MIT Kerberos for Mobile Devices

Zhanna Tsitkova

MIT Kerberos Consortium

March 30, 2009

Mobile Technology Concerns

- Battery
- Limited CPU
- Limited Memory
- Hard for administration
- Network bandwidth
- High packet loss
- High latency
- Signal strength

Caching to reduce DNS traffic

Lite Client on Mac OS X ~450K

Local KDC cross-realm auth

General Rules for Mobile Device SW

- Identify core functionality
- Minimize features
- Minimize memory and storage used
  - Consider minimization of cache footprint
  - Limit allocated memory – consider static vs dynamic memory allocation
- Forfeit
  - Generality
  - Robustness
  - Diagnostics
- Performance
  - Identify few simple metrics

Lite Client

- Lite Client for MAC OS X ~ 450K
  - Server code stripping
  - Dead code stripping
  - Reducing error code strings
  - Disabling PKINIT
  - Disabling Replay Cache
- Defined (extra?) functionality
- Stable build environment
- Restricted flexibility

On-Demand Client

- Advantage
  - Flexibility
  - Customization
  - Optimization
- Difficulties
  - Constructing (building, export list generation)
  - Highest code modularity
  - Support

On-Demand Client

How to achieve:

- Code modularity
  - Examine cross-reference list

krb5_gss_init_sec_context	644
krb5_gss_accept_sec_context	636
krb5_auth_check	481
krb5_fast_auth	475
krb5_get_init_creds_password	475
krb5_verify_init_creds	457
krb5_set_password_using_ccache	439
krb5_gss_import_sec_context	417
krb5_get_in_tkt_with_skey	410….
krb5_ktsrvint_read_entry	58
krb5_fcc_generate_new	56
krb5_mcc_generate_new	55
krb5_fcc_set_flags	54
krb5_rd_rep	54
krb5_ldap_read_server_params	53
krb5_mk_ncred_basic	53
krb5_rd_rep_dce	53
krb5_def_store_mkey	52…..
krb5_set_default_in_tkt_ktypes	5
krb5_string_to_key	5
krb5_auth_con_getaddrs	4
krb5_auth_con_getsendsubkey	4
krb5_c_string_to_key	4

On-Demand Client

krb5_rd_rep: Calls 9 functions	krb5_rd_rep: Expands into 54 functions	
free	calloc	krb5int_c_decrypt_aead_compat
decode_krb5_ap_rep_enc_part	free	asn1buf_sync
decode_krb5_ap_rep	asn1_decode_encryption_key_ptr	asn1_decode_octetstring
memset	asn1_decode_maybe_unsigned	asn1_decode_seqnum
krb5_copy_keyblock	krb5int_c_locate_iov	krb5int_zap_data
krb5_c_decrypt	asn1_decode_unsigned_integer	asn1_decode_kerberos_time
krb5_free_keyblock	asn1_decode_encryption_key	memset
malloc	krb5_free_ap_rep_enc_part	__builtin_va_end
krb5_free_ap_rep	asn1buf_wrap_data	asn1_decode_enctype
	asn1_decode_generaltime	asn1_decode_integer
	memcmp	asn1_decode_encrypted_data
	decode_krb5_ap_rep	vasprintf
	asn1_decode_kvno	asn1buf_imbed
	decode_krb5_ap_rep_enc_part	krb5int_c_free_keyblock
	asn1buf_remove_charstring	krb5int_gmt_mktime
	asn1_decode_int32	asn1_decode_msgtype
	krb5int_c_iov_decrypt_stream	krb5_free_keyblock
	krb5_free_ap_rep	asn1_get_sequence
	asn1buf_remove_octetstring	__builtin_va_start
	asn1buf_skiptail	krb5int_vset_error
	krb5_c_decrypt	memcpy
	asn1_decode_charstring	asn1_get_eoc_tag
	krb5_copy_keyblock	asn1buf_remains
	krb5int_c_free_keyblock_contents	__builtin_va_copy
	vsnprintf	strdup
	malloc	krb5int_set_error
	__assert_fail	asn1_get_tag_2

Kerberos consortium
www.kerberos.org

On-Demand Client

476	krb5_get_init_creds_password	0.60025220681
458	krb5_verify_init_creds	0.761664564943
440	krb5_set_password_using_ccache	0.764186633039
410	krb5_get_in_tkt_with_skey	0.81210592686
398	krb5_get_in_tkt_with_keytab	0.81210592686
392	krb5_get_in_tkt_with_password	0.81210592686
388	krb5_sendauth	0.827238335435
381	krb5_fwd_tgt_creds	0.839848675914
374	krb5_mk_req	0.839848675914
356	krb5_get_credentials_validate	0.843631778058
356	krb5_get_credentials_renew	0.843631778058

On-Demand Client

How to achieve:

- Code modularity
  - Examine cross-reference list
  - Manipulate object files
- Create export list dynamically
- Crypto library plug-in
- Further optimization
  - Hard-coded configuration
  - On-demand - performance
- Identify easy to understand metrics
- Begin from the unit test

On-Demand Client

Targets:

- Ubuntu
  - MID platform
- “On –demand” partners
- Android – G1
  - Must be 100% Java/Dalvik solution
  - Remotely provisioning of the security updates

Keep the Dog on a Diet

Questions?

Comments?