Proposed LURK Charter

Introduction

Classic HTTPS authenticates the server by verifying ownership of a private key associated with a public-key certificate. Most trust models assume an HTTP server owns the private keys and the server is responsible for both the hosted content and network delivery. Although these assumptions were largely true in the past, today the deployment of services on the Internet largely relies on multiple, distributed instances of the service, not necessarily operated by the content owner. In such architectures, the application - like a web browser - expects to authenticate a content provider but is actually authenticating the node delivering the content. In this case, confusion results from using a secure transport layer to authenticate application layer content.

Body of Proposed Charter

The WG will focus on a solution that allows offloading TLS termination to a content delivery network (CDN) without giving the content owner's private key to the CDN. In scope are TLS and DTLS, including TLS 1.0-1.2 and, when available, TLS 1.3. This working group will not propose any changes to the client side of the TLS protocol, and the solution should support all widely deployed TLS cipher suites.

The current work items include:

- An Informative "use cases" document, which will cover the CDN use case but may encompass additional use cases.
- A Standards Track document that defines the interface between an edge server and a content owner. Security is a key concern, specifically avoiding a "signing oracle" where possible. Provisioning/management/monitoring of the protocol's endpoint is out of scope of the working group.

Delegation of RSA/ECDSA keys for other purposes is out of the scope of the working group. Such work would require the working group to recharter.