International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:11, No:6, 2017

BTG-BIBA: A Flexibility-Enhanced Biba Model Using BTG Strategies for Operating System

Gang Liu, Can Wang, Runnan Zhang, Quan Wang, Huimin Song, Shaomin Ji

***Abstract*—**Biba model can protect information integrity but might deny various non-malicious access requests of the subjects, thereby decreasing the availability in the system. Therefore, a mechanism that allows exceptional access control is needed. Break the Glass (BTG) strategies refer an efficient means for extending the access rights of users in exceptional cases. These strategies help to prevent a system from stagnation. An approach is presented in this work for integrating Break the Glass strategies into the Biba model. This research proposes a model, BTG-Biba, which provides both an original Biba model used in normal situations and a mechanism used in emergency situations. The proposed model is context aware, can implement a fine-grained type of access control and primarily solves cross-domain access problems. Finally, the flexibility and availability improvement with the use of the proposed model is illustrated.

***Keywords*—**Biba model, break the glass, context, cross-domain, fine-grained.

I. Introduction

WITH the continuous development of modern information technology, information security problems have been increasingly attracting attention. Information security mainly rests on confidentiality, integrity and availability. To ensure the safety of information, a system must provide effective access control [1].

Researchers have proposed a variety of access control models for protecting different aspects of information security, such as Bell-LaPadula (BLP) [2] for confidentiality, Biba [3] and Clark Wilson [4] for integrity and Role-based Access Control (RBAC) [5] for security and integrity [6]. Information integrity is typically defined in terms of preventing improper or unauthorized change and aims to maintain data consistency [7]. There are several research works on integrity protection such as [8], which proposes a new model, Integrity-OrBAC, to preserve critical infrastructure integrity. Reference [9] provides a review of the prevalent data integrity models, evaluation mechanisms and integrity centric implementations.

The Biba model is the earliest multi-level security integrity model with the MAC (mandatory access control) [10] framework. Mainstream operating-system vendors did not adopt the Access-Control Frameworks until the early 2000s with the MAC Framework on FreeBSD [11] and shortly after, Linux Security Modules (LSM) [12]. The MAC Framework appeared in 2003 and FreeBSD 8.0 in 2009 included the framework as a production feature, compiled into the default kernel [13]. The system is classified into several integrity levels. Each subject and object is assigned an integrity level. Biba proposed five policies and strictly formalized the definitions of the policies. One of the policies is the mathematical dual of the BLP model [2] called the strict integrity policy (SIP) [3]. This policy is very strict, so it is difficult for the SIP to meet system flexibility needs; it has not been widely implemented. In order to solve the model flexibility problem, various improved models have been proposed. To a certain extent, dynamic enforcement of the strict integrity policy (DESIP) proposed in [14] solves the problem that some non-malicious access requirements may be unable to obtain adequate access permission. The concepts of check domain and subject with privilege are advanced in [15]; a method is introduced to dynamically change the security label in the check domain to solve the contradiction of BLP and Biba. However, this check is time-consuming and is not necessarily guaranteed in real-time. An improved SIP with dynamic characteristics is presented in [16], which can increase software compatibility while keeping the integrity and SIP intact. Reference [17] proposes a model that enhances the data integrity. The proposed model is based on the Biba integrity model but uses more elaborate integrity measurements. An improved model based on the low-water-mark policy is proposed in [18], which reduces the integrity level decline rate, prolongs the system life cycle and enhances the system availability.

For traditional access control models, there is typically the assumption that access permissions are known in advance and that rules have been set up correctly. However, in real situations, errors are made and unanticipated or emergency situations may occur [19], [20]. The improved Biba [3] models above, however, are not well behaved in fine-grained control and flexibility control. Motivated by disaster management use cases, break-glass strategies were introduced as one approach for resolving these problems [21].

There are many existing problems in the Biba model, such as integrity level assignments, the lack of fine-grained control and context-sensitivity. Considering the defects of Biba, the BTG-Biba model is proposed in this work that integrates Break the Glass (BTG) strategies [22] into the Biba model. In this paper, through the principle of BTG, such as governance, accessibility, awareness and accountability, BTG-Biba can maintain the regular access operation which are allowed in Biba and open the BTG mode in an emergency situation to solve the irregular access problem by detecting the system state variable. All access operations under emergency mode must obey the rule that only a single subject can have a request to access a single object. By monitor of the audit, all the

Can Wang is with the Department School of Computer Science and Technology, XIDIAN University, No. 2 Taibai South Road, Xi'an, China, 710071 (e-mail: gliu_xd@163.com).

Gang Liu, Runnan Zhang, Quan Wang, Huimin Song and Shaomin Ji are with XIDIAN University.

irregular accesses could be allowed to execute then BTG-Biba enhance the flexibility and usability of the system.

This paper is organized as follows: Section II analyzes the existing problems in the Biba model. The research foundation including cross-domain access problems and the BTG strategies are illustrated in Section III. In Section IV, the proposed model is introduced and the concept of context and fine-grained control are described. An available analysis is presented to illustrate the advantage of BTG-Biba in Section V. Finally, in Section VI, the studys conclusions are presented, and future work is discussed.

II. Primitive Biba Model Analysis

The Biba model does not have a strict standard to measure integrity level, cannot provide fine-grained control and does not support context. Furthermore, the original Biba model is static and does not allow cross-domain access; various non-malicious subject access requests are also denied. The existing problems in Biba model are analyzed in detail in the following section.

A. Integrity Level Assignments

An entire system must use consistent classification criteria, meaning that for the same system, integrity levels are certain. However, different systems have different classification techniques. The individual integrity level assignment is based on the trustworthiness of the individuals, but human behavior cannot be so clearly divided. So, a system cannot assign a precise integrity level to users with this model. The Biba model indicates that the subject integrity level assignment is determined by the permitted integrity level range of the associated user [3] so it is difficult to classify the integrity level of the subject.

In general, there is no objective criterion to assign the integrity level to all of the subjects and objects in an initial system. Meanwhile, in mandatory access control, once the subject and object are assigned an integrity level, the level cannot be changed through the entire life cycle. Even if the assigned level is incorrect, it cannot be altered; this characteristic may affect future access.

B. Lack of Fine-Grained Control

The Biba model is a security integrity model with multilevel security policy. The same integrity level may consist of a number of subjects and objects. All of the policies of the original Biba model are designed for integrity level. For example, in SIP, a subject may observe an object only if the integrity level of the subject is less than or equal to the integrity level of the object. Using the integrity level as the operand, the fine-grained control appears insufficient.

C. Cross-Domain Problem

The set of integrity levels is defined by the product of the set of integrity classes (C) and the powerset of the integrity compartments (K). Integrity level is a two-tuples (C, K). Integrity classes are ordered and may be defined as CRUCIAL (CR), VERY IMPORTANT (VI), IMPORTANT (I), partially ordered $I \leqslant VI \leqslant CR$. The set of integrity compartments are aimed to partition the sets of subjects and objects on the basis of functional area [3]. "The power set of integrity compartments" phrase is regarded as the word "domain" without distinction is this study. That is to say, the element in K can form a lattice.For example, a given set $\{CHN, JAP, KOR\}$ forming a lattice under the operation $\subseteq$ is shown in Fig. 1.

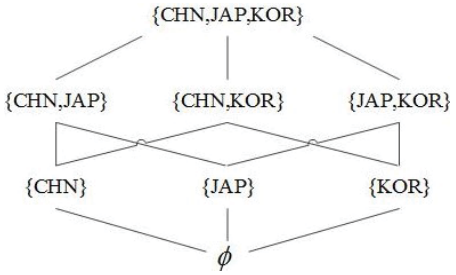

Fig. 1 Lattice generated by {CHN, JAP, KOR}. The lines represent the ordering relation induced by $\subseteq$

The integrity level relations are defined as follows: the integrity level (C, K) dominates the integrity level (C', K') if and only if $C' \leqslant C$ and $K' \leqslant K$ [2]. As can be seen from the definition, the integrity levels are ordered and can be compared; however, the integrity domains are a powerset and are not always in inclusion relation. Therefore, the integrity levels are not always ordered in every situation. For example, a subject with (C_S, K_S) clearance requests access to an object with (C_O, K_O) clearance. C_S equals CRUCIAL, K_S is $\{CHN, JAP\}$, C_O is CRUCIAL and K_O is equal to $\{CHN, KOR\}$. Although C_S and C_O can be compared, $\{CHN, JAP\} \nsubseteq \{CHN, KOR\}$. Therefore, the integrity level cannot be compared and access is denied. Indeed, categories are based on the "need to know" principle [2]. The integrity classes and integrity domain assignments are based on trustworthiness. The lack of an accurate classification criterion may cause difficulties later, and cross-domain access may be necessary; however, the system may not be able to properly address this problem.

D. Lack of Context

Once the integrity level is determined in the original Biba model, the system will run with the chosen policy. The system does not provide external environment change detection. However, there are various special requirements under emergency situations, so it is necessary to introduce context control into the system.

In conclusion, there are many existing problems in the original Biba model, such as integrity level assignments, the lack of fine-grained control, the cross domain problem and context-sensitivity. Biba model can be used to protect the integrity of systems, but it cannot reflect the diversified behaviour of subjects since the integrity level of subject and object are static without considering for the complicated action of subject, hence the compatibility of system might

be decreased. By the accessibility principle of the BTG, it can detect the context at present and decide whether the glass should be broken. If the glass is broken, the whole system will get into the emergency mode. BTG can ensure the irregular access to be allowed by controlling the fine-grained of the operation thus enhanced the flexibility and usability of the system. Thus, the following sections will discuss the BTG-Biba model in detail.

III. Research Foundations

A. Formal Definition of Biba Model with Domain

Biba is often referred to as the Bell-LaPadula upside down model. In BLP [2], information cannot flow towards levels of lower confidentiality because this would cause information leakage. Conversely, in Biba, information cannot flow towards levels of higher integrity or the "impure" data from the lower-integrity levels may contaminate the "pure" data held in the higher levels. This may be formulated in terms of the "No Read Down" and "No Write Up" properties that are the exact duplicates of the corresponding properties in BLP [23]. The model is based on the reliability that an entity with high integrity level is more reliable than the lower ranked entity.

Referring to [3], the elements in the Biba model within a domain are defined as follows:

- S: set of subjects.
- O: set of objects.
- U: set of the legitimate system user u; element u is the owner of the subject, and u(s) represents the user who owns subject s.
- I: set of integrity level identification.
- il: $S \cup O \rightarrow I$, a function returning the integrity level of each subject and object that makes the lattice under the relation leq available.
- $\leqslant$ (leq): a relation defining a partial ordering "less than or equal" on the set of integrity levels I. If the integrity level x is not greater than y, then mark $x \leqslant y$.
- $\underline{o}$: relation (subset of $S \times O$) defining the capability of subject, $s \in S$, to observe an object, $o \in O : S \ \underline{o} \ O$.
- $\underline{m}$: relation (subset of $S \times O$) defining the capability of subject, $s \in S$, to modify an object, $o \in O : S \ \underline{m} \ O$.
- $\underline{i}$: relation (subset of $S \times S$) defining the capability of subject, $s_1 \in S$, to invoke another subject, $s_2 \in S$: $s_1 \ \underline{i} \ s_2$.
- A: a set of access operations A=$\{\underline{o}$, $\underline{m}$, $\underline{i}\}$.

The formulation definition of the policies in the Biba model is given as follows:

- The Strict Integrity Policy:
  $\forall s \in S, o \in O \quad s \ \underline{m} \ o \ \Rightarrow il(o) \ \ leq \ \ il(s)$
  $\forall s \in S, o \in O \quad s \ \underline{o} \ o \ \Rightarrow il(s) \ \ leq \ \ il(o)$
  $\forall s_1, s_2 \in S \quad s_1 \ \underline{i} \ s_2 \ \Rightarrow il(s_2) \ \ leq \ \ il(s_1)$
- The RING Policy:
  $\forall s \in S, o \in O \quad s \ \underline{m} \ o \ \Rightarrow il(o) \ \ leq \ \ il(s)$
  $\forall s_1, s_2 \in S \quad s_1 \ \underline{i} \ s_2 \ \Rightarrow il(s_2) \ \ leq \ \ il(s_1)$
- The Low-Water-Mark Policy:
  $\forall s \in S, o \in O \quad s \ \underline{m} \ o \ \Rightarrow il(o) \ \ leq \ \ il(s)$
  $\forall s \in S, o \in O \quad s \ \underline{o} \ o \ \Rightarrow il'(s) = min\{il(o), il(s)\}$
  $\forall s_1, s_2 \in S \quad s_1 \ \underline{i} \ s_2 \ \Rightarrow il(s_2) \ \ leq \ \ il(s_1)$

The definition of the integrity levels will be discussed in detail. As mentioned above, the set of integrity levels is defined by the product of the set of integrity classes and integrity domains, which satisfies the lattice definition after being mathematical analysis. Thus, the sets of domains form a lattice under the operation $\subseteq$ (subset of). However, the lattice problem will occur in a domain when comparing the integrity levels of the subject and the object. In an actual system, domain problems may occur in the following cases:

- the initial domain configured by a system is not accurately completed.
- the problem may occur that the subject cannot access the object when they are in the same integrity classification but different integrity domains because of the limitations of the mathematical model lattice.
- non-malicious access requests of subjects may be denied in an emergency.

In the system, these three types of situations are called cross-domain access problems. Indeed, researchers of the original Biba model and newly proposed models, do not treat this problem from the cross-domain angle. These domains are typically expected to follow the "need to know" principle according to BLP [2]. So, research of the Biba model is only based on the level of integrity and the two-tuples (C, K); however, no consideration is given to possible cross-domain problems.

After analyzing the Biba model, it is necessary to discuss the cross-domain access problem. The cross-domain itself is a violation of the policy in the Biba model, but it can enhance the system flexibility. More details regarding cross-domain problems, such as when a subject may access objects and violate the policy in the Biba model and how to do it, are illustrated in Section IV.

B. Break the Glass Strategies Analysis

BTG are introduced as one approach to resolve problems in disaster management [22]. The name originates from breaking the glass to trigger a fire alarm. The mechanism is only effective in dealing with emergency situations, not interfering in other activities during normal operations. The generic idea of BTG is to empower users to decide if a denied access should be overridden. BTG strategies can provide overwrite of the access control decision but may bring risks to a system in some cases. To reduce risk, BTG supports system monitoring and audits. This gives four fundamental principles for BTG [24] as governance, accessibility, awareness and accountability.

The following are two specific ways to achieve BTG [21], [25]:

- Emergency account

In general, the system is divided into two modes. One is the normal mode of the original model; the other node is the BTG mode in the emergency situation. Emergency accounts are created in advance to allow careful thought to be given to access control policies and audit trails. When an emergency occurs, the emergency account logs in and addresses all of the access problems.

BTG strategies provide two boolean variables, which are the System BTG mode boolean variable (Sys_Btg) and the User BTG mode boolean variable (User_Btg). Sys_Btg is used to decide whether the entire system could turn on BTG mode. User_Btg is used to decide whether the user could turn on BTG mode and access an object that violated a policy in the primitive Biba model. When both of the two boolean variables are set to TRUE, the user should grant special access permission to his subject. When using this permission to access an object for the first time, the subject should report to its owner. The user returns a confirmation to his subject when permitting this access or a rejection when the access is not granted. When obtaining confirmation from its user, the subject could access the object without prompting the system. Until the BTG mode finished, this operation will only be monitored.

- Emergency level

The regular situation applys the regular policy without considering the BTG strategies while the emergency situation applys a hierarchy of these policies from the domain requirement. Finally, a special policy is defined to describe the subjects allowed to activate and de-activate emergency policies during normal runtime.

Both of the above methods can realize BTG strategies. To easily combine the Biba and the BTG models, the first method is used in this study.

BTG strategies can increase the access control granularity and introduce context awareness to the system. Emergency accounts only have permission assigned to a single individual, and the subject must request this exception access. Due to the small scale of the emergency situation, BTG strategies cannot assign special permission to most system users, so system security can still be guaranteed to some extent. Furthermore, in regard to context, the system is divided into the regular and emergency situations. For security models, BTG provides extra support to address complicated matters with context.

This section detailed the research foundation including cross-domain access problems and BTG strategies. To solve the problems mentioned above, this research proposes a new solution model called the BTG-Biba model.

IV. BTG-Biba Model

The BTG-Biba model is compatible with each policy in the primitive Biba model and also supports context and fine-grained access control. A specific description of the BTG-Biba model is presented in Fig. 2.

A. Model Description

The proposed model uses the original Biba framework in a regular situation and BTG strategies in an emergency situation. Its specific framework is presented in Fig. 2.

The entire system contains four boolean variables, which are the System BTG mode identifier variable (Sys_Btg), the User BTG mode identifier variable (User_Btg), the Subject BTG mode identifier variable (Sub_Btg) and the Object BTG mode identifier variable (Obj_Btg). Sys_Btg and User_Btg were previously mentioned in Section III.A. Sub_Btg is used for checking if the subjects are permitted to enter in BTG mode. Obj_Btg shows if any subjects have accessed the object. The value of all boolean variables is TRUE (effective) or FALSE (ineffective), and the initial value is FALSE.

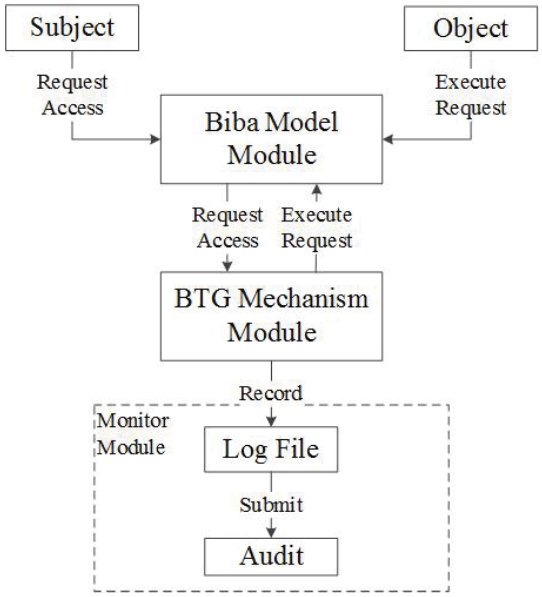

Fig. 2 BTG-Biba model framework

In the BTG-Biba model, when the subject accesses objects, they first obey the policy according to the primitive Biba model. The Biba model gives the corresponding access permission such as YES for permitting or NO for denying. When the subject obtains a NO permission, the system checks whether the BTG mode is on open state. Sub_Btg is equal to TRUE, if and only if Sys_Btg and User_Btg are equal to TRUE. At this time, the subjects are allowed to enter into BTG mode. Otherwise, this access is denied. When Sub_Btg is equal to TRUE, the system checks the Obj_Btg variable. If Obj_Btg equals FALSE, the subject accesses the object for the first time, and this subject is required to obtain confirmation from the user who owns it. After successful confirmation, Obj_Btg is set to TRUE; otherwise, the variable remains unchanged. If Obj_Btg equals TRUE, the subject can access the object directly.

After checking the Sub_Btg and Obj_Btg, the system makes an access decision whether object access can be granted to the subject under BTG mode.

A security monitor module should be included in this configuration to monitor abnormal access. Whenever emergency access is permitted, the system should perform the following [25]:

1) The subject request of the override access decision must be confirmed as exception access and provides a reasonable ground for exceptions.
2) The system records the exception access in a log file containing the name of subject, the object and the access time.
3) A notification about the override activity will be sent to the security officer and the internal auditor.

In the BTG monitor module, the audit operation is

implementation dependent. Although the monitor module monitors unconventional access, the integrity of the destroyed information cannot be completely guaranteed. The log file is sent to the auditing department for auditing, and the auditor may find that the system allowed unsafe operations. Next, the auditor reports to the system, and the system may mitigate the issue by utilizing a trace tactic or distrusting subjects who unsafely accessed the system; the system can then not assign privileges to these subjects in BTG mode.

The BTG-Biba model improves and expands the primitive Biba model, primarily by solving the cross-domain problem. The proposed model also brings context and fine-grained control to the system and enhances the capability of the system to address emergency situations.

Under BTG mode, the detailed flow of BTG-Biba model is shown in Fig. 3.

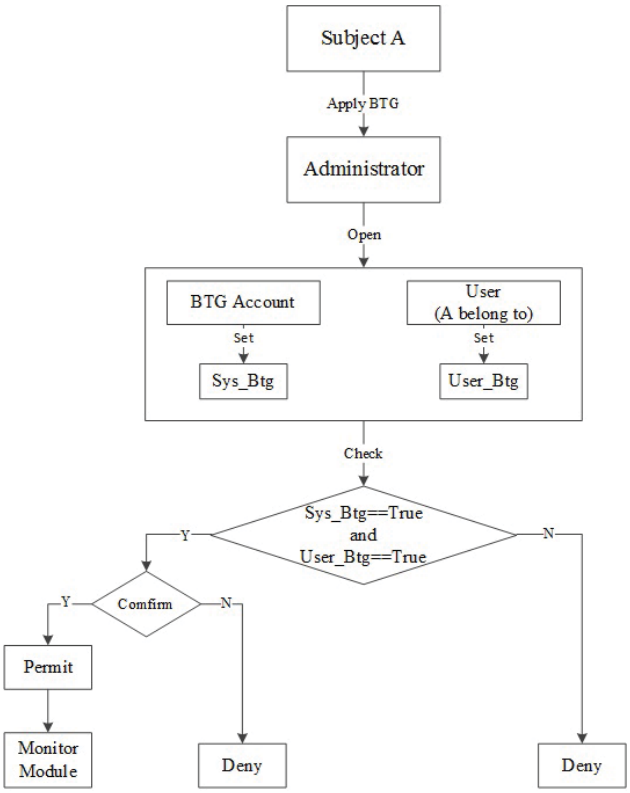

Fig. 3 Detailed flow of the BTG-Biba model

1) In an emergency situation, the subject requests access to an object which is not allowed in a regular situation.
2) The administrator receives the application from the subject and opens the emergency account.
3) Sys_Btg variable is set.
4) The user is found that the subject belongs to, and User_Btg variable is set.
5) The value of the Sub_Btg variable is checked.
6) When Sub_Btg equals TRUE, the value of Obj_Btg is checked; then, the access operation is executed.
7) All exception access is recorded in a log file and sent to the auditor for auditing.

This paper recommends that an administrator has the right to revoke the BTG privilege in the entire system by setting the Sys_Btg to FALSE and revoke the BTG privilege of a single user by setting the User_Btg to FALSE.

B. Security Policies of BTG-BIBA

The Biba model can be divided into two types of policies: mandatory and discretionary. Within these two divisions, there are a number of policies that can be selected based on the security needs. The mandatory policy includes many security policies, such as the Strict Integrity Policy, the Low-Water-Mark Policy, the Ring Policy, etc [16]. The proposed model could ensure that these policies work well and are able to handle emergency situations. The policies in the BTG-Biba model are given as follows:

- BTG-SIP Policy:
  $\forall s \in S, o \in O \quad s \ \underline{m} \ o \ \Rightarrow il(o) \ \ leq \ \ il(s)$
  $or \ Sub\_Btg == TRUE$
  $\forall s \in S, o \in O \quad s \ \ \underline{o} \ o \ \Rightarrow il(s) \ \ leq \ \ il(o)$
  $or \ Sub\_Btg == TRUE$
  $\forall s_1, s_2 \in S \quad s_1 \ \underline{i} \ s_2 \ \Rightarrow il(s_2) \ \ leq \ \ il(s_1)$
- BTG-RING Policy:
  $\forall s \in S, o \in O \quad s \ \underline{m} \ o \ \Rightarrow il(o) \ \ leq \ \ il(s)$
  $or \ Sub\_Btg == TRUE$
  $\forall s_1, s_2 \in S \quad s_1 \ \underline{i} \ s_2 \ \Rightarrow il(s_2) \ \ leq \ \ il(s_1)$
- BTG-Low-Water-Mark Policy:
  $\forall s \in S, o \in O \quad s \ \underline{m} \ o \ \Rightarrow il(o) \ \ leq \ \ il(s)$
  $or \ Sub\_Btg == TRUE$
  $\forall s \in S, o \in O \quad s \ \ \underline{o} \ o \ \Rightarrow il'(s) = min\{il(o), il(s)\}$
  $or \ Sub\_Btg == TRUE$
  $\forall s_1, s_2 \in S \quad s_1 \ \underline{i} \ s_2 \ \Rightarrow il(s_2) \ \ leq \ \ il(s_1)$

The policies in the BTG-Biba model are defined by axiom. When the integrity level cannot be compared in the original model, BTG strategies were applied to it. This shows that the original axioms can be applied in the proposed model. Thus, the BTG-Biba model can be perceived as an extension of the original model.

C. Illustration of the BTG-SIP Policy

As mentioned in the third section, BTG strategies could provide fine-grained control for an entire system. In the original Biba model, the access granularity is an integrity level rather than a single individual, similar to the ”No Read Down” and ”No Write Up” properties. However, due to the small scale of an emergency situation and the risks that implementing BTG strategies may bring, it is unreasonable to open the BTG mode to most of subjects in the system. So, all access under BTG mode must obey the rule that each access can only process a single subject and a single object. Thus, the fine-grained access control in the BTG-Biba model is enhanced and the system security is assured as much as possible. Using the BTG-Biba model with SIP as an example, suppose that subject 1 has $il_1 = (C_1, K_1)$ clearance and object 2 has $il_2 = (C_2, K_2)$ clearance. All of the access cases are listed in Table I.

As seen in Table I, only a part of access is permitted in the original Biba model because of the SIP restriction. All

TABLE I
ALL ACCESS CASES UNDER THE BIBA AND BTG-BIBA MODELS

Level comparison	observe		modify	
	Biba	BTG-Biba	Biba	BTG-Biba
$C_1<C_2, K_1<K_2$	YES	YES	NO	YES cross - c & domain
$C_1<C_2, K_1=K_2$	YES	YES	NO	YES cross - class
$C_1<C_2, K_1>K_2$	NO	YES cross - domain	NO	YES cross - class
$C_1=C_2, K_1<K_2$	YES	YES	NO	YES cross - domain
$C_1=C_2, K_1=K_2$	YES	YES	YES	YES
$C_1=C_2, K_1>K_2$	NO	YES cross - domain	YES	YES
$C_1>C_2, K_1<K_2$	NO	YES cross - class	NO	YES cross - domain
$C_1>C_2, K_1=K_2$	NO	YES cross - class	YES	YES
$C_1>C_2, K_1>K_2$	NO	YES cross - c & domain	YES	YES

denied access occurs because the integrity of the classification or the integrity of the domain does not meet the access conditions. However, under BTG mode, cross-classification and cross-domain access may be permitted when necessary. BTG strategies restrict each access from a single subject to a single object instead of restricting all the subjects in the same integrity level. Through the fine-grained access control, BTG-Biba allows a number of irregular operations in an emergency situation. Similarly, the proposed model can be applied in any other policies.

The following section presents the details of the experiment that demonstrates how a system runs with the BTG-Biba model.

V. AVAILABLE ANALYSIS

In general, Biba access control and BTG-Biba access control takes the following model:

```
BTG-Biba Model (S, O, A)
{
    If (Biba_checkaccess (S, O, A) = grant) Then
        output (grant)
    Else
        output (deny)
    endIf
}
BTG-Biba Model (S, O, A, Sys_Btg, User_Btg)
{
  If (Biba_checkaccess (S, O, A) = grant) Then
        output (grant)
  Else If ((Sys_Btg = true) and (User_Btg = true))
        output (BTG_check_access (S, O, A))
      Else
        output (deny)
      endIf
  endIf
}
```

As with the above code block, multilevel security policy model based on Biba can prevent the low integrity client partitions to modify the information of high integrity level file system to ensure the integrity of the system. In the Biba model, all request which violate the ruled is restricted. That is to say, Biba doesn't permit the operation which violates its policy. However, in the BTG-Biba, this context-aware model check the system state variables and change the context of the system into BTG mode with setting the system state variables. By controlling the access grain, system only allows a subject to modify an object at this time. This exception access is recorded in a log file and sent to the auditor for auditing.

The above analysis shows that the BTG-Biba model provides fine-grained access control and brings context for systems to address various access operations in different situations more effectively. Compared to the Biba model, the proposed model is much flexible and usable.

VI. CONCLUSION

This paper analysed the existing problems of Biba in detail, such as integrity level assignments, the lack of fine-grained control and context-sensitivity. Then it proposed the BTG-Biba model that integrated the BTG strategies into the Biba model to address the problems above. Next, in the following sections, the paper put forward the formal definition and access control policy of BTG-Biba. An available analysis is presented to illustrate the advantage of this model.

First, the improper of integrity level assignments will lead some non-malignity access be denied. By integrating the BTG strategies, BTG-Biba model can permit such irregular access operation in emergency situation and enhance the usability of the system. Second, for the irregular access request, system could judge the state variables to decide whether the whole system should get into emergency mode or not. This strategies make the static original model be context-aware and increase the flexibility of the system. Meanwhile, Biba model is a multi-level access model, the access grain are decide by the integrity level while BTG-Biba takes the rule that only a single subject can have a request to access a single object in the emergency situation to improve the access granularity. Besides, BTG-Biba model only allows the small-scale irregular access operation to be permitted. As mentioned above, fine-grained control is implemented in the system, and the concept of context is introduced so that the irregular access containing cross domain access could be allowed by system under the monitor of audit. Thus, the BTG-Biba model enhance the flexibility and availability of the system. What's more, the obvious advantage of the BTG-Biba model is that it occurs in real-time and has little influence on normal system operation.

The BTG-Biba is a model to provide emergency access in the Biba model. The BTG-Biba model is implementation dependent, so future research includes studying various handling methods when unsafe access is found after auditing.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation (NNSF) of China (Grant No. 61572385).

Conflict of interest statement: there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Tu, Shan Shan and Niu, Shao Zhang and Li, Hui, "A fine-grained access control and revocation scheme on clouds," *J. Concurrency and Computation: Practice and Experience,* vol. 28, no. 6, pp. 2381-2395, 2016, doi: 10.1002/cpe.2956.

[2] D. Elliott Bell and Leonard J. LaPadula, et al., "Secure Computer Systems: Mathematical Foundations," MITRE Technical Report MTR-2547, Secure Computer Systems Mathematical Foundations, vol. 1, Mar. 1973.

[3] K. Biba, "Integrity Considerations for Secure Computer Systems," Technical Report MTR-3153, MITRE Corporation, Bedford, MA, Apr. 1977.

[4] Chun-Yang Yuan and Chen-Lei Deng, "Enforcement of Clark-Wilson Model in Combination of RBAC and TE Models," *J. the Graduate School of the Chinese Acad,* vol. 24, no. 4, pp. 538-546, Jul. 2010.

[5] Zhou L, Varadharajan V, Hitchens M, "Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage," *J. Information Forensics & Security IEEE Transactions on,* vol. 10, no. 11, pp. 2381-2395, 2015, doi: 10.1109/TIFS.2015.2455952.

[6] Xu D., Kent M., Thomas L., et al. "Automated Model-Based Testing of Role-Based Access Control Using Predicate/Transition Nets," *J. IEEE Transactions on Computers*, vol. 64, no. 9, pp. 2490-2505, Sep. 1 2015, doi: 10.1109/TC.2014.2375189.

[7] Bishop M., *"Computer Security: Art and Science,"* Boston: Addison Wesley, pp. 3-6, 2003.

[8] EI Hassani A. A., EI Kalam A. A., Bouhoula A., et al., "Integrity-OrBAC: A New Model to Preserve Critical Infrastructures Integrity," *J. International Journal of Information Security*, vol. 14, no. 4, pp. 367-385, Aug. 2014, doi: 10.1007/s10207-014-0254-9.

[9] Garnaut P., Thompson J., "Review of Data Integrity Models in Multi-Level Security Environments," Technical Report DSTO-TN-0971, Defence Science And Technology Organisation Edinburgh Command Control Communications And Intelligence Div, Australia, Feb. 2012.

[10] Alexander P, Pike L, Loscocco P, et al., "Model Checking Distributed Mandatory Access Control Policies," *J. Acm Transactions on Information & System Security,* vol. 18, no. 6, pp. 1-25, Dec. 2015, doi: 10.1145/2785966.

[11] Watson, R.N.M.Feldman, B., Migus, A. and Vance,C. Design and implementation of the TrustedBSD MAC Framework. *Proc. the Third DARPA Information Survivability Conference and Exhibition,* Washington,DC: IEEE, pp. 38-49. Apr. 2003, doi:10.1109/DISCEX.2003.1194871.

[12] Wright, C., Cowan, C., Morris, J., Smalley, S. and Kroah-Hartman, G., Linux security modules: General security support for the Linux kernel. *Proc. the 11th Usenix Security Symposium,* Berkeley, CA: Usenix Association, pp. 17-31, Dec. 2002, doi: 10.1109/FITS.2003.1264934.

[13] Robert N.M. Wats on. "A Decade of OS Access-control Extensibility." *J. Communications of the Acm,*vol. 56, no. 2, pp. 52-63, Feb. 2013, doi:10.1145/2408776.2408792.

[14] Zhang X., Sun Y., "Dynamic Enforcement of the Strict Integrity Policy in Biba's Model," *J. Jisuanji Yanjiu yu Fazhan(Comput. Res. Dev.),* vol. 42, no. 5, pp. 746-754, Apr. 2005.

[15] JUN ZHANG, LI-JUN YUN, ZHENG ZHOU, "Research of BLP and Biba Dynamic Union Model Based on Check Domain," *Proc. the Seventh International Conference on Machine Learning and Cybernetics,* Kunming: IEEE, pp. 3679-3683, Jul. 2008, doi:10.1109/ICMLC.2008.4621044.

[16] Mingxi Zhang, "Strict Integrity Policy of Biba Model with Dynamic Characteristics and Its Correctness," *Proc. International Conference on Computational Intelligence and Security(CIS '09),* Beijing: IEEE, pp. 521-525, Dec. 2009, doi:10.1109/CIS.2009.58.

[17] Oleshchuk V., "Trust-enhanced Data Integrity Model," *Proc. IEEE 1st International Symposium on Wireless Systems (IDAACS-SWS),* Offenburg: IEEE, pp. 109-112, Sep. 2012, doi:10.1109/IDAACS-SWS.2012.6377645.

[18] Liu G., Zhang J., Liu J., et al., "Improved Biba Model Based on Trusted Computing," *J. Security and Communication Networks,* vol. 8, no. 16, pp. 2793-2797, Apr. 2015, doi:10.1002/sec.1201.

[19] A. Ferreira, D. Chadwick, P. Farinha, R. Correia, G. Zao, R. Chilro, and L. Antunes, "How to Securely Break into RBAC: The btg-rbac model," *Proc. Computer Security Applications Conference, Annual(ACSAC),* Honolulu, Hawaii: IEEE Computer Society, pp. 23-31. Dec. 2009, doi:10.1109/ACSAC.2009.12.

[20] Rissanen E., Firozabadi S., Sergot M., "Towards a Mechanism for Discretionary Overriding of Access Control," *12th International Workshop,* Bruce Christianson, Bruno Crispo, James A. Malcolm, Michael Roe, eds., Cambridge, UK: Springer Berlin Heidelberg, pp. 312-319. 2006, doi:10.1007/11861386_38.

[21] Achim D. Brucker, Helmut Petritsch, "Extending Access Control Models with Break-glass,"*Proc. the 14th ACM symposium on Access Control Models and Technologies(SACMAT'09),* NY, USA: ACM New York, pp. 197-206, 2009, doi:10.1145/1542207.1542239.

[22] *"Break-glass: An Approach to Granting Emergency Access to Healthcare Systems,"* White paper, Joint NEMA/COCIR/JIRA Security and Privacy Committee(SPC), 2004.

[23] Anderson R., Stajano F., Lee J.H., "Security Policies," *J. Advances in Computers,* vol. 2, no. 4, pp. 185-235, 2002.

[24] Helmut Petritsch, *Handling Exceptional Situations in Access Control,* Springer Fachmedien Wiesbaden, pp. 37-50, Sep. 2014, doi:10.1007/978-3-658-07365-7_3.

[25] Georgakakis, E., Nikolidakis, S.A., Vergados, D.D., and Douligeris, C., "Spatio Temporal Emergency Role Based Access Control (STEM-RBAC): A time and location aware role based access control model with a break the glass mechanism," *proc.IEEE Symposium on Computers and Communications (ISCC),* pp. 764-770, Jul. 2011, doi:10.1109/ISCC.2011.5983932.

Gang Liu received M.S. and Ph.D. degrees in computer science and technology from Xi'an Jiaotong University, Xian, China, in 2001 and 2004 respectively. He has been a faculty member of School of Computer Science and Technology at Xidian University since 2007, where he is currently an associate professor. His major research interests include embedded system, information security and trusted computing.

Can Wang is currently a M.S. at Xidian University, Xi'an, China. Her research interests include information security, access control and security model of integrity and confident in embedded system. *The corresponding author. Email: $gliu\_xd@163.com$

Runnan Zhang is currently a M.S. at Xidian University, Xi'an, China. His research interests include information security, access control and security model of integrity and confident in embedded system.

Quan Wang received the B.S., M.S. and Ph.D. degrees in Computer Science from Xidian University in 1992, 1997 and 2008 respectively. He is now a professor at the School of Computer Science and Technology and the institute director of the Institute of Computer Peripheral Equipment. His research interest includes embedded system.

Huimin Song is currently a M.S. at Xidian University, Xi'an, China. Her research interests include information security, access control and security model of integrity and confident in embedded system.

Shaomin Ji is currently a M.S. at Xidian University, Xi'an, China. His research interests include information security, access control and security model of integrity and confident in embedded system.