Secmech BOF

IETF 63

Agenda

Generally Usable Authentication Mechanism (GUAM)

jsalowey@cisco.com

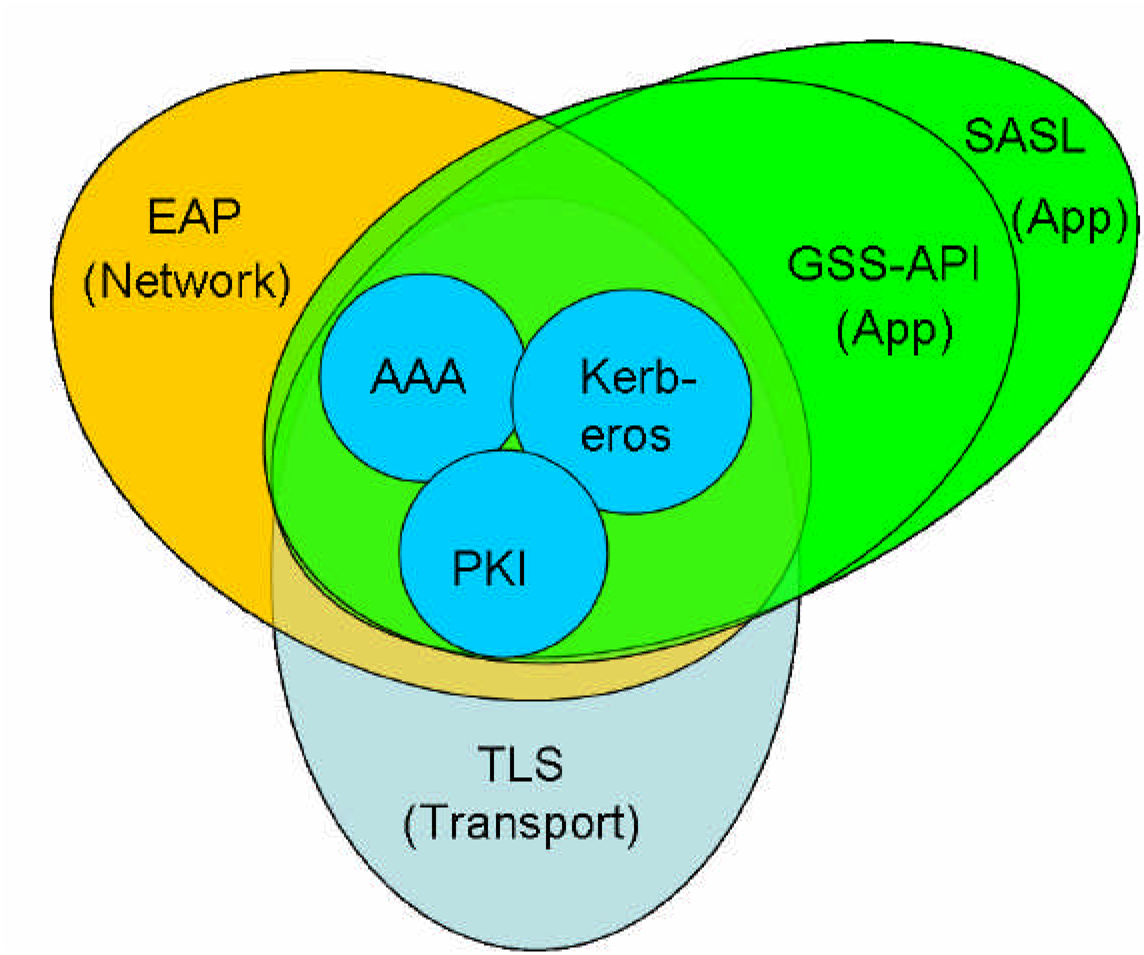
Problem 1:
Framework goals are very similar

- EAP, GSS-API and SASL all focus on authentication plus context establishment
- Differences are few
- Convergence is happening, but slowly
  - GSS-API recent work on PRF API for key material access
- Duplication of effort, slow rate of mechanism standardization (EAP)

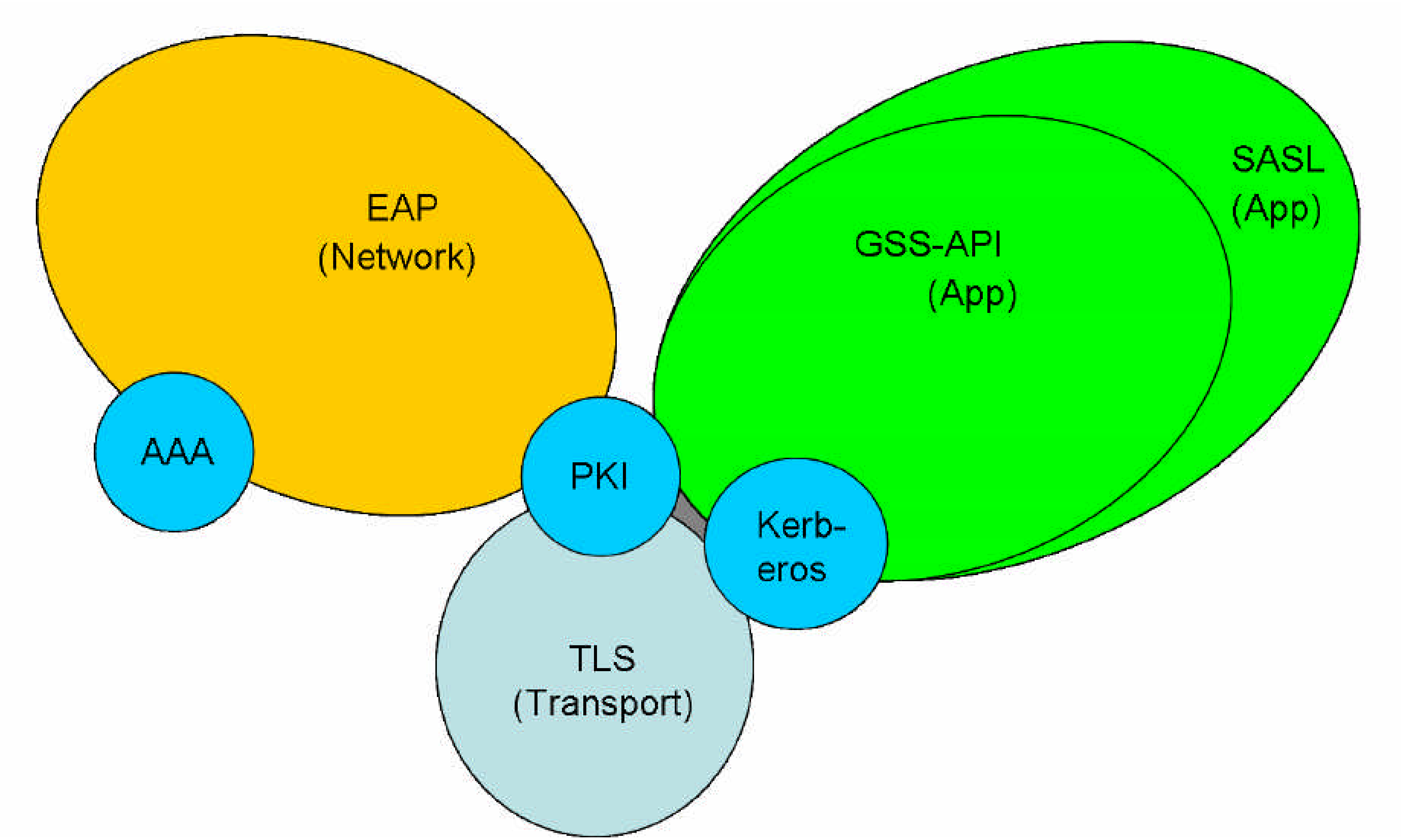
Problem 2: Inconsistent Mechanism Support

- Inconsistent support for security infrastructure
  - GSS-API primarily Kerberos, shared secret and PKI support tend to be proprietary
  - EAP primarily shared secrets in AAA, no Kerberos support
- Infrastructure is costly to deploy and maintain, yet it is difficult to re-use infrastructure for different purposes

Desired Situation



Current Situation



Framework/Mechanism Availability

- EAP has (or may soon have)
  - AAA integration, PKI
- TLS has
  - PKI,KRB-5 (sort of, don’t ask)
- GSS-API has
  - KRB-5, PKI (sort of, don’t ask)
- SASL has
  - Shared secret mechs, GSS-API mechs

Framework Applicability

- GSS-API
  - General applicability
- SASL
  - Connection oriented application
- EAP
  - Network access

Solution GUAM

- Develop mechanisms so the are useful in any frameworks
  - Mandate support for a required subset of capabilities
- Don’t require changes to frameworks
  - Frameworks are already tuned to their domain
  - Frameworks can be enhanced, enhancements optional

GUAM

- draft-salowey-guam-00.txt
- Discussion – secmech@ietf.org
- Unify approach to developing mechanisms for SASL, GSS-API and EAP
- Consistent interface to mechanism capabilities

Which Mechanisms?

- Any mechanism that is generally useful
  - Standard mechanisms
- Hopefully all
  - Capabilities are similar
  - Should not be much incremental work to define a mechanism

Capabilities of Authentication Mechanisms

- Mutual Authentication
- Key Material Access
- Security Layer
- Channel Bindings
- Authenticated Data Exchange

Requirements for Mechanisms

1. ID for each framework (GSS-API OID, EAP ID, SASL name)
2. Mutual authentication
3. Key derivation/export
4. Security layer – generic security layer possible
5. Channel bindings
6. Authenticated data exchange during authentication

Requirements for Mechanisms

7. Protocol support for initiation from either peer
8. Obtain credentials “in-band” (e.g. IAKERB)
9. Maintain security (integrity maybe confidentiality) through an arbitrary number of proxies
10. Document security properties
11. Naming
    - EAP Realm, GSS-API target, SASL authorization ID, Name Attributes

Next Steps

- Secmech BOF at Paris IETF
- Charter secmech WG to tackle EAP methods and GUAM
- (?) Work on generic security layer descriptions – CFRG?,reuse exisiting?
- (?) Tie into TLS – TLS WG
- (?) Naming/credentials interfaces – Kitten WG
- (?) Enrollment – (?) WG

SecMech

Jsalowey@Cisco.com

What should be done in Secmech?

- Work towards unification of security mechanisms
- Initially
  - EAP Methods
  - GUAM

Why Work on EAP Methods in SecMech?

- Not on any groups charter currently
- Set of mechanisms need to be chosen
- Cross area review is needed
  - Leverage experience from multiple groups
- Incremental work for GUAM is likely small
  - Both efforts may proceed in parallel

Proposal

- Determine what EAP mechanisms to fast-track
- Work on these mechanisms in parallel with GUAM
- GUAM mechanism requirements document
  - What features must a mechanism support
- GUAM mechanism process document
  - How do we define a GUAM mechanism

Possible Future Work

- Common Security Layer
- Naming enhancements and interfaces
- GUAM + TLS
- Additional mechanisms
- Other security unification work…

Next Steps

- Select Fast-Track EAP Mechanisms
- Charter to work on GUAM and EAP mechanisms