Leveraging DNS for timely SSL Certificate Revocation

Eirini Degkleri[1,2], Antonios A. Chariton[1], Panagiotis Ilia[1,2]
Panagiotis Papadopoulos[1,2], Evangelos P. Markatos[1,2]

[1] FORTH-ICS, Greece
[2] University of Crete, Greece

ABSTRACT

Trust in SSL-based communication on the Internet is provided by Certificate Authorities in the form of signed certificates. When an organization uses an SSL certificate, it protects users' sensitive information by encrypting all traffic between its servers and the users' web browser. Sadly, current web browsers' approaches to check the revocation status of a certificate, suffer from certain performance issues and privacy implications. To address these issues, we propose DCSP: a new low-latency approach that by leveraging the existing infrastructure of DNS, provides performant and accurate certificate revocation information. Our initial performance results show that DCSP has the potential to perform an order of magnitude faster than the current state-of-the-art alternatives.

1. INTRODUCTION

More and more websites are moving from the plain HTTP protocol to the more secure HTTPS (i.e. HTTP over SSL). HTTPS protects the transmitted data by encrypting all the messages exchanged between the communicating parties. The security provided by SSL is based on the authentication of the participants. That is, no security can be guaranteed by the protocol without first ensuring that the communicating parties are indeed who they claim to be. To implement such authentication mechanism, SSL, uses digital certificates: a form of identity, which contains the public key of the unique key pair owned by the certificate's subject. Responsible for issuing and publishing these certificates is a trusted 3rd party entity, namely Certificate Authority (CA). This entity, by signing each certificate it issues, vouches that the subject of the certificate is indeed the owner of the key pair.

In most cases, certificates are valid for a specific period of time, however, there are cases where they need to be revoked earlier: for example, when the private key of a web server is stolen and hence, users need to immediately stop establishing secure connections with this web server. In 2014, there were such a case, where a security bug called Heartbleed [2], left around half a million of the Internet's secure web servers vulnerable to theft of the servers' private keys. The issuer CA is also responsible to revoke the certificates that are considered as unsafe. In this way, each CA by revoking a specific certificate, warns the users to not trust SSL connections using this certificate any more. Web browsers use two main approaches to check the revocation status of a certificate: *i)* the Certificate Revocation Lists (CRL), and *ii)* the Online Certificate Status Protocol (OCSP).

Unfortunately, there are some significant performance issues with these state-of-the-art mechanisms. Specifically, in the case of CRLs, the browsers need to periodically download several Megabytes of data [5] for being able to check the status of each received certificate, while in the case of OCSP, they have to wait until receiving a response from the OCSP server (hundreds of milliseconds per query [6]). This poor performance has led some of the contemporary web browsers to sacrifice security for performance. The result of such a choice is the incomplete validity check of the accepted certificates [3], which leaves the users unprotected against possible man-in-the-middle (MITM) and impersonation attacks. In addition, recent studies indicate that mobile browsers uniformly *never* check the certificate revocation status, because it is considered costly [4]. As a consequence, in this work we seek a validation mechanism able to reduce this high latency, encouraging thus the browsers to perform full certificate validation for each SSL negotiation.

To summarize, we aim to put an end to the false dilemma of "*performance vs security*" by proposing a new certificate revocation approach, which demonstrates that it is possible to obtain both good performance and high levels of security at the same time. Our approach, namely DCSP [1], leverages the existing and publicly accessible infrastructure of DNS, and by capitalizing on its scalability and proven robustness, distributes timely certificate revocation information to the end-users.

2. DESIGN

DCSP uses the DNS system to store certificate revocation information. When a web browser is required to check whether a certificate has been revoked, it queries the DNS to find revocation information regarding that certificate. To ensure the authenticity of that information, each CA signs the revocation status of every certificate it has issued. To remedy the threat of possible replay attacks, DCSP employs epochs, where the information of each certificate is timestamped before signed. To mitigate the additional overhead this may impose, and to reduce the number of signatures that needs to be performed in each epoch, we introduce the notion of *collective records.* These collective records contain a set of domains along with the latest version number of each domain's revocation list. So when a certificate of a domain D is revoked, the CA adds in the DNS an individual record about D, which contains a list of all the revoked certificates of D along with the latest version number of this revocation list. At each epoch, and for each collective record, the CA updates the collective record with the most recent information, timestamps it and signs it.

2.1 Epochs

As mentioned, DCSP divides time into epochs and timestamps the validity information of each certificate in order to mitigate replay attacks. This way if an attacker attempts to replay a stale certificate [1], it will not be accepted. However, if the validity of information changes within the epoch, the system is vulnerable. To address this problem, we propose a fine tuning of the duration of an epoch, to make the window of vulnerability within an epoch significantly small.

2.2 Certificate Format

In order for our system to work, we add a custom certificate extension to an existing certificate that is marked as non-critical, the "DNS Revocation Domain". The information can also be present in the "Certificate Authority Information Access" as a new method, under the name "DCSP". The URI of this entry is set to a valid DNS domain which will be queried for answers using the DNS protocol. We will refer to this value as *Revocation Domain*.

2.3 DNS Record Format

The Certificate Authority is responsible for adding the DNS records to the authoritative name servers for the Revocation Domain. Accordingly, the CA divides the total amount of domain names into small groups. This can be done arbitrarily by the CA and groups can be of any size. Additionally, the CA must perform at least as many cryptographic signs per day as the total number of groups available. Each group must be given a unique name that can be used as a subdomain, for example "group-00001". The size of the group is dynamic and can easily change at any time, without impacting old certificates. To find the optimal size of groups we have performed some measurements whose results are seen in Figure 1. Based on our simulations, we propose that the Group Size should be around 100 records, to keep the packet size small and fully take advantage of the faster UDP protocol, decreasing total transmission time.

2.3.1 Collective Records

After the grouping has been performed, the CA generates a new domain in the form of "group-name.revocation.ca-name.com". This domain name is then included in the certificate as the Revocation Domain. Currently there is no technical limitation in our system, even if arbitrary domains are used for each group, however we recommend a more elegant and scalable approach.

The CA then proceeds to add a TXT record for each domain[2] in this group, following the format below:

$$\underline{DOMAIN} - \underline{VERSION} - (\underline{POSITION}/\underline{TOTAL})$$

In the $\underline{DOMAIN}$ variable, the top level domain of the site is included. The content of the $\underline{VERSION}$ variable is the latest revision of this domain's records. For the $\underline{POSITION}$ and $\underline{TOTAL}$ variables we include the domain name's serial number within the particular group and the group size respectively.

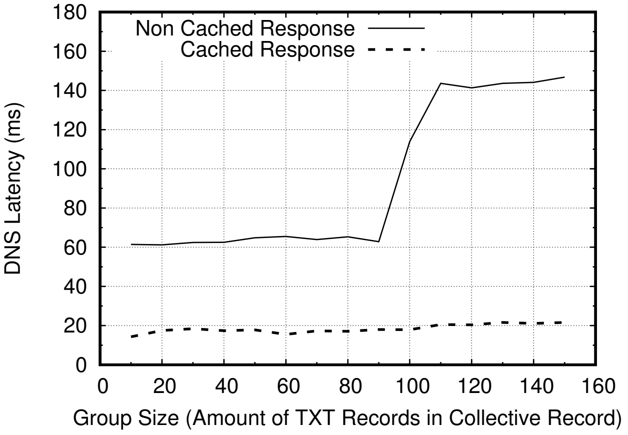

Figure 1: Average query time for various group sizes. The rapid increase after 90 records is due to the switch from UDP to TCP. When the record is cached, it is around 20 ms.

2.3.2 Individual Records

The CA needs to keep individual TXT records for each domain, in a domain that has the following format:

$$\underline{domain.name}.\underline{groupname}.revocation.ca.com$$

If there is no certificate revocation regarding this domain name, then the word $\underline{NONE}$ followed by the revision number $\underline{REV}$, which is an always increasing positive number, and the string "(1/1)", is included. If there are revoked, non expired certificates, the records format is the following:

$$\underline{CERTID} - \underline{REV} - (\underline{POSITION}/\underline{TOTAL})$$

The $\underline{\text{CERTID}}$ variable contains the SHA-1 fingerprint of the revoked certificate.

3. CONCLUSION

To conclude, DCSP leverages DNS to quickly distribute fresh revocation information. By using UDP-based communication it offers faster revocation than the state-of-the-art approaches, achieving hence both security and performance. Also by introducing collective records, it significantly reduces the amount of signatures required by the CAs. Initial performance results show that DCSP has the potential to perform an order of magnitude faster than OCSP. Finally, in lieu of the existing server-client, query-based model, where the server is able to reconstruct the entire browsing history of the users, DCSP ensures that the browsing history will not be revealed to any third entity except from the already aware DNS (it already resolves IP-to-domains), providing, hence, privacy guarantees to the end-users.

4. ACKNOWLEDGMENTS

This work was supported in part by the project GCC, funded by the Prevention of and Fight against Crime Programme of the European Commission – Directorate-General Home Affairs under Grant Agreement HOME/2011/ISEC/AG/INT/40000 02166, by the FP7 Marie-Curie iSocial ITN, funded by the EC under Grant Agree-

[1] Stale in this case means that the certificate was timestamped a previous epoch

[2] In case of a certificate with an IP Address, its "in-addr.arpa" format can be used.

ment No 31680, and by the European Commission through the project SHARCS under Grant Agreement No. 644571.

5. REFERENCES

[1] A. A. Chariton, E. Degkleri, P. Papadopoulos, P. Ilia, and E. P. Markatos. Dcsp: Performant certificate revocation a dns-based approach. In *Proceedings of the 9th EuroSec '16*.

[2] Codenomicon. The heartbleed bug. http://heartbleed.com.

[3] A. Langley. Revocation still doesn't work. https://www.imperialviolet.org/2014/04/29/revocationagain.html.

[4] Y. Liu, W. Tome, L. Zhang, D. Choffnes, D. Levin, B. Maggs, A. Mislove, A. Schulman, and C. Wilson. An end-to-end measurement of certificate revocation in the web's pki. In *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*, IMC '15.

[5] Netcraft. CRL sites ordered by average body size. http://uptime.netcraft.com/perf/reports/performance/CRL.

[6] Netcraft. Total http time of ocsp sites. http://uptime.netcraft.com/perf/reports/performance/OCSP.