ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

A New Approach for Information Security in an Embedded Executable Build

M H Pradeep Kumar

Asst. Professor, Dept of ECE, BIT Institute of Technology, Hindupur, India

ABSTRACT: Information Security has become a major concern in recent years. Hackers are using new techniques to gain access to sensitive data, disable application and perform other malicious activities. The need to secure an application is important for today's world. This paper discusses the ways of ensuring security in a software build that goes onboard the flight control system on an aircraft. The control system is designed and the code is complied and executed on the actual hardware. The compiled code is certified. Various attacks and cyber terrorism has lead to a possibility that an outsider can intentionally load a malicious code on the processor card and harm the aircraft and passengers. Therefore various cryptographic algorithms have been proposed to ensure security. This paper discusses two such algorithms that provides cryptographic primitives such as integrity, confidentiality and authentication.

KEYWORDS: Security Threats, ECDH, ECDSA, RSA, MD5.

I INTRODUCTION

Security has been the subject of intensive research in the context of general-purpose computing and communications systems. Various attacks on electronic and computing system have shown that hackers always rely on exploiting security vulnerabilities in the software and the implementation of hardware components. Poorly chosen security measures can prove to be useless, or even counter-productive, in the face of a well executed attack. As such, the security system designer must consider the design of the entire system, and not incorporate security technologies at random. Applying security technologies without understanding the system and its threats can give users a false sense of security. Prior to applying security measures, one must fully understand the threats to the system. The process of threat modeling helps system architects assess and document the security risks associated with a system. Identifying threats helps develop realistic and meaningful security requirements. This is particularly important, for if the security requirements are faulty, the definition of security for that system is faulty, and thus the system cannot be secure. Proper identification of threats and appropriate selection of countermeasures helps reduce the ability of attackers to misuse the system

II RELATED WORK

Threat modeling involves understanding the complexity of the system and identifying all possible threats to the system, regardless of whether or not they can be exploited. A good threat model allows security designers to accurately estimate the attacker's capabilities. Threat modeling process involves three steps.

- Characterizing the System: This involves understanding every component of the system and its interconnections, defining usage scenarios, and identifying assumptions and dependencies.
- Identifying Assets and Access Points: An Asset is a resource of value, such as the data in a database or on the file system. Access points are what the attacker is going to use to gain access to the assets. Ex: open sockets, RPC interfaces, configuration files, hardware ports, file system read/write.
- Identifying threats: In threat modeling, a system model shows all security critical entities such as assets, access points, and communication channels. Threats can be identified by going through all security critical entities and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

creating threat hypotheses that violate confidentiality, integrity, or availability of the entity. Identify all the threats and categorize different threats according to STRIDE which is the acronym used by Microsoft.

Finally after the threats are identified they can be rated based on the risks they pose. This allows us to address the threats that present the most risk first, and then resolve the other threats. At Microsoft, the DREAD model is used to help calculate risk. Threat Modeling can be done manually, using UML diagrams or using threat modeling tools [1, 2]. Some of the possible threats to the aircraft wireless communication are

- Corruption of information assets: The adversary may attempt to corrupt certain critical data to create unwarranted concerns about aircraft system safety or create false alarms and late detection of corruption will delay flights and cost airlines and passengers. Some examples include AC data communications, such as ADSB message, avionics software updates or flight bag used in flight operation and management, health diagnostics used to detect/monitor faults.

- Misuse of information assets. Communicated assets may provide knowledge useful for the adversary in side channel attacks. Certain assets may also be considered to be intellectual property with business value, e.g., RFID tag or engine sensor data which may contain some sensitive part maintenance data.

- Delay of information assets: Time-critical assets may become inaccessible due to intentional jamming of wireless communication channels, potentially degrading the performance of the system.

- Repudiation: An entity in the system could deny having sent or received information assets after detection of corruption or misuse, thereby disrupting liability for accident or failure events in the system. Thus security is an important aspect which should be considered throughout the design process, along with other metrics such as cost, performance, and power.

III CRYPTOGRAPHY

Cryptography, defined as the science and study of secret writing concerns the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers and other methods, so that only certain people can see the real message. Security often requires that data be kept safe from unauthorized access. And the best line of defense is physical security (placing the machine to be protected behind physical walls). However, physical security is not always an option, due to cost and/or efficiency considerations. Instead, most computers are interconnected with each other openly, thereby exposing them and the communication channels that they use. With regards to confidentiality, cryptography is used to encrypt data residing on storage devices or travelling through communication channels to ensure that any illegal access is not successful. Also, cryptography is used to secure the process of authenticating different parties attempting any function on the system. Since a party wishing be granted a certain functionality on the system must present something that proves that they indeed who they say they are. That something is sometimes known as credentials and additional measures must be taken to ensure that these credentials are only used by their rightful owner. The most classic and obvious credential are passwords. Passwords are encrypted to protect against illegal usage. Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what it's packaging and labeling claims to be. Authorization is a layer built on top of authentication in the sense that the party is authenticated by presenting the credentials required (passwords, smart cards etc.). After the
credentials are accepted the authorization process is started to ensure that the requesting party has the permissions to perform the functions needed. Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms. Data Integrity and Non-Repudiation are achieved by means of digital signature, a method that includes performing cryptography among other things.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

IV HYBRID ALGORITHM

It is necessary to provide high security to information on controlled networks. There are various types of cryptographic algorithms that provide high security. This new security protocol has been designed for better security using a combination of asymmetric cryptographic techniques.

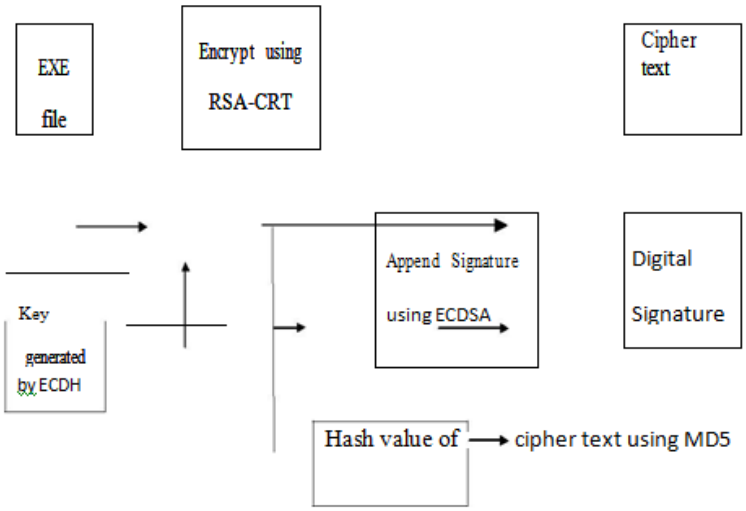

Figure 1: Security Scheme for sender file upload

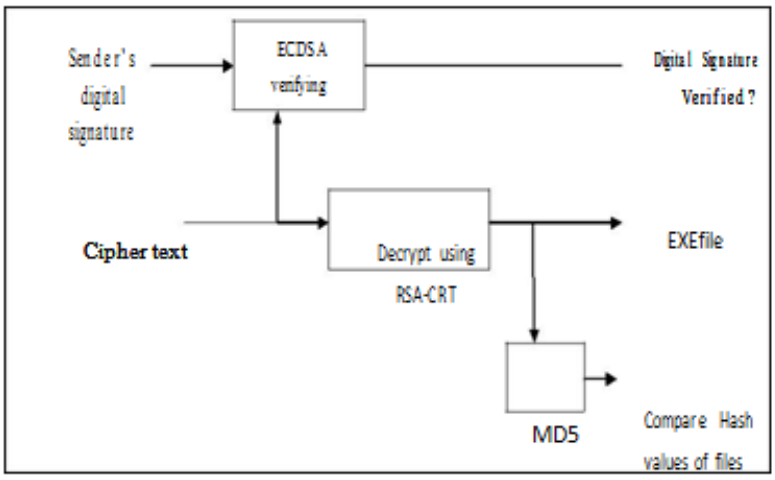

Figure 2: Security Scheme for Receiver file download

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

The given plain text can be encrypted with the help of key that is generated by the type Elliptic Curve Cryptography, i.e., ECDH. The encryption algorithm used is RSA-CRT, which takes as the original information and the key. The derived cipher text is appended with the digital signature for more authentication, generated by the ECDSA algorithm. Simultaneously, the hash value of this encrypted cipher text is taken through the Message Digest 5 algorithm. Now the generated cipher text and the signature can be communicated to the destination through any secured channel. On the other side, i.e., on decryption end, the hash value is first evaluated and integrated. This is compared with the signature, for the verification of the digital signature appended at the end of message. Thereafter, the decryption of cipher text is done by RSA-CRT. Hence, the plaintext can be derived. The intruders may try to hack the original information from the encrypted messages. He may be trapped both the encrypted messages of plain text and the hash value and he will try to decrypt these messages to get original one. He might get the hash value and it is impossible to extract the plain text from the cipher text, because, the hash value is derived from the RSA-CRT and appended signature, and the plain text is encrypted with RSA-CRT, with the key generated by ECDH algorithm. Hence, the message can be communicated to the destination with highly secured manner. The new hash value is calculated with MD5 for the received originals messages and then it is compared with decrypted hash message for its integrity. By which, we can ensure that either the original text being altered or not in th e communication medium. This is the primitive feature of this hybrid protocol [3,4]. One main advantage of ECC is its small key size. A 160- bit key in ECC is considered to be as secured as 1024-bit key in RSA.The algorithm shown in Figure 3 and 4 uses ECC for encryption and decryption instead of RSA.The second algorithm is more stronger than the first one but it consumes more time as ECC is used for encryption.

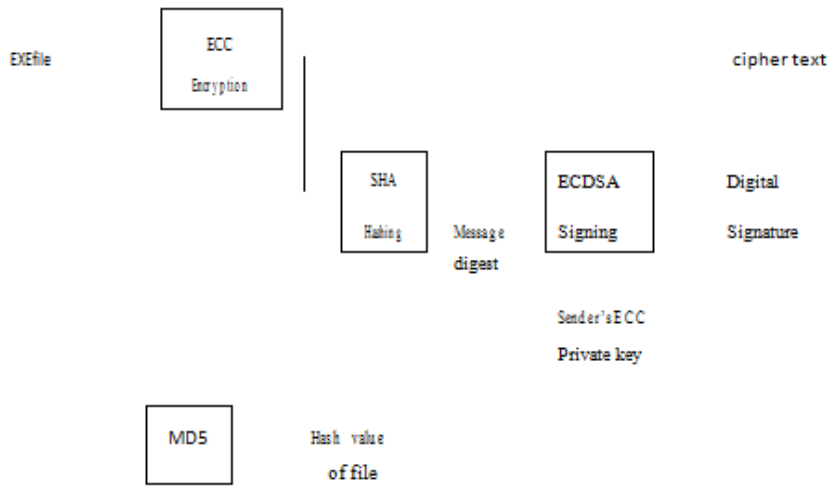

Figure 3: Security Scheme for Sender file upload

A. *ECC-Elliptic Curve Cryptography*- Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations..
The mathematical operations of ECC is defined over the elliptic curve $y = x + ax + b$, where $4a + 27b \neq 0$. Each

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G , the curve parameters ' a ' and ' b ', together with few more constants constitutes the domain parameter of ECC [5,7]. Discrete Logarithm Problem: The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem. Let P and Q be two points on an elliptic curve such that kP = Q, where k is a scalar. Given P and Q, it is computationally infeasible to obtain k, if k is sufficiently large is the discrete
logarithm of Q to the base P [5, 7].

***B**. ECDH – ELLIPTIC CURVE DIFFIE HELLMAN*-Using ECDH in the hybrid algorithm generates the key which is far secured than any other algorithm. ECDH is a key agreement protocol that allows two parties to establish a shared secret key that can be used for private key algorithms. Both parties exchange some public information to each other. Using this public data and their own private data these parties calculates the shared secret. Any third party, who doesn't have access to the private details of each device, will not be able to calculate the shared secret from the available public information [5]. Key exchange between users A and B can be accomplished as follows.

- A selects an integer n_A less than n. This is A's private key. A then generates a public key $P_A = n_A \times G$; where G is the generator point on the elliptic curve. The public key is a point in $E_q(a,b)$.
- B similarly selects a private key n_B and computes a public key $P = n \times G$.
- A generates the secret key $K = n \times P$ .B generates the secret key $K = n \times P$.

The two calculations in step 3 produce the same result because $n \times P = n \times (n \times G) = n \times (n \times G) = n \times P$
To break this scheme, an attacker would need to be able to compute k given G and kG, which is assumed to be hard .
C. RSA-The scheme developed by Rivest, Shamir and Adleman makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to log (n); in practice, the block size is k bits, where $2 < n \leq 2$ .Encryption and decryption are of the following form, for some plaintext block M and cipher text

block C:
$C = M \bmod n$
$M = C \bmod n = (M) \bmod n = M \bmod n$
Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of KU = {e, n} and a private key of KR ={d, n} [7].The RSA algorithm is given below.

- Select p, q where p and q both are prime and $p \neq q$.
- Compute $n = p \times q$
- Compute $\emptyset(n) = (p - 1)(q - 1)$
- Select integer e such that $\gcd(\emptyset(n), e) = 1; 1 < e < \emptyset(n)$.
- Compute $d \equiv e \bmod \emptyset(n)$.
- Compute Ciphertext $C = M \bmod n$.
- Compute Plaintext $M = C \bmod n$.

To reduce the execution time of decryption Chinese Remainder Theorem (CRT) is used in RSA decryption. RSACRT improved the performance of RSA in terms of computation cost and memory storage requirements. It
achieves parallelism. The CRT Decryption is achieved roughly ¼ times faster than original RSA. Time required to perform the encryption and decryption operation is less compared to RSA because RSA-CRT perform encryption and decryption by two blocks at a time. The decryption algorithm is as follows:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

- Compute dp = d mod(p − 1)
- Compute dq = d mod(q − 1)
- Compute qinv=q (mod p)

Compute m1 = C (mod p)

- Compute m2 = C (mod q)
- Compute h = qinv × (m1 − m2)(mod p)
- Compute the plaintext m = m2 + (h × q).

This is more efficient than computing m = C mod n even though two modular exponentiations have to be computed. The reason is that these two modular exponentiations both use a smaller exponent and a smaller modulus. When the primes p and q are roughly the same size, the computational cost for decryption using CRT-decryption is theoretically 1/4 the cost for decryption using the original method.

***D**. ECDSA – Elliptic Curve Digital Signature Algorithm* -The ECDSA is known to be the variant of DSA,which sends a signed message from A to B. Unlike the ordinary discrete logarithmic problem, or the factorization problem, ECDSA algorithm is known for elliptic curve discrete logarithmic problem (ECDLP). The elliptic curve discrete logarithm problem can be stated as follows. Fix a prime p and an elliptic curve. Q=xP, where xP represents the point P on elliptic curve added to itself x times. Then the elliptic curve discrete logarithm problem is to determine x given P and Q. It is relatively easy to calculate Q given x and P, but it is very hard to determine x given Q and P. It is for this reason ECDSA is used to provide security [6].

The ECDSA signature scheme includes three phases:

- Key Generation
- Signature generation
- Signature Verification

1. KEY GENERATION

In this phase we first obtain a set of elliptic curve domain parameters.

1. We select a random number d which belongs to the interval [1, n − 1]. Here d is considered as the private key.
2. Then we compute the public key Q = dG.
3. Thus the private key is d and the public key is (E, Q, G, n).

2. SIGNATURE GENERATION

Input: Message m and(d,Q).

1. Select a random number k [1, n − 1].
2. Compute kG = (x1, y1) and r = x1 mod n , if r = 0 go to step 1.
3. Compute s = k (e + d × r) mod n with e = H(m) ,if s = 0 go to step 1.
4. The signature of m is (r, s).

3. SIGNATURE VERIFICATION

Input: (r,s),m,Q.r, s), m, Q.

1. Verify r, s [1, n − 1].
2. Compute w = s mod n.
3. Compute u1 = e × w mod n and u2 = r × w mod n with e = H(m).
4. Compute X1 = u1G + u2Q and V = X1 modn.
5. If V = r then signature accepted.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

E. MD5

MD5 processes a variable length message into a fixed length output of 128 bits. The input message is broken up into chunks of 512-bit blocks; the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. The remaining bits are filled up with a 64-bit integer representing the length of the original message [5]. The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C and D. These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based
on a nonlinear function F, modular addition, and left rotation [12]. Many message digest functions have been proposed and are in use today. Here are just a few like HMAC, MD2, MD4, MD5, SHA, SHA-1[8].

V RESULTS

The two algorithms has been implemented using Matlab and the total time taken to perform the encryption and decryption is shown in figure 5 and 7.The table and the graph clearly shows that RSA is faster than ECC. If encryption is required at a faster rate then RSA algorithm is a better choice. Figure 6 and 7 shows the performance analysis of RSA and RSA using CRT for decryption. From this figure it is clear that the total computation time for encryption and decryption using RSA-CRT is less that the ordinary RSA. So for authentication RSA with CRT is used.

Figure 4: Execution times of RSA and ECC

EXE File Size (Kb)	Execution Time (secs)	
	RSA	ECC
26.5	9.334660	28.295172
30.5	12.132404	52.898257
35.0	15.921886	72.126783
41.0	21.853872	90.164325
50.0	31.644582	123.078053
65.0	53.003655	185.460029

Figure 5: Execution times of RSA and RSA-CRT

EXE File Size (Kb)	Execution Time (secs)	
	RSA	RSA-CRT
26.5	9.334660	6.295172
30.5	12.132404	8.123896
35.0	15.921886	12.33066
41.0	21.853872	15.96882
50.0	31.644582	25.331235
65.0	53.003655	45.56963

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

The above two tables show the execution times of RSA and ECC, and execution times of RSA and RSA-CRT. The table clearly shows that RSA is faster than ECC

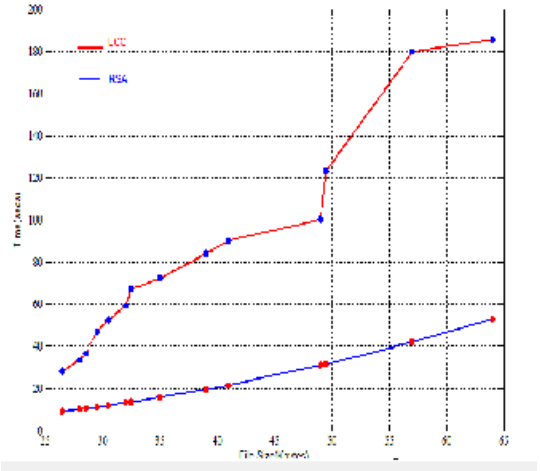

Figure 6: Execution times of RSA and ECC

The above graph shows the execution times of RSA & ECC. the graph clearly shows that RSA is faster than ECC. The above graph shows the performance analysis of RSA and RSA using CRT for decryption..

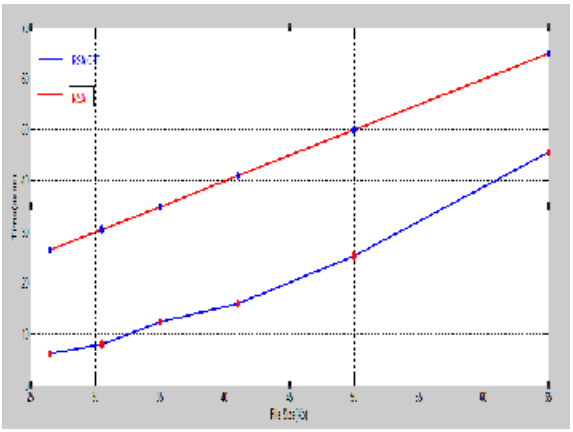

Figure 7: Execution times of RSA and RSA-CRT

The above graph shows the execution times of RSA and RSA-CRT. From this figure it is clear that the total computation time for encryption and decryption using RSA-CRT is less that the ordinary RSA.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

VI CONCLUSION

Devising a cipher scheme as presented in this study is one way to ensure security and be able to address the Confidentiality, Authentication, Integrity and Non-repudiation issues in system. The attractiveness of ECC, compared to RSA, is that it appears to offer better security for a smaller key size, thereby reducing processing overhead. Therefore it can be used to provide better security.

REFERENCES

[1] Myagmar, Adam Lee, B Yurcik, "Threat Modeling as a basis for Security Requirement",National Center for Supercomputing Applications (NCSA) University of Illinois at Urbana-Champaign.
[2] MSDN ,"Improving Web Applications :Security Threats and Countermeasures". http://msdn.microsoft.com/en-us/library/ff648644.aspx
[3] Martin Drahansky and Maricel Balitanas, "Cipher for Internet-based Supervisory control and Data Acquisition Architecture",Journal of Security engineering,vol 8,no 3,2011.
[4] Dubal,Mahesh, "Design of New Security Algorithm using Hybrid Cryptography Architecture",IEEE Conference on Electronic Computer Technology,2011.
[5] Anoop MS, "Elliptic curve Cryptography: An Implementation tutorial".
[6] Aqeel Khalique,Kuldip Singh,Sandeep Sood, "Implementation of Elliptic curve Digital Signature Algorithm",Journal of Computer Applications,vol 2,no 2,May 2010.
[7] William Stallings, " Cryptography and Network Security – Principles and Practices", 3rd Edition, Pearson Education Asia – 2003.
[8] Forouzan and Debdeep , "Cryptography and Network Security",2nd edition Mc Graw Hill-2008.

BIOGRAPHY

M H PRADEEP KUMAR is an Assistant Professor in the Department of Electronics & Communication Engineering, BIT Institute of Technology, Hindupur, JNTU Anantpur. He received Master of Technology in Computer Networks Engineering in 2010 from BITM, Ballari, Karnataka, India. And he received Bachelor of Engineering degree in Electronics & Communication Engineering, in 2006, from SJCE, Mysore, Karnataka. His research interests are Network Theory, Control systems, Computer Networks etc.