Network Security
and
Middleware Nirvana
or
Be careful what you ask for ...

RL “Bob” Morgan
SALS Workshop
August 12, 2003
Why security infrastructure?

• Make the right things easy
  – discovery
  – manageability
  – separating enforcement from management
  – translating policy to mechanism

• Make the wrong things hard
  – strong authentication
  – strong authorization, ie explicit permissions
What is this infra?

• Identity management
  - “accounts” (user ids, passwords, certs)
  - attributes (affiliations, groups, entitlements)
  - people and devices

• Authorization data management
  - roles, groups, organizations, entities
  - permissions, capabilities

• “Other” management
  - configuration, keys, logs, ...
Federation

- Interop among distinct organizations
  - aka “security domains”
  - specific purposes, limited interaction

- Organizational representation
  - interaction is typically organization-based
  - but: departments, consortia, virtual orgs
  - but: who exactly is “member”, official contact

- A well-paved road
  - but real ones starting to happen, e.g. grids, InCommon
P2P vs Infra

• we're in “peer mode” at SALS ... and everywhere
  – recognition based on real-world clues
  – building new interaction based on previous

• necessary conflict with org infra?
  – well-managed vs “friendly”
  – policy-based vs get-something-done-based

• work to bring these together ...
  – turn “contacts” into “accounts”
  – strong mechanisms without strong identification ...
Support for security management

- Network security management is “enterprise app”
- benefits from
  - strong user identification (sysadmins, net admins)
  - department definitions
  - policy-based authorization
  - federation (inter-org contacts)
  - device definition
- but hard to integrate “point tools” ...
IPsec to the rescue?

• suppose all communication were IPsec-protected?
  – i.e., no response unless security can be negotiated
• and key management were made easy enough
  – infra support via id mgt, key mgt
  – P2P integration
  – cross-app, cross-level integration in platform
• sounds like a big win ...
  – but is it feasible enough to be worth the large effort?
Wireless access drives PKI?

- wireless authn has strong requirements
  - strong mutual authentication
  - location-based access control
  - transparency necessary for usability
- hence PKI-based end-user authn
  - on new generation of devices, APs, protocols
  - primarily intra-org ...
- if it works for wireless ...
  - why not wired, dialup, etc?
New protocols drive PKI?

• new protocols explicitly multi-hop
  – SIP, XMPP, Diameter, SOAP, P2P
  – implies message protection end-to-end, i.e. S/MIME
  – what means “end to end” in brave new world?

• feasible with global-reach applications?
  – key discovery to make a phone call?
  – too much X.509 baggage in deployed “PKI”?
Middlebox communication

- IETF work on middleboxen
  - define architectural features
  - infra support
  - app interaction
- Is failure of transparency part of the problem?
  - i.e., problem isn't presence of middlebox itself
- If so, is adding middlebox manageability and app-visibility the solution?
When it all works ...

• protection can happen at all levels ... at once
  - network (e.g. WEP replacements)
  - internet (IPsec)
  - “transport” (SSL/TLS)
  - application (S/MIME etc)
  - the last mile ... of code paths

• optimization implies cross-layer service hooks ...
  - high-speed apps may need dispensation to turn off some security measures