USABLE SECURE WEBMAIL

Kent Seamons
Computer Science Department
Brigham Young University
Director, Internet Security Research Lab

Webmail

Problem

- Sent in the clear
- Available to the provider

Gmail by Google

YAHOO! MAIL

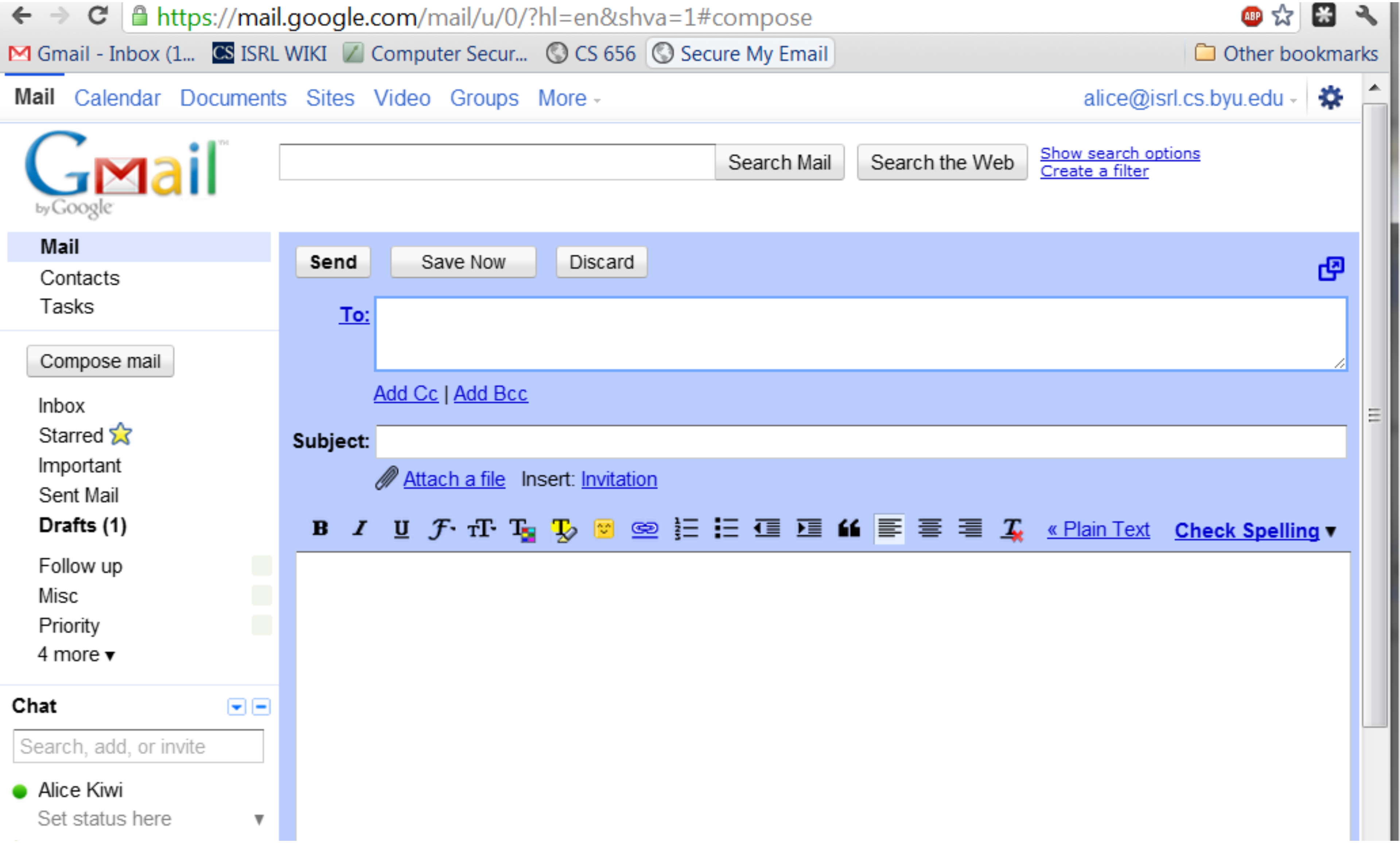
Windows Live Hotmail

Solution

- Familiar interface
- Easy deployment
- Key management

Kiwi

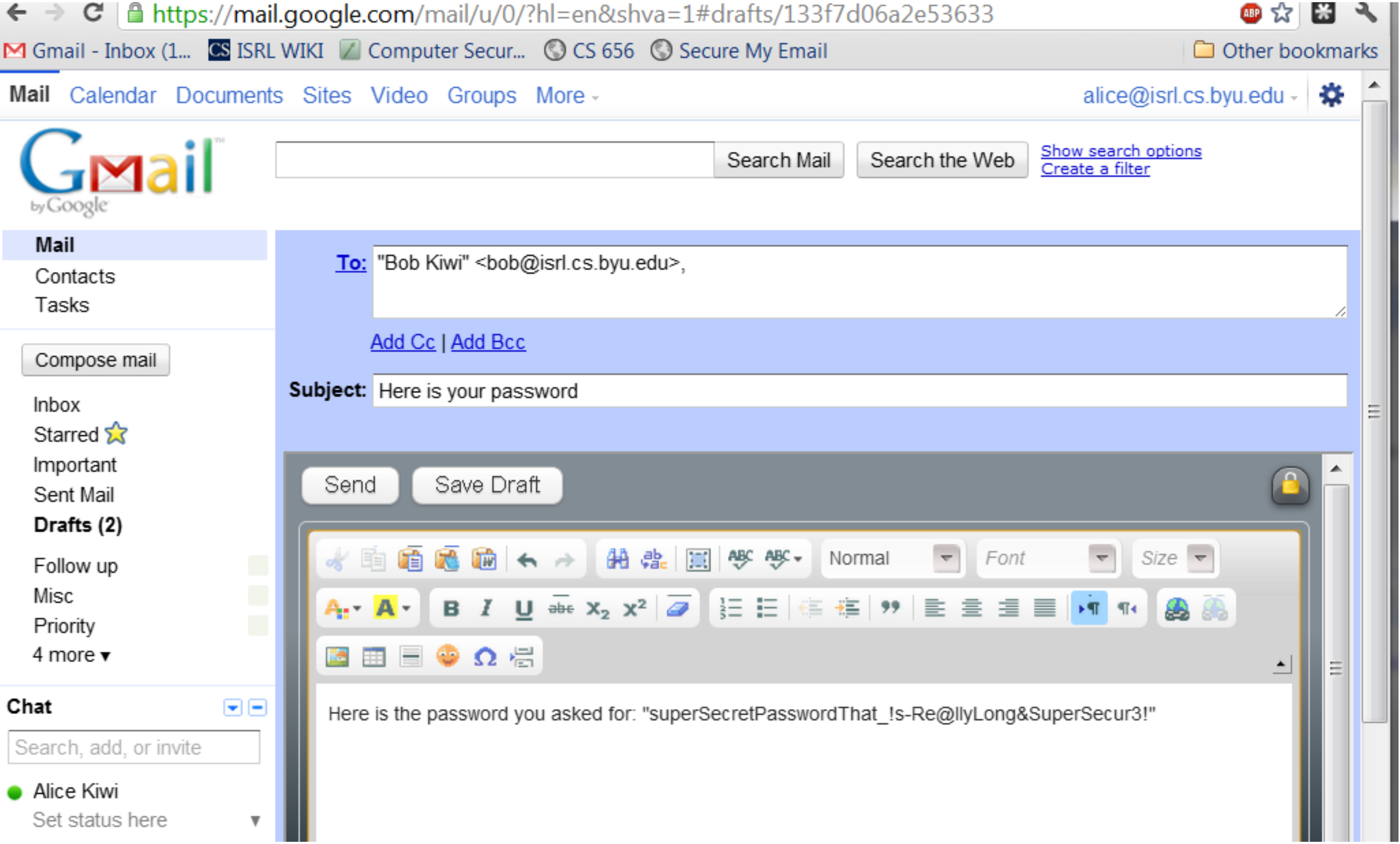
- Secure Overlays
  - Existing email clients
  - Plaintext not accessible to email provider
- Easy deployment
  - No setup between the sender and recipient
  - Browser bookmarklet or plugin
- Key management
  - Key escrow
  - Symmetric key system



https://mail.google.com/mail/u/0/?hl=en&shva=1#compose

alice@isrl.cs.byu.edu

● Alice Kiwi

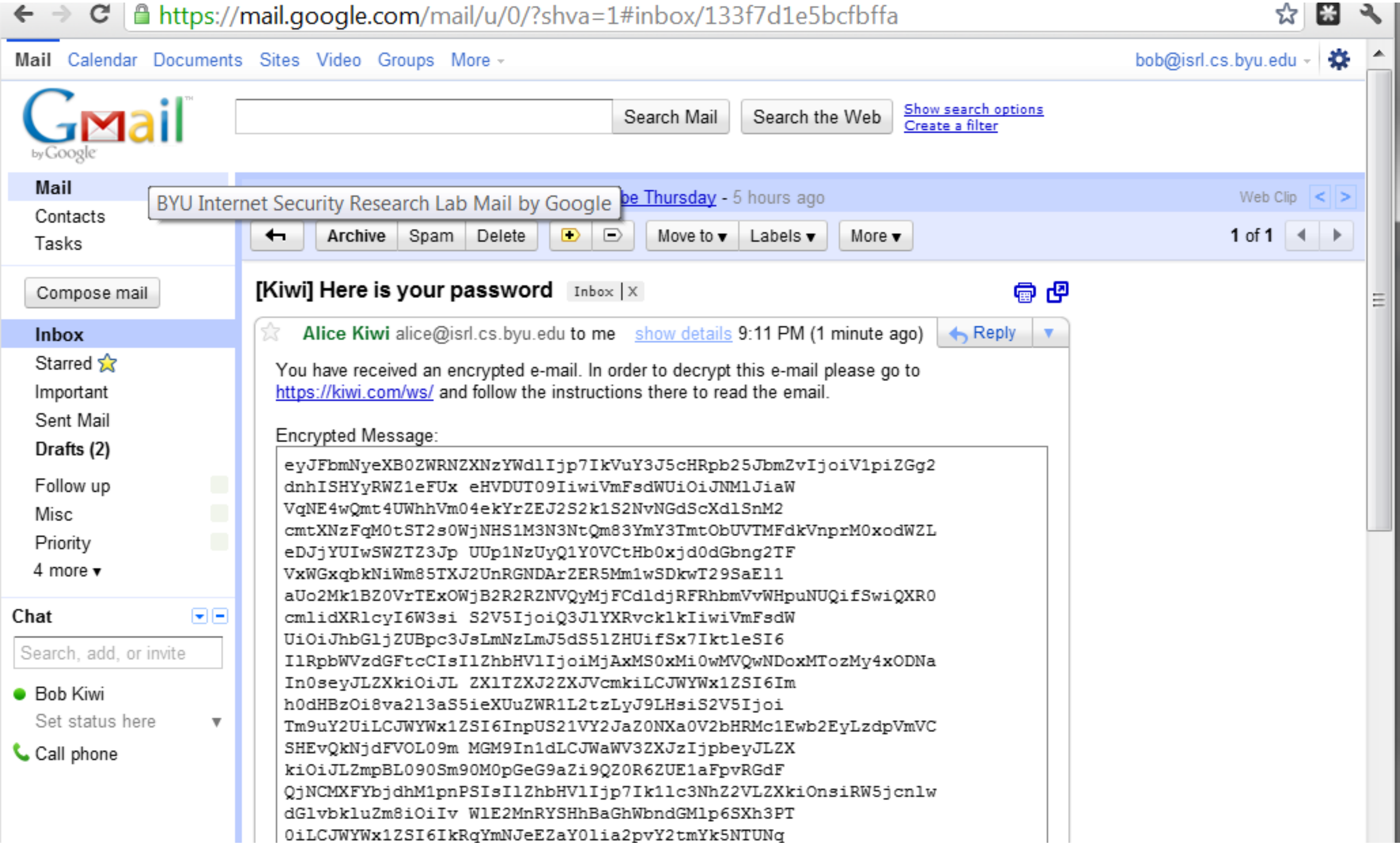


https://mail.google.com/mail/u/0/?hl=en&shva=1#drafts/133f7d06a2e53633

To: "Bob Kiwi" <bob@isrl.cs.byu.edu>,

Subject: Here is your password

Here is the password you asked for: "superSecretPasswordThat_!s-Re@llyLong&SuperSecur3!"



[Kiwi] Here is your password

Alice Kiwi alice@isrl.cs.byu.edu to me 9:11 PM (1 minute ago)

You have received an encrypted e-mail. In order to decrypt this e-mail please go to https://kiwi.com/ws/ and follow the instructions there to read the email.

Encrypted Message:

eyJFbmNyeXB0ZWRNZXNzYWdlIjp7IkVuY3J5cHRpb25JbmZvIjoiV1piZGg2
dnhISHYyRWZ1eFUx eHVDUT09IiwiVmFsdWUiOiJNMlJiaW
VqNE4wQmt4UWhhVm04ekYrZEJ2S2k1S2NvNGdScXdlSnM2
cmtXNzFqM0tST2s0WjNHS1M3N3NtQm83YmY3TmtObUVTMFdkVnprM0xodWZL
eDJjYUIwSWZTZ3Jp UUp1NzUyQ1Y0VCtHb0xjd0dGbng2TF
VxWGxqbkNiWm85TXJ2UnRGNDArZER5Mm1wSDkwT29SaEl1
aUo2Mk1BZ0VrTExOWjB2R2RZNVQyMjFCdldjRFRhbmVvWHpuNUQifSwiQXR0
cmlidXRlcyI6W3si S2V5IjoiQ3JlYXRvcklkIiwiVmFsdW
UiOiJhbGljZUBpc3JsLmNzLmJ5dS5lZHUifSx7IktleSI6
IlRpbWVzdGFtcCIsIlZhbHVlIjoiMjAxMS0xMi0wMVQwNDoxMTozMy4xODNa
In0seyJLZXkiOiJL ZXlTZXJ2ZXJVcmkiLCJWYWx1ZSI6Im
h0dHBzOi8va2l3aS5ieXUuZWR1L2tzLyJ9LHsiS2V5Ijoi
Tm9uY2UiLCJWYWx1ZSI6InpUS21VY2JaZ0NXa0V2bHRMc1Ewb2EyLzdpVmVC
SHEvQkNjdFVOL09m MGM9In1dLCJWaWV3ZXJzIjpbeyJLZX
kiOiJLZmpBL090Sm90M0pGeG9aZi9QZ0R6ZUE1aFpvRGdF
QjNCMXFYbjdhM1pnPSIsIlZhbHVlIjp7Ik1lc3NhZ2VLZXkiOnsiRW5jcnlw
dGlvbkluZm8iOiIv W1E2MnRYSHhBaGhWbndGMlp6SXh3PT
0iLCJWYWx1ZSI6IkRqYmNJeEZaY0lia2pvY2tmYk5NTUNq

Future Work

- Usability studies
  - How usable and effective is a bookmarklet compared to a plug-in?
  - How will a user trust the initial encrypted message?
    - Spear phishing problem turned on its head
    - Personalized greeting to motivate receiver to install the bookmarklet
- Security analysis
- Key management comparison
- Standard Webmail API
  - Too difficult to stay up-to-date with webmail client changes
  - Attachments difficult to support