Disposition of some potential TLS WG drafts

...

the chairs

Process

1. We (the chairs) display the draft's abstract.
2. We ask the following questions and you (the WG members) hum:
    a. Have you read the draft?
    b. If you understand what it's about would you support adopting it as a WG item?
    c. If adopted would you participate in the draft's development?
3. We provide a sense of the room.
4. We take these question to the list.
5. We judge consensus later.

Exported Authenticators in TLS

This document describes a mechanism in Transport Layer Security (TLS) to provide an exportable proof of ownership of a certificate that can be transmitted out of band and verified by the other party.

Delegated Credentials

The organizational separation between the operator of a TLS server and the certificate authority that provides it credentials can cause problems, for example when it comes to reducing the lifetime of certificates or supporting new cryptographic algorithms. This document describes a mechanism to allow TLS server operators to create their own credential delegations without breaking compatibility with clients that do not support this specification.

TLS 1.2 Update for Long-Term Support

This document specifies an update of TLS 1.2 for long-term support on systems that can have multi-year or even decade-long update cycles, one that incorporates as far as possible what's already deployed for TLS 1.2 but with the security holes and bugs fixed. This document also recognises the fact that there is a huge amount of TLS use outside the web content-delivery environment with its resource-rich hardware and software that can be updated whenever required and provides a long-term stable, known-good version that can be deployed to systems that can't roll out ongoing changes on a continuous basis.

TLS Server Identity Pinning with Tickets

Misissued public-key certificates can prevent TLS clients from appropriately authenticating the TLS server. Several alternatives have been proposed to detect this situation and prevent a client from establishing a TLS session with a TLS endpoint authenticated with an illegitimate public-key certificate, but none is currently in wide use.

This document proposes to extend TLS with opaque pinning tickets as a way to pin the server's identity. During an initial TLS session, the server provides an original encrypted pinning ticket. In subsequent TLS session establishment, upon receipt of the pinning ticket, the server proves its ability to decrypt the pinning ticket and thus the ownership if the pinning protection key. The client can now safely conclude that the TLS session is established with the same TLS server as the original TLS session. One of the important properties of this proposal is that no manual management actions are required.