# Chapter 62
# Data Security in Wired and Wireless Systems

**Abhinav Prakash**
*University of Cincinnati, USA*

**Dharma Prakash Agarwal**
*University of Cincinnati, USA*

## ABSTRACT

*The issues related to network data security were identified shortly after the inception of the first wired network. Initial protocols relied heavily on obscurity as the main tool for security provisions. Hacking into a wired network requires physically tapping into the wire link on which the data is being transferred. Both these factors seemed to work hand in hand and made secured communication somewhat possible using simple protocols. Then came the wireless network which radically changed the field and associated environment. How do you secure something that freely travels through the air as a medium? Furthermore, wireless technology empowered devices to be mobile, making it harder for security protocols to identify and locate a malicious device in the network while making it easier for hackers to access different parts of the network while moving around. Quite often, the discussion centered on the question: Is it even possible to provide complete security in a wireless network? It can be debated that wireless networks and perfect data security are mutually exclusive. Availability of latest wideband wireless technologies have diminished predominantly large gap between the network capacities of a wireless network versus a wired one. Regardless, the physical medium limitation still exists for a wired network. Hence, security is a way more complicated and harder goal to achieve for a wireless network (Imai, Rahman, & Kobara, 2006). So, it can be safely assumed that a security protocol that is robust for a wireless network will provide at least equal if not better level of security in a similar wired network. Henceforth, we will talk about security essentially in a wireless network and readers should assume it to be equally applicable to a wired network.*

DOI: 10.4018/978-1-5225-8176-5.ch062

## INTRODUCTION

Although a wireless network offers multifold advantages, albeit it is also vulnerable to several security and privacy threats as itis a dynamic open medium (Kaufman, Perlman, & Speciner, 1995). Different types of clients such as laptops, cell phones, smart devices, etc. can join or leave the network anytime they wish. This opens up issues like fake registrations and packet sniffing. This chapter deals with the issues of security and privacy of a network in great detail by discussing countermeasures for different kinds of attacks. Weseparately discuss privacy and its importance also known as network anonymity that is usually achieved by employing redundancy at the cost of some associated overheads. We start off with the introduction of the basic idea in data security, then discuss available standards for different types of networks and powerful tools like Encryption. From there, we build up to known types of attacks and a brief study of major data breaches of recent times. We also discuss various experimental measures and proposed solutions. We end the chapter with our projections on data security and the summarize what to expect in future.

## GOALS OF SECURITY

### Data Authentication

This implies verifying and guaranteeing the identity of the sender and receiver of the data before any data transmission is initiated.

### Data Confidentiality

This feature is the core of secured communication and this mechanism assures that the data being transferred is only divulged to the authenticated sender and receiver. Attributes like date, time, content type, etc. are included in the data.

### Data Integrity

This property assures that the data remains intact in its original form during the transmission from the sender to receiver. This means that no one is able to modify the data along the way during transmission which should also be verifiable at both the ends of communication. Checksum is one example of such a service.

### Non-Repudiation

This is generally a combination of Authentication and Integrity of the data. This service facilitates proof of origin and integrity of data. In other words, no user can falsify the true ownership of data. Digital Signature is an example of such a service.