

# SSARES: Secure Searchable Automated Remote Email Storage<sup>\*†</sup>

Adam J. Aviv

Department of Computer and Information Science  
University of Pennsylvania  
aviv@seas.upenn.edu

Shaya Potter

Department of Computer Science  
Columbia University  
spotter@cs.columbia.edu

Michael E. Locasto

Department of Computer Science  
Columbia University  
locasto@cs.columbia.edu

Angelos D. Keromytis

Department of Computer Science  
Columbia University  
angelos@cs.columbia.edu

## Abstract

*The increasing centralization of networked services places user data at considerable risk. For example, many users store email on remote servers rather than on their local disk. Doing so allows users to gain the benefit of regular backups and remote access, but it also places a great deal of unwarranted trust in the server. Since most email is stored in plaintext, a compromise of the server implies the loss of confidentiality and integrity of the email stored therein. Although users could employ an end-to-end encryption scheme (e.g., PGP), such measures are not widely adopted, require action on the sender side, only provide partial protection (the email headers remain in the clear), and prevent the users from performing some common operations, such as server-side search.*

*To address this problem, we present Secure Searchable Automated Remote Email Storage (SSARES), a novel system that offers a practical approach to both securing remotely stored email and allowing privacy-preserving search of that email collection. Our solution encrypts email (the headers, body, and attachments) as it arrives on the server using public-key encryption. SSARES uses a combination of Identity Based Encryption and Bloom Filters to create a searchable index. This index reveals little information about search keywords and queries, even against adversaries that compromise the server. SSARES remains largely transparent to both the sender and recipient.*

## 1 Introduction

Most email is both sent and stored in a plaintext format. During transmission, encryption standards, such as SSL, can protect a message from eavesdroppers. However, email “at rest” (stored on the server) remains at risk. Servers that store email and provide remote access and easy backups of a user’s mailbox are also trusted to protect the email’s contents; a compromised server implies the compromise of the users’ email, and a user cannot easily prevent such a situation. Even though email content can be secured using public-key encryption (e.g., PGP), this solution alone is not viable for two reasons. First, PGP preserves the headers of the email so that the message can be properly delivered. Consequently, an attacker can still partially compromise the users’ privacy by determining who the user is communicating with. More importantly, PGP-style protection relies on the correspondents actively employing the tool. Unfortunately, the use of public-key encryption is not widespread among the general public.

The first step toward a solution to the email “at rest” problem involves the construction of an email system that provides confidentiality protection without the direct interaction of the user. Having a transparent procedure would allow for the average user to not change his/her normal email practices while still being assured of the protection provided. Incoming email can be completely encrypted on the email server as it arrives. More precisely, the email body, headers, and attachments are entirely encrypted using a RSA-style public key so that once encrypted, the email can not be read except by the appropriate recipient. Doing so assures that, regardless of who the sender is, the content will be protected once it arrives. The users’ email practices need not change, and they do not need to convince their correspondents to alter theirs.

---

<sup>\*</sup>This work was partially supported by the National Science Foundation through Grant ITR CNS-04-26623.

<sup>†</sup>all work done at the Network Security Lab at Columbia University Department of Computer Science

















