Some possible BCP 72 additions

Jari Arkko

IETF 108 SAAG

Context: Model-T Discussions

We may want to extend the set of threats considered, due to success (encryption use), and the emergence of new issues

- Reducing the protection offered by comsec tools is a non-goal.
- IAB program is about documents and discussion, not about changing IETF BCPs

Two kinds of discussions:

- Documenting threats, issues, and design guidelines
- Suggestions for (small) eventual additions to RFCs 3552 & 7258 (see next slide)

thomson-tmi
mcfadden-smart-endpoint-taxonomy-for-cless
mcfadden-smart-threat-changes
lazanski-users-threat-model-t
lazanski-protocol-sec-design-model-t
arkko-farrell-arch-model-t
…

Possible BCP 72 (RFC 3552) additions

Approach: BCP 72 shouldn’t be a listing of kitchen sink guidelines

- Also, the threat model is a small part of the RFC

However, some bigger issues should be recognised (briefly)

Drart-arkko-farrell-arch-model-t-3552-additions is one tentative suggestion:

> ”In general, we assume that the end-system engaging in a protocol exchange has not itself been compromised. Protecting against an attack of a protocol implementation itself is extraordinarily difficult. It is, however, possible to design protocols which minimize the extent of the damage done when the other parties in a protocol become compromised or do not act in the best interests the end-system implementing a protocol.”

> New small subsections on ”Other endpoint compromise”, ”Limiting scope of compromise”, ”Forcing active attacks”, ”Traffic analysis”, and ”Containing compromise of trust points” (text largely by Ekr & Chris W.)

Thank you

Questions, comments, feedback?