Outline

• Statement of Objectives
• Analyze both LKS and KSP
• Convergence
Statement of Objectives

• The goal of the 802.1 WG is to come up with a group session key agreement protocol based on pre-shared master key CAK

• The group session key agreement process MUST not assume the presence of a dedicated server known to everyone

• The protocol MUST prove the liveliness of the entities existing on the same LAN
Analysis of LKS and KSP

• Both intend to achieve liveliness proof using effectively a group random challenge-response process

• As a third person new to both protocols, my understanding comes slower than expected because the group random challenge-response phase is merged with the session key distribution/agreement process

• I will attempt to digest both in the next few slides...
LKS Further Analysis

• LKS uses randomly generated session key as the challenge, the response from every one is:
  – Sorry, I think I should generate the key OR
  – You are the man and give me your latest!

• The obvious benefit is that after this challenge-response process, key is already distributed and every one agreed who is the distributor (server)

• Disadvantages
  – Since every step involves session key generation, it is less efficient if the PRF gets complicated
  – When does the server A know everyone has responded and the session key is ready for good?
  – Even worse, if server A delivers the final session key to B and C, when does B know to use the session key to communicate to C? The key distribution is broadcasted, the traffic encryption is not.
KSP Further Analysis

• KSP uses randomly generated key contribution (KC) as the challenge, the response from every one is a hash of all KCs

• Every one knows the convergence time when their own computed KC matches the KCs they receive, therefore the ‘actor’ is elected

• There is a final key distribution phase from the ‘actor’ to everyone

• Advantages
  – The obvious convergence point in the first phase
  – Every one contributed to the session key entropy

• Disadvantage
  – Since everyone got the everyone else's entropy, the final key distribution seems a bit redundant
  – It is not obvious to me as a first time reader how is the final session key distribution confirmed by the group members
Converge LKS and KSP

• Recommend borrowing the randomly generated MI as the challenge or KC, even if the MI is skewed, a portion of it should still be fairly random.

• Rather than distribute the session key, I recommend all group members advertising the session key they generated as the confirmation to KC.

• The convergence point would be that everyone has generated a common session key!

• There is no need for final key distribution because everyone has it.
I call this new scheme GCRKAP: group challenge-response key agreement protocol