Abstract. Thanks to the widespread success of the Internet, the use of e-mail has become common practice. More and more people are even using it as a primary means of communication. Unfortunately, regular users are not aware of the risks they are facing. If you send a regular letter, you can rely on the confidentiality of its content but not so with plain e-mail. Each message can be intercepted by a trained computer user connected to the net. Indeed in this paper we will show how easy it is to read other people’s e-mail, and even change it without being caught. Thanks to an extensive use of cryptography, we can limit these risks. We will present and analyze an overview of the latest available standards and tools.

1 Introduction

Even in the previous era of central mainframes, there was the possibility of monitoring or active attacks on the serial lines which connected terminals to the central mainframe. However, the move to LANs in general, and Ethernet in particular, has made matters much worse. The Internet is a prime example of this. The attacks are very much easier to carry out on an Ethernet than they were on serial lines. Indeed, these attacks can often be carried out using just software, with no hardware-level interception or modification required.

Tools that are used to check the functionality of the network (LAN analyzers, also known as network sniffers) can also be used to listen in on any traffic on the Internet. Using this software (Esniff is an example of such a public domain tool), it is very easy to read all e-mail messages that pass by your computer. Services such as anonymous remailers make it impossible to track down a message received through one of them. Important e-mail messages can be altered with the use of some hardware. The need for an electronic equivalent of registered mail where you can prove to an arbitrator that the letter was sent and delivered, has become imminent due to the emergence of services as Electronic Commerce.

The rest of the paper is organized as follows. In section 2 we will describe the basic cryptographic protocol used by most of the available tools for securing Internet e-mail. Section 3 will elaborate on some of the vocabulary used in the
Internet security sector. An overview of the available systems and standards will be given in section 4. A commercially available product (CryptMail) that implements most of these standards is detailed in section 5. We will finish with our conclusion.

2 Basic Cryptographic Protocol

The properties of secret key cryptography and public key cryptography are well known [1]. In this real world situation we will combine both in a hybrid system to take advantage of their respective benefits. The basic e-mail scenario is the one illustrated in figure 1. We have two entities taking part in the protocol. We have the sender (A) of the message and the receiver (B). An important aspect is that it is a one step protocol. There is usually no prior interaction between sender and receiver to setup cryptographic keys or to authenticate each other. Basically the services that we want to offer are:

- confidentiality of the message
- authenticity of the receiver/sender of the message
- integrity of the message
- non-repudiation of origin and delivery of the message

![Fig. 1. Secure e-mail scheme](image)

To protect against an intruder listening in on the electronic mail, the message will be enciphered using a symmetric key algorithm. The reason for using symmetric technology is obvious: performance. The key that is used in this way