Negotiation in Keying Management Protocols
draft-liang-karp-negotiation-kmp-00

IETF80 Prague, Czech Republic
April 1, 2011

Xiaoping Liang (Ellen)
ZTE Corporation
liang.xiaoping@zte.com.cn
Motivation

• Negotiation is one prominent capability of KMPs
• KMPs especially group KMPs lack SA Negotiation for Routing Protocols
Goals

• Discuss reasons and concerns of using negotiation in KMPs
• Discuss three types of negotiation in KMPs
Prior Work

- draft-wei-karp-analysis-rp-sa-01
- draft-liang-karp-auto-sa-management-rp-01
Draft Outline

• Why Need Negotiation
• Concerns and Possible Solutions When Using Negotiation
• Negotiation in KMPs
Why Need Negotiation

• Main reason
  • Diverse security requirements & security
  • Objective: interconnectivity, interoperation, cooperation

• Specific reasons in KMPs
  • Algorithm agility
  • Implementation
  • Configuration
  • Deployment and incremental deployment
Concerns and Possible Solutions When Using Negotiation

• Concerns
  • Improper implementations cause unexpected consequences when using negotiation

• Two possible solutions
  • Translator/transformer
  • Falling-back negotiation mechanism/re-negotiation mechanism
Negotiation in KMPs

• Initial SA negotiation to establish secure channel
  • Phase 1 exchange of ISAKMP, initial exchange in IKEv2

• Peer-to-peer SA negotiation for application data, e.g. RP
  • Phase 2 exchange of ISAKMP, IKE_AUTH&CREATE_CHILD_SA exchange of IKEv2

• Group SA negotiation for application data, e.g. RP
  • One possible approach: GCKS collects security parameters from GMs, and generates GSA according to security parameters supported by all or most GMs
Q&A

Any discussion and comment are welcome!