Layered Security Policy Enclaves in Wireless Classified Environments

Luay A. Wahsheh

***Abstract*—One fundamental key to successful implementation of secure wireless classified environments is the design and implementation of security policies. For wireless classified environments enforcing multiple concurrent policies, the design of correct implementation mechanisms is a challenging and difficult task. To simplify this task, our research work introduces a layered model that establishes a security policy assurance methodology that is applied to increase the overall security in wireless classified environments. In this model, multiple independent policies are specified that describe relationships between sets of entities in the classified environment. These multiple policies are then integrated into a single layered enclave system by applying an inter-enclave multi-policy classification paradigm for wireless information access. Our methodology is structured to assist system security managers in reducing the complexity of policy development and implementation, and is applicable to a spectrum of wireless classified environments.**

***Index Terms*—Classified environment, security policy, wireless.**

I. Introduction

CLASSIFIED environments are ones that need special handling due to the sensitive nature of the information exchanged, as well as due to a hierarchy of access privileges to the information and network resources. One detail involving wireless environments is the need to have them restricted only to those who have a need to use these environments [1]. Examples of users who would have a need to access these environments would include military commanders on the battlefield requesting real-time information on enemy movements operating in a foreign country as well as doctors using personal digital assistants to enter medical information from a patient.

In the computer security literature, the term *policy* has been used in a variety of ways. Policies can be a set of rules to manage resources (e.g., actions based on a certain event(s)) or definite goals to determine present and future decisions. Broadly speaking, a computer policy should address security issues: CIA (Confidentiality, Integrity, Availability). It is not trivial to provide a definition of *security* that is broad enough to be applied to a variety of computer systems, yet specific enough to accurately represent what security entails. Security can be viewed as mechanisms that are designed to enforce *secure* (proper) behavior on the operation of computers. Secure is defined by a security policy that addresses information confidentiality, integrity, and availability. We consider a system secure if the security policy is being correctly enforced.

Manuscript received July 15, 2012; revised August 16, 2012.

Luay A. Wahsheh is an Assistant Professor in the Department of Computer Science and Information Assurance Research, Education, and Development Institute (IA-REDI) at Norfolk State University in Norfolk, Virginia, USA.

Security in wireless classified environments involves protecting systems' entities from unauthorized access. We use the term *entity* to refer to any source or destination through which information can flow (e.g., user, subject, object, file, printer). Several issues have to be addressed in order to have systems function in a secure manner, including authorization, authentication, and software and hardware correctness. Our work focuses on security policies in relation to wireless communication. In this paper, we use the following terms: *security enclave* (coalition) to refer to a logical boundary for a group of entities that have the same security level; and *message* to refer to any data that has been encoded for transmission to or received from an entity (e.g., a method invocation, a response to a request, a program, passing a variable, a network packet).

Policy-based computer systems are concerned with developing a framework that provides control over the management of services; that is, specifying and using policies. There are certain issues that have to be addressed while developing such a framework, including using a language for specifying policies, an architecture design that consists of a policy manager that not only makes decisions based on the triggered policies, but also resolves policy conflict, and a policy enforcement mechanism that applies the actions specified by the policies. There are several advantages for having a well-defined policy, including improved scalability and flexibility in managing computer systems. Scalability is improved by applying the same policy to large sets of devices, whereas flexibility is achieved by separating the policy from the system implementation (policies can be changed without modifying the implementation).

In this proposed research work, we show how layered security policy enclaves can be deployed in wireless classified environments. We present a model that manages multiple policies within wireless classified environments. With the use of proper management techniques, system security managers can deploy secure systems, reducing the number of security vulnerabilities and breaches in wireless classified networks.

The access control and management of the layered policy enclaves will be implemented using different trusted components (e.g., guards). Security policies in wireless classified environments can be multi-level (e.g., based on security classification: Top Secret, Secret, Confidential, and Unclassified) where each entity is assigned an appropriate security level that is associated with the information stored in that entity. Policies in our model contain mandatory rules to guarantee that only authorized message transmission between entities can occur by imposing constraints on the actions (operations) of these entities. However, our work is not limited to military policies. Layered security policy enclaves can support other types of policies, such as corporate

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

security policies, discretionary access control, role-based access control, security laws, and so forth.

We discussed and presented security techniques and issues in wireless classified environments in our earlier work [2], [3], [1], [4], [5], [6], [7]. This proposed work outlines a layered approach that is used to express a wide range of security policies in wireless classified environments. This approach will provide system security managers with a framework for supporting the enforcement of diverse security policies in wireless classified environments. We present a model that provides a basis for the support of multiple policies, both individually and in composition. In our proposed classified environment model, security policies are designed not only to guide information access, but also to control conflicts and cooperation of security policies of different security enclaves. The problems and techniques that this research presents are significant because security policies play an important role in the success of a secure wireless classified environment.

We found very little research in the literature that considers a layered policy approach in wireless classified environments. Among those we did find was Montanari et al. [8] who analyzed policy violations detection in network multi-organization systems and introduced two protocols for selecting events to share between organizations to ensure the detection of all possible policy violations. Tomur et al. [9] proposed an architecture that provides secure wireless access to information resources of organization network from remote locations. Manley et al. [10] examined wireless security policies in sensitive organizations. They examined the Department of Defense's real world implementation of wireless security policies and pointed out its deficiencies based on their proposed framework.

II. Multi-Policy Paradigm

In this research work, we introduce a paradigm for information access that we call *Layered Inter-Enclave Multi-Policy* (LIEMP). LIEMP manages multiple security policies (i.e., it controls the conflicts and cooperation of policies from different enclaves) within heterogeneous systems. LIEMP is "*a policy about policies*" that ensures the enforcement of end-to-end mandatory information flow security policies, where the management and evolution of policies can be separated from applications.

As the use of computer systems becomes more commonly employed, managing security becomes more complex. With the coexistence of different distributed environments, security is often expressed using different policies that control information access. These policies must specify the authorized transactions of the system and actions for unauthorized transactions, all in a form that is implementable. Implementing the enforcement of policies is difficult and becomes very challenging when the system must enforce multiple policies.

A. Why LIEMP?

Security policies address different aspects of systems' security, such as information flow, availability, auditing, and authentication. Entities in an enclave can communicate with one another according to an individual security policy that is responsible for that enclave. In a multi-enclave environment where multiple policies exist, entities in different security enclaves cannot interact with one another in a secure way without the existence of a mechanism that controls the interaction. In this research work, we introduce a technique where all interactions between policies are controlled by a global multi-policy that guarantees the integration of various heterogeneous systems. For example, in a coalition model, LIEMP can integrate Army, Air Force, and Navy forces with a joint staff that ensures policy-compliant interaction between the coalition members.

In many environments, an application or resource may be shared by multiple entities, with each entity having its own security constraints for the application. In such a diverse environment, a single consistent open framework for policy integration is needed to handle the conflicts and cooperation of policies; this is the role of LIEMP. LIEMP is "a policy about policies" that ensures the enforcement of end-to-end mandatory information flow security policies. LIEMP can manage multiple security policies that can be applied to a spectrum of wireless classified environments. This allows the system security manager to manage the evolution of policies without modifying the applications to which these policies apply.

B. Multi-Policy Paradigm

In order to address the move towards the multi-policy paradigm that was first adopted by the United States Department of Defense (DoD) in 1993, we are applying the LIEMP paradigm to wireless classified environments. A LIEMP system in wireless classified environments is a multi-policy security system that supports a variety of independent security enclaves. A policy in the system can effectively deal with its enclave interactions (the entities that can communicate with one another in regards to that policy). When entities in different enclaves communicate with one another, the complexity of guaranteeing no conflicts between policies greatly increases. Our goal is to enable the system to effectively support secure information processing within multi-enclave-multi-policy environments.

III. Proposed Model

Wireless classified environments are convenient environment for applying LIEMP for many reasons, including: different processes in the system enforce different security policies with different security goals in mind (e.g., confidentiality, integrity, and availability), the system deals with different entities at different security levels, and wireless classified environments consist of separate components that interact with one another. Each component has its own functionality, potentially with its own security policy. To achieve security, our goal is to secure all interactions between the system's components using a *Security Policy Group* (SPG).

A. Policy Architecture

Information access controls are the mechanisms that are involved in the mediation of every request to resources and data maintained by a system. Based on the security policy, they determine whether the request should be granted or

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

denied. This mediation must be performed by a trusted component: the Policy Manager.

The *policy manager* makes access decisions in individual enclaves or between different enclaves, and the *policy database* stores the policies that the policy manager will need. The system security manager has the authority to specify security policies that are enforced by the system. Entities interact with the system to send requests through an entity interface. Auditing can be performed for entity requests; information about a request can be logged, which can be used for analysis of activities in the system.

The policy manager is the policy enforcement mechanism that mediates message transmission between entities. Once an entity makes a request to pass information, the request will trigger the policies that are related to the requesting and receiving entities. The policy manager receives the request and identifies the policies that have been triggered. The policy manager is separate from the policy database, which makes the system flexible and simple; the system security manager will be able to change policies without modifying the enforcement mechanism.

The policy manager is consistent and complete. It is *consistent* because an entity request is either accepted or denied, but not both. This is due to the conflict resolution techniques that force the policy manager to make a decision. The policy manager is *complete* because for each entity request, there is a unique result (the access request being accepted or denied).

Different policy models in the literature (e.g., Bell-LaPadula [11], Role-Based Access Control [12], Chinese wall [13], and Clark-Wilson [14]) have been developed to restrict information access. Although most systems are restricted to a single policy model to provide security [15], our proposed approach is capable of dealing with multiple policies from different models that are being enforced by the system. Different policies can all exist in one policy database. The policy manager checks the triggered policies and resolves potential conflicts (see Section IV). If the invoking entity is allowed to access another entity, then access is granted; otherwise it is denied. The policy manager is responsible for enforcing and monitoring the individual security policies and the multi-policies that are related to entities involved in the access.

B. Security Policy Groups

The meta-policy concept "*policies about policies*" was introduced by Hosmer [16], [17]. Hosmer argued that policies are seen in the context of large and interrelated trusted systems and understood as a set of constraints established by an accepted authority to facilitate group activity. Meta-policies provide a framework for explicitly stating the assumptions about policies and the control process for policies. Hosmer proposed interesting conflict resolution strategies. She showed that the conflict resolution process can be simple no matter how many different policies are included.

Kühnhauser [18] followed Hosmer's views of meta-policies, but he targeted a specific area of interest; the focus of his work was on application-specific policy development. A limitation of his policy model is that the model must be adapted to each modification of the application interface which limits the generality and reusability of policies. He argued that large computer networks connecting several independent organizations have security domains and each domain has potentially independent security policies. Kühnhauser and von Kopp Ostrowski [19] engaged meta-policies to construct a formal framework that supports multiple policies. The focus of their effort was to provide support for application-specific policy development and coexistence in open environments. Kühnhauser [18] defined *policy groups* as a combination of a set of regular (individual domain) security policies and a set of security policies that control inter-domain actions. An advantage of the policy groups' approach is that a policy group composes the sets of regular policies and inter-domain policies into a single structure, thus providing a single point of reference for the discussion and analysis of the system's security properties.

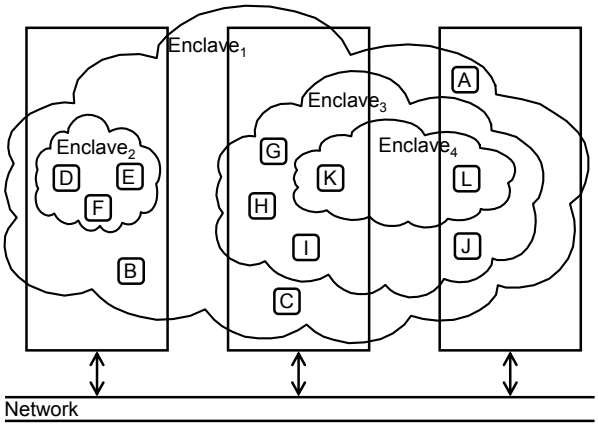
The LIEMP paradigm is an extension of Kühnhauser's work, but it focuses on policy specification for policy development in distributed multi-policy systems. Unlike Kühnhauser's approach, LIEMP is:

- Scalable: by applying the same policy to large sets of entities.
- Flexible: by separating the policy from the system implementation.
- Bi-directional: LIEMP is not limited to uni-directional information access requests between the system's entities; it is capable of supporting bi-directional information flow.

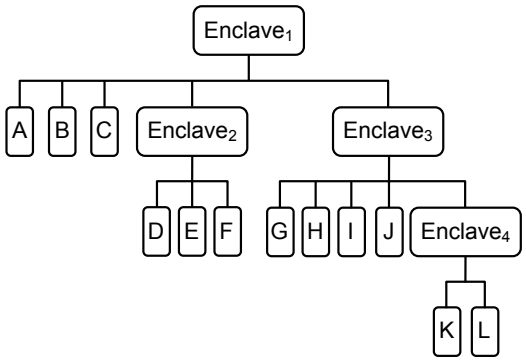
LIEMP is well suited for wireless classified environments, which is a multi-policy system that supports separate security policies for different enclaves in a diverse environment. An enclave sets a logical boundary for a group of entities that can communicate with one another according to an individual security policy responsible for that enclave. Each enclave has its own individual security policy that controls communication between entities that belong to the enclave. While an individual policy controls message communication within its enclave, *inter-enclave multi-policies* handle message communication between two or more enclaves. Enclaves can be arranged in a hierarchical structure and may exist across multiple processors; Figure 1 shows enclaves distributed over separate processors in *user view* (Figure 1(a)) and *system view* (Figure 1(b)).

Any interaction between entities is modeled as an entity e_1 accessing another entity e_2 through access operation op (e.g., $read(message)$ and $write(message)$). A message consists of many components, such as a payload (the fundamental content of a message) and type (e.g., GIOP, HTML, and TCP/IP). For example, a message might be represented by $G(p)$, where p represents the payload and G represents the type GIOP. $P(e_1, e_2, op)$ denotes the application of policy P to access (e_1, e_2, op), so $P(e_1, e_2, op)$ is of type *grant* or *reject*. Based on the sender's identity, recipient's identity, and some of the message content or type, a decision is made to grant or reject access. We assume that a policy manager should be able to respond to a certain request only to the entity that made the request (e.g., entity A should not receive information requested by another entity B). A policy

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)



(a) User View Structure.



(b) System View Structure.

Fig. 1. Enclaves Distributed over Separate Processors.

manager should make a decision and respond to a request within a period of time specified by the system security manager. The system security manager assigns different time limits based on entity priority (importance).

C. Layers

In this paper, we use the following notations: $Enclave_P$ to refer to the domain belonging to P which consists of all entities that are submitted to P. For any access (e_1, e_2, op), a policy P will contain an access rule if and only if $e_1, e_2 \in Enclave_P$; $S_e = \{P | e \in Enclave_P\}$ to refer to the set of security policies that have entity e within their enclave; $|C|$ to refer to the cardinality of some set C; I to refer to a finite set of indices; and $\{P_i\}_{i \in I}$ to refer to a set of security policies.

In a multi-policy enclave system with a set of security policies $\{P_i\}_{i \in I}$ and $e_1, e_2 \in \bigcup_{i \in I} Enclave_{P_i}$, any access (e_1, e_2, op) belongs to one of the following three disjoint layers:

Layer 1: $|S_{e_1}| = |S_{e_2}| = 1 \quad \wedge \quad S_{e_1} = S_{e_2}$

Layer 1 identifies the case in which conflict-free interactions occur when both entity e_1 and entity e_2 belong to exactly one enclave (the same enclave) and are not members of any other enclave. Since no inter-enclave communication is required, a single policy P makes the access decision. Figure 2 shows an example of Layer 1 access.

Layer 2: $|S_{e_1} \cap S_{e_2}| = 0$

Layer 2 identifies the case in which no security policy exists that has both entity e_1 and entity e_2 in its enclave; no security policy can provide the rule for interaction across multiple enclaves. An additional *completeness policy* is required to handle the communication. Two sub-layers exist:

a. $|S_{e_1}| = 1 \quad \wedge \quad |S_{e_2}| = 1$
Where each entity is a member of only one enclave. Figure 3 shows an example of Layer 2.a access.

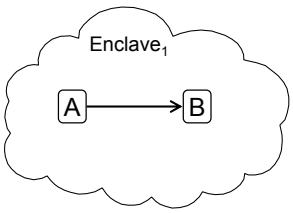


Fig. 2. An Example of Layer 1 Access.

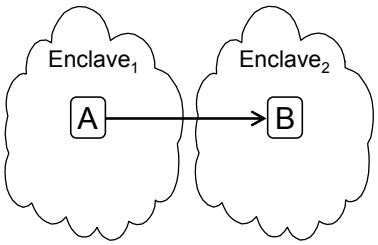


Fig. 3. An Example of Layer 2.a Access.

b. $\exists e \in \{e_1, e_2\} : |S_e| > 1$
Where at least one of the entities is a member of more than one enclave. Figure 4 shows an example of Layer 2.b access.

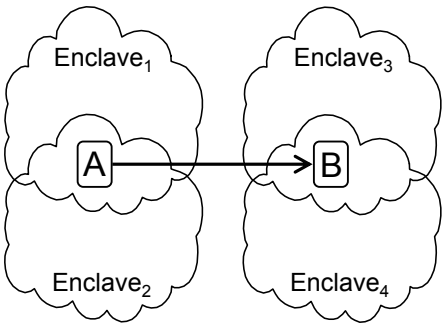


Fig. 4. An Example of Layer 2.b Access.

Layer 3: $|S_{e_1} \cap S_{e_2}| \geq 1 \quad \wedge \quad \exists e \in \{e_1, e_2\} : |S_e| > 1$

Layer 3 identifies the case in which at least one policy provides an access rule for both entities and at least one of the involved entities is a member of more than one enclave. This may cause a conflict which requires a *mediation policy* to identify appropriate rules. Inter-enclave multi-policies are mechanisms that resolve such conflicts between two or more policies. Two different types of conflicts exist:

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

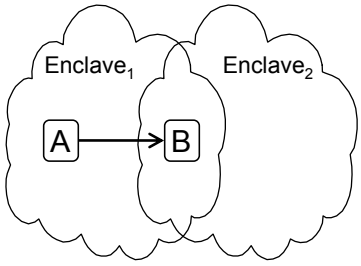


Fig. 5. An Example of Layer 3.a Access.

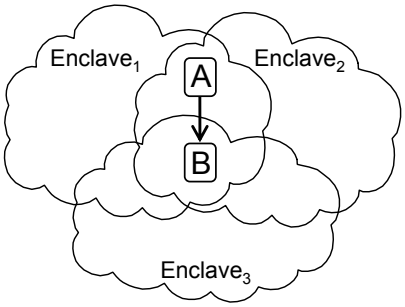


Fig. 6. An Example of Layer 3.b Access.

a. $|S_{e_1} \cap S_{e_2}| = 1$
An *enclave conflict* where an entity is a member of more than one policy enclave. Figure 5 shows an example of Layer 3.a access.

b. $|S_{e_1} \cap S_{e_2}| > 1$
A *rule conflict* where more than one policy exist for both entities that provide rules for the access. Figure 6 shows an example of Layer 3.b access.

An SPG is defined by combining the regular security policies, completeness policy, and conflict mediation policy into a single policy group. Let I be a finite index set and $\{P_i\}_{i \in I}$ be the set of regular security policies of a given multi-policy system. The security policy group $SPG = (\{P_i\}_{i \in I}, T, F, c)$ consists of the following:

- A set of regular security policies $\{P_i\}_{i \in I}$ implementing the security requirements for Layer 1 access.
- A completeness policy T implementing the security requirements for Layer 2 access.
- A conflict mediation policy F implementing the security requirements for Layer 3 access.
- A classification function c that for each access $(e_1, e_2), e_1, e_2 \in \bigcup_{i \in I} Enclave_{P_i}$ produces the class (e_1, e_2).

T and F are enforced with the same mechanisms as any regular security policy of a multi-policy system. In contrast to any regular security policy, the enclaves of T and F include the enclaves of every single regular security policy: $Enclave_T = Enclave_F = \bigcup_{i \in I} Enclave_{P_i}$.

The classification function c is of type $\bigcup_{i \in I} Enclave_{P_i} \times \bigcup_{i \in I} Enclave_{P_i} \rightarrow \{P_i\}_{i \in I} \cup T \cup F$. For any $e_1, e_2 \in \bigcup_{i \in I} Enclave_{P_i}$, c is defined as follows:

$$c(e_1, e_2) = \begin{cases} P_k & : \ |S_{e_1}| = |S_{e_2}| = 1 \ \wedge \ S_{e_1} = S_{e_2} \\ T & : \ |S_{e_1} \cap S_{e_2}| = 0 \\ F & : \ |S_{e_1} \cap S_{e_2}| \geq 1 \ \wedge \ \exists e \in \{e_1, e_2\} : |S_e| > 1 \end{cases}$$

The classification function is part of the policy manager that implements access mediation by overwriting the regular security policy call that is issued on every entity interaction. While any Layer 1 interaction is directed to its regular security policy, Layer 2 interactions are diverted to T and Layer 3 interactions are diverted to F.

D. Example

A wireless classified environment consists of different components, each of which has its own security policy. Figure 7 shows an example of interactions between components using an SPG for four enclaves; each enclave has separate security policies. The outer enclave indicates an enclave of a global policy and the innermost one indicates a more restrictive policy. Assume that $Enclave_1$ represents the University, $Enclave_2$ represents the Research Office, $Enclave_3$ represents the College of Engineering, and $Enclave_4$ represents the Department of Computer Science. Assume an employee Karen, denoted K, who works full-time at the Department of Computer Science, is temporarily assigned to work at the Research Office. This temporary assignment is considered a process of crossing over policy boundaries. Once K logs in to the system at the Research Office, she becomes an entity within $Enclave_2$. When K tries to access a file, denoted *W*, within her original enclave, $Enclave_4$, it is considered an inter-enclave access.

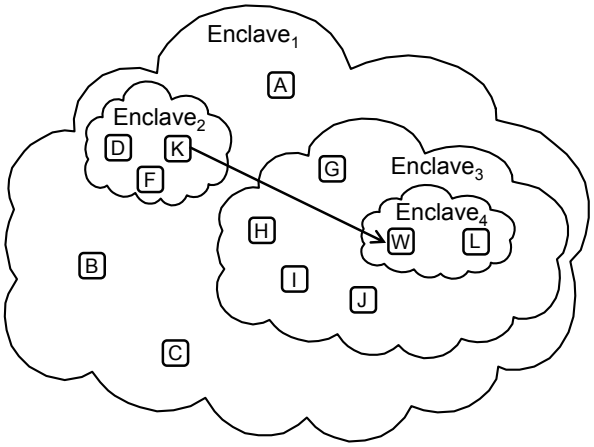


Fig. 7. A Structure of Policy Enclaves.

For now, let us ignore the policies of $Enclave_1$ and $Enclave_3$. Since $Policy_2$ does not have a rule for W in $Enclave_4$, and $Policy_4$ does not have a rule for K in $Enclave_2$, an SPG is needed to control the access.

- The SPG is $(\{Policy_2, Policy_4\}, T, F, c)$. S_K is $\{Policy_2\}$ and S_W is $\{Policy_4\}$.
- K's access is classified by function c as Layer 2 access: $|S_K \cap S_W| = |\{Policy_2\} \cap \{Policy_4\}| = |\emptyset| = 0$.

Therefore, policy T is selected for the access. The exact role of policy T will reflect the method of inter-enclave access in a wireless classified environment. For example, T could map K in $Enclave_2$ to K in $Enclave_4$ giving K the ability to have access rights in both $Enclave_4$ and $Enclave_2$.

In the case of policy conflicts, consider the previous example, but this time take all the policies of the enclaves into account.

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

- Entities in $Enclave_2$ are indirect members of $Enclave_1$ and entities in $Enclave_4$ are indirect members of $Enclave_3$ and of $Enclave_1$.
- The SPG is $(\{Policy_1, Policy_2, Policy_3, Policy_4\}, T, F, c)$.
- When K is in $Enclave_4$, S_K is $\{Policy_1, Policy_3, Policy_4\}$.
- When K is in $Enclave_2$, S_K is $\{Policy_1, Policy_2\}$.
- S_W is $\{Policy_1, Policy_3, Policy_4\}$.
- K's access is classified by function c as Layer 3 access: $|S_K \cap S_W| \geq 1$ in both cases, and each S contains more than one policy.

Therefore, policy F is selected for the access. The exact role of policy F will reflect the method of resolving conflicts in inter-enclave access in a wireless classified environment. There are two situations which can give rise to these potential conflicts:

1. Rule conflicts: rule conflicts occur in Layer 3 from Section III-C ($|S_K \cap S_W| > 1$). When K accesses her file while in $Enclave_4$, a rule conflict arises between policies $\{Policy_1, Policy_3, Policy_4\}$. One choice F could define is that the innermost policy overrides the outermost one, and, therefore, the innermost policy ($Policy_4$) will control K's request and make the access decision. With hierarchical policies, it is often easy to make such a determination.
2. Enclave conflicts: enclave conflicts occur in Layer 3 from Section III-C ($|S_K \cap S_W| = 1$). When K accesses her file while in $Enclave_2$, an enclave conflict arises between $Enclave_2$ and $Enclave_4$. Since no inner policy is able to make the decision, the global policy $Policy_1$ will control K's request and make the access decision. Or, as provided by policy T, K in $Enclave_2$ could be mapped to K in $Enclave_4$. When the conflicts are not hierarchical, *a priori* decisions must be made for any potential enclave conflict.

IV. Policy Conflicts

The LIEMP paradigm allows actions to be specified to resolve policy conflicts. With the coexistence of different policies in a diverse environment, interactions between the system's entities can result in policy conflicts. One policy may allow certain operations to be performed by an entity while another policy may not. LIEMP should not only control the cooperation of enclave individual policies to detect conflicts, but also take appropriate actions to resolve these conflicts.

A. Conflict Types

As mentioned in Section III-C, Layer 3 identifies the case in which at least one policy provides a rule for the access and at least one of the involved entities is a member of more than one enclave. LIEMP identifies two types of conflicts:

1. An enclave conflict, where an entity is a member of more than one policy enclave; Figure 5 showed an example.
2. A rule conflict, where more than one policy exist that provide rules for the access; Figure 6 showed an example.

B. Conflict Resolution

LIEMP should immediately decide how to resolve policy conflicts in a proper way. Resolving conflicts involves determining which policy will take precedence or what actions will resolve the conflicts. It must be noted that LIEMP is not allowed to rewrite enclave policies to resolve the conflict; this could lead to more conflicts. Instead, the system security manager can modify or remove existing policies and add new policies.

Potential conflicts could be identified at the time policies are being defined, but this tends to be time-consuming and, therefore, inefficient. A better approach is to have rules that control the interaction once a conflict has been detected. Many conflicts will be resolved if each entity is assigned an explicit priority by the system security manager based on its position in the hierarchy (importance). Once a conflict has been detected, LIEMP refers to the priority of the involved entities, and the policy of the entity that has the highest priority will be considered. Another approach is to give priority to the innermost policy over the outermost one (based on which enclaves the involved entities belong to, as shown in Figure 1). The innermost policy will become stronger and resolve the conflict. For example, when a conflict arises regarding a CS student in the CS Department, the policy of the CS Department will refine (add to) that of the University.

V. Conclusion

Although current wireless systems attempt to manage access to information, work on the specification and enforcement of policies is still needed because a precise specification and enforcement of policies is crucial in order to maintain secure systems, especially when multiple security policies of different enclaves need to cooperate. Our research work establishes a layered approach that is used to express a wide range of security policies in wireless classified environments. This approach is designed to assist system security managers in the specification and implementation of security policies in a way that increases the overall security in wireless classified environments.

The field of wireless security policies in classified environments is relatively new. There exists various research work in the literature that discusses security policies. However, very little of this work discusses enforcing policies using a structured approach in the context of wireless communication technology. In order to minimize security risks, a better understanding of wireless technology and its effect on the enforcement of security policies is essential. The relationship between wireless technology and security engineering introduces new challenges that need to be investigated. The approach proposed in this research work is an important step towards defining (understanding) this relationship.

References

[1] D. E. Burgner, L. A. Wahsheh, A. Ahmad, J. M. Graham, C. V. Hinds, A. T. Williams, and S. J. DeLoatch, "Using multi-level role based access control for wireless classified environments," in *Proceedings of the International Conference on Communications Systems and Technologies*, October 2011, pp. 828–832.

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[2] D. M. Thomas, A. Ahmad, C. Matarazzo, L. A. Wahsheh, J. M. Graham, A. T. Williams, F. R. Doswell, C. V. Hinds, and S. J. DeLoatch, "Smart meter design for wireless advanced metering infrastructure (AMI)," in *the Emerging Researchers National Conference in Science, Technology, Engineering and Mathematics (STEM)*, February 2012.

[3] D. M. Thomas, A. Ahmad, L. A. Wahsheh, J. M. Graham, A. T. Williams, F. R. Doswell, C. V. Hinds, and S. J. DeLoatch, "Automatic incident response wireless local area networks (AIR-WLANs) for advanced metering infrastructure (AMI)," in *the "Norfolk State University: Taking the Lead in Educational Attainment" Research Colloquium for Norfolk State University Faculty and Graduate Students*, March 2012.

[4] S. L. Cebula, A. Ahmad, J. M. Graham, C. V. Hinds, L. A. Wahsheh, A. T. Williams, and S. J. DeLoatch, "Empirical channel model for 2.4GHz IEEE 802.11 WLAN," in *Proceedings of the 10th International Conference on Wireless Networks*, July 2011, pp. 278–282.

[5] S. L. Cebula, A. Ahmad, L. A. Wahsheh, J. M. Graham, A. T. Williams, C. V. Hinds, and S. J. DeLoatch, "Location determination systems for WLANs," in *Proceedings of the 10th International Conference on Wireless Networks*, July 2011, pp. 438–443.

[6] D. E. Burgner and L. A. Wahsheh, "Security of wireless sensor networks," in *Proceedings of the 8th International Conference on Information Technology: New Generations*, April 2011, pp. 315–320.

[7] S. L. Cebula, A. Ahmad, L. A. Wahsheh, J. M. Graham, S. DeLoatch, and A. T. Williams, "How secure is WiFi MAC layer in comparison with IPsec for classified environments?" in *Proceedings of the 14th Communications and Networking Simulation Symposium*, April 2011, pp. 109–116.

[8] M. Montanari, L. T. Cook, and R. H. Campbell, "Multi-organization policy-based monitoring," in *Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks*, July 2012.

[9] E. Tomur, R. Deregozu, and T. Genc, "A wireless secure remote access architecture implementing role based access control: WiSeR," in *Proceedings of the World Academy of Science, Engineering and Technology*, December 2006.

[10] M. E. Manley, C. A. McEntee, A. M. Molet, and J. S. Park, "Wireless security policy development for sensitive organizations," in *Proceedings of the 6th Information Assurance Workshop*, June 2005, pp. 150–157.

[11] D. E. Bell and L. J. LaPadula, "Secure computer systems: Unified exposition and MULTICS interpretation," MITRE Corporation MTR-2997 Rev. 1, Tech. Rep. ESD-TR-75-306, March 1976.

[12] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control: A multi-dimensional view," in *Proceedings of the 10th Conference on Computer Security Applications*, December 1994, pp. 54–62.

[13] D. F. C. Brewer and M. J. Nash, "The Chinese wall security policy," in *Proceedings of the IEEE Symposium on Security and Privacy*, May 1989, pp. 206–214.

[14] D. D. Clark and D. R. Wilson, "A comparison of commercial and military computer security policies," in *Proceedings of the IEEE Symposium on Security and Privacy*, April 1987, pp. 184–194.

[15] R. Spencer, S. Smalley, P. Loscocco, M. Hibler, D. Andersen, and J. Lepreau, "The Flask security architecture: System support for diverse security policies," in *Proceedings of the 8th USENIX Security Symposium*, August 1999, pp. 123–139.

[16] H. H. Hosmer, "Metapolicies I," *ACM SIGSAC Review — Special Workshop on Data Management Security and Privacy Standards*, vol. 10, no. 2–3, pp. 18–43, Jun. 1992.

[17] H. H. Hosmer, "The multipolicy paradigm for trusted systems," in *Proceedings of the New Security Paradigms Workshop*, August 1993, pp. 19–32.

[18] W. E. Kühnhauser, "Policy groups," *Computers & Security Journal*, vol. 18, no. 4, pp. 351–363, 1999.

[19] W. E. Kühnhauser and M. von Kopp Ostrowski, "A framework to support multiple security policies," in *Proceedings of the 7th Annual Canadian Computer Security Symposium*, May 1995, pp. 1–19.

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)