, or by having had legitimate authority over the domain before.

4.2. Additional Use of a DNS Challenge

If the CA detects an attack on one validation, e.g., web based DV, it may use ACME-DNS instead.

4.2.1. Limitations

This challenge does not provide full resillience against all attacks. It however increases the effort an adversary has to put into an attack significantly.

4.3. Additional Use of an Email Challenge

If the CA detects an attack on one validation, e.g., web based DV, it may use ACME-EMAIL instead.

4.3.1. Limitations

This challenge does not provide full resillience against all attacks. It however increases the effort an adversary has to put into an attack significantly.

4.3.2. Limitations

4.4. Out-of-Band and offline validation

If a party is unable to proof prior-key-ownership, and any of the attack indicators outlined before is detected by the CA, the CA should perform a traditional extended validation, requesting appropriate documentation from the requesting party.

4.4.1. Limitations

EV is a manual process which prevents ACME from being used. It is significantly more costly and smaller CAs may be unable to provide the necessary infrastructure to support EV.

5. IANA Considerations

There are no IANA considerations.

6. Security Considerations

This document itself serves as a summary of additional security considerations. Operators of CAs should carefully follow the recommendations made in this document to prevent issuing certificates to unauthorized parties.

7. Acknowledgements

8. References

8.1. Normative References

[BAMBOO] Mittal, P., "Bamboozling Certificate Authorities with BGP", August 2018, <https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee>.

[CSTRIFE] Vigna, G., "Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates", February 2018, <http://dx.doi.org/10.14722/ndss.2018.23327>.

[DVP] Waidner, M., "https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee", n.d..

8.2. URIs

[1] https://bgpmon.net

[2] https://bgpmon.net

Authors' Addresses

Tobias Fiebig
TU Delft

Email: t.fiebig@tudelft.nl

Kevin Borgolte
Princeton University

Email: kevinbo@iseclab.org