EFFICIENT MULTICAST KEY MANAGEMENT FOR DYNAMIC ARMY TACTICAL NETWORKS*

Extended Abstract

Brian J. Matt†
McAfee Research
Rockville, MD

1. INTRODUCTION

Many of the applications vital to the Objective Force will rely on multicast and other forms of group communication using the wireless battlefield networks of Future Combat Systems. Achieving secure and survivable communications for these applications requires group key management techniques that meet the unique challenges of battlefield networks. These challenges include minimizing re-keying delay while maximizing re-keying reliability, minimizing energy consumption, etc. The techniques must also provide scalability, and minimize communication while conforming to key storage and processing constraints.

Achieving acceptable performance in tactical networks is impeded by the fact that members of a group will typically be in motion, using a network that is changing and operating in a dynamic environment. Such an environment favors keying techniques that are flexible; however, the communications used by traditional, efficient, hierarchical group keying schemes, such as Logical Key Hierarchy (LKH) (Wallner et al., 1998; Wong et al., 1998), One Way Function Tree (OFT) (Sherman and McGrew, 2003), One Way Function Chain (OFC) (Canetti et al., 1999), and related schemes (Rafaeli et al., 2001; Zhu et al., 2003, Loukas and Poovendran, 2004) to perform re-keying operations are rather rigid. In order to evict a group member, the group key manager must establish a new group key by sending new cryptographic secrets to certain subgroups corresponding to sub-trees of the "key trees" used by those schemes. When the manager has only expensive, unreliable, or slow communications with some of these subgroups, the manager will want the flexibility to limit communications with those subgroups. LKH provides no such flexibility, while OFT and OFC provide limited flexibility.

We have developed a new hierarchical keying technique, OFC-X. OFC-X has lower communication costs than LKH, OFT, and OFC since it distributes fewer secrets; moreover, OFC-X provides the group manager with greater flexibility to lower secret distribution costs, increase secret distribution reliability, etc., than previous schemes.

2. THE OFC-X TECHNIQUE

We provide a brief summary of OFC-X. OFC-X constructs and maintains a hierarchy of keys. The group manager and each group member generate a shared secret using a practical non-interactive identity-based key agreement scheme (Sakai et al., 2000; Dupont and Engre, 2003). The manager and member generate a series of leaf node secrets for use with OFC-X, using a special key derivation function plus their shared secret. To establish these shared secrets the manager distributes "key material" to the group members in LKH, OFT, and OFC.

In OFC-X each node v of a key tree has a node secret x_v and a node key k_v. The group key is the root node secret. To compute node keys and interior node secrets OFC-X uses three special one-way functions: 1) e is used to compute a new instance of a node secret x'_v from the current secret x_v; 2) f is used to compute a parent node secret from current instance of the left child node secret or the right child secret; and 3) g is used to compute node keys from node secrets $k_v = g(x_v)$. $E(k : m)$ denotes the encryption of message m under key k.

The node secrets are used to derive group keys in a bottom up fashion. Let v be an interior node of an OFC-X key tree and let L and R be, respectively, the left and right child nodes of v. During a re-key operation, one of four possible conditions will apply to node v: 1) neither subtree of v has changed and no action is taken for this node; 2) the left subtree of v has changed, and the manager computes a new node secret for v by using $x_v = f(x_L)$ and sending a node secret distribution

*Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program, DAAD19-01-2-0011. The U. S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

†The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U. S. Government.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 DEC 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Efficient Multicast Key Management for Dynamic Army Tactical Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **McAfee Research Rockville, Md**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**2**	

message containing $E(k_R : x_v)$ to the members in right subtree, or by using $x_v = f(x'_R = e(x_R))$[1] and sending $E(k_L : x_v)$ to the left subtree; 3) the right subtree of v has changed, and the operations performed are the mirror image of condition 2; and 4) both subtrees have changed and the manager computes either $x_v = f(x_L)$ or $x_v = f(x_R)$ and sends the encrypted result to the members of the appropriate subtree.

3. COMPARISON

Since OFC-X uses non-interactive identity based key agreement and key derivation to establish leaf node secrets for the key tree, OFC-X distributes one less secret than do OFT and OFC when a member is added or evicted.[2] OFC-X provides greater node secret distribution flexibility than the other schemes. Whenever the secret of an interior key tree node changes in LKH, a new secret must be sent to both subtrees of the node. The group key manager has no flexibility. When an interior node secret changes in OFT and OFC, due to membership changes in either its left or right subtree, the group manager must send a new secret to the opposite subtree. The manager's flexibility is limited to what order changes are made and where additions are made.

The greater flexibility provided by OFC-X results in better performance – e.g., lower re-key energy consumption. For a single member eviction, the energy cost of LKH is the sum of the cost of updating both sub-trees for each interior node along a path through the key tree plus the cost of updating a leaf node. On average the typical cost of an interior node update at a certain level of the tree is about twice the average cost of updating a subtree at that level. For OFT and OFC, the energy cost is the sum of updating one of the sub-trees for each interior node along a path plus the cost of updating a leaf node. On average the typical cost of an interior node update at a certain level of the tree is the average cost of updating a sub-tree at that level. For OFC-X the cost is the sum of the minimum of the cost of updating either of the node's sub-trees, for each interior node along a path. On average the typical cost of an interior node update at a certain level is the average minimum of the cost of updating either of its sub-trees.

For energy consumption minimization, OFC-X offers the greatest benefits compared to the other schemes when communication with a subgroup is very expensive, and the subgroup is localized to a portion of the key tree. Our analysis has shown that OFC-X offers the greatest benefits when the metric of interest is especially sensitive to localized network problems.[3]

[1]For future re-key operations, $x_R = x'_R$.

[2]LKH distributes twice as many secrets as do the other schemes.

[3]E.g., the delay in re-keying the entire group, which is determined by a maximum of a set of values, rather than energy consumption, which is based on a sum of values.

4. CONCLUSION

We have presented some important aspects of a new hierarchical key management scheme that is particularly well suited for mobile Army battlefield networks. The OFC-X scheme provides enhanced perfromance and reliability by enabling a group key manager to decide on the fly which subtree of a node, with a changing membership, should receive a new node secret. By exerting such control over which subtrees receive new node secrets (which subsets of the members of the group need to receive new secrets), the group manager is able to adapt to changing environments, network topology, and adversary actions.

REFERENCES

Canetti R., Garay J., Itkis G., Micciancio D., Naor M., and Pinkas B., Multicast security: A taxonomy and some efficient constructions. In *Proc. IEEE INFOCOM'99*, 1999.

Dupont R. and Enge A., Practical non-interactive key distribution based on pairings. In *International Workshop on Coding and Cryptography (WCC)*, 2003.

Lazos L. and Poovendran R., Cross-layer design for energy-efficient secure multicast communications in ad hoc networks. In *IEEE International Conference on Communications (ICC)*, 2004.

Rafaeli S., Mathy L., and Hutchison D., EHBT: An efficient protocol for group key management. In *Networked Group Communication 2001*, 2001.

Sakai R., Ohgishi K., and Kasahara M., Cryptosystems based on pairing. In *2000 Symposium on Cryptography and Information Security (SCIS2000)*, 2000.

Sherman A. and McGrew D., Key Establishment in Large Dynamic Groups Using One-way Function Trees. *IEEE Transactions on Software Engineering*, 29(5), May 2003.

Wallner D., Harder E., and Agee R., Key management for multicast: issues and architectures. INTERNET DRAFT, September. 1998.

Wong C., Gouda M., and Lam S., Secure group communications using key graphs. In *Proceedings of the ACM SIGCOMM '98*, 1998.

Zhu F., Chan A., and Noubir G., Optimal tree structure for key management of simultaneous join/leave in secure multicast. In *Proceedings of MILCOM '03*, 2003.