

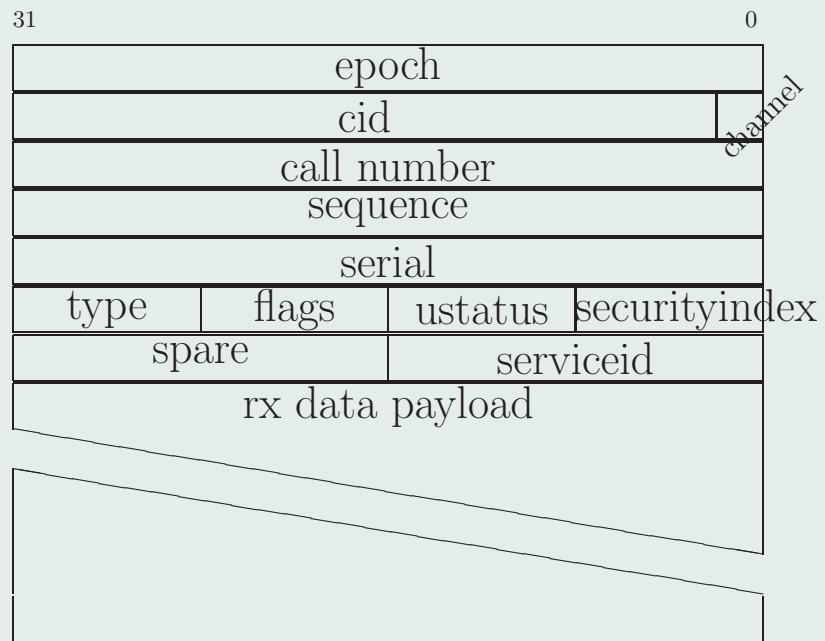
Marcus Watts
mdw@umich.edu

basic timeline

- document protocol - done
- produce split-out patches - pending
- rxk5ng ?

- authenticator max_calls 4
- PRF RFC 4402
- initial packet encryption
- k5ssl
- ubik_SRXServerProcV2 and afsconf_ServerAuthV2
- cell_max 256
- cm properties
- way for app to add data to authenticator

authenticator - max_calls 4

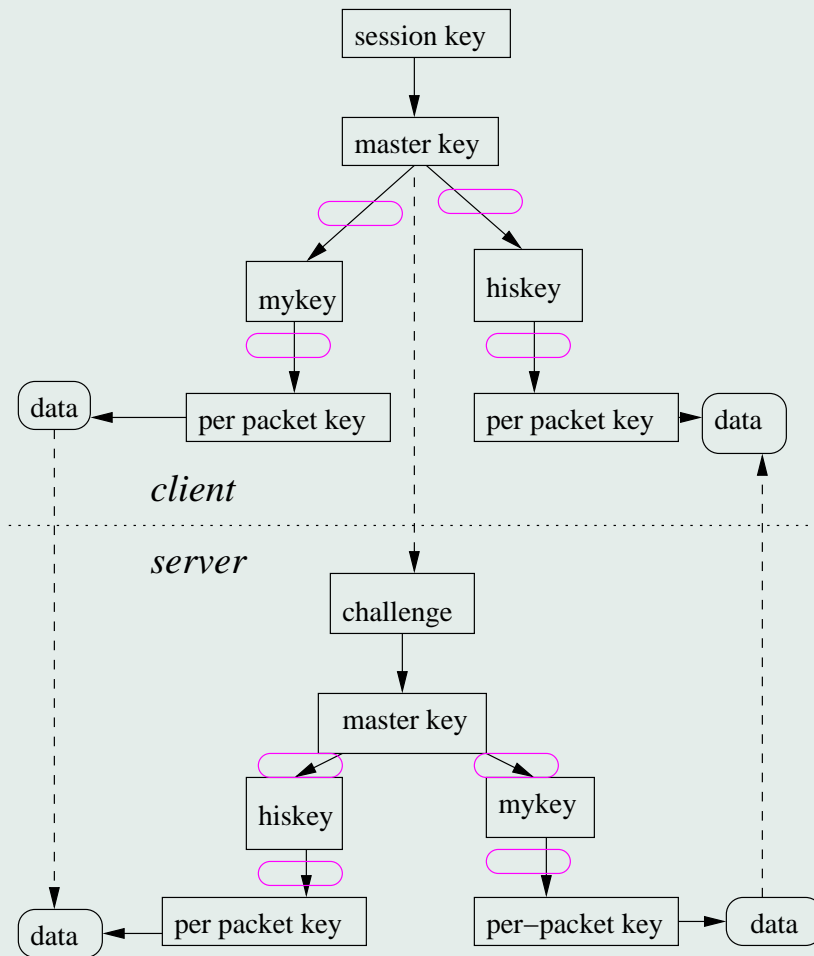


rx header

rxk5 authenticator₀

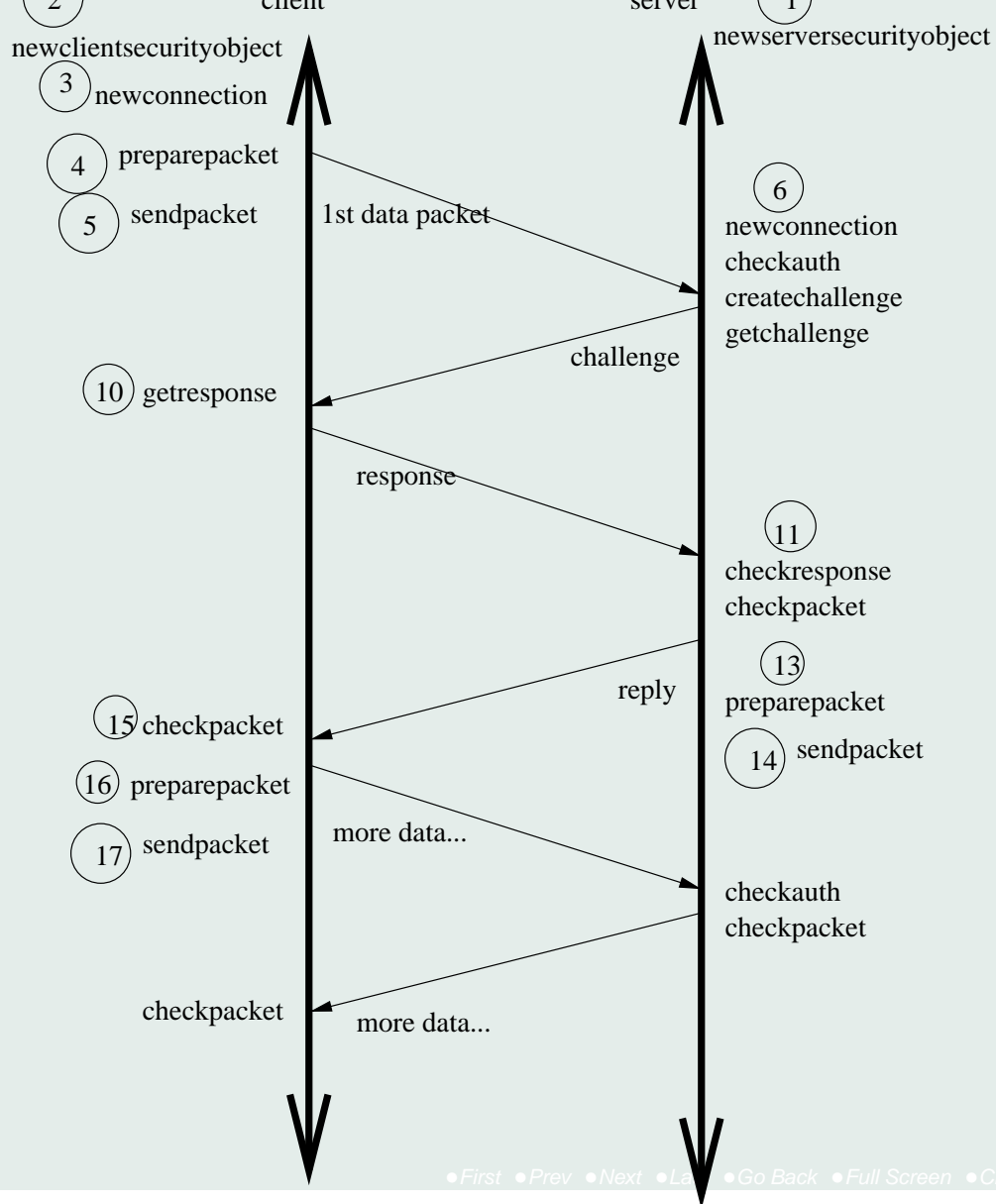
epoch		} endpoint
cuid	0	
securityindex		
1+challengeid		
level		
cktype		
dktype		
callnumber	0	
callnumber	1	
callnumber	2	
callnumber	3	
master key length		
master key data		

PRF RFC 4402



rxk5 key flow

initial packet encryption



packet flow

k5ssl

ubik_SRXServerProcV2 and afsconf_ServerAuthV2

cell_max 256

```
const AFSTOKEN_UNION_NOAUTH = 0;
const AFSTOKEN_UNION_K5 = 5;
union afstoken_soliton switch (int32_t at_type)⇒
⇐ {
    case AFSTOKEN_UNION_K5:
        token_rpk5 at_rpk5;
};
const AFSTOKEN_LENGTH_MAX = 16384;
const AFSTOKEN_CELL_MAX = 64;
const AFSTOKEN_MAX = 8;
typedef opaque token_opaque<AFSTOKEN_LENGTH_MAX ⇒
⇐>;
struct pioctl_set_token {
    int32_t flags;
    string cell<AFSTOKEN_CELL_MAX>;
    token_opaque tokens<AFSTOKEN_MAX>;
};
```

cm properties

rxk5.enctypes 18 17 16 23 8 3 2 1 24

string

xdr

others?

way for app to add data to authenticator

Conversion issues

- create keytab (but NOT kdc entry)
- deploy rxk5 servers & keytab - slow as you please
- add principal and key to kdc
- upgrade clients - slow as you please
- done!

openafs timeline

- 1.6 in 6 months - no possibility of improved encryption before then

rxk5:

- 8 items from hackathon for discussion
- split-out patches
- revised protocol?

Thanks!

Questions?