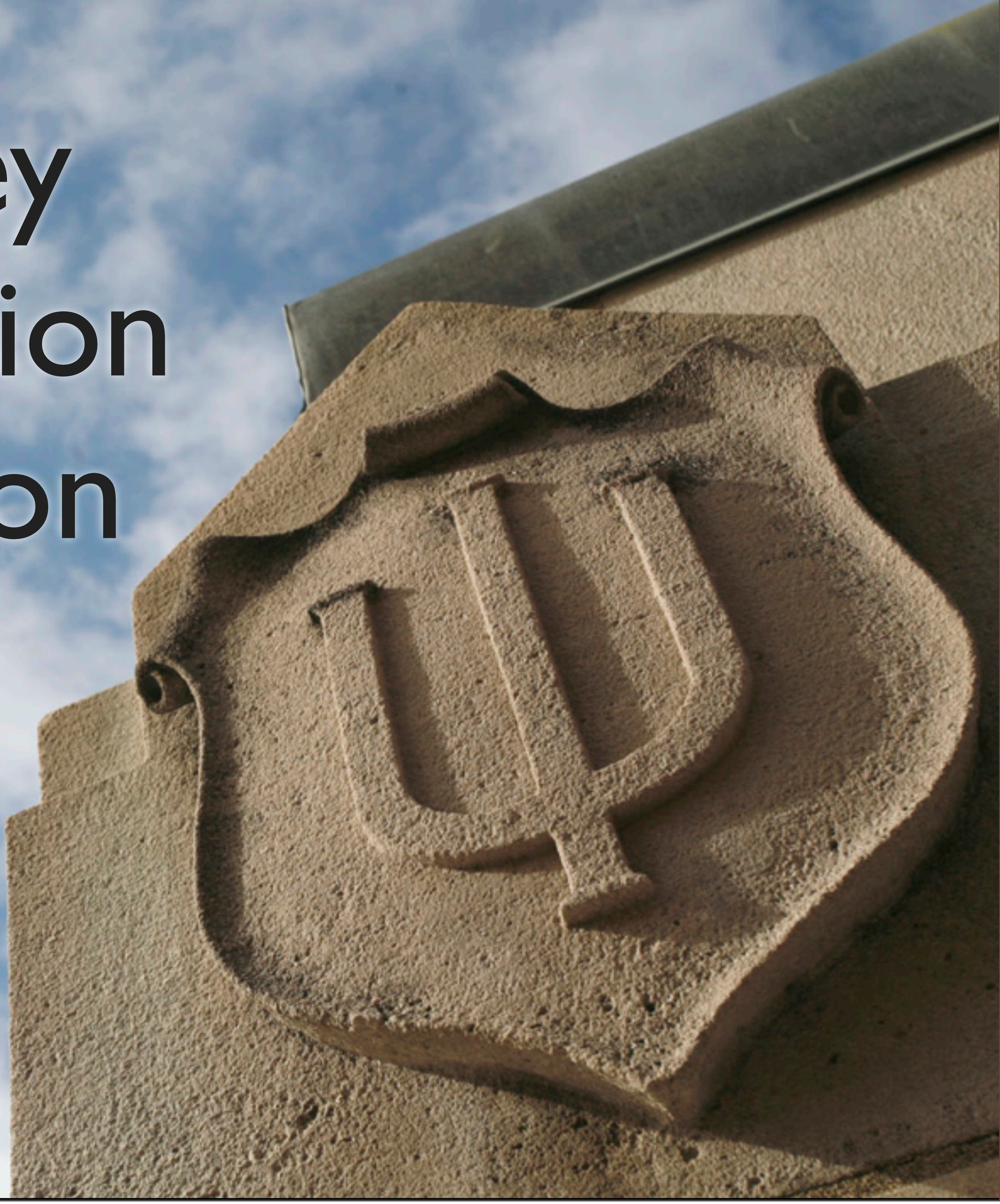
Lustre Shared-Key Authentication & Encryption

Andrew Korty
Indiana University



New Code

GSSAPI Mechanism	Lustre Security Flavor	Authentication	Encryption
null	*sknull*		
sk	*ski*	HMAC-SHA256	
	skpi	HMAC-SHA256	AES CTR mode

GSSAPI Challenges

FIXED	Lustre build problems
PENDING	Dependency on Kerberos, in both tests and code
FIXED	Not enabled on Intel test nodes
PENDING	Both user- and kernel-space mechanisms needed

Build-Time Change

	Before	After
nothing specified	GSSAPI disabled	GSSAPI enabled if prereqs satisfied; else disabled
`--enable-gss` specified	GSSAPI enabled if prereqs satisfied; else disabled	unchanged
`--disable-gss` specified	GSSAPI disabled	unchanged

Two Different APIs

Stripped-down Kernel GSSAPI	Real GSSAPI

gss_import_sec_context()
gss_copy_reverse_context()
gss_inquire_context()
gss_get_mic()
gss_verify_mic()
gss_wrap()
gss_unwrap()
gss_prep_bulk()
gss_wrap_bulk()
gss_unwrap_bulk()
gss_delete_sec_context()
gss_display()
	gss_acquire_cred()
	gss_release_cred()
	gss_init_sec_context()
	gss_accept_sec_context()
	gss_process_context_token()
	gss_delete_sec_context()
	gss_context_time()
	gss_sign()
	gss_verify()
	gss_seal()
	gss_unseal()
	gss_display_status()
	gss_indicate_mechs()
	gss_compare_name()
	gss_display_name()
	gss_import_name()
	gss_release_name()
	gss_inquire_cred()
	gss_add_cred()
	gss_export_sec_context()
	gss_import_sec_context()
	gss_inquire_cred_by_mech()
	gss_inquire_names_for_mech()
	gss_inquire_context()
	gss_internal_release_oid()
	gss_wrap_size_limit()
	gss_duplicate_name()
	gss_set_allowable_enctypes()
	gss_verify_mic()
	gss_export_lucid_sec_context()
	gss_free_lucid_sec_context()
	gss_get_mic()
	gss_wrap()
	gss_unwrap()
	gss_canonicalize_name()
	gss_export_name()

Current Status

- *null* GSSAPI mechanism & *sknull* security flavor in test now
- *skp* & *skpi* mechanisms & security flavors still in development

Conclusions

- Need better documentation of GSSAPI code & security flavors
- If you happen to have Lustre’s Kerberos support working in production, please contribute your changes

“When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl.”