UCI University of California, Irvine

Fooling AWS Certificate Manager Domain Validation

Rakshit Mehra
Hari Kishore Chaparala
Surya Teja

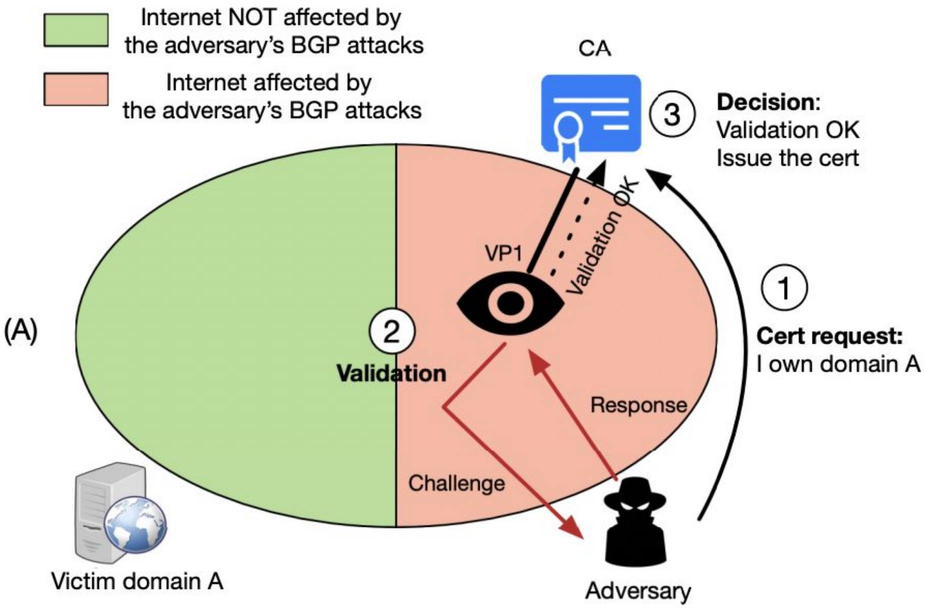
Problem

- Important to ensure security of public key infrastructure (PKI)
- Traditional Certificate Authorities (CAs) used to verify the identity offline
- Modern CAs (such as Let’s Encrypt and AWS Certificate Manager) have automated the process of verifying domain ownership
- Prior work has focused on Let’s Encrypt, GoDaddy, Comodo, Symantec, GlobalSign [1]
- No prior work to explore the security of AWS Certificate Manager that makes our work **novel**
- We verify if AWS certificate manager does DNS domain validation using multiple vantage points
- We attack email domain validation mechanism of AWS certificate manager

Context

- Two ways of doing automated domain validation:
  - DNS validation
  - Email validation
- Both are based on challenge response mechanism
- DNS validation works on the ability to control the nameserver
- Email validation works by challenging the requestor to prove access to the mail server of the domain

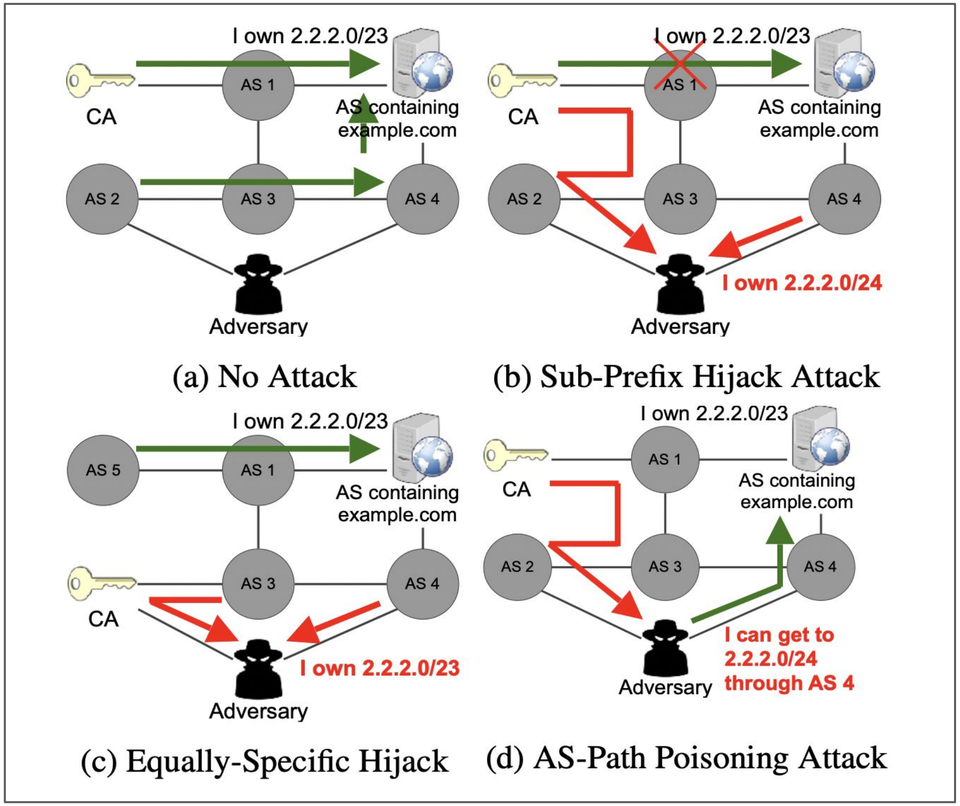
DNS domain validation using single VP


Internet NOT affected by the adversary's BGP attacks
Internet affected by the adversary's BGP attacks
CA
3
Decision: Validation OK Issue the cert
VP1
Validation OK
1
Cert request: I own domain A
(A)
2
Validation
Response
Challenge
Victim domain A
Adversary

Note: Image taken from [2]

Attacks on DNS domain validation

These attacks hold when the CA is using single vantage point as the source sending the challenge.



(a) No Attack

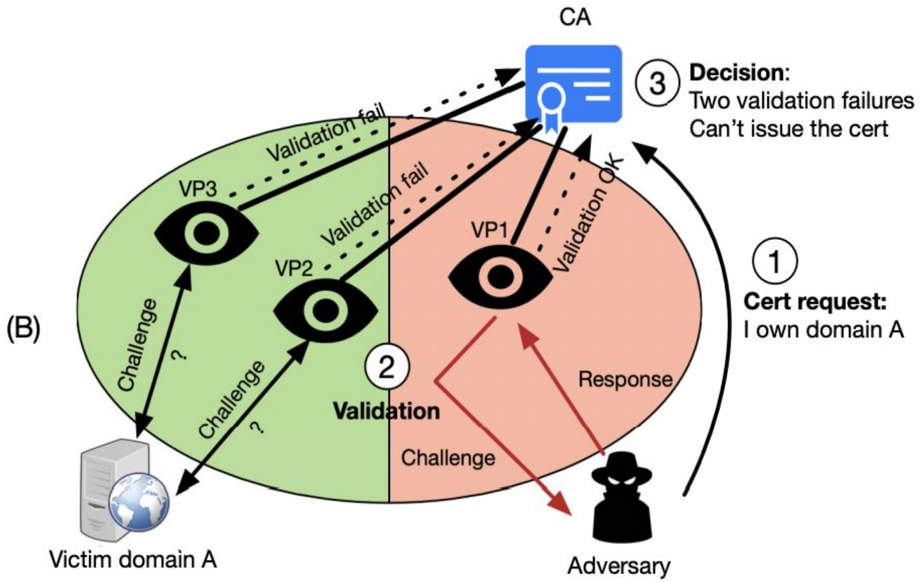
(b) Sub-Prefix Hijack Attack

(c) Equally-Specific Hijack

(d) AS-Path Poisoning Attack

Note: Image taken from [1]

Solution: Using multiple vantage points



Note: Image taken from [2]

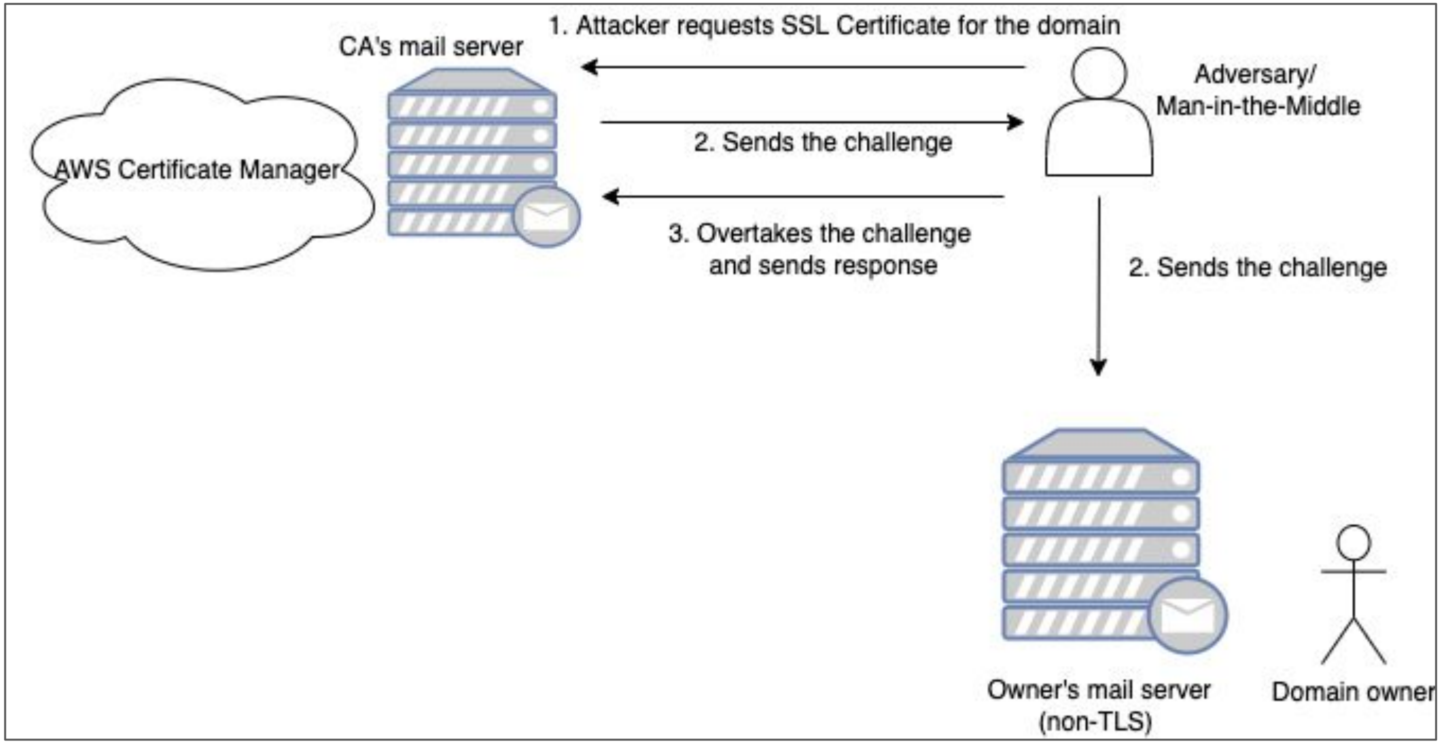
Domain validation using Email

- AWS Certificate Manager sends email to the following ids for approval:
  - administrator@your_domain_name
  - hostmaster@your_domain_name
  - postmaster@your_domain_name
  - webmaster@your_domain_name
  - admin@your_domain_name
- Check if email validation is vulnerable to a MITM attack when TLS is enabled and disabled on the domain owner’s mail server

Approach

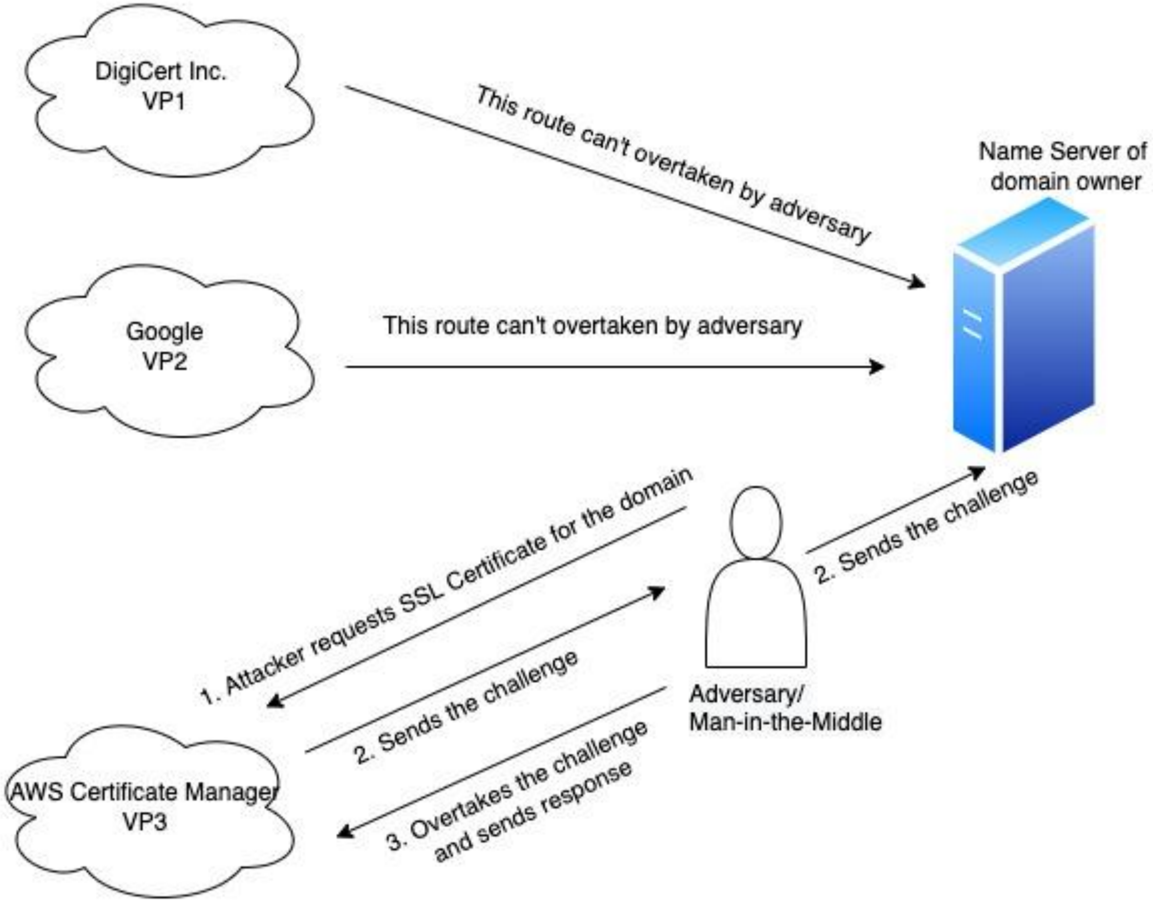
- Following tools are used to test if multi-vantage design is adopted by AWS certificate manager and if domain validation by email is vulnerable:
    - BIND (Berkeley Internet Name Domain) on Google Cloud to run DNS service
    - Postfix in Ubuntu to emulate victim's mail server
    - AWS Certificate Manager
    - Namecheap to buy domain (www.acmetest.me)

Threat Model - Email Validation



Demo

Results - Robustness of DNS domain validation


DigiCert Inc.
VP1
This route can't overtaken by adversary
Name Server of domain owner
Google
VP2
This route can't overtaken by adversary
1. Attacker requests SSL Certificate for the domain
2. Sends the challenge
2. Sends the challenge
Adversary/
Man-in-the-Middle
AWS Certificate Manager
VP3
3. Overtakes the challenge and sends response

Results - Domain validation by Email

- Attacker can easily hijack the challenge in case of domain validation by email if the domain owner’s mail server is not using TLS/SSL
- Even if the domain owner’s mail server is using SSL/TLS, man-in-the-middle adversary can inform the AWS Cert Manager that the domain owner’s mail server does not use SSL/TLS leading to above attack
- Even if AWS Certificate Manager mandates SSL/TLS, adversary can generate own public-private key pair

Conclusion

- Domain validation by DNS is robust and very easy to use.
- Domain validation by email is prone to the attacks indicated previously.
- Due to the above reasons, AWS Certificate manager should only employ DNS validation to allot certificates.

References

[1] https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-birge-lee.pdf

[2] https://www.usenix.org/system/files/sec21fall-birge-lee.pdf

[3] https://dl.acm.org/doi/10.1145/3460120.3484815

[4] https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html

[5]https://www.blackhat.com/docs/us-15/materials/us-15-Gavrichenkov-Breaking-HTTPS-With-BGP-Hijacking-wp.pdf