Poster: Topology Agnostic Security Policies

Gareth Taylor
Security Lancaster Research Centre
University of Lancaster
United Kingdom
g.a.taylor1@lancaster.ac.uk

Awais Rashid
Security Lancaster Research Centre
University of Lancaster
United Kingdom
marash@comp.lans.ac.uk

Abstract

Network policy enforcement is a prominent area of cyber security, however it is becoming increasingly difficult to enforce or patch policies that allow access to network data from untrusted locations, or even accessing data on devices not known to the network while maintaining security integrity. This paper looks at key features of popular policies and integrates these features into policies that do not always know the topology of a network or its hardware while still maintaining security integrity,

Keywords— (Network Topology, encryption, security polcies, RBAC, LBAC)

I. INTRODUCTION

Many businesses are moving away from formerly in house services in favour of outsourcing them. A service such as data storage, is now often handled by off site data storage centres or remote cloud systems owned by third part companies [1]. The current hyper connectivity of a business results in many issues. One such issue is guaranteeing hardware integrity when the hardware is not always owned by the business. Another issue is that of network access: how can a business guarantee security when it does not always manage the network from which the data is being accessed? As businesses move away from in-house server traffic and storage to alternatives such as that of cloud services, while also allowing employees to use their own devices to access the data from unknown networks, it is evident that popular security policies are not directly scalable when a network topology is considered *agnostic*. An agnostic network is a network of unknown size, for example, a company may not know all of the public access points its employees use to remote access data.

Role Based Access Control (RBAC) and Location Based Access Control (LBAC), or variants thereof, are amongst the most popular access control policies currently being utilised [2]. However, these access control policy types were originally designed with static networks in mind. There is a need for a set of access control policies that have been designed to scale to incorporate known network topology such as in house systems, however also include unknown network topology of third party systems such as cloud services and off-site storage providers. The newly designed set of policies must also view the network topology as agnostic as not all network access points can be mapped, while still maintaining strict access control rules, such as those found in RBAC and LBAC type access control policies. This paper presents early stage work in this regard. We propose the concept of topology agnostic polices that cater for an unknown network topology while still maintaining data access integrity.

Assuming valid logon details, we define a topology agnostic policy as follows: For hardware *H* being used to access the information from a network access point *N*, the level of access D is defined as a function *f*:

$$D = f(H, N) \chi K$$

where χ represents the composition of *f* with a value K generated by the framework to indicate the security properties that can be guaranteed about the network topology – depending on what is known or can be guaranteed about *H* and *N*.

II. BACKGROUND OF EXSISTING POLICIES

A. Role Based Access Control Policies

RBAC policies were original designed to govern the level of access for user groups. RBAC is typically designed as a hierarchal policy structure [3]. A typical example might be that of a company with four levels of access. Level one is the lowest level of access that most users use; this level will not allow access to business critical information. Levels two and three offer increments in access rights, with Level four being the highest level of access. Level four is restricted to key users as this level would have full read and write access to business critical information.

Benefits of RBAC access control polices are that only users of trusted levels can access sensitive data. Files can be split into levels of access to segregate user groups. Access is not hardware dependent meaning users can use their own hardware such as laptops and mobile devices without the company having to supply them, keeping costs lower.

One of the drawbacks of the RBAC access control policy structure is the trust placed in the level of access given to a user, without taking into account the user's access location and type. This drawback could result in a high-level user using valid credentials to access sensitive files over an unsecure network such as a public WIFI. The onus is placed on the user to verify that the connection type is secure without policies in place to verify and override if this is not the case.

B. Location Based Access Control Policies

LBAC policies are designed to govern the level of access via the means of location. LBAC is typically designed as a hierarchal policy structure similar to that of RBAC. LBAC is generally used over RBAC when there are multiple users sharing one piece of hardware [4]. An example might be that of a hospital that has fixed departmental workstations with a high number of users at each workstation. The lowest level of access would be an admin staff's workstation used for checking patient contact information and booking appointments with no access to patient records. The highest level of access would be a doctor's workstation – the doctor would have full read and write access to relevant patients' medical history.

Benefits of LBAC polices are that only workstations of trusted levels can access sensitive data. Files can be split into levels of access to segregate access types by location.

Drawbacks of the LBAC policy structure are firstly the hardware limitation of access via location. Although the location is the biggest security policy gain, it also limits the hardware use to a single function, which is not the most efficient use of a hardware resource. Secondly the network structure needs to be mapped and this results in access not being permitted via remote login, such as that of a user accessing files from a public location.

C. Original Access Control Policies in the modern world

A given modern scenario may be an employee checking a business report in a coffee shop using public WIFI.

- If we were to apply RBAC policies to the scenario there is a risk of several type of attacks. One such attack is a man in the middle attack, resulting in valid

user credentials being made available to malicious users [5].

- We could not apply LBAC policies, as the network is unknown and therefore could not be included in any workstation access.

It is clear that modern policies should be mutually exclusive of being able to keep data secure without always knowing the hardware or network the data is being accessed from. Policies such of that found in Trust Policy Language (TPL) address the issues of not knowing a user and then integrating that user to the network [6]. However such policies still rely on knowing the network topology. Traditional RBAC access control policies cannot be applied to networks of unknown user groups as they rely on a trusted infrastructure in order to regulate the access [7]. However TPL uses encryption to build trust from the bottom up with an unknown user on a known network. The encrypted data stream is then usually relied on as a means of trusted channel communication, however the data over the channel is still exposed in its encrypted form. Although encryption is a valued powerful tool it does not protect against malicious actions such that of a man in the middle type attack [8]. Currently encryption is relied on to bridge the gaps in policies like TPL and we are suggesting this does not have to be the case.

III. Initial Topology Agnostic Policy Solution

The proposed solution is that of one that guarantees security of data access integrity at the most sensitive data layer, while still offering data access even when the connection to the network is assessed as being that of the most exposed.

Figure 1 shows a proposed access criteria for policies that still abide by the same hierarchal principals of RBAC and LBAC policies, yet take into account the possibility of not knowing the topology of the network whilst also including the possibility of unknown hardware accessing data on the network.

An example of each assurance of integrity level of access is given in Fig. 1:

Each access level is only accessible with validated user logon details

- Basic Level Access- Level of access would occur when the hardware (H) and network (N) access points are unknown. A typical example would be access from any Internet enabled network such as public WIFI using any unregistered hardware like a public computer.
- Working level Access – Level of access would occur when the hardware (H) is known however; the network (N) access point is unknown. A typical example would be access from any Internet enabled network such as public WIFI using registered hardware such that of a company provided laptop.
- Trusted level Access – Level of access would occur when the hardware (H) and network (N) access points are known, however the network assessment (K) does not meet the security threshold for Administration level access. A typical example would be access using onsite company WIFI and registered hardware such as a company provided laptop.
- Administration level Access - Level of access would occur when the hardware (H) and network (N) access points are known, the network assessment (K) also meets the security threshold for Administration level access. A typical example would be access from an onsite desktop computer connected to the wired network of the company that has been verified by the framework as a secure access point.

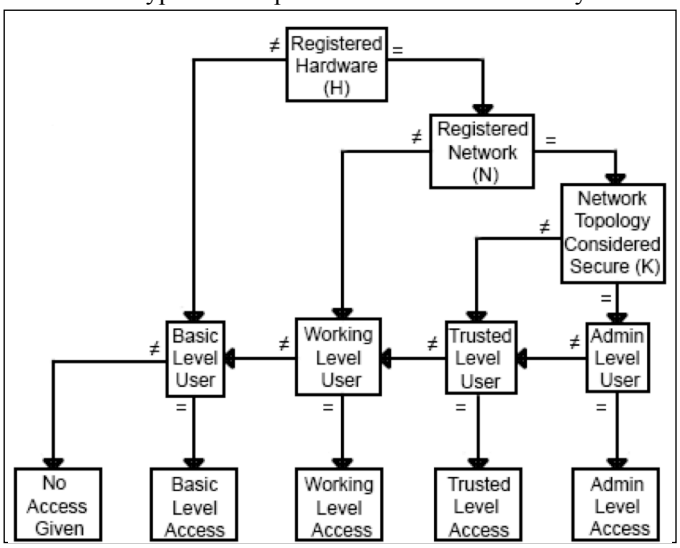

Figure 1. Topology Agnostic Security Policies Access Tree

K is shown as an assessed framework output from the security properties of the network topology, the framework calculates if the topology is considered to be secure based on a given threshold of K. Only when the network is considered completely secure the highest level of access is given to users with administration level privileges. A drawback of this type of policy enforcement is the inability to have administration level access from any location, or hardware. However, this results in guarantees of security enforcement while still offering some access at more exposed levels.

IV. Conclusion and Future works

This paper has been presented to show that policies can be written to offer similar access control benefits of both RBAC and LBAC type polices whilst also being scalable to including previsions for an agnostic network and unknown hardware. Although this work is in its infancy further development will be concentrated on developing a policy framework that not only enforces the access control polices discussed but also actively assesses the given security properties of individual network access connections in order to determine the value of K that results in a final framework access decision. Further work will also concentrate on areas of the framework that allow accurate assigning of access levels to a given set of data, without compromising on that data access integrity.

References

[1] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka and J. Molina, "Controlling data in the cloud", Proceedings of the 2009 ACM workshop on Cloud computing security - CCSW '09, 2009.

[2] R. Focardi, Foundations of security analysis and design. Berlin [u.a.]: Springer, 2001, pp. 137-196.

[3] Sohr, K.; Drouineaud, M.; Ahn, G.-J.; Gogolla, M., "Analyzing and Managing Role-Based Access Control Policies," in *Knowledge and Data Engineering, IEEE Transactions on* , vol.20, no.7, pp.924-939, July 2008

[4] F. Lin, D. Lee and B. Lin, Proceedings of the 2006 ACM Symposium on Information, computer and communications security. New York, NY: ACM Press, 2006.

[5] Rizvi, S.; Mitchell, J., "A Semi-distributed Access Control Management Scheme for Securing Cloud Environment," in Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on , vol., no., pp.501-507, June 27 2015-July 2 2015

[6] A. Herzberg, Y. Mass, J. Mihaeli, D. Naor and Y. Ravid, "Access control meets public key infrastructure, or: assigning roles to strangers", *Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000.*

[7] M. Kirkpatrick, G. Ghinita and E. Bertino, "Privacy-Preserving Enforcement of Spatially Aware RBAC", *IEEE Transactions on Dependable and Secure Computing*, 2011.

[8] Cleveland, Frances, "IEC TC57 Security Standards for the Power System's Information Infrastructure - Beyond Simple Encryption," in *Transmission and Distribution Conference and Exhibition, 2005/2006 IEEE PES* , vol., no., pp.1079-1087, 21-24 May 2006