USABLE SECURE WEBMAIL

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

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Sent in the clear</td>
<td>• Familiar interface</td>
</tr>
<tr>
<td>• Available to the provider</td>
<td>• Easy deployment</td>
</tr>
<tr>
<td></td>
<td>• Key management</td>
</tr>
</tbody>
</table>

- Gmail
- Yahoo Mail
- Windows Live Hotmail
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
To: "Bob Kiwi" <bob@isrl.cs.byu.edu>,

Subject: Here is your password

Here is the password you asked for: "superSecretPasswordThat_Is-Re@llyLong&SuperSecur3!"
[Kiwi] Here is your password

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:

eyJFbmNyeXB0ZWRNZXzYjWdlIj7IkVvY3J5cHRpb25JbmZ2vIjoiVlpiZGg2
dnhISYyRWZ1eFUXeHVDUT09IiwiVmsWdWU1ciJMN1J1aW
VqNE4wQm4t4UWhV0m4ekYrZEJZS2k1S2NyNGdScXdlSnM2
cmtXNZFgM0tST2s0WjNH51M3N3NtQm83Ym93MtcOBUVTMFdkVnprM0xodWZL
eDJjYUIwSW2TZ3JpUUp1NzUyQ1Y0VChb0xj0dGbnq2TF
VxWQxgbkNiM85TZj2UNrRGNDaEZERSMm1w5DkwT29sE11
aUo2Mk1B0VrTEoxQjB2R2ZNVQyMjFc1djRFhbmVvWWhpNUQifSwiQX0
clmidXRlcj6W3siS2V5IjoiQ3J1YXRvcklKIiwiVmsWdW
UiO1JhbGljZUBpc3JpZnMzLm5dS1ZHUifSx7IktleSI6
IIlRpbWNzdGFtcCiliI2ZhbHVlIjoiMjAxM0x0MiwvMjQwNDoxMTozMy4xODnA
InOseyJLZXkiOlJLZXI2JXVcmkLCJWYWx1ZSI6I
h0DBzoi8va213aS5iXUuZWR1IltzLyJ9LHsiS2V5Ijoi
Tm9uYUliCJWYWx1ZSI6InpUS12YJ2a20NXa0V2bHRCm1Ewb2EyLzdpVmVC
SHEvQknJdFVLO9mMGM9In1dLCJWAwV3ZXJljpbeYLZX
kiO1JjLzmpPBLo90SM0opGeG9aZi9Q20R6UE1aFpvrGdf
QlJNMcXFBjdhM1npPSisIz2hbbHV1Ij7Iklc3NhZ2VLZXkiOnsiRW5jcmlw
dGlvbklu2m8oiIVWlE2MnRYShBaGhWbndGM1p6Sxh3PT
0iLCJWYWx1ZSI6IkRgYmNJeZ2aY0li2pvY2tmYk5NTUNq
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