Fooling AWS Certificate Manager Domain Validation

Rakshit Mehra
University of California, Irvine
rakshim1@uci.edu

Hari Kishore Chaparala
University of California, Irvine
hchapara@uci.edu

Surya Teja
University of California, Irvine
palavals@uci.edu

Abstract

The Public Key Infrastructure (PKI) allows users to safely browse the Internet. Public Certificate Authorities (CAs) are responsible for assuring the genuinity of the domain names of the servers existing on the Internet. They ensure this by issuing digitally signed certificates to the servers by validating the domain ownership. Popular public CAs perform either DNS (Domain Name System) or Email domain validation by sending a challenge to the server over the Internet which is run by Border Gateway Routing (BGP) protocol. The BGP protocol is prone to session hijacking by man-in-the-middle adversaries. In order to prevent the fraudulent issuance of certificates, CAs implement multi-vantage point design with which the adversary needs to hijack most parts of the Internet at the same time to hijack the domain validation challenge. This makes the attack on domain validation challenges impractical. However, multi-vantage design exists only for the DNS domain validation. Implementing domain validation by email can still prove to be harmful for the CAs. We analyze the design of one of the most popular CA - AWS (Amazon Web Services) Certificate Manager which supports both DNS and email domain validation techniques. There has been no prior work related to the security of AWS Certificate Manager. Most of the prior work has focused on CAs such as Let's Encrypt, GoDaddy, Comodo, Symantec, and GlobalSign which makes our work novel. Our finding indicates that AWS Certificate Manager is using multi-vantage point design for DNS domain validation which makes it robust. However, we find that domain validation by email is sending the challenges to the client's mail server in plain text in case the client's mail server does not support SSL/TLS. We believe that this is harmful for domain owners who use TLS unsupported email servers and attackers can use AWS Certificate Manager as a tool to obtain unauthorized certificates.

1 Introduction

SSL and TLS protocols are used to encrypt network communications and the sensitive data carried over the Internet. SSL and TLS certificates are used to establish the identity of a website on the Internet and assure users of their data protection when interacting with the website. These certificates are issued by a Certificate Authority. Traditional CAs issued certificates by verifying the identity offline. This method was not expensive and not scalable which resulted in poor adoption of SSL/TLS for communication. New radical CAs like Lets encrypt provide automatic identity verification along with free certificates [10]. The introduction of these new systems on the internet is a game changer for encrypted communications. The CAs automatically validate identity using a challenge response system. There are numerous types of challenges a domain owner can solve to prove ownership of the domain commonly referred as Domain Validation. On verifying if the challenge is performed successfully by the domain owner, CA gives the certificate to the domain. Domain validation plays a very important role in ensuring the security of PKI. Validation is still a problem today. The CA could be compromised especially with the trusted third party scheme or an imposter gets hold of the certificate. This is why entities like certificate transparency logs [8] and certificate revocations lists [7] exist to minimize the damage.

The CAs rely on a challenge response mechanism to issue certificates to the correct domain owners. There are several flaws highlighted in the domain validation techniques adopted by the CAs. In case of DNS domain validation, CAs employ two types of designs - single vantage and multi-vantage points. Vantage points can be thought of as the source of challenge origination. In case of a single vantage point, it becomes easy for an adversary to perform a man-in-the-middle attack by using various known BGP hijacking techniques [1]. The adversary only needs to hijack one routing path between the vantage point and the client name server to hijack the challenge. To prevent these attacks, Let's Encrypt recently adopted the design consisting of multi-vantage points. In this design, challenge originators (vantage points) are present in various geographical regions. If the attacker intends to perform the same attacks as on single vantage points, the attacker needs to get hold of all the paths between all multiple vantage points

and the nameservers at the same time. As the vantage points are located in different geographical regions across the world, this ideally means that the attacker should hijack a major part of the Internet at the same time which is very impractical.

Majority of the CAs stick to domain validation by DNS. Email validation technique is unique to AWS Certificate Manager. This technique is not used by most CAs as it is more vulnerable as compared to DNS domain validation technique. Due to its low popularity, there has been very little prior work analyzing its robustness.

We perform various experiments to attack the DNS and email domain validation techniques used by AWS Certificate Manager. The organization of the paper is as follows: Section 2 elaborates the related works on attacking against the domain validation techniques employed by the CAs and the defense mechanisms that can be used for these attacks. Section 3 contains the background for our study. From there, we move onto explaining the methodology of our experiments and threat models involved in section 4. We finish by performing evaluation on our findings and highlighting limitations and future work for our study.

2 Related Work

BGP hijacking attacks can be performed by various known techniques highlighted in [1]. These BGP attacks can be used to hijack the challenge originating from the CA. BGP hijacking can be performed using a traditional sub-prefix attack in which an adversary announces a more specific IP prefix as compared to the victim's prefix into BGP. This makes all the traffic directed to the specific victim IP prefix go through the adversary. An adversary can also perform traditional equally-specific-prefix-attack by advertising an equal length prefix as compared to the victim's IP prefix into the BGP. An adversary may employ the prepended sub-prefix attack to claim reachability to a more-specific IP prefix via a non-existent connection to the victim. Another attack that can be performed is an AS path poisoning attack in which the adversary poisons the BGP AS path to come in between the traffic flowing from CA to the nameserver or the client email server and vice versa.

The work presented in [2] shows the multi-vantage point design that is used by Let's Encrypt to defend against the above attacks. The paper presents a design that has negligible latency and communication overhead with a benign failure rate when compared to conventional one vantage point designs. The work presented uses real world operational data from Let's Encrypt to evaluate the security of the design presented.

Recent work [3] how multi-vantage points design of Let's Encrypt can be attacked by performing a downgrade attack. The authors demonstrate how multi-vantage points can be tricked into using the attacker-selected nameserver to send the challenge. The authors present an off-path attack that

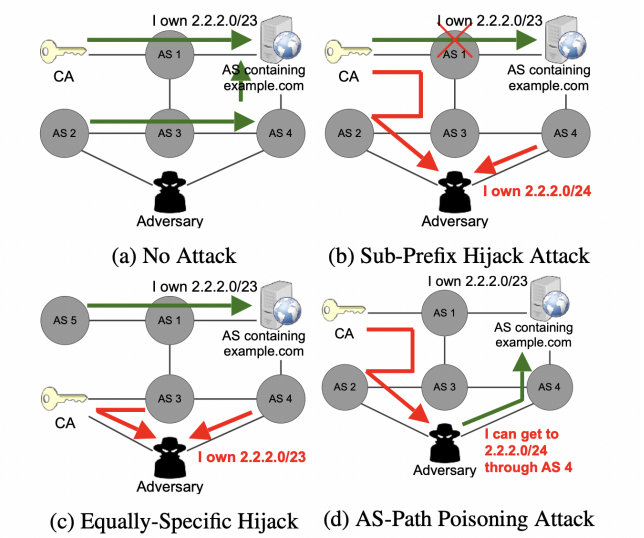

Figure 1: BGP hijacking attacks [1]

is automated, against the single server domain validation to obtain fraudulent certificates for more than 107K domains.

All the works discussed take into account the design of Let's Encrypt, GoDaddy, Comodo, Symantec, and GlobalSign. With the popularity of AWS, many organizations are moving to the cloud. This makes the use of AWS Certificate Manager to increase at a rapid speed. It is surprising to see none of the above work focused on the AWS Certificate Manager service. This motivated us to focus our work on AWS Certificate Manager to validate the robustness of the domain validation techniques used by the service.

3 Background

3.1 Multi-Vantage Point Design

The multi-vantage design ensures that diverse routing paths exist between the vantage points and the legitimate domain. The quorum policy ensures that voting among the vantage points happens securely before issuing the certificate to the domain.

The multi-vantage point design requires more managing and auditing as the challenge originates from multiple data centers located distributed across the globe. The system should be able to handle failures caused by DNS propagation delay and configuration errors. This design mitigates the BGP attacks discussed above.

3.2 AWS Certificate Manager Email Validation

Among the popular CAs at present, email validation is a feature unique to AWS Certificate Manager [5]. To verify the

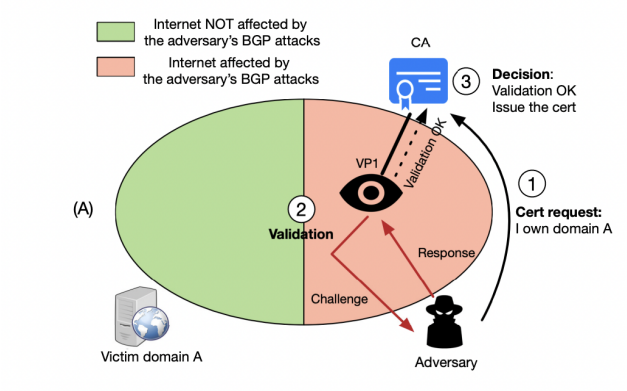

Figure 2: Single Vantage Point Design [1]

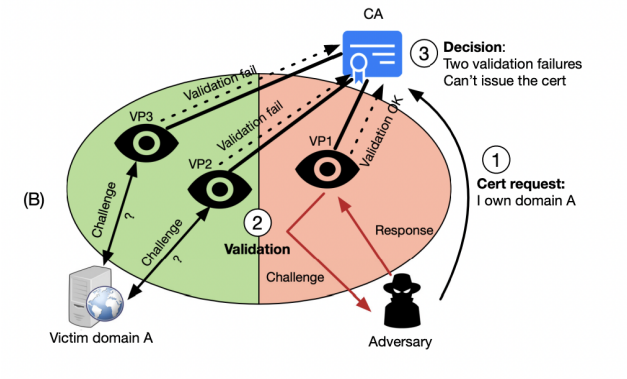

Figure 3: Multi Vantage Point Design [1]

domain, email messages are sent to the three contact addresses listed in the WHOIS database and also to five common system addresses for each domain specified. The registered contact addresses considered are - Domain registrant, Technical contact, and Administrative contact. The five email addresses that receive the messages from ACM are as follows:

- administrator@your-domain-name
- hostmaster@your-domain-name
- postmaster@your-domain-name
- webmaster@your-domain-name
- admin@your-domain-name

These email messages contain the challenge that needs to be approved in order to get a certificate. The certificates issued by ACM expire after 13 months (395 days). In order to get renewed, the email-validated certificates require the domain owner to perform an action. The certificate request can be issued from the AWS GUI (Graphical User Interface) console and the AWS CLI (Command Line Interface).

3.3 DNS Record Types

The challenge that is issued by the CA during DNS domain validation requires adding a CNAME record in the legitimate client nameserver. Hence, it is important to understand various record types present in DNS. The DNS server contains records in the form of a tuple consisting of Name, Value, Type, and TTL. There are four types of records that exist in the DNS server - A, NS, CNAME, and MX. Type A record provides the hostname to IP address mapping. NS record points to the authoritative DNS server that holds the hostname to IP mapping of the queried hostname. For the CNAME record, value points to a canonical hostname for the alias hostname Name while in the MX record, value is a canonical hostname for the alias hostname name.

4 Methodology

4.1 AWS Certificate Manager DNS domain validation

The domain is created using one of the renowned hosting websites - Namecheap as indicated in Figure 4. The domain we create for our experiments is acmetest.me.

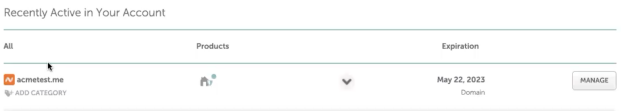

Figure 4: Domain registered on Namecheap [11]

We use Google Compute Engine to install a Linux Server on the top of which Bind service [6] is installed which is an open source implementation of DNS. We used Google Compute Engine instead of Amazon EC2 instance because AWS Certificate Manager already runs on AWS infrastructure. Choosing any cloud other than AWS guarantees that the challenge from vantage points to the domain owner's name server is routed across different BGP AS numbers which makes our experiments more realistic.

Figure 5: Domain Owner's DNS Server [6]

Type A record is created in the zone file on the name server to indicate that requests for www.acmetest.me should go to 34.125.241.84 which is our Google Cloud Compute Engine's

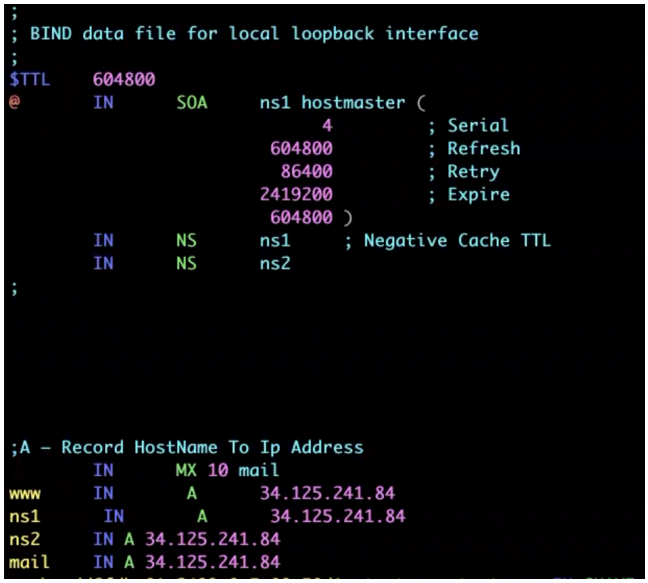

Figure 6: Zone File Created on DNS Server

public IP. MX records are also created as shown in Figure 6 to indicate that the mail server for acmetest.me belongs to 34.125.241.84.

Figure 7: Challenge given by AWS Certificate Manager

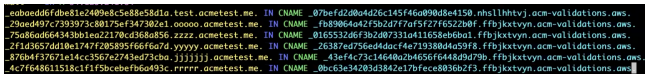

Figure 8: Challenge executed on the DNS Server

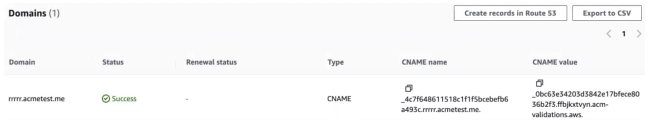

Figure 9: SSL/TLS Certificate Issued

The above figures indicate the challenge that is given by the AWS Certificate Manager needs to be executed in order to get the SSL/TLS certificate. This challenge involves putting the CNAME record issued by the AWS Certificate Manager to the name server. On verifying if the CNAME record has been put onto the required name server, AWS Certificate Manager issues the certificate. Our experiments involve monitoring these incoming requests to the name server to see if these are originated from different AS numbers. If these originate from different ASes, that means that AWS Certificate Manager uses multi-vantage points design. On the other hand, single origin AS indicates that single vantage point design is used that is prone to BGP hijacking attacks discussed in the previous section. The results of these experiments are outlined in the following section.

4.2 AWS Certificate Manager Email domain validation

As discussed above, email domain validation is something unique to AWS Certificate Manager. We perform experiments to see if the man-in-the-middle adversaries can hijack the challenge given by the CA to the email server of the domain owner. As discussed, the challenge is sent to 5 email addresses mentioned above. Because of this reason, the security of the domain owner's email servers is of utmost importance.

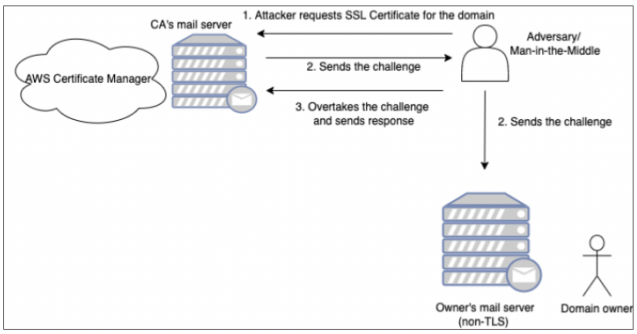

Figure 10: Threat Model

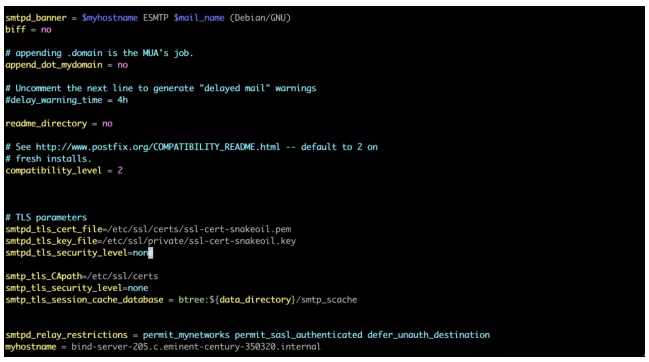

Figure 11: Disable SSL/TLS on email server

Even if adversary is able to hijack the challenge, no sense can be made out of the challenge if the content of the email is encrypted. It is very important for the AWS Certificate Manager to ensure that the domain owner's email server is using SSL/TLS to ensure encrypted transfer of email content over the Internet. This motivates our work to see if the challenge from our CA(AWS Certificate Manager) is transferred

in clear text over the Internet on disabling SSL/TLS on the email server. We use Postfix [12] email server installed on the Google Cloud's Compute Engine that has public IP of 34.125.241.84. The results of the experiments are outlined in the below section.

5 Evaluation

5.1 DNS based domain validation

Figure 12: DNS validation challenge

Figure 13: Successful DNS validation

In DNS based validation, we have CNAME records generated by AWS as shown in Figure 12 which have to be added to our DNS server for challenge completion. We completed the challenge and obtained the certificate: Figure 13 indicates the monitored network traffic through our Bind server logs. We have used the IP to ASN mapping service provided by Team Cymru [9] to check if AWS uses multi vantage points.

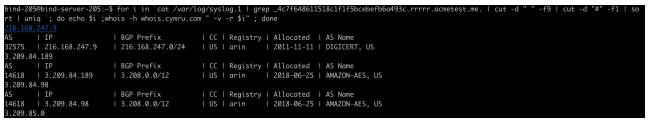

Figure 14: DNS traffic during certificate validation

Figure 14 shows that apart from AWS servers, we also get traffic from DIGICERT.

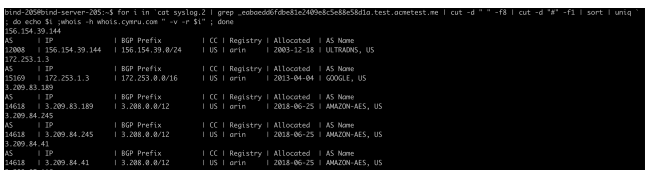

Figure 15: DNS traffic during certificate validation with DIGICERT blocked

We tried blocking the DIGICERT IP address and observed that the validation now uses different vantage points (Google and ULTRADNS) as shown in Figure 15. In order to test if the validation works we only allowed the traffic from AWS servers, we added the firewall rules manually whitelisting only the AWS servers' traffic. We couldn't obtain the certificate in this manner, thus proving that AWS uses multiple vantage point based domain validation.

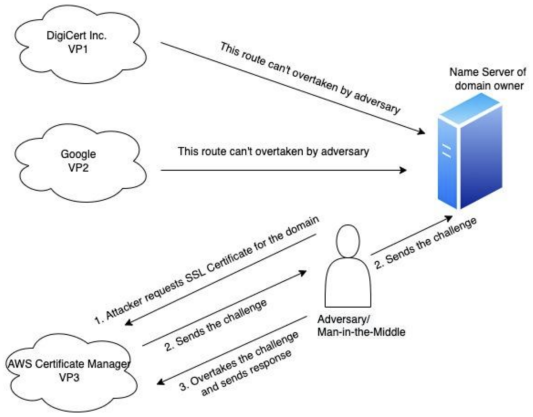

Figure 16: Observed flow of DNS based validation with AWS certificate manager

Figure 16 shows the observed DNS based validation method in AWS as per our evaluation.

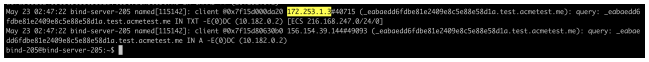

Figure 17: DNS query types during certificate validation

We also observed that other vantage points only query on DNS record types A and TXT consistently unlike the CNAME based verification done by AWS servers as shown in Figure 17. We haven't performed a thorough analysis on the robustness of this type of domain validation in our current work and there are some limitations of our multi-vantage point validation which are discussed in section 7.

5.2 Email based domain validation

We used Postfix [12] for setting up our custom email server. After disabling the TLS in our postfix setup as shown in Figure 11, we sniffed the traffic and results in Figure 18 clearly show the plain text domain validation links from AWS.

We use the link in the un-encrypted email to approve the validation request as shown in Figure 19 and obtain the certificate: Figure 20

This shows that an attacker can use the AWS certificate manager as an attack tool to obtain unauthorised certificates for any domain that is backed by non-TLS email server.

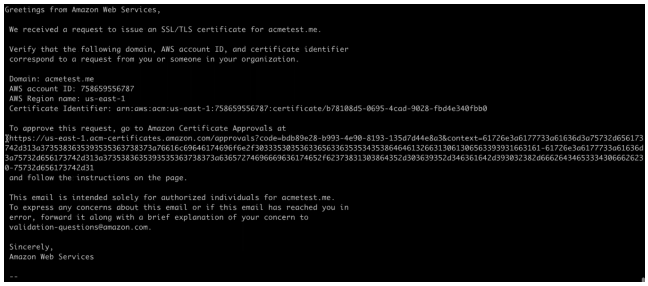

Figure 18: Sniffing un-encrypted Domain validation mail from AWS

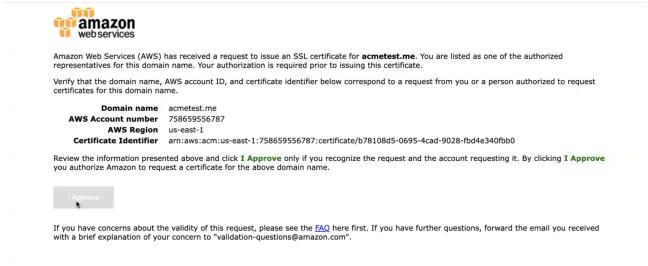

Figure 19: Approving the validation request

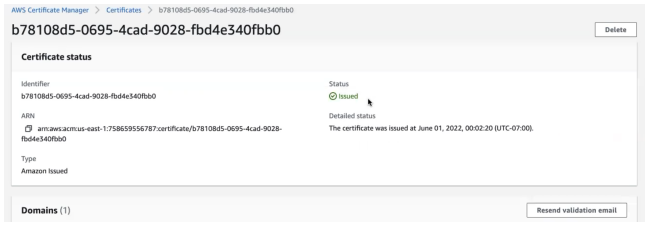

Figure 20: Successful email based validation by the attacker

We have also changed the Postfix email configuration to opportunistic TLS such that Postfix doesn't mandate TLS encryption. We observed that AWS prefers TLS in this setting and the validation email is encrypted.

6 Conclusion

We emphasize the importance of maintaining security of Public Key Infrastructure (PKI). Verifying domain ownership is very critical for the issuance of a TLS/SSL certificate to the legitimate domain owner. There are a vast number of known BGP attacks that can be performed to hijack the challenge issued to the domain owners by the CAs. Popular public CAs like Let's Encrypt perform automated validation of domain ownership by employing multi-vantage points design. Let's Encrypt supports only DNS validation at present. We perform various experiments on DNS and email domain validation techniques employed by AWS Certificate Manager. Our experiments show that AWS Certificate Manager uses multi-vantage points design for DNS domain validation. AWS Certificate Manager uses third-party services to help with multi-vantage design during DNS domain validation. It uses services of Google, Ultra DNS, and other entities that own a public Autonomous System (AS) in BGP. Our experiments on email validation show that the attacker can easily hijack the challenge if the domain owner's email server is not using TLS/SSL. The attacker can act as man-in-the-middle adversary to capture the challenge sent in plain-text if the domain owner's email server does not support TLS/SSL. Our findings indicate that AWS Certificate Manager should only use DNS domain validation to allot certificates.

7 Limitations and Future Work

We perform all our experiments assuming that the adversary is present outside the organization. Currently, our DNS server is installed as a compute engine instance on Google Cloud. We rely on the services provided by Team CYMRU [9] for determining live IP to ASN mappings to get the origin AS from where the DNS challenge is sent. Although this service [9] updates its database every four hours, we plan to install a virtual router in our local environment to track the live incoming BGP traffic and know the AS path from the BGP routing table. For this, we will be using a DNS server installed in our local environment next to our virtual router so that the live incoming traffic can be captured on the router. This will remove our dependency on the third party service [9] and will give more realism to our findings indicating the robustness of DNS domain validation technique.

Our Multi-Vantage evaluation uses firewall rules to selectively allow traffic from only the AWS servers by manually adding whitelisted IP addresses. We observed that AWS uses several endpoints to call our DNS server and adding them manually each time is not feasible. A better approach would be to use automated packet filtering to allow only the traffic from AWS servers. This would be a definite way of proving that AWS certificate manager indeed uses multiple vantage points. During our testing, we also noticed that the queries from other vantage points are on A and TXT DNS record types whereas AWS certificate challenge is based on CNAME records. The current AWS documentation [4] only talks about CNAME based verification and we couldn't find more information about the roles of other vantage points in domain validation. We plan to study this aspect further and test the robustness of current ACM implementation.

We talk about the BGP hijacking attacks that can be performed by man-in-the-middle adversaries to intercept the plain-text challenge sent to the email server in case the domain owner's email server is not using TLS/SSL. As a part of future work, we plan to demonstrate these BGP hijacking attacks by setting up an email server in our local environment as compared to the cloud environment. We also believe that even if the domain owner's email server is using TLS/SSL, man-

in-the-middle adversaries can inform the AWS Cert Manager that the domain owner's email server does not use SSL/TLS leading to the above attack discussed. On successfully demonstrating these end to end attacks, we plan to report this flaw to AWS and ask them to revoke the email validation technique employed by AWS Certificate Manager.

References

[1] Henry Birge-Lee et al. "Bamboozling Certificate Authorities with BGP". In: *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 833–849. ISBN: 978-1-939133-04-5. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee.

[2] Henry Birge-Lee et al. "Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt". In: *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021, pp. 4311–4327. ISBN: 978-1-939133-24-3. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/birge-lee.

[3] Tianxiang Dai, Haya Shulman, and Michael Waidner. "Let's Downgrade Let's Encrypt". In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. CCS '21. Virtual Event, Republic of Korea: Association for Computing Machinery, 2021, pp. 1421–1440. ISBN: 9781450384544. DOI: 10.1145/3460120.3484815. URL: https://doi.org/10.1145/3460120.3484815.

[4] *AWS DNS Domain Validation*. https://docs.aws.amazon.com/acm/latest/userguide/dns-validation.html. Accessed: 2022-06-10.

[5] *AWS Email Domain Validation*. https://docs.aws.amazon.com/acm/latest/userguide/email-validation.html. Accessed: 2022-06-10.

[6] *Bind9 DNS System*. https://www.isc.org/bind/. Accessed: 2022-06-10.

[7] *Certificate Revocation List*. https://www.thesslstore.com/blog/crl-explained-what-is-a-certificate-revocation-list/. Accessed: 2022-06-10.

[8] *Certificate Transparency Logs*. https://certificate.transparency.dev/howctworks/. Accessed: 2022-06-10.

[9] *IP TO ASN Mapping*. https://team-cymru.com/community-services/ip-asn-mapping/. Accessed: 2022-06-10.

[10] *Let's Encrypt Design*. https://letsencrypt.org/. Accessed: 2022-06-10.

[11] *Namecheap*. https://www.namecheap.com/. Accessed: 2022-06-10.

[12] *The Postfix Home Page*. https://www.postfix.org/. Accessed: 2022-06-10.