CS 465 Homework 5: Waterhouse

Sorry for the small text -- Google Docs keeps breaking our layout

Steve Bezek, Alex Lambert

A brief overview

We tested were linking a user's Facebook account to the Waterhouse email system, and judging e-mails' security properties.

We tested two interfaces for linking a user's Facebook account to their Waterhouse account. One used highly technical language when creating the association. The second used informal, non-technical language.

We also tested two interfaces for displaying e-mail security information. As before, one used highly technical language when describing the message's security properties. The second used informal, non-technical language. We also presented the users with a message with no security information (i.e. no Waterhouse-created UI). We asked users about the security properties of a message presented with each of the interfaces.
Subject: Campaign Request

Hi once again! We’re going to be wrapping things up here pretty soon. You’ve been really great so far.

Can you please send a copy of the schedule to Ben Donnelly (ben@campaign.cw.com) and to Sarah Carson (carson@campaign.cw.com)?

Thanks!

---Steve
Dear Campaign Coordinator,

Thanks for your email. It's great that you are settling in. There is chocolate in the file cabinet on your left if you want any. Also, feel free to use the phone for phone calls, but be sure that at least one phone line is available at all times.

In any event, I want you to know that we have finalized the speaking dates for Pennsylvania. Here they are:

- **Monday 10/10**: Harrisburg
  - 9:30am - Rally on the Green. Lots of media attention.
  - Noon - Photo-op at city library.
  - 3:30 - Sit-in at the mayor's office.

- **Saturday 10/15**: Hershey
  - 10:00am - Chocolate factory tour.
  - 6:00pm - Campaign dinner to honor chocolate workers.

- **Tuesday 10/18**: Philadelphia
  - 10:00am - 'Break the bell' at the Liberty Bell.
  - 4:00pm - Constitution 2 at Liberty Hall.

- **Friday 10/21**: Pittsburgh

You can be confident that Steve Beack really sent this message, and that evil hackers can't read it.

Learn more.
Script / Task Narratives

Overview

Thanks for agreeing to take part in our study. To give you a brief overview, today you will be interacting with Waterhouse, a security email system. Waterhouse allows you to send/receive secure email messages with your Facebook friends. Waterhouse uses your Facebook account to verify the identity of your friends.

Description of objectives

Our goal for today is to experiment with different user interfaces to determine which one is the easiest to use and what improvements we need to make. We will be examining the interface for linking a Facebook account to Waterhouse, and the interface for reading email.

Equipment being used

We will be using a web browser in the experiment

Data being collected

We will be recording your reaction to the interface and the feedback you give us.

Additional Info

https://docs.google.com/a/quickfire.org/View?docID=dffpsv9_91hpznrgg&revision=_latest&hgd=1&spi=1
Keep in mind that we are evaluating the interface not you. If you are having issues, it's because the interface was designed poorly, not because of you.
If you are able to talk through what you are thinking that would be very helpful to us.
You are free to quit participating at any time for whatever reason.
Do you have any questions?

First Task
The first task you will be doing is attempting to set up Waterhouse to work with your Facebook account. We have a laptop set up for you. The Waterhouse login screen is already open.
Use the following credentials (We presented these on a piece of paper to the user):
Webmail username: don
Webmail password: 6826C2
Facebook username: don@firstmx.net
Facebook password: 6826C2
Make sure you capitalize the C in the password.

I have some questions for you:
Do you think you successfully set up Waterhouse?
How comfortable were you with this interface?
Do you understand any technical terms that were used?
Were there any confusing aspects of the interface?

Second Task
In the second task, we will have you read an email message and afterwards answer some questions. Here you go.

I have some questions for you:
Do you believe anyone besides Steve could have sent this message?
Do you think someone could have read this message while it was in transit over the internet?
If Steve sent this message from the free wifi at Starbucks and a malicious person at Starbucks wanted to read the message, do you think he'd be able to?
Did you understand any technical terms that were used?

Questionnaire forms
We integrated our questions into our script. Our users were all sophomores living in Scott Hall. They were all Facebook users, but none were very familiar with computer security.

Metrics
A word on quantitative results
We were more interested in qualitative results than in quantitative data. We're not trying to optimize an existing task or improve productivity for a well-known workflow. Instead, we're trying to change our users' perception of security.

We did not see any reasonable or valuable time metrics for the message analysis task, because our task was focused around reading both the message contents and our security text. The time spent reading the message contents dwarfed the time spent reading the security text. Additionally, our users read the message content as well our additional UI -- if we asked them to read only our UI, then our UI additions would be the focus of their attention. Instead, we wanted to paint a more natural scenario, where our UI was secondary to the message itself.

For the account linking task: linking an account is a one-time operation performed after Waterhouse is installed. Additionally, much of the link flow is dictated by Facebook's application security processes; we can only make slight changes to the experience (such as the UI text). Our changes focused, then, on evaluating the UI text and not the productivity or error rates of the users.

Qualitative results
Our qualitative questions are presented in our script.

Results and interpretation
Link with Facebook
When attempting to link with Facebook, each user at least once entered their login information in the upper right corner.

https://docs.google.com/a/quickfire.org/View?docID=ddfpvsf9_91hpznrgg&revision=_latest&hgd=1&spi=1
of the Facebook screen instead of clicking on the "Continue" button. This surprised us, since we would always click on the "Continue" button during testing.

2 of our subjects described the initial screen as confusing because there were two ways of continuing: clicking the "Continue" button, and entering login information.

One of the subjects was confused by the text saying to close the window because he wasn't sure whether he should close the whole window, or close just the tab.

All of the subjects mentioned that they routinely add Facebook applications so they were very familiar with the workflow of authorizing an application. Because of this 2 of the subjects said they only skimmed over the text.

**Email security box**

Overall the users preferred the friendly text. They felt that the technical text seemed like legal terms.

For our question about the email not being from the listed sender, many of the subjects focused on non-technical aspects of security. One subject mentioned that Steve (the person listed as the sender in the emails), could have let his friends use his account, or had his secretary use the account. Another subject examined the content of the email, and thought it was very possible Steve didn't send the email since the email wasn't personalized and started with the generic line "Dear Campaign Coordinator."

All the users had previously heard that email in itself isn't very secure and had a vague notion that other people could potentially read their email. One subject felt that if an email originates at and is delivered to a university, it is more private and exclusive, and thus more secure. He also felt email from Hotmail or Gmail was less secure.

When we displayed the friendly text saying that the message was secure the reactions were mixed. One subject said that because of the security message no one but the listed sender could have sent the message, no one could read it in transit, and that a malicious user at Starbucks couldn't read it. After reading the security text another subject mentioned that there is a little extra assurance that message sender was authentic and that the email couldn't be read, but said it was still possible. The last subject didn't even mention the security text when we asked him to talk about whether he would trust the email or not. After further questioning we found out that he had definitely read the security box but thought that the security box could have come from the sender himself and thus could not be trusted more than normal email. He didn't realize that the box was instead part of the Waterhouse product.

Two of the users liked the technical security message better than the friendly security message. Although they didn't completely understand the message, they recognized some of the terms such as "key" and "encryption" from dealing with setting up WiFi networks. They felt the message with technical terms was much more "legit" than the friendly security message. One of the users felt that the friendly text was "somewhat mocking".

**Visual summary**

Not applicable; see "A word on quantative results"

**Recommendations for improvement**

Our users reminded us that we must analyze security holistically. One of the first reactions I get after telling engineers about Waterhouse is "What if the user's Facebook account is compromised? It's useless then." I tell them that, in that case, all bets are off. Waterhouse doesn't attempt to solve every possible problem -- but neither does anything else. Kerberos is an industry-standard authentication protocol used in many large businesses, governments, and universities. Kerberos handles authentication; it doesn't protect the physical machine from compromise. If an attacker controls the machine, he can steal users' Kerberos passwords; Kerberos doesn't advertise that it prevents this attack, and the potential for the attack that doesn't make it useless. Other security technologies (such as OS integrity checks and a secure attention sequence) work in concert with Kerberos to prevent these attacks. Similarly, the popular SSH remote-access program uses a technique called "imprinting" (or "key continuity management") for its security, but there's no guarantee that the initial authentication is secure. In the real world, though, this imperfect-security solution works very well, it works much better than the no-security solution of unencrypted remote access protocols like Telnet.

After these reflections, we thought about how we'd placed Waterhouse's UI text on the spectrum between presenting strictly technically-correct language and presenting Waterhouse as "magical security dust" that users don't need to understand. We realized that, in revolting against the former's not-useful style, we'd gone to the other extreme in hiding some important details and (as one user put it) "dumbing down" the interface too much. We'll now be looking for a better spot in the middle -- giving users basic information about Waterhouse's purpose and a few details about how it works.

We collected some screenshots of existing browsers' UI warnings; we find these too technical to be useful but closer to the mean we're searching for.
In addition to changing our UI text to be closer to the middle of this spectrum, we'd like to introduce a "ten-second-tour" of Waterhouse. One of our participants theorized about Waterhouse "creating codes" for his friends, and then using those "codes" to verify their identities. (He made an analogy to Nintendo's Wii friend-codes.) This might be abstract enough to give users a better sense about how our system works, while avoiding many technical terms. We're considering using the tour widget on Google's AdWords home page (https://adwords.google.com/select/Login) as a template for our efforts:

The tour widget would be displayed after the initial client setup. A highly condensed, easy-to-follow informational comic book, like the one used to launch Google Chrome (http://www.google.com/googlebooks/chrome/), may also help new users.

In the initial client setup, we never expected users to log in via Facebook's upper-right-corner logon box instead of hitting "Continue". (We didn't even know if this path would work!) Users said they were confused from the presence...
of a "Login" and "Continue" button. To combat this, we're considering changing the association UI to present a box in the middle of the screen with an overview of the setup process and prominent, well-labeled "Continue" buttons. This will draw attention away from the upper-right-corner logon box (though we'll ensure it still continues to work.) We'll style the box to look similar in placement and in style to Facebook's clean, simple, and elegant application logon box: