# On Secure Group Admission Control Using ICMetrics

Hasan Tahir*, Gareth Howells†, Huosheng Hu*, Dongbing Gu*, Klaus McDonald-Maier*

* School of Computer Science and Electronic Engineering, University of Essex, United Kingdom
htahir@essex.ac.uk, hhu@essex.ac.uk, dgu@essex.ac.uk, kdm@essex.ac.uk

† School of Engineering and Digital Arts, University of Kent, United Kingdom
W.G.J.Howells@kent.ac.uk

*Abstract* - **The security of a system cannot be certified unless there are formal methods of admission control. Many techniques and protocol have been proposed that try to provide security yet do not focus on the most important question about who has access to the system. When considering group communications it is more important to understand this problem as the security of the system is dependent upon having authorized entities in the group communicating securely. Admission control has previously been studied indistributed systems but repeatedly overlooked in security. In this paper we provide a polling centred admission control system based on ICMetrics. We choose the polling based system as it considers the opinion of current group members when giving access to members wishing to join the group. Our proposed protocol is based on the use of the secure ring signature along with the latest ICMetrics technology.**

***Keywords– ICMetrics; admission control; polling; ring signatures; group secure communications, group security.***

## I. INTRODUCTION

Secure group communications offer a unique environment that is composed of many clients communicating securely in a group. The complexity here is the availability of multiple points of attack and an overall environment where clients may join or leave a group at any moment. Since there are multiple clients involved thereforethe prevailing complexity at the architectural level requires the design and implementation of strict and robust security protocols [1].

Much research work has been done in designing security protocols that address the essential security goals of authentication, confidentiality, integrity, and non-repudiation. Most proposed protocols try to fulfill the above requirements by using modern cryptographic techniques [2]. Security protocols can be considered fairly robust and secure but they miss out on a major detail i.e. admission control. Admission control is an area of research that has been missed out in its entirety when considering security protocols [3]. Some may argue that the requirements of admission control are already being fulfilled by the post admission protocols. The important fact is that admission control activities should begin before an entity applies to become part of a group communication. Admission control in a group setting is important because without this element of security there is no way of insuring who is part of the group. In the absence of an admission control methods the group is at the mercy of malicious or dishonest participants. Group admissions is composed of but not limited to the following crucial activities:

- Define method of admission (permission, polling, access control list).
- New member verification.
- Verification of counterpart/group.
- Obtaining permission for admission from existing members.

To this end we present a description of what types of groups exist and what their individual characteristics are. Section III then discusses the techniques through which admission can be obtained. A description of the ICmetrics technology is preceded by a detailed description of the building blocks of the protocol. Section VII provides a detailed description of the proposed admission scheme using a step by step breakdown of how ring signatures are generated using ICMetrics. In the end the paper analyzes the proposed security scheme from an information security standpoint.

## II. TYPES OF GROUPS

Secure group communications require first the formation of a group. The type of group dictates the level of security dispensed to the group. Some clients may require a group that allows them to communicate openly without security provisions while others may require a very secure group that provides the highest level of security. Once a group is established it is not possible to lower the security level of a group by converting it to a less restrictive group. Below we discuss the types of groups and their features.

### A. Public Groups/ Open Groups

Public groups are those groups that are open to the public. Mostly these groups do not have a formal admission control procedure hence any client can connect to the group and communicate. The content of the group, members of the group are all visible to the public. These groups can be used for communicating insecurely within a group. The advantage of these groups is that they allow collaborations among clients without the security overhead. These groups are established for those clients that wish to collaborate insecurely much like a public chat.

### B. Restricted Groups

Restricted group are more secure when compared to public groups. The contents and members of the restricted group are only visible to the registered/ admitted members of the group. This implies that a formal group admission policy is put into place and the clients are given admission following group members or group controller's permission. Hence mandatory access controls are defined for obtaining access to a group. Once a client has left the group he will not have access to future communications in the group. These groups can be resource (time, memory) demanding as there are multiple policies like admissions and departures, keying, rekeying and finally key structuring. Forecasting the resource demand can be difficult since the size of the group has primary influence on the amount of resources required.

### C. Private Groups

Private groups provide the highest level of security because these groups are purely invitation based. Other possible variants also include a friend to friend architecture where a client can only communicate with the persons it invites into the group. There may be many clients in the group but a client can communicate with only those who it has invited. This feature strengthens the security provisions within clusters inside a group. A common concern for clients in a group is that they are always at the risk of being exposed due to clients that have gone rogue in the group. Defining a circle of friends provides better protection from rogue clients. This technique does not entirely eliminate rogue clients from the group. Examples of these groups are commonly seen in a social networking environment.

## III. ADMISSION MECHANISMS

Before formally presenting the admission control we present the basic elements of the protocol.

Obtaining group membership requires identification and authentication procedures so that impersonation can be prevented. Admission to a group can be obtained by multiple methods like polling upon request, invitation and access control list. The choice of technique is based on the type of group and how the members wish to get registered.

### A. Polling Upon Request

Polling based admission control procedures allow a prospective member to be admitted into the group if the existing members vote in its favour [4] [5]. A polling request is executed by taking a random subset of clients from the entire group population. The selected clients will poll in favour or against the admission of the new client. An important measure to be established while voting is the quorum. The quorum defines the minimum number of favourable votes that will allow an expecting client entry into the system.

The polling request is an efficient mechanism as obtaining permission from all clients in large sized groups can be very time consuming. The selected candidates will form a small subset that will be representing the entire population of the group.

### B. Access Control List

An access control list (ACL) provides a simple yet strict method of control that is frequently seen in networks, file systems and database administration [6]. Using an ACL the members of a group name those clients that will be allowed admission into the group. In secure group communications only a single inbound access control list is sufficient. Unlike many network protocols that use an inbound and an outbound traffic access control list. Once a client tries to gain access to the group it is the group controller's responsibility to process the ACL top-down to determine if the incoming request for admission should be entertained.

### C. Timed Invitations

Another method of controlling admissions is through the use of a timed invitation. This technique is employed by private groups and is considered secure because only present group clients can invite other members into the group. After they accept the invitation the new members undergo a formal identification and authentication process. Timed invitations are initiated when a group client sends an invitation to a member who should "consider" joining the group in a secure conversation. Each invitation is time based and has a definite time within which it can be accepted. Just before sending the invitation the client requests the group controller to add the expected incoming member into the ACL along with a future time stamp after which the group controller will remove the clients name from the ACL. Thus prohibiting access to the group until another invitation is not sent.

Having a time based invitation has the added advantage of preventing an open ended access mechanism where an invitation can be used fraudulently.

## IV. KEYING PERSPECTIVES

Keying in group communications is a complex task owing to the existence of large number of group members. Depending upon the architecture one must choose between controller based keying or the collaborative client based

keying mechanism. Although many protocols exist for both of the above techniques but they do not study the problem of admission control. When adopting a polling based system we note that selected existing clients have a choice whether to let a client join the group or not. The group admission procedure should not allow an intending client to find out who voted in his favour and who voted against him. The sole purpose of the polling procedure is to allow or deny admission regardless of who voted in favour and who voted against an entities admission. Hence group admission should protect the identity and opinion of the voters.

A technique that promises such functionality is the Ring signature. Originally proposed by Rivest et al [7], it allows a group member to leak a secret from a group by using a verifiable signature. Their scenario is based on the fact that one may wish to leak a secret that is signed but the signature should not link the secret to the exact entity. Seemingly ring signatures have no association with group admissions. Upon further investigation we discover the need for a polling method that allows group members to poll for an intending member without their opinion or identity being exposed.

## V. INTEGRATED CIRCUIT METRICS (ICMETRICS)

Ever since security has been designed it has been based on the use of a key which is essential in decrypting of text. Just like modern cryptography ancient cryptographic techniques like the Freemason cipher, rail fence cipher and many others were also based on the use of keys [7]. These keys if leaked can cause system infiltration and this is why every effort is made to keep the keys as confidential as possible. Although these keys are crucial for providing security, these keys have no relationship with their owner. A person is for instance recognized by his fingerprint but a key pair has no relation with its system. ICMetrics advocates the generation of security data that is based on characteristics of a device. Every device has a unique hardware and software environment. Consider two devices having the same model and manufacturer. Even though these devices physically look the same they have vast differences in their internal environments. Some of the unique features that can be used for generating an ICMetric basis number are serial numbers, addresses, program counter data, data in the RAM, data in the cache and other similar features that can be used to distinguish one device from the other. ICMetrics supports this notion and encourages the use of unique characteristics to generate an ID for every device [9]. ICMetrics is a vast paradigm shift as compared to the conventional information security. ICMetrics can be considered more secure because of the following points.

- ICMetrics is both hardware and software based.
- The ICMetric basis number is generated from unique characteristics found on the system.
- The ICMetric basis number does not need to be stored on the system as it can be generated in real time.
- Any attempt to physically alter/ vandalize the system will cause the ICMetric module to either malfunction or give erroneous results.
- The ICMetric basis number is never communicated to the outer world to further protect the system from unwanted exposure.

The ICMetric ID is a number that is generated by combining unique device attributes. There are two techniques that are used for generating this number. The number size and stability are two important factors that are influenced by the choice of technique. The first technique is called the feature addition combination technique and is based on the addition of individual features of a device. This technique generates a number that is small in size yet more stable. On the other hand the feature concatenation- combination technique generates the ICMetric number through the concatenation operation. The generated number has the advantage of being long lengthed yet less stable. To generate the number both techniques undergo feature extraction along with the application of normalization maps [9].

Based on the advantages that ICMetrics has to offer researchers have proposed and have performed in depth studies on the many environments where ICMetrics can be implemented. Some of the recent advancements have been seen in electronic wheelchair security provision, cloud computing, wireless sensor networks, embedded systems, intrusion detection systems.

## VI. BUILDING BLOCKS

Besides ICMetrics the admission control protocol is composed of some foundation blocks without which the security module cannot be considered secure. The essential modules are trapdoor functions, hashing. Both techniques are discussed below.

### *A. Hash Functions*

Hash functions are frequently used in cryptography to convert an arbitrary length text input to a standard fixed length. The use of a hash function thus converts a length of text into seemingly random text outputs. This means that no matter how big the original text is the hash algorithm produces a single output of a relatively smaller length of text [10] [11]. Hashing has been used for many purposes like to verify if a file/ text has been modified. Another prominent use of hashing is to conceal data in situations where the data cannot be transmitted in its original form. The reason for preferring hash functions over encryption schemes is that encrypted text can be decrypted whereas hash functions are not reversible.

Hashes possess unique properties owing to which they are considered secure. A prominent property of hash functions is that they are not reversible, secondly it should be infeasible to produce the original text if the hash is provided. A single text if passed through the hash algorithm multiple times (not repeatedly) should produce the same output hash. Although other secure properties also exist we have suggested the use of hash functions owing to the above properties. In our proposed admission control protocol we have passed the ICMetric number through a hash to prevent exposure of the ICMetric

number. An added benefit that is also obtained is that the hashed ICMetric number cannot be used to identify the owner. This property preserves the identity and the opinion of clients regarding the admission of an intending member.

### B. Trap Door Functions

A trapdoor function is a procedure that is simple to compute in one direction yet is difficult to compute it back (inverse) if only the result is provided. To find the inverse of a trapdoor function it is important that some critical information be given relating to the solution so that it can be properly reversed. Hence the trapdoor function is hard to inverse without the special information but easy to inverse if the special information is provided. Rivest et al in their work[6] have suggested the use of an extended trapdoor permutation. The basic trapdoor is RSA [13] based and allows a member having RSA public key $P_i = (n_i, e_i)$ to specify a trapdoor permutation of $f_i$ such that:

$$f_i(x) = x^{e_i} (\mathrm{mod} n_i) \quad (1)$$

Consider $g$ to be an extended trapdoor permutation over $\{0,1\}^{\mathrm{b}}$. For any input m defines non negative integers $q$ and $r$ so that $m = qn + r$ The extended trapdoor permutation is dependent on the basic trapdoor permutation $f$ over $\mathbb{Z}_{\mathrm{n}}$. Hence to solve the trapdoor permutation $g$ it is important that the trapdoor permutation $f$ be solved first.

$$g(m) = \begin{cases} qn + f(r), & (q+1)n \leq 2^b \\ m, & \text{Otherwise} \end{cases} \quad (2)$$

## VII. PROPOSED SCHEME

### A. Admission Request

The admission procedure is initiated by an intending member$\mathrm{M}_x$. This member will request the group controller (GC) for permission to join the group. The admission request will be supported by a certificate of the intending member. This certificate will allow the members to verify the entity.

### B. Threshold Determination

In the initial phase the group controller will determine the number of clients needed for voting. These clients should be selected randomly and the quantity called the threshold number$t$ should be optimized to reduce excessive communication overhead. In large sized groups this can be a problem because having a large sized population sample for polling can be both time and network intensive [12].

Once this has been determined it is the responsibility of the controller to determine the quorum which will give the number of favourable votes required. The quorum should not be taken as a percentage. If this is the case then in a large sample population the percentage is not an accurate indicator of acceptance. To highlight this consider a sample population of 200 voters. If we define the number of acceptable votes to be 80% then out of 200 the number of opposition votes is 40. Out of the 200 voters many clients may not vote or they may not vote in a timely manner. Hence it is evident that 40 negative votes out of 200 is not a negligible number. Instead we recommend the use of an absolute number that is representative of the population's opinion. Hence out of 200 we recommend negative votes to be no more than 15. Although this may seem to be absurdly high but we must consider that the security of the entire group is at stake. While determining the threshold it must be clearly pointed out what will happen if the group population is too low to effectively create a polling threshold.

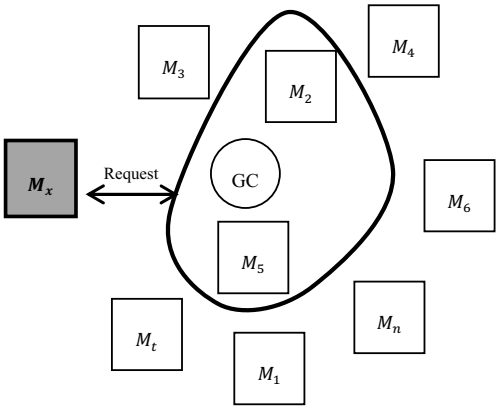


Fig. 1. A prospective member $M_x$ being voted by randomly selected existing group members

### C. Polling

Once the group controller has determined the polling parameters it will send a polling request to the randomly selected members. The group members will first verify the correctness of the certificate. The voters will then cast either a positive or negative opinion and will forward this vote to the group controller. The individual members cannot communicate directly with an intending member.

### D. Ring Signature Generation

The group controller will gather all the positive votes and will determine if the required quorum has been met. If the quorum has been met then the group controller proceeds forward with a ring signature generation. This ring signature will be generated by using the positive voters ICMetric number hashes. In our proposed protocol we have adapted the ring signature proposed by Rivest et al for our group admission control problem. Originally the use of the scheme for admission control has not been explored and secondly we propose the use of ICMetrics to further enhance the security of the system.

If a group controller determines that the intending member should be given permission to enter the group then it will not send a message to the applicant. The problem with such schemes is that the message can be adapted resulting in an attack on the admission control protocol. Given the ICMetric number ($IC_i$) hashes of those members that voted in favour of the admission. Each public key $P_i$ specifies a trapdoor function with the properties discussed in section VI. The secret key $S_i$ holds information that can be used to compute $g_i^{-1}$. The Ring signature generation will take place as follows.

*1) Symmetric key determination*

The group controller first generates a symmetric key by collecting the hashes of ICMetric numbers of those members that voted in favour of the intending member. After collecting the hashes a product is obtained of the collected hashes.

$$k = \prod_{i=1}^{t} h(IC_i) \quad (3)$$

Where $i$ has a non-sequential value from 1 to $t$.

*2) Glue value generation*

The group controller will generate a random glue value $v$ from $\{0,1\}^b$.

*3) Pick random values of $x_i$*

The group controller on its own generates a random value $x$ from $\{0,1\}^b$ on behalf of the group members that gave a positive vote. The selected value does not have to be communicated to the respective group members. The generated value is then used to solve the following equation for every positive voter.

$$y_i = g_i(x_i) \text{ where} 1 \leq i \leq t \quad (4)$$

*4) Solve the ring equation*

The group controller solves the following ring equation for all the above generated values of $y$.

$$C_{k,v}(y_1, y_2, \cdots, y_i) = v, \text{ where} 1 \leq i \leq t \quad (5)$$

*5) Trapdoor function inversion*

The group controller uses the trapdoor function to invert the values of $g_i$ and $y_i$ to obtain $x_i$.

$$x_i = g_i^{-1}(y_i), \text{ where} 1 \leq i \leq t \quad (6)$$

*6) Ring signature output*

The signature on the positive voters ICMetric number hash is defined to be the $(2t + 1)$ tuple:

$$(P_1, P_2, \cdots, P_t; v; x_1, x_{2,\ldots}, x_t) \quad (7)$$

*E. Ring Signature Verification*

An intending member may wish to verify the correctness of a signature. To do this Rivest et al propose the following steps.

*1) Apply the trapdoor permutations*

The verifier computes the following equation for

$$y_i = g_i(x_i), \text{ where } 1 \leq i \leq t \quad (8)$$

*2) Symmetric key computation*

The verifier computes the product of the ICMetric hashes to compute the symmetric key.

$$k = \prod h(IC) \quad (9)$$

*3) Ring equation verification*

The verifier checks that the computed $y_i$ satisfy the base equation

$$C_{k,v}(y_1, y_2, \cdots, y_i) = v, \text{where} 1 \leq i \leq t \quad (10)$$

If the equation is satisfied then the verifier accepts the signature to be valid.

## VIII. Analysis And Discussion

Admission control procedures form an important part of the secure communications. In group communications this is even more important as there is always room for welcoming new members into the group. Our proposed protocol is based on the latest ICMetrics technology which provides feature based key generation thus giving resilience against a wide range of attacks. The admission procedure is polling based thus preventing a single entity from making admissions on behalf of a group of clients. The polling procedure consists of a defined threshold and a quorum which is essential part of voting process.

Once voting is complete it is the task of the group controller to inform the intending member that he has been granted permission to join the group. Most admission control protocols focus on the polling phase and the details regarding the identity of voters and their opinion is largely overlooked. Our proposed scheme informs an intending voter about the positive feedback without disclosing the identity and opinions of the voters. The admission scheme is based on the use of ring signatures that allow a person to leak a secret by signing but not linking the signature to his identity. In our particular scenario the document which needs to be communicated is the polling outcome and the ring signature is used to sign the document without using any key that is associated with the group. The ring signature is generated using an extended trapdoor function which increases the security stability of the scheme. The first step of the ring signature generation is the generation of a symmetric key. Our proposed scheme uses a product of ICMetrics hashes to generate the symmetric key. This technique firstly prevents the ICMetric number from being exposed and secondly the product further produces diffusion to eliminate any possibility of a pattern being

exposed. The product has been taken so that the scheme can be used in very small groups. If the product was not used then the hashed ICMetric numbers would form the symmetric key which can be considered insecure.

## CONCLUSION

Security in a group cannot be certified until there is a formal admission control procedure. Traditionally most research has been geared towards post admission activities and hence admission control has been largely overlooked. Admission control defines a set of procedures that come into play when a client needs to be admitted into a secure group communication. A client can be given access to a group by voting, use of access control list or by invitation. The choice of technique depends upon the level of security and the membership policy that governs the group. In this paper we discussed three types of groups that can be formed for group communications. The most common admission control is based on the use of polling. This allows a group of clients to vote for a particular intending member. The advantage that polling has over other techniques is that it allows a collection of clients to vote on behalf of the entire group. This results in a reduction in the communication overhead and at the same time prevents a single entity from making decisions on behalf of many existing members.

Our proposed admission scheme allows a group controller to generate a right of admission by using ICMetrics and ring signatures. The role of ICMetrics is that it prevents fraudulent entities from casting votes and hence influencing the polling procedure. The proposed scheme uses a combination of hashing, RSA based trapdoor permutation and extended trapdoor permutations to generate a signature that can be used to sign a right of admission without exposing the identity and opinion of the clients involved in polling for admission. This scheme can be considered secure owing to the use of trapdoors and hashing. To provide security to the intending member the generated resulting ring equation is verifiable.

## ACKNOWLEDGEMENT

This research is financially supported by the COALAS Project, http://www.coalas-project.eu/, that has been selected in the context of the INTERREG IVA France (Channel) England European cross-border co-operation programme, which is co-financed by the ERDF.

## REFERENCES

[1] T. Hardjono, L. R. Dondeti, ”Information Security Series – Multicast and Group Security”. Artech House, Boston, 2003.

[2] M. T. Thai, “Group Testing Theory in Network Security An Advanced Solution”. Springer, New York, 2012.

[3] R. Sandhu, "Access Control: The Neglected Frontier, "Lecture Notes in Computer Science, Vol. 1172, no. pp. 219-227, 1996.

[4] J. Groth, “Evaluating Security of Voting Schemes in the Universal Composability Framework”. Lecture Notes in Computer Science Volume 3089, 46-60.

[5] Y. Kim, D. Mazzocchi, G. Tsudik, I. Superiore, M. Boella. “Admission Control in Peer Groups”. IEEE International Symposium on Network Computing and Applications,131-139.

[6] S. Malik, “Network Security Principles and Practices”. Cisco Press, Indianapolis, 2004.

[7] R. L. Rivest, A. Shamir, Y. Tauman, “How to leak a secret: Theory and applications of ring signatures”. Essays in Theoretical Computer Science, 3895. 164-186.

[8] D. Sutherland, M. E. Koltko-Rivera, “Cracking Codes and Cryptograms For Dummies”. Wiley Publishing, Hoboken, 2010.

[9] R. Tahir, K. McDonald-Maier, “Improving Resilience against Node Capture Attacks in Wireless Sensor Networks using ICMetrics” in IEEE Conference on Emerging Security Technologies, Portugal, Spain, 2012.

[10] R. Tahir, K. McDonald-Maier, “An ICMetrics Based Lightweight Security Architecture Using Lattice Signcryption” in Third International Conference on Emerging Security Technologies (EST). Cambridge, UK, 2013.

[11] I. Mironov, “Hash functions: Theory, attacks, and application Microsoft Research”, 2005.

[12] NIST, Federal Information Processing Standards Publication 180-3, Secure Hash Standards (SHS), October 2008.

[13] V. Shoup, “Practical Threshold Signatures” in Proceedings of the 19th international conference on Theory and application of cryptographic techniques, Springer Verlag.

[14] Rivest R.L., Shamir, A., A. L. Adleman. “Method for Obtaining Digital Signatures and Public-key Cryptosystems”. Communications of the ACM. 21(2). 120-126.