Life cycle key management costs in secure multicast (draft-irtf-gsec-lifecycle-00.txt)

Authors: M. Howarth, S. Iyengar
H. Cruickshank and Z. Sun
University of Surrey, UK

GSEC at IETF-57, Vienna, Austria
16 July 2003

Introduction

- Normally, the user join/ leave rekeying is the principal cost of key management, with tree initialization costs being negligible:
  - However, applications exist, where the tree initialization costs is significant, such as file transfer and videoconferences
- We introduce the concept of the life cycle key distribution cost for hierarchical tree such as LKH. It takes account of:
  - The cost of rekeying when users join or leave an established group
  - The costs of building a tree during initialization of a multicast group
- We show how the optimum outdegree (k) in a hierarchical tree varies with the expected user volatility and rekey factor.

User volatility implications on tree outdegree k

- Three cases are considered:
  - Case 1: Receivers with perfect memory
  - Case 2: A receiver gets all the keys at the time of joining
  - Case 3: Rekey the group on each join (backward secrecy)
- We define the volatility factor alpha as the mean number of rekeys per Group Member (GM).
- We observe that:
  - In Case 2, key life cycle cost can be reduced significantly at low volatility by optimizing k, for example corporate videoconferencing
  - Backward secrecy has the highest cost
  - For frequent rekeying (alpha>>1) the curves in all cases converge and the cost is independent of the initialization approach

Group key updating implications on tree outdegree k

- The life cycle cost can also be considered by taking into account periodic rekeying to prevent cryptanalysis.
- We define a normalized rekey factor beta = T / N.tau; where T is the lifetime of the group; tau group update and N is total number of group members.
- We observe that:
  - low beta, i.e when the number of rekeys per GM is low, the optimum value of k is >>3
  - At high beta, i.e rekeying to prevent cryptanalysis predominates over initial tree building costs, and so the optimum value of k is 2

	k = 3	k optimized for min cost
Volatility alpha	1.Perfect memory reqd (pre-reg)	2. Tx as (int arr arrival)	3. PBS 1.Perfect memory reqd (pre-reg)	2. Tx as (int arr arrival)	3. PBS
0.0001	1500	6290	12580	1020	1100	12410
0.001	1520	6310	12590	1090	1560	12420
0.01	1680	6470	12760	1400	2610	12590
0.1	3280	8070	14410	3220	5870	14290
1	19360	24150	30940	19340	23810	30940
10	180130	184920	196210	179350	184560	195590

Table 1: life cycle cost as a function of volatility alpha
(N = 1000 receivers)

Volatility alpha	1. Perf mem (pre-register)	2. Tx as reqd (Intermittent arrivals)	3. PBS (Intermittent arrivals)
0.01	9	38	4
0.1	4	9	4
1	3	4	3
10	3	3	3

Table 2: optimum value of tree outdegree k as a function of volatility alpha (N = 1000 receivers)

Outdegree k	1. Perf mem (pre-register)	2. Tx as reqd (Intermittent arrivals)	3. PBS (Intermittent arrivals)
2	3890	11860	16890
3	3280	8070	14410
4	3230	6880	14400
6	3410	6070	15760
10	4010	5900	19450
20	5560	6820	28770

Table 3: cost sensitivity illustrated for volatility alpha = 0.1
(N = 1000 receivers)

Conclusions

- We have shown how pre-registration (case 1) can reduce the hierarchical tree initialization cost.
- For applications with low volatility alpha, there is an optimum tree outdegree that varies with the volatility alpha.
- Similarly, the optimum tree outdegree varies with the rekey factor beta that reflects the number of group key updates.
- Possible future direction: Focusing on the key lifecycle cost for GSAKMP and GDOI.
- The authors are pleased to acknowledge the support from the European Union Growth Programme and the ASP-NET project.