Self Imposed Limitations of Kerberos

Douglas E. Engert

DEEngert@anl.gov

Argonne National Laboratory

08/04/04

Outsiders views

- Kerberos has been too successful
- Thousands of users in a realm
- Hundreds of hosts in realm
- What is the extended trust model
- Once ticket is obtained or forwarded, if stolen it can compromise all the systems a user can access
- Kerberos won't work well across institutions

Trust

- Trust in user's workstation is low
- Trust = 1/(Number of host)
  - * 1/(Number of sites)
  - * 1/(Diversity of security)
  - * 1/(Number of users)

Why Kerberos is Limited

- Single sign-on – Total reliance on user's workstation
- Delegated (forwarded) tickets as good as original
  - No control by user of the use of delegated tickets
  - No trace of hosts involved in delegation
  - No good bindings to host on which it can be used
    - » Channel bindings to IP in all but useless
- No black-listing of tickets by KDC, especially with cross realm

What to do about trust of users workstation?

- Better maintenance
- Restricted operating systems
- Boot from CD
- Dumb terminals
- Hardware token/smartcard/PDA/… does Kerberos for workstation

What can be done about Delegated tickets

- User sets restrictions when doing kinit/login
  - Limit use of delegated tickets by sites/hosts/services
  - Further delegation may impose further restrictions
  - KDC or end service needs to check restrictions before issuing or using tickets
- Trace of hosts/sites involved in delegation included in ticket
  - Used to detect/prevent unusual activity
- Real time feedback to user about use of tickets, for logging, or even permission to use.

Black Listing Tickets

- Once a TGT is issued, it can continue to be used.
  - Principals can be disabled so no new tickets issued.
  - KDC could refuse to issue additional tickets.
- What about issued cross-realm TGTs
  - Can one KDC/admin notify other KDCs to black list cross-realm TGTs?
  - Keep a log of active cross-realm TGTs so other KDCs can be contacted ASAP?

Conclusion

- The WG has been deeply involved with protocol issues, but has neglected the problems of being so successful.
- I believe that these issues can all be addressed which will improve the trust in the use of the protocol, and lead to its wider deployment.

The End