https://doi.org/10.48009/2_iis_2013_393-399
Issues in Information Systems
Volume 14, Issue 2, pp.393-399, 2013

MULTI-DOMAIN ACCESS CONTROL POLICY IN WIRELESS CLASSIFIED ENVIRONMENTS USING STEGANOGRAPHY

Luay A. Wahsheh, Norfolk State University, law@nsu.edu

ABSTRACT

Security policies are critical aspects of secure computer systems. For wireless classified environments enforcing multiple concurrent policies across multiple domains, the design of correct implementation mechanisms is a challenging and difficult task. In order to simplify this task, our research work applies an additional layer of defensive mechanism using steganography to secure data in our multi-domain access control model. 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 enclave system by applying an inter-enclave multi-policy classification paradigm for information access using steganography. 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.

Keywords: Security Policy, Steganography and Classified Environment

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 [2]. 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.

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). 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).

In our previous research work [20], we showed how security policy enclaves can be deployed in wireless classified environments using a model that manages multiple policies within wireless classified environments. We introduced a paradigm for information access that we called *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. In this proposed research work, we show how this model can use secure access control using steganography techniques. 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. 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.

We discussed and presented security techniques and issues in wireless classified environments in our earlier work [2, 3, 4, 5, 15, 16]. This proposed work outlines a layered approach that is used to express a wide range of security policies in wireless classified environments using steganography. 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. 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. [14] 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. [17] proposed an architecture that provides secure wireless access to information resources of organization network from remote locations. Manley et al. [13] 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.

STEGANOGRAPHY

One method that provides more security in computer systems is the use of hidden messages. The hidden message can be plaintext, ciphertext, or image. Steganography is hiding messages within data. This technique makes secret messages appear invisible to entities. Although steganography algorithms use different formats including image, audio, and video, we focus on hiding messages within images. The image would be the carrier that holds the hidden message and the original content of the image. The hidden messages are embedded in a way that does not significantly change the properties of the original image. Steganography software tools (e.g., WinHip, EzStego, and OpenPuff) allow embedding hidden messages in an image and then extract that information.

Both steganography and cryptography are concerned with preventing unauthorized access to information. One advantage of steganography over cryptography is that a secret message that is generated by using steganography does not attract attention to itself because no encryption is used. When steganography is combined with cryptography, the security of data increases; in this situation, steganography is used to hide a ciphertext, and if the use of steganography was discovered, then cryptography is used to encrypt the plaintext.

The original image is the one in which the secret message is embedded. The payload is the secret message that will be embedded in the original image. The stego image is the final image that resulted from embedding the payload in the original image. Figure 1 shows an example of an original image, payload, and stego image. We used WinHip steganography software tool to produce the stego image. The human naked eye cannot detect the difference between the original image and the stego image.

More discussions of steganography are found in the literature [1, 6, 7, 12, 18, 19].

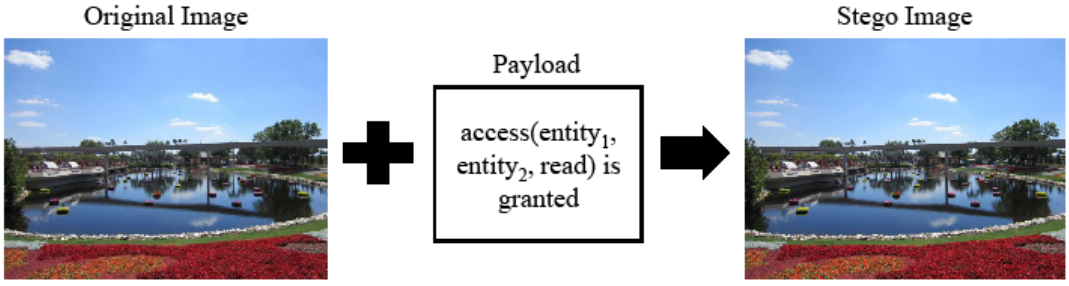

Figure 1. An Original Image, Payload, and Stego Image

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) that incorporates steganography techniques.

As indicated earlier, in our previous research work [20], we showed how security policy enclaves can be deployed in wireless classified environments using a model that manages multiple policies within wireless classified environments. The next sections provide a detailed summary of this work and how steganography is applied.

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 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.

Different policies can all exist in one policy database. The policy manager checks the triggered policies and resolves potential conflicts. 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.

Security Policy Groups

The meta-policy concept "*policies about policies*" was introduced by Hosmer [8, 9]. 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 [10] 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 [11] 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 [10] 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.

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 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).

Layers

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 $e_1, e_2 \in Enclave_P$; $S_e = \{P \mid e \in Enclave_P\}$ 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 $e_1, e_2 \in \bigcup_{i \in I} Enclave_{Pi}$, 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.

- 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.

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.

- 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:

  a. $|S_{e_1} \cap S_{e_2}| = 1$

  An *enclave conflict* where an entity is a member of more than one policy enclave.

  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.

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), $e_1, e_2 \in \bigcup_{i \in I} Enclave_{Pi}$ 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: $Enclave_T = Enclave_F = \bigcup_{i \in I} Enclave_{Pi}$.

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

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

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.

When a request for information access is made between entities across different domains, based on the security policy, the policy manager will determine whether the request should be granted or denied. The granted or denied request communication across domains will be hidden in images using steganography. Using steganography software tools, the policy manager is capable of hiding secret messages in images and unhiding the secret messages.

CONCLUSIONS

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 by adding an additional layer of defense using steganography. 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 wireless classified environments using steganography. The relationship between classified environments, 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. Begum, J. N., Kumar, K., & Sumathy, V. (2010). Design and implementation of multilevel access control in synchronized audio to audio steganography using symmetric polynomial scheme. *Journal of Information Security*, *1*, 29–40.
2. Burgner, D. E., Wahsheh, L. A., Ahmad, A., Graham, J. M., Hinds, C. V., Williams, A. T., & DeLoatch, S. J. (2011). Using multi-level role based access control for wireless classified environments. *Proceedings of the International Conference on Communications Systems and Technologies*, 828–832.
3. Cebula, S. L., Ahmad, A., Graham, J. M., Hinds, C. V., Wahsheh, L. A., Williams, A. T., & DeLoatch, S. J. (2011). Empirical channel model for 2.4GHz IEEE 802.11 WLAN. *Proceedings of the 10th International Conference on Wireless Networks*, 278–282.
4. Cebula, S. L., Ahmad, A., Wahsheh, L. A., Graham, J. M., DeLoatch, S., & Williams, A. T. (2011). How secure is WiFi MAC layer in comparison with IPsec for classified environments? *Proceedings of the 14th Communications and Networking Simulation Symposium*, 109–116.
5. Cebula, S. L., Ahmad, A., Wahsheh, L. A., Graham, J. M., Williams, A. T., Hinds, C. V., & DeLoatch, S. J. (2011). Location determination systems for WLANs. *Proceedings of the 10th International Conference on Wireless Networks*, 438–443.
6. Chanu, Y. J., Tuithung, T., & Singh, K. M. (2012). A short survey on image steganography and steganalysis techniques. *Proceedings of the 3rd National Conference on Emerging Trends and Applications in Computer Science*.
7. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Journal of Signal Processing*, *90*(3), 727–752.
8. Hosmer, H. H. (1992). Metapolicies I. *ACM SIGSAC Review – Special Workshop on Data Management Security and Privacy Standards*, *10*(2–3), 18–43.
9. Hosmer, H. H. (1993). The multipolicy paradigm for trusted systems. *Proceedings of the New Security Paradigms Workshop*, 19–32.
10. Kühnhauser, W. E. (1999). Policy groups. *Computers & Security Journal*, *18*(4), 351–363.
11. Kühnhauser, W. E., & von Kopp Ostrowski, M. (1995). A framework to support multiple security policies. *Proceedings of the 7th Annual Canadian Computer Security Symposium*, 1–19.
12. Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, *2*(2), 142–172.
13. Manley, M. E., McEntee, C. A., Molet, A. M., & Park, J. S. (2005). Wireless security policy development for sensitive organizations. *Proceedings of the 6th Information Assurance Workshop*, 150–157.
14. Montanari, M., Cook, L. T., & Campbell, R. H. (2012). Multi-organization policy-based monitoring. *Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks*.
15. Thomas, D. M., Ahmad, A., Matarazzo, C., Wahsheh, L. A., Graham, J. M., Williams, A. T., Doswell, F. R., Hinds, C. V., & DeLoatch, S. J. (2012). Smart meter design for wireless advanced metering infrastructure (AMI). *The Emerging Researchers National Conference in Science, Technology, Engineering and Mathematics (STEM)*.
16. Thomas, D. M., Ahmad, A., Wahsheh, L. A., Graham, J. M., Williams, A. T., Doswell, F. R., Hinds, C. V., & DeLoatch, S. J. (2012). Automatic incident response wireless local area networks (AIR-WLANs) for advanced

metering infrastructure (AMI). *The "Norfolk State University: Taking the Lead in Educational Attainment" Research Colloquium for Norfolk State University Faculty and Graduate Students*.

17. Tomur, E., Deregozu, R., & Genc, T. (2006). A wireless secure remote access architecture implementing role based access control: WiSeR. *Proceedings of the World Academy of Science, Engineering and Technology*.
18. Vanmathi, C., & Prabu, S. (2013). A survey of state of the art techniques of steganography. *International Journal of Engineering and Technology*, *5*(1), 376–379.
19. Venkatraman, S., Abraham, A., & Paprzycki, M. (2004). Significance of steganography on data security. *Proceedings of the International Conference on Information Technology: Coding and Computing*.
20. Wahsheh, L. A. (2012). Layered security policy enclaves in wireless classified environments. *Proceedings of the International Conference on Communications Systems and Technologies*, 888–894.