A Flaw in a Self-Healing Key Distribution Scheme

Carlo Blundo, Paolo D'Arco, and Massimiliano Listo
[1] Dipartimento di Informatica ed Applicazioni
Università di Salerno, 84081 Baronissi (SA), Italy
e-mail: {carblu, paodar}@dia.unisa.it
e-mail: maslis@diaedu.unisa.it

February 4, 2003

Abstract

A self-healing key distribution scheme enables a dynamic group of users to establish a group key over an *unreliable* channel. In such a scheme, a group manager, to distribute a session key to each member of the group, broadcasts packets along the channel. If some packet get lost, users are still capable of recovering the group key using the received packets, without requesting additional transmission from the group manager. A user must be member both before and after the session in which a particular key is sent in order to recover the key through "self-healing". This novel and appealing approach to key distribution is quite suitable in military applications and in several Internet-related settings, where high security requirements should be satisfied. In this paper we show a *ciphertext-only* attack that applies to a proposed scheme.

1 Introduction

How to distribute session keys for secure communication to groups of users of a network, in a manner that is resistant to packet loss, is an issue that has not been addressed in-depth in the past. Indeed, the greatest part of the literature assumes an underlying reliable network. Recently, in [29], an interesting approach to deal with this scenario has been proposed. A *self-healing key distribution scheme* [29] enables a dynamic group of users to establish a group key over an unreliable channel. In such a scheme, a group manager, to distribute a session key to each member of the group, broadcasts packets along the channel. If some packet get lost, users are still capable of recovering the group key using the received packets, without requesting additional transmission from the group manager. The only requirement is that a user must be member both before and after the session in which a particular key is sent, in order to recover the missing key through self-healing. The benefit of such an approach basically are: reduction of network traffic, reduction of the work load on the group manager, and a lower risk of user exposure through traffic analysis.

Previous work. Broadcast Encryption is one of the closest area to the subject of this paper. Originated in [2], and formally defined in [12], it has been extensively studied (e.g., [3, 4, 15, 31, 22, 32]), and it has grown up in different directions: mainly, re-keying schemes for *dynamic* groups of users (see, [36, 5, 6, 27, 10] to name a few), and broadcast schemes with tracing capability for dishonest users [7, 26, 11, 13, 33, 34, 35, 30, 14, 28, 17, 18]. Moreover, several papers have addressed the special case of *users revocation* from a privileged subset [19, 1, 24, 23, 16, 20].

However, all the above papers assume that the underlying network is reliable. The authors of [25] and [37], have considered a setting in which packets can get lost during transmission. In the first case, error correction techniques have been employed. In the second, short hint messages are appended to the packets. The schemes given in [19], by accurately choosing the values of the parameters, can provide resistance to packet loss as well. Recently, in [29, 21] the problem has been addressed, and the key recovery approach pursued in both papers is quite similar: each packet enables the user to recover the current key and a share of previous and subsequent ones. Finally, in [9] also this problem is considered. The paper generalises several known constructions in order to gain resistance to packet loss.

Our Contribution. In this paper we analyse the self-healing approach to key distribution introduced in [29], and a scheme therein proposed. We describe a simple multiple-message attack which enables an adversary to easily compute the group session keys generated and sent by the group manager. Then, we show how such a scheme can be modified in order to be secure.

2 Model

The Model we consider in this paper is the same given in [29]. Let GM be a group manager, and let $U_1, \ldots, U_n$ be n users of the network. Each user U_i stores a personal key, S_i, which can be seen as a subset of elements of a certain field F_q, where $q > n$. Individual personal keys can be related. All the operations of the schemes take place in F_q.

We denote the number of sessions by m, and the set of users revoked in session j by R. Moreover, for $j = 1, \ldots, m$, the session key K_j is sent to the group members through a broadcast, B_j, from the group manager. For any non-revoked user U_i, the j-th session key, K_j, is determined by B_j and S_i. Denoting by $\mathbf{S}_i, \mathbf{B}_j, \mathbf{K}_j$ the random variables associated with the above elements, and by $\mathbf{Z}_{i,j}$ a random variable which represents the amount of information $Z_{i,j}$ that user U_i gets from the broadcast B_j and S_i, and using the entropy function, we state the following definition:

Definition 2.1 *[Self-Healing Key Distribution Scheme with Revocation][29]*
Let $t, i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$.

1. *$\mathcal{D}$ is a session key distribution scheme if the following are true:*
   - *For any member U_i, the key K_j is determined by $Z_{i,j}$. Formally, it holds that: $H(\mathbf{Z}_{i,j}|\mathbf{B}_j, \mathbf{S}_i) = 0$ and $H(\mathbf{K}_j|\mathbf{Z}_{i,j}) = 0$*
   - *For any subset $F \subseteq \{U_1, \ldots U_n\}$, such that $|F| \leq t$ and $U_i \notin F$, the users in F cannot determine anything about S_i. Formally, it holds that: $H(\mathbf{S}_i|\{\mathbf{S}_{i'}\}_{U_{i'} \in F}, \mathbf{B}_1, \ldots, \mathbf{B}_m) = H(\mathbf{S}_i)$.*
   - *What members $U_1, \ldots, U_n$ learn from the broadcast B_j cannot be determined from the broadcast or personal keys alone. Formally, it holds that: $H(\mathbf{Z}_{i,j}|\mathbf{B}_1, \ldots, \mathbf{B}_m) = H(\mathbf{Z}_{i,j}|\mathbf{S}_1, \ldots, \mathbf{S}_n) = H(\mathbf{Z}_{i,j})$.*
2. *$\mathcal{D}$ has t-revocation capability if, given any set $R \subseteq \{U_1, \ldots, U_m\}$, where $|R| \leq t$, the group manager can generate a broadcast B_j such that, for all $U_i \notin R$, the user U_i can recover K_j but the revoked users cannot. Formally, it holds that: $H(\mathbf{K}_j|\mathbf{B}_j, \mathbf{S}_i) = 0$ while $H(\mathbf{K}_j|\mathbf{B}_j, \{\mathbf{S}_{i'}\}_{U_{i'} \in R}) = H(\mathbf{K}_j)$.*
3. *$\mathcal{D}$ is self-healing if, for any $1 \leq j_1 < j < j_2 \leq m$, the following properties are satisfied:*
   - *For any U_i who is member in session j_1 and j_2, the key K_j is determined by $\{Z_{i,j_1}, Z_{i,j_2}\}$. Formally, it holds that: $H(\mathbf{K}_j|\mathbf{Z}_{i,j_1}, \mathbf{Z}_{i,j_2}) = 0$.*
   - *Given any two disjoint subsets $F, G \subset \{U_1, \ldots, U_n\}$, where $|F \cup G| \leq t$, the set $\{Z_{i',j}\}_{\{U_{i'} \in F\}} \cup \{Z_{i',j}\}_{\{U_{i'} \in G\}}$, contains no information on K_j. Formally, it holds that: $H(\mathbf{K}_j|\{\mathbf{Z}_{i',j}\}_{\{U_{i'} \in F\}}, \{\mathbf{Z}_{i',j}\}_{\{U_{i'} \in G\}}) = H(\mathbf{K}_j)$.*

$\triangle$

The definition is divided in three parts: the first one states the conditions that must be satisfied in a session key distribution scheme.

The second and the third parts define the additional t-revocation capability and self-healing property. As we will show later on, the first construction given in [29] does not satisfy the third condition of a session key distribution scheme. An adversary who gets the sequence of broadcast $B_1, \ldots, B_m$, recovers K_j, for any $j = 2, \ldots, m-1$.

3 Construction and Attack

In this section we describe the basic self-healing key distribution scheme given in [29], and we show how an adversary can recover the session keys broadcasted by the group manager.

Construction 1 **of [29].** A self healing session key distribution scheme without revocation capability.

SET-UP: Let t be a positive integer. The group manager chooses $2m$ polynomials in $F_q[x]$ each of degree t, say $h_1, \ldots, h_m, p_1, \ldots, p_m$, and m session keys, $K_1, \ldots, K_m \in F_q$, all at random. Then, for each $j = 1, \ldots, m$, he defines a polynomial in $F_q[x]$, $q_j(x) = K_j - p_j(x)$. For $i = 1, \ldots, n$, user U_i stores the personal key $S_i = \{i, h_1(i), \ldots, h_m(i)\} \subseteq F_q$.

BROADCAST: In session $j \in \{1, \ldots, m\}$, the group manager broadcasts $B_j = \{h_1(x) + p_1(x), \ldots, h_{j-1}(x) + p_{j-1}(x), h_j(x) + K_j, h_{j+1}(x) + q_{j+1}(x), \ldots, h_m(x) + q_m(x)\}$.

SESSION KEY AND SHARES RECOVERY IN SESSION j: For all $i \in \{1, \ldots, n\}$, U_i recovers K_j from the broadcast B_j by evaluating $h_j(x) + K_j$ at i and subtracting $h_j(i)$. Similarly, U_i recovers session key shares $\{p_1(i), \ldots, p_{j-1}(i), q_{j+1}(i), \ldots, q_m(i)\}$.
Self-healing is then possible because in session $j_1 < j$, user U_i recovers share $p_j(i)$, and $p_j(i) + q_j(i) = K_j$.

Attack. An adversary can recover a session key as follows: if the adversary has received B_{j-1}, B_j, and B_{j+1}, then he has $h_j(x) + q_j(x)$, $h_j(x) + K_j$, and $h_j(x) + p_j(x)$, respectively. But, $2(h_j(x) + K_j) - [(h_j(x) + q_j(x)) + (h_j(x) + p_j(x))] = K_j$, since $p_j(x) + q_j(x) = K_j$. ■

The attack does not apply to Constructions 3, 4 and 5, due to the use of unrelated polynomials in each broadcast. We will give more details in the full version of this paper.

4 Avoiding the Attack

If the structure of the broadcast is opportunely modified, it is possible to avoid the multiple-message attack described before. More precisely, let $B_j = \{h_1(x) + p_1(x), \ldots, h_{j-1}(x) + p_{j-1}(x), \mathbf{2 \cdot h_j(x) + K_j}, h_{j+1}(x) + q_{j+1}(x), \ldots, h_m(x) + q_m(x)\}$.
In this case it is not difficult to see that a straightforward application of the above attack does not work since $2h_j(x) + K_j - [(h_j(x) + q_j(x)) + (h_j(x) + p_j(x))] = 0$.

More precisely, we can show the following result:

Theorem 4.1 *An adversary, once received $B_1, \ldots, B_m$, does not learn any information about the key K_j, for $j = 1, \ldots, m$.*

Proof. To simplify the discussion we can assume, without loss of generality, that in Construction 1 the polynomials $h_j(x), p_j(x)$ and $q_j(x)$ are simple constants h_j, p_j and q_j, since we are studying just the self-healing property.

The information that can be recovered from $B_1, \ldots, B_m$ is given by $2 \cdot h_1 + K_1, \ldots, 2 \cdot h_m + K_m, h_1 + p_1, \ldots, h_{m-1} + p_{m-1}, h_2 + q_2, \ldots, h_m + q_m$.

It is pretty easy to see that the available values do not enable us to infer any information about any single key. Indeed, for K_1 and K_m, we can set up two systems with 3 equations in 4 variables, with infinite solutions.

$$\begin{cases} h_1 + p_1 = P_1 \\ 2 \cdot h_1 + K_1 = C_1 \\ p_1 + q_1 = K_1. \end{cases} \quad \text{and,} \quad \begin{cases} h_m + p_m = Q_m \\ 2 \cdot h_m + K_m = C_m \\ p_m + q_m = K_m, \end{cases}$$

Notice that, K_1 and K_m were already safe in the original scheme, since the proposed attack does not apply to those cases. About, $K_2, \ldots, K_{m-1}$, we can set up the following system:

$$\begin{cases} h_2 + p_2 = P_2 \\ \dots \\ h_{m-1} + p_{m-1} = P_{m-1} \\ 2 \cdot h_2 + K_2 = C_2 \\ \dots \\ 2 \cdot h_{m-1} + K_{m-1} = C_{m-1} \\ h_2 + q_2 = Q_2 \\ \dots \\ h_{m-1} + q_{m-1} = Q_m \\ p_2 + q_2 = K_2. \\ \dots \\ p_{m-1} + q_{m-1} = K_{m-1}. \end{cases}$$

The above system has $4 \cdot (m-2)$ equations and $4 \cdot (m-2)$ variables. However, the last $(m-2)$ equations are linear combinations of the others. Indeed, the system

$$\begin{cases} h_j + p_j = P_j \\ 2 \cdot h_j + K_j = C_j \\ h_j + q_j = Q_j \\ K_j - p_j - q_j = 0 \end{cases}$$

can be expressed in matrix form as

$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 1 \end{bmatrix} \times \begin{bmatrix} h_j \\ K_j \\ p_j \\ q_j \end{bmatrix} = \begin{bmatrix} P_j \\ C_j \\ Q_j \\ 0 \end{bmatrix},$$

and simple algebra shows that the above matrix has determinant equal to zero. Hence, for $j = 2, \dots, m-1$, we can write down $m-2$ systems of 4 equations in 4 variables, where, in each system, an equation is a linear combination of the others. Therefore, no information can be computed about key K_j, since each system has infinite solutions. ■

Actually, we can show that, for any fixed m-tuple of values for $K_1, \dots, K_m$, the complete system has one and only one solution. Indeed,

$$\begin{cases} h_1 + p_1 = P_1 \\ \dots \\ h_{m-1} + p_{m-1} = P_{m-1} \\ 2 \cdot h_1 + K_1 = C_1 \\ \dots \\ 2 \cdot h_m + K_m = C_m \\ h_2 + q_2 = Q_2 \\ \dots \\ h_m + q_m = Q_m \\ p_1 + q_1 = K_1. \\ p_m + q_m = K_m. \end{cases}$$

has solution given by

$$\begin{cases} p_1 = P_1 - \frac{C_1 - K_1}{2} \\ \dots \\ p_{m-1} = P_{m-1} - \frac{C_{m-1} - K_{m-1}}{2} \\ h_1 = \frac{C_1 - K_1}{2} \\ \dots \\ h_m = \frac{C_m - K_m}{2} \\ q_2 = Q_2 - \frac{C_2 - K_2}{2} \\ \dots \\ q_m = Q_m - \frac{C_m - K_m}{2} \\ q_1 = K_1 - [P_1 - \frac{C_1 - K_1}{2}]. \\ p_m = K_m - [Q_m - \frac{C_m - K_m}{2}]. \end{cases}$$

Thus, an adversary holding the sequence $B_1, \dots, B_m$, does not learn any information about the whole sequence $K_1, \dots, K_m$.

Remark 4.2 *Notice that the above property is stronger than what required by Definition 2.1. Indeed, Definition 2.1 requires no information on a single key but does not exclude the possibility of computing partial information about the whole sequence.*

Remark 4.3 *The modified scheme is still tight with respect to the lower bound on the size of the personal key of each user, given in [29]. It will be interesting to provide (if possible) self-healing schemes with shorter broadcast size.*

5 Conclusions and Open Problems

In this paper we have described an attack which enables an adversary to break a key distribution scheme given in [29] in a very simple way. Then, we have suggested a change in the broadcast message structure, in order to gain resistance to the described attack.

The self-healing approach is a new and suitable method to do key distribution. As pointed out by the authors who introduced such an idea in [29], many applications can benefit from efficient and secure schemes. Further research could be done in order to clearly identify the attacks that might be implemented in such a model, and to design efficient and provable secure schemes with respect to the specified adversarial model.

References

[1] J. Anzai, N. Matsuzaki, and T. Matsumoto, *A Quick Group Key Distribution Scheme with Entity Revocation*, Advances in Cryptology - Asiacrypt '99, Lecture Notes in Computer Science, Vol. 1716, pp. 333-347.

[2] S. Berkovits, *How to Broadcast a Secret*, Advances in Cryptology - Eurocrypt '91, Lecture Notes in Computer Science, vol. **547**, pp. 536–541, 1991.

[3] C. Blundo and A. Cresti, *Space Requirements for Broadcast Encryption*, Advances in Cryptology - Eurocrypt '94, Lecture Notes in Computer Science, vol. 950, pp. 287–298, 1995.

[4] C. Blundo, Luiz A. Frota Mattos, and D. R. Stinson, *Generalised Beimel-Chor Schemes for Broadcast Encryption and Interactive Key Distribution*, Theoretical Computer Science, vol. 200, pp. 313–334, 1998.

[5] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, *Issue in Multicast Security: A Taxonomy and Efficient Constructions*, Infocom '99, pp. 708–716, 1999.

[6] R. Canetti, T. Malkin, and K. Nissim, *Efficient Communication-Storage Tradeoffs for Multicast Encryption*, Advances in Cryptology - Eurocrypt '99, Lecture Notes in Computer Science, vol. 1592, pp. 459–474, 1999.

[7] B. Chor, A. Fiat, M. Naor and B. Pinkas, *Traitor Tracing*, IEEE Transactions on Information Theory, vol. 46, No. 3, pp. 893–910, May 2000.

[8] T. M. Cover and J. A. Thomas, **Elements of Information Theory**, John Wiley & Sons, 1991.

[9] P. D'Arco and D. R. Stinson, *Fault Tolerant and Distributed Broadcast Encryption*, to appear at the Cryptographers' Track RSA Conference 2003 (CT-RSA 2003), April 13-17, San Francisco, (USA), 2003.

[10] G. Di Crescenzo and O. Kornievskaia, *Efficient Multicast Encryption Schemes*, Security in Communication Network (SCN02), Lecture Notes in Computer Science, 2002.

[11] C. Dwork, J. Lotspiech, and M. Naor, *Digital Signets: Self-Enforcing Protection of Digital Information*, Proceedings of the 28-th Symposium on the Theory of Computation, pp. 489–498, 1996.

[12] A. Fiat and M. Naor, *Broadcast Encryption*, Proceedings of Crypto '93, Lecture Notes in Computer Science, vol. 773, pp. 480-491, 1994.

[13] A. Fiat and T. Tessa, *Dynamic Traitor Tracing*, Journal of Cryptology, Vol. 14, pp. 211–223, 2001.

[14] E. Gafni, J. Staddon, and Y. L. Yin, *Efficient Methods for Integrating Traceability and Broadcast Encryption*, Advances in Cryptology - Crypto '99, Lecture Notes in Computer Science, vol. 1666, p. 372–387, 1999.

[15] J. Garay, J. Staddon, and A. Wool, *Long-Lived Broadcast Encryption*, Advances in Cryptology - Crypto 2000, Lecture Notes in Computer Science, vol. 1880, pp. 333–352, 2000.

[16] D. Halevy and A. Shamir, *The LSD Broadcast Encryption Scheme*, Advances in Cryptology - Crypto '02, Lecture Notes in Computer Science, vol. 2442, pp. 47-60, 2002.

[17] A. Kiayias and M. Yung, *Traitor Tracing with Constant Transmission Rate*, Advances in Cryptology - Eurocrypt '02, Lecture Notes in Computer Science, vol. 2332, pp. 450-465, 2002.

[18] A. Kiayias and M. Yung, *Self Protecting Pirates and Black-Box Traitor Tracing*, Advances in Cryptology - Crypto '01, Lecture Notes in Computer Science, vol.2139, pp. 63-79, 2001.

[19] R. Kumar, S. Rajagopalan, and A. Sahai, *Coding Constructions for Blacklisting*

Problems without Computational Assumptions, Advances in Cryptology - Crypto '99, Lecture Notes in Computer Science, Vol. 1666, pp. 609–623, 1999.

[20] H. Kurnio, R. Safani-Naini, and H. Wang, *A Group Key Distribution Scheme with Decentralised User Join*, Security in Communication Network (SCN02), Lecture Notes in Computer Science, 2002.

[21] H. Kurnio, R. Safani-Naini, and H. Wang, *A Secure Re-keying Scheme with Key Recovery Property*, ACISP 2002, Lecture Notes in Computer Science, Vol. 2384, pp. 40–55, 2002.

[22] M. Luby and J. Staddon, *Combinatorial Bounds for Broadcast Encryption*, Advances in Cryptology - Eurocrypt '98, Lecture Notes in Computer Science, vol. 1403, pp. 512–526, 1998.

[23] D. Naor, M. Naor, and J. Lotspiech, *Revocation and Tracing Schemes for Stateless Receivers* Advances in Cryptology - Crypto '01, Lecture Notes in Computer Science, vol. 2139, pp. 41–62, 2001.

[24] M. Naor and B. Pinkas, *Efficient Trace and Revoke Schemes*, Financial Cryptography 2000, Lecture Notes in Computer Science, vol. 1962, pp. 1–21, 2000.

[25] A. Perrig, D. Song, and J. D. Tygar, *ELK, a new Protocol for Efficient Large-Group Key Distribution*, in IEEE Symposium on Security and Privacy (2000).

[26] B. Pfitzmann, *Trials of Traced Traitors*, Information Hiding, Lecture Notes in Computer Science, vol. 1174, pp. 49-64, 1996.

[27] R. Safavi-Naini and H. Wang, *New Constructions for Multicast Re-Keying Schemes Using Perfect Hash Families*, 7th ACM Conference on Computer and Communication Security, ACM Press, pp. 228–234, 2000.

[28] R. Safavi-Naini and Y. Wang, *Sequential Traitor Tracing*, Lecture Notes in Computer Science, vol. 1880, p. 316–332, 2000.

[29] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin and D. Dean, *Self-Healing Key Distribution with Revocation*, IEEE Symposium on Security and Privacy, May 12-15, 2002, Berkeley, California.

[30] J. N. Staddon, D.R. Stinson and R. Wei, *Combinatorial properties of frameproof and traceability codes*, IEEE Transactions on Information Theory vol. 47, pp. 1042-1049, 2001.

[31] D. R. Stinson, *On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption*, Designs, Codes and Cryptography, vol. 12, pp. 215–243, 1997.

[32] D. R. Stinson and T. van Trung, *Some New Results on Key Distribution Patterns and Broadcast Encryption*, Designs, Codes and Cryptography, vol. 15, pp. 261–279, 1998.

[33] D. R. Stinson and R. Wei, *Key preassigned traceability schemes for broadcast encryption*, Proceedings of SAC'98, Lecture Notes in Computer Science, vol. 1556, pp. 144-156, 1999.

[34] D. R. Stinson and R. Wei, *Combinatorial properties and constructions of traceability schemes and frameproof codes*, SIAM Journal on Discrete Mathematics, vol. 11, pp. 41–53, 1998.

[35] D. R. Stinson and R. Wei, *An Application of Ramp Schemes to Broadcast Encryption*, Information Processing Letters, Vol. 69, pp. 131–135, 1999.

[36] D. M. Wallner, E. J. Harder, and R. C. Agee, *Key Management for Multicast: Issues and Architectures*, Internet Draft (draft-wallner-key-arch-01.txt), ftp://ftp.ieft.org/internet-drafts/draft-wallner-key-arch-01.txt.

[37] C. Wong, and S. Lam, *Keystone: A Group Key Management Service*, in International Conference on Telecommunications, ICT 2000.