Delayed/Long Running Process vs Credential Exposure

Shawn Emery <shawn.emery@sun.com>

Problem Statement

There is no provision in a Kerberos environment where users make use of delayed execution or long running set of processes such that they need credentials to access applications like secure NFS with Kerberos authentication.

There are number of hacks in the wild that pose various degrees of security risk:

a. extend the lifetime of TGT to infinity
b. create a keytab with the user's long term key stored
c. create a secure channel with the KDC and access the user's keys directly

Proposed Solution (1/1)

The general concept is that you can create multi-component principals per service and host as outlined below. With this you can easily create/imply authorization rules based on principal nomenclature.

Create implicit authorization for multi-component principals (mcp) that make use of naming based on the user principal's single component name.

For example:

<user>/<service>/<fqhn>@<realm>

Proposed Solution (1/1) - cont.

Advantages:

If the machine is compromised then the attacker only has the mcps long term keys and once compromise is detected the administrator can disable the particular mcp account.

Authorization is granted for authentication for mcps, but do not have administrative rights for the associated user principal.

The administration component can be extended to support systems that already have host service principals to create other service principals for that particular host.

When the user changes their keys they are not required to login to every machine that holds the user's keytab file to update keys.

Provides unique principal name for auditing.

Proposed Solution (1/1) - cont.

Disadvantages:

The implied authorization gives the mcp all rights as that user. So if the machine that holds the mcp's keys is compromised and if this is not known then they will have implied rights as that user until the administrator becomes aware.

Implementations may have an alias SPN design that wouldn't provide separation.

Proposed Solution (2/2)

Post dated tickets

Advantage: Already in standard

Disadvantage: Discrete time line vs. nebulous execution time

Comments?