CONTENTS

1 ABOUT AUTHOR: 7

2 INTRODUCTION 8

- 2.1 Enterprise Architecture Framework (EAF) 9
- 2.2 Components of enterprise architecture framework 12
  - 2.2.1 Enterprise architecture domains and subdomains 13
  - 2.2.2 View model 13

3 ELEMENTS OF CRYPTOGRAPHY 16

- 3.1 Principles of cryptography 17
- 3.2 Three types of cryptography techniques 18
- 3.3 Public Key Cryptography 18
- 3.4 Hash Functions 19
- 3.5 Types of Encryption 19
- 3.6 Encryption and Decryption 19
- 3.7 Symmetric-Key Encryption 20
- 3.8 Symmetric-key encryption 20
- 3.9 Public-Key Encryption 21
- 3.10 Public Key and Private Keys 22
- 3.11 Digital Signatures 23
- 3.12 Digital Certificate 25
- 3.13 Public key Encryption Example 26
- 3.14 Decryption with B′s Private Key 27

4 RSA ALGORITHM 29

- 4.1 RSA algorithm 29
- 4.2 RSA Algorithm in Cryptography 30
  - 4.2.1 Key Generation 30
  - 4.2.2 Encryption 31
  - 4.2.3 Decryption 32
- 4.3 RSA Algorithm Limitations: 33
- 4.4 Diffie-Hellman Algorithm 33
  - 4.4.1 Where is the Diffie-Hellman key exchange used? 35
  - 4.4.2 Variations of the Diffie-Hellman key exchange 36
  - 4.4.3 Elliptic-curve Diffie-Hellman 36
  - 4.4.4 TLS 36
  - 4.4.5 ElGamal 37
  - 4.4.6 STS 37

5 FIREWALL 38
5.1 Netfilter/Iptables 41
5.2 Load balancing and fault tolerance 46
5.3 L7 Filtering 49
6 NETWORK ADDRESS TRANSLATION (NAT) 52
7 ATTACKS 62
7.1 Attacks on low levels of the ISO / OSI stack. 62
7.1.1 Physical attacks 62
7.1.2 Connection level connections 62
7.1.3 Network-level attacks 64
7.2 Attacks on high levels of the ISO / OSI stack 70
7.2.1 Transport level attacks 70
7.2.2 Attacks on middleware 72
7.2.3 SQL Injection 72
7.2.4 Cross-Site-Scripting (XSS) 75
7.2.5 Attacks on higher protocols 77
7.3 Buffer overflow 79
8 SECURITY OF WIRELESS NETWORKS 81
8.1 802.11 and Wi-Fi protocol 84
8.2 Insecurities of the 802.11 protocol 92
8.3 The 802.11i protocol 101
8.4 Security tools 107
9 NETWORK MANAGEMENT 109
9.1 Internet 117
9.2 Routing 122
9.3 Quality of Service 132
9.4 Network Management 143
10 CONCLUSION 150

LIST OF FIGURES

Figure 1 Enterprise Architecture Framework Model 10
Figure 2 Enterprise Architecture Framework 11
Figure 3 View model of Architecture 14
Figure 4 Same Key 18
Figure 5 Different Key 19
Figure 6 Hash Function 19
Figure 7 Type Of Encryption 20
Figure 8 Encryption And Decryption 21
Figure 9 Public Key Encryption 22
Figure 10 Digital Signature 24
Figure 11 Digital Certificates and Certification Authorities 26
Figure 12 Example-Public Key Encryption 27
Figure 13 Decryption with B's Private Key 28
Figure 14 Key Generation 31
Figure 15 ENCRYPTION 31
Figure 16 DECRYPTION 32
Figure 17 Flow Design of RSA Algorithm 32
Figure 18 Step by Step Explanation 34
Figure 19 Diffie-hellman algorithm- Example 35
Figure 20 Double Firewall Configuration 41
Figure 21 Logical diagram of the firewall 42
Figure 22 Complete Netfilter Scheme 43
Figure 23 Example of attempting to connect to a host on the internal network with a destination port higher than 1024 45
Figure 24 Conntrack state machine for TCP connections 46
Figure 25 Primary-configuration backup 48
Figure 26 Multi-primary hash-based stateful firewall-clusters 49
Figure 27 Performance with and without state replication 49
Figure 28 Non-Routable Address Space 52
Figure 29 On the left an example of dynamic NAT, on the right an example of NAPT 53
Figure 30 Possible ways of configuring NAPT and IPsec 54
Figure 31 STUN Diagram (RFC 3489) 59

1

ABOUT AUTHOR:

Joseph Thachil George is a Technical consultant for International Game Technology (IGT), Rome, Italy. He completed M. S in Cyber Security from the Università degli Studi di Firenze, Italy. Additionally, he also doing research in the Università degli Studi di Firenze, Italy. His research interests cover Blockchain technology- Hyperledger fabric, and cyber security. He published three books *Cybercrime and Social Media Relationships, Designing Distributed Systems* and *Social Network Analysis,* respectively. In IGT he is been a part of various project related to game configuration and integration in various platform. Specialized in Java and spring boot-based projects.

He has also worked in various companies in India, Angola, Portugal and UK. In total he has seven years of experience in various IT companies.

2

INTRODUCTION

In today's globalized world, each and every activity is interlinked in one way or the other way. In this book we shall be analysing computer networks and understand how data can be transferred securely form one system to another system. The concept of security can be briefly described as the protection of information of a system from theft or from hardware or software damage to the system itself. The main ones security properties are three:.

[1]. Confidentiality: Ensure that the information is not accessible by unauthorized persons.

[2]. Integrity: Ensure that the information is not altered by unauthorized persons in any way which is not detectable by authorized users.

[3]. Authentication: Ensuring that users are the people those who are authorized.

Achieving these goals, however, is not that simple. It is also very common to confuse the concept of *security* with that of *safety*:

- **Security.** This term expresses the set of measures aimed at preventing or reducing the probability that a given unwanted event will occur.

- **Safety.** With this term we mean the "response" of the system to the occurrence of a particular unwanted event. Safety is linked to danger / damage to people, and not just to things.

In general, security is sought for the safety of a system (e.g. control tower in an airport). Moreover, It is always good to keep in mind the costs related to security: security is not free. This in fact implies a greater complexity of the system, higher operational and implementation costs and the workflow change (some things may not be feasible, or may be done with limitations).

3

ELEMENTS OF CRYPTOGRAPHY

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.

Secure Communication refers to the scenario where the message or data shared between two parties can't be accessed by an adversary. In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security.

1. **Availability:** the service must always be available. Availability is violated in case of a Denial of Service (DoS) attack. Availability of the service is the most difficult thing to be guaranteed, since there are always physical limits of resources and a DoS attack must be implemented cost as much as possible. Availability is generally obtained with an accurate design of the network.

2. **Security:** the data exchanged must remain confidential between the parties participating in the exchange. Keep in mind that ethernet networks generally allow packet sniffing. For to obtain this property, cryptographic algorithms (symmetric, asymmetric, distributed, etc.).

3. **Data integrity:** refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.

4. **Authentication:** is the process of making sure that the piece of data being claimed by the user belongs to it.

5. **Non-repudiation:** whoever sends a message cannot later deny having sent it. This property is especially important at the application level when exchanging documents.

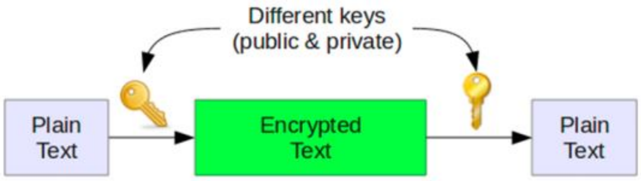

Figure 5: Different Key

message to bob, then Alice will encrypt it with Bob's public key and Bob can decrypt the message with its private key.

3.4 HASH FUNCTIONS

Not an key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altered, compromised or affected by virus.

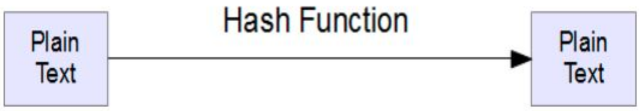

Figure 6: Hash Function

3.5 TYPES OF ENCRYPTION

3.6 ENCRYPTION AND DECRYPTION

- Encryption is the process of transforming information so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible again.

- A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption. In most cases, two related functions are employed, one for encryption and the other for decryption.

- With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, which