EAP roadmap
Or
What to do about methods?

Erik Nordmark
erik.nordmark@sun.com

Methods, methods, methods

- At what point will we have a good enough set of documents to review methods?
- Who should review documents? (WG or elsewhere)
  - WG capacity
- Requirements on methods?
  - From IEEE 802.11, 3GPP, ourselves
- Selecting mandatory methods?
  - Using what criteria?

Stable base

- Believe to be sufficient to have
  - RFC 2284bis
  - Keying framework
- Sufficient to say whether methods are well-specified and conforming with the base
- Doesn't tell whether the methods are suitable for a particular environment

Requirements?

- IEEE 802.11: requirement on methods
  - Support the following credentials: digital certificates, user-names and passwords, existing secure tokens, and mobile network credentials (GSM and UMTS secrets).
  - Generate keying material
  - Support mutual authentication
  - Are resistant to dictionary attacks, and
  - Provide protection against man-in-the-middle attacks.
- 3GPP: Publish legacy methods
- Ourselves? Better mandatory method than MD5?

Requirements

- Useful write them down
- First decide purpose of writing them down
  - Difference between a list of requirements as documentation, and
  - Criteria used to select a (single) winner
- The IEEE 802.11 list might be a reasonable starting point

Select methods?

- IEEE 802.11 requests that we augment the set of mandatory to implement methods
- Do we want a better mandatory than MD5?
- How can we select which one(s) get “mandatory to implement” stamp of approval?
  - “ One size fits all” or dependent on environment?
  - Signficant delay (9-12 months) to run selection
    - Develop criteria document, ask for submissions, jury evaluation

Strawman proposal (½)

- Finish 2284bis and keying framework
  - Keep MD5 mandatory
- Capture 802.11 requirements and goals in I-D
  - Not evaluation criteria
- Verify that some set of methods consistent with base
  - In WG or outside WG?
  - OK to publish those as informational
  - Can start this before 2284bis + keying are RFC

Strawman proposal (2/2)

- Start work on a BCP document to capture mapping from environment and threats to properties of methods?
  - If concerned about X the method needs to support Y and Z, etc
- Decline the request from 802.11 to select mandatory to implement
  - Suggest that they do this themselves, perhaps based on the BCP, for their environment
- Consider later changing “default” from MD5