Certificate Revocation Guard (CRG)

Certificate Revocation Guard ensures your connections are protected through certificate validation without changes in legacy infrastructure.

The challenge
In the Public Key infrastructure (PKI) model, digital certificates play a vital role in securing online communication. Communicating parties exchange and validate these certificates to ensure each party is the legitimate intended party. Without validation of these certificates there is no way to know both whether you are communicating with a legitimate party, and if your data is being taken by a third party.

While this model works in principle, many programs, web browsers in particular, do not use the recommended methods for checking certificate revocation as part of the validation process. The main reason behind this could be program efficiency, bandwidth overhead, network latency, storage overhead or even privacy risks. This is incredibly problematic, as bypassing the certificate revocation check can result in session hijacking, unauthorised issuance of new certificates and data syphoning.

While there is incentive to make programs directly check certificates, existing program companies are unwilling. Be this due to decreased program efficiency or incurred overheads, program companies would rather strive for immediate customer satisfaction.

The solution
Certificate Revocation Guard is a plug and play solution offering a separation between the client program and the revocation checking mechanism. Using our technology, secure connections are guaranteed without degrading program performance and affecting usability.

Our novel method will save bandwidth cost, network latency and storage cost. Based on OCSP, caching the certificate revocation status locally, Certificate Revocation Guard takes advantages of both OCSP and CRL methods. Furthermore, Certificate Revocation guard can be installed at any level, including user machine, organisational gateway and ISP levels.

Technology advantages
- Can be installed anywhere - User machine, organisational gateway/proxy or ISP level
- Outperforms existing revocation methods

Key benefits
- Does not require any changes in the legacy infrastructure.
- Does not require any existing user or program changes.
- Visualize rules to illustrate relationships between data

IP Position
Provisional Patent has been filed.

Contact
Stephen Flint
Commercialisation Manager
+64 9 933 4989 or +64 21 240 3076
s.flint@auckland.ac.nz