A Survey on Cryptographic Algorithms and Access Control Mechanisms to Develop Security to Cyber Physical Systems

M.Sharada Varalakshmi
Associate professor, CSE
Department of Computer Science and Engineering
St.Peters Engineering College, Hyderabad, India

Abstract

Cyber Physical Systems (CPS) are sensing, communication and processing platforms, that are deeply embedded in physical processes and provide real time monitoring and actuation services. Securing a Cyber Physical System is of primary concern, as CPS is an automated unit that manages the information and physical process of an environment. Cyber Physical systems interact with the physical world wherein each system require different levels of security based on their sensitivity of information they carry. A high level of elevation is required on security for Cyber Physical System to counter the violations of security and preserve the privacy of the integrated systems. It is highly important to provide security to CPS. Confidentiality and Access Control are two important factors that need to be handled to provide protection to the information of CPS.

I. INTRODUCTION

Cryptography is the process that converts a plain text into a ciphered text. A cyber physical system is a connection between a group of systems in wireless world. Hence the data has to be encrypted in the cyber world . Also the access mechanisms to the physical system must be highly protected. This importance lead to the survey of various access methods and encryption methods available to incorporate them in a Cyber Physical System.

II. SURVEY ON CRYPTOGRAPHY

A. Symmetric cryptography

If, identical key is used for the process of encryption and decryption, then we call it symmetric key cryptography. In symmetric key concept, the exchange of key is only between the sender and receiver. This method of encryption provides high authentication in the process of exchange. So as long as both parties maintain secrecy, each party can be sure of authentication until the decrypted message continues to make sense. Symmetric key exchange disallows usage of dissimilar keys for encryption and decryption [Baker et al, 2006].

Symmetric key encryption is normally done in two ways. a) When the data is long, symmetric encryption divides the data into blocks and then encrypts each block into cipher text. This is called block cipher. b) Keys are expanded from the short keys and XOR'd on the plain text to form a cipher text. This is called stream cipher [Kahn.D et al, 1967].

B. Block Ciphers

Block ciphers take the input in the form of blocks, where each block has the key size as that of block size. Generally the key and the block are of the same size. An initialization vector is a random key generated that is taken as the first block to add randomness for encryption.

C. DES Algorithm

DES algorithm is the most popular symmetric algorithm that takes the plain text and key as input for encryption [Davis.R, 1978]. The plain text is 64 bit long for each block and the size of the key is 56 bit. At first, the 64 bit plain text undergoes initial permutations to rearrange the bits. It is then divided into two parts the left part and the right part of 32 bits each. This procedure is performed for 16 rounds of permutations and substitution [Gurujeevan Singh, et.al, 2012].

Initially, the key undergoes a permutation function. A sub key is generated by a fusion of left circular shift and right circular shift. At each round, plain text is split into two halves, 32 bits of the right half and 32 bits of the left half. With reference of expansion table, it is expanded into 48 bits and XOR'd with the key in the substitution table and generates 32 bit output. This output is then XOR'd with the 32 bit plain text on the left half to get the 32 bit cipher text on the right half using the predefined table and permutations. At the end of the first round 32 bit plain text of the right half pads with the 32 bits of the left pre cipher text and this process continues for 16 rounds [Nanda.A, 2005; Moyer et al, 1999].

Decryption algorithm is the same as encryption except that the sub keys are generated in the reverse order. Avalanche effect is a property defined to know the strength of any cryptographic algorithm. If a minor change in the plain text or size of key gives a major difference in the cipher text, then it can be noted that the strength of algorithm is effective. This property is very strong in DES algorithm [Biham.E 1996; Luck.S, 1998].

The DES algorithm is the building block of data security. The strength of DES is 2^{56} as the length of the key is 56 bits. That means, it takes 2^{56} attempts to break the key by brute force attack. Encryption algorithms may be applied in any of the four modes of operations that are defined. These modes are applied on various applications for encryption.

- Electronic Code Book (ECB) mode: This mode separates the plain text into blocks $b_1,b_2,..b_n$ and computes the cipher text $c_i = E_i(b_i)$. ECB is vulnerable to spicing attacks where encrypted blocks of one message are replaced with that of another [William Stallings, 1996; Alfred, 1996].
- Cipher Block Chaining (CBC) mode: This method starts with an initialization vector IV and XOR's it with plain text that is input to each encryption block Cipher text $c_i = E_k(C_{i-1} \text{ XOR } b_i)$. In this mode every block depends upon the previous block and the initialization vector. So, no spicing attack is possible as the initialization vector is unique [E.Biham, 1998].
- Cipher feedback mode (CFB) mode: In this mode, message is divided k bits of data units. Unlike CBC, this method transfers the values of plain text instantly one time. In CFB mode, the output cipher text is XOR'd with a current cipher text to produce a new cipher text [Coppersmith, et al, 1997]. CFB is a mode that finally derives a steam cipher text from a block cipher [William Stallings, 1996; Alfred, 1996].
- Output Feedback mode (OFB) mode: The OFB mode modifies the CFB where the output of the encryption is the feedback. The XOR value is formed independent of the plain text and cipher text [William Stallings, 1996; Alfred, 1996].

D. Triple DES Encryption

Triple DES encryption method uses two keys, where encryption is performed with first key, decryption with second key, followed by encryption with first key. This method helps in reducing the cost of key length and the man in the middle attacks. Triple DES has an advantage over the DES as this method performs multiple encryptions with multiple keys. Triple DES is an alternative to DES and is popularly used in key management standards [E. Thambiraja et al, 2012].

E. Advanced Encryption Standard

The process of encryption and decryption is performed with the same key in this most popular symmetric key. It uses only one key for generating the cipher text. AES uses three different keys like, AES 128, AES 192 and AES 256 respectively which indicates the length of the bit keys. The plain text is taken as 16 byte block. These bytes are arranged in a 4*4 matrix, where each block of the matrix has one byte of data. The rounds of encryption depend upon size of the key. If the key size is 128 bits, 10 rounds of encryption are performed [Daemen.J et al, 2001; Daemen.J, Rijamenl, 2002]. If the key size is 192 bits, then 12 rounds of encryption are performed. If key size is 256 bits, then 24 rounds of encryption are performed [Osvik et al, 2006; Courtois et al, 2002]. Steps for encryption/decryption:

1. Sub-Byte – This uses a substitution table(S-Box) that is constructed by multiplicative inverse and affine transformations. This is a non linear substitution
2. Shift Rows – In this step, the rows are shifted by byte transposition. Shifts are in circular manner where shifting varies from one to three bytes.
3. Mix Columns- This transformation is a mixing operation that operates on the columns of the state matrix. This is similar to matrix multiplication.
4. Add Round Key- A round key is XOR'd to the state matrix after mixing the columns. The resultant cipher text is a state matrix.

The strength of the AES algorithm is given as $2^{128.}$ That means breaking the algorithm by brute force takes 2^{128} times more computational power than 128 bit key.

F. Stream Ciphers

A stream cipher, ciphers a bit or byte of plain text at a time. The key is an infinite stream of pseudo random bits. For the security of the cipher text the pseudorandom generator should be unpredictable and should be used only once. Stream ciphers are of two types: synchronous and asynchronous. The popular stream cipher is RC4 encryption algorithm which requires secured key exchange.

G. RC4 Encryption

The key length of RC4 generally varies from 40 bit to 256 bits. An ACII code table is generated, that translates the 40 bit key into its equivalent ASCII 40 character binary equivalent. This table is used to generate pseudo random bytes and in turn generates pseudo random streams that are XOR'd with plain text to give cipher text. Swapping is done for each element at least once. RC4 has the capacity to use bits from 1 to 2048. This algorithm is used in commercial applications like Lotus, Oracle, etc.

The encryption of RC4 is 10 times faster than the DES algorithm. The key once used cannot be reused. The weakness of this algorithm is that there may be one weak key in every 256 keys [R.L.Rivest, 1995].

H. Asymmetric Encryption

RSA algorithm is the most popular asymmetric encryption algorithm [Henry Baker, 1982; William Stalling, 1998]. Asymmetric encryption is also called public key encryption. Asymmetric encryption involves two keys known as public key and Personal key [Diffie.W, 1976]. Public key is published to the receiver and Personal key is kept secret [Hellman, 1978]. Encryption of data is performed by one key

and decryption by other key. To send encrypted data, sender encrypts it with the receiver's Personal key. The receiver decrypts it with his own Personal key. The computational requirement is high for asymmetric encryption compared to symmetric encryption methods. So this encryption is not well suited for large volumes of data [C.A. Ardagna et al, 2008].

The strength of RSA for 128 bit is $3*10^{26}$ times stronger than that of 40 bit RC4 encryption. The strength of different encryption algorithms vary based upon the key lengths. Studies shows that key of length 52 bits in symmetric algorithms achieve equal strength with key of length 512 bits of asymmetric algorithms [Rivest, 1995].

RSA Key Generation Algorithm

1. Let p and q be two large prime numbers.
2. Calculate x = pq and r = (p-1) (q-1).
3. Select m so that 1<m<r and GCD(m, r) = 1.
4. Calculate n the Personal key such that nm = 1 mod r.

Therefore one key is (x, m) and the other key is (x, n). These keys must be kept secret and also the values of p, q and r must not be revealed.

- x is called the modulus.
- m is public key.
- n is a secret key.

Encryption Process

Steps at Sender A:

1. Gets receiver B's public key (x,m).
2. Identify a plain text message as positive integer k.
3. Calculate cipher text $C = k^m \bmod x$.
4. Transmits the cipher text C to receiver B

Decryption Process:

Steps at receiver B:

1. Consider his own Personal key (x, n) and computes plain text $k = c^n \bmod x$.
2. Convert the integer form to plain text.

I. Digital Signatures

Steps at sender A:

The message that is to be sent to the receiver is converted to Message Digest form. Using Personal key this Message Digest form is converted into encryption form. This encryption form is transmitted to the receiver [R.L Rivest, 1992].

Steps at receiver B:

The Message Digest received by the receiver is decrypted using sender's public key. The receiver computes the message of the Message Digest that is signed by the sender [A.S.R.L.Rivest, L.Adleman, 1978]. If both the Message Digests of the sender and the receiver are identical, then the signature is valid.

III. ACCESS CONTROL MECHANISMS

A logical security policy or the organization of rights is termed as access control [Mohammed Ennahbaoui, Said Elhajji, 2011]. Confidentiality and integrity are two fundamental properties of security policy for which the access control models must implement in order to build a tight security for organizations [P.Samarati, 2000].The access control policies are high level directives. These define three major rules as who (subject) should access what data (object) under which permission (action). The access control policy discusses the rules as

Subject – Active entity Eg. User's IP addresses, application etc.

Object - This is a passive entity that represents the data to be protected. Eg. File, Relational tables, class etc.

Action – This is the action taken by the subject on the object for a job. Eg. Read, Write, Execute.

The three most famous models of access control mechanism are DAC, MAC, and RBAC.

A. Discretionary Access Control Model

DAC is a flexible access control mechanism. The DAC allows one subject to grant access privileges to another subject. Privileges to subjects are granted and revoked by the policy of administration. The UNIX operating system is the most famous example of discretionary access control mechanism. The two well-known models of DAC are the Lampson model and the HRU model.

Lampson Model: This is a well-known model built by Lampson in 1971 [B. W. Lampson, 1974]. The access control mechanism is given as a matrix of access model by Lampson. This model is given by three terms(S, O, M) where S is the subject, O is the object and the matrix M_{so}. The access rights are granted to subject S on object O in a matrix model, that are usually read, write, execute. There is an ambiguity in the term "discretionary" that whether the rights given in the matrix model are the authority of the rights or if the users have the authority to grant.

The HRU model: The Harrison Ruzzo Ullman model is developed in 1976 [Harrisson, Razzo, Ullman, 1976]. The HRU model is an improvement to the Lampson model. This model uses the Lampson model and in addition also assigns specific commands to access rights (read, write, owner). This model also creates and deletes access to subjects. In this model, a right 'own' on (s, o) says that the subject s owns rights on object o. In other words, the subject has rights on object o which allows permissions to access entire column. The possible permissions that can be granted are Create Subject, Create Object, Destroy subject, Destroy Object, Enter, Delete, etc. Users can be trusted as, they follow the policies of the organization and processes running on their behalf. Hence, the subjects and the processes running on the subjects need to be distinguished.

B. Mandatory Access Control Model

The Mandatory Access Control (MAC) [E. D. Bell and J. L. La Padula, 1976] model creates a set of essential rules that forces the compliance of access control requirements. In this model access control

policy works in a centralized manner. Each access class has two components [R.S. Sandhu, 1993].

1. Level of security – Represents the data elements based on their security levels. E.g. Top Secret (TS), Secret (Se), Confidential (Co) and Unclassified (Uc) such that TS > Se > Co > Uc [D.E. Denning, 1976].

2. Category set – This specifies about the categories of fields in a set. E.g. Hierarchies and categories in military databases, financial databases, administrative databases, etc.

There are various algorithms defined by different authors on MAC.

1. SCOMP: This is one of the important products of multi level security and a derivative of MULTICS, launched in 1983. This is non expensive implementation by US defence department where messages are handled in multiple levels. This method is used in military data bases. It allows mails to pass from low level to high level and then distribute as commands to lower levels at an appropriate time [G.E. Lanwehr 1981; D.E. Bell, LaPadula, 1973].

1. Biba Model**:** This model is developed Kenneth J. Biba in 1975, this model ensures data integrity. It describes a set of rules to integrity and access control, where data is grouped into different levels [G.E.Ferraiolo, 1992].

In general, data integrity has three goals:

- Prevention of data modification by unauthorized users.
- Prevention of unauthorized modification of data by authorized users.
- Maintenance of consistent data.

2. Bell-LaPadula Model**:** This was developed by David Elliott Bell and Leonard J. LaPadula, This model is used for implementing access control models in military database applications in the U.S. department of Defence [Bell, LaPadula, 1973]. It ensures "no read up" and no "write down" mechanisms.
3. Lattice Model: This model is an interactive access control model that interacts with objects like resources, computers, subjects, entities, objects [R.S. Sandhu, 1993].
4. Watermark Model**:** This model extends Biba Model. Biba model, does not allow write-up and read-down operations. This is opposite to Bell-Lapadula model where write-down is permitted [D.E. Denning, 1996].

C. Role Base Access Control Model

An alternative approach to DAC and MAC is RBAC. This approach aims to facilitate the administration policy of access control. The term role is introduced in this access model, which is the responsibility of the person in an organization [R.T. Simon, M.E. Zurko 1997]. The person who plays this role may be an Engineer, Technician, Director, Professor, etc. Unlike the previous models, RBAC can grant access permission to subjects based on roles they play in an organization. For example, a person may be a Doctor and also a Director of an organization, where he has to have two types of permission to play in the organization.

The RBAC deals with four models

- Core RBAC.
- The Hierarchy role.
- The Constraints model.
- The Hierarchy Constraint model.

Role Based Access Control is further extended to take decision on access policies based on context of the user. This leads to the development context aware RBAC [G.J. Ahn, R.S. Sandhu 2000; A.E.KALAM, 2003].

D. Context Aware RBAC (CA-RBAC)

Decision making in CA-RBAC is considered by spatial, temporal, and resource context [M.J. Covington, W. Long, and S. Srinivasan 2001] presents a team based access control method known as the Context Aware Access Control model [K. Hendrix et.al.2004] analyse the temporal considerations of role based access control [A.Corradi, et.al, 2004].

E. User Control Access Model (UCON)

UCON is a combination of trust management and digital rights management. UCON provides trusted access to subjects, new to the systems. RBAC and its models are static in nature and do not have ability to change privileges of subjects [J. Park, R.S. Sandhu, 2002].

F. Optimistic Access Control (OAC)

This method allows the subjects to exceed their privileges given few constraints as 1) maintains a record of all actions performed by subjects beyond their privileges 2) Subjects are allowed to perform only that actions that can be rolled back [D. Povey, 2000].

G. Policy spaces (PS)

Another type of access control model is the policy space [D. Carman, B. Matt, and G. Cirincione, 2002] model. This model is adaptive in nature and divides the policies into groups called as policy spaces. In policy spaces approach the subjects wait for the access request and is reactive in nature.

H. Criticality Oriented Access Control (COAC)

This method enables action control privileges during the criticalities [S. K. S. Gupta et.al. 2006]. The role is added to a specific subject during the time of criticality for taking response actions. Detailed log will be maintained to prevent any malicious attacks during the time of criticalities. The scope of COAC is limited to single criticalities.

CONCLUSION

Several concepts of cryptography techniques, and access control mechanisms available in the literature. . A thorough review was performed on Cryptography and types of cryptography to understand the types of cryptographic algorithms their advantages and pitfalls, their strengths and weaknesses. A detailed study is performed on the concepts of access control and multilevel security mechanisms. This study helped us to know the various types of access control mechanisms in the literature and their applications.

REFERENCES

[1] Bardram, Jakob E., Rasmus E. Kjær, and Michael Ø. Pedersen. "Context-aware user authentication–supporting proximity-based login in pervasive computing." International Conference on Ubiquitous Computing. Springer Berlin Heidelberg, 2003.

[2] Bell, David Elliott. "Looking back at the bell-la padula model." Computer Security Applications Conference, 21st Annual. IEEE, 2005.

[3] Bell, D. Elliott, and Leonard J. La Padula. Secure computer system: Unified exposition and multics interpretation. No. MTR-2997-REV-1. MITRE CORP BEDFORD MA, 1976.

[4] Covington, Michael J., et al. "Securing context-aware applications using environment roles." Proceedings of the sixth ACM symposium on Access control models and technologies. ACM, 2001.

[5] Esposito, Floriana, Donate Malerba, and Giovanni Semeraro. "Decision tree pruning as a search in the state space." European Conference on Machine Learning. Springer Berlin Heidelberg, 1993.

[6] Harrison, Michael A., Walter L. Ruzzo, and Jeffrey D. Ullman. "Protection in operating systems." Communications of the ACM 19.8 (1976): 461-471.

[7] Lunt, Teresa F., et al. "The SeaView security model." IEEE Transactions on software engineering 16.6 (1990): 593-607.

[8] S. Mehrotra, Kalashnikov, Dmitri V., et al. "Index for fast retrieval of uncertain spatial point data." Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems. ACM, 2006.

[9] Lewis, David, and William Gale. "Training text classifiers by uncertainty sampling." (1994).

[10] Ngai, Eric WT, Li Xiu, and Dorothy CK Chau. "Application of data mining techniques in customer relationship management: A literature review and classification." Expert systems with applications 36.2 (2009): 2592-2602.