Chapter 6
Internet Security Using Biometrics

Shrikant Tiwari
Institute of Technology, Banaras Hindu University, India

Aruni Singh
Institute of Technology, Banaras Hindu University, India

Ravi Shankar Singh
Institute of Technology, Banaras Hindu University, India

Sanjay K. Singh
Institute of Technology, Banaras Hindu University, India

ABSTRACT

Internet security is a big challenge for Internet users, and passwords are the primary means of authenticating users. Establishing identity is becoming difficult in this vastly interconnected society. The need for reliable Internet security techniques has increased in the wake of heightened concerns about security and rapid advancements in networking, communication, and mobility. Biometrics is the science of identifying an individual based on his physical (static) or behavioral (dynamic) characteristics, and it is beginning to gain acceptance as a legitimate method for determining an individual's identity. Biometrics has been used for many years in high security government and military applications, but the technology is now becoming affordable for use as an authentication methods and general security feature. In this chapter, the authors provide an overview of Internet security using Biometrics.

INTRODUCTION

Internet security is concerned about the protection and access of information elements (e.g. multimedia data) thereby ensuring that only authorized users are able to access the contents available in digital media. Hackers and impostors are posing threat to a country (by hacking sensitive documents) and the society (by economic fraud and accessing secret information). Internet users such as military, intelligence, organizations, authors, authorized distributions or individual users are losing billions of dollars or their secret information.

DOI: 10.4018/978-1-4666-0203-8.ch006

Earlier, security was synonymous with secrecy and the shared secret between two business parties was a worldwide approach. But secret passwords require a great deal of trust between secret sharing parties. It is difficult to trust the administrator or other users of the internet network service provider that we access.

Most computers hacking today are due to compromise by system users or hackers using legitimate accounts to gain access to security. The identity of a person is becoming challenging in vastly connected information society. A large number of biometric-based identification systems are being deployed for many civilian and forensic applications invoking considerable interest.

It is difficult to ignore the presence of the internet economy or its future potential growth. It is always been suggested that there is no way of making the internet 'hundred percent safe and secure. Therefore, organizations and Government are forcing to implement high security policies to prevent unauthorized access into corporate networks to overcome risk. (Reid, 2003)

INTERNET SECURITY

Existing Security Primitives and Their Limitations

The existing security primitives use a generic cryptographic system, the user authentication method is possession based. It means the possession of the decrypting key is sufficient to establish the authenticity of the user. Since cryptographic keys are long and random they are difficult to member. So, these keys are stored and released based on some alternative authentication mechanism i.e. password. As shown in Figure 1 if internet users use simple password then it is easy to guess, and they compromise security and complex password which are difficult to remember, and are costly to maintain. Most internet users use the same password across different application, as hacker or impostor after getting a single password can now access multiple applications. So in a multiuser account case, passwords are unable to provide no repudiation.

Password Survey (Nov. 2006)

1. 26%- use common words, dates, phone, address numbers
2. 38%- recycle old passwords
3. 62%- change password only if perceiving a security threat
4. 17%- keep password list on monitor, keyboard or desk drawer.

Need for Security

Security is a major concern with internet users and system administrators find it difficult to protect confidential information in individual files, for which they lock a computer system to unauthorized users. To control access to an intranet or extranet, or conduct business on the Internet, one needs to determine an appropriate level of security and the effective means to achieve the objectives. The threat to internet security is one of the main barriers to electronic transaction.

Internet uses Simple Mail Transfer Protocol (SMTP) to transmit electronic mail and most business transactions. These transmissions have as much privacy as a postcard and travel over insecure, untrusted lines. Anyone anywhere along the transmission path can obtain access to a message and read the contents with a simple text viewer or word processing program. Because the transmission lines are insecure, it is easy to forge e-mail or use another person's name. Theft of identity is becoming the nation's leading incidence of fraud due to which a person can even claim that someone else have sent a message.

Organizations in both the public and the private sectors are well aware of the needs of Internet security that is why they are protecting their Internet data and corporate systems. To provide a secu-