Security Services for Samba4

Andrew Bartlett

Samba Team

Who Am I

- Samba Developer
- Authentication Systems
  - I care about who you are
- Interesting Infrastructure Challenges
  - Somebody told me this stuff is meant to be hard!
- Real World Experience
  - Samba at Hawker College

Samba4

- Samba, reborn
  - Matching the market leader
  - Proof by comparative testing
  - The rewrite we always needed
- People want 'Active Directory'
  - Compatibility and testing demands these interfaces
- Security Services Challenge

New infrastructure

- The 'big leap forward'
- An infrastructure basis for a real chance to match the dominate market player.
- New modular basis
  - NTVFS (Server side interface CIFS -> File-systems)
  - CIFS Client lib
  - GENSEC
  - and much more

Active Directory

- 'Extended tree structured LDAP integrated into every aspect of your software'
- 'Ministry of Truth for authentication'
  - Single Sign on
  - Single source of password
- Desktop Management
  - This is the primary reasons sites upgrade to AD

Challenges In Active Directory

- Protocol friends, new and old:
  - CIFS
  - DCE/RPC
  - LDAP
  - CLDAP
  - Kerberos
  - HTTP
    - Yes, we have DCE/RPC over HTTP
  - DCOM
    - Interest in WMI

Goal: WinXP Domain Join

- Samba3 does NT4 only
  - But WinXP joins fine
- Goal to have WinXP join Samba4
- We want this to be an AD join
  - Client should think it is joining AD
- Lots of 'security' protocols along the way

Authentication Definitions

- Authentication
  - Proof of who you are
- Authorization
  - Determine what you are allowed to access
- Security
  - Meaningless term attached to anything and everything in this area
- Single Sign on
  - Enter your password once, and once only

Security Services

- Single Source of 'Security' for your system
  - Use, don't care...
- Security Protocols
  - NTLMSSP
  - Kerberos
  - SPNEGO
  - SASL
  - DIGEST-MD5
- These must all use the **same** password

NTLMSSP

- Backbone of windows authentication
- Hails from the earliest days of SMB
- Challenge-response
- Negotiated options
  - 3-leg authentication exchange
- Problems with the authentication exchange
  - 56-bit by default
  - 128 bit by option (that nobody sets)

Microsoft Kerberos

- Kerberos
  - Internet Standard
  - Strong cryptography
  - Trusted third party authentication system
- Microsoft's changes:
  - Added Authorization data
  - New 'encryption type'

SPNEGO

- Security Negotiation Protocol
- Fits into the GSSAPI modal
- Selects:
  - Kerberos
  - NTLMSSP
  - Something else in future
- New work to add the 'P' for protected back in

SCHANNEL

- Microsoft's own security standard
- Between 'domain members' and 'domain controllers'
- Never intentionally documented
  - There are some similarities with new Kerberos standards
- Tied closely with DCE/RPC and Domain Controllers

History and Precedent

- Basic support for these 'security' protocols
  - Scattered in various parts of the code
  - Connected to the protocol they support (CIFS, LDAP)
  - 3 **Different** implementations of NTLMSSP
- Microsoft has SSPI
  - This shows up in the use of the same security protocols everywhere.

NTLMSSP In Samba

- Historical 'temporary' implementation from Samba 2.0.
  - rpc_client/cli_pipe_hnd.c
  - rpc_server/srv_pipe_hnd.c
- Tridge's NTLMSSP for SPNEGO
  - Simple parse functions
- Rewritten as a state machine
  - Client and server combined
  - Generic interface

GENSEC

GENSEC

- 'One Ring' to rule them all
  - Samba needed a single place to deal with these details
  - A single function interface, regardless of subsequent security protocol
- Reinvent this particular wheel for Samba
- Ideally have only one backend per security protocol

GENSEC Further Services

- Beyond Authentication
- CIFS Session Key
  - Not something we can get from another generic layer
- Authorization Data
  - Breaks the GSSAPI layer, but hooks are being put in place
- Data Integrity (Sign)
- Data Encryption (Seal)

Choosing the right interface

- Multiple names per security protocol:
  - OID (GSSAPI likes OIDs)
  - SASL Name (SASL uses simple text strings)
  - DCE/RPC auth type
    - Well known numbers
- gensec_start_by_oid(context, oid)
- gensec_start_by_sasl_name(context, name)
- gensec_start_by_auth_type(context, type, level)

GENSEC Plugin Interface

```
static const struct gensec_security_ops gensec_ntlmssp_security_ops
= {
        .name           = "ntlmssp",
        .sasl_name      = "NTLM",
        .auth_type      = DCERPC_AUTH_TYPE_NTLMSSP,
        .oid            = GENSEC_OID_NTLMSSP,
        .enabled        = True,
        .client_start   = gensec_ntlmssp_client_start,
        .server_start   = gensec_ntlmssp_server_start,
        .update         = gensec_ntlmssp_update,
        .sig_size       = gensec_ntlmssp_sig_size,
        .sign_packet    = gensec_ntlmssp_sign_packet,
        .check_packet   = gensec_ntlmssp_check_packet,
        .seal_packet    = gensec_ntlmssp_seal_packet,
        .unseal_packet  = gensec_ntlmssp_unseal_packet,
        .wrap           = gensec_ntlmssp_wrap,
        .unwrap         = gensec_ntlmssp_unwrap,
        .session_key    = gensec_ntlmssp_session_key,
        .session_info   = gensec_ntlmssp_session_info,
        .have_feature   = gensec_ntlmssp_have_feature
};
```

GENSEC Success

- GENSEC implemented SPNEGO
  - Used for HTTP, and CIFS
- Tridge added the code to wrap SPNEGO on DCE/RPC
  - Took about a morning
- Worked first time
  - GENSEC picked the 'auth type', and just called the backend

GENSEC Futures

- Biggest future change is for asynchronous support
- GENSEC is already a state machine
  - But this will require more state
- Better support for GSSAPI
  - Avoid needing our own 'GSSAPI' code would be nice

GENSEC Further than Samba?

- Move beyond Samba
- How could WINE use GENSEC?
- Could an windows network app on WINE use GENSEC?
- Linux apps built against Samba4 libraries?

Credentials Interface

Credentials - Definitions

- Credentials are:
  - Username
  - Domain
  - Passwords
  - Kerberos tickets
  - Kerberos realm

Credentials Interface

- Flexible password specification
- Need to work with Kerberos
  - We want to allow single sign on, really!
- Better interfaces
  - Not fixed 'username, domain, password'
  - We might be in a Kerberos realm instead
  - Password on demand, not upfront
- Single Context pointer

Credentials Callbacks

- User-specified password callbacks
- Allows callback from generic code into
  - Command line
  - GTK
  - Anything else..

How well do you know this?

- A value is set when a credential detail is specified:
- CRED_GUESS
  - Input from an environment variable
- CRED_CALLBACK
  - Use this callback function to get the value
- CRED_SPECIFIED
  - This was specified, say on the command line

C Interfaces

- cli_credentials_init()
  - Create a new, uninitialised credentials context.
- cli_credentials_get_*()
  - Return a value off the context, potentially calling the supplied callback to get the information.
- cli_credentials_set_*()
  - Set a particular value onto the context, The caller must specify 'how well' they know the value.

Further C Interfaces

- cli_credentials_guess()
  - Guess the username, password and domain from the available environment variables.
- cli_credentials_set_anonymous()
  - Setup an anonymous user context

Unexpected windfall

- Simplified access to machine account details
  - Each machine in a windows domain has its FREDSMACHINE$ account
  - This is used by Samba for certain tasks
- cli_credentials_set_machine_account()
  - Hides all the details of reading our secrets file from the various callers
  - Allows any command line app to have -P to use the machine account

Questions? Rotten Fruit?

- abartlet@samba.org
- http://hawkerc.net/staff/abartlet/Samba-GENSEC-2005.sxi