By its nature, email has a tendency to stay on a mail provider’s servers for long periods of time. In fact, this behavior is desirable in that it enables access to messages on an account from multiple devices. While the user may trust the provider or the provider’s policies, there is potential for a “curious observer” to view private messages—someone who, while not necessarily malicious, is curious enough to violate policy (or is otherwise put in a position to see those messages).

Legacy email, the collected archives of mail already received by the provider, stays at the provider for a long time, thus increasing its exposure to curious observers.

**Goals**

- To create a system for enabling email providers to encrypt mail on receipt of messages.
- To allow a wide variety of clients to access the messages, even if the clients do not necessarily support message decryption.
- Both of the above should protect legacy email from a “curious observer” at the provider’s servers for extended periods of time.

**Protection Analysis**

This approach provides security against a “curious observer.” An adversary who could violate the policies of the provider would be able to siphon plaintext messages as they were received, for example. Thus if the users’ trust in their provider were violated, legacy email would still be protected, but future email could be compromised.

The content filter uses the GNU Privacy Guard (GPG) software to perform its encryption, using the public keys of the recipients. This provides strong encryption against active adversaries. It also increases the control the user has over the retention of old messages.

The offlineimap system requires a trusted server, such as a local computer running the software with only the IMAPS port open to the Internet (or only open to the local network).

**Implementation**

An after-queue content filter for the mail transfer agent postfix is used to encrypt messages at an email provider prior to delivery to the mailbox as per PGP/MIME and the OpenPGP specification. While many Mail User Agents (MUAs) support the PGP/MIME format, devices such as the iPhone and the current trunk of K-9 (the development branch of the Android MUA) do not currently offer PGP support. A modification to offlineimap, an IMAP synchronization program, automatically decrypts messages encrypted by the provider’s content filter. This allows a user to set up a local trusted IMAP server to provide access to various devices.

**Related Work and Further Issues**

Usable and effective public key distribution is a topic of open research. An ideal system of email encryption would involve true end-to-end encryption. This would also allow digital signatures on all email, something that this system does not address.

Use of a system such as the one described requires trust in the provider, and well-defined policies. Possible legal requirements for data retention are not addressed by this system, although they raise issues similar to those of curious observers.