A Comprehensive Survey on Access Control

Rashmi Hegde[#1], Dr. T H Sreenivas[#2]
#1 PG student, Department of IS&E,
The National Institute of Engineering, Mysore, India
#2 Professor, Department of IS&E,
The National Institute of Engineering, Mysore, India

***Abstract*— Access control is a way to manage access to enterprise resources. The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform. It provides protection, integrity, availability and auditing capability to an organization. The different authentication techniques, common access control methods and smart card based access control and its advantages are discussed in this paper.**

***Index Terms* — Access control, authentication, smart card**

I. Introduction

Access control is the selective restriction of access to a resource. It plays a major role in protecting an organization's resources. In today's complex and constantly changing business world, employees, partners, customers, vendors and contractors all require different levels of access to different areas at different times for different business purposes. As a result, enterprises must have business security solutions that provide detection and enforcement at every point of network access. To that end, corporations need a comprehensive, strategic approach to access control[1]. Figure 1 shows the basic access control system with security services

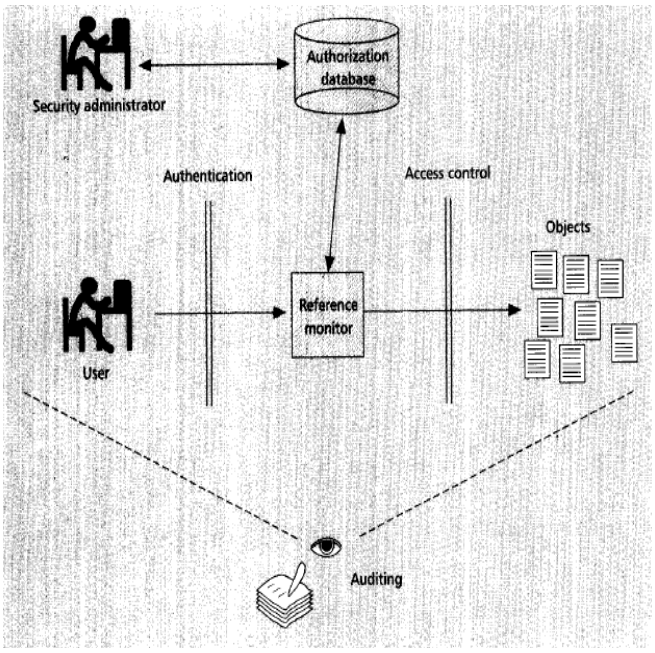

Figure 1: Access control and other security services

II. Background

Access control is the traditional center of gravity of computer security. It is where security engineering meets computer science. Its function is to control which principals (persons, processes, machines, . . .) have access to which resources in the system—which files they can read, which programs they can execute, how they share data with other principals, and so on[2].

In the first decade of the 21st century, physical security technology, like other technologies, has advanced at blinding speed. Physical access control, digital surveillance, building automation, and intrusion alarms now offer unprecedented features and capabilities in security. In the 21st century access control means intelligent,secure, and scalable biometric readers and data networks as well as open software platforms that can accommodate any number of business applications and changesin standards[3].

III. Existing Authentication Techniques [5]

1. User Password Authentication

It is the most common form of providing identification. When user accesses the resource, access control framework asks for the user name password provided to the user. The credentials are validated against the one stored in the system's repository.

2. Windows user based authentication

Usually, organizations have a list of users stored in the windows active directory. Access control framework should be able to provide authentication for the user of the Primary Domain Controller (PDC).

3. Directory based authentication.

With the rising volume of business over the web, millions of users often try to access the resource simultaneously. In such a scenario, the authentication framework should be able to provide for faster authentication. One such technique is Directory Based Authentication where user credentials are validated against the one which is stored in the LDAP Directory.

4. Certificate based authentication

This is probably one of the strongest authentication techniques where the user is asked to provide his/her digital ID. This digital ID, known as digital certificate, is validated against the trusted authority that issued the digital ID. There are various other parameters that are checked to ensure the identification of the user.

5. **Smart card based authentication**
   This is also used as a second factor authentication. Smart cards are small devices containing co-processors to process cryptographic data.

6. **Biometrics**
   This is the strongest authentication. Known as third factor authentication, it is based on something the user is. It works after the users have provided something they know (User name password) and something they own (either a grid or token) or something they are (retina-scan, thumbprint or thermal scan). It is required in cases where data is top confidential, such as in Military/Defense.

7. **Grid based Authentication**
   This is used as a second factor authentication. It authenticates the user based on something he knows (User name password authentication) and then asks for something he owns (grid card information). Entrust Identity Guard provides such an authentication.

8. **Knowledge-based authentication**
   One of the simplest mechanisms for gaining additional confidence in a user's identity is to challenge the user to provide information that an attacker is unlikely to be able to provide. Based on "shared secrets", this allows for the organization to question the user, when appropriate, to confirm information that is already known about the user through a registration process, or from previous transactions.

9. **Machine Authentication**
   Machine authentication provides validation of the user's computer in a way that secures against a variety of threats in a zero touch fashion, reducing user impact. This is an especially effective method of user authentication where users typically access their accounts from a regular set of machines, allowing for stronger authentication to be performed without any significant impact on the user experience.

10. **One Time Password (OTP)**
    A one time [assword is dynamically generated and it is valid only for once. The advantage of one time password is that if an intruder hacks it, he cannot reuse it. There are two types of OTP token generators: synchronous and asychronous. A synchronous token device synchronizes with the authentication service by using time or an event as the core piece of the authentication process. A token device, which is using an asynchronous token generating method, uses a challenge response scheme to authenticate the user.

IV. Common Access Control Methods

The four fundamental access control paradigms, which are found and distinguished in practice today, are:

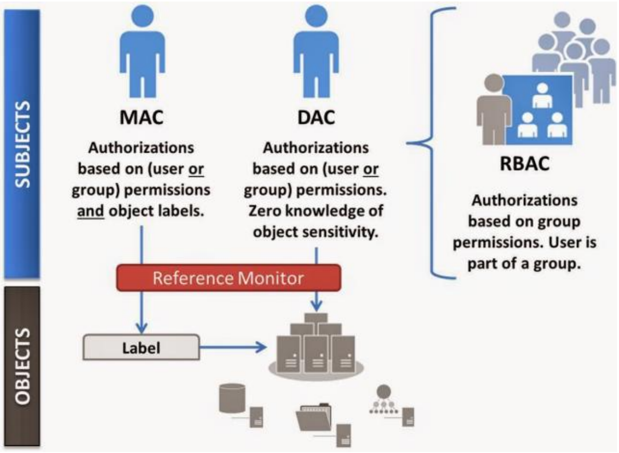
SUBJECTS
OBJECTS
MAC
Authorizations based on (user or group) permissions and object labels.
DAC
Authorizations based on (user or group) permissions. Zero knowledge of object sensitivity.
RBAC
Authorizations based on group permissions. User is part of a group.
Reference Monitor
Label

Figure 2: Common access control methods[6]

1. Discretionary Access Control (DAC) : In computer security, **discretionary access control** (**DAC**) is a type of**access control** defined by the Trusted Computer System Evaluation Criteria "as a means of restricting **access** to objects based on the identity of subjects and/or groups to which they belong.The validation and grant of access permissions is solely performed on the basis of the concrete identity of a subject and its group membership. Subjects who possess access rights for a certain resource may pass those on to other subjects. In a quite common implementation of DAC (such as used in UNIX), to each resource a special property called the "owner" is assigned, who may exclusively grant or deny any access rights to users or other groups for this resource.

2. Mandatory Access Control (MAC) : In computer security, mandatory access control (MAC) refers to a type of access control by which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target.The validation and grant of access rights is performed by utilizing sensitivity levels/labels, rules, and/or policies. In the simplest case each protected resource and each user possesses a set of security attributes: the user is usually assigned a clearance level, whereas the resource is assigned to a sensitivity level. Rules determine how those levels may concretely correlate and whether and how users of one clearance level may grant access rights to other users of different clearance levels. Depending on these rules different security objectives can be supported; e.g., if confidentiality is the major objective the Bell-LaPadula Model is more appropriate while integrity protection is better supported by the Biba model. In many running systems further dimensions – e.g., a specialty – are added for dealing with equivalency classes of sensitivity and/or clearance levels (lattice-model).

3. Role-Based Access Control (RBAC) : In computer systems security, role-based access control (RBAC) is an approach to restricting system access to authorized users.The RBAC-model is not assigning access rights to any resource directly to a subject's identity. Instead, each subject's identity is assigned with a set of roles, in which any access rights are defined. The concrete executing of access rights is therefore not directly bound to the user but acquired through its current role. The roles and its concrete permissions may be defined hierarchically (hierarchical RBAC) and rules may be constructed, which defines limitations (constraints) for the role assignment and permissions-granting (constrained RBAC).

4. Context-Aware Access Control : The shift from DAC and MAC to RBAC come along with a decoupling of subject related issues (identities and roles) and resource related issues (permissions encoded within policy sets). Context-aware access control goes even a step further by breaking up the static assignment of identities to roles and the static assignment of policies to roles or resources. It does so mainly by providing additional rules that control these assignments and as such introduces a new level of indirection.

V. Smart Card Based Acess Control

The merging of physical access technology with public key-enabled smart card technology has been an emerging trend that has occurred in the security industry over the past few years. A smart card is a credit card-sized piece of plastic, with a small microchip embedded on the face of one side. The microchip is actually a very small computer – complete with an operating system, application software, permanent storage, and I/O communication facilities[4]. Smart card technology today is bringing new advantages over proximity for physical access control as well as other applications.

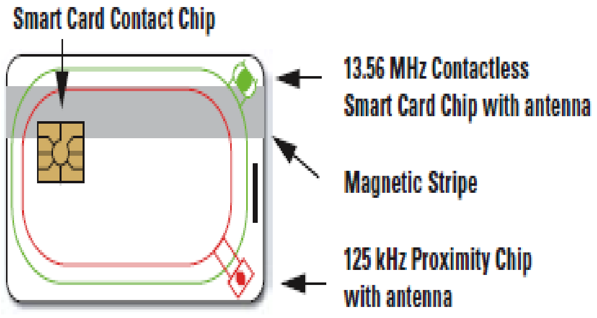
Smart Card Contact Chip
13.56 MHz Contactless Smart Card Chip with antenna
Magnetic Stripe
125 kHz Proximity Chip with antenna

Figure 3: A Smart Card and close-up of the Embedded Chip

Some of the potential benefits of smart cards are

1. Two-factor authentication: Most IT environments require users to authenticate via username and password – “something you know”. Requiring a PIN-protected smart cardfor authentication leverages an additional factor: “something you have” (the card), plus “something you know” (your PIN). This higher degree of assurance can help increase the security posture of a network environment.

2. Non-Repudiation : Most PKI-enabled smart cards are capable of generating RSA public and private key pairs on the card, where the private key cannot be extracted from the card under any circumstances. Therefore, any digitally signed email or documents created using these keys must have come from someone who had access to the card and knew its PIN code.

3. Less Dependence on Passwords : Since they are never sent over the network, card PIN values generally do not need to be changed as frequently as network passwords do. Windows systems can be configured to allow users to log in to their computers using only their card and their PIN, rather than a network password. This would even enable a scenario in which users did not even know their network password.

4. Automatic Screen Locking : Systems can be configured in such a way that the user’s screen is automatically locked when their smart card is removed from the reader; the user would then be required to re-insert the card and enter their PIN to regain access to his computer. If implemented properly, this can help reduce the security threat of an unattended logged-in workstation more effectively than inactivity timeouts.

5. Improves the Security of Kerberos : Microsoft’s implementation of Smart Card Login uses the PKINIT standard for Kerberos-based login. In short, a user still receives a Kerberos Ticket-Granting Ticket (TGT) as a result of a successful login to their domain via smart card login – just as they would if they had used their password. In addition, unlike the standard password-based Kerberos login, the initial response packet from the Domain Controller is not subject to offline password-guessing attacks.

Benefits of Contactless Smart Cards for Access Control

1. Contactless smart cards achieve a higher security level of the credential and the overall access control system.

2. Contactless physical access control credentials can carry secure IT applications such as secure logon to networks, digital signature, and encryption.

3. Contactless smart cards provide more storage and the secure reading and writing of data.

4. The capability to add other applications to the card is one of the most important advantages of contactless smart cards over proximity technology.

5. Organizations considering biometrics for either physical access or IT security applications can use contactless smart cards as a secure carrier of the biometric template.

6. Users can define and control their access keys.

7. Future-proofing - the desire to embark on a path offering greater expandability in the years to come.

8. Contactless smart card technology is affordable.

VI. Conclusion

Access control plays a major role in accessing resources. Contactless smart card technology is well-suited for access control applications. It provides higher levels of security than traditional access control technologies and the platform from which additional applications can be implemented on the same credential. While Public Key Infrastructure, smart cards, and physical security devices have all been around for many years, the convergence and overall maturity of these technologies is beginning to make their widespread use a real possibility for many corporate environments.

ACKNOWLEDGMENT

We are greatly thankful to our family and friends for the continuous support that has provided a healthy environment to drive us to do this project. We also thank the Principal and the Management of NIE for extending support to this work.

REFERENCES

[1] HP ProCurve Networking Access Control Security Solution, White paper.
[2] Security Engineering: A Guide to Building Dependable Distributed Systems.
[3] Deploying Smart Cards in Your Enterprise, www.css-security.com
[4] Access control in the 21st century, 3M Cogent, Inc., White paper.
[5] Authentication and Access Control - The Cornerstone of Information Security, Vinay Purohit, September 2007, White paper.
[6] www.cloudauditcontrols.com

AUTHOR PROFILE

Rashmi Hegde was born in Mysore,India (1993). She obtained B.E. in 2014. She is presently a student of M.Tech at National Institute of Engineering , Mysore in Computer Network Engineering. Her research interests are in the field of Ad Hoc networks, android, network security.

Dr.T.H.Sreenivas is Professor in the Department of Information Science & Engineering. He has received his Ph.D. from IIT, Madras, M.Tech. from IIT, Kanpur and B.E. from University of Mysore.
His teaching and research interests are in the field of Operating Systems, Networking, Schedule Optimization and Wireless Sensor Network.